TCVN TIÊU CHUẨN QUỐC GIA

TCVN 13721:2023
ISO/IEC 20543:2019

Xuất bản lần 1

KỸ THUẬT AN TOÀN CÔNG NGHỆ THÔNG TIN – PHƯƠNG PHÁP KIỂM THỬ VÀ PHÂN TÍCH CHO CÁC BỘ TẠO BIT NGẪU NHIÊN TRONG TCVN 11295 (ISO/IEC 19790) VÀ TCVN 8709 (ISO/IEC 15408)

Information technology – Security techniques – Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

HÀ NỘI – 2023

Mục lục

Lời nói đầu

TCVN 13721:2023 hoàn toàn tương đương với ISO/IEC 20543:2019.

TCVN 13721:2023 do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã biên soạn, Ban Cơ yếu Chính phủ đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Giới thiệu

Các ứng dụng mật mã đòi hỏi các số ngẫu nhiên cho nhiều tác vụ khác nhau. Một bộ tạo bit ngẫu nhiên (RBG) mật mã mạnh phù hợp với các ứng dụng mật mã nói chung, bộ tạo bit ngẫu nhiên đó được kỳ vọng sẽ cung cấp các chuỗi bit đầu ra không thể phân biệt được với các chuỗi bit có cùng độ dài được lấy ngẫu nhiên đều với bất kỳ khả năng tính toán thực tế và với bất kỳ kích cỡ mẫu thực tế. Hơn nữa, một RBG như vậy được kỳ vọng sẽ cung cấp khả năng độ an toàn phía trước nâng cao và độ an toàn phía sau nâng cao.

Kỹ thuật an toàn công nghệ thông tin – Phương pháp kiểm thử và phân tích cho các bộ tạo bit ngẫu nhiên trong TCVN 11295 (ISO/IEC 19790) và TCVN 8709 (ISO/IEC 15408)

Information technology – Security techniques – Test and analysis methods for random bit generators with in ISO/IEC 19790 and ISO/IEC 15408

1 Phạm vi áp dụng

Tiêu chuẩn này quy định một phương pháp luận để đánh giá các bộ tạo bit ngẫu nhiên tất định hoặc bộ tạo bit ngẫu nhiên bất định được dự định sử dụng cho các ứng dụng mật mã. Các quy định được đưa ra trong tiêu chuẩn này cho phép nhà cung cấp RBG gửi các công bố về an toàn đã được xác định rõ ràng cho cơ quan đánh giá và sẽ cho phép đánh giá viên hoặc kiểm thử viên, ví dụ như: cơ quan xác nhận, đánh giá, kiểm thử, chứng nhận hoặc bác bỏ các công bố này.

Tiêu chuẩn này được triển khai độc lập, không phụ thuộc vào công nghệ và thiết kế. Do đó, nó không cung cấp hướng dẫn cụ thể về các quyết định thiết kế và triển khai cho bộ tạo bit ngẫu nhiên. Tuy nhiên, các vấn đề về thiết kế và triển khai ảnh hưởng đến việc đánh giá RBG trong tiêu chuẩn này, chẳng hạn vì nó yêu cầu sử dụng mô hình ngẫu nhiên của nguồn ngẫu nhiên và vì bất kỳ mô hình nào như vậy đều được hỗ trợ bởi các lập luận kỹ thuật liên quan đến thiết kế của thiết bị.

Bộ tạo bit ngẫu nhiên như được đánh giá trong tiêu chuẩn này nhằm mục đích đưa ra các chuỗi bit phân bố đều. Tuy nhiên, tùy thuộc vào sự phân bố các số ngẫu nhiên mà ứng dụng yêu cầu sử dụng, cần lưu ý rằng các bước bổ sung có thể cần thiết (và có thể rất quan trọng đối với an toàn) để ứng dụng sử dụng biến đổi các chuỗi bit ngẫu nhiên do RBG tạo ra thành số lượng ngẫu nhiên phân phối phù hợp với các yêu cầu ứng dụng. Các biến đổi tiếp theo như vậy nằm ngoài phạm vi đánh giá được thực hiện trong tiêu chuẩn này.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu có ghi năm công bố thì áp dụng phiên bản đã nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả sửa đổi, bổ sung).

- TCVN 8709 (ISO/IEC 15408), Công nghệ thông tin - Kỹ thuật an toàn - Tiêu chí đánh giá về an toàn công nghệ thông tin.
- TCVN 12212:2018 (ISO/IEC 17825:2016), Công nghệ thông tin - Kỹ thuật an toàn - Phương pháp kiểm thử để giảm thiểu các lớp tấn công không xâm lấn chống lại các mô-đun mật mã.
- TCVN 12853:2020 (ISO/IEC 18031:2011), Công nghệ thông tin - Kỹ thuật an toàn - Bộ tạo bit ngẫu nhiên.
- TCVN 11295:2016 (ISO 19790:2012), Công nghệ thông tin - Kỹ thuật an toàn - Yêu cầu an toàn đối với mô-đun mật mã.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các định nghĩa và thuật ngữ sau đây:

3.1

Độ an toàn phía trước (backward secrecy)

Đảm bảo rằng các giá trị trước đó không thể xác định được từ các thông tin của giá trị đầu ra hiện tại hoặc các giá trị tiếp theo.

[Nguồn: 3.2, TCVN 12853:2020 (ISO/IEC 18031:2011)]

3.2

Dòng bit (bit stream)

Các bit đầu ra liên tục từ một thiết bị hoặc một cơ chế.

[Nguồn: 3.4, TCVN 12853:2020 (ISO/IEC 18031:2011)]

3.3

Hộp đen (black box)

Cơ chế lý tưởng chấp nhận các giá trị đầu vào và tạo các giá trị đầu ra, nhưng được thiết kế sao cho người quan sát không thể nhìn thấy bên trong hộp hoặc xác định chính xác điều gì đang xảy ra bên trong hộp đó.

CHÚ THÍCH 1: Thuật ngữ này hoàn toàn trái ngược đối với hộp trắng (3.13).

[Nguồn: 3.6, TCVN 12853:2020 (ISO/IEC 18031:2011)]

3.4

Kiểm thử viên sự phù hợp (conformance-tester)

Kiểm thử viên (tester)

Cá nhân được giao thực hiện các hoạt động kiểm thử tương ứng với một tiêu chuẩn kiểm tra sự phù hợp nhất định và phương pháp kiểm tra tương ứng.

Ví dụ: Một ví dụ giống như trong TCVN 11295:2016 (ISO 19790:2012) và phương pháp kiểm tra được quy định trong TCVN 11295:2016 (ISO 19790:2012).

[Nguồn: 3.2, TCVN 13723-1:2023 (ISO/IEC 19896-1:2018)]

3.5

Bộ tạo bit ngẫu nhiên tất định (deterministic random bit generator)

DRBG

Bộ tạo bit ngẫu nhiên tạo ra một chuỗi bit xuất hiện ngẫu nhiên bằng cách sử dụng một thuật toán tất định từ một giá trị khởi tạo ngẫu nhiên thích hợp được gọi là mầm và có thể gồm một số đầu vào thứ cấp mà không ảnh hưởng đến độ an toàn của bộ tạo bit ngẫu nhiên.

CHÚ THÍCH 1: Các nguồn bất định cũng có thể là một phần của các đầu vào thứ cấp này.

CHÚ THÍCH 2: Tính an toàn của bộ tạo bit ngẫu nhiên xác định chủ yếu dựa vào độ an toàn của các thuật toán mật mã được sử dụng và tính ngẫu nhiên có trong giá trị mầm. Trong một bộ tạo bit ngẫu nhiên tất định thích hợp cho ứng dụng mật mã, ít nhất phải đảm bảo độ an toàn phía sau và độ an toàn phía trước mà không cần gọi các đầu vào thứ cấp cho RBG hoặc thay mầm mới.

[Nguồn: 3.10, TCVN 12853:2020 (ISO/IEC 18031:2011)]

3.6

Độ an toàn phía trước nâng cao (enhanced backward secrecy)

Đảm bảo rằng kiến thức về trạng thái hiện tại bên trong của bộ tạo bit ngẫu nhiên không cho phép kẻ tấn công thu được kiến thức về các giá trị đầu ra trước đó bằng nỗ lực tính toán thực tế.

CHÚ THÍCH 1: Khái niệm về độ an toàn phía trước nâng cao là ít quan trọng đối với RBG không nhớ. Do đó, nó chỉ là một khái niệm hữu ích cho các bộ tạo bit ngẫu nhiên lai ghép và tất định, tính an toàn của chúng ít nhất một phần dựa vào các thuộc tính mật mã của hàm chuyển trạng thái và hàm tạo đầu ra của bộ tạo bit ngẫu nhiên.

3.7

Độ an toàn phía sau nâng cao (enhanced forward secrecy)

Đảm bảo rằng việc biết trạng thái hiện tại bên trong của bộ tạo bit ngẫu nhiên không mang lại các ràng buộc có liên quan thực tế đối với các giá trị đầu ra tiếp theo (trong tương lai).

CHÚ THÍCH 1: Bộ tạo bit ngẫu nhiên tất định không thể đạt được độ an toàn phía sau nâng cao. Độ an toàn phía sau nâng cao phụ thuộc hoàn toàn vào khả năng của quá trình thay mầm mới liên tục để cung cấp entropy nhiều nhất theo yêu cầu để làm cho việc dự đoán đầu ra trong tương lai không khả thi.

CHÚ THÍCH 2: Một bộ tạo ngẫu nhiên có thể đạt được độ an toàn phía trước nâng cao nhưng vẫn mở rộng entropy, tức là tạo ra một chuỗi bit về nguyên tắc có thể được nén đáng kể. Ví dụ, người ta có thể xem xét thiết kế RBG với nguồn ngẫu nhiên tạo ra tại mỗi lần gọi một chuỗi ngẫu nhiên R có độ dài 128-bit với ước tính min entropy 120-bit, với trạng

thái bên trong $S(n)$ có độ dài 512-bit, một hàm chuyển trạng thái cho $S(n+1) := SHA3-512(S(n)||R)$ và một hàm tạo đầu ra áp dụng SHAKE-256 trên $S(n)||R$ với đầu ra lên đến 1024-bit cho mỗi lần gọi.

CHÚ THÍCH 3: Một thuật ngữ khác hay được tìm thấy trong các tài liệu có thể thay thế cho việc độ an toàn phía sau nâng cao là tính kháng dự đoán.

3.8

Entropy (Entropy)

Độ đo sự hỗn loạn, tính ngẫu nhiên hoặc biến đổi trong một hệ thống đóng.

CHÚ THÍCH 1: Có nhiều khái niệm khác nhau về entropy đóng vai trò trong mật mã. Đáng nói trong số đó là: entropy theo Shannon, min entropy, va chạm entropy, entropy dự đoán, thuật toán entropy và entropy Renyi (khái niệm sau là các trường hợp đặc biệt của entropy theo Shannon, min entropy và va chạm entropy).

CHÚ THÍCH 2: Lượng entropy chứa trong một chuỗi bit chưa biết luôn liên quan đến người quan sát. Đánh giá RBG thiết lập các ước lượng entropy khi đối với kẻ tấn công có kiến thức chi tiết về nguồn entropy và cũng xem xét khả năng của nó để quan sát hoặc tác động đến trạng thái của nguồn entropy.

CHÚ THÍCH 3: Không phân biệt loại entropy đã chọn, thuật ngữ "entropy đầy đủ" luôn có nghĩa giống nhau, cụ thể là các số ngẫu nhiên độc lập và phân bố đồng đều, tức là ngẫu nhiên lý tưởng.

CHÚ THÍCH 4: Một thuật toán entropy là một logarit đến cơ số 2 của độ dài của mã hóa ngắn nhất trong một số ngôn ngữ hình thức nhất định. Độ đo của nó dựa trên khái niệm về độ nén tối ưu. Thuật toán entropy của một chuỗi bit phụ thuộc vào ngôn ngữ hình thức cơ bản và thậm chí được cung cấp cho một ngôn ngữ hình thức được xác định rõ ràng, nói chung là không thể tính toán trừ khi ngôn ngữ bị hạn chế rất nhiều. Tuy nhiên, các khái niệm liên quan là phù hợp trong bối cảnh mật mã. Ví dụ, người ta có thể hỏi có thể nén bao nhiêu chuỗi số ngẫu nhiên thô bất nguồn từ một số nguồn nhiễu vật lý bằng cách sử dụng một số chiến lược nén hiệu quả về mặt tính toán cố định được thông báo bởi sự hiểu biết chính xác về nguồn nhiễu vật lý và quá trình chuyển đổi đầu ra của nguồn nhiễu thành các số ngẫu nhiên thô.

3.9

Nguồn entropy (entropy source)

Thành phần, thiết bị hoặc sự kiện tạo đầu ra theo một số cách nhất định nào đó, tạo ra một xâu bit chưa entropy.

CHÚ THÍCH 1: Trong phạm vi của bộ tạo bit ngẫu nhiên tất định thuần túy, việc tạo entropy có thể được thực hiện chỉ một lần và trong trường hợp này, thiết bị tạo bit ngẫu nhiên có thể không chứa nguồn entropy. Tuy nhiên, nguồn entropy được sử dụng bởi một bộ tạo bit ngẫu nhiên như vậy cần phải được đánh giá theo cùng các tiêu chuẩn được yêu cầu.

CHÚ THÍCH 2: Trong một số trường hợp, có thể chấp nhận bộ tạo bit ngẫu nhiên tất định được nạp mầm với entropy được tạo bên ngoài thay vì chứa phần cứng tạo ra entropy bên trong chính bộ tạo bit ngẫu nhiên đó. Trong trường hợp đó, entropy được tạo ra bên ngoài sẽ chỉ có sẵn đối với bộ tạo bit ngẫu nhiên nhằm mục đích chứng minh.

3.10

Đánh giá viên (evaluator)

Cá nhân được giao thực hiện đánh giá với một tiêu chuẩn đánh giá nhất định và phương pháp đánh giá liên quan.

CHÚ THÍCH 1: Ví dụ về tiêu chuẩn đánh giá là TCVN 8709 (ISO/IEC 15408) với phương pháp đánh giá liên quan được đưa ra trong TCVN 11386:2016 (ISO/IEC 18045:2008).

[Nguồn: 3.5, TCVN 13723-1:2023 (ISO/IEC 19896-1:2018)]

3.11

Độ an toàn phía sau (forward secrecy)

Đảm bảo rằng thông tin của các giá trị tiếp theo (tương lai) không thể được xác định từ các giá trị hiện tại hoặc các giá trị trước đó.

[Nguồn: 3.13, TCVN 12853:2020]

3.12

Hộp trắng (glass box)

Cơ chế lý tưởng chấp nhận các giá trị đầu vào và tạo các giá trị đầu ra và được thiết kế sao cho người quan sát có thể nhìn thấy bên trong và xác định chính xác điều gì đang xảy ra.

Chú thích 1: Thuật ngữ này hoàn toàn trái ngược với Hộp đen (3.3).

[Nguồn: 3.12, TCVN 11367-2:2016]

3.13

Kiểm tra chất lượng (health test),

Kiểm tra trực tuyến và kiểm tra tổng số lỗi (online test and total failure test)

Bất kỳ cơ chế nào (thử nghiệm thống kê hoặc cách khác) phát hiện ít nhất một trong hai trường hợp sau:

a) Sự cố tạm thời hoặc vĩnh viễn của nguồn entropy, tức là một sự giảm mạnh entropy biểu hiện ở một số lượng nhỏ các dấu hiệu dễ phát hiện.
b) Độ lệch nhỏ hơn so với trạng thái bình thường của nguồn entropy, nhưng không thể chấp nhận được, điều này làm giảm các tuyên bố về an toàn do nhà cung cấp đưa ra. Ngược lại với lỗi toàn bộ, nó thường yêu cầu cỡ mẫu lớn hơn một chút cho đến khi những sai lệch này được phát hiện một cách đáng tin cậy.

3.14

Phân phối độc lập và đồng nhất (independent and identically distributed)

IID

Thuộc tính của một họ các biến ngẫu nhiên nói rằng chúng có cùng phân phối và độc lập với nhau đôi một.

3.15

Phòng thử nghiệm (laboratory)

Tổ chức có hệ thống quản lý cung cấp công việc đánh giá hoặc kiểm thử sự phù hợp với bộ chính sách, thủ tục được xác định và sử dụng một phương pháp luận được xác định để kiểm thử hoặc đánh giá chức năng an toàn của các sản phẩm công nghệ thông tin (CNTT).

CHÚ THÍCH 1: Các tổ chức này thường được các cơ quan phê duyệt khác nhau đặt cho các tên thay thế. Ví dụ: Cơ sở đánh giá an toàn CNTT (ITSEF), Phòng thử nghiệm kiểm tra tiêu chí chung (CCTL), Cơ sở đánh giá Thương mại (CLEF).

[Nguồn: 3.8, TCVN 13723-1:2023 (ISO/IEC 19896-1:2018)]

3.16

Min entropy (min entropy)

Min entropy của một biến ngẫu nhiên hữu hạn X là $-log2(p\_max)$ trong đó p_max biểu thị xác suất của kết quả có khả năng xảy ra lớn nhất. Tức là $p\_max >= p\_x$ với mọi x.

3.17

Entropy dự đoán (guessing entropy)

Sự phỏng đoán (guess work)

<cho X> là số kỳ vọng mà một kẻ tấn công thực hiện một chiến lược dự đoán tối ưu cần phải đưa ra để đoán giá trị của x [19], với X là một biến hữu hạn ngẫu nhiên và x là giá trị hiện thực hóa của X (một biến ngẫu nhiên tương ứng).

