Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI – Technische Richtlinie

Bezeichnung:	**Kryptographische Verfahren: Empfehlungen und Schlüssellängen**
Kürzel:	BSI TR-02102-1
Version:	2023-01
Stand:	09. Januar 2023

Version	Datum	Änderungen
2017-01	03.01.2017	Grundlegende Überarbeitung des Abschnitts zur Zufallszahlenerzeugung unter Windows. Anpassung des Sicherheitsniveaus der vorliegenden Richtlinie für den Vorhersagezeitraum nach 2022 auf 120 Bits. Entsprechend Anpassung der empfohlenen Schlüssellängen für RSA-Verfahren und DL-Verfahren in endlichen Körpern.
2018-01	15.12.2017	Grundlegende Überarbeitung des Abschnitts zur Primzahlerzeugung. Überarbeitung der Aussagen zur Hashfunktion SHA1 als Reaktion auf die Veröffentlichung einer Kollision für SHA1. Die Dokumentenhistorie wird aus Platzgründen auf die letzten drei Jahre beschränkt.
2019-01	22.02.2019	Aufnahme des CCM-Modus unter die empfohlenen Betriebsarten. Aufnahme des PKCS1.5-Paddings unter die Legacy-Verfahren.
2020-01	24.03.2020	Empfehlung von FrodoKEM und Classic McEliece mit geeigneten Sicherheitsparametern für PQC-Anwendungen zusammen mit einem bisher empfohlenen asymmetrischen Verfahren. Empfehlung von Argon2id für Passwort-Hashing. Übergangsweise Verlängerung der Konformität von RSA-Schlüsseln mit einer Schlüssellänge ab 2000 Bits auf Ende 2023.
2021-01	08.03.2021	Überarbeitung des Kapitels zu Zufallsgeneratoren, insbesondere im Hinblick auf die Verwendung von DRG.3- und NTG.1-Zufallsgeneratoren. PTG.2-Zufallsgeneratoren werden für allgemeine Einsatzzwecke nicht mehr empfohlen. Aufnahme standardisierter Versionen hashbasierter Signaturverfahren.
2022-01	28.01.2022	Grundlegende editorische Überarbeitung des gesamten Textes, geringfügige Anpassungen des Layouts. Aktualisierungen in den Bereichen Seitenkanalanalyse, QKD und Seed-Generierung für Zufallszahlengeneratoren.
2023-01	09.01.2023	Anhebung des Sicherheitsniveaus auf 120 Bit, Aktualisierung im Bereich PQ-Kryptographie.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn, Germany
E-Mail: tr02102@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Tabellenverzeichnis 5

Notationen und Glossar 7

1. Einleitung 17
   - 1.1. Sicherheitsziele und Auswahlkriterien . . . 18
   - 1.2. Allgemeine Hinweise . . . 20
   - 1.3. Kryptographische Hinweise . . . 22
   - 1.4. Implementierungsaspekte . . . 22
   - 1.5. Umgang mit Legacy-Algorithmen . . . 23
   - 1.6. Weitere relevante Aspekte . . . 24

2. Symmetrische Verschlüsselungsverfahren 27
   - 2.1. Blockchiffren . . . 27
     - 2.1.1. Betriebsarten . . . 28
     - 2.1.2. Betriebsbedingungen . . . 29
     - 2.1.3. Paddingverfahren . . . 30
   - 2.2. Stromchiffren . . . 30

3. Asymmetrische Verschlüsselungsverfahren 31
   - 3.1. Asymmetrische Schlüssellängen . . . 33
     - 3.1.1. Allgemeine Vorbemerkungen . . . 33
     - 3.1.2. Schlüssellängen bei langfristig schützenswerten Informationen und in Systemen mit langer vorgesehener Einsatzdauer . . . 35
   - 3.2. Sonstige Bemerkungen . . . 36
     - 3.2.1. Seitenkanalangriffe und Fault-Attacken . . . 36
     - 3.2.2. Public-Key-Infrastrukturen . . . 36
   - 3.3. ECIES-Verschlüsselungsverfahren . . . 37
   - 3.4. DLIES-Verschlüsselungsverfahren . . . 38
   - 3.5. RSA . . . 39

4. Quantensichere Kryptographie 42

5. Hashfunktionen 46

6. Datenauthentisierung 48
   - 6.1. Sicherheitsziele . . . 48
   - 6.2. Message Authentication Code (MAC) . . . 49
   - 6.3. Signaturverfahren . . . 50
     - 6.3.1. RSA . . . 52
     - 6.3.2. Digital Signature Algorithm (DSA) . . . 53
     - 6.3.3. DSA-Varianten basierend auf elliptischen Kurven . . . 53
     - 6.3.4. Merkle-Signaturen . . . 54
     - 6.3.5. Langfristige Beweiswerterhaltung für digitale Signaturen . . . 55

7. Instanzauthentisierung 56
7.1. Symmetrische Verfahren . . . 56
7.2. Asymmetrische Verfahren . . . 57
7.3. Passwortbasierte Verfahren . . . 57
7.3.1. Empfohlene Passwortlängen für den Zugriff auf kryptographische Hardwarekomponenten . . . 57
7.3.2. Empfohlene Verfahren zur Passwort-basierten Authentisierung gegenüber kryptographischen Hardwarekomponenten . . . 58

8. Schlüsseleinigungsverfahren, Schlüsseltransportverfahren und Key-Update 60
8.1. Symmetrische Verfahren . . . 61
8.2. Asymmetrische Verfahren . . . 62
8.2.1. Diffie-Hellman . . . 62
8.2.2. EC Diffie-Hellman . . . 63

9. Secret Sharing 65

10. Zufallszahlengeneratoren 67
10.1. Physikalische Zufallszahlengeneratoren . . . 68
10.2. Deterministische Zufallszahlengeneratoren . . . 70
10.3. Nicht-physikalische nicht-deterministische Zufallszahlengeneratoren . . . 70
10.4. Verschiedene Aspekte . . . 71
10.5. Seedgenerierung für deterministische Zufallszahlengeneratoren . . . 72
10.5.1. GNU/Linux . . . 72
10.5.2. Windows . . . 73

A. Anwendungen kryptographischer Verfahren 75
A.1. Verschlüsselungsverfahren mit Datenauthentisierung . . . 75
A.2. Authentisierte Schlüsselvereinbarung . . . 76
A.2.1. Vorbemerkungen . . . 76
A.2.2. Symmetrische Verfahren . . . 76
A.2.3. Asymmetrische Verfahren . . . 77

B. Zusätzliche Funktionen und Algorithmen 79
B.1. Schlüsselableitung . . . 79
B.1.1. Schlüsselableitung nach Schlüsseleinigung . . . 79
B.1.2. Passwort-basierte Schlüsselableitung . . . 80
B.2. Erzeugung unvorhersagbarer Initialisierungsvektoren . . . 80
B.3. Erzeugung von EC-Systemparametern . . . 81
B.4. Generierung von Zufallszahlen für probabilistische asymmetrische Verfahren . . . 82
B.5. Erzeugung von Primzahlen . . . 83
B.5.1. Vorbemerkungen . . . 83
B.5.2. Verfahren zur Erzeugung von Primzahlen . . . 83
B.5.3. Erzeugung von Primzahlpaaren . . . 85
B.5.4. Hinweise zur Sicherheit der empfohlenen Verfahren . . . 86

C. Protokolle für spezielle kryptographische Anwendungen 88
C.1. SRTP . . . 88

Literaturverzeichnis 90

Tabellenverzeichnis

1.1. Beispiele für Schlüssellängen für ein Sicherheitsniveau von mindestens 120 Bits. . . . 19
1.2. Empfohlene Schlüssellängen für verschiedene kryptographische Verfahren. 19

2.1. Empfohlene Blockchiffren. 27
2.2. Empfohlene Betriebsarten für Blockchiffren. 29
2.3. Empfohlene Paddingverfahren für Blockchiffren. 30

3.1. Empfohlene asymmetrische Verschlüsselungsverfahren sowie Schlüssellängen und normative Referenzen. 32
3.2. Ungefährer Rechenaufwand R (in Vielfachen des Rechenaufwandes für eine einfache kryptographische Operation, zum Beispiel das einmalige Auswertung einer Blockchiffre auf einem Block) für die Berechnung diskreter Logarithmen in elliptischen Kurven (ECDLP) beziehungsweise die Faktorisierung allgemeiner zusammengesetzter Zahlen mit den angegebenen Bitlängen. 35
3.3. Empfohlenes Formatierungsverfahren für den RSA-Verschlüsselungsalgorithmus. . . 40

5.1. Empfohlene Hashfunktionen. 46

6.1. Empfohlene MAC-Verfahren. 50
6.2. Parameter für empfohlene MAC-Verfahren. 51
6.3. Empfohlene Signaturverfahren. 52
6.4. Empfohlene Formatierungsverfahren für den RSA-Signaturalgorithmus. 52
6.5. Empfohlene Signaturverfahren basierend auf elliptischen Kurven. 54

7.1. Schematische Darstellung eines Challenge-Response-Verfahren zur Instanzauthentisierung. 56
7.2. Empfohlene Passwortlängen und Anzahl der Zugriffsversuche für den Zugriffsschutz kryptographischer Komponenten. 57
7.3. Empfohlenes passwortbasiertes Verfahren für den Zugriffsschutz auf kontaktlose Chipkarten. 59

8.1. Empfohlene asymmetrische Schlüsseleinigungsverfahren. 62

9.1. Berechnung der Teilgeheimnisse im Shamir Secret-Sharing-Verfahren. 65
9.2. Zusammensetzen der Teilgeheimnisse im Shamir Secret-Sharing-Verfahren. 66

10.1. Empfohlenes Verfahren zur Seedgenerierung unter GNU/Linux. 72

A.1. Empfohlenes symmetrisches Verfahren zur Schlüsselvereinbarung mit Instanzauthentisierung. 76
A.2. Empfohlene asymmetrische Verfahren zur Schlüsselvereinbarung mit Instanzauthentisierung. 77

B.1. Empfohlenes Verfahren zur Schlüsselableitung. 79
B.2. Empfohlene Verfahren zur Erzeugung unvorhersagbarer Initialisierungsvektoren. . . 80

B.3. Empfohlene EC-Systemparameter für asymmetrische Verfahren, die auf elliptischen Kurven basieren. 81
B.4. Empfohlener probabilistischer Primzahltest. 84

Notationen und Glossar

ggT Der größte gemeinsame Teiler (ggT) (englisch greatest common divisor (gcd)) $\mathrm{ggT}(a, b)$ zweier ganzer Zahlen $a, b \in \mathbb{Z}$ ist diejenige natürliche Zahl mit der Eigenschaft, dass sie sowohl a als auch b teilt und dass jede andere natürliche Zahl, die die Zahlen a und b ebenfalls teilt, bereits Teiler von $\mathrm{ggT}(a, b)$ ist.

$\mathbb{F}_n$ Körper mit n Elementen, auch als Galoiskörper $\mathrm{GF}(n)$ bezeichnet.

$\mathbb{Z}_n$ Ring der Restklassen modulo n in $\mathbb{Z}$, auch als $\mathbb{Z}/n\mathbb{Z}$ bezeichnet.

kgV Das kleinste gemeinsame Vielfache (englisch lowest or least common multiple (lcm)) $\mathrm{kgV}(a, b)$ zweier ganzer Zahlen $a, b \in \mathbb{Z}$ ist die kleinste positive natürliche Zahl, die sowohl Vielfaches von a als auch Vielfaches von b ist.

φ Eulersche Phi-Funktion $\varphi\colon \mathbb{Z} \to \mathbb{Z}$, definiert als $\varphi(n) \coloneqq \mathrm{Card}(\{a \in \mathbb{N}\colon 1 \leq a \leq n,\ \mathrm{ggT}(a, n) = 1\}) = \mathrm{Card}(\mathbb{Z}_n^*)$.

R^* Einheitengruppe des kommutativen Rings R.

Card Anzahl der Elemente $\mathrm{Card}(M)$ (auch $|M|$) einer endlichen Menge M.

Ceiling-Funktion Ceiling-Funktion $\lceil\cdot\rceil\colon \mathbb{R} \to \mathbb{Z}$, definiert als $\lceil x\rceil \coloneqq \min\{z \in \mathbb{Z}\colon z \geq x\}$.

Floor-Funktion Floor-Funktion $\lfloor\cdot\rfloor\colon \mathbb{R} \to \mathbb{Z}$, definiert als $\lfloor x\rfloor \coloneqq \max\{z \in \mathbb{Z}\colon z \leq x\}$.

A

AES Advanced Encryption Standard, von der NIST in FIPS 197 [84] standardisierte Blockchiffre mit einer Blockgröße von 128 Bits. Entsprechend der Länge der verwendeten Schlüssel werden AES-128, AES-192 sowie AES-256 unterschieden. Abgesehen von Related-Key-Angriffen gegen AES-192 und AES-256 sind keine Angriffe gegen AES bekannt, die einen wesentlichen Vorteil gegenüber generischen Angriffen auf Blockchiffren erzeugen.

Asymmetrische Kryptographie Oberbegriff für kryptographische Verfahren, in denen die Ausführung mancher kryptographischer Operationen (etwa die Verschlüsselung einer Nachricht oder die Prüfung einer Signatur) durch Parteien erfolgen kann, die keine geheimen Daten kennen.

Authentication Tag Kryptografische Prüfsumme über Daten, die dem Zweck dient, zufällige Fehler oder absichtliche Veränderungen der Daten aufzuzeigen.

Authentisierte Verschlüsselungsverfahren Verschlüsselungsverfahren, die nicht nur die Vertraulichkeit, sondern auch die Integrität der zu verschlüsselnden Daten schützen.

Authentisierung Verfahren mit dem Ziel der sicheren Identifikation einer Person oder eines informationsverarbeitenden Systems. Im Kontext der vorliegenden Technischen Richtlinie

geht es dabei um Personen oder Systeme, die Quelle oder Ziel einer Kommunikationsverbindung darstellen und die Authentisierung erfolgt unter Ausnutzung eines kryptographischen Geheimnisses.

Authentizität Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit einer Person, eines Systems oder von Daten.

B

Backward Secrecy (eines kryptographischen Protokolls) Auch Future Secrecy oder Post-Compromise Security („Selbstheilung“) genannt, Sicherheitseigenschaft eines kryptographischen Protokolls, welche garantiert, dass verschlüsselte Nachrichten auch dann geheim bleiben, wenn in der Vergangenheit ein Schlüssel kompromittiert wurde.

Betriebsmodus einer Blockchiffre Ein Betriebsmodus oder eine Betriebsart ist ein Verfahren, das beschreibt, wie mit einer Blockchiffre Nachrichten verschlüsselt werden. Erst die Kombination von Blockchiffre und Betriebsmodus erlaubt es, Nachrichten zu verschlüsseln, die länger als die Blocklänge sind. Üblicherweise wird dazu die Nachricht in mehrere Blöcke aufgeteilt und durch sogenanntes Padding auf eine passende Länge gebracht. Ein Initialisierungsvektor kann das Verfahren zusätzlich unabhängig vom verwendeten Schlüssel randomisieren.

Blockchiffre Schlüsselabhängige, effizient berechenbare, umkehrbare Abbildung, die Klartexte einer festen gegebenen Bitlänge n auf Chiffrate der gleichen Länge abbildet. Ohne Kenntnis des Schlüssels sollte es nicht praktisch möglich sein, die Ausgabe der Blockchiffre von der Ausgabe einer zufällig gewählten bijektiven Abbildung zu unterscheiden.

Brute-Force-Angriff Wörtlich Methode der rohen Gewalt, auch Exhaustionsmethode (kurz Exhaustion); Angriffsmethode, die auf einem automatisierten, oftmals systematischen Ausprobieren aller möglichen Fälle beruht, um beispielsweise geheime Schlüssel oder Passwörter zu ermitteln. Bei Verwendung ausreichend langer Schlüssel sind Angriffe dieser Art auf moderne Verschlüsselungsalgorithmen in der Praxis aussichtslos, da der erforderliche Rechenaufwand (und damit der Zeit- und/oder Kostenaufwand) zu groß wäre. Da die Leistung moderner Hardware kontinuierlich steigt und sich der Zeitaufwand für das Durchprobieren aller Schlüssel einer bestimmten Länge dadurch reduziert, muss die minimale Schlüssellänge ausreichend groß gewählt und regelmäßig angehoben werden, um Angriffen durch vollständige Exhaustion vorzubeugen.

C

Challenge-Response-Verfahren Ein Challenge-Response-Verfahren (übersetzt etwa Aufforderung-Antwort-Verfahren) ist ein Verfahren zur Authentifizierung eines Gegenübers auf Basis von Wissen. Hierbei stellt ein Prüfender eine Aufgabe (englisch challenge), die der Beweisende lösen muss (englisch response), um nachzuweisen, dass er eine bestimmte Information kennt, ohne diese Information selbst preiszugeben.

Chinesischer Restsatz (Chinese Remainder Theorem, CRT) Satz über Lösbarkeit und Eindeutigkeit der Lösungen von Kongruenzsystemen. Es seien $n_1, \ldots, n_k \in \mathbb{N}$ paarweise teilerfremde, natürliche Zahlen, $n \coloneqq n_1 \cdot \ldots \cdot n_k$ deren Produkt und $a_1, \ldots, a_k \in \mathbb{Z}$ beliebig. Dann

besitzt das System von Kongruenzen

$$\begin{aligned} x &= a_1 \bmod n_1, \\ &\vdots \\ x &= a_k \bmod n_k \end{aligned}$$

genau eine Lösung $x \in \{0, \ldots, n-1\}$.

Chosen-Ciphertext-Attacke Kryptographischer Angriff, in dem der Angreifer Zugriff auf Klartexte zu von ihm gewählten Chiffraten erhalten kann. Das Ziel des Angreifers ist es in der Regel, ein gegebenes Chiffrat zu dechiffrieren, das zu keinem dieser Klar-Geheim-Kompromisse gehört. Abhängig davon, ob der Angreifer dieses Chiffrat vor oder nach dem Ende des Angriffes kennt, unterscheidet man zwischen adaptiven und nicht-adaptiven Chosen-Ciphertext-Attacken.

Chosen-Plaintext-Attacke Kryptographischer Angriff, in dem der Angreifer Zugriff auf Chiffrate zu von ihm gewählten Klartexten erhalten kann.

Cipher Block Chaining Mode (CBC-Modus) Betriebsart einer Blockchiffren, bei der ein Klartextblock vor dem Verschlüsseln mit dem im vorhergehenden Schritt erzeugten Geheimtextblock per XOR verknüpft wird. Für eine sichere Verwendung dürfen nur unvorhersagbare Initialisierungsvektoren wie beispielsweise eine Zufallszahl zum Einsatz kommen.

Counter Mode (CTR-Modus) Betriebsart, in der Blockchiffren betrieben werden können, um aus ihnen eine Stromchiffre zu erzeugen. Hierbei wird ein erzeugter Geheimtextblock mittels XOR mit dem Klartext kombiniert. Die Besonderheit des Counter Mode im Vergleich zu anderen Betriebsarten stellt die Tatsache dar, dass der Initialisierungsvektor aus einer für jedes Chiffrat neu zu wählenden Nonce verknüpft mit einem Zähler besteht, der mit jedem weiteren Block hochgezählt wird. Die Verknüpfung kann zum Beispiel durch Konkatenation, Addition oder XOR erfolgen.

Counter with Cipher Block Chaining Mode (Counter with CBC-MAC, CCM-Modus) Betriebsart einer Blockchiffre, die den den Counter Mode zur Verschlüsselung mit dem CBC-MAC-Modus zur Integritätssicherung kombiniert und somit aus einer Blockchiffre ein Authenticated-Encryption-Verfahren macht, das in der Lage ist, sowohl Vertraulichkeit als auch Integrität zu garantieren. Beim CCM ist darauf zu achten, dass ein Initialisierungsvektor nicht zweimal mit dem gleichen Schlüssel verwendet werden darf, da der CCM von Counter Mode abgeleitet ist und letzterer eine Stromchiffre darstellt.

D

Datenauthentisierung Schutz der Integrität einer Nachricht durch kryptographische Verfahren.

Diffie-Hellman-Problem (DH) Problem der Berechnung von g^{ab} gegeben g, g^a, g^b in einer durch $g \in G$ erzeugten zyklischen Gruppe G. Die Schwierigkeit dieses Problems ist abhängig von der Darstellung der Gruppe. Das DH-Problem ist leicht lösbar für Angreifer, die diskrete Logarithmen in G berechnen können.

Diskreter-Logarithmus-Problem (DL) Problem der Berechnung von d gegeben g^d in einer durch $g \in G$ erzeugten zyklischen Gruppe G. Die Schwierigkeit dieses Problems ist abhängig von der Darstellung der Gruppe.

DLIES Discrete Logarithm Integrated Encryption Scheme, hybrides authentisiertes Verschlüsselungsverfahren auf DH-Basis in $\mathbb{F}_p^*$.

E

ECIES Elliptic Curve Integrated Encryption Scheme, hybrides authentisiertes Verschlüsselungsverfahren auf DH-Basis in elliptischen Kurven.

Einwegfunktion Mathematische Funktion, die „leicht“ berechenbar, aber „schwer“ umzukehren ist. An dieser Stelle sind die Begriffe leicht und schwer im komplexitätstheoretischen Sinne zu verstehen, insbesondere im Kontext der Lösung von Problemen in polynomieller Zeit. In einem erweiterten Sinn werden auch Funktionen so bezeichnet, zu denen bisher keine in angemessener Zeit praktisch ausführbare Umkehrung bekannt ist. Eine Einwegpermutation ist eine Einwegfunktion, die gleichzeitig eine Permutation ist, das heißt, eine bijektive Einwegfunktion. Trapdoorfunktionen, auch Trapdoor-Einwegfunktionen oder Falltürfunktionen genannt, sowie Falltürpermutationen stellen eine spezielle Art von Einwegfunktionen dar. Sie lassen sich nur dann effizient umkehren, wenn man eine gewisse Zusatzinformation besitzt. Falltürfunktionen kommen in asymmetrischen Verschlüsselungsverfahren wie zum Beispiel RSA zum Einsatz.

EME-OAEP Encoding Method for Encryption-Optimal Asymmetric Encryption Padding, Padding Verfahren für RSA, siehe auch OAEP.

Ephemeralschlüssel Ein kryptographischer Schlüssel wird als ephemeral (kurzlebig) bezeichnet, wenn er für jede Ausführung eines kryptografischen Protokolls (zum Beispiel Schlüsselaushandlung, Signaturerzeugung) neu generiert wird. Je nach Anwendung können weitere Anforderungen an den jeweiligen Schlüsseltyps gestellt werden, darunter Eindeutigkeit je Nachricht oder Sitzung.

F

Faktorisierungsproblem Aufgabenstellung aus der Zahlentheorie, bei der eine zusammengesetzte Zahl in das Produkt ihrer Primfaktoren zerlegt beziehungsweise allgemeiner ein nichttrivialer Teiler bestimmt werden soll.

Falltürfunktion, Falltürpermutation Siehe Einwegfunktion.

Fault-Attacke Angriff auf ein kryptographisches System, in dem der Angreifer eine fehlerhafte Ausführung einer kryptographischen Operation nutzt beziehungsweise aktiv hervorruft.

Festplattenverschlüsselung Vollständige Verschlüsselung eines Datenträgers mit dem Ziel, dass aus dem verschlüsselten System zumindest in abgeschaltetem Zustand keine vertraulichen Informationen ausgelesen werden können.

Forward Secrecy (eines deterministischen Zufallszahlengenerators) Sicherheitseigenschaft eines deterministischen Zufallsgenerators, die besagt, dass künftige Ausgabewerte des Zufallsgenerators nicht mit mehr als vernachlässigbarem Vorteil vorhergesagt werden können durch Angreifer, die nur frühere Ausgabewerte des Zufallsgenerators, aber nicht dessen inneren Zustand kennen und deren Rechenleistung sich unterhalb einer Schranke bewegt, die durch das Sicherheitsniveau des deterministischen Zufallsgenerators gegeben ist [29].

Forward Secrecy (eines kryptographischen Protokolls) Sicherheitseigenschaft eines kryptographischen Protokolls, die besagt, dass eine Preisgabe kryptographischer Langzeitgeheimnisse es einem Angreifer nicht möglich macht, vergangene Sitzungen des Protokolls zu kompromittieren [44]. Es ist zu beachten, dass für ein beliebiges Protokoll Forward Secrecy nur dann erfüllt sein kann, wenn bei der Erzeugung der Ephemeralschlüssel innerhalb des Protokolls ein Zufallsgenerator eingesetzt wurde, der mindestens Enhanced Backward Secrecy nach [29] garantiert. Sollen darüber hinaus nicht durch einen Angreifer manipulierte *künftige* Sitzungen im Fall einer Kompromittierung aller langfristigen Geheimnisse geschützt bleiben, muss bei der Erzeugung der Ephemeralschlüssel ein Zufallsgenerator eingesetzt werden, der zusätzlich Enhanced Forward Secrecy [29] bietet.

G

GCM Galois Counter Mode, ein Betriebsmodus für Blockchiffren, der aus der Blockchiffre ein authentisiertes Verschlüsselungsverfahren konstruiert und die Authentisierung nichtverschlüsselter Daten unterstützt.

Geburtstagsparadoxon Unter Geburtstagsparadoxon (auch Geburtstagsproblem) wird das Phänomen verstanden, dass bestimmte Wahrscheinlichkeiten intuitiv häufig falsch geschätzt werden. So liegt die Wahrscheinlichkeit, dass bei 23 Personen mindestens zwei von ihnen am gleichen Tag im Jahr Geburtstag haben, bei über 50%, was von den meisten Menschen um eine Zehnerpotenz falsch eingeschätzt wird. Dieser Effekt spielt im Kontext der Kryptographie unter anderem bei kryptographischen Hashfunktionen eine Rolle, die einen eindeutigen Prüfwert aus einer Eingabe berechnen sollen. Es ist dabei viel einfacher, zwei zufällige Eingaben zu finden, die denselben Prüfwert haben, als zu einer vorgegebenen Eingabe eine weitere zu finden, die denselben Prüfwert aufweist (siehe auch Kollisionsangriff).

Gleichverteilung Im Kontext dieser Technischen Richtlinie bedeutet *gleichverteilte* Erzeugung einer Zufallszahl aus einer Grundmenge M, dass der erzeugende Prozess praktisch nicht von einer ideal zufälligen (also von einer echt zufälligen, gleichverteilten, unabhängigen) Ziehung von Elementen aus M unterschieden werden kann.

GMAC Message Authentication Code, der sich aus einer Verwendung des GCM ohne zu verschlüsselnde Daten ergibt.

H

Hashfunktion Funktion $h\colon M \to N$, die effizient berechenbar ist und für die M deutlich größer ist als N. Der Ausgabewert einer Hashfunktion wird als Hashwert oder kurz als Hash bezeichnet. Ist h sowohl kollisionsresistent als auch resistent gegen Berechnung erster und zweiter Urbilder, so heißt h *kryptographische* Hashfunktion. Sofern nicht anders angegeben bezeichnet der Begriff *Hashfunktion* in der vorliegenden Technischen Richtlinie eine kryptographische Hashfunktion.

Hybrides Verschlüsselungsverfahren Verschlüsselungsverfahren, das Public-Key-Kryptographie zum Schlüsseltransport für ein symmetrisches Verschlüsselungsverfahren nutzt, das im Anschluss zur Verschlüsselung der Nachricht verwendet wird.

I

Informationstheoretische Sicherheit Ein kryptographisches Verfahren heißt *informationstheoretisch sicher*, wenn jeder Angreifer bei dem Versuch, das Verfahren zu brechen, an *Mangel an Information* scheitert. In diesem Fall wird das Sicherheitsziel Vertraulichkeit unabhängig von der dem Angreifer zur Verfügung stehenden Rechenleistung erreicht, solange die Annahmen über die dem Angreifer zugänglichen Informationen über das System zutreffend sind. Es existieren informationstheoretisch sichere Verfahren in vielen Bereichen der Kryptographie, zum Beispiel zur Verschlüsselung von Daten (One Time Pad), zur Authentisierung von Daten (Wegman-Carter-MAC), oder im Bereich Secret Sharing (Shamir Secret Sharing, siehe auch Kapitel 9). In der Regel gibt es in Verfahren dieser Art *keinerlei* Sicherheitsgarantien, wenn die Einsatzvoraussetzungen des Verfahrens nicht exakt erfüllt sind.

Initialisierungsvektor (IV) Ein Initialisierungsvektor ist eine Eingabe in ein kryptographisches Primitiv, die zur Herstellung eines initialen Zustandes verwendet wird. Üblicherweise müssen Initialisierungsvektoren (pseudo-) zufällig sein, in manchen Anwendungsfällen genügt es hingegen auch, wenn sie unvorhersagbar sind oder sich nicht wiederholen.

Instanzauthentisierung Nachweis des Besitzes eines Geheimnisses durch einen Benutzer oder ein informationsverarbeitendes System gegenüber einer anderen Stelle.

Integrität Sicherheitsziel der Bindung des verändernden Zugriffs auf eine Information an das Recht zur Veränderung der Information. Im kryptographischen Kontext bedeutet dies, dass eine Nachricht nur unter Verwendung eines bestimmten geheimen kryptographischen Schlüssel unbemerkt verändert werden kann.

K

Kollisionsangriff Ein Kollisionsangriff ist ein Angriff auf eine kryptographische Hashfunktion mit dem Ziel, zwei verschiedene Eingabewerte zu finden, die auf einen identischen Hashwert abgebildet werden. Im Gegensatz zu Preimage-Angriffen sind dabei beide Eingabewerte (und damit auch der Hashwert) frei wählbar.

Kollisionsresistenz Eine Funktion $h\colon M \to N$ heißt kollisionsresistent, wenn es praktisch unmöglich ist, $x, y \in M$, $x \neq y$ zu finden mit $h(x) = h(y)$.

Kryptoagilität Ein Kryptosystem gilt als kryptoagil, wenn es durch ein anderes Kryptosystem (zum Beispiel in Bezug auf kryptografische Algorithmen, Schlüssellängen, Schlüsselgenerierungsverfahren, technische Umsetzung...) ersetzt werden kann, ohne dass wesentliche Änderungen am Rest des Gesamtsystems vorgenommen werden müssen.

M

MAC Message Authentication Code, schlüsselabhängige kryptographische Prüfsumme. Ohne Kenntnis des Schlüssels sollte es einem Angreifer praktisch nicht möglich sein, die MACs von sich nicht wiederholenden Nachrichten von Zufallsdaten zu unterscheiden. Erfolgreiche Fälschungen von Tags sind in diesem Fall für keinen Angreifer mit einer Wahrscheinlichkeit deutlich über 2^{-t} möglich, wobei t die Länge der Authentisierungs-Tags bezeichnet. Vorgaben zur Länge von t sind stark anwendungsabhängig.

Man-in-the-Middle-Angriff Angriffsart, bei der sich ein Angreifer unbemerkt entweder physisch oder – heutzutage meist – logisch zwischen zwei oder mehrere Kommunikationspartnern einklinkt, um beispielsweise Informationen mitzulesen oder zu manipulieren. Der Angreifer begibt sich also „in die Mitte“ der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt.

Min-Entropie Die Min-Entropie einer diskreten Zufallsvariablen X ist definiert als $-\log_2(p)$, wo p die Wahrscheinlichkeit des wahrscheinlichsten Wertes für X bezeichnet.

N

Nonce Eine (kryptographische) Nonce ist eine beliebige Zeichenfolge, die nur einmal in einer kryptographischen Kommunikation verwendet werden darf. Es handelt sich häufig um eine Zufalls- oder Pseudozufallszahl, die in ein Authentifizierungsprotokoll integriert wird, um zu verhindern, dass vorherige Kommunikation für Replay-Angriffe ausgenutzt werden kann. Ferner werden Noncen häufig als Initialisierungsvektoren und in kryptografischen Hash-Funktionen genutzt.

O

OAEP Optimal Asymmetric Encryption Padding, auf Deutsch etwa Optimales asymmetrisches Verschlüsselungs-Padding; Paddingverfahren, das oft im Zusammenhang mit RSA verwendet wird. Das OAEP stellt eine spezielle Form eines Feistel Netzwerks dar, mit dem im Random-Oracle-Modell ein Verschlüsselungsverfahren aus beliebigen Falltürpermutationen konstruiert werden kann, welches semantisch sicher gegen Chosen-Plaintext-Attacken sind. Wenn OAEP zusammen mit der Falltürpermutation RSA verwendet wird, ist das resultierende Verfahren ferner sicher gegen Chosen-Ciphertext-Attacken. Im allgemeinen erfüllt ein OAEP die beiden folgenden Ziele: Es randomisiert ein ansonsten deterministisches Verschlüsselungsverfahren und beugt einer partiellen Entschlüsselung von Chiffraten (oder einer anderen Form des Informationsabflusses) vor, indem es sicherstellt, dass ein Gegner keine Teile des Klartextes rekonstruieren kann, ohne in der Lage zu sein, die Falltürpermutation zu invertieren.

P

Padding Bezeichnung für das Auffüllen von Nachrichten mit Fülldaten, bevor sie verschlüsselt werden. Padding dient überwiegend dazu, vorhandene Daten in die Gestalt einer durch einen Algorithmus oder ein Protokoll vorgegebenen Struktur zu bringen, das Ergebnis (zum Beispiel den Chiffretext oder die digitale Signatur) einer Verschlüsselung/Signatur zu randomisieren oder Anfang und Ende des Inhalts eines versandten Chiffrats zu verschleiern.

Partitionsverschlüsselung Partitionsverschlüsselung bezeichnet die vollständige Verschlüsselung einer Partition eines Datenträgers. Die eingesetzten Verfahren ähneln denen zur Festplattenverschlüsselung.

Pepper Geheime, von einem Server gewählte Zeichenfolge, die vor Berechnung eines Hashwertes an ein Passwort angehängt wird, um Wörterbuch- und Brute-Force-Angriffe weiter zu erschweren, wird von NIST auch als *secret salt* bezeichnet. Der Pepper wird nicht in derselben Datenbank gespeichert wie der Hashwert, sondern an einem anderen, möglichst sicheren Ort hinterlegt.

Personal Identification Number (PIN) Unter einer PIN wird im Kontext dieser Technischen Richtlinie ein nur aus den Ziffern 0-9 bestehendes Passwort verstanden.

Pseudozufällige Funktion (Pseudo Random Function, PRF) Familie von deterministischen, effizient berechenbaren Funktionen, die von einem Zufallsorakel praktisch ununterscheidbar sind.

Public-Key-Infrastruktur System, das digitale Zertifikate ausstellen, verteilen, speichern, prüfen und widerrufen kann und insbesondere zur Verwaltung von öffentlichen Schlüsseln (Public Keys) im Rahmen asymmetrischer kryptographischer Verfahren zum Einsatz kommt.

Public-Key-Kryptographie Siehe Asymmetrische Kryptographie.

R

Random Oracle, Random-Oracle-Modell Siehe Zufallsorakel.

Regenbogentabelle (Rainbow Table) Datenstruktur, die eine schnelle, speichereffiziente Suche nach der ursprünglichen Eingabe (in der Regel ein Passwort) für einen gegebenen Hashwert ermöglicht. Die Suche über eine Table ist erheblich schneller als bei der Brute-Force-Methode, allerdings ist der Speicherbedarf deutlich höher (Time-Memory Tradeoff).

Related-Key-Attacke Angriff auf ein kryptographisches Verfahren, bei dem ein Angreifer Verschlüsselungen und gegebenenfalls Entschlüsselungen nicht nur unter dem eigentlich verwendeten Schlüssel K, sondern auch unter einer Anzahl anderer, dem Angreifer nicht bekannter Schlüssel abfragen darf, die mit K in einer dem Angreifer bekannten Beziehung stehen. Dieses Modell ist für den Angreifer sehr günstig, dennoch gibt es Situationen, in denen Related-Key-Attacken praktisch relevant sein können, zum Beispiel im Zusammenhang der Konstruktion einer kryptographischen Hashfunktion aus einer Blockchiffre.

RSA Asymmetrisches kryptographisches Verfahren (benannt nach seinen Erfindern Ronald Rivest, Adi Shamir und Leonard Adleman), das zum Verschlüsseln und zum digitalen Signieren verwendet werden kann und auf der Schwierigkeit des Faktorisierungsproblems basiert.

S

Salt Zufällig gewählte Zeichenfolge, die an einen gegebenen Klartext vor dessen weiterer Verarbeitung (zum Beispiel vor Eingabe in eine Hashfunktion) angehängt wird, um die Entropie der Eingabe zu erhöhen. Salts werden häufig für die Speicherung und Übermittlung von Passwörtern benutzt, um die Nutzung von Regenbogentabellen zu erschweren.

Schlüsselableitungsfunktion (Key Derivation Function) Kryptographische Funktion, die aus einem geheimen Eingabewert, beispielsweise einem Hauptschlüssel, einem Passwort oder einer Passphrase, einen oder mehrere andere Schlüssel erzeugt. Schlüsselabhängige kryptographische Hash-Funktionen stellen eine häufig verwendete Möglichkeit dar.

Schlüssellänge Für symmetrische kryptographische Verfahren ist die Schlüssellänge einfach die Bitlänge des verwendeten geheimen Schlüssels. Für RSA (Signatur- und Verschlüsselungsverfahren) wird die Bitlänge des RSA-Moduls n als Schlüssellänge bezeichnet. Für

Verfahren, die auf dem Diffie-Hellman-Problem oder diskreten Logarithmen in $\mathbb{F}_p^*$ basieren (DLIES, DH-Schlüsseltausch, DSA), wird als Schlüssellänge die Bitlänge von p definiert. Für Verfahren, die auf dem Diffie-Hellman-Problem oder diskreten Logarithmen in einer elliptischen Kurve C über dem endlichen Körper $\mathbb{F}_n$ aufbauen (ECIES, ECDH, ECDSA und Varianten), ist die Schlüssellänge die Bitlänge von n.

Schlüsselstreckung (Key Stretching) Kryptographische Schlüsselableitungsoperation, die einen schwachen Schlüssel, üblicherweise ein Passwort, sicherer machen soll, indem sie dafür sorgt, dass zum Durchprobieren aller Möglichkeiten mehr Mittel (Zeit, Speicher) benötigt werden. Dabei darf es keine Möglichkeit geben, den verbesserten Schlüssel mit geringerem Aufwand aus dem Anfangsschlüssel berechnen zu können.

Secret Sharing Verfahren zur Verteilung geheimer Daten (zum Beispiel eines kryptographischen Schlüssels) auf mehrere Personen oder Speichermedien. Das ursprüngliche Geheimnis kann dabei nur unter Auswertung mehrerer Teilgeheimnisse rekonstruiert werden. Zum Beispiel kann ein Secret-Sharing-Schema vorsehen, dass von insgesamt n Teilgeheimnissen mindestens k bekannt sein müssen, um den zu schützenden kryptographischen Schlüssel zu rekonstruieren.

Seed Startwert, mit dem ein Zufallszahlengenerator initialisiert wird, um infolgedessen eine Folge von Zufallszahlen bzw. Pseudozufallszahlen zu generieren. Verwendet man in deterministischen Zufallszahlengeneratoren den gleichen Seed, so erhält man die gleiche Folge von Pseudozufallszahlen.

