Wolfgang Killmann
T-Systems debis Systemhaus Information Security Services, Bonn

Priv.-Doz. Dr. Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

Ein Vorschlag zu:

Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren[1]

Version 3.1
25.09.2001

Inhaltsverzeichnis

[1] Die Autoren bedanken sich für zahlreiche Anmerkungen, Anregungen und Hinweise, die in die Erstellung des vorliegenden Dokuments eingeflossen sind.

A. Motivation, Zielsetzung und inhaltliche Übersicht

A.1 Motivation und Zielsetzung: Zufallszahlen spielen in vielen kryptographischen Anwendungen eine wichtige Rolle. Dennoch geben ITSEC und CC keine einheitlichen Evaluationskriterien für Zufallszahlengeneratoren vor. Dieses Dokument beschreibt Evaluationskriterien für physikalische Zufallszahlengeneratoren. Das vorliegende Papier ist ein Pendant zur mathematisch-technischen Grundlage der [AIS20].

A.2 Inhaltliche Übersicht: In Kapitel B wird der Untersuchungsgegenstand beschrieben. In Kapitel C werden zwei Funktionalitätsklassen (P1, P2) eingeführt. Diese Einteilung wird begründet. Kapitel D beschreibt Aufgaben des Evaluators, soweit sie für die Untersuchung der TRNG spezifisch sind, ohne Anspruch auf vollständige Wiedergabe der Anforderungen der ITSEC- bzw. CC-Kriterien. In Kapitel E werden die klassenspezifischen Anforderungen an mehreren Beispielen ausführlich erläutert.

A.3 Bemerkung:

(i) Die vorliegende Evaluationsmethodik ist nicht auf Zufallszahlengeneratoren anwendbar, deren Rauschquelle außerhalb des EVG liegt (z.B. zufällige Tastatureingaben des Benutzers).

(ii) Verwendet der Antragsteller ein physikalischer Zufallszahlengenerator, der weder der Funktionalitätsklasse P1 noch P2 zugeordnet werden kann und wird ein Deutsches IT-Sicherheitszertifikat angestrebt, ist eine Abstimmung mit dem BSI erforderlich.

B. Definitionen und Notation

B.1 Definitionen: Ein *physikalischer Zufallszahlengenerator* (abgekürzt TRNG für true random number generator) erzeugt aus den Rauschsignalen einer internen physikalischen Rauschquelle Zufallszahlen. Die Werte, die sich unmittelbar aus der Digitalisierung analoger Rauschsignale ergeben, werden im folgenden als *digitalisierte Rauschsignale* bezeichnet. Als *interne Zufallszahlen* werden die Werte nach der mathematischen Nachbearbeitung (optional; siehe auch C.2) der digitalisierten Rauschsignalfolge bezeichnet. Ein *idealer Zufallszahlengenerator* (Fiktion!) erzeugt unabhängige Zufallszahlen, die alle möglichen Werte mit derselben Wahrscheinlichkeit annehmen. Unter *Onlinetests* verstehen wir im folgenden statistische Tests, oder genauer gesagt, eine Testvorschrift, die während des Wirkbetriebs auf die vom TRNG erzeugte digitalisierte Rauschsignalfolge oder auf interne Zufallszahlen angewandt wird, um das ordnungsgemäße Funktionieren des TRNG zu verifizieren. Eine durch einen Onlinetest festgestellte statistische Auffälligkeit führt zu einem *Rauschalarm*, der wiederum zu

einer zumindest vorübergehenden Stillegung des TRNG führt. Wir sprechen von einem *Totalausfall (der Rauschquelle)*, falls die digitalisierte Rauschsignalfolge von diesem Zeitpunkt an konstant ist. Je nach Zusammenhang verstehen wir unter der *Entropie pro Bit* den Quotienten (Entropie pro digitalisiertes Rauschsignal / Breite der Binärdarstellung eines digitalisierten Rauschsignals) bzw. (Entropie pro interne Zufallszahl / Anzahl der Bits in der Binärdarstellung einer internen Zufallszahl).

C. Funktionalitätsklassen

C.0 Motivation zur Einführung von Funktionalitätsklassen: Ein TRNG enthält eine interne physikalische Rauschquelle. Sie liefert meist ein analoges Signal, das für die weitere Verarbeitung digitalisiertisiert wird. Das digitalisierte Rauschsignal kann durch eine Nachbereitung zur internen Zufallszahlenfolge verarbeitet werden, um auf diese Weise die Wahrscheinlichkeitsverteilung der digitalisierten Rauschsignalfolge zu verbessern. Für gute physikalische Rauschquellen kann die Nachbereitung entfallen und das digitalisierte Rauschsignal direkt an den Ausgabeblock übermittelt werden. In diesem Fall entspricht die Folge der internen Zufallszahlen der digitalisierten Rauschsignalfolge. Der Ausgabeblock synchronisiert die kontinuierliche oder aperiodische Erzeugung der internen Zufallsfolge mit dem Abrufen der (externen) Zufallszahlenfolge. Die Rauschquelle liefert die Entropie der ausgegebenen Zufallszahlenfolge, die sich mit jeder erzeugten Zufallszahl erhöht.

Es ist zu klären, ob, oder besser gesagt, in welchem Maß sich ein physikalischer Zufallszahlengenerator wie ein idealer Zufallszahlengenerator verhält. Im Gegensatz zu [AIS20] können jedoch kaum theoretische Beweise geführt werden. Die Bewertung eines physikalischen Zufallszahlengenerators basiert stattdessen im wesentlichen auf statistischen Tests. Aufgrund unterschiedlicher potentieller Angriffsszenarien können verschiedene Anwendungen unterschiedliche Anforderungen an die Eigenschaften der externen, und damit natürlich auch der internen Zufallszahlen stellen. Um diesem Umstand Rechnung zu tragen, werden im folgenden zwei Funktionalitätsklassen (P1, P2) eingeführt. In Bezug auf die avisierten Anwendungen entsprechen die Klassen P1 bzw. P2 im wesentlichen den Klassen K1 und K2 bzw. K3 und K4 aus [AIS20].

Grob gesprochen, verlangt die P1-Eigenschaft eine statistische Unauffälligkeit der internen Zufallszahlen. Die P2-spezifischen Anforderungen sollen deren praktische Unbestimmbarkeit auch dann sicherstellen, falls Vorgänger oder Nachfolger bekannt sind. Abhängig vom maximalen Angriffspotential (hier angegeben in der Mechanismenstärke), das einem potentiellen Angreifer zugebilligt wird, muss der EVG einen Totalausfall bzw. Störungen der Rauschquelle selbst erkennen und gegebenenfalls resistent gegen gezielte Manipulationsversuche sein.

In Kapitel E werden verschiedene Beispiele diskutiert.

C.1 Vom Antragsteller ist mindestens anzugeben:

(i) Die angestrebte Funktionalitätsklasse (P1, P2) mit der Stärke der Mechanismen (ITSEC) bzw. der Funktionen (CC).

(iia) Ab ITSEC E2 sind im Feinentwurf bzw. ab CC EAL 4 im Entwurf auf niedriger Ebene gemäß ADV_LLD.1 Informationen über den Aufbau und die Funktionsweise des TRNG bzw. mit der für die Evaluationsstufe geforderten Spezifikationsform und Spezifikationstiefe zu liefern. Für ITSEC E1 ist eine Darlegung des Aufbaus und der Funktionsweise des TRNG vom Antragsteller im Rahmen des Nachweises für die Stärke des Mechanismus gemäß [JIL], Abschnitt 6.5, zu erbringen.

(iib) Ab ITSEC E3 muss unter Implementierung bzw. CC EAL5 unter ATE_DPT.2 Testen: Entwurf auf niedriger Ebene der Antragsteller Nachweise zu den statistischen Tests gemäß der angestrebten Funktionalitätsklasse zu liefern.

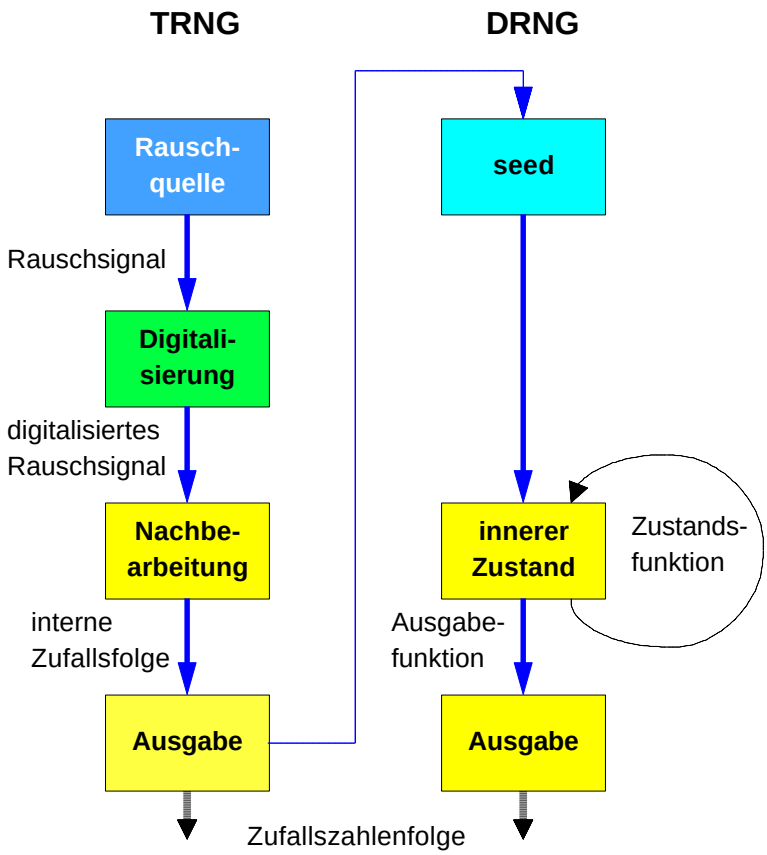
(iii) Eine nachvollziehbare Beschreibung, wie das Rauschsignal generiert wird samt einer Begründung, weshalb auf diese Weise ein zufälliges digitalisiertes Rauschsignal induziert werden soll.

+ zusätzliche Angaben, die im Unterpunkt f) der entsprechenden Funktionalitätsklasse spezifiziert sind.

C.2 Abgrenzung des Untersuchungsgegenstands TRNG:

Ein deterministischer Zufallszahlengenerator (DRNG) erhält von außen einen seed vorgegeben und berechnet mit der Zustandsfunktion daraus eine Folge innerer Zustände. Ein mit der Ausgabefunktion erzeugtes Abbild dieser Folge wird als Zufallszahlenfolge ausgegeben. Die gesamte Entropie der Ausgabefolge liegt im Startwert. Die Gesamtentropie einer von einem TRNG erzeugten Folge interner Zufallszahlen erhöht sich hingegen mit jeder Zufallszahl. TRNG beruhen auf physikalischen Zufallsprozessen, deren beobachtete analoge Größen für die digitale Verarbeitung aufbereitet werden. Prozesse, die in all ihren Parametern (Zeit, Pegel usw.) digitalisiert, d. h. auf eine endliche Anzahl der Zustände begrenzt sind, werden im allgemeinen ein deterministisches Verhalten besitzen und den DRNG zuzuordnen sein.

Das nachfolgende Schaubild visualisiert die wesentlichen Teile von TRNGs und DRNGs sowie die Seedgenerierung für DRNGs als eine mögliche Anwendung für TRNGs. Es stellt die typische sequentielle Bearbeitung der Signale dar. Netzstrukturen, etwa eine Vermischung verschiedener analoger Rauschquellen und bereits digitalisierter nachbereiteter Signale, sind grundsätzlich möglich, verkomplizieren und erhöhen aber den Analyseaufwand (z. B. Dekomposition). Eine mathematische Nachbearbeitung der digitalisierten Rauschsignale ist optional. Fehlt sie, stimmen die digitalisierten Rauschsignale mit den internen Zufallszahlen überein.



Ein EVG kann einen Zufallszahlengenerator als Kombination aus einem TRNG zur Erzeugung des seed und einem DRNG zur Erzeugung der Zufallszahlenfolge enthalten. Die Analyse des TRNG dient in einem solchen Fall dazu, die in [AIS20], C.1(iv) vom Antragsteller geforderte Begründung zu untermauern, dass die Seedgenerierung tatsächlich die Verteilung p_A induziert. Der DRNG ist gemäß [AIS20] zu evaluieren.

C.3 Allgemeine Anmerkung zur Spezifikation der Funktionalitätsklassen:

Unterpunkt d) beschreibt die klassenspezifischen Anforderungen. Die neben C.1 (i)—(iii) für eine Evaluation erforderlichen Angaben sind in Unterpunkt f) zusammengestellt. Die übrigen Unterpunkte erhellen und begründen Auswahl und Zielsetzung dieser Anforderungen. Die Unterpunkte i) und j) (siehe Kapitel D) beschreiben und erläutern die Aufgaben des Evaluators.

Klasse P1

P1.a) qualitativ-intuitive Beschreibung der P1-spezifischen Anforderungen:

Eine aus internen Zufallszahlen $r_1,r_2,\ldots$ gebildete Folge von Zufallsvektoren ist mit hoher Wahrscheinlichkeit paarweise verschieden. Interne Zufallszahlenfolgen $r_1,r_2,\ldots$ und deren Projektionen auf einzelne Bits passieren bestimmte statistische Tests (Evaluationstests). Ab Stärke der Mechanismen bzw. Funktionen "mittel" soll ein Totalausfall der Rauschquelle beim Einschalten des TRNGs und während des laufenden Betriebs entdeckt werden. Die statistischen Eigenschaften der internen Zufallszahlen werden im laufenden Betrieb getestet („Onlinetests“). Ab Stärke der Mechanismen bzw. Funktionen „hoch“ sollen die statistischen Eigenschaften der internen Zufallszahlen nicht durch äußere Bedingungen (Temperatur, Klima, Alterung) beeinflusst werden.

P1.b) denkbare Anwendungen:

--- Challenge-Response-Protokolle

--- offen übertragene, nichtkonstante Initialisierungsvektoren

--- Seedgenerierung für DRNGs der Klassen K1 und K2 ([AIS20])

P1.c) Zielsetzung:

Die internen Zufallszahlen sollen sich statistisch unauffällig verhalten. Damit sollen Replay- und Korrelationsattacken gegen kryptographische Algorithmen und Protokolle ausgeschlossen werden, die auf statistischen Schwächen der verwendeten externen Zufallszahlen basieren.

P1.d) Anforderungen an P1-TRNGs:

P1.d)(i) Aus internen Zufallszahlenfolgen gebildete Zufallsvektoren passieren den Disjunktheitstest T0. Testdurchführung und Auswertungsregel sind in P1.i)(i) spezifiziert.

P1.d)(ii) Als Binärstring aufgefasst, passieren interne Zufallszahlenfolgen $r_1,r_2,\ldots$ und deren Projektionen auf einzelne Bits bestimmte statistische Tests. Die Auswertungsregeln sind in Unterpunkt P1.i)(ii) spezifiziert.

P1.d)(iii) (ab Stärke der Mechanismen bzw. Funktionen mittel) Liegt beim Einschalten des TRNGs ein Totalausfall der Rauschquelle vor, muss dieser sofort erkannt werden, d.h. es dürfen keine externen Zufallszahlen ausgegeben werden.