CHÚ THÍCH 1: Công thức cho entropy dự đoán là: $\sum\_i = 1^n ip\_i$, trong đó: p_i được sắp xếp $p\_1 >= p\_2 >= ...$ (nghĩa là, chiến lược tối ưu này dự đoán các kết quả có khả năng xảy ra lớn nhất trước).

3.18

Bộ tạo bit ngẫu nhiên bất định không chuyên dụng (non-dedicated non-deterministic random bit generator)

NNRBG

Bộ tạo bit ngẫu nhiên bất định, tính an toàn của nó không dựa trên tính ngẫu nhiên được tạo ra bởi phần cứng được thiết kế rõ ràng để tạo ra tính ngẫu nhiên

CHÚ THÍCH 1: TNRBG là viết tắt của Bộ tạo bit ngẫu nhiên bất định chuyên dụng và NNRBG là viết tắt của Bộ tạo bit ngẫu nhiên bất định không chuyên dụng.

3.19

Bộ tạo bit ngẫu nhiên bất định (non-deterministic random bit generator)

NRBG

Bộ tạo bit ngẫu nhiên liên tục lấy mẫu nhiều nguồn entropy và nếu hoạt động chính xác sẽ tạo đầu ra không thể dự đoán được đối với những kẻ tấn công có khả năng tính toán không giới hạn trong khoảng thời gian ngắn.

3.20

Độ an toàn phía sau lý trưởng (perfect forward secrecy)

Tính chất của một giao thức mật mã, theo đó kẻ tấn công không thể xâm phạm các lần chạy trước đây của giao thức bằng cách tìm hiểu các khóa bí mật dài hạn của những bên tham gia.

3.21

Nguồn entropy vật lý (physical entropy source)

Nguồn entropy dựa trên việc sử dụng hiệu ứng vật lý chuyên dụng (ví dụ: diode nhiễu, phân rã hạt nhân, ...)

3.22

Nguồn nhiễu (noise source)

Yếu tố của hệ thống kỹ thuật hoặc môi trường của nó tạo ra đầu ra không thể dự đoán được. Trong tiêu chuẩn này, "nguồn nhiễu" và "nguồn entropy" được coi là nguồn entropy.

3.23

Nguồn entropy phi vật lý (non-physical entropy source)

Nguồn entropy không dựa trên hệ thống vật lý chuyên dụng mà dựa trên những phần không thể dự đoán trướccủa môi trường hoặc các thành phần kỹ thuật không được thiết kế ban đầu để tạo bit ngẫu nhiên.

CHÚ THÍCH 1: Ví dụ có thể là thông tin được người dùng nhập vào hoặc tập hợp các dữ liệu hệ thống khác nhau khó có thể dự đoán (ví dụ: thời gian truy cập ổ cứng, nhiễu từ thiết bị cảm biến, hệ thống ngắt) trong một máy tính tiêu chuẩn.

3.24

Hậu xử lý (post-processing)

Một phần của bộ tạo bit ngẫu nhiên xử lý đầu ra của nguồn ngẫu nhiên với mục đích loại bỏ sự phụ thuộc giữa các bit ngẫu nhiên hoặc phân bố đều. Thường được gọi là một thành phần điều chế.

3.25

Bộ tạo bit ngẫu nhiên (random bit generator)

RBG

Thiết bị hoặc thuật toán có đầu ra là một chuỗi bit xuất hiện độc lập và đồng xác suất.

CHÚ THÍCH 1: Trong trường hợp bộ tạo bit ngẫu nhiên thuần túy vật lý, có thể cho phép việc hao hụt entropy với một lượng rất nhỏ. Mặt khác, trong thực tế các cấu trúc RBG tất định sẽ cung cấp đầu ra không thể phân biệt được về mặt tính toán với những dữ liệu được phân phối lý tưởng. Ngoài ra, cần lưu ý rằng việc thiết kế kết hợp có lợi thế hơn so với cả thiết kế thuần túy tất định và thiết kế thuần túy vật lý bằng cách kết hợp entropy thực được đảm bảo bởi các RBG vật lý với đầu ra của RBG tất định phân phối gần như lý tưởng và tái sử dụng thuộc tính, Ví dụ: liên quan đến lỗi nguồn nhiễu.

3.26

Số ngẫu nhiên thô (raw random numbers)

Chuỗi bit được tạo ra bên trong bộ tạo bit ngẫu nhiên bằng cách số hóa nguồn nhiễu ngẫu nhiên hoặc phát hiện các sự kiện không thể đoán trước trong máy được đề cập, trước khi thực hiện bất kỳ quá trình hậu xử lý nào ngoài số hóa.

CHÚ THÍCH 1: Cần lưu ý rằng mặc dù các số ngẫu nhiên thô đại diện cho giai đoạn đầu của quá trình tạo bit ngẫu nhiên, các số ngẫu nhiên thô này có thể bao gồm mô hình giả ngẫu nhiên phức tạp bên trong. Ví dụ, một phần của sự ngẫu nhiên trong thời gian tìm kiếm xảy ra với ổ cứng thường liên quan đến các sơ đồ lưu thoát không khí hỗn loạn bên trong ổ cứng; ngay cả khi người ta loại bỏ tất cả các tính năng khác của ổ cứng, có vẻ như khó lập luận rằng một RBG dựa trên hiệu ứng này không có bộ nhớ trong đáng kể. Tuy nhiên, các nguồn có bộ nhớ trong lớn nổi tiếng là khó xác định đúng đặc tính bằng các thử nghiệm thống kê với kích thước mẫu thực tế. Do đó, mức độ mà các mẫu giả ngẫu nhiên được thể hiện bởi một nguồn ngẫu nhiên thô, phụ thuộc vào thiết kế của nguồn entropy và sẽ được xem xét khi phân tích nó. Các thử nghiệm thống kê tổng quát có thể nhầm giữa giả ngẫu nhiên với ngẫu nhiên thực sự và do đó đánh giá quá cao entropy của các số ngẫu nhiên thô. Chính vì lý do này mà điều quan trọng là phải hiểu thiết kế của cơ chế tạo ra các số ngẫu nhiên thô. Điều này bao gồm các ảnh hưởng của chính các cơ chế số hóa, ví dụ: độ phân giải và độ phi tuyến của bộ chuyển đổi A/D (tín hiệu tương tự sang tín hiệu số) hoặc nhiễu do mạch khuếch đại tạo ra.

3.27

Mức an toàn (security strength)

Số tự nhiên lớn nhất *n*, sao cho kẻ tấn công không bị ràng buộc về mặt tính toán không thể phân biệt với lợi thế không đáng kể là giá trị *n-bit* do RBG tạo ra từ giá trị *n-bit* được lấy ngẫu nhiên đồng nhất, khi có phân phối trước của trạng thái thực bên trong RBG.

CHÚ THÍCH 1: Nếu không tồn tại số *n* như vậy, mức an toàn được cho là vô cùng.

CHÚ THÍCH 2: Chỉ bộ tạo bit ngẫu nhiên lai ghép hoặc vật lý mới có thể có mức an toàn được hỗ trợ tối đa, vì bộ tạo bit ngẫu nhiên tất định luôn dựa vào giá trị mầm khởi tạo. Tuy nhiên, cần lưu ý rằng đầu ra của bộ tạo bit ngẫu nhiên vật lý thuần túy thường có thể được phân biệt với dữ liệu ngẫu nhiên trong thực tế nếu kẻ tấn công biết thiết kế của bất kỳ bước điều chỉnh nào có thể được thực hiện.

3.28

Entropy theo Shannon (Shannon entropy)

<cho một biến ngẫu nhiên hữu hạn X> giá trị kỳ vọng của $-log2\ (px)$, trong đó: px là xác suất giá trị được quan sát thực tế $X\ =\ x$.

CHÚ THÍCH 1: Nói cách khác, đối với một biến ngẫu nhiên hữu hạn X với miền giá trị S mà Entropy theo Shannon $H(X)$ được cho bởi công thức $H(X) = -\sum x \in S\ .px\ .log2(px)$, trong đó với mục đích tính toán giá trị kỳ vọng, người ta thông qua quy ước rằng $0 * log2(0)\ =\ 0$.

3.29

Tính ổn định (stationarity)

Thuộc tính của một quá trình ngẫu nhiên, theo đó sự phân phối chung của các trường hợp tiếp theo của quá trình là không thay đổi theo thời gian.

3.30

Mô hình ngẫu nhiên (stochastic model)

Mô tả một phần toán học của bộ tạo bit ngẫu nhiên dựa trên ít nhất sự hiểu biết định tính về nguồn entropy, cùng với một số dữ liệu có thể được thu thập theo kinh nghiệm để ước tính tham số, cho phép suy ra các tuyên bố về entropy

CHÚ THÍCH 1: Trong phạm vi đánh giá bộ tạo bit ngẫu nhiên, mô hình ngẫu nhiên được khuyến nghị nhưng không bắt buộc mô tả trạng thái của các bit ngẫu nhiên thô. Quá trình hậu xử lý sau đó có thể gây khó khăn hơn trong trường hợp đưa ra thuyết phục rằng mô hình ngẫu nhiên tương ứng có khả năng phù hợp với hoạt động của thiết bị được mô hình hóa để hỗ trợ các tuyên bố về entropy được chỉ ra. Ví dụ: một mô hình ngẫu nhiên được áp dụng cho các số ngẫu nhiên đầu ra của bộ tạo bit ngẫu nhiên tất định về cơ bản sẽ không thể kiểm chứng được về mặt thống kê vì quá trình hậu xử lý mật mã mạnh có thể khiến dữ liệu entropy rất thấp không thể phân biệt được với nhiễu ngẫu nhiên ở kích thước mẫu thực tế, ít nhất là từ góc nhìn của bất kỳ kẻ tấn công nào thiếu mô hình ngẫu nhiên của các số ngẫu nhiên thô.

3.31

Bộ tạo bit ngẫu nhiên bất định chuyên dụng (true dedicated non-deterministic random bit generator)

TNRBG

Bộ tạo bit ngẫu nhiên bất định, tính an toàn của nó dựa trên thành phần phần cứng đã được thiết kế rõ ràng để tạo ra tính ngẫu nhiên.

CHÚ THÍCH 1: TNRBG là viết tắt của Bộ tạo bit ngẫu nhiên bất định chuyên dụng và và NNRBG là viết tắt của Bộ tạo bit ngẫu nhiên bất định không chuyên dụng.

3.32

Thẩm quyền kiểm tra hợp lệ (validation authority)

Tổ chức sẽ xác nhận kết quả kiểm thử về sự phù hợp với TCVN 11295:2016 (ISO/IEC 19790:2012).

[Nguồn: 3.132, TCVN 11295:2016 (ISO/IEC 19790:2012)]

3.33

Nhà cung cấp (vendor)

Thực thể, nhóm hoặc hiệp hội gửi mô-đun mật mã để kiểm thử và xác thực.

CHÚ THÍCH 1: Nhà cung cấp có quyền truy cập vào tất cả các tài liệu liên quan và bằng chứng thiết kế bất kể họ có thiết kế hay không thiết kế hoặc phát triển mô-đun mật mã hay không.

[Nguồn: 3.133, TCVN 11295:2016 (ISO/IEC 19790:2012)]

4 Ký hiệu và thuật ngữ viết tắt

CCTL	Common Criteria Testing Laboratory	Phòng thử nghiệm kiểm tra tiêu chí chung
CLEF	Commercial Evaluation Facility	Cơ sở đánh giá Thương mại
ITSEF	IT Security Evaluation Facility	Cơ sở đánh giá an toàn CNTT
LFSR	Linear Feedback Shift Register	Thanh ghi dịch phản hồi tuyến tính
OS	Operating System	Hệ điều hành
SHA	Secure Hash Algorithm	

5 Cấu trúc của tiêu chuẩn

Tiêu chuẩn này được chia thành 05 chủ đề sau: Tổng quan về bộ tạo bit ngẫu nhiên bất định; đánh giá sự phù hợp của NRBG; Tổng quan về bộ tạo bit ngẫu nhiên tất định; Đánh giá sự phù hợp của DRBG và phương pháp đánh giá. Mỗi mục tập trung vào các hoạt động thử nghiệm và đánh giá đối với các bộ tạo bit ngẫu nhiên về một kế hoạch đánh giá tuân thủ sử dụng TCVN 11295:2016 (ISO 19790:2012) và một kế hoạch đánh giá sử dụng TCVN 8709 (ISO/IEC 15408).

6 Tổng quan về bộ tạo bit ngẫu nhiên bất định

6.1 Nhận xét giới thiệu về tạo bit ngẫu nhiên

Điều khoản này trình bày các vấn đề của việc đánh giá bộ tạo bit ngẫu nhiên và các mục tiêu an toàn cần đạt được bằng cách xem xét sự phân bố của việc tung đồng xu. Một mặt của đồng xu được gọi là "mặt sấp" (H) và mặt kia được gọi là "mặt ngửa" (T). Tính ngẫu nhiên được tạo ra bằng cách tung đồng xu lên không trung và quan sát xem mặt nào ngửa khi nó tiếp đất.

Tung đồng xu nhiều lần tạo ra một chuỗi kết quả tung đồng xu theo thứ tự được ký hiệu là một chuỗi gồm "H" và "T". Ví dụ, chuỗi "HTTHT" (từ trái sang phải) biểu thị cho biết "mặt ngửa rồi đến mặt sấp, tiếp theo là mặt sấp, mặt ngửa rồi đến mặt sấp". Chuỗi biểu thị kết quả tung đồng xu này có thể được chuyển thành chuỗi nhị phân một cách đơn giản bằng cách gán H bằng số một nhị phân ("1") và T bằng số không nhị phân ("0"); chuỗi bit kết quả của ví dụ là "10010".

Các thuộc tính cần thiết của tính ngẫu nhiên có thể được kiểm tra bằng cách sử dụng ví dụ về thử nghiệm tung đồng xu được mô tả ở trên. Kết quả của mỗi lần tung xu, theo quan điểm của việc sử dụng đầu ra trong các ứng dụng mật mã, là:

- Không thể dự đoán trước: Trước khi tung, không xác định đồng xu sẽ tiếp đất cho kết quả sấp hay ngửa. Điều này, trong trường hợp tung đồng xu, phụ thuộc vào việc không biết đủ chính xác các thông số vật lý ban đầu của việc tung đồng xu như tốc độ ban đầu, độ cao so với mặt đất, đặc tính vật lý của mặt đất mà đồng xu sẽ nằm yên và tốc độ quay của đồng xu. Nếu có đủ entropy liên quan thấp trong các điều kiện ban đầu của lần lật, thì thử nghiệm trở nên có thể dự đoán được [8]; entropy có liên quan gì chỉ có thể được xác định bằng cách kiểm tra mô hình vật lý của quá trình tung đồng xu. Nhưng nếu các điều kiện ban đầu chứa đủ entropy liên quan, kết quả sẽ được giữ bí mật và nếu các điều kiện ban đầu không được lặp lại quá gần nhau theo cách có thể dự đoán được trong các thử nghiệm tiếp theo, thì không thể xác định được kết quả của việc tung đồng xu là gì, dựa trên hiểu biết về bất kỳ kết quả tiếp theo hoặc trước đó. Việc không thể đoán trước sau khi lật cũng phụ thuộc vào việc liệu kẻ tấn công có thể quan sát được kết quả của việc tung đồng xu hay không. Khái niệm định lượng entropy không thể đoán trước hoặc không chắc chắn liên quan đến người quan sát và được thảo luận kỹ hơn ở phần sau của tiêu chuẩn này;
- Đồng xác suất: Nghĩa là mỗi kết quả có thể đều có cơ hội xảy ra như nhau. Mức độ đúng của điều này phụ thuộc vào các yếu tố tương tự như đã liệt kê ở trên. Đồng xác suất theo nghĩa này có nghĩa là mỗi trường hợp của thử nghiệm tung đồng xu tuân theo một phân phối đồng nhất (trên hai kết quả có thể xảy ra là H và T) và do đó, một loạt các thử nghiệm tung đồng xu được phân phối đồng nhất vì mỗi thử nghiệm có cùng xác suất phân phối;
- Độc lập: Quá trình tung đồng xu được cho là quá trình không nhớ; bất cứ điều gì xảy ra trước khi lật hiện tại không ảnh hưởng đến nó. Điều này có đúng đối với một thử nghiệm tung đồng xu thực hay không phụ thuộc vào việc liệu tính ngẫu nhiên khi tham gia thử nghiệm thông qua các điều kiện ban đầu là không nhớ và có thể vào việc liệu bản thân đồng xu có thay đổi hay không, ví dụ: do hao mòn qua các lần thử nghiệm lặp đi lặp lại.

Mô phỏng một thử nghiệm tung đồng xu được lý tưởng hóa - tức là một nguồn ngẫu nhiên phát ra một dòng bit độc lập, đồng xác suất và phân phối đồng nhất - là những gì các ứng dụng mật mã nói chung có thể hướng tới. Lý do cho điều này là, trong khi một số ứng dụng mật mã có thể chịu được sự sai lệch đáng kể so với độ ngẫu nhiên lý tưởng (ví dụ: khóa AES-256 không thể vét cạn nếu các bit của nó là IID với 60,0%), những ứng dụng khác bắt đầu rò rỉ thông tin ngay cả khi có các phân bố nhỏ (ví dụ: lược đồ chia sẻ bí mật) hoặc thậm chí có thể bị phá vỡ khi một lượng nhỏ thông tin về các bí mật mật mã bị rò rỉ (ví dụ: ECDSA nonces [21]). Ngoài ra, mức an toàn được tuyên bố về mặt lý thuyết của bất kỳ cơ chế mật mã nào thường chỉ đạt được nếu các khóa được phân phối lý tưởng. Các RBG được đánh giá trong tiêu chuẩn này mô phỏng một loạt các lần tung đồng xu được lý tưởng hóa, ngay cả khi được giả định tốt về khả năng của bất kỳ kẻ tấn công nào.