Seitenkanalangriff Angriff auf ein kryptographisches System, der die Ergebnisse von physikalischen Messungen am System (zum Beispiel Energieverbrauch, elektromagnetische Abstrahlung, Laufzeit einer Operation) ausnutzt, um Rückschlüsse auf sensible Daten zu ziehen. Seitenkanalangriffe sind für die praktische Sicherheit informationsverarbeitender Systeme von sehr hoher Relevanz.

Shannon-Entropie Die Shannon-Entropie einer diskreten Zufallsvariablen X ist definiert als $-\sum_{x \in W} p_x \log_2(p_x)$, wobei W der Wertebereich von X ist und p_x die Wahrscheinlichkeit, mit der X den Wert $x \in W$ annimmt, das heißt $p_x = \mathbb{P}(X = x)$.

Sicherheitsniveau (kryptographischer Verfahren) Ein kryptographisches Verfahren erreicht ein Sicherheitsniveau von n Bit, wenn mit jedem Angriff gegen das Verfahren, der das Sicherheitsziel des Verfahrens mit hoher Erfolgswahrscheinlichkeit bricht, Kosten verbunden sind, die zu 2^n Berechnungen der Verschlüsselungsfunktion einer effizienten Blockchiffre (zum Beispiel AES) äquivalent sind.

Symmetrische Kryptographie Oberbegriff für kryptographische Verfahren, in denen alle beteiligten Parteien über vorverteilte gemeinsame Geheimnisse verfügen müssen, um das Verfahren insgesamt ausführen zu können.

T

TDEA Triple DES.

Trapdoor-Einwegfunktion, Trapdoorfunktion, Trapdoorpermutation Siehe Einwegfunktion.

U

Urbild-Angriff Urbild-Angriffe (englisch preimage attack) sind Angriffe auf eine kryptographische Hashfunktion mit dem Ziel, zu einem gegebenen Hashwert eines unbekannten Eingabewerts ein Urbild zu finden (Erstes-Urbild-Angriff, englisch first-preimage attack)

oder zu einem gegebenem Eingabewert ein weiteres Urbild zu finden, das den gleichen Hashwert liefert (Zweites-Urbild-Angriff, englisch second-preimage attack).

Urbildresistenz Eine Funktion $h\colon M \to N$ heißt Urbild-resistent, wenn es praktisch unmöglich ist, zu einem gegebenen $y \in N$ ein $x \in M$ zu finden mit $h(x) = y$. Sie heißt resistent gegen Berechnung *zweiter* Urbilder, falls es zu gegebenem x, y mit $h(x) = y$ praktisch unmöglich ist, ein $x' \neq x$ zu berechnen mit $h(x') = y$.

V

Vertraulichkeit Sicherheitsziel der Bindung des lesenden Zugriffs auf eine Information an das Recht auf Zugriff. Im kryptographischen Kontext bedeutet dies, dass der Zugriff auf den Inhalt einer Nachricht nur Besitzern eines geheimen kryptographischen Schlüssels möglich sein sollte.

Volume-Verschlüsselung Siehe Partitionsverschlüsselung.

W

Wörterbuch-Angriff (Dictionary Attack) Angriffsmethode, um ein unbekanntes Passwort (oder einen Benutzernamen) durch systematisches Ausprobieren einer Passwörterliste (auch als wordlist oder dictionary bezeichnet) zu ermitteln. Der Erfolg derartiger Angriffe beruht auf der Tatsache, dass von Nutzern vergebene Passwörter in der Praxis häufig leicht zu erraten sind, beispielsweise wenn sie aus regulären oder nur leicht abgewandelten Wörterbucheinträgen bestehen oder in ähnlicher Form an verschiedenen Stellen benutzt werden, so dass Passwortlisten aus vormaligen Sicherheitsvorfällen zu einem erfolgreichen Angriff führen.

Z

Zufallsorakel Ein Zufallsorakel (englisch random oracle) ist ein theoretisches Konstrukt, das zu jeder Eingabe einen (gleichverteilt) zufälligen Wert der Ausgabemenge zurückgibt; bei einer wiederholten Anfrage der gleichen Eingabe antwortet es jedes Mal mit der gleichen Ausgabe. Zufallsorakel kommen üblicherweise zum Einsatz, wenn kryptographische Beweise nicht mit schwächeren Anforderungen an eine kryptographische Hashfunktion geführt werden können, da sie aufgrund ihrer Konstruktion die klassischen Anforderungen an eine kryptographische Hashfunktion (starke Kollisionsresistenz und Resistenz gegenüber der Berechnung von Urbildern erster und zweiter Art) perfekt erfüllen. Von Systemen, die beweisbar sicher sind, wenn jede Hashfunktion durch ein Zufallsorakel ersetzt wird, oder von Sicherheitsbeweisen, die ein Zufallsorakel verwenden, sagt man, sie seien sicher im Random-Oracle-Modell bzw. im Random-Oracle-Modell geführt worden, im Unterschied zum Standard-Modell der Kryptographie (das Standard-Modell ist das Berechnungsmodell, in dem ein Angreifer nur durch die ihm zur Verfügung stehende Zeit und Rechenkraft beschränkt wird).

1. Einleitung

In dieser Technischen Richtlinie veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Bewertung der Sicherheit für ausgewählte kryptographische Verfahren, verbunden mit einer langfristigen Orientierung für ihren Einsatz. Die ausgesprochenen Empfehlungen werden jährlich überprüft und bei Bedarf angepasst. Es wird dabei jedoch ausdrücklich kein Anspruch auf Vollständigkeit erhoben, das heißt nicht aufgeführte Verfahren werden vom BSI nicht zwangsläufig als unsicher beurteilt. Umgekehrt ist allerdings auch der Schluss falsch, dass kryptographische Systeme, die als Grundkomponenten nur in der vorliegenden Technischen Richtlinie empfohlene Verfahren verwenden, automatisch sicher sind: Die Anforderungen der konkreten Anwendung und die Verkettung verschiedener kryptographischer und nicht-kryptographischer Mechanismen können im Einzelfall dazu führen, dass die hier ausgesprochenen Empfehlungen nicht direkt umsetzbar sind oder dass Sicherheitslücken entstehen. Aufgrund dieser Erwägungen ist insbesondere zu betonen, dass die in dieser Technischen Richtlinie ausgesprochenen Empfehlungen keine Entscheidungen, etwa im Rahmen staatlicher Evaluierungs- und Zulassungsprozesse, vorwegnehmen.

Die vorliegende Technische Richtlinie richtet sich vielmehr in erster Linie empfehlend an Entwickler, die ab 2023 die Einführung neuer kryptographischer Systeme planen. Aus diesem Grund wird in diesem Dokument auch bewusst auf die Angabe kryptographischer Verfahren verzichtet, die zwar zum derzeitigen Zeitpunkt noch als sicher gelten, mittelfristig aber nicht mehr empfohlen werden können, da sie wenn auch noch keine ausnutzbaren, so doch zumindest theoretische Schwächen zeigen. Bei der Entwicklung neuer kryptographischer Systeme können verschiedene andere, vom BSI herausgegebene Dokumente ebenfalls eine Rolle spielen, darunter [30, 31, 33, 35, 27, 37]. Für bestimmte Anwendungen sind die in diesen Dokumenten enthaltenen Vorgaben – im Gegensatz zu den Empfehlungen der vorliegenden Richtlinie – sogar bindend. Eine Diskussion verschiedener Vorgaben und Empfehlungen findet sich in [56]. Die folgenden beiden Abschnitte beschreiben zunächst die Sicherheitsziele sowie die Auswahlkriterien der empfohlenen kryptographischen Verfahren. Weiter werden sehr allgemeine Hinweise zur konkreten Umsetzung der empfohlenen Verfahren gegeben.

Anschließend werden in den Kapiteln 2 bis 10 die empfohlenen kryptographischen Verfahren für folgende Anwendungen aufgelistet:

2 Symmetrische Verschlüsselung,

3 Asymmetrische Verschlüsselung,

4 Quantensichere Kryptographie,

5 Kryptographische Hashfunktionen,

6 Datenauthentisierung,

7 Instanzauthentisierung,

8 Schlüsselvereinbarung,

9 Secret Sharing und

10 Zufallszahlengeneratoren.

In den jeweiligen Abschnitten werden zudem geforderte (Mindest-) Schlüssellängen und andere zu beachtende Nebenbedingungen genannt.

Damit ein eingesetztes Verfahren die an es gestellten Sicherheitsanforderungen erfüllt, müssen häufig verschiedene kryptographische Algorithmen miteinander kombiniert werden. So ist es beispielsweise oft notwendig, vertrauliche Daten nicht nur zu verschlüsseln, sondern ein Empfänger muss sich auch sicher sein können, von wem die Daten versendet beziehungsweise ob diese während der Übertragung manipuliert wurden. Die zu übertragenden Daten müssen also zusätzlich mit einem geeigneten Verfahren authentisiert werden. Ein weiteres Beispiel stellen Schlüsselvereinbarungsverfahren dar. Hier ist es wichtig zu wissen, mit wem die Schlüsselvereinbarung durchgeführt wird, um sogenannte Man-in-the-Middle-Attacken und Unknown-Key-Share-Attacken [16] ausschließen zu können. Dies wird durch Verfahren ermöglicht, die Schlüsselvereinbarung und Instanzauthentisierung kombinieren. Für diese beiden Einsatzszenarien werden in Anhang A entsprechende Verfahren angegeben, die durch Kombination der in den Kapiteln 2 bis 10 aufgelisteten Verfahren konstruiert werden und das in dieser Technischen Richtlinie geforderte Sicherheitsniveau erfüllen. Zusätzlich werden in Anhang B häufig verwendete Funktionen und Algorithmen empfohlen, die beispielsweise zur Schlüsselableitung für symmetrische Verfahren oder zur Erzeugung von Primzahlen und anderen Systemparametern für asymmetrische Verfahren benötigt werden. Schließlich werden in Anhang C Empfehlungen zur Verwendung ausgewählter kryptographischer Protokolle ausgesprochen. In der aktuellen Version dieser Technischen Richtlinie betrifft dies nur das Protokoll SRTP; Empfehlungen zu TLS, IPsec und SSH wurden in die Technischen Richtlinien TR-02102-2 [24], TR-02102-3 [25] beziehungsweise TR-02102-4 [26] ausgelagert.

1.1. Sicherheitsziele und Auswahlkriterien

Die Sicherheit kryptographischer Verfahren hängt wesentlich von der Stärke der zugrunde liegenden kryptographischen Primitive ab. Aus diesem Grund werden in dieser Technischen Richtlinie nur Verfahren empfohlen, die basierend auf den heute vorliegenden Ergebnissen langjähriger Analysen und Diskussionen entsprechend eingeschätzt und als sicher bewertet werden können. Weitere Faktoren von zentraler Bedeutung für die Sicherheit stellen die konkreten Implementierungen der Algorithmen sowie die Zuverlässigkeit eventueller Hintergrundsysteme, wie zum Beispiel benötigte Public-Key-Infrastrukturen für den sicheren Austausch von Zertifikaten, dar. Die Umsetzung konkreter Implementierungen wird an dieser Stelle aber ebenso wenig betrachtet wie eventuell auftretende patentrechtliche Probleme. Auch wenn bei der Auswahl der Verfahren darauf geachtet wurde, dass die Algorithmen frei von Patenten sind, kann dies durch das BSI jedoch nicht garantiert werden. Zudem finden sich in dieser Technischen Richtlinie einzelne Hinweise auf mögliche Schwierigkeiten und Probleme bei der Implementierung kryptographischer Verfahren, diese sind allerdings nicht als erschöpfende Liste derartiger Probleme zu verstehen.

Insgesamt erreichen alle in dieser Technischen Richtlinie angegebenen kryptographischen Verfahren mit den in den einzelnen Abschnitten genannten Parametern ein Sicherheitsniveau von mindestens 120 Bits. Als Übergangsregelung ist die Verwendung von RSA-basierten Signatur- und Verschlüsselungsverfahren mit einer Schlüssellänge ab 2000 Bits für das gesamte Jahr 2023 noch weiterhin konform zu dieser Richtlinie. [1] Die in dieser Technischen Richtlinie zur Verwendung in neuen kryptographischen Systemen empfohlenen Bitlängen richten sich nach diesem Minimalniveau aber nur insoweit, als dass dieses für kein empfohlenes Verfahren unterschritten wird. Die effektive Stärke der empfohlenen Verfahren ist in vielen Fällen höher als 120 Bits. Damit wird ein gewisser Sicherheitsspielraum gegenüber möglichen künftigen Fortschritten in der Kryptoanalyse geschaffen. Wie bereits in der Einleitung erwähnt gilt im Umkehrschluss nicht, dass in dieser Tech-

[1] Falls RSA mit einer Schlüssellänge von weniger als 3000 Bits zum Schlüsseltransport verwendet wird, sollten auch die übertragenen Schlüssel über das Jahr 2023 hinaus nicht mehr eingesetzt werden (vergleiche Bemerkung 8.1 in Kapitel 8).

nischen Richtlinie nicht angegebene Verfahren das geforderte Sicherheitsniveau nicht erreichen.

Tabelle 1.1 zeigt die Schlüssellängen ausgewählter Algorithmen und Typen von Algorithmen, für die ein Sicherheitsniveau von 120 Bits nach gegenwärtigem Kenntnisstand gerade erreicht wird.

Symmetrische Verfahren		Asymmetrische Verfahren		
Ideale Blockchiffre	Idealer MAC	RSA	DSA/DLIES	ECDSA/ECIES
120	120	2800	2800	240

Tabelle 1.1: Beispiele für Schlüssellängen für ein Sicherheitsniveau von mindestens 120 Bits.

Tabelle 1.2 fasst die *empfohlenen* Schlüssellängen verschiedener Typen kryptographischer Primitive zusammen.

Blockchiffre	MAC	RSA	DH $\mathbb{F}_p$	ECDH	ECDSA
128	128	3000[a]	3000[a]	250	250

Tabelle 1.2: Empfohlene Schlüssellängen für verschiedene kryptographische Verfahren.

[a] Für einen Einsatzzeitraum ab dem Jahr 2023 wird durch die vorliegende Technische Richtlinie empfohlen, eine Schlüssellänge von mindestens 3000 Bits zu nutzen, um ein vergleichbares Sicherheitsniveau für alle asymmetrischen Verfahren zu erreichen. Eine Schlüssellänge von ≥ 3000 Bits wird ab dem Jahr 2023 für kryptographische DLIES- und DSA-Implementierungen verbindlich, die zu der vorliegenden Technischen Richtlinie konform sein sollen. Übergangsweise bleibt eine Schlüssellänge von $\geq$ 2000 Bits für RSA-Schlüssel bis Ende 2023 konform zur Technischen Richtlinie; ab dem Jahr 2024 wird eine RSA-Schlüssellänge von $\geq$ 3000 Bits verbindlich.

Schlüsseltauschverfahren auf Diffie-Hellman-Basis sind in den Tabellen 1.1 und 1.2 entsprechend zu DSA/ECDSA einzugruppieren.

In vielen Anwendungsfällen spielen neben der Schlüssellänge weitere Sicherheitsparameter eine Rolle für die Gesamtsicherheit eines kryptographischen Systems. So stellt im Falle von Message Authentication Codes (MACs) die Länge des Digest-Outputs neben der Schlüssellänge einen wichtigen Sicherheitsparameter dar. Idealerweise sollte ein MAC von einem Angreifer praktisch nicht von einer Zufallsfunktion mit entsprechender Digest-Länge unterschieden werden können. Solange dieses Kriterium erfüllt ist, bleibt dem Angreifer nur die Möglichkeit, gefälschte Nachrichten durch Raten zu erzeugen, wobei er pro Versuch eine Erfolgswahrscheinlichkeit von 2^{-n} hat, wenn n die Tag-Länge ist. In vielen Anwendungen kann in einer solchen Situation $n = 96$ als akzeptabel angesehen werden, dass heißt eine Tag-Länge von $n = 96$ Bits.

Bei Blockchiffren ist die Blockbreite ein von der Schlüssellänge unabhängiger Sicherheitsparameter. In Abwesenheit struktureller Angriffe auf eine Blockchiffre ist die wesentlichste Auswirkung einer geringen Blockbreite, dass ein häufigerer Schlüsselwechsel notwendig wird. Die genauen Auswirkungen hängen vom verwendeten Betriebsmodus ab. In der vorliegenden Technischen Richtlinie werden keine Blockchiffren empfohlen, die eine Blockbreite von unter 128 Bits aufweisen.

Ein wichtiger Typ kryptographischer Primitive, die überhaupt keine geheimen Daten verarbeiten, sind kryptographische Hashfunktionen. Hier stellt die Länge des zurückgegebenen Digest-Wertes

den wichtigsten Sicherheitsparameter dar und sollte für allgemeine Anwendungen mindestens 200 Bits betragen, damit das in dieser Richtlinie minimal geforderte Sicherheitsniveau erreicht wird. Die in Kapitel 5 empfohlenen Hashfunktionen haben eine Mindesthashlänge von 256 Bits, auf Abweichungen von dieser Regel für besondere Anwendungen wird in der vorliegenden Technischen Richtlinie an gegebener Stelle eingegangen.

1.2. Allgemeine Hinweise

Zuverlässigkeit von Prognosen zur Sicherheit kryptographischer Verfahren Bei der Festlegung der Größe von Systemparametern (wie zum Beispiel Schlüssellänge, Größe des Bildraums für Hashfunktionen u.ä.) müssen nicht nur die besten heute bekannten Algorithmen zum Brechen der entsprechenden Verfahren und die Leistung heutiger Rechner berücksichtigt werden, sondern vor allem eine Prognose der zukünftigen Entwicklung beider Aspekte zugrunde gelegt werden, siehe insbesondere auch [71, 70, 36].

Die Entwicklung der Leistungsfähigkeit klassischer Rechner kann heutzutage relativ gut eingeschätzt werden. Grundlegende wissenschaftliche Fortschritte (entweder in Bezug auf Angriffsalgorithmen oder etwa die Entwicklung eines kryptographisch relevanten Quantencomputers) sind dagegen nicht vorhersagbar. Daher ist jede Vorhersage über einen Zeitraum von sechs bis sieben Jahren hinaus schwierig, insbesondere bei asymmetrischen Verfahren, und selbst für diesen Zeitraum von sechs bis sieben Jahren können sich die Prognosen aufgrund unvorhersehbarer Entwicklungen als falsch erweisen. Die Angaben dieser Technischen Richtlinie werden daher nur beschränkt auf einen Zeitraum bis Ende 2028 ausgesprochen.

Allgemeine Leitlinien zum Umgang mit vertraulichen Daten mit längerfristigem Schutzbedarf Da ein Angreifer Daten speichern und später entschlüsseln kann, bleibt ein grundsätzliches Risiko für den langfristigen Schutz der Vertraulichkeit. Daraus ergeben sich als unmittelbare Konsequenzen:

- Die Übertragung und Speicherung vertraulicher Daten sollte auf das notwendige Maß reduziert werden. Dies betrifft nicht nur Klartexte, sondern zum Beispiel in besonderem Maße auch die Vermeidung einer Speicherung von Sitzungsschlüsseln auf jeglicher Art von nichtflüchtigen Medien sowie ihre zügige sichere Löschung, sobald sie nicht mehr benötigt werden.
- Das Kryptosystem muss so ausgelegt sein, dass ein Übergang zu größeren Schlüssellängen und stärkeren kryptographischen Verfahren möglich ist (Kryptoagilität).
- Für Daten, deren Vertraulichkeit langfristig gesichert bleiben soll, wird empfohlen, für die Verschlüsselung der Übertragung über allgemein zugängliche Kanäle wie beispielsweise das Internet von vornherein möglichst starke der in dieser Technischen Richtlinie empfohlenen Verfahren zu wählen. In den meisten Kontexten ist zum Beispiel der AES-256 aufgrund seiner größeren Schlüssellänge als stärker zu betrachten als der AES-128. Da solche allgemeinen Einschätzungen aber schwierig sind – im konkreten Beispiel sind etwa in einigen (konstruierten) Szenarien der AES-192 und der AES-256 *schwächer* als der AES-128 gegenüber den besten bekannten Angriffen (siehe [15]) – sollte nach Möglichkeit bereits früh der Rat eines Experten eingeholt werden.
- Im Hinblick auf die Auswahl kryptographischer Komponenten für eine neue Anwendung ist grundsätzlich zu berücksichtigen, dass das Gesamtsystem im Allgemeinen nicht stärker ist als die schwächste Komponente. Wird daher ein Sicherheitsniveau von beispielsweise 128 Bits für das Gesamtsystem angestrebt, müssen alle Komponenten mindestens diesem Sicherheitsniveau genügen. Die Auswahl einzelner Komponenten, die ein höheres Sicherheitsniveau gegenüber den besten bekannten Angriffen erreichen als das Gesamtsystem, kann unter Um-

ständen trotzdem sinnvoll sein, weil dies die Robustheit des Systems gegenüber Fortschritten in der Kryptoanalyse erhöht.

- Um die Möglichkeit von Seitenkanalattacken und Implementierungsfehlern zu minimieren, sollte im Falle von Software-Implementierungen der hier vorgestellten kryptographischen Verfahren einem Einsatz quelloffener Bibliotheken der Vorzug vor Eigenentwicklungen gegeben werden, wenn davon ausgegangen werden kann, dass die verwendeten Funktionen der Bibliothek einer breiten öffentlichen Analyse unterzogen wurden. Bei der Bewertung eines Kryptosystems ist dabei die Vertrauenswürdigkeit aller Systemfunktionen zu prüfen, insbesondere beinhaltet dies auch Abhängigkeiten der Lösung von Eigenschaften der verwendeten Hardware.

Fokus des vorliegenden Dokuments Die Sicherheitsbewertung der in dieser Technischen Richtlinie empfohlenen kryptographischen Verfahren erfolgt ohne Berücksichtigung der Einsatzbedingungen. Für konkrete Szenarien können sich andere Sicherheitsanforderungen ergeben, denen die in dieser Technischen Richtlinie empfohlenen Verfahren möglicherweise nicht gerecht werden. Beispiele hierfür stellen etwa die Verschlüsselung von Datenträgern, die verschlüsselte Speicherung und Verarbeitung von Daten auf durch externe Anbieter betriebenen Systemen („Cloud Computing“ beziehungsweise „Cloud Storage“) oder kryptographische Anwendungen auf Geräten mit extrem geringen rechentechnischen Ressourcen („Lightweight Cryptography“) dar. Hinweise zu einigen der genannten Anwendungsszenarien finden sich in Abschnitt 1.6. Dieses Dokument kann daher die Entwicklung kryptographischer Infrastrukturen unterstützen, nicht aber die Bewertung des Gesamtsystems durch einen Kryptologen ersetzen oder die Ergebnisse einer solchen Bewertung vorwegnehmen.

Allgemeine Empfehlungen zur Entwicklung kryptographischer Systeme Die folgende Auflistung fasst stichpunktartig einige Grundsätze zusammen, deren Beachtung bei der Entwicklung kryptographischer Systeme generell empfohlen wird:

- Bei der Planung von Systemen, für die kryptographische Komponenten vorgesehen sind, sollte frühzeitig die Zusammenarbeit mit Experten auf kryptographischem Gebiet gesucht werden.
- Die in dieser Technischen Richtlinie aufgeführten kryptographischen Verfahren müssen in vertrauenswürdigen technischen Komponenten implementiert werden, um das geforderte Sicherheitsniveau zu erreichen.
- Die Implementierungen der kryptographischen Verfahren und Protokolle selbst sind in die Sicherheitsanalyse mit einzubeziehen, um zum Beispiel Seitenkanalangriffe oder Implementierungsschwächen zu verhindern.
- Wenn die Übereinstimmung eines Produktes mit den Anforderungen dieser Technischen Richtlinie nachgewiesen werden soll, muss die Sicherheit technischer Komponenten und Implementierungen dem jeweils vorgesehenen Schutzprofil entsprechend durch Common Criteria Zertifikate oder ähnliche Verfahren des BSI, wie zum Beispiel im Zuge einer Zulassung, nachgewiesen werden.
- Nach Entwicklung und vor Produktiveinsatz eines kryptographischen Systems sollte eine Evaluierung des Systems durch unabhängige Experten durchgeführt werden, die nicht an der Entwicklung beteiligt waren. Eine Einschätzung der Verfahrenssicherheit durch die Entwickler allein sollte nicht als belastbar betrachtet werden, auch wenn die Entwickler des Systems über gute kryptographische Kenntnisse verfügen.

- Die Folgen eines Versagens der eingesetzten Sicherheitsmechanismen müssen gründlich dokumentiert werden. Wo es möglich ist, sollte das System so ausgelegt werden, dass das Versagen oder die Manipulation einzelner Systemkomponenten unmittelbar detektiert wird und die Sicherheitsziele durch Übergang in einen geeigneten sicheren Zustand gewahrt bleiben.

1.3. Kryptographische Hinweise

Ein kryptographisches Verfahren kann häufig für verschiedene Anwendungen eingesetzt werden, so können zum Beispiel Signaturverfahren sowohl zur Datenauthentisierung als auch zur Instanzauthentisierung verwendet werden. Grundsätzlich sollten für unterschiedliche Anwendungen jeweils verschiedene Schlüssel eingesetzt werden. Ein weiteres Beispiel stellen symmetrische Schlüssel zur Verschlüsselung und symmetrischen Datenauthentisierung dar. Hier muss bei konkreten Implementierungen dafür gesorgt werden, dass für beide Verfahren jeweils verschiedene Schlüssel eingesetzt werden, die sich insbesondere nicht voneinander ableiten lassen, siehe auch Abschnitt A.1.

An einigen Stellen beschränkt sich diese Technische Richtlinie auf eine informative Beschreibung der kryptographischen Primitive. Da die kryptographische Sicherheit aber nur im Rahmen der jeweiligen exakten Spezifikation und des jeweils verwendeten Protokolls bewertet werden kann, müssen daher die entsprechenden hier angegebenen Standards beachtet werden. Weitere konkrete Hinweise werden, so nötig, in den entsprechenden Abschnitten angegeben.

1.4. Implementierungsaspekte

Neben der kryptanalytischen Sicherheit der verwendeten Algorithmen ist die Sicherheit der Implementierung, beispielsweise gegen Seitenkanal- und Fault-Attacken, für die Sicherheit eines Kryptosystems von entscheidender Bedeutung. Dies gilt insbesondere für symmetrische Verschlüsselungsverfahren. Eine detaillierte Behandlung dieses Themas liegt außerhalb des Rahmens der vorliegenden Technischen Richtlinie, zumal die zu treffenden Gegenmaßnahmen im Einzelfall auch in hohem Maße von der konkreten Implementierung abhängig sind. An dieser Stelle seien lediglich die folgenden, allgemeinen Maßnahmen empfohlen:

- Wann immer es mit vertretbarem Aufwand möglich ist, sollten kryptographische Operationen in sicherheitszertifizierten Hardwarekomponenten durchgeführt werden (also zum Beispiel auf einer geeigneten Smartcard) und die dabei verwendeten Schlüssel sollten diese Komponenten nicht verlassen.

- Angriffe, die durch entfernte, passive Angreifer durchgeführt werden können, sind naturgemäß schwer zu detektieren und können daher zu einem wesentlichen unbemerkten Datenabfluss über einen langen Zeitraum hinweg führen. Dazu zählen etwa Angriffe unter Ausnutzung variabler Bitraten, Dateilängen oder variabler Antwortzeiten kryptographischer Systeme. Es wird empfohlen, die Auswirkungen solcher Seitenkanäle auf die Systemsicherheit bei der Entwicklung eines neuen kryptographischen Systems gründlich zu analysieren und die Ergebnisse der Analyse im Entwicklungsprozess zu berücksichtigen.

- Sowohl bei Angriffen auf symmetrische als auch auf asymmetrische Verfahren kommen in jüngster Zeit vermehrt Angriffsmethoden zum Einsatz, die auf Verfahren aus dem Bereich des Maschinellen Lernens (ML) beziehungsweise der Künstlichen Intelligenz (KI) basieren. Insbesondere neuronale Netze erzielen dabei häufig State-of-the-Art-Resultate. Es zeichnet sich ab, dass KI-basierte Methoden den derzeit zumeist verwendeten klassischen Angriffsmethoden (zum Beispiel basierend auf Korrelationen oder Templates) in einigen Anwendungsfällen

deutlich überlegen sein könnten. Ein KI-Leitfaden, der detailliertere Empfehlungen zu diesem Thema enthält, befindet sich daher in Vorbereitung.

- Auf Protokollebene sollte der Entstehung von Fehlerorakeln vorgebeugt werden. Am wirkungsvollsten kann dies durch eine MAC-Sicherung aller Chiffrate geschehen. Die Authentizität der Chiffrate sollte dabei vor Ausführung aller anderen kryptographischen Operationen geprüft werden und es sollte keine weitere Verarbeitung nicht-authentischer Chiffrate erfolgen.

Wie auch in anderen Zusammenhängen trifft insbesondere auch hier die bereits mehrfach genannte, allgemeine Empfehlung zu, nach Möglichkeit stets Komponenten zu verwenden, die bereits einer intensiven Analyse durch eine breite Öffentlichkeit unterzogen wurden und frühzeitig entsprechende Experten in die Entwicklung neuer kryptographischer Systeme einzubinden.

1.5. Umgang mit Legacy-Algorithmen

Es gibt Algorithmen, gegen die bislang keine praktischen Angriffe bekannt sind und die in einigen Anwendungen noch eine hohe Verbreitung und damit eine gewisse Bedeutung besitzen, die aber grundsätzlich für neue Systeme als nicht mehr dem Stand der Technik entsprechend angesehen werden. Wir gehen im Folgenden kurz auf die wichtigsten Beispiele ein.

Triple-DES (TDEA) mit drei voneinander unabhängigen Teilschlüsseln [93] Die Hauptargumente, die gegen eine Verwendung von 3-Key-Triple-DES in neuen Systemen sprechen, sind die geringe Blockbreite von nur 64 Bits, die im Vergleich zum AES verringerte Sicherheit gegenüber generischen Angriffen auf Blockchiffren sowie verschiedene weitere, aus kryptographischer Sicht unerwünschte Eigenschaften. Zu erwähnen ist zum Beispiel die Existenz von Related-Key-Angriffen gegen Triple-DES mit einer Rechenzeit von $\approx 2^{56}$ Triple-DES-Berechnungen [67]. Auch ohne Berücksichtigung von Related-Key-Angriffen besitzt Triple-DES kryptographische Eigenschaften, die zwar nach heutigem Kenntnisstand nicht auf praktisch nutzbare Schwächen hinweisen, die aber negativer sind, als man es für eine ideale Blockchiffre mit 112 Bits effektiver Schlüssellänge erwarten würde [75]. Insgesamt wird daher empfohlen, Triple-DES in neuen Systemen nicht zu verwenden, es sei denn es wäre aus Gründen der Rückwärtskompatibilität zu bestehender Infrastruktur zwingend erforderlich. Auch in diesem Fall sollte eine Migration zu AES in absehbarer Zukunft vorbereitet werden.

Triple-DES [93] mit zwei voneinander unabhängigen Teilschlüsseln zeigt insgesamt deutlich ernsthaftere Schwächen gegenüber Chosen-Plaintext- und Known-Plaintext-Angriffen im Single-Key-Setting als Triple-DES mit drei Teilschlüsseln [82, 107]. Auch wenn letztendlich keine praktischen Angriffe gegen Triple-DES mit zwei voneinander unabhängigen Teilschlüsseln bekannt sind, wird hier empfohlen, diese Chiffre nicht nur in neuen Systemen nicht zu verwenden, sondern auch bestehende Kryptoverfahren, die Triple-DES mit zwei Schlüsseln verwenden, so bald wie möglich nach AES (oder wenigstens auf drei unabhängige Teilschlüssel) zu migrieren. Soweit Triple-DES noch verwendet wird, sind alle Vorgaben zur Verwendung aus [93] zu beachten.

HMAC-MD5 Die mangelnde Kollisionsresistenz von MD5 stellt in der HMAC-Konstruktion mit MD5 als Hashfunktion [10] noch kein unmittelbares Problem dar, da die HMAC-Konstruktion nur eine sehr schwache Form von Kollisionsresistenz von der Hashfunktion benötigt. Allerdings erscheint es grundsätzlich nicht ratsam, in neuen Kryptosystemen Primitive zu verwenden, die in ihrer ursprünglichen Funktion vollständig gebrochen wurden. Systeme, die MD5 für kryptographische Zwecke verwenden, sind daher nicht mit der vorliegenden Technischen Richtlinie konform.

HMAC-SHA1 SHA1 ist keine kollisionsresistente Hashfunktion. Die Erzeugung von SHA1-Kollisionen ist zwar mit moderatem Aufwand verbunden, aber praktisch möglich [73, 72, 106], auch wenn gegen die Verwendung von SHA1 in Konstruktionen, die keine Kollisionsresistenz benötigen (zum Beispiel als Grundlage für einen HMAC, als Teil der Mask Generation Function in RSA-OAEP oder als Komponente eines Pseudozufallsgenerators) nach gegenwärtigem Kenntnisstand sicherheitstechnisch nichts spricht. Als grundsätzliche Sicherungsmaßnahme wird empfohlen, auch in diesen Anwendungen eine Hashfunktion der SHA2- oder der SHA3-Familie einzusetzen.

RSA mit PKCS1v1.5-Padding Grundsätzlich wird eine Verwendung dieses Formats in neuen Systemen weder für Verschlüsselung noch für Signaturerstellung empfohlen, da es mit RSA-OAEP beziehungsweise RSA-PSS Paddingverfahren mit solideren theoretischen Sicherheitseigenschaften gibt. Außerdem haben sich RSA-Implementierungen mit PKCS1v1.5-Padding als anfälliger gegenüber Angriffen erwiesen, die Seitenkanalinformationen oder Implementierungsfehler ausnutzen.

1.6. Weitere relevante Aspekte

Abschließend werden an dieser Stelle explizit noch einmal einige wichtige Themenbereiche genannt, die in der vorliegenden Technischen Richtlinie nicht oder nicht ausführlich behandelt werden. Die Auflistung erhebt ausdrücklich keinen Anspruch auf Vollständigkeit.

Lightweight Cryptography In diesem Zusammenhang treten besonders restriktive Anforderungen an Rechenzeit und Speicherbedarf der eingesetzten kryptographischen Verfahren auf. Abhängig von der Anwendung können sich außerdem auch die Sicherheitsanforderungen von den sonst üblichen unterscheiden.

Reaktionszeiten eines Systems Beim Einsatz kryptographischer Verfahren in Bereichen, in denen enge Vorgaben an die Antwortzeiten des Systems eingehalten werden müssen, können besondere Situationen auftreten, die in dieser Richtlinie nicht behandelt werden. Die Empfehlungen zur Verwendung von SRTP in Appendix C decken Teile dieses Themas ab.

Festplattenverschlüsselung Im Kontext der Festplattenverschlüsselung tritt das Problem auf, dass in den meisten Anwendungsszenarien weder eine Verschlüsselung mit Datenexpansion noch eine deutliche Expansion der Menge an Daten, die vom Speichermedium gelesen beziehungsweise auf das Speichermedium geschrieben werden müssen, akzeptabel sind. Keiner der empfohlenen Verschlüsselungsmodi ist ohne Weiteres als Grundlage einer Lösung zur Festplattenverschlüsselung geeignet. Unter der Voraussetzung, dass ein Angreifer keine Abbilder des Festplattenzustandes zu mehreren verschiedenen Zeitpunkten miteinander kombinieren kann, bietet XTS-AES relativ gute Sicherheitseigenschaften und gute Effizienz [88]. Wenn der Angreifer zu einer größeren Anzahl verschiedener Zeitpunkte Kopien des verschlüsselten Speichermediums erstellen kann, ist jedoch von einem gewissen, nicht zwingend unwesentlichen Abfluss von Information auszugehen. Der Angreifer kann zum Beispiel durch den Vergleich zweier zu verschiedenen Zeitpunkten angefertigter Abbilder einer mit XTS-AES verschlüsselten Festplatte unmittelbar erkennen, welche Klartextblöcke auf der Festplatte innerhalb dieses Zeitraumes verändert wurden und welche nicht.

Festplattenverschlüsselung von SSD-Platten Im Zusammenhang mit der Verschlüsselung eines Solid State Drives (SSD) ist der Umstand von Bedeutung, dass der SSD-Controller das Überschreiben logischer Speicheradressen physisch nicht in-place umsetzt, sondern auf verschiedene physische Speicherbereiche verteilt. Damit enthält der aktuelle Zustand einer SSD immer auch Information über gewisse frühere Zustände des Speichermediums. Ein Angreifer mit guter Kenntnis der

Funktionsweise des SSD-Controllers kann dies potentiell ausnutzen, um aufeinanderfolgende Zustände einer logischen Speicheradresse nachzuverfolgen. Ein einzelnes Abbild des verschlüsselten Speichermediums ist bei Verwendung einer SSD damit für einen Angreifer unter Umständen wertvoller als ein einzelnes Abbild einer Festplatte.

Cloud-Speicherung Ähnliche Probleme wie bei der Verschlüsselung von Datenträgern stellen sich bei der verschlüsselten Speicherung ganzer logischer Laufwerke auf entfernten Systemen, die nicht unter der Kontrolle des Datenbesitzers stehen (sogenannte Cloud-Speicherung). Kann dem Anbieter des entfernten Servers oder dessen Sicherheitsmaßnahmen nicht in hohem Maße vertraut werden, muss davon ausgegangen werden, dass ein Angreifer unbemerkt Platten-Abbilder zu beliebigen Zeitpunkten anfertigen kann. Werden Dateien mit sensiblen Daten auf einem Speichersystem abgelegt, das regelmäßig unter fremder Kontrolle steht, sollte entsprechend vor der Übermittlung eine kryptographisch starke Dateiverschlüsselung angewandt werden. Dies gilt auch dann, wenn die Daten vor ihrer Übermittlung an das Speichermedium durch eine Volume-Verschlüsselung verschlüsselt werden. Die Verwendung einer Volume-Verschlüsselungslösung allein ist nur empfehlenswert, wenn diese einen wirksamen kryptographischen Schutz vor Manipulation der Daten beinhaltet und die sonstigen Voraussetzungen an den Einsatz des entsprechenden Verfahrens in allgemeinen kryptographischen Kontexten eingehalten werden (beispielsweise ist dies die Erfordernis unvorhersagbarer Initialisierungsvektoren). Insbesondere sollten Verfahren so ausgewählt werden, dass anders als im XTS-Modus bei wiederholtem Schreiben eines Datenblocks kein nennenswerter Abfluss von Information durch Häufigkeitsanalyse aufeinanderfolgender Zustände zu erwarten ist.

Physikalische Aspekte Die vorliegende Richtlinie geht im Wesentlichen nur auf solche Aspekte der Sicherheit kryptographischer Systeme ein, die sich auf die verwendeten Algorithmen reduzieren lassen. Physikalische Aspekte wie die Abstrahlsicherheit informationsverarbeitender Systeme oder kryptographische Systeme, deren Sicherheit auf physikalischen Effekten beruht (zum Beispiel quantenkryptographische Systeme), werden in dieser Technischen Richtlinie – ebenso wie Seitenkanalangriffe, Fault-Attacken und weitere physikalische Sicherheitsfragen – nicht oder nur am Rande behandelt. Etwaige Ausführungen zu Seitenkanalangriffen sind ausdrücklich als beispielhafte Hinweise auf mögliche Gefährdungen ohne Anspruch auf Vollständigkeit zu verstehen.