P1.d)(iv) (ab Stärke der Mechanismen bzw. Funktionen mittel) Tritt während des Betriebs des TRNGs ein Totalausfall der Rauschquelle auf, so ist die Ausgabe von Zufallswerten zu verhindern, deren interne Zufallsfolge vollständig nach dem Totalausfall erzeugt wurde. Ersatzweise genügt es, dass sich der TRNG nach dem Totalausfall der Rauschquelle für jede konstante Rauschsignalfolge wie ein K2-DRNG im Sinne von [AIS20] verhält, dessen Ausgabefolge den vorgesehenen Einsatzzweck erfüllt.

P1.d)(v) (ab Stärke der Mechanismen bzw. Funktionen hoch) Es müssen die in (i) und (ii) geforderten Eigenschaften unter den vorgesehenen äußeren Einsatzbedingungen (Temperatur, Stromversorgung usw.) verifiziert werden, soweit diese die Funktion der Rauschquelle beeinflussen können.

P1.d)(vi) (ab Stärke der Mechanismen bzw. Funktionen mittel) Zum Betrieb des TRNG muss ein Onlinetest implementiert sein, der auf externen Aufruf die Qualität der internen Zufallszahlen überprüft. Eine externe Aufrufbarkeit des Onlinetests ist nicht erforderlich, falls durch Veranlassung des EVG alle erzeugten internen Zufallszahlen mit diesem Onlinetest getestet werden, oder der Onlinetest wenigstens in regelmäßigen Abständen angewandt wird. Für einen idealen Zufallszahlengenerator müsste die Wahrscheinlichkeit, dass innerhalb eines Jahres mindestens ein Rauschalarm auftritt, bei einer typischen Nutzung des TRNG $\geq 10^{-6}$ betragen. Ersatzweise ist es zulässig, dass der Onlinetest anstelle der internen Zufallszahlen die digitalisierte Rauschsignalfolge testet. In diesem Fall muss aber sichergestellt sein, dass die mathematische Nachbearbeitung die durchschnittliche Entropie pro Bit nicht reduziert. (Tatsächlich wird dies der Normalfall sein, falls die Klasse P2 angestrebt wird, da dort gefordert wird, dass die Onlinetests die digitalisierten Rauschsignalfolge testen.)

Bemerkung 1: Der Tot-Test nach P1d)(iv) bzw. der Onlinetest nach P1.d)(vi) sind im Regelfall als Bestandteil des EVG implementiert oder können im begründeten Ausnahmefall als externe Sicherheitsmaßnahmen implementiert werden.

P1.e) Begründung:

Die externen Zufallszahlen sollen die kryptographischen Mechanismen, in denen sie eingesetzt werden, resistent gegen Replay- und Korrelationsattacken machen. Ihre Bestimmbarkeit bzw. Erratbarkeit, gegebenenfalls bei Kenntnis externer Zufallszahlenteilfolgen, spielt bei P1-TRNGs keine Rolle. Um die Zielsetzung zu garantieren, sollten sich die externen Zufallszahlen statistisch unauffällig verhalten, d.h. ähnliche statistische Eigenschaften aufweisen, als ob sie von einem idealen Zufallszahlengenerator erzeugt worden wären. Da die externen Zufallszahlen in aller Regel durch Konkatenation interner Zufallszahlen gebildet werden, wird für P1-TRNGs verlangt, dass die internen Zufallszahlen sich statistisch unauffällig verhalten. Die internen Zufallszahlen werden verschiedenen statistischen Tests unterworfen (siehe P1.d) Absätze (i), (ii), (v), (vi)).

Zu P1.d)(i): Das „Disjunktheitskriterium“ P1.d)(i) ist ein einfacher Test, die Eignung des TRNG, paarweise verschiedene externe Zufallszahlen zu erzeugen (→ Challenge-Response-Protokolle), für ungeeignete TRNGs zu widerlegen. Da er selbst nicht sehr scharf ist, prüfen weitere statistische Tests P1.d)(ii) diese Eigenschaft.

Zu P1.d)(ii): Obwohl nicht allzu scharf, sollten die statistischen Tests stark genug sein, um die bekannten Attacken gegen die kryptographischen Algorithmen auszuschließen, die auf statistischen Schwächen der externen Zufallszahlen basieren. Mit der Projektion der internen Zufallszahlen auf die einzelnen Komponenten werden die einzelnen Zufallszahlenbits auf „Gleichartigkeit“ getestet (vgl. [AIS20], K1.e) und Beispiel E.2).

Zu P1.d)(iii): Nach einem Totalausfall der Rauschquelle nimmt das digitalisierte Rauschsignal, also der Input der mathematischen Nachbearbeitung, einen konstanten Wert an. Insbesondere bedeutet dies, dass nach einem Totalausfall der Rauschquelle bei jedem Neustart des TRNG dieselbe Folge interner Zufallszahlen generiert wird, insofern etwaige, zur mathematischen Nachbearbeitung gehörende Register bei jedem Neustart wohldefinierte Werte annehmen.

Zu P1.d)(iv): Ein Totalausfall der Rauschquelle setzt die digitalisierte Rauschsignalfolge konstant. Insofern vorhanden, kann sich die mathematische Nachbearbeitung nach einem Totalausfall der Rauschquelle wie ein DRNG im Sinne von [AIS20] verhalten. Nach Auftreten des Totalausfalls ist der Inhalt etwaiger Register als seed und der nunmehr konstante Input als Teil der Vorschrift zur Erneuerung des inneren Zustands des DRNG zu interpretieren. Gehört dieser DRNG für jede konstante digitalisierte Rauschsignalfolge wenigstens der Klasse K2 aus [AIS20] an, können auch die nach dem Totalausfall der Rauschquelle erzeugten externen Zufallszahlen dem vorgesehenen Einsatzzweck genügen.

Zu P1.d)(v): Die Funktion physikalischer Rauschquellen kann von den äußeren Einsatzbedingungen (die in den Sicherheitsvorgaben und der Betriebsdokumentation beschrieben sind) abhängen oder über äußere Schnittstellen des EVG (die im Architekturentwurf beschrieben sind) beeinflussbar sein. In diesem Fall muss die ordnungsgemäße Funktion des TRNG unter den verschiedenen Einsatzbedingungen nachgewiesen werden. Hiermit sollen auch gezielte äußere Angriffe gegen die Rauschquelle ausgeschlossen werden, die auf eine Verschlechterung der Qualität der erzeugten internen Zufallszahlen abzielen.

Zu P1.d)(vi): Auch bei einem idealen Zufallsgenerator würde gelegentlich ein Rauschalarm auftreten. Ist diese Wahrscheinlichkeit zu groß, führte dies zu vielen (unberechtigten!) Stilllegungen des idealen Zufallszahlengenerators. Abhängig vom „Defekt“,

d.h. dem "Abstand" zu einem idealen Zufallszahlengenerator (genauer: der Abweichung der Verteilung der internen Zufallszahlen von unabhängigen und gleichverteilten Zufallsvariablen), wird diese Wahrscheinlichkeit für einen realen TRNG in aller Regel größer sein. Ist die Rauschalarmwahrscheinlichkeit für den idealen Zufallszahlengenerator indes extrem klein, werden auch TRNGs, die interne Zufallszahlen mit relativ starken statistischen Defekten (z.B. Ungleichverteilung oder starke Abhängigkeiten der internen Zufallszahlen) erzeugen, durch die Onlinetests mit hoher Wahrscheinlichkeit nicht erkannt. Daher wird in P1.d)(vi) eine Mindestwahrscheinlichkeit für einen Rauschalarm einer idealen Rauschquelle vorgeschrieben. Trivialerweise wächst diese Wahrscheinlichkeit mit der Anzahl der durchgeführten Onlinetests. Ungeeignete mathematische Nachbearbeitungen, d.h. solche, die die durchschnittliche Entropie pro Bit reduzieren, können gute digitalisierte Rauschsignale in schwache interne Zufallszahlen überführen. Werden die Onlinetests auf die digitalisierten Rauschsignale angewandt, ist daher der Nachweis zu führen, dass die mathematische Nachbearbeitung die durchschnittliche Entropie pro Bit nicht reduziert. Tatsächlich wird dies der Normalfall sein, falls die Klasse P2 angestrebt wird, da in P2.d)(xi) verlangt wird, dass die Onlinetests auf die digitalisierten Rauschsignalfolge angewandt werden. Dass die mathematische Nachbearbeitung die durchschnittliche Entropie pro Bit nicht reduziert, muss ohnehin nachgewiesen werden (P2.d)(viii)).

P1.f) vom Antragsteller neben C.1(i)-(iii) anzugeben:

P1.f)(iv) (erforderlich ab Stärke der Mechanismen bzw. Funktionen mittel): Begründung, dass P1.d)(iii) erfüllt ist.

P1.f)(v) (erforderlich ab Stärke der Mechanismen bzw. Funktionen mittel): Begründung, dass ein Totalausfall der Rauschquelle während des Betriebs des TRNGs hinreichend schnell entdeckt wird (siehe P1.d)(iv)). Falls dies nicht sichergestellt ist, ist eine DRNG-Evaluation der mathematischen Nachbearbeitung erforderlich. Der Antragsteller muss insbesondere Parameter M,c und ε angeben, für die der mathematischen Nachbearbeitung die K1-spezifische Eigenschaft zugebilligt werden soll. Die Wahl der Parameter ist im Hinblick auf die avisierten Anwendungen des TRNGs zu begründen.

P1.f)(vi) (erforderlich ab Stärke der Mechanismen bzw. Funktionen mittel): Begründung, dass P1.d)(vi) erfüllt ist. Ferner sind die Konsequenzen eines Rauschalarms zu beschreiben (Stilllegung der Rauschquelle, intensive Tests der Rauschquelle, Protokollierung etc.). Wird die Rauschquelle nach einem Rauschalarm erneut in Betrieb genommen, muss sichergestellt sein, dass die internen Zufallszahlen keine nichttolerierbaren statistischen Schwächen aufweisen.

Bemerkung 2: Die Verpflichtung des Antragstellers zum Nachweis, dass die Anforderungen P1.d)(i), P1.d)(ii) und P.1d)(v) bei Testdurchführungen durch den Antragsteller erfüllt worden sind, und die Bereitstellung der Testergebnisse ergibt sich bereits aus C.1(iib). Wenn die Tot-Tests nach P1d)(iii) und (iv) bzw. der Onlinetest nach P1.d)(vi) als externe Sicherheitsmaßnahmen implementiert werden sollen, so muss der Antragsteller dafür eine Spezifikation und Referenzimplementierung vorlegen. Nachweise gemäß P1.f)(iv) – (vi) können an der Referenzimplementierung geführt werden.

P1.g) Erläuterungen: Ein Mechanismus zur Erkennung eines Totalausfalls der physikalischen Rauschquelle wird im folgenden als *Tot-Test* bezeichnet. Dies kann ein geeigneter statistischer Test der digitalisierten Rauschfolge oder der internen Zufallszahlen sein. Denkbar ist aber auch eine Verifikation, ob die digitalisierte Rauschsignalfolge konstant ist oder ob sich die ersten n Bits, n>15, nach Aktivierung des TRNG im laufenden Betrieb wiederholen (s. Continuous random number generator test, [FI140-1], Abschnitt 4.11.2). Der Parameter n sollte so groß gewählt werden, dass im „Lebenszyklus“ des TRNG ein durch den Tot-Test ausgelöster Rauschalarm vermutlich nie auftritt, insofern nicht tatsächlich ein Totalausfall der Rauschquelle vorliegt.

P1.h) Beispiele: Totalausfall der Rauschquelle / Tot-Test: E.1, E.5, E.6, E.7;

Anlauftest: E.5, E.7;

Onlinetest: E.6, E.7.

Klasse P2

P2.a) qualitativ-intuitive Beschreibung der P2-spezifischen Anforderungen:

Die digitalisierte Rauschsignalfolge verhält sich statistisch unauffällig. Ab Stärke der Mechanismen bzw. Funktionen „mittel“ wird die Funktionalität der physikalischen Rauschquelle beim Einschalten des TRNGs getestet. Ein Totalausfall der physikalischen Rauschquelle beim Einschalten oder während des laufenden Betriebs wird entdeckt. Der TRNG testet die statistischen Eigenschaften der digitalisierten Rauschsignale im laufenden Betrieb zumindest nach externem Aufruf („Onlinetests“). Ab Stärke der Mechanismen bzw. Funktionen „hoch“ muss der EVG die Durchführung der Onlinetests eigenständig veranlassen.

P2.b) denkbare Anwendungen:

--- Erzeugung von Signaturschlüsselpaaren

--- Erzeugung von DSS-Signaturen (privater Schlüssel x oder Zufallszahl k; siehe [FI186])

--- Erzeugung von Spruchschlüsseln für symmetrische Verschlüsselungsverfahren

--- zufällige Paddingbits

--- zero-knowledge-proofs

--- Erzeugen von seeds für DRNG der Klassen K3 und K4

P2.c) Zielsetzung:

Neben der P1-spezifischen Zielsetzung P1.c) soll die Erfolgschance des gezielten Ratens externer Zufallszahlen (realisiert durch gezielte Exhaustionsattacken) auch bei Kenntnis externer Zufallszahlenteilfolgen bestenfalls vernachlässigbar höher sein als dies der Fall wäre, falls die externen Zufallszahlen von einem idealen Zufallszahlengenerator erzeugt worden wären.

2.d) Anforderungen an P2-TRNGs:

Der TRNG gehört der Klasse P1 mit mindestens derselben Stärke der Mechanismen bzw. Funktionen an (Abwärtskompatibilität).

P2.d)(vii) Digitalisierte Rauschsignalfolgen erfüllen bestimmte Kriterien bzw. passieren statistische Tests, die unter anderem Mehrschritt-Abhängigkeiten ausschließen sollen. Ferner wird der Entropietest T8 passiert. Tests und Auswertungsregeln sind in Unterpunkt P2.i) spezifiziert.

Unter bestimmten Voraussetzungen können anstelle der unter P2.i) spezifizierten Kriterien bzw. statistische Tests Ersatzkriterien angewandt werden (vgl. „Ersatzkriterien für P2.d)(vii); Typ 1“ und „Ersatzkriterien für P2.d); Typ 2“).

P2.d)(viii) Insofern vorhanden, darf die mathematische Nachbearbeitung die durchschnittliche Entropie pro Bit nicht vermindern.

P2.d)(ix) (Ab Stärke der Mechanismen bzw. Funktionen mittel) Bei jedem Start des TRNG müssen statistische Mindesteigenschaften der digitalisierten Rauschsignalfolge nachgewiesen werden. Bevor die statistischen Tests nicht beendet sind, dürfen keine Zufallszahlen ausgegeben werden.

P2.d)(x) (ab Stärke der Mechanismen bzw. Funktionen mittel) Tritt während des Betriebs des TRNGs ein Totalausfall der Rauschquelle auf, so ist die Ausgabe von Zufallswerten zu verhindern, deren zugehörige interne Zufallsfolge vollständig nach dem Totalausfall erzeugt wurde.