Để đánh giá xem liệu bộ tạo bit ngẫu nhiên có cung cấp đủ tính ngẫu nhiên hay không, người ta cần phân tích các nguyên tắc hoạt động của thiết bị được đề cập để đi đến mô hình ngẫu nhiên lý tưởng cho các số ngẫu nhiên thô được tạo trong thiết bị. Dựa trên mô hình ngẫu nhiên này, các thử nghiệm thống kê sau đó có thể được chọn để cho phép đánh giá viên thu được các ước tính về entropy có trong các số ngẫu nhiên thô.

6.2 Mô hình hóa các nguồn ngẫu nhiên

6.2.1 Mô hình ngẫu nhiên

6.2.1.1 Yêu cầu chung

Điều khoản 6.2 trong tiêu chuẩn này sẽ giới thiệu các phương pháp được sử dụng trong việc lập mô hình các nguồn ngẫu nhiên để đánh giá và xác định các yêu cầu tài liệu và các hành vi của đánh giá viên liên quan đến các bước trong quá trình đánh giá bộ tạo bit ngẫu nhiên, trong đó kiểm tra tính chất ngẫu nhiên của nguồn entropy được hiểu đầy đủ để thực hiện kiểm thử. Do đó, điều khoản 6.2 không xác định các tiêu chuẩn chất lượng tối thiểu trên nguồn ngẫu nhiên. Thay vào đó, các tiêu chuẩn chất lượng như vậy được xác định bởi các yêu cầu đặt ra đối với các yêu cầu an toàn mà nhà cung cấp trình bày. Một cách trừu tượng để mô hình hóa một quá trình tạo ra

một tín hiệu ngẫu nhiên là sử dụng mô hình ngẫu nhiên. Theo điều khoản 3.26, mô hình ngẫu nhiên là một mô tả một phần toán học của hệ thống được đề cập như một quá trình ngẫu nhiên toán học. Mô hình ngẫu nhiên là một khẳng định rõ ràng hoặc ngầm hiểu rằng đầu ra của một số chu trình theo xác suất phân phối từ một họ phân phối nhất định.

Mục đích của việc đưa mô hình ngẫu nhiên vào đánh giá bộ tạo bit ngẫu nhiên gồm 4 ý như sau:

a) Mô hình ngẫu nhiên của thành phần biến đổi sinh ngẫu nhiên nhìn chung xác định các vấn đề khó giải quyết bằng cách kiểm thử hộp đen xem đầu ra của thiết bị có chứa lượng entropy mong muốn có thể kiểm thử được hay không nhằm xác định xem thử nghiệm thống kê có mang lại kết quả tương thích với giả thuyết rằng cơ chế lấy mẫu từ một trong các phân phối được bao phủ bởi mô hình ngẫu nhiên. Dựa trên mô hình ngẫu nhiên, có thể kiểm tra lượng entropy được tạo ra bởi cơ chế này.

b) Mô hình ngẫu nhiên chứa các đầu ra phân phối tương ứng với các trạng thái thiếu hụt của thiết bị tạo ngẫu nhiên và sau đó có thể sử dụng thử nghiệm thống kê nhằm xác định một trong các chế độ này. Điều này là cần thiết vì nếu không có giả thuyết về tác động của các trạng thái thiếu hụt, thì trên thực tế không thể kiểm chứng.

c) Mô hình ngẫu nhiên có thể và sẽ được hỗ trợ bằng cách sử dụng các kỹ thuật lập luận rút ra từ thiết kế của thiết bị tạo ngẫu nhiên, mục đích để mô hình hóa mô hình ngẫu nhiên. Do đó, một kết nối được thực hiện giữa các đặc tính kỹ thuật của thiết bị được đánh giá và các đặc tính an toàn cốt lõi đã được xác nhận của cơ chế tạo bit ngẫu nhiên.

d) Việc xem xét mô hình ngẫu nhiên trong giai giai đoạn đầu của quá trình tạo bit ngẫu nhiên và cơ sở lập luận kỹ thuật hỗ trợ, cho phép đánh giá viên xác nhận rằng các lập luận kỹ thuật dự đoán khuôn mẫu chung của phân phối đầu ra ngẫu nhiên tại một điểm mà đầu ra này vẫn có thể được phân biệt rõ ràng với đầu ra lý tưởng. Ngược lại, nhiều cấu trúc RBG dẫn đến đầu ra ở giai đoạn cuối của quá trình tạo bit ngẫu nhiên không thể phân biệt được với đầu ra được phân phối lý tưởng, hầu như không phụ thuộc vào lượng entropy thực có trong đó.

Mô hình ngẫu nhiên cần phải bao gồm tất cả các phương thức lỗi hoặc suy giảm hiệu suất hợp lý về mặt kỹ thuật.

Ví dụ: Một mô hình ngẫu nhiên cho đầu ra của thiết bị tạo ngẫu nhiên có thể tuyên bố rằng đầu ra được phân phối đồng nhất và độc lập cho các cơ chế gọi độc lập ở chế độ hoạt động bình thường và duy nhất số "0" trong chế độ lỗi hợp lý về kỹ thuật. Xác suất tự phát (không có sự can thiệp của kẻ tấn công) vào một chế độ có hiệu suất thấp hơn các tuyên bố an toàn cho thiết bị có thể được xác nhận là một số giá trị thấp cho mỗi cơ chế gọi.

Thông thường, mô hình ngẫu nhiên bao gồm một số khẳng định về tính ổn định rằng: Trong các điều kiện kỹ thuật phù hợp, quá trình được đề cập được mô hình hóa bởi một thành viên trong họ xác suất phân bố và trong các thang đo thời gian ngắn, các tham số phân phối liên quan dự kiến sẽ không thay đổi nhiều.

Tuyên bố về tính ổn định thuộc loại này không mâu thuẫn với quan điểm cho rằng thiết bị có thể gặp phải tác động của quá trình lão hóa, tác động nhất thời trong quá trình khởi động hoặc có thể lỗi. Trong trường hợp đầu tiên, sự thay đổi các tham số phân bố quá chậm để ảnh hưởng đáng kể đến việc lấy mẫu trong các khoảng thời gian ngắn; trong trường hợp phản hồi nhất thời, RBG có thể chưa đạt đến trạng thái hoạt động và trên thực tế vẫn chưa thể được sử dụng và trong trường hợp lỗi, phân phối đầu ra có thể thay đổi đáng kể, nhưng điều này xảy ra với khả năng thấp và khả năng xảy ra từ trạng thái bắt đầu hoạt động không thay đổi đáng kể theo thời gian.

Lưu ý rằng câu hỏi liệu một trạng thái có đứng yên hay không một phần phụ thuộc vào mô tả của quá trình đang được sử dụng. Trường hợp một bước ngẫu nhiên tiêu chuẩn là một ví dụ cổ điển của quá trình không cố định (phạm vi giá trị đang được lấy rộng hơn theo thời gian), nhưng nếu các trạng thái đạt được trong một bước ngẫu nhiên được sử dụng làm nguồn ngẫu nhiên, thì có thể (tùy thuộc vào các bước xử lý tiếp theo được sử dụng) tương đương với thay vào đó coi sự khác biệt theo từng bước là đầu vào entropy, tạo ra quy trình Bernoulli độc lập và được phân phối giống hệt nhau.

Các nguồn không phù hợp để được mô hình hóa bằng quá trình đứng yên cơ bản khó mô tả đặc điểm hơn các nguồn gần như đứng im, bởi vì các tham số phân bố mà thử nghiệm thống kê có thể

cố gắng ước tính trong trường hợp này có thể thay đổi trong quá trình lấy mẫu, ngay sau đó hoặc ngay trước đó.

6.2.1.2 Yêu cầu

Tuyên bố về tính ổn định (gần đúng) phải luôn được chứng minh bằng các lập luận kỹ thuật. Do đó, nói chung, một mô hình ngẫu nhiên sẽ:

- Mô tả toán học một phần của một quá trình ngẫu nhiên;

- Mô tả chính xác giai đoạn tạo bit ngẫu nhiên trong thiết bị đang nghiên cứu được cho là đã được mô hình hóa;

- Cho phép thu được hiệu quả các tuyên bố entropy cho việc phân phối của giai đoạn mục tiêu tạo bit ngẫu nhiên từ dữ liệu kiểm thử;

- Bảo đảm các trạng thái thiếu hụt hợp lý về mặt kỹ thuật của cơ chế hướng đến mục tiêu trong mô hình hóa;

- Được hỗ trợ bởi các kỹ thuật lập luận dựa trên thiết kế của cơ chế hướng đến.

Hơn nữa, việc mô tả các trạng thiếu hụt hợp lý về mặt kỹ thuật của nguồn ngẫu nhiên có trong mô hình ngẫu nhiên sẽ cho phép xây dựng các bài thử nghiệm thống kê ("kiểm tra chất lượng trực tuyến") để phát hiện một cách hiệu quả sự suy giảm chất lượng không thể chấp nhận được của nguồn.

Ví dụ: Mô hình ngẫu nhiên có thể chỉ định thống kê phân phối tham số hóa và các tham số của tất cả các thiết bị nằm trong một vùng cho phép để đáp ứng các yêu cầu an toàn. Qua đó, một bài kiểm tra chất lượng trực tuyến có thể áp dụng một bài thử nghiệm thống kê phù hợp để kiểm tra xem tham số của thiết bị có còn nằm trong vùng đó hay không.

6.2.2 Phân tích phỏng đoán entropy của các nguồn

6.2.2.1 Yêu cầu chung

Trong một vài phạm vi, không thể hạn chế việc phân phối dữ liệu tạp âm số hóa bằng mô hình ngẫu nhiên theo nghĩa trên. Có thể khó tìm ra cơ sở kỹ thuật chắc chắn để giả định các đặc điểm cơ bản nhất định của phân phối. Đây thường là trường hợp khi tính ngẫu nhiên hoặc ít nhất là sự xuất hiện của hành vi không thể đoán trước được tạo ra bởi một hệ thống vật lý phức tạp, chẳng hạn như người dùng hoặc máy tính. Trong trường hợp này, hệ thống vật lý lớn thường không thể được hiểu ở mức độ chi tiết đủ để hỗ trợ tóm tắt tính chất kỹ thuật mô hình ngẫu nhiên được yêu cầu trong điều khoản 6.2.1; ngay cả các thuộc tính cơ bản như tính ổn định thường không được đưa ra.

6.2.2.2 Yêu cầu

Nhà cung cấp sẽ cung cấp phân tích phỏng đoán về nguồn entropy. Mục đích của phân tích phỏng đoán là giới hạn cận dưới entropy thu được và xác định bất kỳ điều kiện hợp lý nào có thể dẫn đến những tuyên bố về entropy sai. Ngược lại, một mô hình ngẫu nhiên nhằm mục đích suy ra một ước lượng, nhưng cuối cùng, ước lượng entropy thu được bởi một cơ chế, bao gồm đặc điểm định lượng của sự phân bố ở trạng thái không ổn định của RBG.

Sự phân phối của đầu ra nguồn ngẫu nhiên sẽ bị giới hạn trong một họ phân phối và một cơ sở lập luận sẽ được trình bày giải thích tại sao phân phối thực của các giá trị đang được nghiên cứu có thể được kỳ vọng sẽ nằm trong trong họ phân phối được yêu cầu, mặc dù quá trình tạo đầu ra trung gian mục tiêu được hiểu chưa đầy đủ về mức độ kỹ thuật. Đương nhiên, những phân tích theo phương pháp phỏng đoán như vậy sẽ luôn hướng tới việc thận trọng, tức là đánh giá thấp entropy được cung cấp. Điều này bao gồm việc giả định khả năng hợp lý về mặt kỹ thuật lớn nhất để kẻ tấn công tác động hoặc quan sát việc tạo entropy.

6.2.3 Các nguồn vật lý và phi vật lý

Trong nội dung của tiêu chuẩn này, một cách trực quan, nguồn ngẫu nhiên là một thành phần của RBG tạo ra một dòng bit, tối thiểu một phần không thể đoán trước và nhà cung cấp đã gửi mô hình ngẫu nhiên như được nêu trong điều khoản 6.2.1 hoặc đặc điểm của entropy được tạo ra dựa trên suy luận phỏng đoán như được nêu trong điều khoản 6.2.2. Do đó, chức năng của một nguồn

ngẫu nhiên trong RBG là tạo ra tính chất không xác định. Trong một số trường hợp, các nguồn ngẫu nhiên có thể khá phức tạp: chẳng hạn, hãy nghĩ đến một hệ thống lấy entropy từ các hoạt động của người dùng trên một máy tính tiêu chuẩn. Trong trường hợp này, "nguồn ngẫu nhiên" là thành phần phần mềm bên trong máy tính trích xuất thông tin về trạng thái hệ thống và ghi nó vào bộ đệm thích hợp để hậu xử lý cùng với người dùng thực hiện các hành động ở một mức độ nào đó thực sự không thể đoán trước được.

Mặt khác, các nguồn ngẫu nhiên chuyên dụng có thể dựa trên các hiệu ứng vật lý tương đối đơn giản, ví dụ: hãy xem xét một bo chuyển mạch nhỏ giữa hai trạng thái để phản ứng với các photon đơn va vào một cảm biến ảnh nhỏ và trạng thái của nó được đọc ra tại các khoảng thời gian ngoài quy định bởi đồng hồ bên định.

Sự phân biệt giữa các nguồn ngẫu nhiên đơn giản và phức tạp có tầm quan trọng nhất định trong việc lập mô hình và đánh giá sau đó. Mặc dù, đối với các nguồn vật lý chuyên dụng, có thể đạt được sự hiểu biết chắc chắn về hoạt động của nguồn trên cơ sở kỹ thuật phân tích, nhưng điều này nói chung là không khả thi đối với các nguồn ngẫu nhiên phi vật lý, phức tạp. Do đó, tiêu chuẩn này phân biệt giữa bộ tạo bit ngẫu nhiên bất định thực dựa trên nguồn vật lý chuyên dụng (TNRBG) và bộ tạo bit ngẫu nhiên dựa trên nguồn không chuyên dụng (NNRBG).

CHÚ THÍCH 1: Nó có thể phụ thuộc vào dữ liệu do nhà cung cấp cung cấp để xem NRBG được coi là TNRBG hay NNRBG. Ví dụ: RBG có thể được coi là TNRBG nếu nó lấy entropy từ cả thành phần phần cứng và tương tác của người dùng nếu yêu cầu an toàn cho RBG chỉ dựa trên các thuộc tính được xác nhận trong thành phần phần cứng và nếu một mô hình ngẫu nhiên hỗ trợ các tuyên bố an toàn cho thành phần phần cứng đã được nhà cung cấp đưa ra và có vẻ đúng. Mặt khác, cùng một RBG có thể được coi là NNRBG nếu các tuyên bố an toàn tương tự cho cấu trúc tổng thể được hỗ trợ ít nhất một phần bởi kết luận phỏng đoán liên quan đến entropy xuất phát từ tương tác của người dùng.

CHÚ THÍCH 2: Có thể hiểu rằng, các tuyên bố về entropy cần thận trọng, nguồn ngẫu nhiên của NNRBG có thể được đánh giá ở mức độ đảm bảo tương tự và thực sự việc, sử dụng phương pháp luận tương tự như sẽ thực hiện đối với một nguồn vật lý chuyên dụng. Trong trường hợp đó, một ví dụ trong giao diện thiết bị người dùng sẽ không tập trung vào entropy được cung cấp bởi tương tác của người dùng mà là cảm biến nhiễu nằm bên trong thiết bị, thu được từ sự tương tác của người dùng. Tuy nhiên, trong thực tế, điều này rất khó vì thường ta không có quyền truy cập vào dữ liệu thô lấy được từ các thiết bị như vậy (ví dụ: chuột quang chưa thực hiện chỉnh sửa sẽ không cho phép truy cập dữ liệu thô từ cảm biến quang học của nó). Ngoài ra, ngay cả khi dữ liệu thô có thể truy cập được, bản thân cơ chế số hóa có thể được thực hiện với độ phức tạp ít hơn nhiều trong một RBG chuyên dụng so với trường hợp trong một thiết bị ban đầu được thiết kế cho mục đích khác.

6.2.4 Tổng quan về đánh giá nguồn ngẫu nhiên của TNRBG

Trong đánh giá TNRBG, nghiên cứu về nguồn ngẫu nhiên của TNRBG tập trung vào việc chỉ ra rằng, ở mức đầu ra nguồn ngẫu nhiên (các bit ngẫu nhiên thô) có đủ entropy và nhìn chung các bit ngẫu nhiên thô tuân theo một phân phối phù hợp về mặt hỗ trợ các yêu cầu an toàn được thực hiện cho toàn bộ cấu trúc. Nguồn ngẫu nhiên phải được mô tả bằng mô hình ngẫu nhiên bao gồm tất cả các trường hợp lỗi hợp lý về mặt kỹ thuật và được hỗ trợ bởi các lập luận kỹ thuật dựa trên thiết kế của nguồn. Đánh giá viên phải kiểm tra xem các lập luận kỹ thuật dựa trên thiết kế của nguồn hỗ trợ cho giả định rằng hoạt động của nguồn phù hợp với mô hình ngẫu nhiên của nguồn là hợp lý. Thực tế, đầu ra entropy và các đặc điểm khác liên quan đến an toàn trong phân phối đầu ra của thiết bị thực phải được suy ra bằng cách sử dụng các thử nghiệm thống kê như mô tả trong Phụ lục A, với giả định rằng mô hình ngẫu nhiên phù hợp. Ngoài ra, đánh giá viên phải kiểm tra xem dữ liệu kiểm thử có chỉ ra rằng mô hình ngẫu nhiên được giữ nguyên hay không. Nhà cung cấp phải cung cấp mô hình ngẫu nhiên và tất cả các tài liệu hỗ trợ về mô hình đó và chỉ rõ giai đoạn tạo số ngẫu nhiên trong toàn bộ thiết kế các mục tiêu của mô hình ngẫu nhiên (xem Phụ lục A).