Verkehrsflussanalyse Keines der in dieser Technischen Richtlinie beschriebenen Verfahren und Protokolle zur Datenverschlüsselung erreicht für sich genommen das Ziel der *Sicherheit gegen Verkehrsflussanalyse* (englisch *Traffic Flow Confidentiality*). Eine Verkehrsflussanalyse – also eine Analyse eines verschlüsselten Datenstromes unter Berücksichtigung von Quelle, Ziel, Zeitpunkt des Bestehens einer Verbindung, Größe der übermittelten Datenpaketen, Datenrate und Zeitpunkt der Übermittlung der Datenpakete – kann wesentliche Rückschlüsse auf die Inhalte verschlüsselter Übertragungen erlauben, siehe zum Beispiel [7, 40, 105]. Traffic Flow Confidentiality ist ein Ziel, das im Regelfall nur mit hohem Aufwand vollständig erreicht werden kann und das deshalb auch in vielen Anwendungen, die sensible Informationen verarbeiten, nicht realisierbar ist. Es sollte allerdings in jedem Einzelfall durch Experten überprüft werden, in welchem Umfang und welche vertrauliche Informationen in einem gegebenen Kryptosystem durch Verkehrsflussanalyse (und natürlich andere Seitenkanalangriffe) preisgegeben werden. Je nach konkreter Sachlage kann der Ausgang einer solchen Untersuchung wesentliche Änderungen am Gesamtsystem notwendig machen. Es wird daher empfohlen, die Widerstandsfähigkeit eines kryptographischen Systems gegen Preisgabe sensibler Informationen durch Verkehrsflussanalyse bei der Entwicklung neuer Systeme von Anfang an als Ziel zu berücksichtigen.

Endpunktsicherheit Die Sicherheit der Endpunkte einer kryptographisch abgesicherten Verbindung ist unabdingbar für die Sicherheit der übermittelten Daten. Bei der Entwicklung eines krypto-

graphischen Systems muss eindeutig dokumentiert werden, welche Systemkomponenten vertrauenswürdig sein müssen, damit die angestrebten Sicherheitsziele erreicht werden, und diese Komponenten müssen in einer dem Einsatzkontext angemessenen Weise gegen Kompromittierung gehärtet werden. Entsprechende Überlegungen müssen den gesamten Lebenszyklus der zu schützenden Daten ebenso umfassen wie den gesamten Lebenszyklus der durch das System erzeugten kryptographischen Geheimnisse. Kryptographische Verfahren können die Anzahl der Komponenten eines Gesamtsystems, deren Vertrauenswürdigkeit sicherzustellen ist, um einen Datenabfluss zu vermeiden, zwar verringern, das Grundproblem der Endpunktsicherheit aber nicht lösen.

Quantensichere Kryptographie Verschlüsselungsverfahren müssen einmal übermittelte Daten unter Umständen für lange Zeit schützen. Angriffe durch künftige Quantencomputer sollten daher im Rahmen des Risikomanagements berücksichtigt werden. Andererseits ist die Standardisierung quantencomputerresistenter kryptographischer Verfahren noch nicht abgeschlossen und es gibt zum heutigen Zeitpunkt auch noch nicht so viele Erkenntnisse über deren sichere Implementierung, wie es bei klassischen Public-Key-Verfahren der Fall ist. Kapitel 4 liefert einige vorläufige Empfehlungen zum Umgang mit Themen aus diesem Bereich. Eine Übersicht zum aktuellen Entwicklungsstand der dem Quantencomputing zugrundeliegenden Technik findet sich unter anderem in der Studie [36].

Die vorliegende Richtlinie liefert hinsichtlich der Umsetzung von Verfahren in den zuvor genannten Bereichen keine oder zumindest keine umfassenden Empfehlungen. Es wird daher geraten, bei der Entwicklung kryptographischer Systeme insgesamt – aber insbesondere in diesen Bereichen – von Beginn an Experten aus den entsprechenden Gebieten in die Entwicklungsarbeit mit einzubeziehen.

2. Symmetrische Verschlüsselungsverfahren

In diesem Kapitel werden symmetrische Verfahren behandelt, das heißt Verfahren, bei denen Ver- und Entschlüsselungsschlüssel gleich sind – im Gegensatz zu asymmetrischen Verfahren, bei denen der private aus dem öffentlichen Schlüssel ohne zusätzliche Informationen praktisch nicht berechnet werden kann. Für asymmetrische Verschlüsselungsverfahren, die in der Praxis in der Regel lediglich als Schlüsseltransportverfahren eingesetzt werden, sei auf Kapitel 3 verwiesen.

Symmetrische Verschlüsselungsverfahren dienen der Gewährleistung der Vertraulichkeit von Daten, die zum Beispiel über einen öffentlichen Kanal wie Telefon oder Internet ausgetauscht werden. Authentizität bzw. Integrität der Daten wird dadurch in der Regel nicht automatisch gewährleistet, für einen Integritätsschutz siehe Kapitel 6 und Abschnitt A.1. Auch in Fällen, in denen auf den ersten Blick der Schutz der Vertraulichkeit übermittelter Daten das dominierende oder sogar das einzige Sicherheitsziel zu sein scheint, kann eine Vernachlässigung integritätssichernder Mechanismen leicht zu Schwächen im kryptographischen Gesamtsystem führen, die das System dann auch für Angriffe auf die Vertraulichkeit anfällig machen. Insbesondere können auf solche Weise Schwächen durch bestimmte Arten aktiver Seitenkanalangriffe entstehen, für ein Beispiel siehe etwa [108].

2.1. Blockchiffren

Allgemeine Empfehlungen Eine Blockchiffre ist ein Algorithmus, der einen Klartext fester Bitlänge (zum Beispiel 128 Bits) mittels eines Schlüssels zu einem Chiffretext gleicher Bitlänge verschlüsselt. Diese Bitlänge wird auch als *Blockgröße* der Chiffre bezeichnet. Für die Verschlüsselung von Klartexten anderer Länge werden Blockchiffren in verschiedenen Betriebsarten angewendet, siehe Abschnitt 2.1.1. Für neue kryptographische Anwendungen sollten nur noch Blockchiffren eingesetzt werden, deren Blockgröße mindestens 128 Bits beträgt.

Folgende Blockchiffren werden zur Verwendung in neuen kryptographischen Systemen empfohlen:

AES-128, AES-192, AES-256, siehe [84].

Tabelle 2.1: Empfohlene Blockchiffren.

In Version 1.0 der vorliegenden Technischen Richtlinie wurden auch die Blockchiffren Serpent und Twofish empfohlen. Bislang liegen keine negativen Erkenntnisse zu diesen Blockchiffren vor, allerdings wurde die Sicherheit von Serpent und Twofish seit dem Ende des AES-Wettbewerbs deutlich weniger intensiv untersucht als die des Rijndael-Algorithmus, der als Sieger und somit künftiger AES aus dem Wettbewerb hervorging. Dies gilt sowohl für klassische kryptoanalytische Angriffe als auch für andere Sicherheitsaspekte, zum Beispiel die Seitenkanalresistenz konkreter Implementierungen. Aus diesem Grund wird in der vorliegenden Version dieser Technischen Richtlinie auf eine Empfehlung weiterer Blockchiffren neben dem AES verzichtet.

Related-Key-Angriffe und AES Bei Related-Key-Attacken wird davon ausgegangen, dass der Angreifer Zugriff auf Verschlüsselungen oder Entschlüsselungen bekannter oder gewählter Klartexte oder Chiffrate unter verschiedenen Schlüsseln hat, die zueinander in einer dem Angreifer bekannten Beziehung stehen (also zum Beispiel sich genau in einer Bitposition des Schlüssels unterscheiden). Bestimmte Angriffe dieser Art gegen rundenreduzierte Versionen des AES-256 [14] und gegen unmodifizierte Versionen des AES-192 sowie AES-256 [15] stellen bislang die einzigen bekannten kryptoanalytischen Techniken dar, denen gegenüber AES ein wesentlich schlechteres Verhalten zeigt als eine ideale Chiffre mit entsprechender Schlüssellänge und Blockgröße.

Zum gegenwärtigen Zeitpunkt haben diese Erkenntnisse zur Sicherheit von AES unter spezifischen Typen von Related-Key-Attacken keine Auswirkungen auf die in dieser Technischen Richtlinie ausgesprochenen Empfehlungen. Insbesondere ein Related-Key Boomerang-Angriff auf AES-256 aus [15] mit Rechenzeit- und Datenkomplexität von $2^{99.5}$ ist aufgrund der technischen Voraussetzungen von Related-Key Boomerang-Angriffen nicht als Verletzung des in dieser Technischen Richtlinie mittelfristig angestrebten Sicherheitsniveaus von 120 Bits zu betrachten. Die besten bekannten Angriffe gegen AES, die keine Related-Keys benötigen, erzielen nur einen geringen Vorteil gegenüber generischen Angriffen [19].

2.1.1. Betriebsarten

Wie bereits in Abschnitt 2.1 erwähnt, liefert eine Blockchiffre lediglich einen Mechanismus zur Verschlüsselung von Klartexten einer einzigen festen Länge. Um Klartexte beliebiger Länge zu verschlüsseln, muss aus der Blockchiffre mittels einer geeigneten *Betriebsart* ein Verschlüsselungsverfahren für Klartexte (annähernd) beliebiger Länge konstruiert werden. Ein weiterer Effekt einer kryptographisch starken Betriebsart ist, dass das resultierende Verschlüsselungsverfahren in mancher Hinsicht stärker sein wird als die zugrundeliegende Blockchiffre, zum Beispiel wenn die Betriebsart den Verschlüsselungsvorgang randomisiert und dadurch das Wiedererkennen einer mehrfachen Verschlüsselung gleicher Klartexte erschwert.

Verschiedene Betriebsarten für Blockchiffren können dabei zunächst nur mit Klartexten umgehen, deren Länge ein Vielfaches der Blockgröße ist. In diesem Fall ist der letzte Block eines gegebenen Klartextes möglicherweise zu kurz und muss entsprechend aufgefüllt werden. Eine Formatierung durch das Auffüllen dieses letzten Blocks zu der geforderten Größe wird auch als *Padding* bezeichnet. In Abschnitt 2.1.3 werden geeignete Padding-Verfahren vorgestellt. Unter den empfohlenen Betriebsarten für Blockchiffren benötigt aber nur der CBC-Modus einen Padding-Schritt.

Die einfachste Möglichkeit, einen Klartext zu verschlüsseln, dessen Länge bereits ein Vielfaches der Blockgröße ist, besteht darin, jeden Klartextblock mit dem gleichen Schlüssel zu verschlüsseln; diese Betriebsart heißt auch Electronic Code Book (ECB). Die Verwendung des ECB-Modus führt jedoch dazu, dass gleiche Klartextblöcke zu gleichen Chiffretextblöcken verschlüsselt werden. Der Chiffretext liefert damit zumindest Informationen über die Struktur des Klartextes und ermöglicht bei niedriger Entropie pro Block des Klartextes ggfs. eine Rekonstruktion von Teilen des Klartextes durch Häufigkeitsanalysen. Aus diesem Grund sollte der n-te Chiffreblock nicht nur vom n-ten Klartextblock und dem eingesetzten Schlüssel abhängen, sondern von einem weiteren Wert, wie beispielsweise dem $(n-1)$-ten Chiffretextblock oder einem Zähler (auch Counter genannt).

Dies ist bei den in Tabelle 2.2 empfohlenen Betriebsarten, die für die in Tabelle 2.1 aufgeführten Blockchiffren geeignet sind, der Fall.

Bemerkung 2.1 Sowohl der GCM-Modus als auch der CCM-Modus liefern bei ausreichender Tag-Länge zusätzlich zur Verschlüsselung eine kryptographisch sichere Datenauthentisierung. Für die beiden anderen Betriebsmodi wird generell empfohlen, separate Mechanismen zur Datenauthentisierung im Gesamtsystem vorzusehen. Idealerweise sollte für nicht authentisierte verschlüsselte Daten keine Entschlüsselung oder sonstige weitere Verarbeitung erfolgen. Wenn nicht authentisierte verschlüsselte Daten entschlüsselt und weiter verarbeitet werden, dann ergeben sich erhöhte Restrisiken im Hinblick auf die Ausnutzung von Fehlerorakeln, siehe zum Beispiel [108].

- Counter with Cipher Block Chaining Message Authentication (CCM), siehe [86],
- Galois/Counter Mode (GCM), siehe [87],
- Cipher Block Chaining (CBC), siehe [85], und
- Counter Mode (CTR), siehe [85].

Tabelle 2.2: Empfohlene Betriebsarten für Blockchiffren.

2.1.2. Betriebsbedingungen

Für die in Abschnitt 2.1.1 aufgeführten Betriebsarten werden Initialisierungsvektoren benötigt, zudem müssen für einen sicheren Betrieb bestimmte weitere Randbedingungen eingehalten werden, die im Folgenden zusammengefasst sind:

Für CCM:

- Die Länge der Authentisierungstags muss geeignet gewählt werden. Für allgemeine kryptographische Anwendungen wird eine Tag-Länge von ≥ 96 Bits empfohlen. Allgemein können Angreifer Chiffrate oder authentisierte Daten bei Verwendung der Tag-Länge t im CCM-Modus mit einer Erfolgswahrscheinlichkeit von $\approx 2^{-t}$ pro Versuch unbemerkt verändern. Bei Verwendung geringerer Tag-Längen als der hier empfohlenen müssen die damit einhergehenden Restrisiken sorgfältig durch einen Experten untersucht werden.

Für GCM:

- Für die GCM-Initialisierungsvektoren wird in [87] eine Bitlänge von 96 Bits empfohlen. Dieser Empfehlung schließt sich die vorliegende Technische Richtlinie an, insbesondere mit Verweis auf die Resultate aus [65].[1] In [87] wird gefordert, dass die Wahrscheinlichkeit einer Wiederholung von Initialisierungsvektoren unter einem gegebenen Schlüssel $\leq 2^{-32}$ sein soll. Daraus ergibt sich ein Schlüsselwechselintervall von höchstens 2^{32} Aufrufen der authentisierten Verschlüsselungsfunktion. Bei einer deterministischen Erzeugung der Initialisierungsvektoren muss nachgewiesen werden, dass eine Wiederholung von Initialisierungsvektoren über die gesamte Lebensdauer eines Schlüssels hinweg ausgeschlossen ist.[2]
- Für allgemeine kryptographische Anwendungen sollte GCM mit einer Länge der GCM-Prüfsummen von mindestens 96 Bits verwendet werden. Für spezielle Anwendungen können nach Rücksprache mit Experten auch kürzere Prüfsummen genutzt werden. In diesem Fall müssen die Richtlinien zur Anzahl der erlaubten Aufrufe der Authentisierungsfunktion mit einem gemeinsamen Schlüssel aus [87] strikt eingehalten werden.

Für CCM, GCM und CTR-Modus:

- Initialisierungsvektoren dürfen sich innerhalb einer Schlüsselwechselperiode nicht wiederholen. Genauer dürfen in dem gesamten Mechanismus keine zwei AES-Verschlüsselungen (das heißt Anwendungen der zugrundeliegenden AES-Blockchiffre) mit gleichen Eingabewerten (Schlüssel, Nachricht) durchgeführt werden. Nichtbeachtung dieser Bedingung führt

[1] In [65] wird auf Fehler in bis dahin akzeptierten Sicherheitsbeweisen zum Galois/Counter Modus hingewiesen und es wird eine korrigierte Analyse der Sicherheit von GCM vorgestellt. In dieser korrigierten Analyse erweist sich eine IV-Länge von exakt 96 Bits als vorteilhaft.

[2] Falls die Wiederholung einer Nonce nicht ausgeschlossen werden kann, bietet sich gegebenenfalls die Verwendung des AES-GCM-SIV-Modus an [52], in welchem Vertraulichkeit und Integrität einer Nachricht auch im Falle einer Nonce-Wiederholung sichergestellt sind.

zu einem potentiell vollständigen Verlust der Vertraulichkeit für die betroffenen Klartextblöcke, im Falle des GCM zusätzlich auch der Integrität.

Für CBC:

- Es dürfen nur unvorhersagbare Initialisierungsvektoren verwendet werden.

Zur Erzeugung unvorhersagbarer Initialisierungsvektoren werden in Abschnitt B.2 verschiedene Verfahren empfohlen. Bei Anwendungen, bei denen die hier angegebenen Anforderungen an die Initialisierungsvektoren nicht erfüllt werden können, wird dringend zur Hinzuziehung eines Experten geraten.

2.1.3. Paddingverfahren

Wie bereits in Abschnitt 2.1.1 erläutert, verlangt der CBC-Modus einen zusätzlichen Padding-Schritt: Es kann bei der Partitionierung eines zu verschlüsselnden Klartextes geschehen, dass der letzte Klartextblock kleiner als die Blockgröße der eingesetzten Chiffre ist.

Folgende Paddingverfahren in dieser Technischen Richtlinie werden empfohlen:

- ISO-Padding, siehe [59], padding method 2 und [85], Appendix A,
- Padding gemäß [54], Abschnitt 6.3,
- ESP-Padding, siehe [68] Abschnitt 2.4.

Tabelle 2.3: Empfohlene Paddingverfahren für Blockchiffren.

Bemerkung 2.2 Beim CBC-Mode ist darauf zu achten, dass ein Angreifer nicht anhand von Fehlermeldungen oder anderen Seitenkanälen erfahren kann, ob das Padding eines eingespielten Datenpakets korrekt war [108]. Allgemeiner gilt folgendes: Wenn ein Angreifer bei Verschlüsselungsverfahren Änderungen am Chiffrat durchführen kann, die zu kontrollierten Änderungen am Klartext führen, darf dem Angreifer keine Seitenkanalinformation zur Verfügung stehen, die Aufschluss darüber liefert, ob ein gegebenes Chiffrat zu einem gültigen Klartext korrespondiert oder ob es von ungültigem Format ist.

2.2. Stromchiffren

Bei Stromchiffren wird aus einem Schlüssel und einem Initialisierungsvektor zunächst ein Schlüsselstrom generiert, das heißt eine pseudozufällige Folge von Bits, die dann auf die zu verschlüsselnde Nachricht bitweise XOR-addiert wird. Zurzeit werden keine dedizierten Stromchiffren empfohlen, allerdings kann AES im Counter Modus als Stromchiffre aufgefasst werden. Wird eine Stromchiffre eingesetzt, wird dringend empfohlen, die Integrität der übertragenen Information durch separate kryptographische Mechanismen zu schützen. Ein Angreifer kann in Abwesenheit solcher Mechanismen bitgenaue Änderungen am Klartext vornehmen.

3. Asymmetrische Verschlüsselungsverfahren

Asymmetrische Verschlüsselungsverfahren werden aufgrund ihrer verglichen mit symmetrischen Standardverfahren geringen Effizienz in der Praxis meist lediglich zur Übertragung symmetrischer Schlüssel eingesetzt, siehe auch Kapitel 8. Die zu verschlüsselnde Nachricht (das heißt der symmetrische Schlüssel) wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Der Empfänger kann dann die Verschlüsselung mit dem zum öffentlichen Schlüssel gehörenden privaten Schlüssel wieder rückgängig machen. Dabei darf es praktisch nicht möglich sein, den Klartext ohne Kenntnis des privaten Schlüssels aus dem Chiffretext rekonstruieren zu können. Dies impliziert insbesondere, dass der private Schlüssel praktisch nicht aus dem öffentlichen Schlüssel berechnet werden können darf. Um eine Zuordnung des öffentlichen Schlüssels zum Besitzer des zugehörigen privaten Schlüssels zu garantieren, wird üblicherweise eine Public-Key-Infrastruktur benötigt.

Für die Spezifizierung von asymmetrischen Verschlüsselungsverfahren sind folgende Algorithmen festzulegen:

- Ein Algorithmus zur Generierung von Schlüsselpaaren (inklusive Systemparameter).
- Ein Algorithmus zum Verschlüsseln und ein Algorithmus zum Entschlüsseln der Daten.

Neben Empfehlungen derartiger Algorithmen werden in der vorliegenden Technischen Richtlinie ebenfalls Empfehlungen zu minimalen Schlüssellängen angegeben, siehe Tabelle 3.1.

Bemerkung 3.1 In diesem Kapitel werden ausschließlich „klassische“ asymmetrische Verschlüsselungsverfahren behandelt, das heißt Verfahren, die auf mathematischen Problemen beruhen, die mit der derzeit verfügbaren Hardware nach heutigem Kenntnisstand nicht effizient zu lösen sind. Diese Situation ändert sich grundlegend, wenn universelle Quantencomputer mit ausreichender Leistungsfähigkeit verfügbar sind: Bereits 1994 wurden von Peter Shor Quantenalgorithmen vorgestellt, die die mathematischen Probleme, auf denen die Sicherheit der heutigen Public-Key-Verfahren beruht, effizient lösen können. Für das Thema „Quantensichere Kryptographie“ sei auf Kapitel 4 verwiesen.

Die derzeit praktisch relevantesten asymmetrischen Verschlüsselungs- und Signaturverfahren beruhen vereinfacht ausgedrückt entweder auf der Schwierigkeit des Problems der Berechnung diskreter Logarithmen in geeigneten Repräsentationen endlicher zyklischer Gruppen (Diskreter-Logarithmus-Problem (DL) oder auf der Schwierigkeit, große ganze Zahlen in ihre Primfaktoren zu zerlegen (Faktorisierungsproblem). Es taucht gelegentlich die Frage auf, welcher dieser beiden Ansätze als kryptographisch sicherer einzuschätzen ist. Die vorliegende Technische Richtlinie sieht die Faktorisierung großer Zahlen, das RSA-Problem, das Problem der Berechnung diskreter Logarithmen in geeigneten Körpern $\mathbb{F}_p$ (p prim), das Problem der Berechnung diskreter Logarithmen in geeigneten elliptischen Kurven, und die entsprechenden Diffie-Hellman-Probleme als gut untersuchte, schwere Probleme an und es gibt in dieser Hinsicht keinen Grund, auf Faktorisierung basierende Verfahren gegenüber Verfahren auf Grundlage diskreter Logarithmen zu bevorzugen oder umgekehrt. Für besonders hohe Sicherheitsniveaus ist die Verwendung von EC-Verfahren aus Effizienzgründen vorteilhaft, siehe hierzu auch Tabelle 3.2.

Bemerkung 3.2 Für asymmetrische Verfahren gibt es in der Regel verschiedene äquivalente, praktisch relevante Darstellungen der privaten und öffentlichen Schlüssel. Die Bitlänge der Schlüssel in einem Datenspeicher kann dabei je nach gewählter Repräsentation der Schlüssel unterschiedlich ausfallen. Für die exakte Definition der Schlüssellänge für die empfohlenen asymmetrischen kryptographischen Verfahren wird daher auf den Eintrag Schlüssellänge im Glossar verwiesen.

Die folgende Tabelle 3.1 gibt einen Überblick über die empfohlenen asymmetrischen Verschlüsselungsverfahren und Schlüssellängen l in Bits.

Verfahren	ECIES	DLIES	RSA
Schlüssellänge l in Bits	250	3000[a]	3000[a]
Referenz	[1, 57]	[1]	[83]
Näheres in	Abschnitt 3.3	Abschnitt 3.4	Abschnitt 3.5

Tabelle 3.1: Empfohlene asymmetrische Verschlüsselungsverfahren sowie Schlüssellängen und normative Referenzen.

[a] Für einen Einsatzzeitraum ab dem Jahr 2023 wird durch die vorliegende Technische Richtlinie empfohlen, RSA/DLIES-Schlüssel von mindestens 3000 Bits Länge zu verwenden, um ein vergleichbares Sicherheitsniveau in allen empfohlenen asymmetrischen Verschlüsselungsverfahren zu erreichen. Übergangsweise bleibt eine Schlüssellänge von $\geq$ 2000 Bits für RSA-Schlüssel bis Ende 2023 konform zur Technischen Richtlinie; ab dem Jahr 2024 wird eine RSA-Schlüssellänge von $\geq$ 3000 Bits verbindlich.

Bemerkung 3.3 Aus den aktuellen Empfehlungen resultiert nur noch ein geringer Puffer zwischen dem durch die empfohlenen ECC-Bitlängen mindestens erreichten Sicherheitsniveau von etwa 125 Bits und dem in dieser Richtlinie angestrebten Sicherheitsniveau von 120 Bits. In bestimmten Anwendungen, die besonders hohe Sicherheitsanforderungen haben oder deren Sicherheit deutlich über den Vorhersagezeitraum dieser Technischen Richtlinie hinaus sichergestellt werden muss, kann es zur Vergrößerung des Sicherheitspuffers daher sinnvoll sein, deutlich größere Schlüssellängen für EC-Verfahren vorzusehen. Die Vorgaben zur Schlüssellänge der Country Signer CA aus [38] lassen sich beispielsweise auf diese Art erklären. Da die Sicherheit von EC-Verfahren von der Annahme abhängt, dass ein Angreifer nichts von der mathematischen Struktur einer gegebenen elliptischen Kurve nutzen kann, um diskrete Logarithmen schneller zu berechnen als es der Pollard-Rho-Algorithmus erlaubt, ist es denkbar, dass in den kommenden Jahren die Anforderungen der vorliegenden Technischen Richtlinie in diesem Bereich als grundsätzliche Vorsichtsmaßnahme erhöht werden. Es wird ferner als grundsätzliche Sicherheitsmaßnahme empfohlen, in EC-Verfahren Kurvenparameter zu verwenden, die nachweisbar zufällig erzeugt wurden, deren Konstruktion nachvollziehbar dokumentiert ist und deren Sicherheit einer gründlichen Analyse unterzogen wurde. Ein Beispiel für solche Kurvenparameter stellen die Brainpool-Kurven [74] dar.

Bemerkung 3.4 Die hier empfohlenen asymmetrischen kryptographischen Funktionen benötigen als Bestandteile weitere Unterkomponenten, wie Hashfunktionen, Message Authentication Codes, Zufallszahlenerzeugung, Schlüsselableitungsfunktionen und/oder Blockchiffren, die ihrerseits zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls den Anforderungen der vorliegenden Richtlinie genügen müssen. In einschlägigen Standards [57] wird teilweise die Verwendung von Verfahren empfohlen, die in der vorliegenden Richtlinie nicht empfohlen werden. Grundsätzlich wird empfohlen, bei der Implementierung eines Standards zwei Grundsätzen zu folgen:

- Für kryptographische Unterkomponenten sollten nur die jeweils in dieser Richtlinie empfohlenen Verfahren verwendet werden.
- Sofern sich dies nicht mit Standardkonformität vereinbaren lässt, ist ein Experte hinzuziehen und die letztlich getroffenen Entscheidungen hinsichtlich der gewählten kryptographischen Unterkomponenten sind ausführlich zu dokumentieren und unter Sicherheitsgesichtspunkten zu begründen.

Bei der Auswahl der empfohlenen asymmetrischen Verschlüsselungsverfahren wurde darauf geachtet, dass lediglich probabilistische Algorithmen[1] zum Einsatz kommen. Insbesondere wird also bei jeder Berechnung eines Chiffretextes ein neuer Zufallswert benötigt. Die Anforderungen an diese Zufallswerte sind teilweise nicht direkt durch die Erzeugung gleichverteilter Werte von fester Bitlänge zu erfüllen. Näheres zu diesen Zufallswerten wird in den Abschnitten zu den entsprechenden Verfahren angegeben.

3.1. Asymmetrische Schlüssellängen

3.1.1. Allgemeine Vorbemerkungen

Die in dieser Technischen Richtlinie enthaltenen Einschätzungen zur Sicherheit kryptograpischer Verfahren und Schlüssellängen sind, wie bereits in der Einleitung erwähnt, nur bis 2028 gültig. Die Beschränkung der Aussagekraft dieser Richtlinie ist für asymmetrische Verschlüsselungsverfahren von besonderer Bedeutung, was im Folgenden kurz erläutert wird. Ferner wird kurz auf die Frage eingegangen, auf welchem Wege die angegebenen Schlüssellängen hergeleitet werden können.

3.1.1.1. Sicherheit asymmetrischer Verfahren

Die Sicherheit von asymmetrischen kryptographischen Verfahren beruht auf der angenommenen Schwierigkeit von Problemen aus der algorithmischen Zahlentheorie. Im Falle von RSA ist dies das Problem, e-te Wurzeln in $\mathbb{Z}_n$ zu berechnen, wobei n eine hinreichend große Zahl von unbekannter Faktorisierung in zwei Primfaktoren p, q und e teilerfremd zu $\varphi(n) = (p-1)(q-1)$ ist. Die Sicherheit von DLIES und ECIES kann (was die asymmetrische Komponente anbelangt) auf das Diffie-Hellman-Problem in den jeweils verwendeten Gruppen zurückgeführt werden. Es existieren damit für alle empfohlenen Verfahren Reduktionen auf mathematische Probleme, die allgemein als schwierig eingeschätzt werden.

Im Vergleich zur Situation bei symmetrischen Verschlüsselungsverfahren, die zwar grundsätzlich durch unvorhergesehene wissenschaftliche Fortschritte ebenfalls in ihrer langfristigen Sicherheit bedroht sind, sind jedoch folgende Punkte hervorzuheben:

- Hinsichtlich des Faktorisierungsproblems für allgemeine zusammengesetzte Zahlen und des Problems der Berechnung diskreter Logarithmen in $\mathbb{F}_p^*$ hat es seit der Einführung asymmetrischer kryptographischer Verfahren größere praktisch relevante Fortschritte gegeben als bei der Kryptoanalyse der am besten untersuchten Blockchiffren.

- Bei symmetrischen Algorithmen kann die Bedrohung durch aktive Angriffe (vor allem Chosen-Plaintext- und Chosen-Ciphertext-Angriffe) durch ein geeignetes Schlüsselmanagement zum Teil abgewehrt werden, insbesondere durch eine sichere Löschung symmetrischer Schlüssel nach Ablauf ihrer vorgesehenen Lebensdauer. Falls ein symmetrisches kryptographisches Verfahren erste Schwächen gegen Chosen-Plaintext- oder Chosen-Ciphertext-Attacken zeigt, kann zudem eine Migration auf ein anderes Verfahren erfolgen. Bei asymmetrischen Kryptosystemen hingegen verfügt ein Angreifer dauerhaft zumindest noch über die zu den ihn interessierenden Chiffraten gehörenden öffentlichen Schlüssel, mit dessen Hilfe möglicherweise Rückschlüsse auf den privaten Schlüssel und damit auch auf den Klartext gezogen werden können, wenn das Verfahren gebrochen ist.

- Die in dieser Richtlinie empfohlenen asymmetrischen Verfahren werden unsicher, falls es zu erheblichen Fortschritten bei der Entwicklung von Quantencomputern kommt.

[1] Der RSA-Algorithmus selbst ist nicht probabilistisch, dafür jedoch das hier empfohlene Paddingverfahren zu RSA.

Verglichen mit der Situation bei digitalen Signaturverfahren kommt hinzu, dass ein Angreifer beliebige Chiffrate, zu denen er Zugang hat, für eine Entschlüsselung zu einem späteren Zeitpunkt abspeichern kann. Das Ziel der Authentizitätssicherung eines signierten Dokumentes dagegen lässt sich durch rechtzeitige Erzeugung einer neuen Signatur auch noch nachträglich sicherstellen, solange der Beweiswert des alten Signaturverfahrens zum Zeitpunkt der Erstellung der neuen Signatur als gegeben angenommen werden kann. Außerdem ist es auf der rechtlichen Seite möglich, Signaturen mit kryptographisch gebrochenen Verfahren zum Zeitpunkt der Signaturprüfung nicht mehr zu akzeptieren, wenn keine Übersignatur mit einem gültigen Verfahren erfolgt ist. Im Gegensatz dazu gibt es bei asymmetrischen Verschlüsselungsverfahren in der Regel keine nachträglichen Maßnahmen zum Schutz der Vertraulichkeit eines Klartextes zu einem gegebenen Chiffrat.

3.1.1.2. Äquivalente Schlüssellängen für symmetrische und asymmetrische kryptographische Verfahren

Den Empfehlungen der vorliegenden Technischen Richtlinie zu den Schlüssellängen asymmetrischer kryptographischer Verfahren liegen Berechnungen zu Äquivalenzen symmetrischer und asymmetrischer Schlüssellängen zugrunde, die auf den folgenden Grundannahmen basieren:

- Für Verfahren basierend auf elliptische Kurven: Es wird angenommen, dass keine Methode existiert, das Diffie-Hellman-Problem auf der verwendeten Kurve wesentlich schneller zu lösen als die Berechnung diskreter Logarithmen auf derselben Kurve. Es wird weiterhin angenommen, dass die Berechnung diskreter Logarithmen auf der verwendeten elliptischen Kurve nicht mit wesentlich geringerer Komplexität (gemessen an der Anzahl der ausgeführten Gruppenoperationen) möglich ist als für generische Darstellungen der gleichen zyklischen Gruppe.[2] Für eine generische Gruppe G wird eine Komplexität der Berechnung diskreter Logarithmen von $\approx \sqrt{|G|}$ Gruppenoperationen angenommen.

- Für RSA und Verfahren basierend auf diskreten Logarithmen in $\mathbb{F}_p^*$: Es wird angenommen, dass über den Vorhersagezeitraum dieser Technischen Richtlinie hinweg keine Angriffe bekannt werden, die bei einer Wahl der Parameter wie in der vorliegenden Richtlinie empfohlen effizienter sind als das allgemeine Zahlkörpersieb. Für RSA und Verfahren basierend auf diskreten Logarithmen in $\mathbb{F}_p^*$ werden gleiche Schlüssellängen empfohlen. Im Fall von Verfahren basierend auf diskreten Logarithmen wird angenommen, dass kein Verfahren existiert, um das Diffie-Hellman-Problem in einer Untergruppe $U \subset \mathbb{F}_p^*$ mit $\mathrm{ord}(U)$ prim effizienter zu lösen als durch Berechnung diskreter Logarithmen in U.

- Es wird angenommen, dass es zu keiner Anwendung von Angriffen mit Hilfe von Quantencomputern kommt.

Diese Annahmen sind insofern aus Angreifersicht pessimistisch, als dass sie keinen Spielraum für strukturelle Fortschritte in der Kryptoanalyse asymmetrischer Verfahren enthalten. Fortschritte, die mit den obigen Annahmen inkompatibel sind, können von sehr spezieller Natur sein und sich zum Beispiel auf neue Erkenntnisse zu *einer einzigen* elliptischen Kurve beziehen. Obwohl grundsätzlich eine Berechnung mit 2^{120} Elementaroperationen für den für diese Richtlinie relevanten Zeitraum als nicht praktisch durchführbar angesehen wird, liegen alle empfohlenen Schlüssellängen oberhalb des in dieser Richtlinie minimal angestrebten 120-Bit-Sicherheitsniveaus. Für RSA-basierte Verfahren wird für das Jahr 2023 übergangsweise noch ein Sicherheitsniveau von 100 Bit akzeptiert.

Im Hinblick auf Verfahren, deren Sicherheit auf der Schwierigkeit der Berechnung diskreter Logarithmen beruht, insbesondere diskreter Logarithmen in elliptischen Kurven, können auch Angriffe

[2] Algorithmen, die auf einer generischen Darstellung einer Gruppe operieren, haben auf Elemente und Gruppenoperationen nur Black-Box-Zugriff. Intuitiv kann man sich etwa ein Orakel vorstellen, das verschlüsselte Gruppenelemente annimmt und das Ergebnis von Gruppenoperationen verschlüsselt ausgibt.

$\log_2(R)$	ECDLP	Faktorisierung/DLP in $\mathbb{F}_p^*$
60	120	700
70	140	1000
100	200	1900
128	256	3200
192	384	7900
256	512	15500

Tabelle 3.2: Ungefährer Rechenaufwand R (in Vielfachen des Rechenaufwandes für eine einfache kryptographische Operation, zum Beispiel das einmalige Auswertung einer Blockchiffre auf einem Block) für die Berechnung diskreter Logarithmen in elliptischen Kurven (ECDLP) beziehungsweise die Faktorisierung allgemeiner zusammengesetzter Zahlen mit den angegebenen Bitlängen.

relevant sein, die einen Orakel-Zugriff auf Operationen mit dem privaten Schlüssel eines Nutzers benötigen. Solche Angriffe können die Berechnung diskreter Logarithmen in einer Gruppe deutlich beschleunigen, siehe etwa Angriffe unter Nutzung eines Static-Diffie-Hellman-Orakels [22, 41].

Zur Abschätzung von Laufzeiten folgen wir [46]. Insbesondere wird wie in [46] angenommen, dass die Faktorisierung einer 512-Bit-Zahl von beliebiger Form etwa dem Rechenaufwand von 2^{50} DES-Operationen entspricht. Unter Verwendung der dort angegebenen Methoden ergeben sich – ohne jegliche Sicherheitsmargen für Fortschritte im Hinblick auf Faktorisierungstechniken beziehungsweise Techniken zur effizienten Berechnung diskreter Logarithmen in den jeweiligen Gruppen – ungefähr die in Tabelle 3.2 wiedergegebenen Äquivalenzen (vergleiche [46, Tabelle 7.2] und [45, Tabelle 4.1]). Hinsichtlich empfohlener Schlüssellängen sei auf Tabelle 3.1 verwiesen.

3.1.2. Schlüssellängen bei langfristig schützenswerten Informationen und in Systemen mit langer vorgesehener Einsatzdauer

Unter *langfristig schützenswerten Informationen* sind für die Zwecke dieses Abschnitts solche Informationen zu verstehen, deren Vertraulichkeit deutlich länger gewahrt bleiben soll als es dem Zeitraum entspricht, für den diese Richtlinie Prognosen über die Eignung kryptographischer Verfahren ausspricht, das heißt deutlich über das Jahr 2028 hinaus. Eine zuverlässige Prognose über die Eignung von kryptographischen Verfahren über den gesamten Lebenszyklus eines Systems hinweg ist in diesem Fall nicht mehr möglich. Es wird empfohlen, unter Hinzuziehung eines Experten über die Minimalforderungen dieser Richtlinie wesentlich hinausgehende Schutzmechanismen vorzusehen. Beispielhaft seien nachfolgend verschiedene Wege zur Risikominimierung erläutert:

- Bei der Neuentwicklung von kryptographischen Systemen mit vorgesehener langer Einsatzdauer wird dazu geraten, die Möglichkeit eines künftigen Betriebs mit höheren Schlüssellängen schon bei der Entwicklung vorzusehen. Auch eine möglicherweise in der Zukunft entstehende Notwendigkeit zum Wechsel der eingesetzten Verfahren beziehungsweise die Durchführung solcher Verfahrenswechsel sollte schon während der Entwicklung des ursprünglichen Systems berücksichtigt werden (Kryptoagilität).