P2.d)(xi) (ab Stärke der Mechanismen bzw. Funktionen mittel) Zum Betrieb des TRNG muss ein Onlinetest implementiert sein, mit dem die statistische Qualität der digitalisierten Rauschsignalfolge überprüft werden kann. Dieser Onlinetest muss von extern aufrufbar sein, oder der TRNG muss den

Onlinetest selbständig aufrufen. Letzteres muss ständig oder zumindest in regelmäßigen Abständen geschehen. Der Onlinetest selbst und das Aufrufschema müssen geeignet sein, nicht akzeptable statistische Defekte oder Verschlechterungen der statistischen Eigenschaften der digitalisierten Rauschsignalfolge in angemessener Zeit zu erkennen. Für einen idealen Zufallszahlengenerator müsste die Wahrscheinlichkeit, dass innerhalb eines Jahres mindestens ein Rauschalarm auftritt, bei einer typischen Nutzung des TRNG $\geq 10^{-6}$ betragen.

P2.d)(xii) (ab Stärke der Mechanismen bzw. Funktionen hoch) Es müssen die in P2.d)(vii) geforderten Eigenschaften unter den vorgesehenen äußeren Einsatzbedingungen (Temperatur, Stromversorgung usw.) verifiziert werden, soweit diese die Funktion der Rauschquelle beeinflussen können.

P2.d)(xiii) (ab Stärke der Mechanismen bzw. Funktionen hoch) Der TRNG muss den Onlinetest selbständig aufrufen.

Bemerkung 1: Der Tot-Test nach P1d)(iv) und P2.d)(x), der Anlauftest („Startup-Test“) nach P2.d)(ix) der Onlinetest nach P1.d)(vi), P2.d)(xi) und P2.d)(xiii) sind im Regelfall als Bestandteil des EVG implementiert oder können im begründeten Ausnahmefall als externe Sicherheitsmaßnahmen implementiert werden.

Ersatzkriterien für P2.d)(vii); Typ 1: Zielsetzung von P2.d)(vii) ist die Sicherstellung von P2.c) bei ausgewählten Prototypen durch die Verifikation einer Mindestentropieschranke pro internem Zufallsbit mit einer vernachlässigbar kleinen Irrtumswahrscheinlichkeit. Erfüllt die digitalisierte Rauschsignalfolge das Kriterium P2.d)(vii) nicht, so kann der Antragsteller ersatzweise die folgenden Nachweise vorlegen:

- Interne Zufallszahlenfolgen passieren die in P2.i)(vii) spezifizierten statistischen Tests.
- *Nachvollziehbarer* Nachweis, dass die internen Zufallszahlen die mit Kriterium P2.d)(vii) verfolgte Zielsetzung erfüllen. Der Nachweis ist unter Berücksichtigung der mathematischen Nachbearbeitung und auf Grundlage der empirischen Eigenschaften der digitalisierten Rauschsignalfolge zu führen.

Dem TRNG wird dann zugebilligt, dass er ein zu P2.d)(vii) gleichwertiges Ersatzkriterium erfüllt. Der im zweiten Spiegelpunkt angesprochene "nachvollziehbare Nachweis" kann auf statistischen Tests der interne Zufallszahlen basieren, insofern deren Eignung begründet wird.

Ersatzkriterien für P2.d)(vii); Typ 2 : Zielsetzung von P2.d)(vii) ist die Sicherstellung von P2.c) bei ausgewählten Prototypen durch die Verifikation einer Mindestentropieschranke pro internem Zufallsbit mit einer vernachlässigbar kleinen Irrtumswahrscheinlichkeit. Sind die zum Nachweis der Eigenschaft P2.d)(vii) erforderlichen sta-

tistischen Tests (siehe P2.i)(vii)) an der Rauschsignalfolge nicht möglich, so kann der Antragsteller ersatzweise die folgenden Nachweise vorlegen:

- Interne Zufallszahlenfolgen passieren die in P2.i)(vii) spezifizierten statistischen Tests.
- *Nachvollziehbare und plausible Beschreibung* eines mathematischen Modells der physikalischen Rauschquelle und der daraus abgeleiteten statistischen Eigenschaften der digitalisierten Rauschsignalfolge
- Angabe statistischer Tests, die die mit Kriterium P2.d)(vii) verfolgte Zielsetzung gewährleisten, insofern die internen Zufallszahlen diese Tests passieren. Die Eignung dieser Tests ist *nachvollziehbar* zu begründen. Der Nachweis ist unter Berücksichtigung der mathematischen Nachbearbeitung und auf Grundlage der vom mathematischen Modell der Rauschquelle abgeleiteten statistischen Eigenschaften der Rauschsignalfolge zu führen.

Dem TRNG wird dann zugebilligt, dass er ein zu P2.d)(vii) gleichwertiges Ersatzkriterium erfüllt. Ein Ersatznachweis von Kriterium P2.d)(vii) gemäß „Ersatzkriterien für P2.d)(vii); Typ 2“ ist bedeutend schwieriger und umfangreicher als ein Ersatznachweis gemäß „Ersatzkriterien für P2.d)(vii); Typ 1“. Er wird nur in Ausnahmesituationen möglich sein.

Bemerkung 2: (zu P2.(ix) und P2.(xi)): Werden beim Start des TRNGs bzw. durch die Onlinetests anstelle der digitalisierten Rauschfolge die internen Zufallszahlen getestet, muss der Antragsteller die Wirksamkeit dieser Tests gesondert begründen.

P2.e) Begründung:

Die P2-spezifische Zielsetzung wird sichergestellt falls der durchschnittliche Entropiezuwachs pro interner Zufallszahl — und damit auch der durchschnittliche Entropiezuwachs pro externer Zufallszahl — nahe bei den Werten idealer Zufallszahlengeneratoren liegen.

Zu P2.d)(vii) Die eindimensionale Verteilung der digitalisierten Rauschsignalfolge soll nicht zu sehr von der Gleichverteilung abweichen. Unterschiede der 1-Schritt-Übergangswahrscheinlichkeiten bei verschiedenen Vorgängern werden bis zu einem gewissen Grad toleriert. Die digitalisierte Rauschsignalfolge soll aber keine Mehrschritt-Abhängigkeiten aufweisen. Die Entropie der digitalisierten Rauschsignalfolge ist ein Maß für den aus der Rauschquelle gewonnenen Zufall. Der durchschnittliche Entropiezuwachs pro digitalisiertem Rauschsignal soll daher eine Mindestschranke nicht unterschreiten. Die Entropie einer Zufallszahlenfolge kann empirisch jedoch nur unter gewissen Modellannahmen über die zugrundeliegende Wahrscheinlichkeitsverteilung (unabhängig, markoffsch, endliches Gedächtnis o.ä.) zuverlässig geschätzt werden.

Tatsächlich ist der Erwartungswert der Testgröße T8 gleich der Entropie pro L-Bit-Block, , falls die zu testende Bitfolge von einer unabhängigen, stationären binärwertigen Rauschquelle erzeugt wird (siehe Kapitel F, Test T8). Die Anforderungen an die empirische Verteilung in P2.i)(vii) sollen deshalb u.a. auch die Zuverlässigkeit der Entropieschätzung sicherstellen. (Die in P2.i)(vii.b)-P2.i)(vii.d) definierten Tests tolerieren nur geringe 1-Schritt- und vernachlässigbare 2- und 3-Schritt-Übergangswahrscheinlichkeiten.) Betrachtet man nicht allzu lange Zeiträume, sollte eine Stationaritätsannahme der Rauschquelle realistisch sein. Ein Passieren der in P2.i)(vii) spezifizierten statistischen Tests lässt darauf schließen (kein mathematischer Beweis!), dass die digitalisierte Rauschsignalfolge ein hohes Maß an Entropie besitzt.

Die digitalisierte Rauschsignalfolge dürfte im allgemeinen schief (d.h. ungleichverteilt) sein und gegebenfalls 1- oder gar Mehrschritt-Abhängigkeiten aufweisen, sicherlich aber keine komplizierteren algebraischen Abhängigkeiten. Die Nachbereitung soll diese Schwächen der digitalisierten Rauschsignalfolge mildern und negative Auswirkungen auf die Ausgabewerte verhindern. Jedoch werden durch manche mathematische Nachbearbeitung Schwächen der digitalisierten Rauschsignalfolge nicht reduziert, sondern lediglich verwischt oder in andere Schwächen transformiert, was die Anwendung gebräuchlicher statistischer Tests auf die internen Zufallszahlen häufig unwirksam macht (vgl. Beispiel E.1). Deshalb sollten die P2-spezifischen Tests - wenn immer möglich - auf die digitalisierte Rauschsignalfolge angewandt werden. Wenn die Tests auf die interne Zufallsfolge angewandt werden, so müssen deren Anwendbarkeit und Wirksamkeit begründet werden (vgl. Bemerkung 2).

Zu P2.d)(viii): Die mathematische Nachbearbeitung soll die Entropie der digitalisierten Rauschsignalfolge keinesfalls mindern.

Zu P2.d)(ix): Hierdurch sollen gravierende Schwächen der digitalisierten Rauschsignalfolge erkannt werden, bevor Zufallszahlen ausgegeben werden. Insbesondere wird damit die Anforderung P1.d)(iii) abgedeckt.

Zu P2.d)(xi) und P2.d)(xii): Zur Begründung einer Mindestwahrscheinlichkeit eines Rauschalarms bei einer idealen Rauschquelle vgl. die Begründung zu P1.d(v). Aufgrund von Bauteiltoleranzen ist es möglich, dass Rauschquellen desselben Typs digitalisierte Rauschsignalfolgen mit unterschiedlichen statistischen Eigenschaften erzeugen. Außerdem können sich die Eigenschaften der Bauteile im Lauf der Zeit ändern (Alterungseffekte). Die Aufgabe des Onlinetests ist es, beide Phänomene zu erkennen. Abweichungen der digitalisierten Rauschsignalfolgen von Gleichverteilung und Unabhängigkeit (→ idealer Zufallszahlengenerator) sind unvermeidbar, bis zu einem gewissen Maß aber auch tolerierbar. Bei nichttolerierbaren Abweichungen soll der Onlinetest möglichst rasch einen Rauschalarm liefern. Da jeder Rauschalarm zu einer zumindest vorübergehenden Stilllegung des TRNG führt, sollte der Onlinetest andererseits

bei tolerierbaren Abweichungen keine all zu hohe Wahrscheinlichkeit für einen Rauschalarm aufweisen.

P2.f) vom Antragsteller neben C.1(i)-(iii) und P1.f)(iv)-(vi) anzugeben:

Aus C1.(iib) ergibt sich ab Evaluationsstufe E2 für den Antragsteller die Verpflichtung, Nachweis über die Durchführung der in P2.i)(vii) beschriebenen statistischen Tests zu führen und die Testergebnisse bereitzustellen. Erfüllt die digitalisierte Rauschsignalfolge das Kriterium P2.d)(vii) nicht oder kann die digitalisierte Rauschsignalfolge nicht getestet werden, muss der Antragssteller Ersatzmechanismen angeben und deren Wirksamkeit zu begründen. (vgl. P2.d), „Ersatzkriterien für P2.d)(vii); Typ 1“ und „Ersatzkriterien für P2.d)(vii); Typ 2“).

P2.f)(vii) Begründung, dass P2.d)(viii) erfüllt ist.

P2.f)(viii) Begründung, dass P2.d)(ix) erfüllt ist.

P2.f)(ix) Nachweis, dass P2.d)(x) erfüllt ist.

P2.f)(x) Nachweis und Begründung, dass P2.d)(xi) erfüllt ist (ggf. unter Beachtung von P2.d), Bemerkung 2). Es ist zumindest näherungsweise anzugeben, wie groß die Wahrscheinlichkeit für einen Rauschalarm bei bestimmten (tolerierten / nicht tolerierten) Abweichungen der digitalisierten Rauschsignalfolge vom Idealzustand (Gleichverteilung, Unabhängigkeit →idealer Zufallszahlengenerator) ist. Der Antragsteller hat anzugeben und zu begründen, welche Abweichungen er als akzeptabel ansieht. In die Begründung kann die mathematische Nachbearbeitung eingehen.

P2.f)(xi) Nachweis über Durchführung der in P2.i)(xii) spezifizierten Tests und Bereitstellung der Testergebnisse.

P2.f)(xii) Nachweis, dass P2.d)(xiii) erfüllt ist. Ferner sind die Konsequenzen eines Rauschalarms zu beschreiben (Stilllegung der Rauschquelle, intensive Tests der Rauschquelle, Protokollierung etc.). Wird die Rauschquelle nach einem Rauschalarm erneut in Betrieb genommen, muss sichergestellt sein, dass die digitalisierte Rauschsignale keine nichttolerierbaren statistischen Schwächen aufweisen.

Bemerkung 3: Die Verpflichtung des Antragstellers zum Nachweis, dass die Anforderungen P2.d)(vii) bei Testdurchführungen durch den Antragsteller erfüllt worden sind, und die Bereitstellung der Testergebnisse ergibt sich bereits aus C1.(iib). Wenn der Tot-Test nach P1d)(iv) und P2.d)(x), der Anlauftest („Startup-Test“) nach P2.d)(ix) der Onlinetest nach P1.d)(vi), P2.d)(xi) und P2.d)(xiii) als externe Sicherheitsmaßnahmen implementiert werden soll, so muss der Antragsteller dafür eine Spezifikation und Referenzimplementierung vorlegen. Nachweise gemäß P1.f)(v), P1.f)(vi), P2.f)(viii),

P2.f)(ix), P2.f)(x) und P2.f)(xii) können an einer Referenzimplementierung geführt werden.

P2.g) Erläuterungen: Eine P2-Evaluation mit Stärke der Mechanismen bzw. Funktionen niedrig ist nicht möglich.

P2.h) Beispiele: mathematische Nachbearbeitung: E.1, E.2, E.3;

Ersatzkriterien für P2.d)(vii); Typ 1 und Typ 2: E.4

Anlauftest: E.7;

Tot-Test: E.5, E.6, E.7;

Onlinetest: E.2, E.7.

D. Evaluationsmethodologie

Kapitel D beschreibt, wie der Evaluator die spezifischen Eigenschaften der jeweiligen Funktionalitätsklasse prüfen soll. Die Nummerierung der Unterpunkte beginnt mit i)

D.0 Zusammenhang zur Gesamtevaluation: In den Sicherheitsvorgaben spezifiziert der Hersteller die Anforderungen an die Sicherheitsfunktionalität. Wenn im Einzelfall auf dieser Ebene der Abstraktion die Spezifikation der Zufallszahlenerzeugung und -nutzung bereits sinnvoll ist, wird hier die Funktionalitätsklasse P1 bzw. P2 für den physikalischen Zufallszahlengenerator mit Bezug zur Sicherheitsfunktion des (Gesamt-)EVG angegeben. Oft ist der physikalische Zufallszahlengenerator nur ein Teil des zu evaluierenden Produkts. Die Annahmen an die Einsatzumgebung und für die sichere Nutzung des EVG sind zu benennen.

Für Common Criteria Evaluationen kann

- die Funktionsklasse FIA_SOS aus CC Teil 2 genutzt werden, wenn der ZG für die Erzeugung von Authentisierungsinformation verwendet wird, oder
- die ergänzend zum Teil 2 der CC definierte Familie FCS_RND.