Nhà cung cấp cũng phải chỉ ra rõ ràng những ảnh hưởng nào nếu có đối với nguồn ngẫu nhiên do lão hóa, sự thay đổi trong điều kiện hoạt động (đối với tất cả các điều kiện hoạt động do nhà cung cấp quy định, ví dụ: nhiệt độ) hoặc sử dụng lâu dài.

Cuối cùng, đánh giá viên sẽ xác minh rằng các thuộc tính an toàn được xác nhận của nguồn ngẫu nhiên là đủ để hỗ trợ các tuyên bố an toàn do nhà cung cấp đưa ra đối với mức đầu ra của RBG nếu bất kỳ bước hậu xử lý nào có thể được áp dụng được triển khai chính xác theo mô tả toán học, các bước như vậy do nhà cung cấp cung cấp. Đánh giá viên cũng phải kiểm tra xem mô hình ngẫu nhiên kết hợp với các bài kiểm tra chất lượng trực tuyến và kiểm tra tổng số lỗi cũng như kiểm thử dữ liệu được gửi như một phần của tài liệu đánh giá có hỗ trợ các tuyên bố an toàn được đưa ra cho nguồn hay không. Các giả định về tiêu chuẩn độ cứng mật mã (ví dụ: về tính một chiều của hàm băm hoặc mã khối) có thể được sử dụng làm lập luận sau cùng.

6.2.5 Tổng quan về đánh giá nguồn ngẫu nhiên của NNRBG

Trong trường hợp NNRBG, một nguồn ngẫu nhiên vật lý chuyên dụng không tồn tại và nguồn ngẫu nhiên được sử dụng nói chung là quá phức tạp để đánh giá viên có thể hiểu được hoàn toàn. Bất kỳ lập luận kỹ thuật nào ủng hộ các tuyên bố rằng đầu ra của nguồn ngẫu nhiên tuân theo một phân phối từ một họ phân phối cụ thể, các tuyên bố như vậy sẽ không đầy đủ. Thay vào đó, nhà cung cấp sẽ cung cấp lập luận phỏng đoán theo điều khoản 6.2.2.2 để chỉ ra rằng đầu ra ở nguồn ngẫu nhiên nằm trong một vài mức, có thể được xác định rộng rãi, họ phân bố xác suất. Đánh giá viên phải kiểm tra tính hợp lý đã đưa ra từ kinh nghiệm phân tích. Nhà cung cấp phải cung cấp thêm bằng chứng thực nghiệm rằng lý luận phỏng đoán là hợp lệ và bằng chứng thực nghiệm này cũng sẽ được đánh giá viên xác nhận. Cuối cùng, đánh giá viên sẽ xác minh rằng các thuộc tính an toàn đã tuyên bố của nguồn ngẫu nhiên, trong phạm vi mà chúng được hỗ trợ bởi suy luận phỏng đoán đã cho là đủ để hỗ trợ các tuyên bố an toàn do nhà cung cấp đưa ra đối với các mức đầu ra từ RBG nếu có bất kỳ bước hậu xử lý có thể được áp dụng được thực hiện chính xác theo mô tả toán học của các bước đó do nhà cung cấp cung cấp. Có thể sử dụng các giả định về tiêu chuẩn độ cứng mật mã.

6.3 Mẫu thiết kế chung và phân loại đối với bộ tạo bit ngẫu nhiên bất định

6.3.1 Tổng quan

Trong thiết kế NRBG, các tiêu chuẩn hiện có và các tài liệu thực tiễn tốt nhất thường cho phép nhà thiết kế tự do với hầu hết các kiến trúc mật mã được sử dụng rộng rãi. Bộ tạo bit ngẫu nhiên chuyên dụng vốn liên quan đến việc thiết kế phần cứng chuyên dụng, trong đó các chi tiết cấp thấp của thiết kế phần cứng có ảnh hưởng đến an toàn và hiệu suất của cấu trúc tổng thể. Mặt khác, NRBG không có nguồn chuyên dụng sẽ sử dụng nhiều nguồn entropy thấp khác nhau để tạo ra tính không thể đoán trước. Kết quả của điều này cuối cùng phụ thuộc vào lượng entropy có sẵn từ bất kỳ nguồn nào trong số các nguồn này và trong một tình huống nhất định. Do đó, vấn đề phát triển một bộ tạo bit ngẫu nhiên ít phù hợp với một giải pháp phù hợp với tất cả các trường hợp sử dụng, ví dụ, vấn đề xây dựng một mật mã khối an toàn hoặc một RBG tất định thật sự tinh khiết (thuần túy).

Tuy nhiên, về mặt thiết kế mức cao, có thể xác định được các mẫu cơ bản của các cấu trúc NRBG thực tế nhất và các lựa chọn trong thiết kế mức cao có tác động trực tiếp đến các yêu cầu về tài liệu và các bước đánh giá cần thiết để đánh giá chất lượng của NRBG. Điều khoản 6.3 có các mục đích sau trong phạm vi đó:

- Giới thiệu một mẫu thiết kế chung cho các NRBG được đánh giá trong tiêu chuẩn này;

- Giới thiệu cách phân loại của các bộ tạo bit ngẫu nhiên bất định sẽ được sử dụng trong tiêu chuẩn này và liên kết nó ở một mức độ nào đó với các phần liên quan của TCVN 12853:2020 (ISO/IEC 18031:2011);

- Phác thảo các thực tiễn tốt nhất liên quan đến thiết kế mức cao của NRBG;

- Giải thích các bước đánh giá bị ảnh hưởng bởi thiết kế mức cao của RBG;

- Xác định các yêu cầu tài liệu liên quan đến thiết kế mức cao của RBG.

6.3.2 Mô hình chức năng của NRBG

Nói chung, một NRBG lấy đầu vào là một dòng bit không thể đoán trước được tạo ra bởi một nguồn entropy và có thể được thêm bổ sung, có thể dự đoán được đầu vào và tạo đầu ra từ dòng số ngẫu nhiên này. Trong một cấu trúc NRBG hiệu quả, bộ nhớ được sử dụng hết sẽ không thay

đổi và các chức năng tính toán trạng thái bên trong tiếp theo và đầu ra tiếp theo phải hiệu quả. Những nghiên cứu này hướng đến Hình 1 như một mẫu NRBG chung.

Đối với mục đích của mẫu thiết kế này, nguồn entropy sơ cấp là nguồn entropy mà nhà cung cấp dựa vào các yêu cầu an toàn. Trong tài liệu do nhà cung cấp gửi cho đánh giá viên, nhà cung cấp phải xác định rõ ràng các phần tử tương ứng với các thành phần của Hình 1 trong thiết kế của họ.

Các hoạt động cần được thực hiện và tài liệu mà nhà cung cấp phải gửi trong quá trình đánh giá bộ tạo bit ngẫu nhiên bất định phụ thuộc vào loại bộ tạo bit ngẫu nhiên. Vì lý do đó, tiêu chuẩn này phân loại bộ tạo bit ngẫu nhiên như sau.

NRBG có thể được chỉ định thành các lớp con theo ít nhất ba hệ khác nhau:

a) Các NRBG có thể được phân loại tùy thuộc vào bản chất của nguồn entropy của chúng. Tùy thuộc vào bản chất của nguồn entropy sơ cấp, NRBG sẽ là TNRBG hoặc NNRBG. Điều này tương ứng chính xác với sự phân biệt giữa các nguồn entropy vật lý và phi vật lý trong TCVN 12853:2020 (ISO/IEC 18031:2011). Về các yêu cầu tối thiểu đối với DRBG, đánh giá viên phải xác minh rằng thiết kế TNRBG đáp ứng tối thiểu các yêu cầu của TCVN 12853:2020 (ISO/IEC 18031:2011) điều khoản 8.3.1.2 và điều khoản 8.3.2.2 về RBG có nguồn vật lý và NNRBG đáp ứng các yêu cầu của TCVN 12853:2020 (ISO/IEC 18031:2011) điều khoản 8.3.1.2 áp dụng cho RBG có nguồn entropy phi vật lý. Ngoài tác động này đối với các yêu cầu an toàn tối thiểu, sự lựa chọn giữa TNRBG và NNRBG cũng ảnh hưởng đến tài liệu. Việc đánh giá TNRBG sẽ luôn sử dụng mô hình ngẫu nhiên của nguồn entropy sơ cấp. Thay vào đó, nhà cung cấp NNRBG có thể gửi lập luận phỏng đoán theo điều khoản 6.2.2.

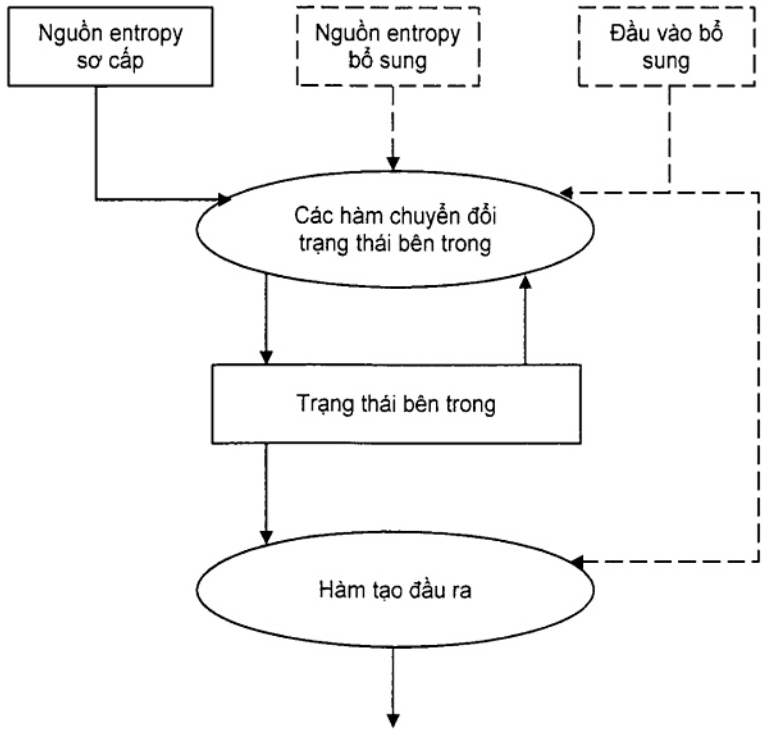
b) NRBG có thể được phân loại tùy thuộc vào việc chúng là NRBG lai ghép hay NRBG thuần túy. Trong một NRBG lai ghép, một phần quan trọng của sự đảm bảo an toàn của NRBG đến từ các quá trình mật mã tương tự như những quá trình được sử dụng trong bộ tạo bit ngẫu nhiên tất định mạnh, ngoài ra entropy còn được thu thập và trộn lẫn vào trạng thái bên trong một cách thường xuyên từ nguồn entropy thực. Ngược lại, trong một NRBG thuần túy, đầu ra của NRBG được lấy từ đầu ra của nguồn ngẫu nhiên bằng một phép biến đổi không thể che giấu hoàn toàn sự thiếu hụt entropy khỏi đối phương: thông thường, các phương tiện phi mật mã, tức là bằng các cơ chế biến đổi, nén hoặc trộn đơn giản hơn nhiều, chẳng hạn như: hiệu chỉnh von-Neumann hoặc thanh ghi dịch phản hồi tuyến tính được sử dụng như bộ tích lũy entropy. Các NRBG lai ghép, nếu được thiết kế đúng cách, có thể đạt được các đặc tính an toàn mà không phải RBG bất định thuần túy và tất định nào cũng có thể đạt được: không giống như các RBG tất định, chúng có thể đạt được độ an toàn phía sau nâng cao; không giống như các RBG bất định thuần túy, một RBG lai ghép có thể tiếp tục tạo ra đầu ra phù hợp cho các ứng dụng mật mã ngay cả khi nguồn nhiễu bị lỗi theo cách mà các bài kiểm tra chất lượng không phát hiện được. Ngoài ra, để đạt khả năng không phân biệt từ một nguồn lý tưởng trong tất cả các thử nghiệm thống kê khả thi về mặt tính toán ít nhất là rất khó trong các RBG thuần túy bất định, nhưng sẽ dễ về mặt khái niệm trong các DRBG và RBG lai ghép. Do đó, liệu NRBG là thuần túy hay lai ghép cần được xem xét khi chứng nhận các tuyên bố an toàn nhất định. Ví dụ: giả sử rằng một yêu cầu an toàn đối với đầu ra của NRBG thuần túy là không thể phân biệt được đầu ra ở kích thước mẫu thực tế với dữ liệu được phân phối lý tưởng. Vì trong một NRBG thuần túy, các hàm tạo đầu ra và cập nhật trạng thái không mạnh về mặt mật mã, do đó cần có các lập luận rất chặt chẽ để hỗ trợ các tuyên bố an toàn như vậy. Dữ liệu chưa được xử lý từ nguồn entropy vật lý ("số ngẫu nhiên thô") biểu hiện độ lệch đặc trưng tối thiểu so với số ngẫu nhiên lý tưởng có thể được phát hiện khi phân tích lượng lớn dữ liệu.

c) Các NRBG có thể được phân loại thông qua việc chúng đang nén entropy hay mở rộng entropy. Một ví dụ về RBG có thể được gọi là bất định một cách hợp lý, nhưng trong các trường hợp có thể mở rộng lượng entropy nhỏ hơn thành một chuỗi dài hơn của giả ngẫu nhiên (mạnh về mặt mật mã) là trình tạo */dev/urandom* trong hệ điều hành giống UNIX: trên thang thời gian đủ ngắn, */dev/urandom* hoạt động chính xác như một bộ tạo bit ngẫu nhiên tất định; nhưng việc gửi lại vẫn diễn ra liên tục, tức là RBG cố gắng truy xuất càng nhiều entropy càng tốt từ các nguồn entropy có trong hệ thống và giả sử hoạt động đúng của quá trình thu thập entropy, có một số đảm bảo về tính không liên quan về mặt lý thuyết thông tin của các đầu ra được tạo ra ở mức phân tách thời gian vừa đủ (nhưng không quá lớn). Cho dù NRBG là nén entropy hay mở rộng entropy, điều quan trọng chủ yếu là về mặt chứng nhận các tuyên bố an toàn liên quan đến các bit entropy đầu ra. Ví dụ, một RBG tạo ra 256-bit đầu ra đối với bất kỳ 128-bit entropy nào thường chỉ có thể hỗ

trợ các ứng dụng mật mã đến mức an toàn 128-bit. Do đó, nhà cung cấp phải tuyên bố rõ ràng có bao nhiêu entropy được yêu cầu cho mỗi lần gọi đến RBG, tùy thuộc vào các tham số mà RBG được gọi. Nhà cung cấp phải cho biết liệu dữ liệu được trả về bởi các lệnh gọi khác nhau tới RBG có thể được coi là dữ liệu ngẫu nhiên độc lập một cách hợp lý theo nghĩa lý thuyết thông tin hay không. Nếu, trong ví dụ trước, RBG phải lưu vào bộ đệm 256-bit đầu ra chứa 128-bit entropy và phân phối 128-bit đầu và 128-bit còn lại trong bộ đệm sẽ dành cho những gọi khác nhau, do đó thì tuyến bố an toàn 128-bit sẽ không còn đúng theo lý thuyết thông tin (mặc dù nó vẫn có thể an toàn trong thực tế). Mặt khác, NRBG nén entropy nhằm mục đích tạo ra các chuỗi bit chứa một lượng entropy bằng hoặc ít nhất là rất gần với độ dài của đầu ra. Để đạt được điều này, họ thường sử dụng tính năng nén, ví dụ: hàm băm, để tăng entropy trên mỗi bit đầu ra gần với "1".

Như trường hợp của bất kỳ tính chất phân loại nào, ranh giới giữa các lớp của bộ tạo bit ngẫu nhiên này không phải lúc nào cũng rõ ràng: ví dụ, bộ tạo bit ngẫu nhiên có thể sử dụng cả nguồn entropy vật lý và phi vật lý và sau đó nó có thể phụ thuộc vào mức đảm bảo rằng đánh giá viên thu được từ một trong hai loại nguồn cho dù nó được xem là NRBG vật lý hay phi vật lý; tương tự như vậy, một số cấu trúc có thể xuất hiện hậu xử lý mật mã ở dạng: ví dụ, một hàm băm nén các số ngẫu nhiên thô, nhưng không hậu xử lý mật mã mà bản thân nó có các đặc tính của RBG tất định mạnh, như được yêu cầu trong định nghĩa về RBG kết hợp ở trên.

Nói chung, các đảm bảo an toàn mạnh nhất có thể đạt được đối với các RBG lai ghép với nguồn vật lý được hiểu rõ không mở rộng entropy và có hậu xử lý mật mã để truyền các đặc tính an toàn mạnh nhất trên đầu ra ngay cả trong trường hợp không phát hiện được lỗi của nguồn ngẫu nhiên. Các yêu cầu về lớp chức năng PTG.3 trong [7] có thể đóng vai trò là thông tin hướng dẫn trong việc đánh giá bộ tạo bit. Yêu cầu cốt lõi đối với nguồn entropy là phải có tuyên bố dựa trên sự hiểu biết thấu đáo về nguyên tắc hoạt động về lượng entropy tối thiểu được tạo ra mà người ta có thể kỳ vọng thu được trên mỗi lần đọc. Tuyên bố này sẽ xem xét mức độ mà kẻ tấn công có thể giám sát trạng thái bên trong của nguồn entropy. Lưu ý rằng khả năng phục hồi chống lại các sự cố ngắn hạn, khó phát hiện của nguồn entropy có thể giúp bảo vệ khỏi các cuộc tấn công phát hiện lỗi của một số kẻ tấn công bên ngoài.