- Bereits bei Einführung des Systems sollten höhere asymmetrische Schlüssellängen als in dieser Richtlinie gefordert eingesetzt werden. Eine naheliegende Möglichkeit besteht darin, für alle Systemkomponenten ein einheitliches Sicherheitsniveau von $\geq$ 128 Bits anzustreben. Hinweise zu den für verschiedene Sicherheitsniveaus minimal erforderlichen asymmetrischen Schlüssellängen können aus Tabelle 3.2 entnommen werden.

- Insgesamt sollte die Menge an Informationen mit langfristigem Schutzbedarf, die über öffentliche Netzwerke übermittelt werden, auf das unbedingt notwendige Maß reduziert werden. Dies gilt insbesondere für Informationen, die mit einem hybriden oder asymmetrischen Kryptoverfahren verschlüsselt übertragen werden.
- Im Bereich des Quantencomputings hat es in den letzten Jahren wesentliche experimentelle und theoretische Fortschritte gegeben. Für den langfristigen Schutz verschlüsselter Informationen ergibt sich dadurch zunehmend ein Bedarf nach einer Absicherung gegen das Risiko von Angriffen mit Quantencomputern, sofern zur Verschlüsselung Public-Key-Verfahren genutzt werden. Die Bedrohung der asymmetrischen Kryptographie durch Quantencomputer und mögliche Gegenmaßnahmen werden in Kapitel 4 behandelt.

Für eine ausführlichere Diskussion über langfristig sichere Schlüssellängen in den bislang verbreiteten asymmetrischen kryptographischen Verfahren sei auf [45, 70] verwiesen.

3.2. Sonstige Bemerkungen

3.2.1. Seitenkanalangriffe und Fault-Attacken

Je nach vorliegender Situation können für asymmetrische Verschlüsselungsverfahren und/oder asymmetrische digitale Signaturverfahren verschiedene Arten von Seitenkanalattacken und/oder Fault-Attacken von Bedeutung sein. Dieses Thema kann in der vorliegenden Richtlinie nicht umfassend behandelt werden. Die Sicherheit einer Implementierung gegen Seitenkanalangriffe und Fault-Attacken muss daher stets im Einzelfall überprüft werden. Detaillierte Empfehlungen zu diesem Thema finden sich für kryptographische Verfahren auf Basis elliptischer Kurven in [33] sowie für RSA, $\mathbb{F}_p$-DH und entsprechende Signaturverfahren in [32].

3.2.2. Public-Key-Infrastrukturen

Die in der vorliegenden Richtlinie beschriebenen asymmetrischen Verschlüsselungsverfahren bieten für sich genommen noch keinerlei Schutz vor Man-in-the-Middle-Angriffen. Die Sicherheitsgarantien der beschriebenen Verfahren sind daher nur gültig, falls Man-in-the-Middle-Angriffe durch zusätzliche Mechanismen zuverlässig verhindert werden können. Dafür muss eine authentische Verteilung der öffentlichen Schlüssel aller Teilnehmer sichergestellt werden.

Dies kann auf verschiedene Arten geschehen, in der Regel kommt eine Public-Key-Infrastruktur (PKI) zum Einsatz. In einer PKI wird das Problem der authentischen Verteilung öffentlicher Schlüssel auf die Verteilung der Wurzelzertifikate der PKI reduziert. Bei der Planung einer PKI für ein asymmetrisches Verschlüsselungs- oder Signaturverfahren wird empfohlen, die folgend aufgelisteten Aspekte zu berücksichtigen. Es handelt sich hierbei nicht um eine erschöpfende Aufzählung von Entwicklungsanforderungen an Public-Key-Infrastrukturen, sondern lediglich um eine Liste mit vergleichsweise generischen Punkten, zu deren Beachtung bei der Entwicklung einer PKI angeraten wird; weitere Informationen finden sich auch in [39]. Bei der Entwicklung und Evaluierung eines konkreten Systems ergeben sich in der Regel weitere Anforderungen, die hier nicht berücksichtigt sind. Die Entwicklung einer geeigneten PKI für eine neue kryptographische Anwendung ist keine triviale Aufgabe und sollte daher nur in enger Abstimmung mit entsprechenden Experten angegangen werden.

- Bei der Ausstellung von Zertifikaten sollte die PKI überprüfen, dass der Antragsteller im Besitz eines privaten Schlüssels zu seinem öffentlichen Schlüssel ist. Dies kann zum Beispiel durch ein Challenge-Response-Verfahren zur Instanzauthentisierung geschehen, das eine Kenntnis des privaten Schlüssels voraussetzt. Auch eine Erzeugung der Schlüsselpaare in einer aus Sicht der PKI sicheren Umgebung ist denkbar, wenn sie mit einem sicheren Transport der erzeugten Schlüsselpaare zum Endnutzer verbunden wird.

- Es sollte Möglichkeiten zur zeitnahen Deaktivierung von Zertifikaten geben und es sollte einem Angreifer nicht möglich sein, unbemerkt zu verhindern, dass einem Teilnehmer zum Zeitpunkt der Prüfung die Information über den aktuellen Status eines Zertifikats zur Verfügung steht.
- Zertifikate sollten nur zeitlich befristet ausgestellt werden.
- Alle Zertifikatsaussteller müssen vertrauenswürdig sein.
- Aus einem Zertifikat sollte hervorgehen, ob es zur Signierung weiterer Zertifikate berechtigt. Generell sollte jedes System, das mit einem Zertifikat in Berührung kommt, eindeutig ermitteln können, wozu dieses Zertifikat verwendet werden darf.
- Die Länge von Zertifikatsketten sollte (durch einen möglichst niedrigen Wert) nach oben beschränkt werden.

3.3. ECIES-Verschlüsselungsverfahren

Ein *Elliptic Curve Integrated Encryption Scheme* (ECIES) ist ein hybrides Verschlüsselungsverfahren, bei dem die Sicherheit der asymmetrischen Komponente auf dem Diffie-Hellman-Problem in der jeweils verwendeten elliptischen Kurve basiert. Im Folgenden wird eine Version von ECIES beschrieben, die mit den übrigen Empfehlungen der vorliegenden Technischen Richtlinie vereinbar ist, wobei sich in der Verfahrensbeschreibung eng an [1] angelehnt wird.

Die hier wiedergegebene Beschreibung von ECIES ist nahezu vollkommen identisch zur Beschreibung des eng verwandten Verfahrens DLIES in Abschnitt 3.4. Der Hauptgrund für eine separate Behandlung beider Verfahren sind potentielle Schwierigkeiten, die sich aus verschiedenen Notationen ergeben könnten, sowie die für beide Verfahren unterschiedlichen Empfehlungen hinsichtlich sicherer Schlüssellängen. Als normative Referenz wird ECIES-HC in [57] empfohlen. Für einen Überblick zur Standardisierung von ECIES und DLIES sei auf [77] verwiesen.

Ein ECIES benötigt folgende Komponenten:

- Symmetrisches Verschlüsselungsverfahren E_K: Alle in der vorliegenden Richtlinie empfohlenen Kombinationen aus Blockchiffre und Betriebsmodus sind hierfür geeignet.
- Message Authentication Code MAC_{KM}: Es können die in Abschnitt 6.2 empfohlenen Verfahren verwendet werden.
- Schlüsselableitungsfunktion H: H kann beispielsweise eine Hashfunktion sein, falls deren Ausgabe mindestens die Länge des gesamten abzuleitenden symmetrischen Schlüsselmaterials besitzt. Alternativ kann auch die in Abschnitt B.1 empfohlene oder eine der in [57] vorgeschlagenen Schlüsselableitungsfunktionen verwendet werden, um aus den gegebenen Daten abgeleitetes Schlüsselmaterial der gewünschten Länge zu erzeugen.

Darüber hinaus benötigt ein ECIES Schlüsselmaterial, wie im folgenden Abschnitt zur Schlüsselgenerierung beschrieben.

Schlüsselgenerierung

1.) Erzeuge kryptographisch starke EC-Systemparameter (p, a, b, P, q, i), siehe Abschnitt B.3.

2.) Wähle d zufällig und gleichverteilt in $\{1, \ldots, q-1\}$.

3.) Setze $G \coloneqq d \cdot P$.

Die EC-Systemparameter (p, a, b, P, q, i) bilden zusammen mit G den öffentlichen Schlüssel und d den privaten Schlüssel. Es wird empfohlen, die in Tabelle B.3 angegebenen Kurvenparameter zu verwenden.

Verschlüsselung Gegeben seien eine Nachricht $M \in \{0,1\}^*$ und ein öffentlicher Schlüssel (p, a, b, P, q, i, G), der auf zuverlässige Weise dem berechtigten Empfänger E der Nachricht zugeordnet werden kann. Zur Verschlüsselung wählt der Sender S eine zufällige Zahl $k \in \{1, \ldots, q-1\}$ und berechnet $B := k \cdot P$, $X := k \cdot G$ und daraus $h := H(X)$. Aus h werden genügend Bits entnommen, um einen Schlüssel K für das symmetrische Verschlüsselungsverfahren sowie einen Schlüssel KM für den MAC zu bilden. Aus der Nachricht M berechnet S das Chiffrat $C := E_K(M)$ sowie einen MAC $T := \mathrm{MAC}_{KM}(C)$ und sendet das Tripel (B, C, T) an den Empfänger E.

Entschlüsselung Der Empfänger E erhält (B, C, T) und berechnet $X := d \cdot B$ sowie damit $h := H(X)$, K und KM. Er bestimmt $T' := \mathrm{MAC}_{KM}(C)$ und überprüft, ob $T = T'$ gilt. Falls dies nicht der Fall ist, bricht er den Entschlüsselungsvorgang ab. Ist $T = T'$, dann erhält E durch $M = E_K^{-1}(C)$ die Nachricht zurück.

Schlüssellänge Für die Ordnung q des Basispunktes P sollte mindestens $q \geq 250$ gelten.

Eine notwendige Voraussetzung für die Sicherheit des ECIES-Verfahrens ist es, dass es praktisch unmöglich ist, das Diffie-Hellman-Problem in der von P erzeugten Untergruppe zu lösen. Dies ist bei den in Tabelle B.3 empfohlenen Kurvenparametern nach derzeitigem Kenntnisstand der Fall.

Bemerkung 3.5 Das vorgestellte ECIES-Verfahren stellt einen probabilistischen Algorithmus dar, da im zweiten Schritt der Schlüsselgenerierung eine Zufallszahl $k \in \{1, \ldots, q-1\}$ zufällig bzgl. der Gleichverteilung auf $\{1, \ldots, q-1\}$ gewählt werden muss. Für empfohlene Algorithmen zur Berechnung der Zufallszahl k sei auf Abschnitt B.4 verwiesen.

3.4. DLIES-Verschlüsselungsverfahren

Ein *Discrete Logarithm Integrated Encryption Scheme* ist ein hybrides Verschlüsselungsverfahren, bei dem die Sicherheit der asymmetrischen Komponente auf der Schwierigkeit des Diffie-Hellman-Problems in einer geeigneten Untergruppe von $\mathbb{F}_p^*$ basiert. Im Folgenden wird eine Version von DLIES beschreiben, die mit den übrigen Empfehlungen der vorliegenden Technischen Richtlinie vereinbar ist, wobei sich in der Verfahrensbeschreibung eng an [1] angelehnt wird.

Ein DLIES benötigt folgende Komponenten:

- Symmetrisches Verschlüsselungsverfahren E_K: Alle in der vorliegenden Richtlinie empfohlenen Kombinationen aus Blockchiffre und Betriebsmodus sind hierfür geeignet.
- Message Authentication Code MAC_{KM}: Es können die in Abschnitt 6.2 empfohlenen Verfahren verwendet werden.
- Schlüsselableitungsfunktion H: H kann beispielsweise eine Hashfunktion sein, falls deren Ausgabe mindestens die Länge des gesamten abzuleitenden symmetrischen Schlüsselmaterials besitzt. Alternativ kann auch die in Abschnitt B.1 empfohlene oder eine der in [57] vorgeschlagenen Schlüsselableitungsfunktionen verwendet werden, um aus den gegebenen Daten abgeleitetes Schlüsselmaterial der gewünschten Länge zu erzeugen.

Darüber hinaus benötigt ein DLIES Schlüsselmaterial, wie im folgenden Abschnitt zur Schlüsselgenerierung beschrieben.

Schlüsselgenerierung

1.) Wähle zufällig eine Primzahl q von geeigneter Bitlänge (siehe Unterabschnitt zu Schlüssellängen).

2.) Wähle k zufällig von einer Bitlänge, die sicherstellt, dass kq von der Länge des zu erzeugenden Schlüssels ist. Wiederhole diesen Schritt, bis $p := kq + 1$ prim ist.

3.) Wähle nun ein $x \in \mathbb{Z}_p^*$ so, dass $x^k \neq 1 \bmod p$ und setze $g := x^k$. Dann ist g ein Element der Ordnung q in $\mathbb{Z}_p^*$.

4.) Wähle zufällig eine natürliche Zahl $a \in \mathbb{N}$ mit $2 \leq a < q$ und setze $A := g^a$.

Dann bilden (p, g, A, q) den öffentlichen Schlüssel und a den privaten Schlüssel.

Verschlüsselung Gegeben seien eine Nachricht $M \in \{0,1\}^*$ und ein öffentlicher Schlüssel (p, g, A, q), der auf zuverlässige Weise dem berechtigten Empfänger E der Nachricht zugeordnet werden kann. Zur Verschlüsselung wählt der Sender S eine zufällige Zahl $b \in \{1, \ldots, q-1\}$ und berechnet $B := g^b$, $X := A^b$ und daraus $h := H(X)$. Aus h werden genügend Bits entnommen, um einen Schlüssel K für das symmetrische Verschlüsselungsverfahren sowie einen Schlüssel KM für den MAC zu bilden. Aus der Nachricht M berechnet S das Chiffrat $C := E_K(M)$ sowie einen MAC $T := \mathrm{MAC}_{KM}(C)$ und sendet das Tripel (B, C, T) an den Empfänger E.

Entschlüsselung Der Empfänger E erhält (B, C, T) und berechnet $X := B^a$ sowie damit weiter $h := H(X)$, K und KM. Er berechnet $T' := \mathrm{MAC}_{KM}(C)$ und prüft, ob $T = T'$ ist. Ist dies nicht der Fall, bricht der Entschlüsselungsvorgang ab. Ist dagegen $T = T'$, dann erhält E durch $M = E_K^{-1}(C)$ die Nachricht zurück.

Schlüssellänge Die Länge der Primzahl p sollte mindestens 3000 Bits betragen, die Länge der Primzahl q sollte mindestens 250 Bits betragen.

Bemerkung 3.6 Das DLIES-Verfahren stellt einen probabilistischen Algorithmus dar, da während der Schlüsselgenerierung mehrere Zufallszahlen benötigt werden, unter anderem eine Zufallszahl $k \in \{1, \ldots, q-1\}$, die zufällig bezüglich der Gleichverteilung auf $\{1, \ldots, q-1\}$ gewählt werden muss. Für empfohlene Algorithmen zur Berechnung der Zufallszahl k sei auf Abschnitt B.4 verwiesen.

Bemerkung 3.7 Die Effizienz des am Anfang des Abschnitts beschriebenen Verfahrens zur Schlüsselerzeugung kann erhöht werden, indem mehrere Nutzer die Werte (p, q, g) verwenden, so dass sie einmalig vorberechnet werden können. Alternativ ist es auch möglich, veröffentlichte Parameter zu verwenden. Die vorliegende Technische Richtlinie empfiehlt in diesem Fall eine Verwendung der MODP-Gruppen aus [69] oder der ffdhe-Gruppen aus [50], jeweils verbunden mit der Wahl geeigneter Schlüssellängen (MODP-1536 ist also zum Beispiel unabhängig vom vorgesehenen Einsatzzeitraum *nicht* geeignet). In den zuvor genannten Gruppen ist jeweils $q = (p-1)/2$ und $g = 2$. Die Verwendung eines gemeinsamen p durch mehrere Nutzer wird nur dann empfohlen, wenn $\log_2(p) \geq 3000$, da die Berechnung diskreter Logarithmen durch Vorberechnungsattacken vereinfacht werden kann, die nur von dem Parameter p abhängen.

3.5. RSA

Das RSA-Verfahren, benannt nach seinen Erfindern R. Rivest, A. Shamir und L. Adleman, ist ein asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln als auch zum digitalen Signieren verwendet werden kann. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Die Sicherheit des Verfahrens beruht auf der angenommenen Schwierigkeit, ganze Zahlen in das Produkt ihrer Primfaktoren zu zerlegen.

Schlüsselgenerierung

1.) Wähle zwei Primzahlen p und q zufällig und unabhängig voneinander aus. Die Zahlen p und q sollten von vergleichbarer Bitlänge sein und nicht zu nah beieinander liegen, da andernfalls, falls beispielsweise p und q unabhängig voneinander aus einem zu kleinen Intervall gewählt werden, Angriffe basierend auf Kenntnis der führenden Bits von p und q möglich sind.

Nähere Hinweise zur Vorgehensweise bei der Primzahlerzeugung finden sich in Abschnitt B.5. Bei einer Wahl von p und q entsprechend Abschnitt B.5 tritt die zuvor genannte Sicherheitslücke nicht auf.

2.) Wähle den öffentlichen Exponenten $e \in \mathbb{N}$ unter den Nebenbedingungen

$$\mathrm{ggT}(e, (p-1)\cdot(q-1)) = 1 \quad \text{und} \quad 2^{16}+1 \leq e \leq 2^{256}-1.$$

3.) Berechne den privaten Exponenten $d \in \mathbb{N}$ in Abhängigkeit von e unter der Nebenbedingung

$$e \cdot d = 1 \bmod \mathrm{kgV}(p-1, q-1).$$

Mit dem sogenannten Modulus $n = p \cdot q$ stellt dann (n, e) den öffentlichen Schlüssel und d den privaten Schlüssel dar. Zusätzlich müssen auch die beiden Primzahlen p und q geheim gehalten werden, da sonst jeder aus dem öffentlichen Schlüssel (n, e) wie unter Punkt 3. den privaten Exponenten berechnen kann. Es wird empfohlen, außer den erzeugten Schlüsseln keine Daten aus der Schlüsselgenerierung persistent abzuspeichern und alle erzeugten Daten nach der Schlüsselgenerierung im Arbeitsspeicher zu überschreiben. Es wird weiter empfohlen, den privaten Schlüssel auf einem geschützten Speichermedium und/oder verschlüsselt so abzuspeichern, dass nur berechtigte Nutzer Entschlüsselungs-Operationen durchführen können.

Bemerkung 3.8 (i) Die Reihenfolge der Wahl der Exponenten während der Schlüsselerzeugung, das heißt erst die Wahl von e und dann die von d, soll die zufällige Wahl kleiner privater Exponenten verhindern, siehe [20].

(ii) Bei der Verwendung probabilistischer Primzahltests zur Erzeugung der beiden Primzahlen p und q sollte die Wahrscheinlichkeit, dass eine der Zahlen doch zusammengesetzt ist, höchstens 2^{-120} betragen, siehe Abschnitt B.5 für geeignete Verfahren.

Ver- und Entschlüsselung Für die Ver- und Entschlüsselung sei auf den Standard [83] verwiesen. Dabei ist zu beachten, dass zusätzlich die Nachricht vor Anwendung des privaten Schlüssels d auf die Bitlänge des Modulus n formatiert werden muss. Das Formatierungsverfahren ist dabei sorgfältig zu wählen, empfohlen wird folgendes Verfahren:

EME-OAEP, siehe [83].

Tabelle 3.3: Empfohlenes Formatierungsverfahren für den RSA-Verschlüsselungsalgorithmus.

Eine Verwendung des älteren PKCS#1v1.5-Paddings wird nicht empfohlen, da sich dabei bereits mehrfach Varianten der Attacke von Bleichenbacher [17] als Problem erwiesen haben, siehe etwa [18] für ein Beispiel aus der jüngeren Vergangenheit.

Schlüssellänge Die Länge des Modulus n sollte mindestens 3000 Bits betragen, siehe auch Tabelle 1.2. Eine notwendige Voraussetzung für die Sicherheit des RSA-Verfahrens ist es, dass es praktisch unmöglich ist, den Modul n ohne Kenntnis von p und q in seine Primfaktoren zu zerlegen. Bei der empfohlenen Mindestbitlänge von 3000 Bits ist das nach derzeitigem Kenntnisstand der Fall.

Bemerkung 3.9 Da der Modulus n sehr groß ist, sind auch die im Rechner verwendeten Bitdarstellungen der Zahlen sehr lang. Der Chinesische Restsatz erlaubt es, die Berechnungen beim Ver- oder Entschlüsseln oder dem Signieren von Nachrichten statt in einer Gruppe der Größe n gleichzeitig in den zwei kleineren Gruppen der Größen p und q durchzuführen und das Ergebnis danach zusammenzusetzen. Da $p, q \ll n$, ist diese Berechnung insgesamt effizienter. Diese Variante wird nach der englischen Bezeichnung des Chinesischen Restsatzes CRT (Chinese remainder theorem) auch CRT-RSA genannt.

Der private Schlüssel besteht in diesem Fall aus den Komponenten $(n, d, p, q, d_p, d_q, q_{\text{inv}})$, wobei

$$d_p = d \bmod p - 1, \qquad d_q = d \bmod q - 1, \qquad q_{\text{inv}} = q^{-1} \bmod p.$$

4. Quantensichere Kryptographie

Im Bereich des Quantencomputings hat es in den letzten Jahren wesentliche experimentelle und theoretische Fortschritte gegeben. Für den langfristigen Schutz verschlüsselter Informationen ergibt sich dadurch zunehmend ein Bedarf nach einer Absicherung gegen das Risiko von Angriffen mit Quantencomputern. Im Folgenden wird das Problem betrachtet, über ein unsicheres Netzwerk hinweg die Vertraulichkeit und Authentizität übermittelter Daten gegen Angreifer zu sichern, die über skalierbare Quantencomputer (und viel klassische Rechenleistung) verfügen. Für eine ausführliche Einführung in die aus Sicht der IT-Sicherheit wichtigsten Entwicklungen im Bereich der Quantentechnologien sowie Handlungsempfehlungen zur Migration auf quantensichere Kryptographie sei auf den BSI-Leitfaden „Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen“ [37] verwiesen.

Eine Möglichkeit, der Bedrohung durch Quantencomputer zu begegnen, stellt die Nutzung eines Public-Key-Verfahrens unter Einbindung eines vorverteilten symmetrischen Geheimnisses dar, etwa indem man dieses in eine Schlüsselaushandlung eingehen lässt. Diese Option eignet sich dann, wenn das benötigte symmetrische Schlüsselmaterial im Vorfeld zuverlässig und sicher an alle Teilnehmer eines Kommunikationskreises verteilt werden kann. Die Kombination symmetrischer und asymmetrischer Methoden zum Schlüsseltransport sorgt in dem Fall dafür, dass ein Angreifer das Gesamtverfahren nur brechen kann, wenn er sowohl das zugrundeliegende Verfahren mit öffentlichen Schlüsseln brechen kann als auch das eingehende symmetrische Geheimnis kennt.

In vielen Fällen ist die Vorverteilung eines symmetrischen Geheimnisses an sämtliche Kommunikationspartner allerdings nicht praktikabel, daher werden aktuell zwei fundamental unterschiedliche Lösungsansätze verfolgt: Zum einen die Ausnutzung quantenphysikalischer Effekte zur sicheren Schlüsselverteilung (englisch *Quantum Key Distribution*, kurz QKD), zum anderen die Verwendung sogenannter *Post-Quanten-Kryptographie* (englisch Post-Quantum-Cryptography, kurz PQC).

Abhängig vom Anwendungsfall sollte frühzeitig, kontinuierlich und angepasst an die aktuellen Entwicklungen im Rahmen eines Risikomanagements abgewogen werden, welche Maßnahmen zu ergreifen sind.

Quantum Key Distribution: Eigenschaften und Anwendbarkeit Im Gegensatz zu Post-Quanten-Kryptographie adressiert QKD das Problem eines sicheren Kommunikationsaufbaus, indem quantenphysikalische Effekte ausgenutzt werden. Allerdings sind die praktischen Einschränkungen von QKD, wie beispielsweise beschränkte Reichweiten und die Notwendigkeit des Einsatzes spezialisierter Hardware, im Vergleich zur Verwendung von PQC-Verfahren stark limitierend und führen dazu, dass QKD nur für spezielle Anwendungsfälle geeignet ist. Da außerdem noch keine standardisierten Protokolle mit zugehörigen Sicherheitsbeweisen vorliegen, spricht das BSI zu diesem Zeitpunkt keine Empfehlung geeigneter Protokolle aus. Sobald die notwendigen Voraussetzungen erfüllt sind, plant das BSI, mittelfristig Empfehlungen zu Protokollen, zur Authentisierung und zur Nutzung von QKD auszusprechen. Unabhängig davon wird das BSI auch in Zukunft die alleinige Nutzung des One-Time-Pads mit über QKD oder über andere Schlüsseleinigungsverfahren vereinbarten Schlüsseln nicht empfehlen.

Post-Quanten-Kryptographie Neben QKD stellt die Verwendung von Post-Quanten-Kryptographie eine weitere Möglichkeit dar, sich vor Angriffen durch Quantencomputer zu schützen. Unter Post-Quanten-Kryptographie versteht man kryptographische Verfahren, die auf klassischer Hardware

ausführbar sind und auf mathematischen Problemen beruhen, die nach heutigem wissenschaftlichen Kenntnisstand auch durch Quantencomputer nicht effizient lösbar sind.

Es gibt inzwischen eine Reihe von Verfahren und Sicherheitsparametern, die kryptographisch geeignet erscheinen, sichere Kommunikationsverbindungen über ein unsicheres Netzwerk hinweg auch dann zu ermöglichen, wenn Angreifer über Quantencomputer verfügen. Die Implementierung dieser Verfahren ist auf Standardhardware möglich und die Sicherheitseigenschaften der resultierenden Systeme sind grundsätzlich identisch zu denen klassischer Public-Key-Verfahren. Somit sind bei der Nutzung von PQC-Verfahren im Vergleich zu QKD deutlich weniger technische Schwierigkeiten zu bewältigen.

Allerdings weisen aktuelle PQC-Verfahren derzeit noch einige praktische Probleme auf: Zum einen ist ihre Standardisierung noch nicht abgeschlossen, so dass es im Vergleich zu klassischen Verfahren bislang nur wenige Forschungsergebnisse zu möglichen Seitenkanalattacken oder Implementierungsfehlern gibt, zum anderen unterscheiden sich ihre Eigenschaften (darunter Schlüssellängen, Speicherplatzbedarf und Rechenzeit) mitunter wesentlich von denen klassischer RSA- und ECC-Verfahren. Ferner müssen bestehende Protokolle angepasst werden, um die Nutzung von PQC-Verfahren zu ermöglichen.

Die internationale Standardisierung von PQC-Verfahren, vor allem durch das amerikanische National Institute of Standards and Technology (NIST), hat inzwischen begonnen und es wurden erste Verfahren zur Standardisierung ausgewählt. Entsprechende Standards werden in den kommenden Jahren erwartet. Eine Einführung aktueller, nicht standardisierter Verfahren in neuen kryptographischen Systemen ist daher immer mit dem Risiko behaftet, Systeme zu erzeugen, die inkompatibel zu für die nahe Zukunft absehbaren Standards sind. In Anwendungen, die die Vertraulichkeit von Informationen mit hohem Wert und langfristigem Schutzbedarf garantieren sollen, wiegen diese Probleme aus Sicht des BSI allerdings weniger schwer als die Möglichkeit künftiger Angriffe. Grundsätzlich wird empfohlen, neue Systeme kryptoagil zu gestalten, siehe im Zusammenhang mit Post-Quanten Kryptographie insbesondere auch [37].

Grover-Angriffe auf symmetrische Kryptographie und andere Angreifermodelle Es gibt zum heutigen Zeitpunkt keine Hinweise darauf, dass symmetrische kryptographische Verfahren durch Quantencomputer in wesentlicher Weise bedroht sind.

Generisch kann ein Angreifer, der über k universelle Quantencomputer verfügt, eine Key-Recovery-Attacke gegen eine Blockchiffre mit einer Schlüssellänge von n Bits bei paralleler Ausführung des Grover-Algorithmus auf allen verfügbaren Quantencomputern innerhalb von $\approx \pi 2^{\frac{n-4}{2}}/\sqrt{k}$ Zeiteinheiten ausführen [51, 110], wobei eine Zeiteinheit der für eine Ausführung der Blockchiffre auf einem Quantencomputer benötigten Zeit entspricht.

Unter der sehr optimistischen Annahme, dass eine *Zeiteinheit* im Fall des AES-128 in einer konkreten Quantencomputer-Implementierung einer Nanosekunde entspricht und dass der Angreifer (etwa aufgrund nicht-idealer Zufallszahlenerzeugung) einen Schlüsselraum der Größe 2^{120} durchsuchen muss, benötigt ein Angriff mit einem einzelnen Quantencomputer ≈ 30 Jahre. Um dies auf ein Jahr zu verkürzen, müsste der Angreifer ≈ 900 baugleiche Quantencomputer parallel rechnen lassen. In Multi-Target-Attacken ist der Vorteil des Angreifers gegenüber klassischen Rechnern geringer.

Für die absehbare Zukunft erscheinen Grover-Angriffe auf symmetrische kryptographische Primitive mit dem in dieser Technischen Richtlinie angestrebten klassischen Sicherheitsniveau daher als nicht relevant. Praktisch können sie dennoch mit geringem Aufwand abgewehrt werden, indem ein höheres klassisches Sicherheitsniveau genutzt wird; zum Beispiel kann anstelle des AES-128 der AES-256 als symmetrische Blockchiffre genutzt werden. In diesem Fall müssen auch die Anforderungen an die genutzten Zufallsquellen entsprechend angepasst werden. Die Nutzung von Mechanismen mit einem klassischen Sicherheitsniveau deutlich über 128 Bits kann auch insofern sinnvoll sein, als dass beispielsweise die Ermittlung eines von l zufälligen AES-128-Schlüsseln generisch einen erwarteten Aufwand von $\approx 2^{127}/l$ hat.

In der Literatur werden teilweise Angriffe diskutiert, in denen eine Verschlüsselung mittels klassischer symmetrischer Primitive auf Quantencomputern ausgeführt und dabei angegriffen wird, siehe etwa [66]. Dieses Angreifermodell wird in der vorliegenden Technischen Richtlinie nicht berücksichtigt.

Empfehlungen Auf dieser Grundlage kommt die vorliegende Technische Richtlinie zu den folgenden Einschätzungen und Empfehlungen, siehe auch [37]:

Empfohlene Verfahren: Die Schlüsselaustauschverfahren FrodoKEM-976 und FrodoKEM-1344 ([4, Abschnitt 2.5]) sowie Classic McEliece mit den Parametern mceliece460896, mceliece6688128 und mceliece8192128 als auch ihren entsprechenden Varianten mceliece460896f, mceliece6688128f und mceliece8192128f [3, Abschnitt 7] werden als kryptographisch geeignet eingeschätzt, um vertrauliche Informationen auf dem in dieser Technischen Richtlinie angestrebten Sicherheitsniveau langfristig zu schützen. Hierbei handelt es sich um eine sehr konservative Einschätzung, die einen erheblichen Sicherheitsspielraum im Hinblick auf künftige kryptoanalytische Fortschritte enthält. Es ist möglich, dass in künftigen Überarbeitungen dieser Richtlinie auch andere Parameterwahlen und PQC-Verfahren als technisch geeignet eingestuft werden.

FrodoKEM wird im Rahmen des PQC-Projektes der NIST nicht standardisiert werden. Dies liegt vor allem an Erwägungen zur Effizienz des Verfahrens, Zweifel an seiner Sicherheit bestehen aktuell nicht [2]. Classic McEliece wurde in die vierte Runde des NIST-Projektes aufgenommen und könnte möglicherweise an deren Ende standardisiert werden. Das BSI hält daher an der Empfehlung von FrodoKEM und Classic McEliece als PQC-Verfahren mit einem hohen Sicherheitsspielraum gegen künftige Angriffe fest.

In Kapitel 6 werden die hashbasierten Signaturverfahren XMSS und LMS sowie ihre Multi-Tree-Varianten empfohlen, die nach aktuellem Kenntnisstand als Quantencomputer-resistent gelten.

Zum jetzigen Zeitpunkt werden in dieser Technischen Richtlinie keine weiteren Post-Quanten-Verfahren empfohlen. Über eine mögliche Aufnahme der vom NIST im Juli 2022 zur Standardisierung ausgewählten Verfahren (siehe [2]) in die Technische Richtlinie wird erst nach Veröffentlichung der Standardisierungsentwürfe entschieden.

Kombination von klassischer und PQC-Sicherheit: Die sichere Implementierung von PQC-Verfahren, insbesondere hinsichtlich Seitenkanalsicherheit, Vermeidung von Implementierungsfehlern und sicherer Implementierung in Hardware, und auch ihre klassische Kryptoanalyse sind deutlich weniger gut untersucht als für RSA- und ECC-basierte kryptographische Verfahren. Außerdem existieren derzeit noch keine standardisierten Versionen dieser Verfahren. Ihr Einsatz in Produktivsystemen wird zum aktuellen Zeitpunkt nur zusammen mit einem klassischen Schlüsselaustausch oder Schlüsseltransport basierend auf ECC- oder RSA-Verfahren empfohlen. Man spricht in diesem Fall von einem sogenannten *hybriden* Verfahren. Parallel zu einem PQC-Schlüsseltransport sollte ein ECC-basierter Schlüsselaustausch unter Verwendung von Brainpool- oder NIST-Kurven mit mindestens 256 Bits Schlüssellänge durchgeführt werden. Die beiden so erzeugten gemeinsamen Geheimnisse sollten mit dem in Abschnitt B.1.1 dieser Technischen Richtlinie angegebenen Verfahren kombiniert werden. Hierbei liefert der Standard [96] in seiner aktuellen Version explizit die Möglichkeit zur Kombination mehrerer Teilgeheimnisse. Ein wie auch hier vorgeschlagenes hybrides Vorgehen wird ferner beispielsweise in [4] als praktikabelste Alternative für einen Einsatz von PQC-Verfahren in der nahen Zukunft beschrieben.

Unter der Voraussetzung, dass die Einschränkungen der in dieser Technischen Richtlinie empfohlenen zustandsbehafteten Verfahren XMSS und LMS sorgfältig berücksichtigt

werden, können diese hashbasierte Signaturen grundsätzlich auch alleine (das heißt, nicht hybrid) zum Einsatz kommen, siehe Kapitel 6.

Perfect Forward Secrecy im PQC-Kontext: Grundsätzlich wird empfohlen, kryptographische Verfahren mit Perfect Forward Secrecy zu verwenden, sofern dies technisch machbar ist. Um in den beschriebenen Verfahren *Perfect Forward Secrecy gegen Quanten-Angreifer* zu erreichen, müssen bei jedem Verbindungsaufbau frische öffentliche Schlüssel erzeugt und authentisiert verteilt werden. Nach Abwägung zwischen Mehraufwand und Restrisiken kann sich hier der kombinierte Einsatz eines PQC-Schlüsseltransports ohne Perfect Forward Secrecy gegen Quanten-Angreifer mit einem klassischen Schlüsseltauschverfahren mit Perfect Forward Secrecy gegen klassische Angreifer anbieten. Solche Verfahren erreichen Perfect Forward Secrecy gegen klassische Angreifer und sichern die Nutzdaten gegen Einsichtnahme durch Quanten-Angreifer *ohne* Zugriff auf den PQC-Langzeitschlüssel. Angreifer *mit* Zugriff auf den PQC-Langzeitschlüssel benötigen zudem für Angriffe auf einzelne Verbindungen einen Quantencomputer.

5. Hashfunktionen

Hashfunktionen $H\colon \{0,1\}^* \to \{0,1\}^n$ spielen in vielen kryptographischen Verfahren eine große Rolle, beispielsweise bei der Ableitung kryptographischer Schlüssel oder bei der Datenauthentisierung. Sie bilden einen Bitstring $m \in \{0,1\}^*$ beliebiger Länge[1] auf einen Bitstring $h \in \{0,1\}^n$ fester Länge $n \in \mathbb{N}$ ab.

Hashfunktionen, die in kryptographischen Verfahren eingesetzt werden, müssen je nach Anwendung die folgenden drei Bedingungen erfüllen:

Einweg-Eigenschaft: Es ist praktisch nicht möglich, für gegebenes $h \in \{0,1\}^n$ einen Wert $m \in \{0,1\}^*$ mit $H(m) = h$ zu finden.

2nd-Preimage-Eigenschaft: Es ist praktisch nicht möglich, für gegebenes $m \in \{0,1\}^*$ einen Wert $m' \in \{0,1\}^* \backslash \{m\}$ mit $H(m) = H(m')$ zu finden.

Kollisionsresistenz: Es ist praktisch nicht möglich, zwei Werte $m, m' \in \{0,1\}^*$ mit $m \neq m'$ und $H(m) = H(m')$ zu finden.

Eine Hashfunktion H, die sämtliche der obigen Bedingungen erfüllt, heißt *kryptographisch stark*.

Mathematisch präziser lassen sich diese drei Begriffe jeweils durch einen Vergleich der besten bekannten Angriffe auf diese Eigenschaften mit optimalen generischen Angriffen fassen. Die Länge des Hash-Outputs ist ein Sicherheitsparameter von zentraler Bedeutung, da er den Aufwand generischer Angriffe bestimmt. Für das in dieser Technischen Richtlinie minimal geforderte Sicherheitsniveau von 120 Bits muss wegen des Geburtstagsparadoxons für eine Hashfunktion $H\colon \{0,1\}^* \to \{0,1\}^n$ mindestens $n \geq 240$ gelten. Eine Fallunterscheidung je nach Einsatzzeitraum des Verfahrens ist an dieser Stelle nicht nötig, da die in dieser Technischen Richtlinie empfohlenen Hashverfahren alle bereits eine Digest-Länge von ≥ 256 Bits aufweisen.

Bemerkung 5.1 Es gibt kryptographische Anwendungen von Hashfunktionen, in denen nicht alle drei angegebenen Eigenschaften einer starken Hashfunktion benötigt werden. Umgekehrt gibt es weitere relevante kryptographische Anforderungen an Hashfunktionen, die sich nicht aus den drei angegebenen Eigenschaften ergeben. Ein Beispiel ist die Eigenschaft der *Zero Finder Resistance* (Resistenz gegen Suche nach Urbildern des Hashwertes Null, [21]), die im Zusammenhang mit ECDSA-Signaturen von Bedeutung ist. Sämtliche der in der vorliegenden Richtlinie empfohlenen Hashverfahren haben im Hinblick auf die in dieser Richtlinie empfohlenen kryptographischen Verfahren, in denen sie eingesetzt werden, keine bekannten kryptographischen Schwächen.

Nach heutigem Kenntnisstand gelten die folgenden Hashfunktionen als kryptographisch stark und sind damit für alle in dieser Technischen Richtlinie genannten Verfahren einsetzbar:

- SHA-256, SHA-512/256, SHA-384 und SHA-512; siehe [90].
- SHA3-256, SHA3-384, SHA3-512; siehe [91].

Tabelle 5.1: Empfohlene Hashfunktionen.

[1] Spezifikationen realer Hashfunktionen beinhalten in der Regel eine Längenbegrenzung, die aber so hoch liegt, dass sie von realen Eingabestrings nicht überschritten wird.