FIA_SOS.2 Generierung von Geheimnissen durch TSF

Familienverhalten

Diese Familie definiert Anforderungen an Mechanismen, die definierte Qualitätsmetriken für ge-gebene Geheimnisse durchsetzen und Geheimnisse generieren, die die definierte Metrik erfüllen.

Komponentenabstufung

FIA_SOS.2 Generierung von Geheimnissen durch TSF erfordert, daß die TSF in der Lage sind, Geheimnisse zu generieren, die definierte Qualitätsmetriken erfüllen.

Management: FIA_SOS.2

Folgende Aktionen kommen für die Managementfunktionen in FMT in Betracht:

a) Management der zur Generierung der Geheimnisse benutzten Metrik.

Protokollierung: FIA_SOS.1, FIA_SOS.2

Folgende Aktionen sollen protokollierbar sein, wenn FAU_GEN Generierung der Si-cherheitspro-tokolldaten Bestandteil des PP/der ST ist:

a) Minimal: Zurückweisung jeglicher getesteter Geheimnisse durch die TSF.

b) Einfach: Zurückweisung oder Annahme jeglicher getesteter Geheimnisse durch die TSF.

c) Detailliert: Identifikation von jeglichen Änderungen an den definierten Qualitätsmetriken.

FIA_SOS.2 Generierung von Geheimnissen durch TSF

Ist hierarchisch zu: Keinen anderen Komponenten.

FIA_SOS.2.1 Die TSF müssen einen Mechanismus bereitstellen, um Geheimnisse zu generieren, die [Zuweisung: *definierte Qualitätsmetri*k] entsprechen.

FIA_SOS.2.2 Die TSF müssen in der Lage sein, den Gebrauch der TSF-generierten Geheimnisse für [Zuweisung: *Liste der TSF-Funktione*n] durchzusetzen.

Abhängigkeiten: keine.

FCS_RND Erzeugung von Zufallszahlen

Familienverhalten

Diese Familie definiert Qualitätsmetriken für die Erzeugung von Zufallszahlen, die für kryptographische Zwecke vorgesehen sind.

Komponentenabstufung

FCS_RND.1 Generierung von Zufallszahlen durch TSF erfordert, daß die Zufallszahlen die definierte Qualitätsmetriken erfüllen.

Management: FCS_RND.1

Es sind keine Managementfunktionen vorgesehen.

Protokollierung: FCS_RND.1

Es sind keine Aktionen definiert, die prokolliert werden sollen.

FCS_RND.1 Qualitätsmetrik für Zufallszahlen

Ist hierarchisch zu: Keinen anderen Komponenten.

FCS_RND.1.1 Die TSF müssen einen Mechanismus bereitstellen, um Zufallszahlen zu generieren, die [Zuweisung: *definierte Qualitätsmetri*k] entsprechen.

FCS_RND.1.2 Die TSF müssen in der Lage sein, den Gebrauch der TSF-generierten Zufallszahlen für [Zuweisung: *Liste der TSF-Funktione*n] durchzusetzen.

Abhängigkeiten: FPT_TST.1 TSF testing.

Anmerkung: FCS_RND.1 wurde zusätzlich zum CC Teil 2 definiert, um in der Verwendung der Zufallszahlen nicht auf die Klasse FIA: Identifikation und Authentisierung eingeschränkt zu sein und explizit eine Verwendung der Zufallszahlen für die Schlüsselerzeugung (FCS_CKM.1) oder in kryyptographischen Algorithmen oder Protokollen (FCS_COP.1) zu beschreiben. Die angestrebte Funktionalitätsklasse P1 bzw. P2 muß mit der Zuweisung *Liste der TSF-Funktionen* in FIA_SOS.2.2 bzw. FCS_RND.1.2 verträglich sein (vergl. mit den oben angegeben Zielsetzungen und denkbaren Anwendungen). FCS_RND.1 stellt darüberhinaus den Zusammenhang mit Einschalt- und Onlinetests des Zufallsgenerators her.

Wenn der Zufallsgenerator eine für den Benutzer sichtbare TSF-Schnittstelle besitzt bzw. als Schnittstelle eines Subsystems das TSF-Verhalten auf hoher Ebene bestimmt, so sind diese Schnittstellen in ADV_FSP bzw. ADV_HLD zu beschreiben. Im Feinentwurf bzw. im Entwurf auf niedriger Ebene liegt der Schwerpunkt auf der Beschreibung des Zufallsgenerators als Sicherheitsmechanismus, der Verwendung des Zufallsgenerators für die sicherheitsspezifischen Funktionen und dem Zusammenwirken mit anderen Sicherheitsmechanismen. Ein TRNG wird als Basiskomponente anzusehen sein, die der Forderung von ITSEC E4.8 bzw. CC ADV_LLD gerecht werden kann, klar definiert, weitgehend voneinander unabhängig aufgegliedert zu sein, um das Testen zu erleichtern und die Möglichkeiten zu einer Verletzung der Sicherheit zu minimieren. Die Beschreibung der Struktur, der Funktionsweise und der internen Schnittstellen des Zufallszahlengenerators ist im Feinentwurf bzw. im Entwurf auf niedriger Ebene enthalten. An den hier definierten internen Schnittstellen muss erkennbar sein, ob und ggf. wie das Rauschsignal, das digitalisierte Rauschsignal und die interne Zufallszahlenfolge ausgelesen werden können. Im Einzelfall, z. B. bei einer Hardware-Evaluation eines Chips für Chipkarten, kann der Onlinetest auch in der Software durch das Chipkartenbetriebssystem implementiert werden. Der Onlinetest könnte dann z. B. als Firmware Bestandteil des EVG vom Antragsteller bereitgestellt und vom Chipkartenbetriebssystem-Hersteller integriert werden.

Der Test von Sicherheitsfunktionen, die TRNG nutzen, erfordern im allgemeinen statistische Tests, die über die für alle TSF durch ATE_DPT angegebene Testtiefe hinausgehen können. Diese Nachweise sind entsprechend der angestrebten Funktionalitätsklasse für

(1) ITSEC zu den Wirksamkeitskriterien – Konstruktion, Aspekt 3 - Stärke der Mechanismen, und ab E2 zur Konstruktion - Der Entwicklungsprozeß, Phase 4 – Implementierung durch den Hersteller

(2) CC für EAL1 soweit durch die Sicherheitsvorgaben als Sicherheitsfunktion identifiziert durch Unabhängiges Testen (ATE_IND) des Evaluators und ab EAL2 für die Stärke der EVG-Sicherheitsfunktionen (AVA_SOF) und Funktionale Tests (ATE_FUN) durch den Hersteller

zu erbringen. Tests des TRNG ergeben sich außerdem als Tests der Sicherheitsfunktionen auf der Ebene des Feinentwurf (ab ITSEC E3) bzw. ATE_DPT.2 Testen: Entwurf auf niedriger Ebene (ab CC EAL5). Statistische Tests der TRNG müssen eventuelle Abhängigkeiten der Rauschquelle von den Umgebungsbedingungen und Alterungserscheinungen beachten. Je nach Rauschquelle sind deshalb statistische Tests in den zulässigen Bereichen der äußeren Schnittstellen Versorgungsspannung und Taktversorgung (z. B. Chipkarten) sowie Temperatur und Lebensalter (z. B. nach künstlicher Alterung) durchzuführen. Die ab Stärke der Mechanismen bzw. Funktionen "mittel" geforderten Onlinetests und die für P2, Stärke der Mechanismen bzw. Funktionen "hoch" geforderten Tests der statistischen Eigenschaften der digitalisierten Rauschsignale im laufenden Betrieb werden ebenfalls unter diesen Bedingungen getestet.

Aus der Analyse der Stärke der Mechanismen (ITSEC) bzw. Stärke der Funktionen (CC) muss hervorgehen, ob die Zufallszahlen unter bestimmten Bedingungen von den P1- bzw. P2-Eigenschaften abweichen. Diese Analyse muss zeigen, ob die Aufwände eines Angreifers, die notwendig sind, um den EVG in einen solchen Zustand zu bringen, mit der angestrebten Stärke der Mechanismen bzw. Funktionen vereinbar sind. Bei „feindlichen“ Umgebungsbedingungen sind die Tests unter dem Aspekt der Stärke der Mechanismen sowie der Schwachstellenanalyse ggf. zu erweitern.

Dies kann im Einzelfall Auswirkungen auf die Dokumentation zu Auslieferung und Konfiguration, Anlauf und Betrieb und die Betriebsdokumentation haben.

D.1 Umfang und Reihenfolge der Evaluationssarbeiten:

Klasse P1 (Fortsetzung)

P1.i) Aufgaben des Evaluators:

Die Aufgaben des Evaluators hängen von der Stärke der Mechanismen bzw. Funktionen ab. Er muss die Anforderungen P1.d) (i) bis (vi) verifizieren, sofern sie für die angestrebte Stärke der Mechanismen bzw. Funktionen relevant sind.

P1.i(i) (Prüfung der Eigenschaft P1.d)(i)): Der Evaluator bestimmt die kleinste Anzahl c interner Zufallszahlen, deren Konkatenation mindestens 48 Bit umfasst. Es bezeichne $\pi_{1..48}$ die Projektion auf die linken 48 Bit. Testvorschrift und Entscheidungsregel: Der Evaluator erzeugt interne Zufallszahlen r_1, r_2,... und bildet hieraus eine Folge von 2^{16} Projektionen $\pi_{1..48}$ $(r_1,\ldots,r_c)$, $\pi_{1..48}$ $(r_{c+1},\ldots,r_{2c})$,…. Auf diese Folge wendet er den Disjunktheitstest T0 an. Wird dieser Test passiert, gilt die Eigenschaft P1.d)(i) als erfüllt. Andernfalls wird der Test T0 auf eine weitere Folge angewandt.

Passiert diese Folge den Test T0, gilt die Eigenschaft P1.d)(i) als erfüllt; andernfalls als nicht erfüllt. Eine zweite Wiederholung ist nicht zulässig.

P1.i(ii) (Prüfung der Eigenschaft P1.d)(ii)): Es bezeichnen f die Breite der vom TRNG erzeugten Zufallszahlen in Binärdarstellung und π_w die Projektion auf die w-te Komponente. Die Unterpunkte (ii.a) und (ii.b)(w) beschreiben die „Grundbausteine", d.h. die einzelnen Tests, während in (ii.c) die gesamte Testvorschrift samt Entscheidungsregel beschrieben wird.

P1.i(ii.a) Der Evaluator erzeugt Zufallszahlen $r_1,r_2,\ldots$ und interpretiert diese als Bitstrings konstanter Länge. Auf die ersten 20.000 Bit dieser Folge wendet er die in Kapitel F beschriebenen Tests T1-T4 mit den angegebenen Verwerfungsgrenzen an. Ferner berechnet er die Testgrößen $Z_1,\ldots,Z_{5000}$ (siehe Test T5 in Kapitel F), bestimmt $\max_{\tau\leq 5000}\{|Z_\tau\text{-}2500|\}$ und wählt ein τ_0 (bei mehreren Kandidaten zufällig), für das dieses Maximum angenommen wird. Anschließend wendet er auf die Teilfolge $b'_1 := b_{10001},\ldots,b'_{10000} := b_{20000}$ den Autokorrelationstest (Test T5) mit Shift τ_0 und den in Kapitel F angegebenen Verwerfungsgrenzen an.

P1.i(ii.b) (w) (Es ist $1 \leq w \leq f$.) Der Evaluator erzeugt Zufallszahlen $r_1,r_2,\ldots,r_{20000}$. Auf die Folge der Projektionen $\pi_w(r_1),\ldots,\pi_w(r_{20000})$ wendet er die in Kapitel F beschriebenen statistischen Tests T1-T4 mit den angegebenen Verwerfungsgrenzen an. Ferner berechnet er die Testgrößen $Z_1,\ldots,Z_{5000}$ (siehe Test T5 in Kapitel F), bestimmt $\max_{\tau\leq 5000}\{|Z_\tau\text{-}2500|\}$ und wählt ein τ_0 (bei mehreren Kandidaten zufällig), für das dieses Maximum angenommen wird. Anschließend wendet er auf die Teilfolge $b'_1 := b_{10001},\ldots,b'_{10000} := b_{20000}$ den Autokorrelationstest (Test T5) mit Shift τ_0 und den in Kapitel F angegebenen Verwerfungsgrenzen an.

P1.i(ii.c) Testvorschrift und Entscheidungsregel: Der Evaluator führt sukzessiv die Testvorschriften (ii.a), (ii.b)(1), (ii.b)(2),…, (ii.b)(f), (ii.a),… durch, bis insgesamt 257 Bitfolgen erzeugt und getestet wurden. Die Eigenschaft P1.d)(ii) gilt als erfüllt, falls alle Einzeltests passiert wurden. Führte mehr als ein Einzeltest zu einer Verwerfung, gilt die Eigenschaft d)(ii) als nicht erfüllt.

Führte genau ein Einzeltest zu einer Verwerfung, ist das gesamte Testverfahren nochmals durchzuführen. Die Eigenschaft d)(ii) gilt genau dann als erfüllt, falls beim Wiederholungsdurchgang alle Einzeltests passiert werden. Eine zweite Wiederholung ist nicht statthaft.

P1.i(iii) (Nachweis von Eigenschaft P1.d)(iii)): Verifikation von P1.f)(iv)

P1.i(iv) (Nachweis von Eigenschaft P1.d)(iv)): Verifikation von P1.f)(v)

P1.i(v) (Prüfung der Eigenschaft P1.d)(v)): Es sind die (in den Sicherheitsvorgaben bzw. dem Architekturentwurf dargelegten/beschriebenen/erklärten)

äußeren Bedingungen zu berücksichtigen, soweit diese die Funktion der Rauschquelle beeinflussen können. Für jede dieser äußeren Bedingungen sind die unter (i) und (ii) beschriebenen Testvorschriften und Entscheidungsregeln anzuwenden. Die Eigenschaft P1.d)(v) gilt als erfüllt, falls die Eigenschaften P1.d)(i) und P1.d)(ii) für alle äußere Bedingungen als erfüllt sind (ggf. nachgewiesen durch Test unter Grenzwerten der äußeren Bedingungen).

Dem TRNG wird die Zugehörigkeit zur Klasse P1 mit Stärke der Mechanismen bzw. Funktionen niedrig bzw. Mechanismenstärke mittel bzw. Mechanismenstärke hoch bestätigt, falls P1.d)(i) bzw. P1.d)(i) und P1.d)(ii) bzw. P1.d)(i), P1.d)(ii) und P1.d)(iii) erfüllt sind.

Bei Stärke der Mechanismen bzw. Funktionen hoch werden die Evaluationstest unter verschiedenen äußeren Bedingungen (Temperatur, Klima, künstlicher Alterungsprozess) durchgeführt, und zumindest auf externen Aufruf testet der TRNG die statistischen Eigenschaften der internen Zufallszahlen im laufenden Betrieb.