Hình 1 – Sơ đồ khối của NRBG.

6.3.3 Các thành phần của NRBG

6.3.3.1 Yêu cầu chung

Các mục sau đây cung cấp một cái nhìn tổng quan về các bước đánh giá cần thiết cho mỗi khối được minh họa trong Hình 1. Trọng tâm của điều khoản phụ này là nội dung kỹ thuật của các bước đánh giá cho mỗi thành phần. Các yêu cầu về tài liệu chi tiết được trình bày trong điều khoản 7.

6.3.3.2 Nguồn entropy sơ cấp

Thành phần này đóng vai trò là nguồn không thể đoán trước trong NRBG bằng cách cung cấp dữ liệu được xử lý bởi hàm chuyển đổi trạng thái bên trong. Trong NRBG, tính không thể đoán trước được dựa trên việc sử dụng một hoặc nhiều nguồn entropy. Những nguồn này được gọi là nguồn entropy và có thể được phân loại thêm là vật lý hoặc phi vật lý.

Nhà cung cấp phải cung cấp mô hình ngẫu nhiên của nguồn entropy sơ cấp của các số ngẫu nhiên thô trong trường hợp nguồn entropy sơ cấp là một thiết bị chuyên dụng (nếu NRBG là TNRBG). Nếu một lỗi được phát hiện, RBG sẽ không xuất ra các bit ngẫu nhiên mà bất kỳ thuộc tính an toàn nào được yêu cầu (ví dụ như: lượng entropy) đã bị ảnh hưởng.

Một giai đoạn khác của quá trình tạo bit ngẫu nhiên, ngoài các số ngẫu nhiên thô có thể là mục tiêu chọn lọc bởi mô hình ngẫu nhiên, nhưng phải rõ ràng phần nào của quá trình tạo bit ngẫu nhiên đang được mô hình hóa. Mô hình ngẫu nhiên ít nhất phải dựa trên cơ sở hiểu biết tính chất của quá trình sinh entropy trong nguồn entropy sơ cấp. Nếu một số nguồn entropy được sử dụng bởi bộ tạo bit ngẫu nhiên, thì nguồn chủ yếu dựa vào các tuyên bố an toàn của nhà cung cấp sẽ được coi là nguồn chính để đánh giá. Mô hình ngẫu nhiên do nhà cung cấp trình phải đáp ứng các yêu cầu của điều khoản 6.2.1.

Nếu nguồn entropy sơ cấp không phải là một thiết bị được thiết kế ban đầu để cung cấp entropy, thì cần phải đề xuất thay cho mô hình ngẫu nhiên một phân tích phỏng đoán của quá trình thu thập entropy có mức giới hạn cận dưới đáng tin cậy đối với entropy được thu thập. Phân tích phỏng đoán này phải đáp ứng các yêu cầu của điều khoản 6.2.2. Trong trường hợp này, thử nghiệm đánh giá và kiểm tra chất lượng trực tuyến với mục đích xác minh các giới hạn cận dưới entropy tương ứng để đảm bảo rằng RBG đã không đi vào một số trạng thái có vẻ hợp lý về mặt kỹ thuật trong đó các giới hạn cận dưới entropy được tuyên bố sẽ không duy trì thực hiện trên dữ liệu entropy thô đã được số hóa trước đó nó đi vào quá trình hậu xử lý.

Hơn nữa, đánh giá viên phải xác minh rằng các kiểm tra chất lượng và kiểm tra tổng số lỗi được thực hiện khi kích hoạt bộ tạo bit và khi lấy entropy từ nó để đưa vào trạng thái bên trong. Lưu ý rằng có thể dùng được khi thực hiện các kiểm tra tổng số lỗi trên nguồn entropy sau lấy dữ liệu và sau đó chờ kết quả kiểm thử trước khi sử dụng dữ liệu. Điều này tránh trường hợp nguồn entropy bị đứt gãy sau khi kiểm tra chất lượng, nhưng phải trước hoặc trong khi thu thập dữ liệu (có thể do kẻ tấn công bên ngoài). Các phép thử này phải có thể phát hiện tất cả các lỗi thực tế của nguồn nhiễu có thể dẫn đến sự suy giảm chất lượng không thể chấp nhận được của các số ngẫu nhiên thô. Các hàm chuyển đổi trạng thái thích hợp và hàm tạo đầu ra được kiểm thử chính xác hơn bằng các bài kiểm tra với câu trả lời đã biết. Nếu các bài kiểm tra với câu trả lời đã biết về các chức năng này được thực hiện trực tuyến, cần đặc biệt lưu ý rằng không có giao diện nào cho các chức năng kiểm tra này có thể truy cập được từ bên ngoài chu vi NRBG. Đặc biệt, các giao diện kiểm thử như vậy phải không được để lộ với ứng dụng tiêu thụ.

Kiểm tra chất lượng được kỳ vọng rằng là dễ dàng nhất để thực hiện trên các số ngẫu nhiên thô, vì các lỗi thống kê có thể dễ dàng phát hiện nhất ở các giai đoạn sớm nhất của quá trình tạo bit ngẫu nhiên. Tuy nhiên, các phương pháp tiếp cận khác có thể hoàn toàn hợp lệ nếu có sự hỗ trợ kỹ thuật cao để đưa ra kết luận rằng các sai lệch không thể chấp nhận được so với phân phối mong muốn được phát hiện. Ngoài ra, điều đáng nói là việc kiểm tra chất lượng có thể được bao phủ một phần bằng các phương pháp tiếp cận không cần kiểm thử các số ngẫu nhiên, ví dụ: giám sát trạng thái vật lý của nguồn nhiễu (ví dụ: điện áp trong một diode nhiễu) để phát hiện giả mạo hoặc lỗi ngẫu nhiên. Nguồn entropy sơ cấp có thể được bổ sung trong một số thiết kế bằng bổ sung các nguồn entropy để cải thiện entropy thu được.

6.3.3.3 Các hàm chuyển đổi trạng thái bên trong

Các hàm chuyển đổi trạng thái bên trong kiểm soát tất cả các hoạt động làm thay đổi trạng thái bên trong. Chúng bao gồm các hàm buộc đặt đầu ra của nguồn entropy đi vào trạng thái làm việc và biểu diễn một phần của trạng thái bên trong cho hàm tạo đầu ra.

Hàm chuyển đổi trạng thái bên trong của RBG nói chung sẽ đóng một vai trò quan trọng trong việc trộn đầu ra của nguồn entropy vào trạng thái bên trong và đảm bảo rằng đầu ra RBG cuối cùng không thể phân biệt được với nguồn lý tưởng.

Về nguyên tắc, hàm chuyển đổi trạng thái bên trong của NRBG có thể là một cấu trúc phi mật mã, chẳng hạn như một hàm biến đổi nhằm mục đích tăng bit entropy và loại bỏ các phụ thuộc thống kê trong đầu ra bằng cách loại bỏ một số thông tin có trong số ngẫu nhiên thô. Ví dụ, hiệu chỉnh Von-Neumann, nếu áp dụng phân phối độc lập và đồng nhất cho nguồn phân bố lệch sẽ mang lại đầu ra độc lập, phân phối đồng nhất và đồng xác suất. Tuy nhiên, để có được sự đảm bảo chắc chắn về đầu ra được tạo ra bằng các phương pháp như vậy, thông thường người ta cần phải hiểu sự phân bố của các số ngẫu nhiên thô, bao gồm bất kỳ sự phụ thuộc nào giữa chúng, một cách khá tốt và chính xác về mặt định lượng.

Các ràng buộc bắt buộc đối với hoạt động của nguồn ngẫu nhiên thô không thể có được hoàn toàn bằng nghiên cứu thực nghiệm về nguồn, ví dụ: nếu người ta cố gắng giả định một cách chung chung rằng nguồn ngẫu nhiên là một máy móc đơn giản với chỉ một số lượng nhỏ các trạng thái bên trong và một số khả năng hạn chế bị ảnh hưởng bởi môi trường của nó, một trạng thái hữu hạn xác suất của máy móc có thể xuất hiện giống như một mô hình toán học tự nhiên của tình huống đó. Máy móc sẽ tạo ra đầu ra (chuỗi bit) và nhận đầu vào (thay đổi điều kiện môi trường như nhiệt độ hoặc điện áp, cần được tùy chỉnh trong mô hình này). Nhưng kích thước mẫu cần thiết để phát hiện những phần phụ thuộc dài hạn tiềm ẩn có thể làm giảm entropy nghiêm trọng của ít nhất một số bit đầu ra phát triển trong trường hợp chung theo cấp số nhân với số trạng thái bên trong giả định đã có trong mô hình này (lưu ý rằng điều này phù hợp với cả hai đối với sự phụ thuộc của đầu ra vào việc thay đổi đầu vào từ môi trường và sự phụ thuộc giữa các bit đầu ra tiếp theo không có đầu vào).

Nói chung, các giả định về tính chất ngẫu nhiên của nguồn sẽ là cần thiết để có được đảm bảo entropy mạnh, chẳng hạn như không có sự phụ thuộc nhiều bước trong khai thác thực tế hoặc sai lệch so với tính cố định. Những giả định này phải được chứng minh bằng các phương tiện khác ngoài thử nghiệm thống kê. Do đó, để áp dụng các phương pháp thử nghiệm thống kê cho vấn đề đảm bảo rằng nguồn số ngẫu nhiên thô tạo ra đủ entropy cho các ứng dụng mật mã, cần phải xuất phát từ thiết kế toán học mô tả một phần của nguồn, tức là mô hình ngẫu nhiên, đặt việc xác định đầu ra entropy của nguồn thành một lớp các bài toán có thể tính toán được một cách hiệu quả.

Ví dụ, đây có thể là trường hợp nếu nhà cung cấp có thể cung cấp bằng chứng chắc chắn rằng thiết kế của nguồn ngụ ý rằng nguồn sẽ phát ra một dòng byte độc lập và được phân phối giống hệt nhau. Trong trường hợp này, một mặt kiểm thử dòng byte entropy tối thiểu có thể thiết lập dựa trên giả định IID và mặt khác kiểm thử giả định IID theo những cách sẽ dựa trên việc biết các chế độ có vẻ sẽ xảy ra của thiết bị được kiểm thử.

Về khả năng phục hồi và các đặc tính an toàn nhìn chung, rất thuận lợi cho các hàm chuyển đổi trạng thái và đầu ra có các đặc tính mật mã mạnh. Tốt nhất, nó phải có khả năng thể hiện độ an toàn phía sau, độ an toàn phía trước và độ an toàn phía trước nâng cao với giả định trạng thái entropy bên trong cao ngay cả khi nguồn nhiễu bị lỗi hoàn toàn sau lần khởi tạo mầm.

Đánh giá viên đánh giá cấu trúc RBG phải kiểm tra xem bất kỳ bước hậu xử lý và bước điều chỉnh nào được thực hiện để chuyển đổi các số ngẫu nhiên thô thành đầu ra ngẫu nhiên đảm bảo theo các giả định tiêu chuẩn về độ cứng mật mã, thuộc tính đầu ra gần lý tưởng của các số ngẫu nhiên dựa trên mô hình ngẫu nhiên của số ngẫu nhiên thô. Các bước đánh giá này sẽ xem xét các thuộc tính của các số ngẫu nhiên thô như được đưa ra bởi mô hình ngẫu nhiên có liên quan.

6.3.3.4 Trạng thái bên trong

Thành phần này bao gồm thông tin được chuyển giữa các lần gọi NRBG và tất cả thông tin được xử lý trong một yêu cầu. Vì lý do này, một trạng thái bên trong là một thành phần bắt buộc. Tuy nhiên, không bắt buộc bất kỳ phần nào của trạng thái nội bộ phụ thuộc vào các trạng thái trước đó,

tức là không có yêu cầu bắt buộc nào đối với bất kỳ phần nào của trạng thái nội bộ phải được chuyển sang lệnh gọi NRBG tiếp theo (ví dụ: trong ví dụ tung đồng xu, không có trạng thái bên trong nào được chuyển từ thử nghiệm lật một đồng xu sang thử nghiệm tiếp theo).

Trong những trường hợp như vậy, trạng thái bên trong của NRBG hoàn toàn phụ thuộc vào đầu ra của nguồn entropy tại thời điểm NRBG được sử dụng, trừ khi có thêm các đầu vào không bắt buộc.

6.3.3.5 Hàm tạo đầu ra

Thành phần này cung cấp đầu ra ngẫu nhiên cho ứng dụng yêu cầu bằng cách xử lý tất cả hoặc một tập con các bit ở trạng thái hiện tại bên trong và bất kỳ tập con nào của các đầu vào bổ sung tùy chọn.

Tùy thuộc vào các thuộc tính của nguồn entropy và hàm chuyển trạng thái, hàm tạo đầu ra nói chung sẽ đóng vai trò là một thành phần quan trọng trong việc đạt được độ an toàn phía trước và đặc biệt là độ an toàn phía sau. Thành phần, nếu được thiết kế phù hợp, có thể ngăn chặn đầu ra ngẫu nhiên tiết lộ thông tin về các giá trị trước đó hoặc trạng thái bên trong hiện tại, đầu vào nguồn entropy hoặc các đầu ra ngẫu nhiên khác trong bối cảnh này.

CHÚ THÍCH: Về mặt lý thuyết, có thể đạt được các tính chất gần như lý tưởng trong RBG với các hàm chuyển đổi trạng thái đầu ra bình thường: Sử dụng "có căn cứ" một nguồn entropy gần như lý tưởng. Tuy nhiên, việc thiết kế tạo ra một nguồn entropy vật lý mà không cần quá trình hậu xử lý mật mã, các bit ngẫu nhiên độc lập, đồng xác suất và phân phối đồng nhất là rất khó; thiết kế một nguồn như vậy có thể được hiển thị ở mức độ tin cậy cao để có các đặc tính này thậm chí còn khó hơn. Ngoài ra, một RBG như vậy vẫn sẽ nhanh chóng bị lỗi nếu nguồn nhiễu bị suy giảm theo mà không được phát hiện bởi các bài kiểm tra chất lượng và kiểm tra lỗi. Mặt khác, việc thiết kế bộ tạo bit ngẫu nhiên tất định cũng được hiểu rõ. Do đó, rất khuyến khích để hàm chuyển đổi trạng thái và hàm tạo đầu ra hoạt động cùng nhau theo cách mà đầu vào RBG sẽ thậm chí có thể dự đoán được từ nguồn entropy sau một số lần khởi tạo mầm tốt tạo ra đầu ra mà kẻ tấn công không thể phân biệt được biết trạng thái bên trong với dữ liệu ngẫu nhiên.

6.3.3.6 Các xem xét khác

Nhà cung cấp RBG phải thực hiện phân loại RBG theo các đặc tính an toàn phù hợp: tối thiểu phải lưu ý xem RBG là tất định hay bất định, mở rộng entropy hay nén entropy, cho dù kết quả đầu ra được mong đợi dựa trên các giả định về tiêu chuẩn mật mã để đạt được khả năng không thể phân biệt được với một nguồn lý tưởng cũng như liệu độ an toàn phía trước, độ an toàn phía sau và độ an toàn phía trước nâng cao và độ an toàn phía sau nâng cao có đạt được hay không và sự đảm bảo này được đưa ra dựa trên cơ sở nào. Ngoài ra, nhà cung cấp phải chỉ ra bất kỳ thuộc tính nào của RBG mà họ biết đến mà sai lệch đáng kể so với mắt xích chung của loại này.

Trường hợp: Giả sử một nhà cung cấp tuyên bố rằng RBG của họ là một RBG lai ghép, mở rộng entropy, độ an toàn phía trước, độ an toàn phía sau và độ an toàn phía trước nâng cao dựa trên các giả định tiêu chuẩn mật mã cũng như độ an toàn phía sau nâng cao dựa trên việc được gửi lại 120-bit entropy từ một nguồn ngẫu nhiên vật lý mạnh tại mỗi lần gọi. Nói chung, sau đó người ta sẽ kỳ vọng rằng các tuyên bố an toàn của nhà cung cấp là không tồn tại thuật toán nào có thể phá vỡ, trường hợp an toàn phía sau với các yêu cầu về dữ liệu, thời gian hoặc bộ nhớ khả thi. Nhưng có thể tưởng tượng rằng với thiết kế được đề cập, điều này hoàn toàn không đúng và thay vào đó, tuyên bố của nhà cung cấp chỉ là an toàn phía sau chỉ có thể bị phá vỡ bởi một thuật toán hiệu quả về thời gian và bộ nhớ sau khi kẻ tấn công thực hiện một lượng lớn thời gian tính toán trước để tìm thuật toán tấn công hoặc nếu kẻ tấn công đã tự tạo ra các tham số nhất định để sử dụng trong thuật toán. Những sai lệch như vậy so với các kỳ vọng an toàn dựa trên các tiêu chuẩn đặc tính an toàn đã được tuyên bố của RBG sẽ được đề cập rõ ràng trong tài liệu gửi cho đánh giá viên và sẽ được đánh giá viên xem xét cẩn thận khi đi đến kết quả đánh giá. Nếu một tính chất an toàn của RBG được phát hiện sai lệch nhiều so với kỳ vọng dựa trên sự phân loại RBG và không được đề cập đến trong cơ sở lập luận thiết kế đã gửi, thì đánh giá viên thường sẽ phải từ chối các yêu cầu an toàn bị ảnh hưởng bởi đặc tính không mong muốn.