Bemerkung 5.2 Die Hashfunktion SHA-224 ist nicht mehr in der Liste der empfohlenen Algorithmen enthalten; auf der anderen Seite sind mit SHA (= SHA2) und SHA3 zwei Familien von Hashfunktionen vertreten. Diesbezüglich gelten die folgende Anmerkungen:

- SHA-224 ist im Kontext dieser Technischen Richtlinie als Legacy-Mechanismus zu betrachten, ist aber einem Sicherheitsniveau von etwa 112 Bits dennoch weiterhin als recht stark einzuschätzen. Die Streichung begründet sich daraus, dass SHA-224 keine Vorteile gegenüber einer Verwendung von SHA-256 aufweist und dem ab 2023 für diese Richtlinie angestrebten Sicherheitsniveau von 120 Bits nicht entspricht.
- Sowohl die Hashfunktionen der SHA2-Familie als auch die der SHA3-Familie werden als kryptographisch stark eingeschätzt. Im Hinblick auf klassische Angriffe auf Kollisionsresistenz und Einwegeigenschaften ist nach derzeitigem Kenntnisstand kein praktisch relevanter Unterschied zwischen den beiden Funktionenfamilien bekannt. In anderen Anwendungsszenarien gibt es hingegen Unterschiede, zum Beispiel sind die Funktionen der SHA3-Familie resistent gegen Length-Extension-Attacken, siehe auch [9].

Bemerkung 5.3 (i) Für die Hashfunktion SHA1 wurden erstmals in [106] Beispiele von Hashkollisionen angegeben. Aufgrund erheblicher kryptoanalytischer Fortschritte [72, 73] konnten die Kosten für die Berechnung einer solchen Kollision inzwischen auf größenordnungsmäßig 10.000 € reduziert werden, und sogar Angriffe, in denen Nachrichten mit zwei willkürlichen Anfangsstücken zur Kollision gebracht werden sollen, sind in der Reichweite akademischer Angreifer. SHA1 sollte daher niemals als sichere kryptographische Hashfunktion verwendet werden. Eine Verwendung in anderen kryptographischen Anwendungen, etwa im Rahmen einer HMAC-Konstruktion, wird dadurch nicht ausgeschlossen, sollte aber ebenfalls vermieden werden.

(ii) Bereits eine einzige Kollision einer Hashfunktion kann zu einer Unsicherheit bei Signaturverfahren führen, siehe zum Beispiel [76] und [49].

6. Datenauthentisierung

Im Kontext dieser technischen Richtlinie werden unter dem Begriff Datenauthentisierung kryptographische Verfahren verstanden, die sicherstellen, dass übersandte oder gespeicherte Daten nicht durch unbefugte Personen und/oder Anwendungen verändert wurden. Dazu benutzt ein Beweisender (üblicherweise der Sender der Daten) einen kryptographischen Schlüssel zur Berechnung der Prüfsumme der zu authentisierenden Daten. Ein Prüfer (üblicherweise der Empfänger der Daten) überprüft dann, ob die empfangene Prüfsumme der zu authentisierenden Daten mit der übereinstimmt, die er bei Unverfälschtheit der Daten und Verwendung des richtigen Schlüssels erwarten würde.

Bei der Datenauthentisierung werden symmetrische und asymmetrische Verfahren unterschieden. Bei symmetrischen Verfahren verwenden Beweisender und Prüfer den gleichen kryptographischen Schlüssel. Ein Dritter kann in diesem Fall nicht überprüfen, wer die Prüfsumme berechnet hat oder ob sie richtig berechnet wurde. Bei asymmetrischen Verfahren wird der private Schlüssel für die Berechnung der Prüfsumme benutzt und mit dem assoziierten öffentlichen Schlüssel überprüft. Dies wird in der Regel durch digitale Signaturen (siehe Abschnitt 6.3) umgesetzt.

In symmetrischen Verfahren zur Datenauthentisierung kann der Prüfer einer Nachricht somit grundsätzlich auch gefälschte Nachrichten erzeugen. Damit eignen sich solche Verfahren nur dann, wenn das zusätzliche Kompromittierungsrisiko tragbar ist, welches aus der Verteilung des symmetrischen Schlüssels und seiner Verfügbarkeit für (mindestens) zwei Parteien entsteht. Zudem muss es unkritisch sein, wenn die prüfende Partei eine Nachricht fälscht. Ist eine dieser Bedingungen nicht erfüllt, sind symmetrische Datenauthentisierungsverfahren ungeeignet und es müssen digitale Signaturen zum Einsatz kommen. In Szenarien, in denen diese Eigenschaften irrelevant sind, ist der Einsatz symmetrischer Verfahren effizienter. Ein Standardszenario, in dem sich die Verwendung symmetrischer Verfahren zur Datenauthentisierung anbietet, stellt der integritätsgesicherte Transport von verschlüsselten Daten über ein Netzwerk nach Aushandlung ephemerer Schlüssel dar.

6.1. Sicherheitsziele

Beim Einsatz kryptographischer Verfahren zur Datenauthentisierung ist eine Klärung der Sicherheitsziele, die im jeweiligen Szenario erreicht werden sollen, für die Auswahl der Mechanismen von entscheidender Bedeutung. Vereinfacht lassen sich die folgenden Szenarien unterscheiden, die in vielen Anwendungen wichtig sind:

- Sicherung der Integrität von Daten, die über ein Netzwerk übermittelt werden, auf dem Weg vom Sender zum Empfänger: In diesem Anwendungsfall besitzen Sender und Empfänger in der Regel ein gemeinsames Geheimnis, und der Empfänger hat kein Interesse daran, gefälschte Übertragungen zu erzeugen. Es bietet sich somit die Nutzung eines symmetrischen Verfahrens zur Datenauthentisierung an.
- Sicherung der Nichtabstreitbarkeit einer Nachricht: Hier soll sichergestellt werden, dass der Besitzer eines bestimmten Schlüssels zuverlässig als Urheber einer Nachricht identifiziert werden kann und dass der Urheber selbst eine signierte Nachricht nicht so erstellen kann, dass über die Validität der Signatur nachträglich Zweifel entstehen können. In solchen Situationen dürfen die Prüfer einer Nachricht nicht über den entsprechenden Signaturschlüssel verfügen, daher kommt in diesem Fall nur die Verwendung digitaler Signaturen

in Frage. Zudem muss der private Signaturschlüssel je nach konkretem Szenario und angestrebtem Schutzniveau gegebenenfalls auch vor Einsichtnahme durch den Signaturgeber selbst geschützt werden. Dies ist zum Beispiel der Fall, wenn die Gefahr besteht, dass der Signaturersteller vergangene Signaturen durch absichtliche Verbreitung des eigenen privaten Schlüssels nachträglich ungültig machen könnte. Außerdem muss sichergestellt werden, dass dem Empfänger die Nachricht genauso angezeigt wird wie dem Ersteller, und dass etwaige nichtsignierte Anteile (zum Beispiel die nichtsignierte Betreffzeile im Fall einer signierten E-Mail) für den Empfänger und auch für den Ersteller eindeutig als solche identifizierbar sind.

- Absicherung eines asymmetrischen Schlüsseltausches gegen Man-in-the-Middle-Angriffe: In diesem Anwendungsfall steht kein gemeinsames Geheimnis zur Verfügung, so dass eine integritätsgeschützte Übermittlung der Key-Exchange-Nachrichten mittels digitaler Signaturen sichergestellt werden muss.

Bemerkung 6.1 In einigen Anwendungsszenarien kann es zu speziellen Anforderungen an die beteiligten Sicherheitsfunktionen kommen. Zum Beispiel verfolgt eine Codesignatur die Sicherheitsziele der Integrität der übermittelten Anwendung sowie der Nichtabstreitbarkeit möglicherweise enthaltener Schadfunktionen in der ausgelieferten Software, obwohl die signierten Daten in der Regel weder beim Empfänger noch beim Ersteller sinnvoll angezeigt und mit vertretbarem Aufwand inhaltlich geprüft werden können. Die Sicherheitsfunktion der sicheren Anzeige auf Erstellerseite verlagert sich damit vollständig auf die Prozesse zur Qualitätssicherung beim Ersteller sowie auf die Sicherheit der von ihm eingesetzten technischen Komponenten.

Bemerkung 6.2 Bei der Verarbeitung authentisierter Daten dürfen nur die Datenbestandteile, die wirklich signiert wurden, als integer angesehen werden. Die Durchsetzung dieses Grundsatzes ist nicht immer einfach, auch weil für eine Anwendung kritische Fälle unter Umständen in legitim signierten Daten niemals auftauchen. Besonders bei der Verwendung komplexerer Signaturformate (zum Beispiel XML-Signaturen) oder in Kontexten, in denen Sicherheitsziele durch digitale Signaturen durchgesetzt werden sollen, die bei der Entwicklung der eingesetzten Komponenten nicht vorhergesehen wurden, sollte daher immer durch einen Experten gründlich überprüft werden, ob gegebenenfalls zusätzliche Schutzmaßnahmen erforderlich sind.

Bemerkung 6.3 Die Authentizität signierter Daten kann durch eine Signatur unter Umständen noch nicht in ausreichendem Maße garantiert werden, etwa wenn Replay-Attacken möglich sind. Derartige Angriffe müssen durch zusätzliche Maßnahmen unterbunden werden. Im Allgemeinen kann dies durch eine geeignete Kombination von Verfahren zur Datenauthentisierung mit Verfahren zur Durchführung einer Challenge-Response-basierten Instanzauthentisierung erreicht werden. In einigen Anwendungsfällen (zum Beispiel Softwareupdates, Schlüsselupdates) kann auch die Überprüfung mitsignierter Versionszähler oder Zeitstempel ausreichend sein.

6.2. Message Authentication Code (MAC)

Message Authentication Codes sind symmetrische Verfahren zur Datenauthentisierung, die üblicherweise auf Blockchiffren oder Hashfunktionen basieren und zum Einsatz kommen, wenn große Datenmengen authentisiert werden sollen oder wenn Prüfung oder Erstellung von Prüfsummen aus anderen Gründen besonders effizient sein muss. Voraussetzung in diesem Fall ist, dass Beweisender und Prüfer vorab einen gemeinsamen symmetrischen Schlüssel vereinbart haben. Häufig müssen sowohl die Vertraulichkeit als auch die Authentizität der Daten gewährleistet werden, derartige Verfahren werden in Abschnitt A.1 behandelt. In Kapitel 8 werden Verfahren vorgestellt, die den Schlüsselaustausch über unsichere Kanäle ermöglichen.

Grundsätzlich gelten die folgenden Verfahren als sicher, wenn im CMAC-Verfahren und im GMAC-Verfahren eine der in Tabelle 2.1 aufgeführten Blockchiffren bzw. im HMAC-Verfahren eine der in Tabelle 5.1 aufgeführten Hashfunktionen eingesetzt wird und die Länge des Schlüssels für sämtliche Verfahren mindestens 128 Bits beträgt.

- CMAC, siehe [92],
- HMAC, siehe [10],
- GMAC, siehe [87].

Tabelle 6.1: Empfohlene MAC-Verfahren.

Bei der Verwendung dieser Verfahren sind folgende Aspekte zu beachten:

- Bei CMAC und HMAC handelt es sich um pseudozufällige Funktionen, bei GMAC hingegen nicht. Ferner benötigt GMAC im Vergleich zu den anderen beiden Verfahren eine 96 Bit-Nonce als Initialisierungsvektor.
- Als Tag-Länge wird für allgemeine kryptographische Anwendungen in allen drei Verfahren eine Länge von ≥ 96 Bits empfohlen. Kürzere Tag-Längen dürfen nur nach Abwägung aller die jeweilige Anwendung betreffenden Umstände durch Experten verwendet werden. Für GMAC-Tags existieren Angriffe, bei denen Fälschungen von Tags der Länge t für Nachrichten, deren Länge n Blöcke beträgt, mit einer Wahrscheinlichkeit von $2^{-t+\log_2(n)}$ pro Versuch möglich sind und sich diese Wahrscheinlichkeit bei Detektion erfolgreicher Fälschungen weiter steigert [47]. Dies bedeutet, dass GMAC (und damit auch der authentisierte Verschlüsselungsmodus GCM) bei gleicher Tag-Länge einen schwächeren Integritätsschutz liefert als es für CMAC oder HMAC mit den jeweils in dieser Technischen Richtlinie empfohlenen Blockchiffren beziehungsweise Hashfunktionen erwartet wird. Die praktische Relevanz dieser Angriffe wächst erheblich, wenn kurze Authentisierungs-Tags (< 96 Bits) eingesetzt werden. Von einer Verwendung kurzer Tags mit GMAC/GCM wird daher dringend abgeraten.
- Bei der Verwendung des HMAC-Verfahrens sollte die Tag-Länge höchstens auf die Hälfte der Ausgabelänge der Hashfunktion gekürzt werden.
- Hinsichtlich des GMAC-Verfahrens gelten die sonstigen Bemerkungen zu den Betriebsbedingungen für GCM aus Abschnitt 2.1.2 entsprechend, soweit sie die Authentisierungsfunktion betreffen.
- Die verwendeten Authentisierungsschlüssel sind ebenso gut zu schützen wie sonstige kryptographische Geheimnisse im gleichen Kontext.
- Allgemein müssen alle Auflagen aus [10, 92, 87] bei dem jeweils verwendeten Verfahren eingehalten und ihre Einhaltung dokumentiert werden.

Die Tabelle 6.2 fasst die Empfehlungen zu Schlüssel- und Prüfsummenlänge bei Verwendung von MAC-Verfahren zusammen.

6.3. Signaturverfahren

In Signaturverfahren werden die zu signierenden Daten zunächst gehasht, bevor aus diesem Hashwert die Prüfsumme bzw. die Signatur mit dem privaten Schlüssel des Beweisenden berechnet wird.

Verfahren	CMAC	HMAC	GMAC
Schlüssellänge	≥ 128	≥ 128	≥ 128
Tag-Länge empfohlen	≥ 96	≥ 128	≥ 96

Tabelle 6.2: Parameter für empfohlene MAC-Verfahren.

Der Prüfer verifiziert anschließend die Signatur mit dem entsprechenden öffentlichen Schlüssel. Wie schon bei asymmetrischen Verschlüsselungsverfahren darf es dabei praktisch nicht möglich sein, die Signatur ohne Kenntnis des privaten Schlüssels zu berechnen. Dies impliziert insbesondere, dass es praktisch nicht möglich sein darf, den privaten Schlüssel aus dem öffentlichen Schlüssel zu konstruieren.

Zur Verteilung der öffentlichen Schlüssel an die Verifizierer wird üblicherweise eine Public-Key-Infrastruktur genutzt. In jedem Fall ist ein zuverlässiger (vor Manipulationen sicherer) Weg zur Verteilung der öffentlichen Schlüssel wie bei allen Public-Key-Verfahren unerlässlich. Eine tiefgehende Diskussion der technischen und organisatorischen Möglichkeiten zur Lösung dieses Problems geht allerdings deutlich über den Rahmen der vorliegenden Technischen Richtlinie hinaus, das Thema wird daher nur am Rande betrachtet.

Für die Spezifizierung von Signaturverfahren sind folgende Algorithmen festzulegen:

- Ein Algorithmus zur Generierung von Schlüsselpaaren.
- Eine Hashfunktion, die die zu signierenden Daten auf einen Datenblock fester Bitlänge abbildet.
- Ein Algorithmus zum Signieren der gehashten Daten und ein Algorithmus zum Verifizieren der Signatur.

Für die Berechnung des Hashwertes sind grundsätzlich alle der in Tabelle 5.1 aufgelisteten Hashfunktionen geeignet, es verbleibt somit die Angabe der unter dem ersten bzw. dritten Punkt aufgeführten Algorithmen und Schlüssellängen. Zusätzlich werden Empfehlungen für minimale Schlüssellängen angegeben.

Tabelle 6.3 liefert einen Überblick über die im Folgenden empfohlenen Signaturverfahren. Alle empfohlenen Verfahren können sowohl zur Signierung von Daten als auch zum Ausstellen von Zertifikaten genutzt werden.

Nach heutigem Kenntnisstand erreichen bei geeigneter Wahl der Sicherheitsparameter alle hier empfohlenen Signaturverfahren ein vergleichbares Sicherheitsniveau, wenn die privaten Schlüssel zuverlässig geheim gehalten werden und insbesondere nicht aufgrund von Implementierungsschwächen, wie beispielsweise durch Seitenkanäle, Fault-Attacken oder gegen eine bestimmte Art der Schlüsselgenerierung ausgerichtete mathematische Angriffe, ermittelt werden können. Für die Erstellung qualifizierter elektronischer Signaturen im Anwendungsbereich des Vertrauensdienstegesetzes können trotz der grundsätzlich für alle empfohlenen Verfahren gegebenen sicherheitstechnischen Eignung formal abweichende Regelungen greifen. Für dieses Thema sei auf den SOGIS-Leitfaden [104] zur Eignung kryptographischer Algorithmen verwiesen.

Bemerkung 6.4 Mit Ausnahme des DS 3 (vergleiche Tabelle 6.4) sind die empfohlenen asymmetrischen Signaturverfahren probabilistische Algorithmen[1]. Es wird also bei jeder Berechnung einer Signatur ein neuer Zufallswert benötigt, die Anforderungen an diese Zufallswerte werden in den entsprechenden Abschnitten angegeben.

[1] Der RSA-Algorithmus selbst ist deterministisch, nicht aber die hier empfohlenen Paddingverfahren zu RSA (außer DS 3).

- RSA, siehe [58],
- DSA, siehe [61] und [89],
- DSA-Varianten auf elliptischen Kurven:
  - ECDSA, siehe [35],
  - ECKDSA, ECGDSA, siehe [35, 61], und
- Merkle-Signaturen, genauer XMSS oder LMS und ihre Multi-Tree-Varianten nach [55, 78, 95].[a]

Tabelle 6.3: Empfohlene Signaturverfahren.

[a] Merkle-Signaturen unterscheiden sich in wesentlichen Aspekten von den anderen an dieser Stelle empfohlenen Signaturverfahren. Für eine genauere Beschreibung der wichtigsten Punkte wird auf Abschnitt 6.3.4 verwiesen.

Bemerkung 6.5 Merkle-Signaturen gelten im Gegensatz zu allen anderen hier aufgeführten Signaturverfahren als sicher gegen Angriffe unter Nutzung von Quantencomputern [23]. Zudem sind sie als einziges der hier genannten Verfahren *forward secure* im Sinne von [11].

6.3.1. RSA

Die Sicherheit des RSA-Verfahrens beruht auf der angenommenen Schwierigkeit der Berechnung e-ter Wurzeln in $\mathbb{Z}_n$, wobei n eine ganze Zahl von unbekannter Faktorisierung in zwei Primfaktoren p, q ist und e ein Exponent, der zu $\varphi(n) = (p-1)(q-1)$ teilerfremd ist.

Schlüsselgenerierung Die Schlüsselgenerierung verläuft analog wie beim RSA-Verschlüsselungsverfahren, für Details siehe Abschnitt 3.5. Der Signaturprüfschlüssel lautet (n, e), wobei $n = p \cdot q$ zusammengesetzt, e invertierbar $\bmod \varphi(n)$ und $2^{16} < e < 2^{256}$ ist, der Signaturschlüssel lautet $d := e^{-1} \bmod \varphi(n)$.

Signaturerzeugung und Signaturverifikation Für die Signaturerzeugung beziehungsweise -verifikation sei auf [58] verwiesen. Dabei muss vor Anwendung des privaten Schlüssels d auf die Bitlänge des Moduls n zusätzlich der Hashwert der Nachricht formatiert werden. Das Formatierungsverfahren ist sorgfältig zu wählen (siehe zum Beispiel [42]), die folgenden Verfahren werden empfohlen:

- EMSA-PSS, siehe [83].
- Digital Signature Scheme (DS) 2 und 3, siehe [63].

Tabelle 6.4: Empfohlene Formatierungsverfahren für den RSA-Signaturalgorithmus.

Schlüssellänge Die Länge des Modulus n sollte mindestens 3000 Bits betragen, siehe auch Tabelle 1.2.

6.3.2. Digital Signature Algorithm (DSA)

Die Sicherheit des DSA-Verfahrens beruht auf der angenommenen Schwierigkeit der Berechnung diskreter Logarithmen in $\mathbb{F}_p^*$.

Schlüsselgenerierung

1.) Wähle zwei Primzahlen p und q, so dass $q \mid (p-1)$.

2.) Wähle $x \in \mathbb{F}_p^*$ und berechne $g \coloneqq x^{(p-1)/q} \bmod p$.

3.) Falls $g = 1$, gehe zu 2.).

4.) Wähle eine Zahl $a \in \{1, \ldots, q-1\}$ und setze $A \coloneqq g^a$.

Dann ist (p, q, g, A) der öffentliche Schlüssel und a der private Schlüssel.

Signaturerzeugung und Signaturverifikation Für die Signaturerzeugung beziehungsweise -verifikation sei auf [61] und [89] verwiesen. Sowohl Signaturerzeugung als auch Signaturverifikation benötigen eine kryptographische Hashfunktion. Dabei sollte eine der in der vorliegenden Richtlinie empfohlenen Hashfunktionen verwendet werden und die Länge der Hashwerte der Bitlänge von q entsprechen. Falls keine der in Tabelle 5.1 empfohlenen Hashfunktionen eine geeignete Hashlänge aufweisen, sollten die k führenden Bits der Hash-Ausgabe verwendet werden, wobei k die Bitlänge von q bezeichnet. Ist die Länge L_H des Hashwertes *geringer* als die Bitlänge von q, resultiert daraus ein Signaturverfahren mit einem Sicherheitsniveau von (höchstens) $L_H/2$ Bits.

Schlüssellänge Die Länge der Primzahl p sollte mindestens 3000 Bits betragen.

Bemerkung 6.6 Das DSA-Verfahren ist ein so genannter probabilistischer Algorithmus, da zur Berechnung der Signatur eine Zufallszahl $k \in \{1, \ldots, q-1\}$ benötigt wird, die bezüglich der Gleichverteilung auf $\{1, \ldots, q-1\}$ gewählt werden sollte, da andernfalls Angriffe existieren, vergleiche [100]. Zwei Algorithmen zur Berechnung von k werden in Abschnitt B.4 vorgestellt.

Bemerkung 6.7 Zur Erzeugung der Systemparameter siehe Bemerkung 3.7.

6.3.3. DSA-Varianten basierend auf elliptischen Kurven

Die Sicherheit dieser Verfahren beruht auf der angenommenen Schwierigkeit der Berechnung diskreter Logarithmen in elliptischen Kurven.

Schlüsselgenerierung

1.) Erzeuge kryptographisch starke EC-Systemparameter (p, a, b, P, q, i), siehe Abschnitt B.3.

2.) Wähle d zufällig und gleichverteilt in $\{1, \ldots, q-1\}$.

3.) Setze $G \coloneqq d \cdot P$.

Dann bilden die EC-Systemparameter (p, a, b, P, q, i) zusammen mit G den öffentlichen Schlüssel und d den privaten Schlüssel.

Signaturerzeugung und Signaturverifikation Die folgenden Algorithmen werden in der vorliegenden Technischen Richtlinie empfohlen:

- ECDSA, siehe [35].
- ECKDSA, ECGDSA, siehe [35, 61].

Tabelle 6.5: Empfohlene Signaturverfahren basierend auf elliptischen Kurven.

Bei Signaturerzeugung und Signaturverifikation wird eine kryptographische Hashfunktion benötigt. Dabei sind grundsätzlich alle in dieser Technischen Richtlinie empfohlenen Hashfunktionen geeignet. Die Länge der Hashwerte sollte der Bitlänge von q entsprechen. Die sonstigen Hinweise zur Wahl der Hashfunktion aus Abschnitt 6.3.2 gelten entsprechend.

Schlüssellänge Alle in Tabelle 6.5 aufgeführten Signaturverfahren garantieren ein Sicherheitsniveau von n Bits, wenn für die Ordnung q des Basispunktes P die Relation $q \geq 2^{2n}$ gilt und angenommen wird, dass die Berechnung diskreter Logarithmen auf den verwendeten Kurven nicht effizienter möglich ist als durch generische Verfahren. Es wird empfohlen, $q \geq 2^{250}$ zu wählen.

Bemerkung 6.8 Wie das DSA-Verfahren sind alle in diesem Abschnitt empfohlenen Signaturverfahren probabilistische Algorithmen. Auch hier muss ein Zufallswert $k \in \{1, \ldots, q-1\}$ gemäß der Gleichverteilung auf $\{1, \ldots, q-1\}$ gewählt werden, da andernfalls Angriffe existieren, vergleiche [100]. Zwei Verfahren zur Berechnung von k werden in Abschnitt B.4 vorgestellt.

6.3.4. Merkle-Signaturen

Im Gegensatz zu den bisher beschriebenen Signaturverfahren beruht die Sicherheit der in [55, 95, 78] beschriebenen Verfahren nur auf der kryptographischen Stärke einer Hashfunktion und einer pseudozufälligen Funktionenfamilie, nicht jedoch auf der angenommenen Schwierigkeit eines mathematischen Problems (Bestimmung einer Primfaktorzerlegung bzw. Berechnung diskreter Logarithmen in ausgewählten Gruppen). Insbesondere werden keine Annahmen zur Abwesenheit effizienter Lösungsalgorithmen für diese Probleme aus der algorithmischen Zahlentheorie benötigt. Nach aktuellem Kenntnisstand gelten Merklesignaturen im Gegensatz zu den anderen in dieser Technischen Richtlinie empfohlenen Signaturverfahren auch gegen Angriffe unter Verwendung von Quantencomputern als sicher.[2]

Die generell geringen komplexitätstheoretischen Annahmen, die der Sicherheit von Merkle-Signaturen zugrundeliegen, lassen Merkle-Signaturen als eine gute Methode für die Erstellung langfristig sicherer Signaturen erscheinen. Dies gilt auch unter der Annahme, dass Angriffe durch Quantencomputer über den Zeitraum hinweg, in dem die Signatur gültig bleiben soll, keine Anwendung finden.

Allerdings kann bei Verwendung von Merkle-Signaturen – anders als bei den restlichen, in der vorliegenden Technischen Richtlinie beschriebenen Signaturverfahren – mit einem gegebenen öffentlichen Schlüssel jeweils nur eine begrenzte Anzahl von Nachrichten authentifiziert werden. Bei den Single-Tree-Varianten XMSS und LMS ist die Rechenzeit zur Erzeugung des öffentlichen Schlüssels proportional zu dieser maximalen Anzahl der mit einem Schlüsselpaar authentisierbarer Nachrichten und damit vergleichsweise lang. Wenn eine große Anzahl von Nachrichten ohne zwischenzeitliche Erzeugung und authentisierte Verteilung eines neuen öffentlichen Schlüssels signiert werden soll, wird der Einsatz der Multi-Tree Varianten XMSS^MT und HSS empfohlen.

[2] Eine Diskussion der Quantencomputer-Sicherheit der Kollisionsresistenz von Hashfunktionen findet sich in [12].

6.3.5. Langfristige Beweiswerterhaltung für digitale Signaturen

Unabhängig von den vorliegenden Empfehlungen zu Verfahren und Schlüssellängen für digitale Signaturen wird dazu geraten, die Möglichkeit künftiger Umstellungen der Systeme auf neue Signaturverfahren oder längere Signaturschlüssel schon bei der Entwicklung zu berücksichtigen, wenn die vorgesehene Zeitdauer, über die hinweg die Authentizität und Integrität der durch ein System zur Datenauthentisierung zu schützenden Daten gesichert bleiben soll, den Vorhersagezeitraum der vorliegenden Richtlinie deutlich übersteigt. Dies sollte Mechanismen zur Übersignierung alter signierter Dokumente unter Verwendung der aktualisierten Verfahren mit einschließen. Nähere Informationen zu diesem Thema finden sich in der Technischen Richtlinie TR-03125 (TR-ESOR) [28].

7. Instanzauthentisierung

Unter Instanzauthentisierung werden in dieser Technischen Richtlinie kryptographische Protokolle verstanden, in denen ein Beweisender einem Prüfenden den Besitz eines Geheimnisses nachweist. Bei symmetrischen Verfahren ist dies ein symmetrischer Schlüssel, der vorab ausgetauscht werden muss. Bei asymmetrischen Verfahren zeigt der Beweisende, dass er im Besitz eines privaten Schlüssels ist. Hierfür wird in der Regel eine PKI benötigt, damit der Prüfende dem Beweisenden den zugehörigen öffentlichen Schlüssel zuordnen kann. Passwortbasierte Verfahren dienen in erster Linie der Freischaltung von Chipkarten oder anderen kryptographischen Komponenten. Hier beweist der Inhaber der Komponente, dass er im Besitz eines Passwortes oder einer PIN ist.

Die Authentisierung sollte – wo sinnvoll und möglich – gegenseitig erfolgen und kann mit einer Schlüsseleinigung einhergehen, um die Vertraulichkeit und Integrität einer anschließenden Kommunikation zu gewährleisten, siehe Kapitel 8 für empfohlene Schlüsselaustausch- und Schlüsseleinigungsverfahren und Abschnitt A.2 für empfohlene Protokolle, die beide Verfahren kombinieren.

In diesem Kapitel werden für die ersten beiden Verfahren (Abschnitte 7.1 und 7.2) nur allgemeine Ideen zur Instanzauthentisierung angegeben und lediglich die entsprechenden kryptographischen Primitive empfohlen. Für die benötigten kryptographischen Protokolle sei auf Abschnitt A.2 verwiesen. Insbesondere werden dort auch Empfehlungen für Schlüssellängen etc. angegeben.

7.1. Symmetrische Verfahren

Für den Nachweis eines Beweisenden (B) gegenüber einem Prüfenden (P), dass B im Besitz des geheimen symmetrischen Schlüssels ist, sendet P einen Zufallswert r an B. Damit das Verfahren das in der vorliegenden Technischen Richtlinie minimal angestrebte Sicherheitsniveau erreicht, sollte r mindestens 120 Bits Min-Entropie besitzen. Wird eine große Anzahl von Authentisierungsverfahren mit dem gleichen privaten Schlüssel durchgeführt, dann sollte die Wahrscheinlichkeit einer Kollision zweier dieser Challenge-Werte auf $\leq 2^{-32}$ beschränkt werden. B berechnet anschließend mittels des gemeinsamen privaten Schlüssels K eine Prüfsumme von r und schickt diese zurück an P, der diese dann prüft. Derartige Verfahren heißen auch *Challenge-Response-Verfahren*, siehe Tabelle 7.1 für eine schematische Darstellung.

Beweisender (B)		Prüfender (P)
		Wähle Zufallswert r
	$\xleftarrow{r}$ (Challenge)	
Berechne Prüfsumme c		
	$\xrightarrow{c}$ (Response)	
		Verifiziere Prüfsumme

Tabelle 7.1: Schematische Darstellung eines Challenge-Response-Verfahren zur Instanzauthentisierung.

Die Berechnung und Verifikation der Prüfsumme hängt vom gewählten Verfahren ab. Grundsätzlich können alle in Kapitel 2 empfohlenen Verschlüsselungsverfahren und alle in Abschnitt 6.2

empfohlenen MAC-Verfahren eingesetzt werden. Für empfohlene Bitlängen und Nebenbedingungen an die benutzten Zufallswerte sei auf Abschnitt A.2 verwiesen.

7.2. Asymmetrische Verfahren

Auch für asymmetrische Verfahren werden Challenge-Response-Protokolle zur Instanzauthentisierung eingesetzt. Hierfür berechnet der Beweisende mit seinem privaten Schlüssel eine Prüfsumme zu einem vom Prüfer gesendeten Zufallswert r. Der Prüfende verifiziert dann die Prüfsumme mit Hilfe des zugehörigen öffentlichen Schlüssels. Grundsätzlich können hierfür alle in Abschnitt 6.3 empfohlenen Verfahren eingesetzt werden. Für empfohlene Bitlängen und Nebenbedingungen an die benutzten Zufallswerte siehe ebenfalls Abschnitt A.2.

Bemerkung 7.1 Wenngleich die in Abschnitt 6.3 empfohlenen Signaturverfahren zur Datenauthentisierung auch zur Instanzauthentisierung genutzt werden können, sollte darauf geachtet werden, dass die eingesetzten Schlüssel verschieden sind, das heißt, dass ein Schlüssel zur Erzeugung von Signaturen nicht zur Instanzauthentisierung eingesetzt wird. Dies muss in den entsprechenden Zertifikaten für die öffentlichen Schlüssel kenntlich gemacht werden.

7.3. Passwortbasierte Verfahren

Passwörter zum Freischalten der auf kryptographischen Komponenten (beispielsweise Signaturkarten) zur Verfügung gestellten kryptographischen Schlüssel sind meist kurz, damit sich der Inhaber der Komponente das Passwort merken kann. In vielen Situationen ist zudem der erlaubte Zeichensatz begrenzt auf die Ziffern $0, \ldots, 9$; in diesem Fall spricht man auch von PIN statt Passwort. Um trotzdem ein ausreichendes Sicherheitsniveau zu erreichen, wird die Anzahl der Zugriffsversuche üblicherweise begrenzt.

7.3.1. Empfohlene Passwortlängen für den Zugriff auf kryptographische Hardwarekomponenten

Folgende Passwortlängen und Anzahl der Zugriffsversuche für den Zugriff auf kryptographische Hardwarekomponenten Nebenbedingungen werden empfohlen:

- Es wird grundsätzlich empfohlen, Passwörter mit einer Entropie von mindestens $\log_2(10^6)$ Bits zu verwenden. Dies kann zum Beispiel durch eine ideal zufällige Vergabe sechsstelliger PINs erreicht werden.
- Die Anzahl der aufeinanderfolgenden erfolglosen Zugriffsversuche muss stark eingeschränkt werden. Bei einer Passwortentropie von $\log_2(10^6)$ Bits wird eine Beschränkung auf drei Versuche empfohlen.

Tabelle 7.2: Empfohlene Passwortlängen und Anzahl der Zugriffsversuche für den Zugriffsschutz kryptographischer Komponenten.

Bemerkung 7.2 Werden Zugriffs-Passwörter für kryptographische Komponenten nicht (zumindest annähernd) ideal zufällig durch einen technischen Prozess erzeugt, sondern durch den Nutzer gewählt, wird dringend eine Sensibilisierung des Nutzers bezüglich der Auswahl sicherer Passwörter

empfohlen. Ferner wird in diesem Fall empfohlen, von der Verwendung rein numerischer Passwörter (PINs) abzusehen. Für Passwörter, die über einem Alphabet gebildet werden, das mindestens die Buchstaben A-Z, a-z, 0-9 und gegebenenfalls Sonderzeichen enthält, wird eine Länge von acht Zeichen empfohlen. Zudem wird empfohlen, Maßnahmen zu treffen, die die Wahl naheliegender Passwörter (zum Beispiel beliebige einzelne Wörter der Landessprache oder einer wichtigen Fremdsprache sowie Datumsangaben in naheliegenden Formaten) ausschließen.

Bemerkung 7.3 In manchen Anwendungen kann nach Abwägung sämtlicher Umstände durch Experten auch eine Nutzung von Passwörtern mit geringerer Entropie als oben empfohlen mit der vorliegenden Richtlinie kompatibel sein. Ein einzelner unautorisierter Zugriffsversuch sollte dabei aber wenigstens niemals mit einer Erfolgswahrscheinlichkeit größer als $\approx 10^{-4}$ erfolgreich sein. Die Anzahl der aufeinanderfolgenden erfolglosen Zugriffsversuche muss stark eingeschränkt werden, die genauen Beschränkungen sind dabei abhängig von der Anwendung. Die Restrisiken sollten gründlich dokumentiert werden und es wird empfohlen, den berechtigten Nutzer falls möglich über erfolgte unberechtigte Zugriffsversuche zu informieren, auch wenn die Komponente in deren Folge nicht gesperrt wurde.

Bemerkung 7.4 (i) Um Denial-of-Service Attacken oder eine versehentliche Sperrung der Komponente zu verhindern, muss ein Mechanismus zum Aufheben einer Sperrung vorgesehen sein. Die Entropie des Schlüssels zur Entsperrung (englisch *Personal Unblocking Key*, kurz PUK) sollte mindestens 120 Bits betragen, wenn Offline-Attacken denkbar sind.

(ii) Wenn keine Offline-Angriffe auf den PUK möglich sind, wird empfohlen, einen PUK mit mindestens 32 Bits Entropie zu verwenden (zum Beispiel 10 Ziffern) und nach einer relativ geringen Anzahl von Zugriffsversuchen (zum Beispiel 20) die in der Komponente enthaltenen kryptographischen Geheimnisse unwiderruflich zu löschen.

(iii) Die allgemeine Empfehlung von mindestens etwa 20 Bits Entropie für das in einem passwortbasierten Authentisierungsverfahren verwendete Passwort gilt nur für die Authentisierung einer Sicherheitskomponente gegenüber, die keine Offline-Angriffe erlaubt und die die angegebenen Beschränkungen hinsichtlich der Anzahl zulässiger Zugriffsversuche zuverlässig durchsetzen kann. In anderen Situationen, in denen diese Bedingungen nicht erfüllt sind (zum Beispiel wenn aus dem Passwort direkt ein kryptographisches Geheimnis abgeleitet wird, das Zugriff zu sensitiven Informationen verschafft), wird empfohlen, Passwörter über ein Verfahren auszuwählen, das mindestens 120 Bits Entropie liefert. Für den Zugang zu Daten oder für die Authentisierung von Transaktionen mit hohem Schutzbedarf wird grundsätzlich von einer Ein-Faktor-Authentisierung abgeraten. Stattdessen wird in dieser Situation eine Zwei-Faktor-Authentisierung durch Wissen (Kenntnis eines Passwortes) und Besitz (einer sicheren Hardwarekomponente) empfohlen.

7.3.2. Empfohlene Verfahren zur Passwort-basierten Authentisierung gegenüber kryptographischen Hardwarekomponenten

Für kontaktbehaftete Chipkarten kann derzeit noch auf eine kryptographische Absicherung der Übertragung der PIN an die Chipkarte abgesehen werden, wenn das Kartenterminal selbst als vertrauenswürdig eingestuft werden kann und ein physikalischer Abgriff beziehungsweise eine Manipulation der zwischen Leser und Karte übertragenen Information durch geeignete Maßnahmen in der Einsatzumgebung verhindert wird. Allerdings wird auch hier die kryptographische Absicherung (im Hinblick auf Integrität und Vertraulichkeit der übertragenen Identifizierungsdaten) empfohlen. Grundsätzlich eignen sich dafür die gleichen Verfahren wie für kontaktlose Karten.

Bei kontaktlosen Chipkarten kann die Kommunikation zwischen Kartenleser und Chipkarte auch noch aus einiger Entfernung mitgelesen werden. In diesem Fall kann das Passwort zur Freischaltung der Chipkarte also nicht einfach vom Kartenleser zur Chipkarte gesendet werden.

Folgendes passwortbasiertes Verfahren wird für den Zugriffsschutz auf kontaktlose Chipkarten empfohlen:

PACE: Password Authenticated Connection Establishment, siehe [34].

Tabelle 7.3: Empfohlenes passwortbasiertes Verfahren für den Zugriffsschutz auf kontaktlose Chipkarten.