P1.i(vi) (Nachweis von Eigenschaft P1.d)(vi)): Verifikation von P1.f)(vi)

P1.j) Erläuterungen zu i):

Zu P1.i)(i): Anders als bei der entsprechenden Eigenschaft K1.d)(i) in [AIS20] sind vom Antragssteller keine individuellen Parameter vorzugeben. Dieser Unterschied liegt darin begründet, dass ein akzeptabler Zufallszahlengenerator, anders als ein deteministischer Zufallszahlengenerator, der internen Zufallszahlenfolge ständig Entropie zuführt. Die „Qualität“ der Disjunktheitseigenschaften der internen Zufallsvektoren sollten daher kaum von der Breite der gewählten Zufallszahlenvektoren abhängen. Einem idealen Rauschgenerator würde die Eigenschaft P1.d)(i) mit einer Wahrscheinlichkeit von ca. 2^{-34} nicht zugebilligt.

Zu P1.i)(ii): Einem idealen Rauschgenerator würde die Eigenschaft P1.d)(ii) mit einer Wahrscheinlichkeit von ca. $2.5 \cdot 10^{-6}$ nicht zugebilligt. (Ist f=1, so stimmen P1.i)(ii.a) und P1.i)(ii.b) trivialerweise überein.)

Klasse P2 (Fortsetzung)

P2.i) Aufgaben des Evaluators:

Die Aufgaben des Evaluators hängen von der Stärke der Mechanismen bzw. Funktionen ab. Er muss die Anforderungen P1.d) (vii) bis (xiii) verifizieren, sofern sie für die angestrebte Stärke der Mechanismen bzw. Funktionen relevant sind.

P2.i)(i) Verifikation der P1-Eigenschaften (siehe P1.i)), soweit diese für die angestrebte Stärke der Mechanismen bzw. Funktionen relevant sind und nicht in P2-spezifischen Anforderungen enthalten sind.

P2.i)(vii) Prüfung der Eigenschaft P2.d)(vii): Es bezeichne k die Breite der Binärdarstellung der digitalisierten Rauschsignale. Für k = 1 werden nachfolgend fünf Einzeltests beschrieben und eine Entscheidungsregel formuliert. Für k > 1 muss der Hersteller im Bedarfsfall Ersatztests angeben. Deren Wirksamkeit ist zu begründen. Diese Ersatztests dürfen nicht schwächer sein als im Fall k = 1.

P2.i)(vii.a) [k=1]: Der Evaluator erzeugt eine digitalisierte Rauschsignalfolge $w_1,\ldots,w_{n0}$ mit $n_0 := 100000$. Es bezeichne $\mu\_emp = (\mu\_emp(0), \mu\_emp(1))$ deren empirische Verteilung. Die Eigenschaft (vii.a) ist erfüllt, falls $|\mu\_emp(1) - 0.5 | < a_0 := 0.025$ gilt.

P2.i)(vii.b) [k=1]: Der Evaluator erzeugt eine weitere digitalisierte Rauschsignalfolge $w_1,w_2,\ldots,$ die er disjunkt in 2 Teilfolgen $TF_{(0)},\ldots,TF_{(1)}$ zerlegt. Dabei gehört das Tupel (w_{2j+1},w_{2j+2}) genau dann zur Teilfolge $TF_{(r)}$, falls $w_{2j+1}= r$. Die Ausgangsfolge $w_1,w_2,\ldots,$ muss so lang sein, dass beide Teilfolgen mindestens $n_1 := 100000$ viele Elemente enthalten. Projiziert man die ersten n_1 2-Tupel der Teilfolge $TF_{(r)}$ auf die zweite Komponente, erhält man die eindimensionale Stichprobe $St_{(r)}$. Dividiert man die Häufigkeiten, mit denen einzelne Werte angenommen werden, durch den Stichprobenumfang n_1, erhält man die empirische 1-Schritt-Übergangsverteilung $\nu\_emp_{(r)}$ (.) bei Vorgänger r. Die Eigenschaft (vii.b) ist erfüllt, falls $|\nu\_emp_{(0)}(1) + \nu\_emp_{(1)}(0) - 1 | < a_1 := 0.02$ gilt.

P2.i)(vii.c) [k=1] Der Evaluator erzeugt eine weitere digitalisierte Rauschsignalfolge $w_1,w_2,\ldots,$ die er disjunkt in $2^2 = 4$ Teilfolgen $TF_{((0)-(0)))},\ldots,TF_{((1)-(1))}$ zerlegt. Dabei gehört das Tripel $(w_{3j+1},w_{3j+2},w_{3j+3})$ genau dann zur Teilfolge $TF_{((r)-(s))}$, falls $(w_{3j+1},w_{3j+2})= (r,s)$. Die Ausgangsfolge $w_1,w_2,\ldots,$ muss so lang sein, dass jede dieser vier Teilfolgen mindestens $n_2 := 100000$ viele Elemente enthält. Projiziert man jeweils die ersten n_2 3-Tupel der Teilfolge $TF_{((r)-(s))}$ auf die dritte Komponente, erhält man die eindimensionale Stichprobe $St_{((r)-(s))}$. Für jedes $s \in \{0,1\}$ vergleicht der Evaluator die zugrundeliegenden Verteilungen der beiden Stichproben $St_{((0)-(s))}$ und $St_{((1)-(s))}$ mit Test T7 auf dem Signifikanzniveau $\alpha\_2:=0.0001$ auf Gleichheit . Die

Eigenschaft (vii.c) ist erfüllt, falls beide Tests passiert werden. Andernfalls gilt Eigenschaft (vii.c) als nicht erfüllt.

P2.i)(vii.d) [k=1]: Der Evaluator erzeugt eine weitere digitalisierte Rauschsignalfolge $w_1,w_2,\ldots,$ die er disjunkt in 8 Teilfolgen $TF_{((0)-(0)-(0))},\ldots,TF_{((1)-(1)-(1))}$ zerlegt. Dabei gehört das Quadrupel $(w_{4j+1},w_{4j+2},w_{4j+3},w_{4j+4})$ genau dann zur Teilfolge $TF_{((r)-(s)-(t))}$, falls $(w_{4j+1},w_{4j+2},w_{4j+3}) = (r,s,t)$. Die Ausgangsfolge $w_1,w_2,\ldots,$ muss so lang sein, dass jede dieser acht Teilfolgen mindestens n_3:= 100000 viele Elemente enthält. Projiziert man jeweils die ersten n_3 Quadrupel der Teilfolge $TF_{((r)-(s)-(t))}$ auf die vierte Komponente, erhält man die eindimensionale Stichprobe $St_{((r)-(s)-(t))}$. Für jedes Paar $(s,t) \in \{0,1\}^2$ vergleicht der Evaluator die zugrundeliegenden Verteilungen der beiden Stichproben $St_{((0)-(s)-(t))}$ und $St_{((1)-(s)-(t))}$ mit Test T7 auf dem Signifikanzniveau α_3:=0.0001 auf Gleichheit . Die Eigenschaft (vii.d) ist erfüllt, falls alle vier Tests passiert werden. Andernfalls gilt Eigenschaft (vii.d) als nicht erfüllt.

P2.i)(vii.e) Der Evaluator erzeugt eine weitere digitalisierte Rauschsignalfolge $w_1,w_2,\ldots$ und wendet hierauf den Entropietest (Test T8) mit den Parametern L=8, Q=2560 und K= 256000 an. Die Eigenschaft (vii.e) ist erfüllt, falls die Testgröße f > 7,976 ist.

Entscheidungsregel: Wurden die Eigenschaften P2.i)(vii.a) - (vii.e) erfüllt, gilt die Eigenschaft P2.d)(vii) als erfüllt. Wurde mehr als eine Teileigenschaft nicht erfüllt, gilt die Eigenschaft P2.d)(vii) als nicht erfüllt. Wurde genau eine Teileigenschaft nicht erfüllt, werden P2.i)(vii.a) - (vii.e) auf eine andere Stichprobe angewandt. Werden bei der Wiederholung alle Teileigenschaften P2.i)(vii.a) - (vii.e) erfüllt, gilt die Eigenschaft P2.d)(vii) als erfüllt. Eine weitere Wiederholung ist nicht zulässig.

Führt der Antragsteller Ersatznachweise gemäß P2.d), „Ersatzkriterien für P2.d)(vii); Typ 1“ bzw. „Ersatzkriterien für P2.d)(vii); Typ 2“ , so hat der Evaluator diese zu prüfen.

P2.i)(vii) (Nachweis von Eigenschaft P2.d)(viii)): Verifikation von P2.f)(vii)

P2.i)(viii) (Nachweis von Eigenschaft P2.d)(ix)): Verifikation von P2.f)(viii)

P2.i)(ix) (Nachweis von Eigenschaft P2.d)(x)): Verifikation von P2.f)(ix)

P2.i)(x) (Nachweis von Eigenschaft P2.d)(xi)): Verifikation von P2.f)(x)

P2.i)(xi) (Prüfung der Eigenschaft P2.d)(xii)): Es sind die (in den Sicherheitsvorgaben bzw. dem Architekturentwurf dargelegten/beschriebenen/erklärten) äußeren Bedingungen zu berücksichtigen, soweit diese die Funktion der Rauschquelle beeinflussen können. Für jede dieser äußeren Bedingungen sind die unter (vii) beschriebenen Testvorschriften und die dort angegebene Entscheidungsregel anzuwenden. Die Eigenschaft P2.d) (xii) gilt als

erfüllt, falls die Eigenschaften P2.d)(vii) für alle äußere Bedingungen erfüllt ist.

P2.i)(xii) (Nachweis von Eigenschaft P2.d)(xiii)): Der Nachweis des selbständigen Aufrufs des Onlinetests ist wie unter D.0 beschrieben zu erbringen.

P2.j) Erläuterungen zu i):

Zu P2.i)(vii.a): Zielsetzung und Begründung: Vergleich der eindimensionalen Verteilung der digitalisierten Rauschsignalfolge mit der Gleichverteilung auf {0,1}. Etwaige Abhängigkeiten von Vorgängern werden in (vii.a) zumindest nicht explizit berücksichtigt. Ist die digitalisierte Rauschsignalfolge gedächtnislos und stationär und erfüllt ihre Verteilung $\mu = (\mu(0), \mu(1))$ die Ungleichung $|\mu(1)-0.5| < 0.025$, so beträgt der durchschnittliche Entropiezuwachs pro Bit mehr als 0.998.

Anmerkung: Damit die empirischen Häufigkeiten mit hoher Wahrscheinlichkeit innerhalb der zulässigen Schranke liegen, d.h. dass digitalisierte Rauschsignalfolgen dieses Evaluationskriterium mit hoher Wahrscheinlichkeit passieren, müssen die exakten Wahrscheinlichkeiten näher bei 0.5 liegen als dies für die empirischen Häufigkeiten zum Passieren des Tests erforderlich ist. Tatsächlich wird dieses Kriterium mit einer Wahrscheinlichkeit von mindestens 1-0.00078 erfüllt, falls $\mu(0)=\text{Prob}(w_j=0)$, $\mu(1)=\text{Prob}(w_j=1) \in [0.5-0.02, 0.5+0.02]$ ist. (Die angegebene Wahrscheinlichkeit gilt für den ungünstigsten Fall, nämlich dass $\text{Prob}(w_j=0), \text{Prob}(w_j=1) \in \{0.48,0.52\}$ gilt.)

Zu P2.i)(vii.b): Zielsetzung und Begründung: Vergleich der 1-Schritt-Übergangswahrscheinlichkeiten der digitalisierten Rauschsignalfolge bei verschiedenen Vorgängern, wobei gewisse Abweichungen toleriert werden. Etwaige Mehrschritt-Abhängigkeiten von Vorgängern werden von dem Kriterium (vii.b) zumindest nicht explizit berücksichtigt. Ist die digitalisierte Rauschsignalfolge stationär und besitzt ein Gedächtnis der Länge ≤ 1, und erfüllen anstelle der empirischen 1-Schritt-Übergangsverteilungen $\nu\_emp_{(0)}(1)$ und $\nu\_emp_{(1)}(0)$ die exakten Übergangswahrscheinlichkeiten $\nu_{(0)}(1)$ und $\nu_{(1)}(0)$ die Anforderung (vii.b), d.h. $|\nu_{(0)}(1) + \nu_{(1)}(0) - 1 | < a_1 := 0.02$, so ist der durchschnittliche Entropiezuwachs pro Bit um maximal 0.00057 geringer als wenn die digitalisierte Rauschsignalfolge gedächtnislos wäre, aber dieselbe stationäre Verteilung besäße. Anmerkung: Für gedächtnislose Rauschsignalfolgen gilt $\nu_{(0)}(0)=\nu_{(1)}(0)$ und $\nu_{(0)}(1)= \nu_{(1)}(1)$, d.h. $\nu_{(1)}(0) = 1-\nu_{(0)}(1)$. Ein kleiner Wert $|\nu\_emp_{(0)}(1) +\nu\_emp_{(1)}(0) -1 |$ ist folglich ein Indikator dafür, dass bestenfalls nur schwache 1-Schritt-Abhängigkeiten vorliegen. Gilt für die exakten 1-Schritt-Übergangswahrscheinlichkeiten die Ungleichung $|\nu_{(0)}(1) +\nu_{(1)}(0) -1 | < 0.012$, so erfüllen die empirischen 1-Schritt-Über-

gangswahrscheinlichkeiten das Kriterium (vii.b) mit einer Wahrscheinlichkeit von mindestens 1-0.00017.

Zu P2.i)(vii.c) und (vii.d): Zielsetzung: Die digitalisierten Rauschsignalfolgen sollen keine höheren als 1-Schritt-Abhängigkeiten aufweisen. Trifft dies zu, so hängen für m > 1 die m-Schritt-Übergangswahrscheinlichkeiten insbesondere vom m-ten Vorgänger nicht ab. Mit anderen Worten: Sind die ersten (m-1) Vorgänger konstant, induzieren alle m-letzten Vorgänger auf {0,1} dieselbe Verteilung.

Zu P2.i)(vii) (Entscheidungsregel): Die Wahrscheinlichkeit, dass ein idealer TRNG bei einmaliger Durchführung die Eigenschaft (vii.a),… bzw. (vii.e) nicht erfüllt, beträgt 0, 0, $2\cdot10^{-4}$, $4\cdot10^{-4}$ bzw. 0 . Die Entscheidungsregel stellt sicher, dass einem idealen TRNG die Eigenschaft (vii) nur mit einer Wahrscheinlichkeit von etwa $6\cdot10^{-7}$ irrtümlich nicht zugebilligt wird. Die Erläuterungen zu (vii.a), (vii.b) und (vii.e) belegen überdies, dass auch TRNGs, bei denen die Schiefe und die 1-Schritt-Abhängigkeiten der digitalisierte Rauschsignalfolgen gewisse Schranken nicht überschreiten, die entsprechenden Einzeleigenschaften ebenfalls mit sehr hoher Wahrscheinlichkeit erfüllen. Die Wahrscheinlichkeiten, die Eigenschaften (vii.c) bzw. (vii.d) zu erfüllen, ist für alle Verteilungen nahezu identisch, solange diese keine Mehrschritt-Abhängigkeiten aufweisen. Für Verteilungen, für die $\mu(0)$, $\mu(1)$, $\nu_{(0)}(1)$ und $\nu_{(1)}(0)$ (anstelle der empirischen Werte) die Voraussetzungen aus (vii.a) und (vii.b) erfüllen, ist die Verwerfungswahrscheinlichkeit beim Entropietest $< 10^{-4}$.