7 Kiểm tra sự phù hợp của NRBG

7.1 Tổng quan

Nói chung, mục tiêu của kiểm thử sự phù hợp với nội dung của RBG là để thấy rằng các yêu cầu an toàn do nhà cung cấp đưa ra được cung cấp triển khai bởi RBG và các yêu cầu an toàn do nhà cung cấp đưa ra ở mức tối thiểu bao gồm các yêu cầu an toàn RBG mẫu thích hợp như đã nêu trong điều khoản 6.3. Liên quan đến nguồn entropy được sử dụng, điều này có nghĩa là nhà cung cấp sẽ trình bày yêu cầu an toàn được xác định rõ ràng dưới dạng ước lượng entropy thu được từ mô hình ngẫu nhiên của giai đoạn tạo bit ngẫu nhiên để hướng đến mục tiêu mô hình ngẫu nhiên, thường là các số ngẫu nhiên thô cùng nhau với các bằng chứng cho rằng, mô hình ngẫu nhiên có vẻ là thiết kế hợp lý với các chi tiết vật lý của nguồn. Sau đó, Kiểm thử viên phải kiểm tra xem lý do liên kết mô hình ngẫu nhiên với thiết kế của nguồn và với các tuyên bố an toàn là hợp lệ và việc tiến hành kiểm thử các số ngẫu nhiên thô không phủ nhận các kết quả với mô hình ngẫu nhiên.

Ngoài ra, kiểm thử sự phù hợp phải đảm bảo rằng các thành phần tất định của cấu trúc RBG như: hàm chuyển đổi trạng thái, tạo đầu ra, kiểm tra chất lượng, kiểm tra lỗi được thực hiện theo đặc điểm kỹ thuật của chúng. Bản thân các đặc tính kỹ thuật của các thành phần này phải được kiểm tra trong một bước kiểm thử riêng biệt để phù hợp với toàn bộ cấu trúc RBG một cách đáng tin cậy, cung cấp một luồng bit ngẫu nhiên không thể phân biệt được với luồng bit được tạo ra bởi một nguồn lý tưởng.

Việc kiểm thử sự phù hợp của một NRBG có thể được thực hiện bởi một phòng thử nghiệm của một cơ quan có thẩm quyền. NRBG có thể là một thành phần của mô-đun mật mã có các yêu cầu được mô tả trong TCVN 11295:2016 (ISO 19790:2012). TCVN 12853:2020 (ISO/IEC 18031:2011) mô tả tổng quan và các yêu cầu đối với NRBG nhưng không thể mô tả cách triển khai hoặc thiết kế cụ thể. Việc triển khai hoặc thiết kế sẽ phụ thuộc vào các nguồn entropy và các yêu cầu của ứng dụng tiêu thụ và có thể được thực hiện trong phần cứng, phần mềm hoặc kết hợp cả hai.

Do đó, mục đích của tiêu chuẩn này là việc kiểm thử sự phù hợp sẽ xác định xem thiết kế và triển khai RBG có hỗ trợ các yêu cầu an toàn do nhà cung cấp đưa ra hay không. Đánh giá viên phải xác định xem liệu các tuyên bố an toàn do nhà cung cấp đưa ra có phù hợp tối thiểu với các yêu cầu về loại bộ tạo bit ngẫu nhiên thích hợp như đã nêu trong điều khoản 6.3 hay không. Bất kỳ tính chất an toàn nào (chẳng hạn như: an toàn về phía sau, an toàn về phía trước, an toàn về phía trước nâng cao) tối thiểu phải được yêu cầu ở mức an toàn 100-bit. Các thuộc tính an toàn có cuộc tấn công lượng tử theo thời gian đa thức đã biết chỉ sử dụng các truy vấn cổ điển tới RBG sẽ không được chấp nhận trong tiêu chuẩn này.

7.2 Kiểm thử

7.2.1 Tài liệu thiết kế

Nhà cung cấp phải cung cấp tài liệu đầy đủ về thiết kế và triển khai NRBG cho phòng thử nghiệm. Tài liệu phải bao gồm một sơ đồ logic chi tiết minh họa tất cả các thành phần, nguồn và cơ chế tạo thành nguồn entropy sơ cấp. Nếu nhiều nguồn entropy được sử dụng, phải chỉ ra rằng bất kỳ nguồn entropy nào không được mô tả đều không thể (theo các giả định tiêu chuẩn về độ cứng mật mã và các giả định hợp lý về mặt kỹ thuật, ví dụ: quan sát về khả năng ảnh hưởng của các thành phần khác đến nguồn sơ cấp) làm giảm entropy của đầu ra RBG.

Các thành phần này có thể bao gồm LFSR, diode gây nhiễu, lấy mẫu nhiệt, bộ chuyển đổi tương tự sang số, lệnh gọi dịch vụ entropy từ các thành phần hoặc mô-đun khác, đọc xung nhịp, số lần truy cập bộ nhớ đệm, cũng như các phép đo khác nhau do con người thực hiện, chẳng hạn như khoảng thời gian giữa các lần nhấn phím, di chuyển chuột, ...

Tiêu chuẩn này sẽ cung cấp cơ sở lý luận của nhà cung cấp về việc xác định mối quan hệ giữa lượng entropy được thu thập và tính ngẫu nhiên được yêu cầu của các số ngẫu nhiên thô.

Tài liệu sẽ cung cấp mô hình ngẫu nhiên của giai đoạn tạo bit ngẫu nhiên thích hợp (thường là của các số ngẫu nhiên thô) hoặc các lập luận phỏng đoán tốt giới hạn entropy thấp hơn được thu thập nếu không khả thi (đối với RNG phi vật lý) để đáp ứng tài liệu yêu cầu đối với mô hình ngẫu nhiên của một số giai đoạn tạo bit ngẫu nhiên như được trình bày trong điều khoản 6.2.1.

Lưu ý: Thông thường, cận dưới entropy được tăng một cách phỏng đoán sẽ không được chặt chẽ, tức là nó sẽ yêu cầu biên độ an toàn lớn khi xét về tỷ lệ entropy được tạo bên trong so với số bit ngẫu nhiên do RBG phát ra (nói cách khác, quá trình hậu xử lý sẽ có "hệ số nén" cao). Các giới hạn entropy thấp hơn bắt nguồn từ các mô hình ngẫu nhiên sẽ chặt chẽ hơn và do đó cho phép các cấu trúc hậu xử lý hiệu quả hơn.

7.2.2 Phân tích entropy

7.2.2.1 Tổng quan

Nhà cung cấp sẽ cung cấp các phân tích về entropy. Điều này có nghĩa là nhà cung cấp phải đưa ra các lập luận cho phép chuyên gia về tạo số ngẫu nhiên hiểu biết về các thành phần cơ bản của thiết bị tạo bit ngẫu nhiên được đề xuất để đi đến một đánh giá tin cậy về việc liệu các tuyên bố về entropy do nhà cung cấp đưa ra có được chấp nhận hay không. Chuẩn mực hướng dẫn này đưa ra giúp hình dung được các trường hợp trong quá trình hoạt động theo các tuyên bố về entropy do nhà cung cấp thực hiện thành công hay thất bại. Vì vậy, phân tích phỏng đoán của nhà cung cấp phải bao gồm các giả định về khả năng kẻ tấn công có thể quan sát hoặc làm ảnh hưởng đến thiết bị trong quá trình hoạt động.

Thông thường, phân tích này phải dựa trên mô hình ngẫu nhiên của một giai đoạn tạo bit ngẫu nhiên thích hợp. Nếu không hiểu được sự tạo thành entropy ở mức độ chi tiết được yêu cầu để có được một mô hình ngẫu nhiên hữu ích, thay vì phân tích bằng cách sử dụng mô hình ngẫu nhiên, thì một phân tích phỏng đoán cận dưới tin cậy cho lượng entropy thu thập được có thể đưa ra để xem xét. Trong trường hợp này, nhà cung cấp phải giải thích lý do tại sao việc xây dựng mô hình ngẫu nhiên là không khả thi.

7.2.2.2 Yêu cầu

Nhà cung cấp phải cung cấp các tài liệu sau:

- Một mô hình ngẫu nhiên của giai đoạn trung gian tạo bit ngẫu nhiên (thường là các số ngẫu nhiên thô) có thể được sử dụng để yêu cầu entropy cho các số ngẫu nhiên nếu các tham số tự do được cố định thành các giá trị cụ thể. Xem điều khoản 6.2.1 để biết các yêu cầu tài liệu chi tiết về điều khoản này. Nếu sử dụng nhiều nguồn entropy, các mô hình ngẫu nhiên sẽ được cung cấp cho mỗi nguồn được cho là góp phần tạo nên entropy tổng thể. Nếu không khả thi để có được một mô hình ngẫu nhiên của nguồn ngẫu nhiên và hỗ trợ bằng các cơ sở lập luận kỹ thuật dựa trên thiết kế của nguồn, thì các lập luận phỏng đoán phù hợp với điều khoản 6.2.2 có cận dưới tin cậy cho lượng entropy thu thập được có thể được gửi thay cho mô hình ngẫu nhiên;

- Suy ra các tuyên bố entropy cho các số ngẫu nhiên đầu ra dựa trên mô hình ngẫu nhiên hoặc phân tích phỏng đoán của giai đoạn tạo số ngẫu nhiên được mô hình hóa ở bước trước;

- Giải thích về bất kỳ bước hậu xử lý nào biến đổi đầu ra các số ngẫu nhiên thô thành các số ngẫu nhiên. Bản thuyết minh phải đủ chi tiết để cho phép thực hiện lại một cách độc lập các bước hậu xử lý. Các vectơ kiểm thử phải được cung cấp cho tất cả các bước hậu xử lý không quan trọng hoặc một tiêu chuẩn phải được tham chiếu có chứa các vectơ kiểm thử đó;

- Giải thích về các bài kiểm tra chất lượng (các bài kiểm tra tổng số lỗi và kiểm thử trực tuyến) được thực hiện trong quá trình khởi động và vận hành thiết bị để đảm bảo rằng các số ngẫu nhiên thô được tạo ra tại nguồn ngẫu nhiên có đủ chất lượng. Các yêu cầu kiểm thử tình trạng đối với bộ tạo bit ngẫu nhiên của lớp chức năng PTG.2 theo Tài liệu tham khảo [7] có thể dùng như thông tin hướng dẫn nếu nguồn ngẫu nhiên chuyên dụng đang được sử dụng. Các bài kiểm tra chất lượng được thực hiện phải bao gồm tất cả các chế độ lỗi thực tế của thiết bị. Việc xác định các dạng lỗi thực tế có thể trông như thế nào phải dựa trên sự hiểu biết về các quá trình vật lý được sử dụng trong nguồn entropy;

- Tài liệu giải thích rõ ràng các thuộc tính an toàn đã được tuyên bố của cấu trúc tổng thể.

Trong trường hợp tính ngẫu nhiên được cung cấp bởi một hệ thống tự nhiên phức tạp chẳng hạn như người sử dụng, mô hình ngẫu nhiên của các sự kiện ngẫu nhiên được có thể được thay thế bằng các giới hạn phỏng đoán trên min entropy được thu thập từ các sự kiện có liên quan. Các giới hạn phỏng đoán này sẽ được lập luận cẩn thận dựa trên khả năng của kẻ tấn công trong việc

quan sát các yếu tố đầu vào môi trường liên quan và dựa trên sự thay đổi, quan sát thay đổi của chúng. Trường hợp hợp lý nhất sẽ được sử dụng.

Nếu nhiều nguồn entropy được sử dụng, có thể chấp nhận việc góp phần thêm vào ước tính entropy chung nếu một mô hình ngẫu nhiên về phân phối chung của chúng được hỗ trợ bởi các lập luận kỹ thuật tốt điều này cho phép hoặc nếu không, nếu các lập luận phỏng đoán mạnh mẽ có thể được đưa ra để giả định chúng độc lập.

7.2.2.3 Ví dụ

7.2.2.3.1 Tổng quan

Trong phần tiếp theo, một vài ví dụ được đưa ra về phân tích phỏng đoán entropy mà nhà cung cấp hoặc phòng thử nghiệm sẽ cung cấp. Chúng có nghĩa là để phác thảo các dòng lập luận chung mà phân tích phỏng đoán có thể tuân theo; Ví dụ, nếu người ta nói rằng 3-bit entropy có thể được trích xuất từ việc đo khoảng thời gian giữa các lần nhấn phím do người dùng thực hiện, thì điều này không có nghĩa là đây là một ước tính chung có thể chấp nhận được. Việc ước tính như vậy có hợp lý hay không phụ thuộc vào các đặc điểm cụ thể của tình huống hiện tại, đặc biệt là mức độ mà kẻ tấn công có thể thu được thông tin về thời gian của các bước đột phá chính nói trên.

7.2.2.3.2 Việc tạo entropy do con người điều khiển

Tạo entropy do con người điều khiển có nghĩa là sử dụng dữ liệu về các sự kiện do con người kích hoạt để tạo ra entropy. Trong trường hợp này, cuối cùng vẫn chưa biết được nguồn nhiễu có thể dự đoán được ở mức độ nào và do đó, việc tìm ra một mô hình phân bố của entropy chứa dữ liệu thô có thể được sao lưu bằng các lập luận kỹ thuật sẽ là điều không thể. Do đó, các tuyên bố về entropy trong trường hợp này sẽ không được suy ra bằng cách kiểm thử mô hình ngẫu nhiên của quá trình tạo entropy nhưng giới hạn thấp hơn của entropy được thu thập bởi các lập luận phỏng đoán.

Trong trường hợp tạo entropy do con người điều khiển, ví dụ: nhà cung cấp có thể nói rằng 3-bit entropy được thu thập bằng cách đo khoảng thời gian giữa các sự kiện nhấn phím tiếp theo. Ví dụ: nhà cung cấp có thể lập luận rằng dựa trên các điều kiện hoạt động của thiết bị, kẻ tấn công có thể ước tính thời gian mà người dùng bắt đầu nhập dữ liệu trên bàn phím với độ chính xác tối đa là một giây và các hạn chế tương tự áp dụng cho việc lấy dữ liệu thời gian trên bất kỳ lần nhấn phím nào tiếp theo; hơn nữa, nhà cung cấp có thể lập luận rằng các bản ghi tốc độ đánh máy cho thấy rằng ngay cả những người được đào tạo chuyên sâu cũng không thể nhấn chính xác hơn khoảng 20 chữ cái mỗi giây, cho thấy rằng độ lệch chuẩn về thời gian gõ phím ở một người đánh máy có tay nghề cao có thể là 10 ms. Nếu phép đo thời gian có độ chính xác mili giây, thì người ta có thể giả định rằng một chuỗi các lần nhấn phím sẽ mang lại 1000 khả năng phân bố đều cho thời gian của lần nhấn phím đầu tiên và ba bit cho mỗi lần nhấn phím tiếp theo. Do đó, ước tính phỏng đoán về lượng entropy được thu thập bằng n lần nhấn phím trong cài đặt này có thể là $[10 + (n - 1) * 3]$ bit. Trong trường hợp này, nhà cung cấp phải cung cấp các phép đo về phân phối thực tế của thời gian gõ phím bằng thiết bị thực như sẽ được sử dụng trong hệ thống đã triển khai và cung cấp lý do để loại trừ các tác động dự kiến có thể sẽ làm mất hiệu lực hoặc làm mất hiệu lực một phần các giả định làm cơ sở cho ước lượng tập hợp entropy đã cho; ví dụ, trong thiết lập của ví dụ đang thảo luận ở đây, tần số lấy mẫu của chính thiết bị đầu vào thay vì bộ đếm thời gian hệ thống được sử dụng có thể cung cấp giới hạn thời gian thực thấp hơn độ chính xác về thời gian, do đó làm mất hiệu lực giả định rằng các bit thấp hơn của thời gian có chứa entropy.

Nếu trong quá trình xem xét entropy được tạo ra bởi bất kỳ loại nguồn entropy nào, rõ ràng là lượng entropy được thu thập bởi một quá trình nhất định phụ thuộc vào các yếu tố bên ngoài có thể thay đổi (ví dụ như trong ví dụ trước, tần số lấy mẫu của một thiết bị phần cứng đi kèm), trường hợp xấu nhất có thể xác định được mà không liên quan đến hành động đối nghịch có thể ngăn ngừa được sẽ được giả định. Nhà cung cấp phải giải thích tình huống xấu nhất mà họ đã xác định và cách họ xác định nó.

7.2.2.3.3 Việc tạo entropy bằng các thiết bị vật lý chuyên dụng

Nếu nguồn entropy sơ cấp là một thiết bị vật lý chuyên dụng, thì nhà cung cấp phải gửi mô hình ngẫu nhiên của một giai đoạn tạo đầu ra phù hợp của thiết bị nói trên.

- Nếu entropy được tạo ra bởi một thiết bị vật lý, chẳng hạn như một mẫu đồng vị phóng xạ được kết hợp với thiết bị phát hiện các sự kiện phân rã hạt nhân, sao cho tốc độ trung bình của các sự kiện phân rã đã phát hiện được và giá trị ngẫu nhiên là số nguyên tử có bị phân rã trong một khoảng thời gian cụ thể, nhà cung cấp hoặc phòng thử nghiệm phải nêu một số dữ kiện đã biết về tốc độ trung bình của quá trình phân rã và thiết bị đo cũng như về sự phân bố hoặc ít nhất là về phương sai của số nguyên tử phân rã và đưa ra giá trị thô ước tính của entropy được tạo ra. Nhà cung cấp sẽ cung cấp mô hình ngẫu nhiên của chuỗi số ngẫu nhiên thô và lý luận để hỗ trợ mô hình đó. Nhà cung cấp sẽ tiếp tục lấy được một ước lượng về entropy thu thập được từ mô hình đó. Cũng lưu ý rằng trong trường hợp này, không phải tất cả các kết quả (số nguyên tử bị phân rã) đều có khả năng xảy ra như nhau. Thay vào đó, phân phối tập trung vào giá trị trung bình của nó. Do đó, nhà cung cấp nên sử dụng ước tính entropy tối thiểu hoặc đưa ra một giới hạn thấp hơn hợp lý và hợp lý về mặt thống kê đối với độ không đảm bảo đo được tạo ra.