Das in Tabelle 7.3 empfohlene Verfahren beweist der kontaktlosen Chipkarte nicht nur, dass der Benutzer im Besitz des korrekten Passwortes ist, sondern führt gleichzeitig ein Schlüsseleinigungsverfahren durch, so dass im Anschluss eine vertrauliche und authentisierte Kommunikation durchgeführt werden kann.

Bemerkung 7.5 Auch bei dem in Tabelle 7.3 empfohlenen Verfahren muss die Anzahl der Versuche beschränkt sein. Es wird empfohlen, die Chipkarte nach drei erfolglosen Versuchen zu sperren. Die weiteren Bemerkungen aus Abschnitt 7.3.1 gelten entsprechend.

8. Schlüsseleinigungsverfahren, Schlüsseltransportverfahren und Key-Update

Schlüsseleinigungsverfahren dienen dem Austausch eines Verschlüsselungsschlüssels über einen unsicheren Kanal. Diese Verfahren müssen unbedingt mit Instanzauthentisierungsverfahren kombiniert werden, da ansonsten keine Möglichkeit besteht zu entscheiden, mit welcher Partei die Schlüsseleinigung durchgeführt wird. Eine Datenauthentisierung allein genügt nicht, da ein Angreifer eine in der Vergangenheit durchgeführte Kommunikation mitgeschnitten haben könnte, um die aufgezeichneten Daten für einen Angriff zu nutzen. Aus diesem Grund werden in diesem Kapitel wie bereits in Kapitel 7 nur allgemeine Ideen für Schlüsseleinigungsverfahren angegeben und für konkrete Verfahren, das heißt für Schlüsseleinigungsverfahren, die auch eine Instanzauthentisierung beinhalten, wird auf Abschnitt A.2 verwiesen.

Nach erfolgreicher Schlüsseleinigung befinden sich beide Parteien im Besitz eines gemeinsamen Geheimnisses. Für empfohlene Verfahren zur Generierung symmetrischer Schlüssel aus diesem Geheimnis siehe Abschnitt B.1. Im Wesentlichen wird für diese Aufgabe die Verwendung einer Schlüsselableitungsfunktion empfohlen. In manchen Situationen kann es sinnvoll sein, ein vorverteiltes Geheimnis in die Schlüsselableitungsfunktion eingehen zu lassen. Damit kann zum Beispiel eine Separierung verschiedener Benutzergruppen erreicht werden. Auch ein zusätzlicher Schutz gegen Angriffe auf das Schlüsseleinigungsverfahren kann auf diese Weise erreicht werden. Hinsichtlich einer Separierung verschiedener Benutzergruppen kann es zudem sinnvoll sein, weitere öffentliche Daten, die spezifisch für beide Kommunikationspartner sind, bei der Schlüsselableitung zu berücksichtigen.

Es wird empfohlen, nur Schlüsseleinigungsverfahren zu verwenden, in denen die jeweiligen Kommunikationspartner gleiche Anteile für den zu generierenden Schlüssel bereitstellen. Beide Seiten sollten dabei mindestens 120 Bits Entropie beitragen. Bei der Auswahl eines Schlüsseleinigungsverfahrens für eine bestimmte Anwendung sollte auch in Betracht gezogen werden, ob in dem gewählten Protokoll eine Seite unter Umständen eine größere Kontrolle über das Schlüsselmaterial hat als die andere und ob eine derartige Asymmetrie in der gegebenen Anwendung sicherheitsrelevante Auswirkungen haben kann.

Neben Schlüsseleinigungs- sind auch Schlüsseltransportverfahren von praktischer Relevanz. Im Rahmen eines Schlüsseltransportverfahrens werden geheime Schlüsseldaten von einer Stelle erzeugt und gesichert zu einem oder mehreren Empfängern transportiert. Die erzeugende Stelle kann eine vertrauenswürdige Drittpartei oder einer der Kommunikationsteilnehmer sein. Im letzteren Fall wird empfohlen, dass alle Teilnehmer nur jeweils selbst erzeugte Schlüssel zur Übertragung eigener sensibler Daten nutzen. Die Empfänger haben an dieser Stelle keine Kontrolle über die verteilten Sitzungsschlüssel.

Schließlich werden in diesem Kapitel auch Key-Update-Verfahren behandelt. Hier teilen zwei Parteien bereits ein gemeinsames Geheimnis und leiten daraus am Ende einer Schlüsselperiode einen neuen Schlüssel ab. Dies kann entweder durch Ableitung neuer Sitzungsschlüssel aus einem dauerhaften Masterschlüssel oder auch durch eine Update-Prozedur, die aus dem aktuellen Schlüssel und gegebenenfalls weiteren Daten einen neuen Schlüssel generiert, erreicht werden. Bei der Festlegung der Lebensdauer von Schlüsselmaterial müssen verschiedenen Faktoren berücksichtigt werden, darunter die Art des Schlüssels, die Einsatzumgebung oder die Sensitivität der zu schützenden Daten. Weitere Informationen zu diesem Thema finden sich beispielsweise in [97].

Bemerkung 8.1 Werden kryptographische Schlüssel mit einem Schlüsseleinigungsverfahren ausgehandelt oder mit einem Schlüsseltransportverfahren gesichert übermittelt, so besitzen diese Schlüssel beziehungsweise die kryptographischen Verfahren, die diese Schlüssel verwenden, maximal das gleiche Sicherheitsniveau wie das Schlüsseleinigungs- bzw. Schlüsseltransportverfahren. Da die Möglichkeit besteht, dass ein Angreifer die Kommunikation bei der Schlüsseleinigung bzw. beim Schlüsseltransport aufzeichnet, haben geänderte Empfehlungen für Schlüsseleinigungs- oder Schlüsseltransportverfahren auch Auswirkungen auf zuvor ausgehandelte bzw. übertragene Schlüssel. Wenn beispielsweise das Schlüsseleinigungs- bzw. Schlüsseltransportverfahren die Konformität zu dieser Technischen Richtlinie verliert, so sollten auch die damit ausgehandelten bzw. übertragenen Schlüssel nicht mehr eingesetzt werden.

Bemerkung 8.2 (Asymmetrische versus symmetrische Schlüsseleinigungsverfahren) Mit asymmetrischen Schlüsseleinigungsverfahren können Sicherheitseigenschaften erfüllt werden, die allein unter Verwendung symmetrischer Kryptographie nicht realisierbar sind. Zum Beispiel erfüllen beide empfohlenen asymmetrischen Schlüsseleinigungsverfahren die Eigenschaft, dass ein Angreifer, der alle gegebenenfalls vorhandenen Langzeitgeheimnisse beider Kommunikationsteilnehmer kennt[1], dennoch nicht den während einer unkompromittierten Protokollausführung ausgehandelten Schlüssel ermitteln kann, falls er das dem verwendeten asymmetrischen Verfahren zugrundeliegende mathematische Problem (hier: das Diffie-Hellman-Problem) nicht effizient lösen kann. Im Vergleich dazu kann in symmetrischen Schlüsseleinigungsverfahren höchstens das Sicherheitsziel *Post-Compromise Security* erreicht werden, das heißt, dass ein Angreifer, der alle Langzeitgeheimnisse beider Teilnehmer kennt, die Ergebnisse *vergangener* korrekt durchgeführter Schlüsseleinigungen nicht ermitteln kann.[2]

8.1. Symmetrische Verfahren

Schlüsseltransport Grundsätzlich können alle der in Kapitel 2 empfohlenen symmetrischen Verschlüsselungsverfahren zum Transport von Sitzungsschlüsseln verwendet werden. Es wird empfohlen, ein in Kapitel 2 empfohlenes Verschlüsselungsverfahren mit einem MAC aus Abschnitt 6.2 zu kombinieren (im Encrypt-then-MAC-Modus), um eine manipulationssichere Übertragung des Schlüsselmaterials sicherzustellen.

Schlüsseleinigung Wenn die Existenz eines gemeinsamen langfristigen Geheimnisses vorausgesetzt werden kann, lassen sich auch Schlüsseleinigungsverfahren auf Basis ausschließich symmetrischer Verfahren realisieren. Key Establishment Mechanism 5 aus [60] stellt ein geeignetes Verfahren dar. Falls eine implizite Schlüsselbestätigung durch Besitz gleicher Sitzungsschlüssel für die jeweils gegebene kryptographische Anwendung nicht ausreichend ist, wird empfohlen, dieses Protokoll noch um einen Schritt zur Schlüsselbestätigung zu erweitern. Als Key Derivation Function sollte dabei der in Abschnitt B.1 empfohlene Mechanismus verwendet werden.

Key Update In manchen Situationen kann es erforderlich sein, die in einem kryptographischen System genutzten Schlüssel synchron bei allen Beteiligten auszutauschen, ohne dass ein erneuter Schlüsselaustausch oder weitere Kommunikation stattfindet. In diesem Fall können Key-Update-Mechanismen zum Einsatz kommen. Unter der Annahme, dass der Masterschlüssel K_t eines Kryptosystems zum Zeitpunkt t über ein solches Verfahren ersetzt werden soll, empfehlen wir

$$K_{t+1} \coloneqq \mathrm{KDF}(s, \mathrm{Label}, \mathrm{Context}, L, K_t)$$

[1] Gemeint sind hier in erster Linie die langfristigen Geheimnisse, die zur Absicherung der Verbindung gegen Man-in-the-Middle-Attacken verwendet werden müssen.

[2] *Merkle Puzzles* stellen in diesem Zusammenhang insofern eine Ausnahme dar, als dass es sich dabei um ein Schlüsseleinigungsverfahren mit öffentlichen Schlüsseln unter ausschließlicher Nutzung symmetrischer Primitive handelt [81]. Dieses Verfahren ist aber nur von akademische Bedeutung.

zu setzen. Hierbei bezeichnet KDF eine zweischrittige kryptographische Schlüsselableitungsfunktion nach [96, Abschnitt 5], und s ist der dabei im Extraktionsschritt genutzte Salt-Wert. Die Parameter Label und Context gehen in dem in [96] vorgesehenen Expansionsschritt gemäß [98] ein. Dabei ist Label ein String, der die Funktion des abzuleitenden Schlüssels kenntlich macht und Context enthält Informationen zum weiteren Protokollkontext. L bezeichnet die Länge des abzuleitenden Schlüssels K_{t+1} und fließt ebenfalls in den Expansionsschritt ein.

Bei diesem Verfahren ist unbedingt darauf zu achten, dass bei einer eventuellen Ableitung weiteren Schlüsselmaterials aus K_t andere Ableitungsparameter verwendet werden als bei der Ableitung von K_{t+1}. Es wird empfohlen, dies durch Verwendung geeigneter Label-Werte zu erzwingen und ferner, in Label oder Context mindestens auch die Kryptoperiode t zu codieren. Als zusätzliche Maßnahme kann es zudem sinnvoll sein, für jede Schlüsselableitung einen neuen Salt-Wert zu verwenden. Es wird empfohlen, K_t unmittelbar nach Berechnung von K_{t+1} ebenso wie alle Zwischenergebnisse der Berechnung sicher zu löschen. Für weitere Empfehlungen zur Implementierung dieser Verfahren wird auf [96, 98] verwiesen.

8.2. Asymmetrische Verfahren

Grundsätzlich können alle der in Kapitel 3 empfohlenen asymmetrischen Verschlüsselungsverfahren zum Transport neuer Sitzungsschlüssel verwendet werden.

Als asymmetrische Schlüsselaushandlungsverfahren werden empfohlen:

- Diffie-Hellman, siehe [80],
- EC Diffie-Hellman (ECKA-DH), siehe [35].

Tabelle 8.1: Empfohlene asymmetrische Schlüsseleinigungsverfahren.

Dabei sind folgende Algorithmen festzulegen:

1.) ein Algorithmus zum Festlegen der Systemparameter und

2.) ein Algorithmus zur Schlüsseleinigung.

8.2.1. Diffie-Hellman

Die Sicherheit dieses Verfahrens beruht auf der angenommenen Schwierigkeit des Diffie-Hellman-Problems in Gruppen $\mathbb{F}_p$, wobei p eine Primzahl ist.

Systemparameter

1.) Wähle zufällig eine Primzahl p.

2.) Wähle ein Element $g \in \mathbb{F}_p^*$ mit $\mathrm{ord}(g)$ prim und $q := \mathrm{ord}(g) \geq 2^{250}$.

Das Tripel (p, g, q) muss vorab authentisch zwischen den Kommunikationspartnern A und B ausgetauscht werden, wobei gleiche Systemparameter prinzipiell durch viele Nutzer verwendet werden. Zur Erzeugung geeigneter Systemparameter siehe Bemerkung 3.7.

Schlüsselvereinbarung

1.) A wählt gleichverteilt einen Zufallswert $x \in \{1, \ldots, q-1\}$ und sendet $Q_A := g^x$ an B.

2.) B wählt gleichverteilt einen Zufallswert $y \in \{1, \ldots, q-1\}$ und sendet $Q_B := g^y$ an A.

3.) A berechnet $(g^y)^x = g^{xy}$.

4.) B berechnet $(g^x)^y = g^{xy}$.

Auch die Schlüsselvereinbarung muss durch starke Authentisierung abgesichert werden, um Man-in-the-Middle-Angriffe zu verhindern. Das ausgehandelte gemeinsame Geheimnis ist g^{xy}. Ein Mechanismus für eine nachfolgende Schlüsselableitung aus diesem Geheimnis wird in Abschnitt B.1 empfohlen.

Schlüssellänge Die Länge von p sollte mindestens 3000 Bits betragen.

Bemerkungen zur Implementierung Bei der Implementierung des Diffie-Hellman-Protokolls ist eine Reihe von Implementierungsfehlern weit verbreitet. Auf einige dieser Implementierungsprobleme wird in [101] eingegangen. Es wird empfohlen, insbesondere Abschnitt 7 von [101] zu beachten.

8.2.2. EC Diffie-Hellman

Die Sicherheit dieses Verfahrens beruht auf der angenommenen Schwierigkeit des Diffie-Hellman-Problems in elliptischen Kurven.

Systemparameter Wähle kryptographisch starke EC-Systemparameter (p, a, b, P, q, i) gemäß Abschnitt B.3. Die damit definierte elliptische Kurve sei mit C und die durch P erzeugte zyklische Untergruppe mit $\mathcal{G}$ bezeichnet. Die Systemparameter (p, a, b, P, q, i) müssen vorab authentisch zwischen den Kommunikationspartnern ausgetauscht werden.

Schlüsselvereinbarung

1.) A wählt gleichverteilt einen Zufallswert $x \in \{1, \ldots, q-1\}$ und sendet $Q_A := x \cdot P$ an B.

2.) B wählt gleichverteilt einen Zufallswert $y \in \{1, \ldots, q-1\}$ und sendet $Q_B := y \cdot P$ an A.

3.) A berechnet $x \cdot Q_B = xy \cdot P$.

4.) B berechnet $y \cdot Q_A = xy \cdot P$.

Auch die Schlüsselvereinbarung muss durch starke Authentisierung abgesichert werden. Das ausgehandelte Geheimnis ist $xy \cdot P$. Ein Mechanismus für eine nachfolgende Schlüsselableitung aus diesem Geheimnis wird in Abschnitt B.1 empfohlen.

Soweit möglich, wird empfohlen, auf beiden Seiten der Schlüsselvereinbarung zu überpüfen, ob die Punkte Q_A und Q_B protokollgerecht gewählt wurden und das Protokoll andernfalls abzubrechen. Bei korrekter Ausführung des obigen Protokolls sollten $Q_A \in \mathcal{G}$, $Q_B \in \mathcal{G}$, $Q_A \neq \mathcal{O}$ und $Q_B \neq \mathcal{O}$ gelten. Im Rahmen der Prüfung $Q_A, Q_B \in \mathcal{G}$ sollte explizit auch überprüft werden, ob $Q_A, Q_B \in C$. Weitere Hinweise finden sich in Abschnitt 4.3.2.1 von [35].

Schlüssellänge Die Länge von q sollte mindestens 250 Bits betragen.

Bemerkungen zur Implementierung Bei der Implementierung des Diffie-Hellman-Schlüsseltausches ist eine Reihe von Implementierungsfehlern weit verbreitet. Auf einige dieser Implementierungsprobleme wird in [101] eingegangen. Es wird empfohlen, insbesondere Abschnitt 7 von [101] zu beachten, ebenso sind die Hinweise in Abschnitt 4.3 von [35] und die AIS46 [33] zu berücksichtigen.

9. Secret Sharing

Häufig müssen kryptographische Schlüssel über einen langen Zeitraum gespeichert werden. Dies erfordert insbesondere, dass Kopien dieser Schlüssel angelegt werden müssen, um einem Verlust der Schlüssel entgegegenzuwirken. Mit wachsender Anzahl der Kopien wächst jedoch auch die Wahrscheinlichkeit, dass das zu schützende Geheimnis kompromittiert wird. Daher wird in diesem Kapitel ein Verfahren angegeben, welches erlaubt, ein Geheimnis wie beispielsweise einen kryptographischen Schlüssel K so in n Teilgeheimnisse $K_1, \ldots, K_n$ aufzuteilen, dass beliebige $t \leq n$ dieser Teilgeheimnisse genügen, um das Geheimnis zu rekonstruieren, $t-1$ Teilgeheimnisse aber keine Information über K liefern. Eine weitere Anwendung dieses Verfahrens ist, ein Vieraugenprinzip oder allgemeiner ein t-aus-n-Augenprinzip zu gewährleisten, um zum Beispiel das Passwort für eine kryptographische Komponente so auf n verschiedene Anwender zu verteilen, dass mindestens t Anwender benötigt werden, um das Passwort zu rekonstruieren.

Das hier vorgestellte Secret-Sharing-Verfahren wurde von A. Shamir entwickelt und wird daher auch als Shamir Secret-Sharing-Verfahren bezeichnet, siehe [103]. Wir nehmen im Folgenden an, dass das zu verteilende Geheimnis ein Schlüssel K der Bitlänge r ist, das heißt $K = (k_0, \ldots, k_{r-1}) \in \{0,1\}^r$. Zur Berechnung der verteilten Geheimnisse auf n Benutzer, so dass t Benutzer das Geheimnis K rekonstruieren können, wird wie folgt vorgegangen:

1.) Wähle eine Primzahl $p \geq \max(2^r, n+1)$ und setze $a_0 := \sum_{i=0}^{r-1} k_i \cdot 2^i \bmod p$.

2.) Wähle unabhängig voneinander $t-1$ zufällige Werte $a_1, \ldots, a_{t-1} \in \{0, 1, \ldots, p-1\}$ gemäß der Gleichverteilung aus $\{0, 1, \ldots, p-1\}$. Die Werte $a_0, a_1, \ldots, a_{t-1}$ definieren ein zufälliges Polynom

$$f(x) = \sum_{j=0}^{t-1} a_j x^j \bmod p$$

über $\mathbb{F}_p$, für das $f(0) = a_0 = \sum_{i=0}^{r-1} k_i \cdot 2^i \bmod p$ gilt.

3.) Berechne die Werte $K_i := f(i)$ für alle $i \in \{1, \ldots, n\}$.

Tabelle 9.1: Berechnung der Teilgeheimnisse im Shamir Secret-Sharing-Verfahren.

Die Teilgeheimnisse K_i werden dann, zusammen mit i, dem i-ten Benutzer übergeben.

Bemerkung 9.1 Die Grundlage für das in Tabelle 9.1 genannte Verfahren stellt die sogenannte *Lagrange-Interpolations-Formel* dar, welche es ermöglicht, die Koeffizienten $a_0, \ldots, a_{t-1}$ eines unbekannten Polynoms f vom Grad $t-1$ aus t Punkten $(x_i, f(x_i))$ wie folgt zu bestimmen:

$$f(x) = \sum_{i=1}^{t} \left[f(x_i) \prod_{\substack{1 \leq j \leq t \\ j \neq i}} \frac{x - x_j}{x_i - x_j} \right] \bmod p.$$

Insbesondere lässt sich auf diese Weise $a_0 = f(0)$ (und damit K) aus t gegebenen Punkten berechnen.

Um aus t Teilgeheimnissen $K_{j_1}, \ldots, K_{j_t}$ (mit paarweise verschiedenen j_l) das Geheimnis K zu rekonstruieren, berechnet man $a_0 = \sum_{i=0}^{r-1} k_i \cdot 2^i \bmod p$ wie folgt:

1.) Berechne für alle $j \in \{j_1, \ldots, j_t\}$ den Wert $c_j = \prod_{\substack{1 \le l \le t \\ j_l \neq j}} \frac{j_l}{j_l - j} \bmod p$.

2.) Berechne $K = \sum_{l=1}^{t} c_{j_l} K_{j_l} \bmod p$.

Tabelle 9.2: Zusammensetzen der Teilgeheimnisse im Shamir Secret-Sharing-Verfahren.

Sowohl bei der Aufteilung in Teilgeheimnisse in Tabelle 9.1 als auch beim Zusammensetzen in Tabelle 9.2 ist zu beachten, dass jeweils in $\mathbb{F}_p$, das heißt modulo p, gerechnet wird.

Bemerkung 9.2 Die Bedingung $p \geq \max(2^r, n+1)$ garantiert, dass einerseits das Geheimnis als Element von $\mathbb{F}_p$ dargestellt werden kann und andererseits mindestens n unabhängige Teilgeheimnisse erzeugt werden können. Das Verfahren erreicht informationstheoretische Sicherheit, es ist also auch einem Angreifer mit unbeschränkten Ressourcen nicht möglich, das verteilte Geheimnis zu rekonstruieren, ohne t Teilgeheimnisse oder einen aus der Kenntnis von t Teilgeheimnissen auf geeignete Weise abgeleiteten Wert in Erfahrung zu bringen.

Die Sicherheit des Verfahrens hängt daher abgesehen von der angegebenen Bedingung nicht von weiteren Sicherheitsparametern ab. Allerdings muss durch organisatorische und technische Maßnahmen sichergestellt werden, dass ein Angreifer keine Kenntnis von t Teilgeheimnissen erlangen kann. Jegliche Kommunikation über die Teilgeheimnisse muss daher verschlüsselt und authentisiert stattfinden, soweit es einem Angreifer physikalisch möglich ist, diese Kommunikation aufzuzeichnen oder zu manipulieren.

Zudem ist die informationstheoretische Sicherheit nur gegeben, wenn die a_i für $i > 0$ echt zufällig und entsprechend der Gleichverteilung aus $\mathbb{F}_p$ gewählt werden. Um mindestens eine komplexitätstheoretische Sicherheit zu garantieren, sollte daher zur Erzeugung der a_i ein physikalischer Zufallsgenerator der Funktionalitätsklasse PTG.3 oder ein deterministischer Zufallsgenerator der Funktionalitätsklasse DRG.3 oder DRG.4 genutzt werden. Die Ausgabewerte dieses Zufallsgenerators müssen so nachbearbeitet werden, dass sie der Gleichverteilung auf $\mathbb{F}_p$ entsprechen; geeignete Verfahren hierzu finden sich in Abschnitt B.4.

10. Zufallszahlengeneratoren

Die Mehrzahl kryptographischer Anwendungen benötigt Zufallszahlen, etwa zur Erzeugung kryptographischer Langzeit- oder Ephemeralschlüssel, Systemparameter oder zur Instanzauthentisierung. Dies trifft für symmetrische und asymmetrische Verschlüsselungsverfahren ebenso zu wie für Signatur-, Authentisierungs- und Paddingverfahren. Ungeeignete Zufallszahlengeneratoren können grundsätzlich starke kryptographische Mechanismen entscheidend schwächen, daher ist bei kryptographischen Anwendungen besonders darauf zu achten, dass geeignete Zufallszahlengeneratoren eingesetzt werden. So sind – im Gegensatz zu beispielsweise numerischen Simulationen oder Experimenten, bei denen Reproduzierbarkeit eine wichtige Rolle spielen kann – im kryptographischen Kontext für die meisten Anwendungen Unvorhersagbarkeit und Geheimhaltung der Zufallszahlen beziehungsweise der aus ihnen abgeleiteten Werte unverzichtbare Eigenschaften. Selbst wenn ein Angreifer lange Teilfolgen von Zufallszahlen kennt, darf ihm dies nicht ermöglichen, deren Vorgänger oder Nachfolger zu bestimmen.

In der Regel wird bei der Erzeugung von Zufallszahlen das Ziel verfolgt, Ausgabewerte gleichverteilt auf $\{0,1\}^n$ zu erzeugen. In einigen Fällen werden jedoch Zufallszahlen mit bestimmten anderen, vorgegebenen Verteilungen benötigt. Aus diesem Grund enthält Anhang B Algorithmen, mit denen man aus den Ausgabewerten eines Zufallszahlengenerators Zufallswerte mit gewünschten Eigenschaften (zum Beispiel gleichverteilt auf $\{0,\ldots,q-1\}$) berechnen kann.

Im deutschen Zertifizierungschema sind die AIS 20 [30] (für deterministische Zufallszahlengeneratoren) und AIS 31 [31] (für physikalische Zufallszahlengeneratoren) verbindlich. Von zentraler Bedeutung ist die ihnen gemeinsame mathematisch-technische Anlage [29], die Funktionalitätsklassen für physikalische Zufallszahlengeneratoren (PTG.1-PTG.3), für deterministische Zufallszahlengeneratoren (DRG.1 - DRG.4) und für nicht-physikalische nicht-deterministische Zufallszahlengeneratoren (NTG.1) definiert. Darüber hinaus erläutert [29] den mathematischen Hintergrund und illustriert die Konzepte an zahlreichen Beispielen.

Bemerkung 10.1 Die mathematisch-technische Anlage zur AIS 20 und AIS 31 [29] wird zur Zeit überarbeitet. Der Draft (siehe `https://www.bsi.bund.de/dok/zufallszahlengenerator`) kann bis zum 15. Februar 2023 kommentiert werden.

In den folgenden Abschnitten wird näher auf die verschiedenen Arten von Zufallszahlengeneratoren eingegangen. Die wichtigsten Empfehlungen zum Einsatz von Zufallszahlengeneratoren in allgemeinen kryptographischen Anwendungen lassen sich wie folgt zusammenfassen:

- Bei Verwendung eines physikalischen Zufallszahlengenerators wird grundsätzlich empfohlen, einen PTG.3-Generator einzusetzen. Dies gilt besonders für die Erzeugung von Ephemeralschlüsseln bei der Berechnung digitaler Signaturen und bei Diffie-Hellman-basierten Schlüsselaushandlungen. In Fällen, in denen für die Zufallszahlenerzeugung der Einsatz einer zertifizierten Kryptokomponente erforderlich ist, gilt diese Empfehlung nur bei Verfügbarkeit entsprechend zertifizierter Komponenten. Andernfalls kann ein PTG.3-Generator in der Regel durch eine zu den Anforderungen der Funktionalitätsklasse PTG.3 kompatible, in Software implementierte kryptographische Nachbearbeitung der Ausgabe eines PTG.2-Generators konstruiert werden.
- Für einige bestimmte kryptographische Anwendungen sind auch PTG.2-Generatoren ausreichend, beispielsweise bei der Erzeugung symmetrischer Sitzungsschlüssel oder bei der Generierung eines Seeds für einen starken deterministischen Zufallszahlengenerator. Zufallszahlen aus PTG.2-konformen Zufallszahlengeneratoren besitzen hohe Entropie, können aber

gewisse Schiefen und/oder Abhängigkeiten aufweisen. Sie können unter Umständen eingesetzt werden, wenn der daraus für einen Angreifer resultierende Vorteil nachweislich gering ist. Generell wird jedoch von der direkten Verwendung von PTG.2-Zufallszahlengeneratoren abgeraten. Dies gilt insbesondere für Anwendungen, in denen die Existenz selbst relativ geringfügiger Schiefen in der Verteilung der erzeugten Zufallszahlen zu ausnutzbaren Schwächen führen kann, etwa bei der Erzeugung von Noncen in DSA-ähnlichen Signaturverfahren.

- Beim Einsatz eines deterministischen Zufallszahlengenerators wird empfohlen, einen DRG.3- oder einen DRG.4-Generator einzusetzen, dessen Seed aus einer physikalischen Zufallsquelle der Klasse PTG.2 oder PTG.3 generiert wird. Falls keine derartige Zufallsquelle verfügbar ist, kann unter Umständen auch die Verwendung eines nicht-physikalischen, nicht-deterministischen Zufallszahlengenerators in Erwägung gezogen werden. So kann ein DRG.3-Generator beispielsweise auch mit einem NTG.1-Generator geseedet werden, für weitere Details sei auf die Abschnitte 10.3 und 10.5 verwiesen.

- Grundsätzlich haben PTG.3-Generatoren und DRG.4-Generatoren verglichen mit PTG.2-Generatoren und DRG.3-Generatoren den Vorteil einer stärkeren Resistenz gegen Seitenkanalattacken und Fault-Angriffe. Im Falle eines PTG.3-Generators bedeutet der stetige Zufluss großer Mengen an Entropie in den inneren Zustand, dass mögliche Seitenkanalangriffe gegen die kryptographische Nachbearbeitung deutlich erschwert werden, da ein Angreifer Informationen über den inneren Zustand zu zwei aufeinanderfolgenden Zeitpunkten t und $t + 1$ nur sehr schwer zusammenführen kann.

- Neben dem Risiko einer langfristigen Kompromittierung durch Seitenkanal- und Fault Attacken kommt bei DRG.3-Zufallszahlengeneratoren ein gegenüber DRG.4- und PTG.3-Generatoren erhöhtes Restrisiko einer langfristig denkbaren kryptoanalytischen Kompromittierung hinzu, wenn der Zufallszahlengenerator große Mengen an langfristig schützenswertem Schlüsselmaterial aus einem einzelnen Seed-Wert erzeugt. Bei der Verwendung von PTG.3- oder DRG.4-Zufallszahlengeneratoren sind Seitenkanal- und Fault-Angriffe zwar ebenfalls relevant, führen aber im Vergleich nur zu der Kompromittierung relativ weniger erzeugter Zufallswerte.

- Im allgemeinen wird für eine Systemsicherheit von n Bits eine Min-Entropie des DRNG-Seeds von n Bits benötigt.

- Sowohl für physikalische als auch für deterministische Zufallszahlengeneratoren sollte im jeweiligen Anwendungskontext eine Widerstandsfähigkeit gegen hohes Angriffspotential gezeigt werden.

10.1. Physikalische Zufallszahlengeneratoren

Physikalische Zufallszahlengeneratoren nutzen dedizierte Hardware (üblicherweise eine elektronische Schaltung), um hieraus „echten“ Zufall, das heißt unvorhersagbare Zufallszahlen, zu erzeugen. In der Regel wird dabei das unvorhersehbare Verhalten einfacher elektrischer Schaltungen genutzt, wie es durch verschiedene Formen von Rauschen in den Schaltungen verursacht werden kann. Letzten Endes beruht die Entropie des Signals üblicherweise physikalisch auf Quanteneffekten oder auf der Verstärkung nicht kontrollierbarer beziehungsweise separat messbarer Umgebungseinflüsse in einem chaotischen System. Ein Angreifer sollte auch bei Kenntnis von Teilfolgen von Zufallszahlen sowie genauer Kenntnis des Zufallszahlengenerators einschließlich der physikalischen Umgebungsbedingungen zum Zeitpunkt der Erzeugung vorheriger oder nachfolgender Zufallszahlen nur einen vernachlässigbaren (im Idealfall gar keinen) Vorteil gegenüber blindem Raten der Zufallszahlen besitzen. Häufig ist eine deterministische Nachbearbeitung der „Rauschrohdaten“ (üblicherwei-

se digitalisierte Rauschsignale) notwendig, um etwaig vorhandene Schiefen oder Abhängigkeiten zu beseitigen.

Bei der Nutzung eines physikalischen Zufallszahlengenerators wird grundsätzlich empfohlen, einen PTG.3-Generator im Sinne der AIS 31 einzusetzen (vergleiche [29, Kapitel 4]). Dies trifft insbesondere auf Anwendungen zu, bei denen ein Angreifer zumindest prinzipiell Informationen über verschiedene Zufallszahlen zusammenführen kann. Sofern eine Implementierung des Zufallszahlengenerators in einer zertifizierten Kryptokomponente erforderlich ist, gilt die Empfehlung einer Verwendung eines PTG.3-Generators nur, soweit geeignete zertifizierte Komponenten existieren.

Es ist möglich, einen PTG.3-Generator aus einem PTG.2-Generator zu konstruieren, indem die Ausgabe des PTG.2-Generators auf geeignete Weise kryptographisch nachbearbeitet wird. Diese Nachbearbeitung kann in der Regel in Software implementiert werden. Die genauen Anforderungen an die Nachbearbeitung finden sich in [29]. Vereinfacht dargestellt muss die Nachbearbeitung einen DRG.3-kompatiblen deterministischen Zufallszahlengenerator implementieren und es muss dem internen Zustand dieses Zufallszahlengenerators jederzeit mindestens soviel neue Entropie durch einen Zufallszahlengenerator der Klasse PTG.2 zugeführt werden, wie durch die kryptographische Anwendung verlangt wird.

Kurz zusammengefasst müssen PTG.2- beziehungsweise PTG.3-konforme Zufallszahlengeneratoren folgende Eigenschaften erfüllen:

- Die statistischen Eigenschaften der Zufallszahlen lassen sich hinreichend genau durch ein stochastisches Modell beschreiben. Auf der Basis dieses stochastischen Modells kann die Entropie der Zufallszahlen zuverlässig abgeschätzt werden.
- Der durchschnittliche Entropiezuwachs pro Zufallsbit liegt oberhalb einer gegebenen Mindestschranke (nahe bei 1).
- Die digitalisierten Rauschsignale werden im laufenden Betrieb statistischen Tests unterzogen, die geeignet sind, nicht akzeptable statistische Schwächen oder Verschlechterungen der statistischen Eigenschaften in angemessener Zeit zu erkennen.
- Ein Totalausfall der Rauschquelle wird de facto sofort erkannt. Es dürfen keine Zufallszahlen ausgegeben werden, die nach einem Totalausfall der Rauschquelle erzeugt wurden.
- Die Feststellung eines Totalausfalls der Rauschquelle oder nicht akzeptabler statistischer Defekte der Zufallszahlen führt zu einem Rauschalarm. Auf einen Rauschalarm folgt eine definierte, geeignete Reaktion (zum Beispiel Stilllegen der Rauschquelle).
- (Nur PTG.3-konforme Zufallszahlengeneratoren): Eine (ggf. zusätzliche) starke kryptographische Nachbearbeitung stellt sicher, dass selbst bei einem unbemerkten Totalausfall der Rauschquelle noch das Sicherheitsniveau eines DRG.3-konformen deterministischen Zufallszahlengenerators vorliegt.

Hybride Zufallszahlengeneratoren vereinen Sicherheitseigenschaften von deterministischen und physikalischen Zufallszahlengeneratoren. Hybride physikalische Zufallszahlengeneratoren der Funktionalitätsklasse PTG.3 besitzen neben einer starken Rauschquelle eine starke kryptographische Nachbearbeitung mit Gedächtnis. Eine typische Realisierung eines hybriden Zufallszahlengenerators besteht darin, dass Zufallszahlen eines PTG.2-konformen Zufallszahlengenerators in geeigneter Weise kryptographisch nachbearbeitet werden.

Entwicklung und sicherheitskritische Bewertung von physikalischen Zufallszahlengeneratoren setzen eine umfassende Erfahrung auf diesem Gebiet voraus. Es wird empfohlen, frühzeitig Experten auf diesem Gebiet zu Rate zu ziehen.

10.2. Deterministische Zufallszahlengeneratoren

Deterministische Zufallszahlengeneratoren (auch Pseudozufallszahlengeneratoren) können aus einem Zufallswert fester Länge, dem sogenannten *Seed*, eine pseudozufällige Bitfolge praktisch beliebiger Länge berechnen. In die Berechnung können auch öffentlich bekannte Parameter eingehen. Dazu wird zunächst der innere Zustand des Pseudozufallszahlengenerators mit dem Seed initialisiert. In jedem Schritt wird dann der innere Zustand erneuert, und es wird eine Zufallszahl (normalerweise eine Bitfolge fester Länge) aus dem inneren Zustand abgeleitet und ausgegeben. Hybride deterministische Zufallszahlengeneratoren erneuern den inneren Zustand von Zeit zu Zeit mit „echten“ Zufallswerten (reseed/seed update). Dies kann auf unterschiedliche Weise veranlasst werden, zum Beispiel regelmäßig oder auf Anfrage der Applikation. Der innere Zustand eines deterministischen Zufallszahlengenerators muss zuverlässig gegen Auslesen und Manipulation geschützt werden. Kommt ein deterministischer Zufallszahlengenerator zum Einsatz, dann wird empfohlen, einen DRG.3- oder DRG.4-konformen Zufallszahlengenerator gegen das Angriffspotentiall „hoch“ im Sinne der AIS 20 zu verwenden (vergleiche [29]).

Bei Verwendung von Zufallszahlengeneratoren der Klasse DRG.3 ist ein regelmäßiger Zufluss von frischer Entropie in den inneren Zustand wünschenswert, auch wenn dieser nicht ausreichend regelmäßig oder qualitativ hochwertig genug ist, um für die Gesamtkonstruktion DRG.4-Konformität zu erreichen. Vereinfacht gesagt, bedeutet DRG.3-Konformität:

- Es ist einem Angreifer praktisch nicht möglich, zu einer bekannten Teilfolge von Zufallszahlen Vorgänger oder Nachfolger von Zufallszahlen zu berechnen oder mit signifikant höherer Wahrscheinlichkeit zu erraten, als dies ohne Kenntnis dieser Teilfolge möglich wäre.

- Es ist einem Angreifer praktisch nicht möglich, basierend auf Kenntnis eines inneren Zustandes zuvor ausgegebene Zufallszahlen zu berechnen oder mit signifikant höherer Wahrscheinlichkeit zu erraten, als dies ohne Kenntnis des inneren Zustands möglich wäre.

Für eine DRG.4-Konformität kommt hinzu, dass selbst wenn ein Angreifer den aktuellen inneren Zustand kennt, es ihm praktisch nicht möglich ist, Zufallszahlen, die nach dem nächsten reseed/seed update erzeugt werden, zu berechnen oder mit signifikant höherer Wahrscheinlichkeit zu erraten, als dies ohne Kenntnis des inneren Zustands möglich wäre.[1] Auch im Hinblick auf Implementierungsangriffe weisen DRG.4-Generatoren gegenüber DRG.3-konformen Zufallszahlengeneratoren gewisse Vorteile auf.

10.3. Nicht-physikalische nicht-deterministische Zufallszahlengeneratoren

Für viele kryptographische Anwendungen, etwa aus dem Bereich des E-Businesses oder des E-Governments, steht weder ein physikalischer noch ein deterministischer Zufallszahlengenerator zur Verfügung, da diese Anwendungen im Allgemeinen auf Computern ohne zertifizierte kryptographische Hardware ausgeführt werden. Stattdessen werden in aller Regel nicht-physikalische nicht-deterministische Zufallszahlengeneratoren (NPTRNG) verwendet, entweder direkt oder zum Seeding eines starken deterministischen Zufallszahlengenerators. Ein bekanntes Beispiel für einen nicht-physikalischen nicht-deterministischen Zufallszahlengeneratoren stellt der Linux-RNG (Gerätedatei `/dev/random`) dar, der in der Studie [6] einer ausführlichen Analyse unterzogen wird.