Zu P2.i)(vii) (Fall k>1): Für den Fall k>1 erscheint es naheliegend, die digitalisierten Rauschsignale (k-Bit-Blöcke) als binärwertige Teilfolgen der Länge k zu interpretieren und auf die Gesamt-Binärfolge die Kriterien (vii.a) – (vii.e) anzuwenden. Bei einem derartigen Vorgehen sind jedoch zwei grundsätzliche Phänomene zu berücksichtigen: Abhängig von der Rauschquelle und der konkreten Form der Digitalisierung müssen die einzelnen Bits der digitalisierten Rauschsignale zum einen nicht „gleichartig“ sein; eine stationäre digitalisierte Rauschsignalfolge bedingt also nicht notwendigerweise eine stationäre binärwertige Folge. Ferner induzieren etwaige 1-Schrittabhängigkeiten der digitalisierten Rauschsignalfolge im allgemeinen k-Schritt-Abhängigkeiten der binärwertigen Folge.

D.2 Bemerkung: Die Evaluation eines TRNG basiert wesentlich auf statistischen Tests. Das Evaluationsergebnis ist daher zumindest nicht mit Sicherheit reproduzierbar. Dieser Umstand wird dadurch abgemildert, dass eine Nichtanerkennung der P1- bzw. P2-Eigenschaft bei „vernünftigen“ TRNGs wenig wahrscheinlich ist. Somit ist das Ergebnis einer TRNG-Evaluation sozusagen „quasireproduzierbar“, was für die

Zuverlässigkeit und Vertrauenswürdigkeit eines Evaluationsverfahrens natürlich unerlässlich ist.

E. Beispiele

In diesem Kapitel werden exemplarisch verschiedene mathematische Nachbearbeitungen und Onlinetestvarianten beschrieben und im Hinblick auf die entsprechenden, in P1.d) und P2.d) formulierten Anforderungen untersucht. Ob die Anforderungen P1.d)i), ii) und v) sowie P2.d)vii) und (xii) erfüllt sind, muss der Evaluator empirisch verifizieren bzw. falsifizieren. Die Eigenschaften P1.d)(i) und (ii) sind relativ schwach und sollten von nahezu jeder physikalischer Rauschquelle erfüllt werden. Als *Nullhypothese* bezeichnen wir die Annahme, die zu testenden Zufallszahlen seien von einer idealen Rauschquelle erzeugt worden.

E.1 Beispiel: (mathematische Nachbearbeitung, Totalausfall der Rauschquelle)

Jedes digitalisierte Rauschsignal umfasst ein Bit. Die mathematische Nachbearbeitung besteht aus einem linear rückgekoppelten Schieberegister der Länge 63 mit primitivem Rückkopplungspolynom $p(x) = x^{63}+x^{31}+1$. Die Digitalisierung des Rauschsignals und der Fortschaltungstakt des Schieberegisters sind synchron getaktet. Das Rückkopplungsbit ist die nächste interne Zufallszahl. In das Schieberegister wird die XOR-Summe des Rückkopplungsbits mit dem aktuellen digitalisierten Rauschsignalbit rückgefüttert.

Für jede Anfangsbelegung bildet die mathematische Nachbearbeitung die Menge der endlichen digitalisierten Rauschsignalfolgen bijektiv auf die Menge der endlichen internen Zufallszahlenfolgen ab. Die mathematische Nachbearbeitung erfüllt somit also insbesondere die Eigenschaft P2.d)(viii).

Ist die digitalisierte Rauschsignalfolge ab einem Zeitpunkt konstant 0,0,..., könnte die interne Zufallszahlenfolge trivialerweise durch das freilaufende lineare Schieberegister erzeugt werden. Dies ist trifft im wesentlichen auch dann zu, falls die digitalisierte Rauschsignalfolge konstant 1,1, ... ist: Es ist lediglich die Anfangsbelegung des Schieberegisters bitweise zu invertieren, und ebenso die Ausgabefolge. (Dies gilt für jedes lineare Schieberegister mit einer geraden Anzahl von Abgriffstellen.) Nach einem Totalausfall der Rauschquelle entspricht die mathematische Nachbearbeitung in beiden Fällen einem K2-DRNG gemäß [AIS20] (siehe auch Beispiel E.3 in [AIS20]).

Selbst bei einem Totalausfall der Rauschquelle dürften die internen Zufallszahlen daher nahezu alle gängigen statistischen Tests passieren. Viel effizienter ist jedoch das Testen der digitalisierten Rauschsignalfolge (vgl. P2.d)(vii), (ix), (xi)).

E.2 Beispiel: (mathematische Nachbearbeitung) Angenommen, die Digitalisierung liefere eine Folge $X = (x_0, x_1, \ldots)$ unabhängiger Bits mit einer Wahrscheinlichkeit $P\{x_i = 1\} = p \le 1/2$.

Zunächst ein Beispiele nach von Neumann. Sei zunächst der Bitstrom in Paare $(x_{2i}, x_{2i+1}), i = 0,1,2,\ldots$, zerlegt. Die Paare (00) und (11) werden verworfen und die verbleibende Folge *y* zu einer internen Zufallsfolge *y'* gemäß

$$y'_k = \begin{cases} 0 \text{ } \textit{für} \text{ } (y_{2k}, y_{2k+1}) = (01) \\ 1 \text{ } \textit{für} \text{ } (y_{2k}, y_{2k+1}) = (10) \end{cases}$$

umgewandelt. Die Folge $(y'_0, y'_1, \ldots)$ ist dann asynchron zur Folge *X*, aber gleichverteilt.

Für weitere Beispiele wird die digitalisierte Rauschsignalfolge in Abschnitte $\overline{X}_j = (x_{64j}, x_{64+1}, \ldots, x_{64j+63})$ zu je 64 Bit eingeteilt und zur internen Zufallsfolge $\overline{Y} = (Y_0,\ Y_1,\ \ldots)$ nachbereitet mit $Y_j = (y_{64j},\ y_{64j+1},\ \ldots,\ y_{64j+63})$. Es werden drei Varianten der Nachbereitung betrachtet:

a) Y_j entspricht den linken 64 Bit des mit einem bekannten Muster gepaddeten und dann gehashten Abschnitts X_j,

b) XOR-Summe zweier aufeinanderfolgender Abschnitte, $Y_j = X_{2j} \oplus X_{2j+1}$

c) Verschlüsselung mit einem Schlüssel aus der digitalisierten Rauschsignalfolge, $Y_j = E_{X_{2j}}(X_{2j+1})$.

Zunächst sei festgestellt, dass jeder Abschnitt der digitalisierten Rauschsignalfolge einen Wert *A* mit einer Wahrscheinlichkeit annimmt, die sich aus dessen Hamminggewicht $|A| = \sum_{i=0}^{63} a_i$, d. h. der Anzahl der Einsen, zu $P\{\overline{X}_j = A\} = p^{|A|} \cdot (1-p)^{(64-|A|)}$ ergibt. Sei $W = (w_0, w_1, \ldots, w_{2^{64}-1})$ die nichtfallende Folge dieser Wahrscheinlichkeiten.

Die Nachbearbeitung in Variante a) kann als zufällige Abbildung interpretiert werden. Sie ist nicht injektiv und erfüllt insbesondere nicht die Eigenschaft P2.d)(viii). Es sei aber bemerkt, dass statistische Eigenschaften kleiner Strukturen, wie z. B. das 0/1-Verhältnis, dadurch verbessert werden können. Die statistischen Eigenschaften der Abschnittsfolge $(\overline{Y}_j)_{j=0,1,\ldots}$, wie z. B. die Wahrscheinlichkeit für Wiederholungen von Abschnittswerten, werden sogar etwas schlechter.

Die Varianten b) und c) komprimieren die digitalisierte Rauschsignalfolge zur internen Zufallsfolge im Verhältnis 2:1. Sie besitzen kein Gedächtnis und erzeugen unabhängige Abschnitte der internen Zufallsfolge. Die Variante b) liefert unabhängige Bits und glättet die Schiefe der Bitverteilung um $p-2p^2$, d. h. $P\{a_i=1\}=2p-2p^2$, $P\{a_i=0\}=1-2p+2p^2$.

Für die Variante c) gilt für alle *j* die Identität $P\{\hat{Y}_j=A\}=\sum_{K\in\{0,1\}^{64}} P\{\overline{X}_{2j}=K\}\cdot P\{\overline{X}_{2j+1}=E_K^{-1}(A)\}$. Wenn $E_K^{-1}(A)$ für festes *A* und laufendes $K\in\{0,1\}^{64}$ eine Permutation liefert[2], so können diese Wahrscheinlichkeiten durch $p^{64}\le 2^{64}p^{64}(1-p)^{64}\le P\{Y_j=A\}\le(1-2p+2p^2)^{64}\le(1-p)^{64}$ abgeschätzt werden. Für $p<1/2$ ergibt sich wiederum eine Glättung der Wahrscheinlichkeitsverteilung. Die Bits innerhalb eines Abschnitts sind aber im allgemeinen nicht unabhängig, wenn auch diese Abhängigkeiten für viele Anwendungen vernachlässigt werden können.

Ein Angreifer kann die Menge der Abschnitte in der digitalisierten Rauschsignalfolge wegen der Schiefe der Bitverteilung nach den Wahrscheinlichkeiten ihres Auftretens ordnen. Dies begünstigt Exhaustionsattacken gegen einzelne Abschnitte der digitalisierte Rauschsignalfolge. Bei Variante a) resultiert daraus eine mindestens ebenso effiziente Exhaustionsattacke gegen die internen Zufallszahlenabschnitte. Dies trifft bei den Varianten b) und c) nicht zu, da in jede interne Zufallszahlen jeweils zwei digitalisierte Rauschsignalabschnitte eingehen.

Wie die digitalisierte Rauschsignalfolge sind auch die internen Zufallszahlen unabhängig. In der Variante b) könnte ein Onlinetest der Rauschquelle gemäß Anforderung (xi) durch eine Überwachung der 0/1-Verteilung der internen Zufallsfolge erfolgen. In den Varianten a) und c) wäre dies wegen der Verwischung der Bitverteilung durch das Hashen bzw. durch die Verschlüsselung wirkungslos.

E.3 Beispiel: (mathematische Nachbearbeitung)

Die Rauschquelle erzeuge einzelne Bits, deren Verteilung aufgrund des mathematischen Modells der Rauschquelle als stationär angesehen werden kann. Die Stationaritätsannahme sei ferner durch statistische Untersuchungen verschiedener Prototypen bestätigt worden. (Genauer: Die Stationaritätsannahme konnte durch entsprechende statistische Tests auf einem kleinen Signifikanzniveau α (z.B. α=0.001) nicht verworfen werden.) Die digitalisierte Rauschsignalfolge muss nicht notwendigerweise unabhängig sein. Ferner sei eine Abbildung f: $\{0,1\}^m \times \{0,1\}^m \rightarrow \{0,1\}^m$ (z.B. m=8) gegeben, welche bei festgehaltener erster (bzw. festgehaltener zweiter) Komponente bijektiv in der zweiten (bzw. in der ersten) Komponente ist.

[2] Man beachte, daß nicht alle Chiffrierabbildungen diese Eigenschaft erfüllen.

Die digitalisierte Rauschsignalfolge werde in nichtüberlappende Blöcke $X_1,X_2,$ ... der Länge m segmentiert, aus denen mittels $Y_1:=f(X_1,X_2)$, $Y_2:=f(X_3,X_4)$, ... die interne Zufallszahlenfolge generiert wird.

Mit einer einfachen Rechnung verifiziert man, dass $H(Y_{j+1} \mid Y_1, ...,Y_j) \geq H(X_{2j+1} \mid X_1, ...,X_{2j})$ gilt, d..h. der Entropiezuwachs pro m-Bit-Block ist bei der internen Zufallszahlenfolge mindestens ebenso groß wie bei der digitalisierten Rauschsignalfolge. Im allgemeinen (verteilungsabhängig!) wird er echt größer sein. Der Entropiezuwachs wird durch eine Halbierung des Durchsatzes "erkauft". Die Abbildung f kann z.B. eine Gruppenoperation auf $\{0,1\}^m$ sein (vgl. auch Beispiel E.2 b) für m = 1).

E.4 Beispiel: (Ersatzkriterien für P2.d)(vii); Typ 1 und Typ 2)

In diesem Beispiel werden verschiedene mathematische Nachbearbeitungen dahingehend untersucht, ob anstelle von P2.d)(vii) eine Evaluation gemäß “Ersatzkriterien für P2.d)(vii); Typ 1“ oder „Ersatzkriterien für P2.d)(vii); Typ 2“ in Betracht kommt. Wir nehmen an, dass die Rauschquelle binärwertige digitalisierte Rauschsignalfolgen erzeugt.

Wir betrachten folgende mathematische Nachbearbeitungen:

a) Beispiel E.1

b) nichtüberlappende, aufeinanderfolgende Rauschsignalbitpaare werden XORiert (=Spezialfall des Beispiel E.3 mit m=1 und $f(X_1,X_2):= X_1 \oplus X_2$)

c) Beispiel E.2b)

Szenario 1: Der Zugriff auf die digitalisierte Rauschsignalfolge ist möglich. Ausgiebige Untersuchungen von Prototypen haben folgendes ergeben: Die Wahrscheinlichkeit für eine "1" liegt im Intervall [0.45,0.47]. Die digitalisierten Rauschsignale verhalten sich statistisch wie Realisierungen unabhängiger Zufallsvariablen. Insbesondere erfüllen sie die Kriterien P2.i)(vii.b), P2.i)(vii.c) und P2.i)(vii.d).

zu a) Eine Evaluierung gemäß “Ersatzkriterien für P2.d)(vii); Typ 1“ ist *nicht* möglich, da die mathematische Nachbearbeitung die Entropie pro Bit nicht erhöht.

zu b) Aus der Unabhängigkeit der digitalisierten Rauschsignalfolge folgt auch die Unabhängigkeit der internen Zufallszahlenfolge. Unter der Unabhängigkeitsannahme der digitalisierten Rauschsignale liegt die Wahrscheinlichkeit für eine “1” bei den internen Zufallszahlen im Intervall [0.49875, 0.50125]. Mit diesem Hinweis ist der im zweiten Spiegelpunkt von “Ersatzkriterien für P2.d)(vii); Typ 1“ geforderte nachvollziehbare Nachweis durchgeführt.

zu c) Statistische Tests der internen Zufallszahlenfolgen können keine (im Sinne der Zielsetzung von Kriterium P2.d)(vii)) brauchbare Aussagen liefern, da derartige Tests

die eindimensionale Verteilung ganzer 64-Bit-Blöcke berücksichtigen müssten. Die erforderlichen Stichprobenumfänge lägen dann weit über 2^{64}, was praktisch unmöglich ist. Für eine Evaluation gemäß den "Ersatzkriterien gemäß P2.d)(vii); Typ 1" käme daher nur ein Nachweis des Antragstellers auf theoretischer Basis in Frage, dass die mathematische Nachbearbeitung die Entropie pro Bit hinreichend erhöht (vgl. P2.j)).