- Nếu entropy được tạo ra bởi các vòng dao động, nhà cung cấp hoặc phòng thử nghiệm phải giải thích thiết kế của bộ tạo nhiễu ngẫu nhiên. Mô tả thiết kế trong Tài liệu tham khảo [3] có thể dùng làm ví dụ. Tuy nhiên, để hoàn thành mô tả nguồn entropy từ bản trình bày được tham chiếu, nhà cung cấp hoặc phòng thử nghiệm phải cung cấp giải thích, ít nhất là về mặt kinh nghiệm, cách đo jitters, các cách phép đo này được sử dụng để tạo ra số ngẫu nhiên thô cho NRBG và số entropy mà số ngẫu nhiên thô mang. Một lần nữa, mô tả thiết kế của nhà cung cấp sẽ dẫn đến mô hình ngẫu nhiên của các số ngẫu nhiên thô được tạo ra bởi nguồn nhiễu có thể được kiểm thử và có thể được sử dụng để lấy ra giới hạn dưới đáng tin cậy cho entropy đã tập hợp.

- Nếu RBG được gửi lại thường xuyên, ước tính về entropy của nhóm có thể được tăng lên tương ứng cho đến khi các giới hạn được đưa ra bởi thiết kế của nhóm entropy và hàm tạo đầu ra được đáp ứng nếu mô hình ngẫu nhiên của entropy cho thấy rằng việc xử lý entropy tiếp theo là độc lập hợp lý. Ví dụ, điều này có thể xảy ra nếu nguồn entropy vật lý là một mẫu đồng vị phóng xạ, tiếp tục phân rã độc lập (theo một nghĩa nào đó, và sau khi điều chỉnh theo số nguyên tử còn lại và thay đổi độ tin cậy của thiết bị phát hiện) của nó lịch sử và do đó trong trường hợp này, các giá trị entropy có thể được thêm vào mà không cần cung cấp thêm bất kỳ lý do nào ngoài việc xem xét các tác động đã đề cập. Tuy nhiên, lưu ý rằng nếu yêu cầu độ an toàn phía sau được đưa ra, ước tính về entropy chứa trong nhóm entropy thích hợp để hỗ trợ các mức an toàn đã tuyên bố phải chính đáng ngay cả sau khi có thỏa hiệp trạng thái đầy đủ.

7.2.2.3.4 Thu nhập entropy từ môi trường hoạt động

Nếu entropy được thu thập từ môi trường hoạt động của một mô-đun, thường sẽ không thể tìm ra một nguồn entropy cụ thể, duy nhất có thể được thu thập trong một mô hình ngẫu nhiên. Do đó, trong trường hợp này, việc đánh giá sẽ tập trung vào việc thu được các ước tính rất thận trọng về lượng entropy được thu thập và đảm bảo rằng các trạng thái hoạt động không an toàn được tránh một cách đáng tin cậy.

- Nếu entropy đến từ môi trường hoạt động của mô-đun, thì một phân tích cẩn thận phải được thực hiện về nguồn entropy và khả năng của những kẻ tấn công thực tế để quan sát hoặc ảnh hưởng đến các phần liên quan của môi trường hoạt động. Nếu nguồn này là nhà cung cấp entropy trong hệ điều hành (ví dụ: *getrandom()* hoặc */dev/random* trong hệ điều hành dựa trên Linux), thì cần phải phân tích cẩn thận entropy được tạo (có thể do nhà cung cấp hệ điều hành cung cấp). Nhà cung cấp hoặc phòng thử nghiệm có thể tham khảo phân tích được tuyên bố độc lập về *dev/random* và *dev/urandom* chẳng hạn như tài liệu tham khảo [9]. Cần thận trọng để đảm bảo rằng tuyên bố về entropy chỉ được đưa ra cho các phiên bản của bộ tạo *dev/random* hoặc *dev/urandom* đã nhận được đánh giá ngang hàng; Cho dù đây là trường hợp trong bất kỳ tình huống nào phụ thuộc vào phiên bản Linux RBG đang được xem xét và trạng thái của bài đánh giá khoa học đã tuyên bố (xem Tài liệu tham khảo [22]). Khi dựa vào kết quả về chất lượng entropy của nhà cung cấp hệ điều hành, điều quan trọng là phải kiểm tra xem các điều kiện hoạt động mà thuật toán được tìm thấy để cung cấp đủ entropy có được đáp ứng hay không. Ví dụ, một phân tích có thể phát hiện ra rằng thuật toán chỉ cung cấp entropy nếu phần cứng là x86 và nếu hệ điều hành không chạy trong máy ảo [xem phần tham khảo sau]:

- Đối với một số phiên bản nhất định của nhân Linux và nếu các điều kiện hoạt động cần thiết được thỏa mãn, dòng lập luận sau có thể được áp dụng trừ khi phân tích cẩn thận thấy khác sự minh chứng của *dev/random* là dễ dàng hơn trong cả hai. Hệ điều hành chỉ đáp ứng yêu cầu cho

một giá trị ngẫu nhiên khi nó thu thập entropy "vừa đủ"; nghĩa là khi ước tính riêng của nó về entropy được thu thập để có thể đáp ứng yêu cầu của mô-đun. Ví dụ: nếu mô-đun cần tạo khóa đối xứng 256-bit và do đó mô-đun yêu cầu 256-bit entropy thì hệ điều hành trả về không phải lệnh gọi *dev/random* cho đến khi nó có thể tạo ra nhiều entropy này. Cho đến lúc đó, mô-đun không thể tạo khóa đối xứng nói trên. Tuy nhiên, cài đặt chi tiết về phiên bản RBG đã sử dụng, nguồn entropy có sẵn trong một thiết bị cụ thể và các yếu tố liên quan khác sẽ được tính đến khi sử dụng bất kỳ bản khởi tạo cụ thể nào của Linux RBG. Ví dụ, không rõ ràng là các giả định được thực hiện bởi công cụ ước lượng entropy bên trong hệ điều hành sẽ giữ nguyên nếu nó chạy trên một máy ảo.

Trong trường hợp yêu cầu *dev/urandom*, hệ điều hành luôn gửi trả lời ngay lập tức trở lại mô-đun. Câu trả lời này có thể có hoặc không thể có lượng entropy mong muốn. Hành động không chặn của *dev/urandom* ngụ ý rằng ứng dụng tiêu thụ không có đảm bảo về lượng entropy mà nó nhận được.

Để đáp ứng các yêu cầu, trước tiên nhà cung cấp phải chứng minh rằng lệnh gọi ban đầu (nghĩa là lần gọi đầu tiên sau khi mô-đun đã được khởi động hoặc khởi tạo) tới *dev/urandom* trả về lượng entropy được yêu cầu. Một cách khả thi để đạt được điều này là phân tích chuỗi sự kiện xảy ra trước lệnh gọi ban đầu này. Ví dụ, nếu trình tự này bao gồm một số lần khởi động lại mô-đun và nếu mỗi lần khởi động lại này bao gồm một số sự kiện được đo và cung cấp độ không đảm bảo mong muốn, thì có thể đưa ra tuyên bố phỏng đoán về entropy trong lần gọi ban đầu. Các sự kiện này có thể bao gồm thời gian giữa các lần khởi động lại, các phép đo hoạt động của người vận hành trong quá trình khởi động lại (nhấp chuột, v.v.), các giá trị được lưu trữ trong các vị trí bộ nhớ nhất định được biết là không thể đoán trước được trong quá trình khởi động lại. Lập luận này có cơ hội thành công đối với các mô-đun độc lập; các mô-đun nhúng thường không yêu cầu khởi động lại nhiều lần vì vậy việc sử dụng *dev/urandom* trong các mô-đun như vậy khó được chứng minh hơn. Các lưu ý tương tự như được giải thích trong ví dụ *dev/random* cũng được áp dụng.

Nếu nhà cung cấp có thể biện minh rằng có 100-bit entropy được trả về trong lần gọi đầu tiên *tới dev/urandom*, thì nhà cung cấp thường có thể tiếp tục tuyên bố rằng ít nhất 100-bit đã đạt được độ bền an toàn trong mỗi lần gọi tiếp theo. Lý do cơ bản cho điều này là nhiều phiên bản của *dev/random* được thiết kế để hoạt động giống như một PRNG mạnh sau khi được tạo hạt giống ban đầu ngay cả khi không có thêm đầu vào entropy. Do đó, theo quan điểm của kẻ tấn công, sự không chắc chắn về bất kỳ tập con nào của chuỗi đầu ra có độ dài ít nhất xấp xỉ bằng lượng entropy trong mầm phải bằng entropy của chúng về trạng thái của mầm.

Lưu ý: Các ứng dụng nhằm mục đích cung cấp độ an toàn phía sau lý tưởng cần một trình tạo số ngẫu nhiên cung cấp ít nhất là độ an toàn phía trước nâng cao, vì nếu không trạng thái RBG có thể được xem như là một bí mật lâu dài cho phép kẻ tấn công xâm phạm các lần chạy giao thức trong quá khứ. Tương tự như vậy, nếu trong cài đặt này, RBG được sử dụng mà không cung cấp khả năng độ an toàn phía sau nâng cao (tức là thường được tạo lại mầm hoặc tạo lại mầm không đủ entropy) thì kẻ tấn công học được trạng thái bên trong của RBG có thể ảnh hưởng đến việc thực thi giao thức trong tương lai. Nói chung, những cân nhắc ví dụ này ngụ ý rằng cần phải cẩn thận để xem xét các yêu cầu của ứng dụng tiêu dùng trước khi xác nhận một RBG cụ thể để sử dụng, trừ khi RBG là bộ tạo số ngẫu nhiên lai ghép với việc tạo lại mầm thường xuyên, độ an toàn phía trước ngay cả trong trường hợp nguồn nhiễu bị hỏng, độ an toàn phía trước nâng cao và lý tưởng là độ an toàn phía sau nâng cao.

7.2.2.3.5 Sự cân nhắc

Trong mọi trường hợp, mô tả thiết kế phải bao gồm thông tin về mức độ ảnh hưởng của sự lão hóa hoặc lỗi gây ra do thiệt hại gây ra đối với hoạt động của nguồn nhiễu. Ví dụ: trong trường hợp bộ tạo bit ngẫu nhiên dựa trên nguồn phóng xạ, sự lão hóa sẽ tự biểu hiện ở việc giảm số nguyên tử không ổn định còn lại theo thời gian cũng như có thể trong cơ chế phát hiện các sự kiện phân rã trở nên kém tin cậy hơn. Hiệu ứng sau khó hiểu rõ trong ví dụ này hơn nhiều so với hiệu ứng trước và do đó đáng được nghiên cứu sâu hơn.

Đối với các nguồn dựa trên chất bán dẫn, đặc điểm lão hóa có thể dựa trên các mô hình.

7.2.3 Min entropy

Việc tính toán entropy theo Shannon của một nguồn nhiễu có thể khó khăn; hơn nữa, entropy theo Shannon có thể sai lệch đáng kể so với entropy dự đoán, tức là nó không (trong trường hợp chung là các phân phối gần như không đồng đều) cho phép dự đoán đáng tin cậy về khối lượng công việc dự kiến mà kẻ tấn công phải thực hiện để đoán, ví dụ: một khóa mật mã. được tạo ra bởi một bộ tạo bit ngẫu nhiên nhất định. Tuy nhiên, những sai lệch này phần lớn là lành tính theo quan điểm mật mã: trong khi không có giới hạn trên đối với entropy dự đoán của một phân phối có thể được rút ra từ việc biết entropy theo Shannon của nó, và trong khi bản thân entropy theo Shannon không phải là giới hạn cận dưới entropy dự đoán, như vậy một giới hạn cận dưới có thể được suy ra từ nó [10]. Về cơ bản, entropy dự đoán không bao giờ vượt quá hai bit, thấp hơn entropy theo Shannon và đối với các phân phối có entropy lớn (hơn một vài bit), nó rất gần, thấp hơn một bit so với entropy theo Shannon.

Nhưng bản thân entropy dự đoán, ngoài việc rất khó ước tính chính xác cho các thử nghiệm ngẫu nhiên trong thế giới thực, không trả lời đầy đủ các câu hỏi mà đánh giá viên quan tâm đến bộ tạo bit ngẫu nhiên mật mã. Có thể khối lượng công việc dự kiến của việc đoán một chuỗi bit được tạo ra bởi một quá trình ngẫu nhiên nào đó là rất cao, nhưng khả năng đoán đúng rất sớm khi thực hiện chiến lược đoán tối ưu (ví dụ: trong lần thử đầu tiên) cũng rất cao. Về nguyên tắc, người ta muốn có một số đảm bảo về hình thức rằng một cuộc tấn công thành công với xác suất p phải thực hiện công việc phỏng đoán theo thứ tự ít nhất là $N * p$, đối với một số N lớn (giả sử, $N > 2^{100}$).

Khái niệm đơn giản nhất về entropy cho phép người ta có được sự đảm bảo thuộc loại này là min entropy. Rõ ràng min entropy là giới hạn cận dưới entropy theo Shannon và do đó nó có thể được sử dụng (với khả năng mất khoảng hai bit) để giới hạn cận dưới entropy dự đoán. Mặt khác, entropy theo Shannon có thể có một số lợi thế thực tế so với min entropy trong một số trường hợp, ví dụ: sự tồn tại của một quy tắc chuỗi entropy đơn giản cho các biến ngẫu nhiên phụ thuộc. Đối với các phân bố có thể chỉ lệch theo một số cách nhỏ so với phân bố lý tưởng, phân bố của entropy theo Shannon sẽ rất giống với min entropy và đôi khi có thể dễ dàng hơn để tính toán.

Ước tính min entropy được tạo ra là sự đơn giản hóa một trong các phương pháp được đề xuất trong Tài liệu tham khảo [2] như sau:

Phương pháp này sẽ chỉ áp dụng nếu các nguồn nhiễu (và bất kỳ thành phần biến đổi nào, nếu có) là IID (biến ngẫu nhiên phân phối độc lập và đồng nhất). Xem Tài liệu tham khảo [2] (điều khoản 9.1.1) hoặc bất kỳ sách giáo khoa thống kê nào để biết giải thích về khái niệm này. Không nhất thiết các nguồn phải tạo ra sự phân bố đồng nhất các kết quả: xác suất của các kết quả khác nhau có thể khác nhau. Tuy nhiên, phân phối xác suất đồng nhất giữa các nguồn (hoặc giữa các kết quả đọc khác nhau của đầu ra ngẫu nhiên trong mỗi nguồn) và các xác suất này không phụ thuộc vào kết quả của các sự kiện khác do các nguồn này tạo ra.

Tìm xác suất của kết quả chung nhất trong số tất cả các sự kiện có thể xảy ra do nguồn nhiễu tạo ra. Nếu xác suất này đã được biết trước, thì nó có thể được sử dụng. Nhà cung cấp hoặc phòng thử nghiệm phải giải thích lý do tại sao xác suất này là giá trị mà nó được tuyên bố. Trường hợp chưa rõ, thì theo Tài liệu tham khảo [2], lấy một tập dữ liệu với N mẫu và đếm số lần xuất hiện của giá trị phổ biến nhất trong tập dữ liệu. Một lần nữa, theo Tham chiếu [2], hãy đếm số lần xuất hiện của giá trị phổ biến nhất này trong tập dữ liệu và biểu thị kết quả.

Tài liệu tham khảo [2] trình bày phương pháp tính toán min entropy của nguồn nhiễu bằng cách tính toán khoảng tin cậy xung quanh tần số quan sát của kết quả có khả năng xảy ra nhất theo kinh nghiệm của thử nghiệm được lấy mẫu ngẫu nhiên. Giới hạn cận trên của khoảng tin cậy này sau đó trong Tài liệu tham khảo [2] được sử dụng như một ước lượng thận trọng của min entropy.

Giả định phân phối độc lập và đồng nhất (IID) cho các số ngẫu nhiên thô sẽ được lập luận riêng dựa trên thiết kế của nguồn ngẫu nhiên thô. Đối với các phân phối có hỗ trợ nhỏ, bản thân giả định IID sau đó đã có thể thỏa mãn như một mô hình ngẫu nhiên của các số ngẫu nhiên thô.

7.2.4 Các kiểm thử thống kê

Nhà cung cấp sẽ tiến hành các bài thử nghiệm thống kê trong giai đoạn tạo bit ngẫu nhiên mục tiêu thông qua mô hình ngẫu nhiên của họ. Liên quan đến vấn đề này, cần nhấn mạnh rằng bằng

chứng cho thấy các kết quả không gây hại của các thử nghiệm thống kê cung cấp nhằm thiết lập sự tin cậy vào một nguồn ngẫu nhiên nhất định phụ thuộc vào nhiều yếu tố khác nhau:

- Bất kỳ bằng chứng thống kê nào hỗ trợ cho các tuyên bố về entropy do nhà cung cấp trình bày sẽ được thu thập riêng biệt với bất kỳ thử nghiệm thống kê nào về các thành phần đã được thực hiện trong quá trình phát triển; tại thời điểm khi bằng chứng thống kê được thu thập, thiết kế sẽ được sửa. Quy tắc này nhằm ngăn chặn tình huống sau: một thiết kế yếu đang được tinh chỉnh để làm cho nó mạnh hơn. Các chỉnh sửa đang được thử không cải thiện thiết kế và các bài thử nghiệm thống kê liên tục bị thất bại. Nhưng sau một vài lần lặp lại, kiểm thử được sử dụng tình cờ giảm xuống dưới mức được chỉ định, mà thiết kế đang nghiên cứu trở nên mạnh mẽ hơn đáng kể và kiểm thử được đánh giá là đã vượt qua.