[1] Unter einer signifikant höheren Wahrscheinlichkeit wird hier eine Wahrscheinlichkeit verstanden, die mindestens über der Wahrscheinlichkeit liegt, die für das Seed-Update erzeugten echten Zufallswerte zu erraten. Für jedes Seed-Update müssen mindestens 120 Bits Min-Entropie erzeugt werden.

Wie physikalische Zufallszahlengeneratoren erzeugen auch nicht-physikalische nicht-deterministische Zufallszahlengeneratoren „echte“ Zufallszahlen und setzen auf Sicherheit im informationstheoretischen Sinn durch hinreichend viel Entropie. Allerdings nutzen sie hierfür keine dedizierte Hardware, sondern Systemressourcen (Systemzeit, RAM-Inhalte usw.) und/oder Nutzerinteraktion (zum Beispiel Tastatureingaben oder Mausbewegungen). Nicht-physikalische nicht-deterministische Zufallszahlengeneratoren werden üblicherweise auf Systemen eingesetzt, die nicht speziell für kryptographische Anwendungen entwickelt wurden, zum Beispiel handelsübliche PCs, Laptops oder Smartphones.

Eine typische Vorgehensweise zur Erzeugung von Zufallszahlen mithilfe nicht-physikalischer nicht-deterministischer Zufallszahlengeneratoren ist die Folgende: Zunächst wird ein langer Bitstring von „zufälligen Daten“ (genauer: von nicht-deterministischen Daten) erzeugt, wobei die Entropie pro Bit normalerweise eher gering ist. Dieser Bitstring wird mit einem inneren Zustand vermischt und aus dem inneren Zustand werden anschließend Zufallszahlen errechnet und ausgegeben.

In der mathematisch-technischen Anlage [29] wird eine Funktionalitätsklasse für derartige Zufallszahlengeneratoren (NTG.1) definiert. Für NTG.1-Zufallszahlengeneratoren wird grob gesagt verlangt, dass die Menge der gesammelten Entropie im laufenden Betrieb zuverlässig geschätzt werden kann und dass die Ausgabedaten eine Shannon-Entropie von > 0.997 Bit pro Ausgabebit aufweisen.

Dieses bedeutet unter anderem:

- Die Entropie des inneren Zustands wird geschätzt. Wird eine Zufallszahl ausgegeben, wird der Entropiezähler entsprechend reduziert.
- Zufallszahlen dürfen nur ausgegeben werden, wenn der Wert des Entropiezählers groß genug ist.
- Es ist einem Angreifer praktisch nicht möglich, aus Kenntnis des inneren Zustandes und der zuvor für Seed-Updates verwendeten zufälligen Bitstrings zuvor ausgegebene Zufallszahlen zu berechnen oder mit signifikant höherer Wahrscheinlichkeit zu erraten, als dies ohne Kenntnis des inneren Zustands und der Bitstrings möglich wäre.

Es ist für NPTRNG von entscheidender Bedeutung, dass die durch den Zufallszahlengenerator verwendeten Entropiequellen nicht durch einen Angreifer im Sinne einer Entropiereduktion manipuliert werden können oder vorhersagbar werden, wenn der Angreifer über präzise Informationen zur Ausführungsumgebung verfügt. Diese Voraussetzung ist auch bei Verwendung eines an sich guten NPTRNG nicht selbstverständlich. Ein Beispiel für eine in dieser Hinsicht kritische Situation stellt die Verwendung von Virtualisierungslösungen dar [102]. In diesem Fall kann der Output eines NPTRNG im Extremfall vollständig vorhergesagt werden, wenn das System zweimal aus dem gleichen Systemabbild heraus gestartet wird und alle Entropiequellen des virtuellen Systems vom Wirtsrechner kontrolliert werden.

Falls ein NPTRNG als alleinige oder als wesentliche Zufallsquelle für ein System verwendet werden soll, das für die Verarbeitung sensibler Daten bestimmt ist, wird dringend empfohlen, einen Experten hinzuzuziehen.

10.4. Verschiedene Aspekte

Hybride Zufallszahlengeneratoren vereinen Sicherheitseigenschaften von deterministischen und physikalischen Zufallszahlengeneratoren. Die Sicherheit eines hybriden deterministischen Zufallszahlengenerators der Klasse DRG.4 beruht in erster Linie auf der Komplexität des deterministischen Anteils, welcher der Klasse DRG.3 angehört. Während der Nutzung des Zufallszahlengenera-

tors wird zudem immer wieder neuer Zufall hinzugefügt. Dies kann beispielsweise in regelmäßigen Abständen oder auf die Anforderung einer Applikation hin erfolgen.

Hybride physikalische Zufallszahlengeneratoren der Klasse PTG.3 besitzen neben einer starken Rauschquelle eine starke kryptographische Nachbearbeitung mit Gedächtnis. Im Vergleich zu PTG.2-konformen Zufallszahlengeneratoren bietet die Funktionalitätsklasse PTG.3 zudem den Vorteil, dass die Zufallszahlen weder Schiefen noch ausnutzbare Abhängigkeiten aufweisen. Insbesondere für Anwendungen, bei denen ein potentieller Angreifer zumindest prinzipiell Informationen über viele Zufallszahlen kombinieren kann (zum Beispiel Ephemeralschlüssel), sollte ein physikalischer Zufallszahlengenerator der Funktionalitätsklasse PTG.3 verwendet werden.

Die Ableitung von Signaturschlüsseln, Ephemeralschlüsseln und Primzahlen (für RSA) o.ä. aus den erzeugten Zufallszahlen hat mit geeigneten Algorithmen zu erfolgen (zu elliptischen Kurven vergleiche [33, Abschitte 5.2 und 5.5.1]). Vereinfacht gesagt, sollte einem potentiellen Angreifer so wenig Information über die abgeleiteten (geheim zu haltenden) Werte zur Verfügung stehen wie möglich. Im Idealfall treten alle Werte innerhalb des jeweilig zulässigen Wertebereichs mit der gleichen Wahrscheinlichkeit auf, und verschiedene Zufallszahlen sollten zumindest keine praktisch ausnutzbaren Zusammenhänge aufweisen. Wie in [29] erläutert, kann ebenso wie Signaturalgorithmen auch die Erzeugung geheim zu haltender Signaturschlüssel, Ephemeralschlüssel und Primzahlen Ziel von Seitenkanalangriffen werden (siehe zum Beispiel [49, 33]).

10.5. Seedgenerierung für deterministische Zufallszahlengeneratoren

Für die Initialisierung eines deterministischen Zufallszahlengenerators wird ein Seed mit hinreichend hoher Entropie benötigt. Dieser Seed sollte mit einem physikalischen Zufallszahlengenerator der Funktionalitätsklassen PTG.2 oder PTG.3 erzeugt werden. Auf PCs steht normalerweise kein physikalischer Zufallszahlengenerator zur Verfügung oder ein derartiger Zufallszahlengenerator wurde zumindest keiner gründlichen herstellerunabhängigen Zertifizierung unterzogen. In solchen Fällen bietet sich die Verwendung eines nicht-physikalischen nicht-deterministischen Zufallzahlengenerators an; empfohlen werden in dieser Technischen Richtlinie NTG.1-konforme Zufallszahlengeneratoren. Zurzeit gibt es noch keine NTG.1-zertifizierten Zufallszahlengeneratoren. Daher werden unten für die zwei wichtigsten PC-Betriebssysteme geeignete Verfahren zur Seedgenerierung angegeben.

Der Einsatz der in den beiden folgenden Unterabschnitten empfohlenen Verfahren zur Seedgenerierung kann aber nur dann als sicher eingestuft werden, wenn der Rechner unter vollständiger Kontrolle der Benutzerin beziehungsweise des Benutzers steht und keine Drittkomponenten direkten Zugriff auf den gesamten inneren Zustand des Rechners haben, wie es zum Beispiel der Fall sein kann, wenn das gesamte Betriebssystem in einer virtuellen Umgebung abläuft. Dies schließt insbesondere die Existenz von beispielsweise Viren oder Trojanern auf diesem Rechner aus. Benutzerinnen und Benutzer sollten über diese Risiken entsprechend aufgeklärt werden.

10.5.1. GNU/Linux

Folgendes Verfahren wird zur Seedgenerierung unter dem Betriebssystem GNU/Linux empfohlen:

Auslesen von Daten aus der Gerätedatei `/dev/random`.

Tabelle 10.1: Empfohlenes Verfahren zur Seedgenerierung unter GNU/Linux.

Bemerkung 10.2 Der durch die Gerätedatei `/dev/random` gelieferte Zufall wurde bisher nur in bestimmten Kernelversionen vom BSI untersucht und bei einer Anwendung in PC-ähnlichen Syste-

men als geeignet bewertet. Der Linux-RNG wird dabei durch die vorliegenden Technische Richtlinie als für allgemeine kryptographische Anwendungen in der Regel geeignet eingeschätzt, wenn die Anforderungen der Funktionalitätsklasse DRG.3 oder NTG.1 nach [29] erfüllt sind. Da sich die zugrundeliegenden Mechanismen aber in Abhängigkeit von der verwendeten Kernel-Version erheblich unterscheiden und die verfügbaren Zufallsquellen von der genauen Systemumgebung abhängig sind, sollte immer ein Experte hinzugezogen werden, wenn `/dev/random` in einem neu zu entwickelnden System als wesentlichste Zufallsquelle eingesetzt werden soll. Eine kryptographische Bewertung von `/dev/random` in verschiedenen Linux-Kernelversionen findet sich in der BSI-Studie [6]. Ein Abgleich der Sicherheitseigenschaften des Linux-Zufallszahlengenerators in verschiedenen Linux-Kernelversionen mit den Funktionalitätsklassen der AIS 20 beziehungsweise AIS 31 wird in den dort enthaltenen Kernelübersichten gegeben.

Bemerkung 10.3 Die Nutzung von `/dev/urandom` kann problematisch sein [53], da hierbei nicht geprüft wird, ob bei der Initialisierung des Zufallszahlengenerators eine für kryptographische Zwecke ausreichende Menge an Systemdaten gesammelt wurde. Hingegen blockiert `/dev/random` in manchen Kernelversionen, wenn der interne Entropieschätzer unter eine festgelegte Schranke fällt. Dies kann die Zufallszahlenerzeugung sehr stark verlangsamen und damit zu Benutzbarkeitsproblemen führen.

Bemerkung 10.4 Grundsätzlich kann `/dev/random` nicht nur zum Seeding eines Pseudozufallsgenerators verwendet werden, sondern auch zur direkten Erzeugung kryptographischer Schlüssel.

10.5.2. Windows

Im Gegensatz zu GNU/Linux-Betriebssystemen gibt es für die Betriebssysteme der Windows-Familie derzeit keine vom BSI untersuchte Funktion, die hinreichend große Entropie gewährleistet. Zur Erzeugung sicherer Seeds sollten daher mehrere Entropiequellen in geeigneter Weise kombiniert werden. Beispielhaft wäre in Windows 10 zur Erzeugung eines Seedwertes von mindestens 120 Bits Entropie die folgende Methode denkbar:

1.) Einlesen von 128 Bits Zufallsdaten in einen 128-Bit-Puffer S_1 aus der Windows-API-Funktion `BCryptGenRandom()`.

2.) Beziehen eines Bitstrings S_2 mit mindestens 120 Bits Entropie aus einer *anderen Quelle*. Hierbei kommen beispielsweise in Frage:

- Auswertung der Zeitabstände zwischen aufeinanderfolgenden Tastaturanschlägen des Benutzers: Wenn diese nachweislich mit einer Genauigkeit von einer Millisekunde erfasst werden können, können hierfür konservativ etwa drei Bits an Entropie pro Tastenanschlag angesetzt werden. Dabei ist im Hinblick auf eine Einschätzung der zeitlichen Auflösung der gemessenen Zeitabstände die gesamte Verarbeitungskette auf die gesammelte Entropie limitierende Faktoren zu untersuchen. Zum Beispiel ist es denkbar, dass die Genauigkeit der internen Uhr eine Auflösungsgrenze angibt, die Abtastfrequenz der Tastatur eine andere, und der Zeitabstand, innerhalb dessen der genutzte Systemtimer aktualisiert wird, eine weitere. Es wird empfohlen, zuvor in praktischen Tests die Verteilung der Tastaturanschlagszeiten zu messen und auf Auffälligkeiten zu untersuchen. Die Sequenz der zeitlichen Abstände einer hinreichend großen Anzahl von Tastaturereignissen kann dann in einen Binärstring B kodiert werden. Anschließend wird $S_2 := \mathrm{SHA256}(B)$ und die aufgenommenen Daten zu den Tastaturanschlagszeiten (und andere Daten, die in dem Prozess erhoben wurden) werden durch Überschreiben mit Nullen aus dem Arbeitsspeicher gelöscht.
- Durch den Benutzer ausgelöste Ereignisse: Die Zeitpunkte $T_1, T_2, T_3, T_4, T_5, T_6$ von sechs durch den Benutzer ausgelösten Ereignissen werden mittels der Windows-API-Funktion

`QueryPerformanceCounter()` aufgenommen. Diese hat in der Regel mindestens eine Genauigkeit von der Größenordnung einer Mikrosekunde. Man kann unter den Voraussetzungen,

(i) dass jedes T_i selbst dann nicht genauer als auf eine Sekunde geschätzt werden kann, wenn T_j dem Angreifer für alle $j \neq i$ bekannt ist,

(ii) dass, auch wenn der Angreifer T_j für alle $j \neq i$ kennt, der Wert von T_i nicht durch andere Erwägungen (zum Beispiel zur Polling-Frequenz der Tastatur) auf weniger als 2^{20} Möglichkeiten beschränkt werden kann, wenn irgendein Intervall von einer Sekunde Länge angegeben wird, das T_i enthält,

annehmen, dass der Bitstring $T := T_1||T_2||T_3||T_4||T_5||T_6$ aus Angreifersicht etwa 120 Bits Entropie enthält. Wie im vorherigen Beispiel setzt man $S_2 :=$ SHA256(T) und löscht T aus dem Arbeitsspeicher.

Es ist nicht immer ganz einfach, die Voraussetzungen an die Unabhängigkeit und Unvorhersagbarkeit der durch den Benutzer ausgelösten Ereignisse zu erfüllen. Das Problem hierbei ist, dass der Zeitpunkt, zu dem die Software vom Benutzer die Auslösung eines Ereignisses anfordert, möglicherweise eng vorhersagbar ist, wenn ein früherer Zeitpunkt bekannt ist. Der Zeitraum, der zwischen der Aufforderung zu einer Eingabe und der Benutzereingabe selbst vergeht, könnte ebenfalls genauer als im Sekundenbereich vorhersagbar sein. Die Erfüllung der Voraussetzungen und die Plausibilität derartiger Entropieeinschätzungen muss stets im konkret vorliegenden Einzelfall untersucht werden.

- Auf ähnliche Weise können auch Mausbewegungen des Benutzers zur Gewinnung von Entropie genutzt werden. Die in Mausbewegungen enthaltene Entropie kann nicht ohne Weiteres genau geschätzt werden. Es bedarf daher stets einer Einzelfallanalyse, bei der Art und Anzahl der aufgenommenen Ereignisse (Zeigerpositionen, gegebenenfalls zusätzlich Zeitmessungen) berücksichtigt werden, so dass sichergestellt werden kann, dass die erhobenen Messungen sich nicht verlustlos auf einen Datensatz von unter 120 Bits Größe komprimieren lassen. Man definiert dann S_2 wieder durch einen SHA2-Hash über die Mausereignisse.

3.) In allen Fällen kann anschließend ein Seed-Wert S für einen geeigneten Pseudozufallsgenerator abgeleitet werden, indem $S :=$ SHA256$(S_1||S_2)$ gesetzt wird. Idealerweise werden dabei so viele unabhängige Entropiequellen $S_1, \ldots, S_n$ wie möglich verwendet, um ein gewünschtes Sicherheitsniveau zu erreichen.

Bemerkung 10.5 Dem BSI liegen keine Erkenntnisse vor, die anzeigen, dass in dem obigen Beispiel ein 128-Bit-Wert bezogen aus `BCryptGenRandom()` nicht bereits näherungsweise 128 Bits Entropie enthält. Allerdings ist die exakte Funktionsweise von `BCryptGenRandom()` weder ausführlich in öffentlich zugänglichen Herstellerdokumenten beschrieben noch wurde die Funktion intensiv durch vom Hersteller unabhängige Parteien untersucht, wie es zum Beispiel für den Zufallszahlengenerator des Linux-Kernels der Fall ist. Daher ist die Kombination von Zufall aus `BCryptGenRandom()` mit der Ausgabe aus anderen Entropiequellen als grundsätzliche Vorsichtsmaßnahme empfehlenswert.

Anhang A.

Anwendungen kryptographischer Verfahren

Häufig müssen die in den vorangegangenen Kapiteln erläuterten Verfahren miteinander kombiniert werden, um den Schutz sensitiver Daten gewährleisten zu können. Insbesondere sollten zu übertragende sensitive Daten nicht nur verschlüsselt, sondern zusätzlich authentisiert werden, um es einem Empfänger zu ermöglichen, etwaige Veränderungen feststellen zu können.

Eine Schlüsseleinigung muss immer mit einer Instanzauthentisierung und einer Authentisierung aller während der Schlüsseleinigung übertragenen Nachrichten einher gehen, damit sich beide Parteien sicher sein können, mit wem sie kommunizieren. Andernfalls kann die Kommunikation durch eine sogenannte Man-in-the-Middle-Attacke kompromittiert werden. Je nach Anwendung können neben Man-in-the-Middle-Attacken auch andere Arten von Angriffen auf die Authentizität der Nachrichtenübermittlung (zum Beispiel Replay-Attacken) die Sicherheit eines informationsverarbeitenden Systems ohne Instanzauthentisierung oder ohne Datenauthentisierung gefährden. Daher werden in diesem Kapitel sowohl für eine Verschlüsselung mit Datenauthentisierung als auch zur authentisierten Schlüsselvereinbarung geeignete Verfahren angegeben.

A.1. Verschlüsselungsverfahren mit Datenauthentisierung

Grundsätzlich können bei der Kombination von Verschlüsselung und Datenauthentisierung alle in Kapitel 2 bzw. Abschnitt 6.2 empfohlenen Verfahren eingesetzt werden. Dabei sind die folgenden beiden Aspekte einzuhalten:

- Verschlüsselte Daten müssen immer authentisiert übertragen werden. Zusätzlich ist es möglich, auch nicht vertrauliche Daten authentisiert, aber unverschlüsselt zu übertragen. Alle weiteren Daten derselben Datenübertragung sind *nicht* authentisiert.
- Verschlüsselungs- und Authentisierungsschlüssel müssen verschieden und dürfen nicht voneinander ableitbar sein.

Bemerkung A.1 Bei der authentisierten Übertragung verschlüsselter Daten wird die Nutzung eines MACs im Encrypt-then-MAC-Modus empfohlen.

Bemerkung A.2 Es besteht die Möglichkeit, Verschlüsselungs- und Authentisierungsschlüssel aus einem gemeinsamen Schlüssel abzuleiten; dies steht nicht im Widerspruch zum zweiten Aspekt von oben. Empfohlene Verfahren sind in Abschnitt B.1 zusammengefasst.

Bemerkung A.3 Falls bei einer Übertragung verschlüsselter Daten zusätzlich das Sicherheitsziel der Nichtabstreitbarkeit des Klartextes angestrebt wird, sollte der Klartext durch eine digitale Signatur gesichert werden. In diesem Fall wird also zunächst der Klartext signiert, dann verschlüsselt, und schließlich wird die verschlüsselte Übertragung durch einen MAC vor Veränderung auf dem Übertragungsweg geschützt. Zusätzlich kann eine Signatur über das Chiffrat sinnvoll sein, wenn darüber hinaus die chiffrierte Nachricht unabstreitbar beziehungsweise nur der Absender (und nicht auch der legitime Empfänger) in der Lage sein soll, das Chiffrat zu ändern. Allerdings kann der Signierer eine chiffrierte Nachricht vor der Signaturerstellung in der Regel nicht sinnvoll daraufhin überprüfen, ob das Chiffrat korrekt ist.

A.2. Authentisierte Schlüsselvereinbarung

Wie bereits erwähnt, muss eine Schlüsselvereinbarung immer mit einer Instanzauthentisierung kombiniert werden. Nach einigen allgemeinen Vorbemerkungen werden Verfahren angegeben, die entweder vollständig auf symmetrischen Algorithmen oder vollständig auf asymmetrischen Algorithmen basieren.

A.2.1. Vorbemerkungen

Ziele Ziel eines Verfahrens zum Schlüsseltausch mit Instanzauthentisierung ist es, dass die beteiligten Parteien im Anschluss ein gemeinsames Geheimnis teilen und am Ende der Protokollausführung sicher sind, mit wem sie es teilen. Für die Ableitung symmetrischer Schlüssel für Verschlüsselungs- und Datenauthentisierungsverfahren aus diesem Geheimnis siehe Abschnitt B.1.

Voraussetzungen an die Umgebung Voraussetzung für einen authentisierten Schlüsseltausch mit symmetrischen Verfahren ist die Existenz vorverteilter Geheimnisse. Bei asymmetrischen Verfahren wird in der Regel vorausgesetzt, dass eine Public-Key-Infrastruktur vorhanden ist, die in der Lage ist, zuverlässig Schlüssel an Identitäten zu binden und die Herkunft eines Schlüssels durch entsprechende Zertifikate zu beglaubigen. Es wird außerdem angenommen, dass die Wurzelzertifikate der PKI allen Teilnehmern auf zuverlässigem Wege bekanntgemacht worden sind und dass alle Teilnehmer zu jedem Zeitpunkt in der Lage sind, sämtliche relevanten Zertifikate auf Gültigkeit prüfen zu können.

Hinweise zur Umsetzung Bei der konkreten Umsetzung der vorgestellten Verfahren müssen die folgenden beiden Bedingungen erfüllt sein:

- Die für die Authentisierung benutzten Zufallswerte müssen bei jeder Durchführung des Protokolls mit großer Wahrscheinlichkeit verschieden sein. Dies kann zum Beispiel erreicht werden, indem jedes Mal ein Zufallswert bezüglich der Gleichverteilung auf $\{0,1\}^{120}$ gewählt wird.
- Die für die Schlüsselvereinbarung benutzten Zufallswerte müssen mindestens eine Entropie erreichen, die den gewünschten Schlüssellängen der auszuhandelnden Schlüssel entspricht.[1] Zusätzlich sollte jeder Teilnehmer an der Schlüsselvereinbarung mindestens 120 Bits Min-Entropie zu dem auszuhandelnden Schlüssel beitragen.

A.2.2. Symmetrische Verfahren

Grundsätzlich kann jedes Verfahren zur Instanzauthentisierung aus Abschnitt 7.1 mit jedem Verfahren zur Schlüsselvereinbarung aus Abschnitt 8.1 miteinander kombiniert werden. Die Kombination muss dabei so erfolgen, dass die ausgetauschten Schlüssel tatsächlich authentisiert sind und somit insbesondere Man-in-the-Middle-Attacken ausgeschlossen werden können. Für diese Anwendung wird folgendes Verfahren empfohlen:

Key Establishment Mechanism 5 aus [60].

Tabelle A.1: Empfohlenes symmetrisches Verfahren zur Schlüsselvereinbarung mit Instanzauthentisierung.

[1] Es wird an dieser Stelle davon ausgegangen, dass nur symmetrische Schlüssel ausgehandelt werden.

Bemerkung A.4 Als Verschlüsselungsverfahren können im Key Establishment Mechanism 5 aus [60] alle in dieser Technischen Richtlinie empfohlenen authentisierten Verschlüsselungsverfahren verwendet werden (siehe Abschnitt A.1).

A.2.3. Asymmetrische Verfahren

Analog wie für symmetrische Verfahren kann auch hier grundsätzlich jedes Verfahren zur Instanzauthentisierung aus Abschnitt 7.2 mit jedem Verfahren zur Schlüsselvereinbarung aus Abschnitt 8.2 kombiniert werden. Um dabei jedoch Fehler in selbst konstruierten Protokollen auszuschließen, werden die in Tabelle A.2 aufgelisteten Verfahren zur Schlüsselvereinbarung mit Instanzauthentisierung basierend auf asymmetrischen Verfahren empfohlen.

Alle empfohlenen Verfahren setzen als Vorbedingung die Existenz eines Mechanismus zur manipulationssicheren Verteilung öffentlicher Schlüssel voraus. Dieser Mechanismus muss die folgenden Eigenschaften aufweisen:

- Der durch einen Nutzer erzeugte öffentliche Schlüssel muss zuverlässig an dessen Identität gebunden sein.
- Der zugehörige private Schlüssel sollte zuverlässig an die Identität des Nutzers gebunden sein (es sollte einem Nutzer nicht möglich sein, einen öffentlichen Schlüssel unter seiner Identität zu registrieren, zu dem er den zugehörigen privaten Schlüssel nicht nutzen kann).

Es gibt mehrere Möglichkeiten, dies zu erreichen. Eine manipulationssichere Schlüsselverteilung kann durch eine PKI realisiert werden. Die Anforderung, dass die Besitzer aller durch die PKI ausgestellten Zertifikate tatsächlich Nutzer der zugehörigen privaten Schlüssel sein sollen, kann durch die PKI überprüft werden, indem sie vor der Ausstellung des Zertifikats eines der in Abschnitt 7.2 beschriebenen Protokolle zur Instanzauthentisierung mit dem Antragsteller unter Verwendung seines öffentlichen Schlüssels durchführt.

Falls die PKI eine solche Prüfung nicht durchführt, wird empfohlen, die unten empfohlenen Verfahren um einen Schritt zur Schlüsselbestätigung zu ergänzen, in dem geprüft wird, dass beide Seiten das gleiche gemeinsame Geheimnis K ermittelt haben und in dem dieses Geheimnis an die Identitäten der beiden Parteien gebunden wird. Zur Schlüsselbestätigung wird das in [94, Abschnitt 5.6.2] beschriebene Verfahren empfohlen. Im zweiten empfohlenen Verfahren (KAS2-bilateral-confirmation nach [94]) ist dieser Schritt bereits enthalten.

- Elliptic Curve Key Agreement of ElGamal Type (ECKA-EG), siehe [35],
- Instanzauthentisierung mit RSA und Schlüsselvereinbarung mit RSA, siehe KAS2-bilateral-confirmation nach [94, Abschnitt 8.3.3.4],
- MTI(A0), siehe [64, Annex D.7].

Tabelle A.2: Empfohlene asymmetrische Verfahren zur Schlüsselvereinbarung mit Instanzauthentisierung.

Bemerkung A.5 Um konform mit der vorliegenden Technischen Richtlinie zu sein, muss bei der konkreten Umsetzung der Protokolle darauf geachtet werden, dass dabei lediglich die in diesem Dokument empfohlenen kryptographischen Komponenten zur Anwendung kommen.

Bemerkung A.6 Bei dem Verfahren ECKA-EG findet keine gegenseitige Authentisierung statt. Hier beweist eine Partei der anderen lediglich im Besitz eines privaten Schlüssels zu sein, und auch dies

geschieht nur implizit, und zwar durch den im Anschluss an die Ausführung des Protokolls vorhandenen Besitz des ausgehandelten Geheimnisses.

Anhang B.

Zusätzliche Funktionen und Algorithmen

Für einige der in dieser Technischen Richtlinie empfohlenen kryptographischen Verfahren werden zusätzliche Funktionen und Algorithmen benötigt, um beispielsweise Systemparameter zu generieren oder aus den von Zufallszahlengeneratoren oder Schlüsseleinigungsverfahren erhaltenen Werten symmetrische Schlüssel abzuleiten. Diese Funktionen und Algorithmen müssen sorgfältig gewählt werden, um das in dieser Technischen Richtlinie geforderte Sicherheitsniveau zu erreichen und kryptoanalytische Angriffe zu verhindern.

B.1. Schlüsselableitung

B.1.1. Schlüsselableitung nach Schlüsseleinigung

Nach einem Schlüsseleinigungsverfahren sind beide Parteien im Besitz eines gemeinsamen Geheimnisses. Häufig müssen aus diesem Geheimnis mehrere symmetrische Schlüssel, zum Beispiel für die Verschlüsselung und zur Datenauthentisierung (siehe auch Bemerkung A.2), abgeleitet werden, was mithilfe einer Schlüsselableitungsfunktion ermöglicht werden kann. Daneben können durch Verwendung einer Schlüsselableitungsfunktion auch folgende Ziele erreicht werden:

- Bindung von Schlüsselmaterial an Protokolldaten (zum Beispiel Sendername, Empfängername,...) durch Verwendung der Protokolldaten in der Schlüsselableitungsfunktion.
- Ableitung von Sitzungsschlüsseln oder Schlüsseln für verschiedene Zwecke aus einem Masterschlüssel auch in rein symmetrischen Kryptosystemen.
- Nachbearbeitung von Zufallsdaten zur Beseitigung statistischer Schiefen bei der Erzeugung kryptographischer Schlüssel.

Für sämtliche Anwendungen von Schlüsselableitungsfunktionen wird folgendes Verfahren empfohlen:

Key Derivation through Extraction-then-Expansion nach [96, Abschnitt 5].

Tabelle B.1: Empfohlenes Verfahren zur Schlüsselableitung.

Im Rahmen der vorliegenden Technischen Richtlinie wird empfohlen, als MAC-Funktion in dem angegebenen Verfahren einen der in Abschnitt 6.2 empfohlenen MACs, die gleichzeitig eine pseudozufällige Funktion darstellen, einzusetzen (das heißt CMAC oder HMAC). Für Schlüssellängen von 128 Bit können gemäß [96, Tabelle 4,5] beide Verfahren gleichermaßen eingesetzt werden, für längere Schlüssel wird ausschließlich die Verwendung von HMAC empfohlen.

B.1.2. Passwort-basierte Schlüsselableitung

Bei der Passwort-basierten Schlüsselableitung wird ein kryptographischer Schlüssel (etwa für eine Festplattenverschlüsselung) direkt aus einem von einem Nutzer eingegebenen Passwort abgeleitet. Bei Verwendung nutzergenerierter Passwörter kann dadurch in der Regel mangels Entropie kein Sicherheitsniveau von 120 Bits erreicht werden.

Die vorliegende Technische Richtlinie empfiehlt in solchen Situationen die Ableitung des entsprechenden Schlüssels durch Anwendung eines MACs mit einem geheimen, nur für diesen Zweck genutzten Schlüssel auf das Passwort. Es wird empfohlen, den MAC auf kryptographisch sicherer, lokal im authentisierenden System vorhandener Hardware zu berechnen. Hierbei sollte ein CMAC oder ein HMAC mit mindestens 128 Bits Schlüssellänge genutzt werden und das Passwort sollte mit einem Salt-Wert von mindestens 32 Bits Länge kombiniert werden. Beim Scheitern einer Authentisierung oder einer Schlüsselableitung sollte die Hardware-Komponente verzögert reagieren, um lokale Brute-Force-Attacken auszuschließen. Die Qualität der Passwörter muss in diesem Fall den Anforderungen aus Abschnitt 7.3.1 entsprechen, wobei Offline-Attacken als ausgeschlossen betrachtet werden können.

Falls die Verwendung einer kryptographischen Sicherheitskomponente zur passwortbasierten Schlüsselableitung nicht möglich ist, sollte die Hashfunktion `Argon2id` [13] genutzt werden. Die Sicherheitsparameter von `Argon2id` und die Anforderungen an die Passwörter sind in Abhängigkeit von dem Anwendungsszenario mit einem Experten abzusprechen.

B.2. Erzeugung unvorhersagbarer Initialisierungsvektoren

Wie bereits in Abschnitt 2.1.2 erwähnt, müssen Initialisierungsvektoren für symmetrische Verschlüsselungsverfahren, die die Betriebsart Cipher Block Chaining Mode (CBC) einsetzen, unvorhersagbar sein. Dies bedeutet nicht, dass die Initialisierungsvektoren vertraulich behandelt werden müssen, sondern lediglich, dass ein möglicher Angreifer praktisch nicht in der Lage sein darf, zukünftig eingesetzte Initialisierungsvektoren zu erraten. Darüber hinaus darf der Angreifer auch nicht in der Lage sein, die Wahl der Initialisierungsvektoren zu beeinflussen.

In dieser Technischen Richtlinie werden die folgenden beiden Verfahren zur Erzeugung unvorhersagbarer Initialisierungsvektoren empfohlen, wobei n die Blockgröße der eingesetzten Blockchiffre bezeichnet:

Zufällige Initialisierungsvektoren:	Erzeugung einer zufälligen Bitfolge der Länge n mithilfe eines geeigneten Zufallszahlengenerators (siehe Kapitel 10) und Nutzung dieser Bitfolge als Initialisierungsvektor.
Verschlüsselte Initialisierungsvektoren:	Nutzung eines deterministischen Verfahrens zur Erzeugung von Prä-Initialisierungsvektoren (zum Beispiel einem Zähler). Verschlüsselung des Prä-Initialisierungsvektors mit der einzusetzenden Blockchiffre und einem vom eigentlichen Schlüssel verschiedenen Schlüssel (zum Beispiel Hashwert des einzusetzenden Verschlüsselungsschlüssels), und Nutzung des Chiffretexts als Initialisierungsvektor.

Tabelle B.2: Empfohlene Verfahren zur Erzeugung unvorhersagbarer Initialisierungsvektoren.

Bei der zweiten Methode muss darauf geachtet werden, dass sich die Prä-Initialisierungsvektoren während der Lebensdauer des Systems nicht wiederholen. Falls ein Zähler als Prä-Initialisierungsvektor verwendet wird, bedeutet dies, dass Zählerüberläufe während der gesamten Systemlebensdauer nicht auftreten dürfen.

B.3. Erzeugung von EC-Systemparametern

Die Sicherheit asymmetrischer Verfahren auf Basis elliptischer Kurven beruht auf der angenommenen Schwierigkeit der Berechnung diskreter Logarithmen in diesen Gruppen.

Zur Festlegung von EC-Systemparametern werden folgende Komponenten benötigt:

1.) Eine Primzahl p,

2.) Kurvenparameter $a, b \in \mathbb{F}_p$ mit $4a^3 + 27b^2 \neq 0$, die eine elliptische Kurve

$$E = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p;\ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}_E\}$$

festlegen, und

3.) ein Basispunkt P auf $E(\mathbb{F}_p)$.

Die *EC-Systemparameter* sind dann durch die Werte (p, a, b, P, q, i) gegeben, wobei $q := \mathrm{ord}(P)$ die Ordnung des Basispunktes P in $E(\mathbb{F}_p)$ bezeichnet, $p > 3$ und $i := \mathrm{Card}(E(\mathbb{F}_p))/q$ der sogenannte *Kofaktor* ist.

Nicht alle EC-Systemparameter sind für die in dieser Technischen Richtlinie empfohlenen asymmetrischen Verfahren, die auf elliptischen Kurven basieren, geeignet, in der Hinsicht, dass für einige Parameterkonstellationen das diskrete Logarithmusproblem in den von diesen elliptischen Kurven generierten Gruppen effizient lösbar ist. Neben einer ausreichenden Bitlänge von q müssen zusätzlich die folgenden Bedingungen erfüllt sein, siehe [74] für weitere Informationen:

- Die Ordnung $q = \mathrm{ord}(P)$ des Basispunktes P ist eine von p verschiedene Primzahl,
- $p^r \neq 1 \bmod q$ für alle $1 \leq r \leq 10^4$, und
- die Klassenzahl der Hauptordnung, die zum Endomorphismenring von E gehört, beträgt mindestens 10^7.

EC-Systemparameter, die die obigen Bedingungen erfüllen, werden auch als *kryptographisch stark* bezeichnet.

Bemerkung B.1 Es wird empfohlen, die EC-Systemparameter nicht selbst zu erzeugen, sondern stattdessen auf standardisierte Werte zurückzugreifen, die von einer vertrauenswürdigen Instanz zur Verfügung gestellt werden.

Die in Tabelle B.3 aufgelisteten Systemparameter werden empfohlen:

- brainpoolP256r1, siehe [74],
- brainpoolP320r1, siehe [74],
- brainpoolP384r1, siehe [74],
- brainpoolP512r1, siehe [74].

Tabelle B.3: Empfohlene EC-Systemparameter für asymmetrische Verfahren, die auf elliptischen Kurven basieren.

B.4. Generierung von Zufallszahlen für probabilistische asymmetrische Verfahren

In dieser Technischen Richtlinie werden mehrere asymmetrische Verfahren behandelt, die Zufallszahlen $k \in \{0, \ldots, q-1\}$ (zum Beispiel als Ephemeralschlüssel) benötigen, wobei q in der Regel keine 2er-Potenz ist. Bereits in den Bemerkungen 3.6, 3.5, 6.6 und 6.8 wurde darauf hingewiesen, dass k nach Möglichkeit (zumindest nahezu) gleichverteilt gewählt werden sollte. Hingegen erzeugen die in Kapitel 10 vorgestellten Zufallszahlengeneratoren gleichverteilte Zufallszahlen auf $\{0, 1, \ldots, 2^n - 1\}$ („zufällige n-Bitstrings“). Die Aufgabe besteht also darin, aus diesen Zufallszahlen (wenigstens nahezu) gleichverteilte Zufallszahlen auf $\{0, 1, \ldots, q-1\}$ herzuleiten.

In den Algorithmen B.1 und B.2 werden zwei Verfahren genannt, die dies ermöglichen, wobei $n \in \mathbb{N}$ so gewählt ist, dass $2^{n-1} \leq q < 2^n - 1$ gilt, das heißt q hat die Bitlänge n.

Algorithmus B.1: Verfahren 1 zur Berechnung von Zufallswerten auf $\{0, \ldots, q-1\}$.

Input: $n \in \mathbb{N}$ mit $2^{n-1} \leq q < 2^n - 1$
Output: $k \in \{0, 1, \ldots, q-1\}$ gleichverteilt

1: Wähle $k \in \{0, 1, \ldots, 2^n - 1\}$ gleichverteilt.
2: **while** $k \geq q$ **do**
3: Wähle $k \in \{0, 1, \ldots, 2^n - 1\}$ gleichverteilt.
4: **end while**

Algorithmus B.2: Verfahren 2 zur Berechnung von Zufallswerten auf $\{0, \ldots, q-1\}$.

Input: $n \in \mathbb{N}$ mit $2^{n-1} \leq q < 2^n - 1$
Output: $k \in \{0, 1, \ldots, q-1\}$ (nahezu) gleichverteilt.

1: Wähle $k' \in \{0, 1, \ldots, 2^{n+64} - 1\}$ gleichverteilt.
2: Setze $k = k' \bmod q$.

Bemerkung B.2 (i) Verfahren 1 in Algorithmus B.1 überführt eine Gleichverteilung auf $\{0, \ldots, 2^n - 1\}$ in eine Gleichverteilung auf $\{0, \ldots, q-1\}$, genauer liefert Verfahren 1 die bedingte Verteilung auf $\{0, \ldots, q-1\} \subset \{0, \ldots, 2^n - 1\}$. Hingegen erzeugt Verfahren 2 in Algorithmus B.2 selbst für ideale Zufallszahlengeneratoren mit Werten in $\{0, \ldots, 2^n - 1\}$ keine (perfekte) Gleichverteilung auf $\{0, \ldots, q-1\}$. Die Abweichungen sind jedoch so gering, dass sie nach derzeitigem Wissensstand von einem Angreifer nicht ausgenutzt werden können.