Szenario 2: Der Zugriff auf die digitalisierte Rauschsignalfolge ist nicht möglich. Aufgrund der konkreten technischen Realisierung der physikalischen Rauschquelle (i.e. unter Berücksichtigung der Schalt- und Totzeiten einzelner Bauteile, der Abtastrate, etc.) sei die Annahme plausibel, dass die erzeugten digitalisierten Rauschsignalfolgen unabhängig sind. (Der Begründung zur Herleitung dieser Modellannahme kommt entscheidende Bedeutung zu.)

Bemerkung: Im Gegensatz zu Szenario 1 kann es sein, dass die digitalisierte Rauschsignalfolge Kriterium P2.d)(vii) erfüllt, nur ist der direkte Nachweis nicht möglich.

zu a) Aus den internen Zufallszahlen kann die digitalisierte Rauschsignalfolge bestimmt werden. Die Tests P2.i)(vii.a) - P2.i)(vii.e) können auf die rückgerechnete digitalisierte Rauschsignalfolge angewandt werden. Erfüllt die digitalisierte Rauschsignalfolge die Tests P2.i)(vii.a) - P2.i)(vii.e) nicht, ist eine Evaluierung gemäß den "Ersatzkriterien für P2.d)(vii); Typ 2" *nicht* möglich.

zu b) Mit der digitalisierten Rauschsignalfolge ist auch die interne Zufallsbitfolge unabhängig (vgl. Szenario 1). Ein im dritten Spiegelpunkt von "Ersatzkriterien für P2.d)(vii); Typ 2" geforderter geeigneter statistischer Test ist dadurch gegeben, dass der Test P2.i)(vii.a) auf die interne Rauschsignalfolge angewendet wird. (Man beachte, dass dieser Test aufgrund des ersten Spiegelpunkts ohnehin durchzuführen ist.)

zu c) Statistische Tests der internen Zufallszahlenfolgen können keine (im Sinne der Zielsetzung von Kriterium P2.d)(vii)) brauchbare Aussagen liefern, da derartige Tests die eindimensionale Verteilung ganzer 64-Bit-Blöcke berücksichtigen müssten. Die erforderlichen Stichprobenumfänge lägen dann weit über 2^{64}, was praktisch unmöglich ist. Eine Ersatzevaluierung gemäß "Ersatzkriterien für P2.d)(vii); Typ 2" erscheint daher kaum möglich.

E.5 Beispiel: (Tot-Test, Anlauftest)

Der TRNG erzeugt fortlaufend binärwertige digitalisierte Rauschsignalfolgen. Eine mathematische Nachbearbeitung findet nicht statt, d.h. die digitalisierten Rauschsignale entsprechen den internen Zufallszahlen. Die Ausgabe von Zufallzahlen erfolgt aus einem 512-Bit-FIFO. Sind im FIFO nicht mehr als 256 Bit Zufallszahlen enthalten, können keine weiteren Zufallszahlen entnommen werden, sondern es muss das FIFO zunächst wieder aufgefüllt werden. Sind mindestens 48 aufeinanderfolgende interne Zufallszahlen (Bits) identisch, so wird der TRNG mit Verdacht auf Totalausfall

der Rauschquelle stillgelegt. Derselbe Test wird beim Einschalten des TRNGs durchgeführt (Anlauftest).

Diese Testvorschrift erfüllt T1.d(iii), T1.d(iv) und T2.d(x), da keine Zufallszahlen ausgegeben werden können, die nach einem Totalausfall der Rauschquelle erzeugt wurden. Die Eigenschaft P2.d)(ix) ist jedoch nicht erfüllt, da dieser Test auch sehr offensichtliche statistische Schwächen nicht entdeckt. Insbesondere handelt es sich um keinen brauchbaren Onlinetest.

E.6 Beispiel: (Onlinetest, Tot-Test)

Der TRNG erzeugt fortlaufend interne Zufallszahlen. Die Ausgabe von Zufallzahlen erfolgt aus einem 512-Bit-FIFO. Auf externen Aufruf werden die Binärdarstellungen aufeinanderfolgender interner Zufallszahlen als Bitstring interpretiert. Ist das FIFO zur Hälfte leer, wird es mit aktuell erzeugten, aufeinanderfolgenden internen Zufallszahlen $r_1,r_2,...$ aufgefüllt. Alle internen Zufallszahlen, die zum Auffüllen des FIFOs genutzt werden, werden getestet. Zum Testen werden diese als Bitstring interpretiert und in 4-Bit-Worte segmentiert. Auf jeweils 80 (4-Bitworte) wird ein χ^2-Anpassungstest angewandt (siehe z.B. [Ka], 69). (Man beachte, dass diese Zufallszahlen außerhalb des FIFOs nicht noch ein weiteres Mal vorgehalten werden müssen; es genügt vielmehr, intern 16 Worthäufigkeitszähler mitzuführen.) Die Nullhypothese wird verworfen, falls die Testgröße > 65.0 ist. Gemäß ([Ka], 69) ist die Testgröße annähernd χ^2-verteilt mit 15 Freiheitsgraden, woraus sich das Signifikanzniveau $3.8 \cdot 10^{-7}$errechnet (vgl. hierzu Beispiel E.7 nach Tabelle 1). Führt dieser Test zu einer Verwerfung der Nullhypothese wird der TRNG mit einer entsprechenden Fehlermeldung stillgelegt. Die Fehlermeldung wird protokolliert, und der TRNG muss manuell neu gestartet werden. Interne Zufallszahlen, die nicht zum Auffüllen des FIFOs genutzt werden, werden weder gespeichert noch getestet. Es ist zu erwarten, dass der Onlinetest vom TRNG pro Jahr ca. 1000 Mal aufgerufen wird. Die χ^2-Verteilungsfunktion ergibt für ideale Zufallszahlengeneratoren eine Wahrscheinlichkeit von etwa $3.8 \cdot 10^{-4}$ für wenigstens einen Rauschalarm pro Jahr. Die Anforderung P1.d)(vi) ist somit erfüllt.

Ob mit diesem Onlinetest ein Totalausfall der Rauschquelle erkannt wird, hängt von der mathematischen Nachbearbeitung ab. Bei der Nachbearbeitung aus Beispiel E.1 wird ein Totalausfall nicht erkannt. Allerdings verhält sich der TRNG in diesem Fall auch nach einem Totalausfall der Rauschquelle wie ein K2-DRNG im Sinne von [AIS20] (vgl. P1.d)(iv)).

E.7 Beispiel: (Onlinetest, Tot-Test, Anlauftest)

Wie in Beispiel 4.6 werden die internen Zufallszahlen in ein 512-Bit-FIFO geschrieben, das mit aktuell erzeugten, aufeinanderfolgenden internen Zufallszahlen $r_1,r_2,...$ aufgefüllt wird, sobald es wenigstens zur Hälfte leer ist; spätestens aber, wenn nur noch 128 Bits im FIFO enthalten sind. Sämtliche digitalisierten Rauschsignalbits, aus

denen die zum Auffüllen des FIFOs verwendeten internen Zufallszahlen erzeugt werden, gehen in einen Onlinetest („Basistest“; s.u.) ein. Ist das FIFO wieder vollständig gefüllt, aber die Stichprobe zur Durchführung eines Basistests noch nicht vollständig, wird diese mit den nachfolgend erzeugten digitalisierten Rauschsignalbits aufgefüllt und der Test ausgewertet. Erst dann können wieder interne Zufallszahlen ausgegeben werden. Außerdem führt der TRNG selbständig einen weiteren Onlinetest pro Minute durch.

Der Anlauftest beim Start des TRNG besteht aus einem einzigen χ^2-Test über 128 (4-Bit-Worte). Der TRNG passiert den Anlauftest, falls die Testgröße ≤ 65.0 ist (vgl. auch Beispiel E.6). Die Aufgabe des Anlauftests besteht darin, die Funktionalität der Rauschquelle sicherzustellen und ganz offensichtliche statistische Schwächen zu erkennen. Der Anlauftest erfüllt somit die Eigenschaft P2.d)(ix). Das Offenlegen weniger offensichtlicher statistischer Schwächen bleibt den Onlinetests vorbehalten (vgl. auch [Sch]).

Zunächst wird der Basistest-Typ festgelegt. Dabei sollte das mathematische Modell der Rauschquelle berücksichtigt werden, da ein ungeeignet gewählter Basistest die Wirksamkeit der Onlinetests unter Umständen deutlich reduzieren kann. (Auf die Auswahl des Basistests wird im folgenden nicht näher eingegangen.) In diesem Beispiel ist der Basistest ein χ^2-Test über 128 (4-Bitworte).

Eine *Testsuite* besteht aus maximal N=512 Basistests (= χ^2-Tests über 128 (4-Bitworte)). Die Testgrößen der Basistests bezeichnen wir im folgenden mit $C_1,C_2,....$ Ferner gelte $H_0:=EW_0(C_1)$ (=Erwartungswert der Basistestgröße unter der Nullhypothese) und $H_j:=(1-\beta)H_{j-1}+\beta C_j$ für $j\geq 1$ mit $\beta=2^{-6}$, wobei die Testgrößen C_j und H_j jeweils auf 6 Nachkommabits gerundet werden. (Dies ermöglicht insbesondere, dass die "Historienvariablen" $H_1,H_2,...$ mit einer Ganzzahlarithmetik berechnet werden können.) In jedem Schritt $1 \leq j \leq N$ gelten die beiden Auswertungsregeln:

(i) Ist $C_{j-2}, C_{j-1}, C_j > 26.75$, dann Rauschvoralarm

(ii) Ist $H_j \notin [13.0,17.0]$, dann Rauschvoralarm

Tritt innerhalb einer Testsuite kein Rauschvoralarm auf, beginnt nach 512 Basistests eine neue Testsuite. Jeder Rauschvoralarm führt zum Abbruch der laufenden Testsuite und zur Löschung des FIFOs, und der Rauschvoralarm wird protokolliert. Wurden drei aufeinanderfolgende Testsuiten wegen eines Rauschvoralarms abgebrochen, erfolgt ein Rauschalarm, und der TRNG wird mit einer entsprechenden Fehlermeldung stillgelegt.

Der Einfachheit halber wird im folgenden angenommen, dass die digitalisierten Rauschsignale unabhängig sind. Konkret:

Verteilungsannahme für die digitalisierte Rauschsignalfolge (in Beispiel E.7): Aufgrund des mathematischen Modells der Rauschquelle und statistischer Untersuchungen an Prototypen kann die Verteilung der digitalisierten Rauschsignalbits als stationär und unabhängig angesehen werden. Abhängigkeiten von Vorgängern konnten nicht festgestellt werden, und die untersuchten Prototypen erfüllten die

Anforderung P2.d)(vii). Die digitalisierte Rauschsignalfolge kann somit als Realisierung unabhängiger Zufallsvariablen angesehen werden, wobei die Wahrscheinlichkeit $\mu(1)$, mit der der Wert "1" angenommen wird, vom einzelnen Gerät abhängen und sich im Lauf der Zeit auch ändern kann (Alterungseffekte).

Vorgaben (für Beispiel E.7; vgl. auch P2.d)(xi)): Für die beabsichtigten Anwendungen ist es völlig ausreichend, falls $\mu(1) \in [0.49,0.51]$ gilt. Liegt diese Wahrscheinlichkeit außerhalb von [0.475,0.525], so sollen dies die Onlinetests bald erkennen und einen Rauschalarm auslösen.

Tabelle 1 enthält die Wahrscheinlichkeiten für einen Rauschvoralarm innerhalb einer Testsuite und die durchschnittliche Anzahl von Rauschalarmen pro Jahr. Dabei wurde angenommen, dass pro Tag 1584 Basistests durchgeführt werden (davon 144 anlassbezogen beim Auffüllen des FIFOs).

Tabelle 1

$\mu(1)$	Wahrscheinlicheit für einen Rauschvoralarm innerhalb einer Testsuite	Durchschnittliche Anzahl von Rauschalarmen pro Jahr
0.500	0.0162	0.0047
0.495 bzw. 0.505	0.0187	0.0072
0.490 bzw. 0.510	0.0292	0.027
0.485 bzw. 0.515	0.0794	0.52
0.480 bzw. 0.520	0.2954	21.1
0.475 bzw. 0.525	0.7670	
0.470 bzw. 0.530	0.9912	

Vergleich mit dem Onlinetest aus Beispiel 4.6: Dort erfolgt ein Rauschalarm, falls ein einziger Test einen Wert liefert, der größer als 65.0 ist. (Ferner wurden in Beispiel 4.6 die internen Zufallszahlen getestet.) Dies ist ein Ereignis, das zumindest unter der Nullhypothese (= unabhängige und gleichverteilte 4-Bitworte) sehr selten eintritt. Ein solches Vorgehen ist jedoch mit Nachteilen verbunden: Einerseits kennt man die Verteilung der Testgröße auch unter der Nullhypothese normalerweise nur asymptotisch, d.h. die Grenzverteilung bei gegen unendlich strebendem Stichprobenumfang (= χ^2-Verteilung mit 15 Freiheitsgraden). Bei kleinem Stichprobenumfang kann der relative Fehler $| p_{exakt} - p_{näherung} | / p_{näherung}$ für große Verwerfungsschranken jedoch groß sein. (Dabei bezeichnen p_{exakt} die exakte, $p_{näherung}$ die aus der χ^2-Verteilung errechnete, näherungsweise Verwerfungswahrscheinlichkeit.) Dies hat dann zur Folge, dass die Anzahl der Rauschalarme deutlich größer ist, als dies unter Berücksichtigung der asymptotischen Grenzverteilung zu erwarten ist. Wurde "knapp" kalkuliert, führt dies zu einer überhöhten Ausfall- bzw. Stilllegungsrate. (Beispielsweise liegt der relative

Fehler bei einer Stichprobengröße von 80 (4-Bitworten) für die Verwerfungsgrenze 65.0 bei 10.1. Der Onlinetest aus E.6 genügt den Anforderungen P1.d). Eine Erhöhung des Stichprobenumfangs erscheint dennoch sinnvoll.) Eine "großzügige" Kalkulation wiederum kann dazu führen, dass nichttolerierbare Schwächen nicht oder wenigstens erst sehr spät erkannt werden. Ferner sind kaum Aussagen zur Verwerfungswahrscheinlichkeit möglich, falls die der Stichprobe zugrundeliegende Verteilung von der Nullhypothese abweicht.

Bei dem in Beispiel 4.7 vorgeschlagenem Onlinetest-Verfahren ist die Situation günstiger: Unter der Nullhypothese ist $\text{Prob}(C_j > 26.75) \approx 0.03$. Hier hat die χ^2-Verteilung noch "Masse", und der relative Fehler ist gering. Auch die Entscheidungsregel (ii) hängt nicht vom Eintritt eines einzigen, sehr seltenen Ereignisses, sondern von der Aufeinanderfolge zahlreicher, für sich betrachtet, keineswegs seltener Ereignisse ab. Hierfür sorgt der kleine Gewichtungsfaktor β.

Weicht die Verteilung der zu testenden digitalisierten Rauschfolge von der Nullhypothese (unabhängig und gleichverteilt) ab, kann die Verteilungsfunktion der Testgröße näherungsweise mit Hilfe stochastischer Simulationen bestimmt werden (siehe z.B. [Dev]). Hierzu erzeugt man mit einem Pseudozufallszahlengenerator (z.B. mit einem linearen Kongruenzgenerator oder einem linearem Schieberegister; Unvorhersagbarkeitseigenschaften der Pseudozufallszahlen sind hier ohne Belang) Standardzufallszahlen, d.h. auf dem Intervall [0,1] gleichverteilte Pseudozufallszahlen. Hieraus leitet man gemäß der gewünschten Verteilung eine lange Bitfolge (z.B. (4*128)*1000000 Bit) ab, segmentiert diese Folge in Teilfolgen der Länge 512 Bit und wendet auf jedes Segment einen χ^2-Test an. Für die in Tabelle 1 berücksichtigten Verteilungen lieferten stochastische Simulationen die folgenden Wahrscheinlichkeiten, dass die Testgröße >26.75 ist: 0.0299 (Nullhypothese), 0.0303, 0.0331, 0.0371, 0.0416, 0.0526 und 0.0656 (Reihenfolge wie in Tabelle 1).

Die Basistestgrößen $C_1, C_2, \ldots$ können als Realisierungen unabhängiger Zufallsvariablen interpretiert werden. Die Entscheidungsregeln (i) und (ii) definieren eine homogene Markoffkette auf dem endlichem Zustandsraum $\Omega = \{(2^{-6}k, i) \mid k \in \mathbb{N},\ 2^{-6}k \in [13.0,17.0],\ 0 \le i \le 2\} \cup \{\omega\}$, wobei ω einen absorbierenden Zustand bezeichnet. Der Zustand (v,i) wird erreicht, falls die Historienvariable den Wert v annimmt und die letzten $i \le 2$ Testgrößen größer als 26.75 waren. Der absorbierende Zustand ω wird erreicht, falls ein Rauschvoralarm ausgelöst wird (vgl. auch [Sch]).

Der Onlinetest erfüllt die Anforderungen P2.d)(xi) und (xiii), und insofern die mathematische Nachbearbeitung der Anforderung P2.d)(viii) genügt, auch P1.d)(vi).

Für jeden Wert H_{j-1} verursacht $C_j \ge 269.5$ aufgrund der Entscheidungsregel (ii) stets einen Rauschvoralarm. Dies ist insbesondere garantiert, falls die letzten 220 Bit einer Stichprobe konstant 0 oder konstant 1 sind. Nach einem Totalausfall der Rauschquelle führt nicht notwendigerweise der aktuelle, spätestens aber der darauffolgende Basistest zu einem Rauschvoralarm. Zu diesem Zeitpunkt hat aber keine interne Zufallszahl, die nach Eintritt des Totalausfalls zum Auffüllen des FIFOs genutzt wurde, das FIFO

verlassen. Nach zwei weiteren Onlinetests wird der TRNG stillgelegt, ohne dass zuvor weitere interne Zufallszahlen ausgegeben wurden. Somit ist auch die Anforderung P2.d)(x) erfüllt.

F. Statistische Tests

Nachfolgend sind die statistischen Tests aufgelistet, die zur Verifikation der P1-spezifischen Eigenschaft P1.d)(i), (ii) und (v) und der P2-spezifischen Eigenschaften P2.d)(vii) und (xii) benötigt werden.

F.1 Bemerkung:

(i) Die Tests T0 bis T5 werden auf interne Zufallszahlen angewendet (siehe P1.i)). Unter der Annahme, dass die Folgen $w_1,\ldots,w_{2\wedge16}$ bzw. $b_1,\ldots,b_{20000}$ von idealen Rauschquellen erzeugt werden, ergeben sich folgende Verwerfungswahrscheinlichkeiten: Test T0: 2^{-17}, Test T1 bis T5: jeweils 10^{-6} .

(ii) Die Tests T6 und T8 werden auf digitalisierte Rauschsignalfolgen angewandt (siehe P1.i)). Unter der Annahme, dass die Folgen $w_1,\ldots, w_n$, bzw. $b_1,\ldots,b_{(Q+K)L}$ von idealen Rauschquellen erzeugt werden, sind die Verwerfungswahrscheinlichkeiten bei der in P2.i) gewählten Parameterwahl vernachlässigbar. Da digitalisierte Rauschfolgen realer TRNGs in aller Regel statistische Defekte aufweisen (Schiefe, Abhängigkeiten) sind die Verwerfungsgrenzen so gewählt, dass TRNGs mit tolerierbaren Schwächen diese Tests bestehen sollten (siehe P2.j)).

(iii) Die Tests T1 – T4 sind samt Bezeichnung und Verwerfungsgrenzen dem Dokument [FI140-1] (4.11.1) entnommen. Um einer denkbaren Konfusion vorzubeugen, sei präventiv darauf hingewiesen, dass in [FI140-2] ebenfalls die Tests T1-T4 beschrieben werden, allerdings mit anderen Verwerfungsgrenzen. Unter der Annahme, dass die Bitfolgen $b_1,\ldots,b_{20000}$ von einer idealen Rauschquelle erzeugt werden, betragen die Verwerfungswahrscheinlichkeiten in [FI140-2] pro Test 10^{-4}.

(iv) Der theoretische Hintergrund des Entropietests (Test T8) wird in [Cor] beschrieben.

Test T0 (Disjunktheitstest)

Die Folge $w_1,\ldots,w_{2\wedge16} \in \{0,1\}^{48}$ passiert den Disjunktheitstest, falls die Folgenglieder paarweise verschieden sind.

Test T1 (Monobittest)

$$X = \sum_{j=1}^{20000} b_j$$

Die Bitfolge $b_1,\ldots,b_{20000}$ passiert den Monobittest, falls $9654 < X < 10346$.

Test T2 (Pokertest)

Für $j = 1,\ldots,5000$ sei $c_j = 8\cdot b_{4j-3}+4\cdot b_{4j-2}+2\cdot b_{4j-1}+b_{4j}$. Ferner bezeichnet $f[i] := |\{j: c_j=i\}|$.

$$Y = (16/5000)\cdot\left(\sum_{i=0}^{15} f[i]^2\right) - 5000$$

Die Bitfolge $b_1,\ldots,b_{20000}$ passiert den Pokertest ($=\chi^2$-Anpassungstest mit 15 Freiheitsgraden), falls $1.03 < Y < 57.4$.

Test T3 (Runtest)

Ein Run bezeichnet eine maximale Teilfolge aufeinanderfolgender Nullen bzw. Einsen.

Die Bitfolge $b_1,\ldots,b_{20000}$ passiert den Runtest, falls die Anzahl der auftretenden Runlängen innerhalb der zulässigen Intervalle liegen, die nachfolgend spezifiziert werden. Die Null- und Einsruns werden getrennt ausgewertet.

Runlänge	zulässiges Intervall
1	2267-2733
2	1079-1421
3	502-748
4	233-402
5	90-223
≥ 6	90-233

Test T4 (Long Runtest)

Ein Run der Länge ≥ 34 wird als Long Run bezeichnet.

Die Bitfolge $b_1,\ldots,b_{20000}$ passiert den Long Runtest, falls kein Long Run auftritt.

Test T5 (Autokorrelationstest)

Für $\tau \in \{1,\ldots,5000\}$ ist $Z_t = \sum_{j=1}^{5000} (b_j \oplus b_{j+t})$.

Die Bitfolge $b_1,\ldots,b_{20000}$ passiert den Autokorrelationstest (mit Shift τ), falls $2326 < Z_t < 2674$. (Man beachte, dass die Teilfolge $b_{10001},\ldots,b_{20000}$ nicht in die Testgröße eingeht.)

Test T6 (Gleichverteilungstest)

Die Folge $w_1,\ldots,w_n \in \{0,1\}^k$ passiert den Gleichverteilungstest mit den Parametern (k,n,a), falls

(*) $\frac{1}{n} \cdot \left| j \le n \mid w_j = x \right| \in [2^{-k} - a, 2^{-k} + a]$ für alle $x \in \{0,1\}^k$

gilt.

Bemerkung: Für k=1 vereinfacht sich Bedingung (*) zu $\frac{1}{n} \cdot \left| j \le n \mid w_j = 1 \right| \in [2^{-k} - 0{,}5, 2^{-k} + 0{,}5]$. Gilt zudem n = 20000 und a = 0.0173, so entspricht der Gleichverteilungstest dem Monobittest T1.

Test T7 (Vergleichstest für Multinomialverteilungen)

Für jedes $i \in \{1,\ldots h\}$ nehme die n-elementige Stichprobe $w_{i1},\ldots,w_{i,n}$ Werte in der Menge {0,1,…,s-1} an. Die Nullhypothese besagt, dass die den einzelnen Stichproben zugrundeliegenden Multinomialverteilungen identisch sind. Für $t \in \{0,\ldots,s-1\}$ sei ferner $f_i[t] := |\{j: w_{ij}=t\}|$, und $p_t := (f_1[t]+\ldots+ f_h[t])/(hn)$ bezeichne die aus der Gesamtheit aller Stichproben ermittelte relative Häufigkeit für das Auftreten des Wertes t. Unter der Nullhypothese ist die Testgröße $\sum_{i=1,\ldots,h} \sum_{t=0,\ldots,s-1} (f_i[t] - np_t)^2 / np_t$ näherungsweise χ^2-verteilt mit (h-1)(s-1) Freiheitsgraden ([Ka], Test 76). Im Spezialfall h = s =2 und Signifikanzniveau α = 0.0001 (vgl. P2.i)(vii.c) und P2.i)(vii.d)) beträgt die Verwerfungsgrenze 15.13.

Test T8 (Entropietest)

Der Entropietest wird nach Coron [Cor] durchgeführt. Die Bitfolge $b_1,\ldots,b_{(Q+K)L}$ wird in nichtüberlappende Ausgabewörter $w_1,\ldots,w_{Q+K}$ der Länge L segmentiert. Es bezeichnet A_n den Abstand von w_n zu seinem wertgleichen Vorgänger, und zwar ist

$$A_n = \begin{cases} n & \text{wenn kein } i \le n \text{ existiert mit } b_n = b_{n-i} \\ \min\{i \mid i \ge 1,\ w_n = w_{n-i}\} & \text{sonst} \end{cases}$$

- Die Testgröße f: $\{0,1\}^{(Q+K)L} \rightarrow$R ist für den Coron-Test durch

$$f_C(\bar{s}) = \frac{1}{K}\sum_{n=Q+1}^{Q+K} g(A_n), \text{ mit } g(i) = \frac{1}{\log(2)}\sum_{k=1}^{i-1}\frac{1}{k},$$

gegeben. Für $i \geq 23$ kann die Summe in der Funktion $g(i)$ mit einem Fehler unter 10^{-8} durch

$$\sum_{j=1}^{n}\frac{1}{j} = \log n + g + \frac{1}{2n} + \frac{1}{12n^2} + \mathrm{O}\left(\frac{1}{n^4}\right),\ g \approx 0{,}577216 \text{ (EULERSCHE Konstante)}$$

abgeschätzt werden.

Für eine stationäre, binärwertige Zufallsquelle mit endlichem Gedächtnis ist der Erwartungswert der Testgröße f_C eng mit dem Entropiezuwachs pro L-Bit Block verknüpft. Ist die Rauschquelle sogar unabhängig, gilt die Gleichheit. Für ideale Rauschquellen wird die Verteilung der Testgröße f_C in guter Näherung durch eine Normalverteilung mit Erwartungswert μ_C und Varianz $(\sigma_C)^2$ approximiert

$$s_C = c_C(L,K)\sqrt{Var\left(g(A_n)\right)/K},\quad c_C(L,K) = d(L) + \frac{e(L)\cdot 2^L}{K}$$

Tabelle 2 (Die Werte gelten für ideale Rauschquelle ([Cor]))

L	Varianz Var($g(A_n)$)	d(L)	e(L)
3	2.5769918	0.3313257	0.4381809
4	2.9191004	0.3516506	0.4050170
5	3.1291382	0.3660832	0.3856668
6	3.2547450	0.3758725	0.3743782
7	3.3282150	0.3822459	0.3678269
8	3.3704039	0.3862500	0.3640569
9	3.3942629	0.3886906	0.3619091
10	3.4075860	0.3901408	0.3606982
11	3.4149476	0.3909846	0.3600222
12	3.4189794	0.3914671	0.3596484
13	3.4211711	0.3917390	0.3594433
14	3.4223549	0.3918905	0.3593316
15	3.4229908	0.3919740	0.3592712
16	3.4233308	0.3920198	0.3592384

unendlich	3.4237147	0.3920729	0.3592016

Beispiel: Für L=8, K=256000 ist $\sigma_C \approx 0.0014$.

Im Gegensatz zum Maurertest ([Mau], [CoNa]) liefert der Coronsche Test zumindest bei unabhängigen Zufallsfolgen nicht nur asymptotische Entropieaussagen. Für den Maurertest liegt eine Implementierung durch das NIST auf http://csrc.nist.gov/rng/ [STS] vor.

G. Literatur

[AIS20] AIS 20 (Version 1 vom 02.12.99): Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren.

[CC] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; May 1999 und ISO 15408-2:1999.

[Cor] J.-S. Coron: On the Security of Random Sources, Gemplus' Corporate Product R&D Division, Technical Report IT02-1998.

Auch in: H. Imai und Y. Zheng (Hrsg.): Public Key Cryptography. Second International Workshop on Practice and Theory in Public Key Cryptography, PKC‘99. Springer, Lecture Notes in Computer Science 1560, Berlin 1999, 29-42.

[CoNa] J.-S. Coron and D. Naccache: An Accurate Evaluation of Maurer’s Universal Test. In: S. Tavares and H. Meijer (Hrsg.): Selected Areas in Cryptography ’98, SAC ’98. Springer, Lecture Notes in Computer Science, Vol 1556, Berlin 1999, 57-71.

[FI140-1] FIPS PUB 140-1 (January 11, 1994), NIST, Security Requirements for Cryptographic Modules.

[FI140-2] FIPS PUB 140-2 1999, NIST, Security Requirements for Cryptographic Modules.

[FI186] FIPS PUB 186-1 (December 15, 1998), NIST, Specifications for the Digital Signature Standard (DSS).

[ITSEC] Information Technology Security Evaluation Criteria (ITSEC); Provisional Harmonised Criteria, Version 1.2, June 1991.

[ITSEM] Information Technology Security Evaluation Manual (ITSEM); Provisional Harmonised Methodology, Version 1.0, September 1993.

[JIL] Information Technology Security Evaluation Criteria ITSEC Joint Interpretation Library (ITSEC JIL), Version 2.0, November 1998.

[Ka] G.K. Kanji: 100 Statistical Tests. Sage Publications, London 1995.

[Mau] U. Maurer: A Universal Statistical Test for Random Bit Generators. J. Cryptology (1992), 89-105.

[RSA] PKCS#1: RSA Encryption Standard. An RSA Laboratories Technical Note, Version 1.5, November 1, 1993.

[Sch] W. Schindler: Efficient Online Tests for True Random Number Generators. Erscheint in: C.K. Koc, D. Naccache, C. Paar (Hrsg.): Cryptographic Hardware and Embedded Systems – CHES 2001, Springer, Lecture Notes in Computer Science, Vol. 2162, Berlin 2001.

[STS] A Statistical Test Suite for Random and Pseudorandom Numbers. NIST Special Publication 800-22 (December 2000).