(ii) Das zweite Verfahren besitzt den Vorteil, dass etwaige vorhandene Schiefen auf $\{0, \ldots, 2^n - 1\}$ in aller Regel reduziert werden. Für PTG.2-konforme Zufallszahlengeneratoren wurde daher nur dieses Verfahren empfohlen. Es sei jedoch darauf hingewiesen, dass die direkte Nutzung von PTG.2-Generatoren nicht mehr empfohlen wird.

(iii) Verfahren 1 besitzt den Nachteil, dass die Anzahl der Iterationen (und damit die Laufzeit) nicht konstant ist. Für manche Anwendungen kann es jedoch notwendig sein, eine obere Laufzeitschranke zu garantieren. An dieser Stelle sei angemerkt, dass die Wahrscheinlichkeit, dass eine auf $k \in \{0, 1, \ldots, 2^n - 1\}$ gleichverteilte Zufallszahl kleiner als q ist, größer als $q/2^n \geq 2^{n-1}/2^n = 1/2$ ist.

B.5. Erzeugung von Primzahlen

B.5.1. Vorbemerkungen

Bei der Festlegung der Systemparameter für RSA-basierte asymmetrische Verfahren müssen zwei Primzahlen p und q gewählt werden. Für die Sicherheit der Verfahren ist es nötig, dass diese Primzahlen geheim gehalten werden. Dies setzt insbesondere voraus, dass p und q zufällig gewählt werden. Im Hinblick auf die Benutzerfreundlichkeit einer Anwendung, in der RSA-basierte Verfahren zum Einsatz kommen, ist es zudem wichtig, dass die Primzahlerzeugung effizient durchgeführt werden kann. Dabei ist zu beachten, dass proprietäre Geschwindigkeitsoptimierungen in der Schlüsselerzeugung zu signifikanten kryptographischen Schwächen führen können, siehe etwa [99]. Es wird daher dringend empfohlen, Verfahren einzusetzen, die öffentlich bekannt und hinsichtlich ihrer Sicherheit untersucht worden sind.

Routinen zur Erzeugung von zufälligen Primzahlen werden ferner für die Erzeugung von Systemparametern für ECC- beziehungsweise Körperarithmetik-basierte Kryptosysteme ohne spezielle Eigenschaften benötigt. Die Anforderungen an diese Primzahlen unterscheiden sich insofern von denen für das RSA-Verfahren, als dass Primzahlen nicht geheim gehalten werden müssen, sondern stattdessen eine *nachweisbare Zufälligkeit* ihrer Erzeugung von Relevanz sein kann. Weitere Einzelheiten und Hinweise zu diesem Thema finden sich in Abschnitt B.3.

B.5.2. Verfahren zur Erzeugung von Primzahlen

Zur Erzeugung zufälliger Primzahlen, die in einem vorgegebenen Intervall $[a, b] \cap \mathbb{N}$ liegen, sind drei Verfahren zulässig, die sich wie folgt kurz zusammenfassen lassen:

1.) Gleichverteilte Erzeugung zufälliger Primzahlen durch Verwerfungsmethode (englisch *rejection sampling*);

2.) Gleichverteilte Auswahl einer invertierbaren Restklasse r bezüglich $B\#$, wobei $B\#$ die *Primfakultät* von B ist, also das Produkt aller Primzahlen kleiner B, gefolgt von der Wahl einer Primzahl von geeigneter Größe mit Rest $r \bmod B\#$ durch Verwerfungsmethode;

3.) Erzeugung einer zufälligen Zahl s passender Größe, die zu $B\#$ teilerfremd ist, und Suche nach der nächsten Primzahl in der arithmetischen Folge, die durch $s, s+B\#, s+2\cdot B\#, \ldots$ gegeben ist.

Die ersten beiden Verfahren werden gleichermaßen empfohlen, das dritte Verfahren erzeugt gewisse statistische Schiefen in der Verteilung der erzeugten Primzahlen, die grundsätzlich unerwünscht sind. Es ist allerdings in der Praxis weit verbreitet (siehe etwa Table 1 in [109]) und es gibt zum aktuellen Zeitpunkt keine Hinweise darauf, dass sich die induzierten statistischen Schiefen für Angriffe nutzen lassen. Daher wird dieses Verfahren in der vorliegenden Technischen Richtlinie als Legacy-Verfahren akzeptiert.

Die folgenden Tabellen liefert eine genauere Beschreibung der drei durch diese Technische Richtlinie unterstützten Verfahren:

Algorithmus B.3: Empfohlenes Verfahren 1 zur Erzeugung von Primzahlen durch Verwerfungsmethode.

Input: Intervall $I := [a, b] \cap \mathbb{N}$
Output: $p \in I$ prim

1: Wähle $p \in I$ ungerade und gleichverteilt auf I.
2: **while** p zusammengesetzt **do**
3: Wähle $p \in I$ ungerade und gleichverteilt auf I.
4: **end while**

Algorithmus B.4: Empfohlenes Verfahren 2 zur Erzeugung von Primzahlen durch effizienzoptimierte Verwerfungsmethode.

Input: Intervall $I := [a, b] \cap \mathbb{N}$, $B \in \mathbb{N}$ mit $S := B\# \ll b - a$
Output: $p \in I$ prim

1: Wähle r in $(\mathbb{Z}/S)^*$ gleichverteilt (äquivalent: Wähle $r < S$ zufällig mit $\mathrm{ggT}(r, S) = 1$).
2: Wähle $k \in \mathbb{N}$ zufällig, so dass $p := kS + r \in I$ (äquivalent: Wähle k gleichverteilt auf $[\lceil (a - r)/S \rceil, \lfloor (b - r)/S \rfloor]$).
3: **while** p zusammengesetzt **do**
4: Wähle $k \in \mathbb{N}$ zufällig, so dass $p := kS + r \in I$ (äquivalent: Wähle k gleichverteilt auf $[\lceil (a - r)/S \rceil, \lfloor (b - r)/S \rfloor]$).
5: **end while**

Algorithmus B.5: Legacy-Verfahren zur Erzeugung von Primzahlen durch inkrementelle Suche.

Input: Intervall $I := [a, b] \cap \mathbb{N}$, $B \in \mathbb{N}$ mit $S := B\# \ll b - a$
Output: $p \in I$ prim

1: **repeat**
2: Wähle r in $(\mathbb{Z}/S)^*$ gleichverteilt (äquivalent: Wähle $r < S$ zufällig mit $\mathrm{ggT}(r, S) = 1$).
3: Wähle $k \in \mathbb{N}$ zufällig, so dass $p := kS + r \in I$ (äquivalent: Wähle k gleichverteilt auf $[\lceil (a - r)/S \rceil, \lfloor (b - r)/S \rfloor]$).
4: **while** p zusammengesetzt, $p \in I$ **do**
5: $p \leftarrow p + S$
6: **end while**
7: **until** p prim

Als Primzahltest in den oben beschriebenen Algorithmen kommt aus Effizienzgründen meist ein probabilistischer Primzahltest zum Einsatz. Im Rahmen dieser Technischen Richtlinie wird der folgende Algorithmus empfohlen:

Miller-Rabin, siehe [80, Algorithmus 4.24].

Tabelle B.4: Empfohlener probabilistischer Primzahltest.

Bemerkung B.3 (Miller-Rabin-Algorithmus) Der Miller-Rabin-Algorithmus benötigt neben der zu untersuchenden Zahl p einen Zufallswert $x \in \{2, 3, \ldots, p - 2\}$, die sogenannte Basis. Ist x zufällig bezüglich der Gleichverteilung auf $\{2, 3, \ldots, p - 2\}$ gewählt, so beträgt die Wahrscheinlichkeit, dass p zusammengesetzt ist, obwohl der Miller-Rabin-Algorithmus ausgibt, dass p eine Primzahl sei, höchstens $1/4$.

Worst Case: Um die Wahrscheinlichkeit, dass eine feste Zahl p mittels des Miller-Rabin-Algorithmus als Primzahl ausgegeben wird, obwohl sie zusammengesetzt ist, auf 2^{-120} zu beschränken, muss der Algorithmus 60-mal mit jeweils unabhängig voneinander bezüglich der Gleichverteilung gewählten Basen $x_1, \ldots, x_{60} \in \{2, 3, \ldots, p - 2\}$ aufgerufen werden, siehe auch Abschnitt B.4 für empfohlene Verfahren zur Berechnung gleichverteilter Zufallszahlen aus $\{2, 3, \ldots, p - 2\}$.

Average Case: Um eine zufällig bezüglich der Gleichverteilung gewählte ungerade Zahl $p \in [2^{b-1}, 2^b - 1]$ mit der gewünschten Sicherheit auf ihre Primzahleigenschaft zu testen, reichen bei weitem weniger Iterationen des Miller-Rabin-Algorithmus aus, als es die

eben genannte Abschätzung nahelegen würde, vergleiche [43], [89, Appendix F] und [62, Annex A]. So werden für $b = 1536$ lediglich vier Iterationen benötigt, um bei einer verbleibenden Fehlerwahrscheinlichkeit von 2^{-128} auszuschließen, dass p zusammengesetzt ist, obwohl der Miller-Rabin-Algorithmus p als Primzahl erkennt [62]. Auch hierfür müssen die Basen unabhängig und zufällig bezüglich der Gleichverteilung aus $\{2, 3, \ldots, p-2\}$ gewählt werden. Die konkrete Anzahl an notwendigen Operationen hängt von der Bitlänge von p ab, da die Zahlen, für die die Abschätzungen des Worst-Case-Falles zutreffen, mit steigender Größe der Zahlen in ihrer Dichte deutlich abnehmen.

Optimierungen: Zur Optimierung der Laufzeit etwa von Algorithmus B.3 kann es hilfreich sein, zusammengesetzte Zahlen mit sehr kleinen Faktoren durch Probedivision oder Siebtechniken vor Anwendung des probabilistischen Primzahltests zu eliminieren. Ein solcher Vortest hat nur geringfügige Auswirkungen auf die Wahrscheinlichkeit, dass vom Test als Primzahl klassifizierte Zahlen doch zusammengesetzt sind. Die Empfehlungen zur erforderlichen Anzahl der Wiederholungen des Miller-Rabin-Tests gelten daher für auf solche Art optimierte Varianten des Verfahrens unverändert.

Sonstige Anmerkungen: Entsprechend [89, Appendix F.2] wird auch in dieser Richtlinie empfohlen, bei der Erzeugung von Primzahlen, die in besonders sicherheitskritischen Funktionen eines Kryptosystems Verwendung finden sollen oder deren Erzeugung wenig zeitkritisch ist, eine Verifikation der Primzahleigenschaft mit 60 Runden des Miller-Rabin-Tests durchzuführen. Dies betrifft zum Beispiel Primzahlen, die als dauerhafte Parameter eines kryptographischen Verfahrens einmal erzeugt und dann über einen längeren Zeitraum nicht gewechselt sowie unter Umständen von vielen Nutzern verwendet werden.

Zur Erzeugung der benötigten Zufallszahlen kann ein Zufallszahlengenerator der Funktionalitätsklassen PTG.3, DRG.4, DRG.3 oder NTG.1 genutzt werden. Bei Verwendung eines deterministischen Zufallszahlengenerators ist aus informationstheoretischer Sicht zwar keine gleichverteilte Primzahlerzeugung möglich, allerdings entsteht dadurch keine Sicherheitslücke: Ein Zufallszahlengenerator der Funktionalitätsklasse DRG.3 oder DRG.4 erzeugt unter kryptographischen Standardannahmen Zufallszahlen mit einer Verteilung, die bei Verwendung klassischer Computer durch keinen bekannten Angriff mit realistischem praktischem Aufwand von einer idealen Verteilung unterschieden werden kann.

Es ist allerdings in diesem Zusammenhang zu beachten, dass das Sicherheitsniveau der erzeugten RSA-Moduln in diesem Fall möglicherweise durch das Sicherheitsniveau der Zufallszahlenerzeugung beschränkt wird. Dies wäre etwa der Fall, wenn ein Zufallszahlengenerator mit 120 Bits Sicherheitsniveau zur Erzeugung von RSA-Schlüsseln einer Länge von 4096 Bits genutzt würde.

Alternative Primzahltests: Die Auswahl eines Primzahltests ist aus kryptoanalytischer Sicht nicht sicherheitskritisch, solange der gewählte Test Primzahlen nicht fälschlicherweise als zusammengesetzt klassifiziert und solange die Wahrscheinlichkeit, dass zusammengesetzte Zahlen ihn bestehen, vernachlässigbar gering ist. Daher können andere Tests, für die diese Eigenschaften in der Literatur nachgewiesen worden sind, anstelle des Miller-Rabin-Tests eingesetzt werden, ohne dass die Konformität zu der vorliegenden Technischen Richtlinie verloren geht. Die Verwendung des sehr weit bekannten Miller-Rabin-Verfahrens ist allerdings unter anderem im Hinblick auf eine Überprüfung der Korrektheit einer Implementierung sowie auf eine Prüfung der Seitenkanalresistenz vorteilhaft.

B.5.3. Erzeugung von Primzahlpaaren

Um die Sicherheit von Schlüsselpaaren, für die die zugrundeliegenden RSA-Moduln durch Multiplikation zweier unabhängig voneinander mit einem der geeigneten Verfahren erzeugten Primzahlen

berechnet wurden, zu gewährleisten, ist es wichtig, dass das Intervall $I := [a, b] \cap \mathbb{N}$ nicht zu klein ist. Wenn Schlüsselpaare erzeugt werden sollen, deren Modulus N eine vorher festgelegte Bitlänge n aufweist, bietet es sich an, $I = [\lceil \frac{2^{(n/2)}}{\sqrt{2}} \rceil, \lfloor 2^{(n/2)} \rfloor] \cap \mathbb{N}$ zu wählen. Eine andere Wahl von I ist zu dieser Technischen Richtlinie konform, wenn für p und q das gleiche Intervall I genutzt wird und $\mathrm{Card}(I) \geq 2^{-8} b$ ist.

B.5.4. Hinweise zur Sicherheit der empfohlenen Verfahren

Im Folgenden bezeichne π die Primzahlfunktion, also $\pi(x) := \mathrm{Card}(\{n \in \mathbb{N} : n \leq x, n \text{ prim}\})$. Nach dem Primzahlsatz ist $\pi(x)$ asymptotisch äquivalent zu $x/\ln(x)$, das heißt

$$\lim_{x \to \infty} \frac{\pi(x) \cdot \ln(x)}{x} = 1.$$

Die Sicherheit der hier empfohlenen Verfahren zur Primzahlerzeugung stützt sich auf die folgenden Beobachtungen:

- Alle drei Verfahren können jede Primzahl erzeugen, die in dem vorgegebenen Intervall enthalten ist, falls der zugrundeliegende Zufallszahlengenerator alle Kandidaten aus dem jeweils zulässigen Bereich erzeugen kann.
- Die ersten beiden Verfahren erzeugen Primzahlen, deren Verteilung bei Verwendung der empfohlenen Sicherheitsparameter praktisch nicht von einer Gleichverteilung unterschieden werden kann. Dies ist unmittelbar ersichtlich für das erste Verfahren; für das zweite Verfahren ergibt es sich heuristisch aus dem *Dirichlet'schen Primzahlsatz*: Die relative Häufigkeit von Primzahlen ist in allen invertierbaren Restklassen modulo S asymptotisch gleich, und die Restklasse modulo S der zu erzeugenden Primzahl wird gemäß der Gleichverteilung auf $(\mathbb{Z}/S)^*$ gewählt.
- Das im vorhergehenden Punkt genannte Argument für die Sicherheit des zweiten Verfahrens liefert strenggenommen keine Garantie dafür, dass für ein konkretes S und ein konkretes Intervall I die Häufigkeit von Primzahlen während der Suche tatsächlich nicht von der gewählten Restklasse $r \bmod S$ abhängig ist. In der Tat ist klar, dass diese asymptotische Aussage nicht gültig sein wird, wenn S sich der Größenordnung von $b - a$ annähert. Es ist aber anzunehmen, dass es keine wesentlichen Unterschiede bezüglich der Primzahldichte zwischen den verschiedenen Restklassen gibt, wenn die Anzahl der Primzahlen in den einzelnen Restklassen groß ist. Das Intervall I enthält $\pi(b) - \pi(a)$ Primzahlen, für jede Restklasse $\mathrm{mod} S$ werden daher $\frac{\pi(b)-\pi(a)}{\varphi(S)}$ Primzahlen erwartet. Für Zahlen der Größenordnung von etwa 1000 Bits kann dieser Erwartungswert mit einem geringen relativen Fehler auf $\frac{b\ln(a)-a\ln(b)}{\ln(a)\ln(b)\varphi(S)}$ geschätzt werden, solange $\varphi(S)$ klein im Vergleich zum Zähler des Bruches ist. Es wird empfohlen, S so zu wählen, dass $\frac{b\ln(a)-a\ln(b)}{\ln(a)\ln(b)\varphi(S)} \geq 2^{64}$ gilt.
- Die oben wiedergegebenen qualitativen Erwägungen sind ausreichend, um das zweite Verfahren als geeignet einzuschätzen. In der Literatur gibt es genauere Untersuchungen zu eng verwandten Mechanismen zur Primzahlerzeugung, siehe etwa [48].
- Das dritte Verfahren erzeugt Primzahlen, die nicht gleichverteilt sind, auch wenn die erzeugten Schiefen in der Verteilung der Primzahlen nach derzeitigem Kenntnisstand als praktisch durch einen Angreifer nicht ausnutzbar gelten. Die Wahrscheinlichkeit einer Primzahl p in dem Intervall I, durch dieses Verfahren ausgegeben zu werden, ist proportional zur Länge des primzahlfreien Abschnitts in der arithmetischen Folge $p - kS$, $p - (k-1)S, \ldots, p - S$, p, die durch p beendet wird. Da die Primzahldichte in diesen arithmetischen Folgen für große S tendenziell zunimmt, wird erwartet, dass dieser Effekt für $S = 2$ am stärksten ausgeprägt

ist. Auch hier bedeutet er aber in der Praxis nur einen sehr begrenzten Entropieverlust. Man kann die Verteilungsschiefe nach oben begrenzen, indem die Suche abgebrochen und mit einem neuen Startwert wieder aufgenommen wird, falls nach einer angemessenen Zahl T von Schritten keine Primzahl gefunden wurde: In diesem Fall werden alle Primzahlen, die einer Lücke der Länge $\geq T$ folgen, mit gleicher Wahrscheinlichkeit ausgegeben.

Anhang C.

Protokolle für spezielle kryptographische Anwendungen

In diesem Kapitel werden Protokolle behandelt, die als Bausteine kryptographischer Lösungen benutzt werden können. In der aktuellen Version der vorliegenden Technischen Richtlinie betrifft dies nur das Protokoll SRTP (Secure Real-Time Transport Protocol), da entsprechende Informationen für TLS [24], IPsec [25] und SSH [26] inzwischen in die Teile zwei bis vier der Richtlinie ausgelagert wurden.

Im Allgemeinen hat die Verwendung etablierter Protokolle bei der Entwicklung kryptographischer Systeme den Vorteil, dass auf eine umfangreiche öffentliche Analyse zurückgegriffen werden kann. Eigenentwicklungen können demgegenüber leicht Schwächen enthalten, die für einen Entwickler nur schwer zu erkennen sind. Es wird daher empfohlen, wo immer es möglich ist, allgemein zugängliche, gegebenenfalls standardisierte und vielfach evaluierte Protokolle eigenen Protokollentwicklungen vorzuziehen.

C.1. SRTP

SRTP ist ein Protokoll, das das Audio- und Videoprotokoll RTP (Real-Time Transport Protocol) um Funktionen zur Sicherstellung von Vertraulichkeit und Integrität der übertragenen Nachrichten ergänzt. Es wird in RFC 3711 [8] definiert. SRTP muss mit einem Protokoll zum Schlüsselmanagement kombiniert werden, da es keine eigenen Mechanismen zur Aushandlung eines Kryptokontextes vorsieht.

Im Rahmen dieser Technischen Richtlinie werden folgende Spezifikationen bei der Verwendung von SRTP empfohlen:

- Als symmetrisches Verschlüsselungsverfahren mit kombiniertem Integritätsschutz wird AES im Galois/Counter Mode wie in [79] empfohlen.
- Als alternative Verschlüsselungsverfahren werden sowohl AES im Counter-Modus als auch im f8-Modus wie in [8] empfohlen. Als Integritätsschutz darf hier ein auf SHA1 basierender HMAC verwendet werden, da in [8] die Nutzung von Hashfunktionen der SHA2- oder SHA3-Familie nicht spezifiziert ist. Dieser HMAC darf im Kontext des Protokolls auf 80 Bits gekürzt werden.
- Als Schlüsselmanagementsystem sollte MIKEY [5] verwendet werden. Dabei werden die folgenden Schlüsselmanagementverfahren aus [5] empfohlen: DH-Schlüsseltausch mit Authentisierung über PKI, RSA mit PKI sowie Pre-Shared-Keys. Generell sollten innerhalb von MIKEY und SRTP als Komponenten nur in dieser Richtlinie empfohlene kryptographische Verfahren verwendet werden.
- zRTP sollte nur eingesetzt werden, wenn es mit unverhältnismäßig hohem Aufwand verbunden ist, das Problem der Schlüsselverteilung durch ein Public-Key-Verfahren unter Verwendung einer PKI oder durch Vorverteilung geheimer Schlüssel zu lösen.

- Es wird dringend empfohlen, die in [8] vorgesehenen Mechanismen zum Replay- und Integritätsschutz in SRTP zu nutzen.

Bei Anwendungen zur sicheren Übertragung von Audio- und Videodaten in Echtzeit sollte besonders darauf geachtet werden, die Entstehung von Seitenkanälen, beispielsweise durch Datenübertragungsrate, die zeitliche Abfolge verschiedener Signale oder eine sonstige Verkehrsanalyse, zu minimieren. Andernfalls sind Angriffe wie die in [7] vorgestellten möglich.

Literaturverzeichnis

[1] M. Abdalla, M. Bellare, and P. Rogaway. DHIES: An encryption scheme based on the Diffie-Hellman problem. 2001. https://cseweb.ucsd.edu/~mihir/papers/dhies.pdf.

[2] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tonel. Status report on the third round of the nist post-quantum cryptography standardization process, 2022. https://csrc.nist.gov/publications/detail/nistir/8413/final.

[3] M. R. Albrecht, , D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurich, R. Misoczki, R. Niederhagen, K. G. Paterson, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C. J. Tjhai, M. Tomlinson, and W. Wang. Classic McEliece: conservative code-based cryptography: cryptosystem specification, 2022. https://classic.mceliece.org/mceliece-spec-20221023.pdf.

[4] E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. FrodoKEM: Learning With Errors Key Encapsulation. Einreichung zur dritten Runde des NIST PQC-Standardisierungswettbewerbs, 2021. https://frodokem.org/files/FrodoKEM-specification-20210604.pdf.

[5] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman. MIKEY: Multimedia Internet KEYing. RFC 3830, 2004. https://datatracker.ietf.org/doc/html/rfc3830.

[6] atsec information security GmbH. Documentation and Analysis of the Linux Random Number Generator. Dauerstudie im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/LinuxRNG.

[7] L. Ballard, S. Coull, F. Monrose, G. Masson, and C. Wright. Spot me if you can: recovering spoken phrases in encrypted VoIP conversations. *IEEE Symposium on Security and Privacy*, 2008.

[8] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman. The Secure Real-time Transport Protocol (SRTP). RFC 3711, 2004. https://datatracker.ietf.org/doc/html/rfc3711.

[9] M. Bellare, R. Canetti, and H. Krawczyk. Keying Hash Functions for Message Authentication. In *Advances in Cryptology – CRYPTO 1996*, volume 1109 of *LNCS*, pages 1–15. Springer, 1996.

[10] M. Bellare, R. Canetti, and H. Krawczyk. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, 1997. https://datatracker.ietf.org/doc/html/rfc2104.

[11] M. Bellare and S. K. Miner. A Forward-Secure Digital Signature Scheme. In *Advances in Cryptology – CRYPTO 1999*, volume 1666 of *LNCS*, pages 431–448, 1999.

[12] D. J. Bernstein. Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? *SHARCS*, 2009.

[13] A. Biryukov, D. Dinu, D. Khovratovich, and S. Josefsson. Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications. RFC 9106, 2021. https://www.rfc-editor.org/info/rfc9106.

[14] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir. Key Recovery Attacks of Practical Complexity on AES-256 Variants With Up to 10 Rounds. In *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 299–319, 2010.

[15] A. Biryukov and D. Khovratovich. Related-Key Cryptanalysis of the Full AES-192 and AES-256. In *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 1–18, 2009.

[16] S. Blake-Wilson and A. Menezes. Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol. In *Public Key Cryptography*, Volume 1560 of LNCS, pages 154–170. Springer, 1999.

[17] D. Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1. In *Advances in Cryptology – CRYPTO 1998*, volume 1462 of *LNCS*, pages 1–12. Springer, 1998.

[18] H. Böck, J. Somorovsky, and C. Young. Return Of Bleichenbacher's Oracle Threat (ROBOT). In *27th USENIX Security Symposium (USENIX Security 18)*, pages 817–849. USENIX Association, 2018.

[19] A. Bogdanov, D. Khovratovich, and C. Rechberger. Biclique cryptanalysis of the full AES. In *Advances in Cryptology – ASIACRYPT 2011*, Volume 7073 of LNCS, pages 344–371. Springer, 2011.

[20] D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE transactions on Information Theory*, 46(4):1339–1349, 2000.

[21] D. R. L. Brown. Generic Groups, Collision Resistance, and ECDSA. *Designs, Codes and Cryptography*, 35(1):119–152, 2005.

[22] D. R. L. Brown and R. P. Gallant. The Static Diffie-Hellman Problem. Cryptology ePrint Archive, Report 2004/306, 2004. https://ia.cr/2004/306.

[23] J. Buchmann, E. Dahmen, and A. Hülsing. XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In *Post-Quantum Cryptography*, volume 7071 of *LNCS*, pages 117–129. Springer, 2011.

[24] Bundesamt für Sicherheit in der Informationstechnik. BSI TR 02102-2: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS). https://www.bsi.bund.de/TR-02102.

[25] Bundesamt für Sicherheit in der Informationstechnik. BSI TR 02102-3: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von IPsec. https://www.bsi.bund.de/TR-02102.

[26] Bundesamt für Sicherheit in der Informationstechnik. BSI TR 02102-4: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 4 – Verwendung von Secure Shell (SSH). https://www.bsi.bund.de/TR-02102.

[27] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html.

[28] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03125: Beweiswerterhaltung kryptographisch signierter Dokumente. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html.

[29] Bundesamt für Sicherheit in der Informationstechnik. A proposal for: Functionality classes for random number generators. Version 2, 2011. https://www.bsi.bund.de/dok/ais-20-31-appx-2011.

[30] Bundesamt für Sicherheit in der Informationstechnik. AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren. Version 3, 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.pdf.

[31] Bundesamt für Sicherheit in der Informationstechnik. AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren. Version 3, 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.pdf.

[32] Bundesamt für Sicherheit in der Informationstechnik. Anhang zu AIS 46: *Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations*. Version 1, 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_BSI_guidelines_SCA_RSA_V1_0_e_pdf.pdf.

[33] Bundesamt für Sicherheit in der Informationstechnik. Anhang zu AIS 46: *Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations*. Version 2, 2016. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_ECCGuide_e_pdf.pdf.

[34] Bundesamt für Sicherheit in der Informationstechnik. BSI TR 3110-2: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS). Version 2.21, 2016. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf.

[35] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03111: Elliptic Curve Cryptography. Version 2.10, 2018. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf.

[36] Bundesamt für Sicherheit in der Informationstechnik. Entwicklungsstand Quantencomputer. Version 1.2, 2020. https://www.bsi.bund.de/qcstudie.

[37] Bundesamt für Sicherheit in der Informationstechnik. Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen. 2021. https://bsi.bund.de/dok/997274.

[38] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03116-2: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 2 – Hoheitliche Ausweisdokumente. 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-2.pdf.

[39] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03116-4: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4 – Kommunikationsverfahren in Anwendungen. 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf.

[40] S. Chen, R. Wang, X. Wang, and K. Zhang. Side-Channel Leaks in Web Applications: A Reality Today, a Challenge Tomorrow. In *2010 IEEE Symposium on Security and Privacy*, pages 191–206. IEEE, 2010. http://research.microsoft.com/pubs/119060/WebAppSideChannel-final.pdf.

[41] J. H. Cheon. Security analysis of the strong Diffie-Hellman problem. In *Advances in Cryptology – EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 1–11. Springer, 2006.

[42] J.-S. Coron, D. Naccache, and J. P. Stern. On the security of RSA padding. In *Advances in Cryptology – CRYPTO 1999*, volume 1666 of *LNCS*, pages 1–18. Springer, 1999.

[43] I. Damgård, P. Landrock, and C. Pomerance. Average Case Error Estimates for the Strong Probable Prime Test. *Mathematics of computation*, 61(203):177–194, 1993.

[44] W. Diffie, P. C. Van Oorschot, and M. J. Wiener. Authentication and Authenticated Key Exchanges. *Designs, Codes and Cryptography*, 2(2):107–125, 1992.

[45] ECRYPT – CSA. Algorithms, Key Size and Protocols Report, 2018. https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[46] ECRYPT – II. Algorithms, Key Size and Protocols Report, 2012. https://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf.

[47] N. Ferguson. Authentication weaknesses in GCM. *Comments submitted to NIST Modes of Operation Process*, 2005. https://csrc.nist.gov/csrc/media/projects/block-cipher-techniques/documents/bcm/comments/cwc-gcm/ferguson2.pdf.

[48] P.-A. Fouque and M. Tibouchi. Close to uniform prime number generation with fewer random bits. *IEEE Transactions on Information Theory*, 65(2):1307–1317, 2019.

[49] M. Gebhardt, G. Illies, and W. Schindler. A note on the practical value of single hash collisions for special file formats. In *Sicherheit 2006, Sicherheit – Schutz und Zuverlässigkeit*, pages 333–344. Gesellschaft für Informatik e.V., 2006. https://dl.gi.de/bitstream/handle/20.500.12116/24792/GI-Proceedings-77-41.pdf.

[50] D. Gillmor. Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS). RFC 7919, 2016. https://datatracker.ietf.org/doc/html/rfc7919.

[51] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pages 212–219. Association for Computing Machinery, 1996.

[52] S. Gueron, A. Langley, and Y. Lindell. AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption.

[53] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman. Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices. In *21st USENIX Security Symposium (USENIX Security 12)*, pages 205–220. USENIX Association, 2012. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final228.pdf.

[54] R. Housley. Cryptographic Message Syntax (CMS). RFC 5652, 2009. https://datatracker.ietf.org/doc/html/rfc5652.

[55] A. Hülsing, D. Butin, S.-L. Gazdag, J. Rijneveld, and A. Mohaisen. XMSS: eXtended Merkle Signature Scheme. RFC 8391, 2018. https://datatracker.ietf.org/doc/html/rfc8391.

[56] G. Illies, M. Lochter, and O. Stein. Behördliche Vorgaben zu kryptografischen Algorithmen. *Datenschutz und Datensicherheit-DuD*, 35(11):807–811, 2011.

[57] International Organization for Standardization. ISO/IEC 18033-2:2006 Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers, 2006.

[58] International Organization for Standardization. ISO/IEC 14888-2:2008 Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms, 2008.

[59] International Organization for Standardization. ISO/IEC 9797-1:2011 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, 2011.

[60] International Organization for Standardization. ISO/IEC 11770-2:2018 Information security – Key management – Part 2: Mechanisms using symmetric techniques, 2018.

[61] International Organization for Standardization. ISO/IEC 14888-3:2018 Information technology – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, 2018.

[62] International Organization for Standardization. ISO/IEC 18032:2020 Information security – Prime number generation, 2020.

[63] International Organization for Standardization. ISO/IEC 9796-2:2010 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2020.

[64] International Organization for Standardization. ISO/IEC 11770-3:2021 Information security – Key management – Part 3: Mechanisms using asymmetric techniques, 2021.

[65] T. Iwata, K. Ohashi, and K. Minematsu. Breaking and Repairing GCM Security Proofs. In *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *LNCS*, pages 31–49. Springer, 2012.

[66] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In *Advances in Cryptology – CRYPTO 2016*, volume 9815 of *LNCS*, pages 207–237. Springer, 2016.

[67] J. Kelsey, B. Schneier, and D. Wagner. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In *Advances in Cryptology – CRYPTO 1996*, volume 1109 of *LNCS*, pages 237–251. Springer, 1996.

[68] S. Kent. IP Encapsulating Security Payload (ESP). RFC 4303, 2005. https://datatracker.ietf.org/doc/html/rfc4303.

[69] T. Kivinen and M. Kojo. More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE). RFC 3526, 2003. https://datatracker.ietf.org/doc/html/rfc3526.

[70] A. K. Lenstra. Key lengths. In *Handbook of Information Security*, volume II, 2006.

[71] A. K. Lenstra and E. R. Verheul. Selecting Cryptographic Key Sizes. *Journal of Cryptology*, 14(4):255–293, 2001.

[72] G. Leurent and T. Peyrin. From Collisions to Chosen-Prefix Collisions Application to Full SHA-1. In *Advances in Cryptology – EUROCRYPT 2019*, volume 11478 of *LNCS*, pages 527–555. Springer, 2019.

[73] G. Leurent and T. Peyrin. SHA-1 is a Shambles: First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1839–1856. USENIX Association, 2020. https://www.usenix.org/system/files/sec20-leurent.pdf.

[74] M. Lochter and J. Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. RFC 5639, 2010. https://datatracker.ietf.org/doc/html/rfc5639.

[75] S. Lucks. Attacking Triple Encryption. In *Fast Software Encryption*, volume 1372 of *LNCS*, pages 239–253. Springer, 1998.

[76] S. Lucks and M. Daum. The Story of Alice and her Boss: Hash Functions and the Blind Passenger Attack. Presentation. https://www.cits.rub.de/imperia/md/content/magnus/rumpec05.pdf.

[77] V. G. Martínez, F. H. Álvarez, L. H. Encinas, and C. S. Ávila. A Comparison of the Standardized Versions of ECIES. In *Sixth International Conference on Information Assurance and Security, IAS 2010*, pages 1–4. IEEE, 2010.

[78] D. McGrew, M. Curcio, and S. Fluhrer. Leighton-Micali Hash-Based Signatures. RFC 8554, 2019. https://datatracker.ietf.org/doc/html/rfc8554.

[79] D. McGrew and K. Igoe. AES-GCM Authenticated Encryption in the Secure Real-Time Transport Protocol (SRTP). RFC 7714, 2015. https://datatracker.ietf.org/doc/html/rfc7714.

[80] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[81] R. C. Merkle. Secure Communications over Insecure Channels. *Communications of the ACM*, 21(4):294–299, 1978.

[82] R. C. Merkle and M. E. Hellman. On the security of multiple encryption. *Communications of the ACM*, 24(7):465–467, 1981.

[83] K. Moriarty, B. Kaliski, J. Jonsson, and A. Rusch. PKCS #1: RSA Cryptography Specifications Version 2.2. RFC 8017, 2016. https://datatracker.ietf.org/doc/html/rfc8017.

[84] National Institute of Standards and Technology. Federal Information Processing Standards FIPS PUB 197: Advanced Encryption Standard (AES), 2001. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[85] National Institute of Standards and Technology. Special Publication NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf.

[86] National Institute of Standards and Technology. Special Publication NIST SP 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, 2007. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38c.pdf.

[87] National Institute of Standards and Technology. Special Publication NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf.

[88] National Institute of Standards and Technology. Special Publication NIST SP 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, 2010. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38e.pdf.

[89] National Institute of Standards and Technology. Federal Information Processing Standards FIPS PUB 186-4: Digital Signature Standard (DSS), 2013. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[90] National Institute of Standards and Technology. Federal Information Processing Standards FIPS PUB 180-4: Secure Hash Standard, 2015. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

[91] National Institute of Standards and Technology. Federal Information Processing Standards FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, 2015. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf.

[92] National Institute of Standards and Technology. Special Publication NIST SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2016. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-38b.pdf.

[93] National Institute of Standards and Technology. Special Publication NIST SP 800-67 Revision 2: Recommendation for the Triple Data Encryption Standard (TDEA) Block Cipher, 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf.

[94] National Institute of Standards and Technology. Special Publication NIST SP 800-56B Revision 2: Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography, 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf.

[95] National Institute of Standards and Technology. Special Publication NIST SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf.

[96] National Institute of Standards and Technology. Special Publication NIST SP 800-56C Revision 2: Recommendation for Key-Derivation Methods in Key-Establishment Schemes, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf.

[97] National Institute of Standards and Technology. Special Publication NIST SP 800-57 Part 1 Revision 5: Recommendation for Key Management: Part 1 – General, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.

[98] National Institute of Standards and Technology. Special Publication NIST SP 800-108r1: Recommendation for Key Derivation Using Pseudorandom Functions, 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-108r1.pdf.

[99] M. Nemec, M. Sys, P. Svenda, D. Klinec, and V. Matyas. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1631–1648. Association for Computing Machinery, 2017.

[100] P. Q. Nguyen and I. E. Shparlinski. The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces. *Designs, Codes and Cryptography*, 30(2):201–217, 2003.

[101] J.-F. Raymond and A. Stiglic. Security Issues in the Diffie-Hellman Key Agreement Protocol. 2000.

[102] T. Ristenpart and S. Yilek. When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography. In *Network and Distributed System Security Symposium (NDSS) 2010*, 2010.

[103] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.

[104] SOG-IS Crypto Working Group. SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms. Version 1.2, 2020. https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf.

[105] D. X. Song, D. A. Wagner, and X. Tian. Timing Analysis of Keystrokes and Timing Attacks on SSH. In *10th USENIX Security Symposium (USENIX Security 01)*. USENIX Association, 2001. https://www.usenix.org/legacy/events/sec2001/full_papers/song/song.pdf.

[106] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov. The First Collision for Full SHA-1. In *Advances in Cryptology – CRYPTO 2017*, volume 10401 of *LNCS*, pages 570–596. Springer, 2017.

[107] P. C. van Oorschot and M. J. Wiener. A Known-Plaintext Attack on Two-Key Triple Encryption. In *Advances in Cryptology – EUROCRYPT 1990*, volume 473 of *LNCS*, pages 318–325. Springer, 1991.

[108] S. Vaudenay. Security Flaws Induced by CBC Padding – Applications to SSL, IPSEC, WTLS, ... In *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 534–545. Springer, 2002.

[109] P. Švenda, M. Nemec, P. Sekan, R. Kvašňovskỳ, D. Formánek, D. Komárek, and V. Matyáš. The Million-Key Question – Investigating the Origins of RSA Public Keys. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 893–910. USENIX Association, 2016. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_svenda.pdf.

[110] C. Zalka. Grover's quantum searching algorithm is optimal. *Physical Review A*, 60:2746–2751, 1999.