- Phải tránh tình huống trong đó một nguồn ngẫu nhiên được "điều chỉnh" lặp đi lặp lại để vượt qua các thử nghiệm thống kê nhất định. Mối quan tâm lớn nhất ở đây là quá trình phát triển như vậy có thể dẫn đến một cấu trúc che giấu những điểm yếu của thiết kế ban đầu khỏi bộ thử nghiệm thống kê được sử dụng mà không loại bỏ chúng; xem ví dụ RBG được trình bày trong Tài liệu tham khảo [11] và phần tiếp theo của nó trong Tài liệu tham khảo [12] để làm ví dụ thực tế về sự nguy hiểm của việc sử dụng một bộ các thử nghiệm thống kê làm tiêu chuẩn chính cho RBG mật mã.

- Việc kiểm thử sẽ nhắm vào giai đoạn đầu của quá trình tạo bit ngẫu nhiên được mô tả bằng mô hình ngẫu nhiên. Tùy thuộc vào quá trình hậu xử lý nào được thực hiện để thu được các số ngẫu nhiên đầu ra từ các số ngẫu nhiên thô, tiện ích của việc thực hiện các thử nghiệm thống kê trên đầu ra của một RBG có phạm vi từ không dùng được đến không rõ ràng, ít nhất là khi mục tiêu là đánh giá mức độ phù hợp của nguồn ngẫu nhiên cơ bản. Các kiểm thử về số ngẫu nhiên đầu ra cũng có thể hữu ích, nhưng nói chung chỉ để đảm bảo rằng việc chuyển đổi từ số ngẫu nhiên thô sang số ngẫu nhiên đầu ra đã được thực hiện một cách thỏa đáng.

Nhà cung cấp phải chứng minh thêm rằng kết quả kiểm thử hỗ trợ cơ sở lý luận do nhà cung cấp cung cấp. Thông thường, cần một số thử nghiệm thống kê để có được một ước lượng hợp lý về entropy. Một số kiểm thử thiết lập mức độ tin cậy về tính độc lập của các giá trị quan sát được. Các bài kiểm thử khác có thể kiểm tra các lần chạy ngắn và dài của các bit và kiểm tra lại một lần nữa hoạt động của các lần chạy này để biết tính nhất quán của chúng với các thuộc tính được yêu cầu của nguồn được kiểm thử. Các tài liệu tham khảo [1], [2] và [7] có thể được sử dụng làm hướng dẫn cung cấp thông tin. Cơ sở lý luận phải đúng về mặt toán học và phù hợp với các tuyên bố của nhà cung cấp về tính ngẫu nhiên. Việc lựa chọn kiểm thử phải phù hợp để bác bỏ mô hình ngẫu nhiên của nguồn ngẫu nhiên do nhà cung cấp cung cấp nếu nó không thành công theo những cách có vẻ hợp lý khi kiểm thử kết cấu của nguồn.

Nhà cung cấp phải cung cấp tài liệu về quá trình phát triển của nguồn ngẫu nhiên cùng với cơ sở thiết kế. Đánh giá viên sau đó sẽ kiểm tra xem quá trình phát triển có tránh được những liên quan về việc thiết kế đã được điều chỉnh để vượt qua một tiêu chuẩn thống kê nhất định hay không.

Phụ lục B cung cấp thông tin kiểm thử cho các thử nghiệm thống kê mẫu. Tài liệu tham khảo [2] cho thấy một chuỗi các thử nghiệm thống kê cho phép nhà cung cấp kiểm tra xem các nguồn nhiễu có phải phân phối độc lập và đồng nhất (IID) hay không. Các bài kiểm thử này có thể được sử dụng để kiểm tra giả định IID theo nghĩa là trường hợp họ có thể ngẫu nhiên bác bỏ nó. Tuy nhiên, giả định IID cũng sẽ được hỗ trợ bởi sự hiểu biết định tính về nguồn nhiễu. Chỉ riêng các bài thử nghiệm thống kê là không đủ để hỗ trợ tuyên bố về sự phân phối độc lập và giống hệt nhau của các bit ngẫu nhiên thô. Kết quả kiểm thử phải được thu thập ở các điều kiện môi trường đại diện bên trong dải hoạt động bình thường (ví dụ: 25°C, 0°C, +100°C đối với nhiệt độ). Trong phạm vi mà bản thân thiết bị không có khả năng phát hiện việc lệch khỏi phạm vi hoạt động bình thường, thì theo hướng dẫn vận hành phải đảm bảo rằng thiết bị không phải chịu các điều kiện bên ngoài chế độ đã chỉ ra.

Chú thích: Có nhiều cách mà nguồn ngẫu nhiên có thể không tạo ra đầu ra IID, nhưng một tập hợp hữu hạn các thử nghiệm thống kê trong thực tế chỉ có thể phát hiện một số sai sót cụ thể. Ví dụ, một nguồn entropy có sự phụ thuộc phức tạp giữa các bit đầu ra của nó hoặc có các bit đầu ra liên quan không gần nhau thì không phải là IID và có thể có các điểm yếu có thể khai thác được. Nhưng có thể tưởng tượng được rằng một nguồn như vậy vẫn có thể vượt qua các bài thử nghiệm thống kê hộp đen cho IID một cách đáng tin cậy.

7.3 Đánh giá

7.3.1 Yêu cầu chung

Việc đánh giá NRBG có thể được thực hiện bởi phòng thử nghiệm phù hợp với tiêu chuẩn đánh giá nhất định và phương pháp đánh giá liên quan. NRBG có thể là một thành phần của ứng dụng hoặc thiết bị mật mã có các yêu cầu được mô tả trong TCVN 8709 (ISO/IEC 15408).

7.3.2 Đầu vào của nhà cung cấp để kiểm tra sự phù hợp

7.3.2.1 Yêu cầu chung

Có một số yếu tố nhất định trong quá trình xác thực thiết kế của bộ tạo bit ngẫu nhiên mà đánh giá viên sẽ chủ yếu dựa vào thông tin do nhà cung cấp cung cấp. Điều khoản này sẽ cung cấp một số chi tiết về các yêu cầu đối với đầu vào của nhà cung cấp đối với quá trình đánh giá.

Nhà cung cấp phải cung cấp tất cả các tài liệu cần thiết để có bằng chứng chứng minh về việc đã thực hiện theo các yêu cầu:

- Mục tiêu an toàn được xác định rõ ràng;

- Mô tả kỹ thuật của nguồn entropy;

- Một mô hình ngẫu nhiên trong một giai đoạn thích hợp của quá trình tạo bit ngẫu nhiên (hoặc lập luận phỏng đoán cận dưới entropy được thu thập nếu việc thu thập mô hình ngẫu nhiên là không khả thi);

- Dữ liệu kiểm thử thu được từ thiết bị và đánh giá thống kê của dữ liệu kiểm thử thu được, bao gồm cả việc giải thích dựa trên mô hình ngẫu nhiên về lý do tại sao các thử nghiệm thống kê đã chọn phù hợp để sao lưu các tuyên bố an toàn liên quan đến nguồn ngẫu nhiên được thực hiện theo mục tiêu an toàn;

- Đặc điểm kỹ thuật của bất kỳ bước kiểm tra chất lượng và kiểm tra tổng số lỗi;

- Giải thích lý do tại sao toàn bộ các kiểm tra chất lượng và kiểm tra tổng số lỗi đã chọn là phù hợp;

- Đặc điểm kỹ thuật của bất kỳ bước hậu xử lý hoặc điều kiện nào được thực hiện để thu được kết quả đầu ra từ các số ngẫu nhiên thô;

- Việc minh chứng dựa trên các thuộc tính của nguồn ngẫu nhiên và của bất kỳ bước hậu xử lý nào biện minh cho tất cả các tuyên bố an toàn được đưa ra trong mục tiêu an toàn.

7.3.2.2 Mục tiêu an toàn

Nhà cung cấp sẽ cung cấp mục tiêu an toàn cho RBG. Mục tiêu an toàn phải xác định rõ ràng min entropy dự kiến sẽ được cung cấp bởi mỗi lần gọi tới NRBG trong các điều kiện hoạt động ít thuận lợi nhất vẫn nằm trong vùng hoạt động của thiết bị. Ước tính entropy theo Shannon có thể chấp nhận được thay vì ước tính min entropy nếu sai sót entropy rất thấp.

Yêu cầu về entropy sẽ được biểu thị định lượng, tức là dưới dạng số bit entropy trên mỗi lần gọi RBG.

Mục tiêu an toàn cũng phải phác thảo rõ ràng phạm vi điều kiện hoạt động của thiết bị để hoạt động theo và bất kỳ giả định bổ sung nào cần thiết để hỗ trợ hoạt động an toàn. Nó sẽ bao gồm một tuyên bố về các thuộc tính cơ bản của bộ tạo bit ngẫu nhiên. Tuyên bố này sẽ được hỗ trợ bởi tài liệu thiết kế phù hợp và phải bao gồm liệu RBG là tất định hay bất định, liệu việc tạo mầm có dựa trên các hiệu ứng vật lý chuyên dụng hay không, liệu tính an toàn của nó có thể được sao lưu bằng các lập luận về mật mã theo các giả định tiêu chuẩn hay không và liệu chuyển độ an toàn phía sau, độ an toàn phía trước và các phiên bản nâng cao của chúng được hỗ trợ.

Mục tiêu an toàn sẽ phác thảo bất kỳ thuộc tính nào của RBG mà nhà cung cấp biết được và những thuộc tính nào khác với các mong muốn chung về tính chất RBG dựa trên phần còn lại của các yêu cầu an toàn do nhà cung cấp đưa ra.

7.3.2.3 Mô tả kỹ thuật của nguồn entropy

Nhà cung cấp phải cung cấp mô tả kỹ thuật đầy đủ của nguồn entropy. Nếu một nguồn entropy chuyên dụng được sử dụng, ví dụ, điều này có thể có dạng sơ đồ mạch hoàn chỉnh của một mạch điện tử có đầu ra của nó là các số ngẫu nhiên thô. Trong trường hợp này, mô tả phải có giải thích về tác động vật lý cơ bản nào được khai thác để có được tính ngẫu nhiên.

Nếu nguồn không chuyên dụng được sử dụng, mô tả phải bao gồm danh sách tất cả các thành phần phần cứng dự kiến sẽ có trong hệ thống và phải giải thích cách các thành phần phần cứng này đang được truy vấn để thu được entropy. Nếu các tuyên bố an toàn tiếp theo dựa trên các hiệu ứng vật lý xảy ra trong một số thành phần phần cứng, thì mô tả phải có giải thích lý do tại sao các hiệu ứng vật lý này được mong đợi tạo ra sự ngẫu nhiên.

7.3.2.4 Mô hình ngẫu nhiên

Nhà cung cấp sẽ cung cấp mô hình ngẫu nhiên của các số ngẫu nhiên thô hoặc của một giai đoạn gần nhất thích hợp của quá trình tạo bit ngẫu nhiên, như một phần của tài liệu hỗ trợ tuyên bố về entropy của họ. Xem điều khoản 6.2.1 để biết chi tiết về các yêu cầu liên quan đến mô hình ngẫu nhiên. Nếu không thể xây dựng một mô hình ngẫu nhiên thì có thể đệ trình lập luận phỏng đoán theo các yêu cầu của điều khoản 6.2.2.

7.3.2.5 Kiểm thử do nhà cung cấp xác định

Nhà cung cấp sẽ cung cấp bằng chứng dựa trên thử nghiệm thống kê sao lưu tuyên bố về entropy của họ. Nhà cung cấp phải cung cấp cơ sở lý luận cho thấy rằng các phép thử thống kê được sử dụng cùng với mô hình ngẫu nhiên của nguồn ngẫu nhiên có thể hạn chế lượng entropy do nguồn ngẫu nhiên phát ra ở mức bằng hoặc cao hơn tuyên bố entropy với mức độ tin cậy cao (xem Phụ lục A).

7.3.2.6 Kiểm tra chất lượng

Nhà cung cấp phải cung cấp tài liệu về kiểm tra chất lượng và kiểm tra tổng số lỗi được thực hiện tại nguồn. Tiêu chuẩn này phải đủ chính xác để cho phép thực hiện lại quá trình kiểm tra chất lượng và kiểm tra tổng số lỗi. Nó cũng phải chỉ định chính xác giai đoạn tạo bit ngẫu nhiên đang được kiểm thử. Nhà cung cấp phải chỉ ra rằng các sai lệch so với hiệu suất dự kiến gây ra việc thiếu hụt entropy dưới yêu cầu an toàn do nhà cung cấp đưa ra sẽ được phát hiện bằng các bài kiểm tra chất lượng được chọn với xác suất cao.

7.3.2.7 Các thành phần biến đổi

Nếu sử dụng thành phần biến đổi, nhà cung cấp phải cung cấp thông số kỹ thuật của thành phần biến đổi. Thông số kỹ thuật do nhà cung cấp cung cấp phải bao gồm phân tích toán học tại sao tuyên bố entropy được đưa ra lại được đáp ứng ở đầu ra của thành phần biến đổi. Nó phải bao gồm lập luận chặt chẽ về việc liệu thành phần có can thiệp vào bất kỳ phương pháp kiểm tra chất lượng nào được sử dụng hay không và làm thế nào để bản thân thành phần đó có thể bị hỏng.

8 Tổng quan về bộ tạo bit ngẫu nhiên tất định

8.1 Nhận xét chung

Ranh giới giữa bộ tạo bit ngẫu nhiên tất định lai ghép và bộ tạo bit ngẫu nhiên thuần túy về bản chất không được phân định rõ ràng; một DRBG có thể thay mầm mới thường xuyên. Đối với mục đích của tiêu chuẩn này, bộ tạo bit ngẫu nhiên được gọi là tất định nếu việc thay mầm mới không được thực hiện liên tục. Thuộc tính quan trọng của RBG tất định được đánh giá là trong một loạt các tình huống tấn công, nó cung cấp đầu ra không thể phân biệt được với dữ liệu ngẫu nhiên được phân phối lý tưởng bởi một kẻ tấn công bị giới hạn về mặt tính toán.

Trong thiết lập này, về nguyên tắc, có những phạm vi sau đây cần được kiểm tra trong quá trình đánh giá DRBG:

- Khởi tạo mầm: Nhà cung cấp phải chứng minh rằng quá trình khởi tạo và phân phối mầm không thể bị khai thác bởi một kẻ tấn công có đầy đủ thông tin về thiết kế DRBG để phá vỡ bất kỳ thuộc tính an toàn nào đã được tuyên bố của DRBG nhanh hơn đáng kể so với mức mức an toàn được xác nhận cho DRBG. Khi lập luận rằng việc tạo mầm ban đầu có thuộc tính này, nhà cung cấp có

thể sử dụng các giả định về độ cứng mật mã được chấp nhận chung, nhưng họ sẽ làm cho các giả định này rõ ràng.

Chú thích: Một mầm có entropy cao, thậm chí cùng với hàm chuyển đổi trạng thái và hàm tạo đầu ra hoạt động tốt cùng nhau nói chung không đủ để đảm bảo các đặc tính tốt ở mức đầu ra RBG. Ví dụ: không khó để xây dựng một DRBG có độ an toàn phía sau, độ an toàn phía trước và độ an toàn phía trước nâng cao nếu trạng thái mầm được chọn ngẫu nhiên đồng nhất từ tập hợp tất cả các trạng thái có thể, nhưng đối với hàm chuyển đổi trạng thái mức cao cũng có số lượng điểm cố định có thể tính toán hiệu quả. Trong cách xây dựng như vậy, có thể hình dung quá trình tạo mầm chỉ tạo ra các điểm cố định của hàm chuyển đổi trạng thái trong khi vẫn giữ nguyên entropy cao, do đó làm mất tác dụng của tất cả các đảm bảo an toàn của DRBG.

- Thay mầm mới: Nếu một vài dự đoán độ bền đang được xác nhận trong mục tiêu an toàn do nhà cung cấp cung cấp, thì việc thay mầm mới sẽ sử dụng nguồn entropy có chất lượng cao. Entropy thu thập được trong quá trình thay mầm mới sẽ được định lượng và quá trình thay mầm mới sẽ phải tuân theo các bước đánh giá tương tự như khi khởi tạo mầm. Các tiêu chí tương tự sẽ được áp dụng bất cứ khi nào quá trình thay mầm mới có thể làm giảm entropy của trạng thái bên trong DRBG (ví dụ: nếu một phần của trạng thái bên trong bị ghi đè bằng dữ liệu ngẫu nhiên mới được tạo). Trong tất cả các trường hợp khác, nên sử dụng nguồn entropy có chất lượng cao.

- Thiết kế của quá trình chuyển đổi trạng thái và hàm tạo đầu ra phải được đánh giá. Các tuyên bố an toàn được đưa ra cho DRBG trong mục tiêu an toàn đã gửi sẽ có thể giảm thiểu các vấn đề khó khăn về mật mã, ví dụ: đối với các thuộc tính được nghiên cứu kỹ lưỡng các nguyên thủy mật mã được sử dụng, chẳng hạn như tính một chiều của hàm băm hoặc của mật mã khối khi được xem như một chức năng của khóa. Lập luận hỗ trợ các thuộc tính an toàn được tuyên bố sẽ xem xét sự phân phối giả định của các giá trị mầm như được suy ra từ các thuộc tính của quá trình tạo mầm. Tất cả các thuộc tính an toàn được xác nhận quyền sở hữu sẽ được chứng minh là có khả năng tuân theo các tính toán mật mã tiêu chuẩn chống lại những kẻ tấn công có thể thực hiện các nguyên thủy mật mã cơ bản (chẳng hạn như hàm băm, mật mã khối) lên đến 2^n lần hoặc để thực hiện các phép tính khác với hệ số chi phí tương tự, trong đó n là khẳng định độ an toàn của RBG.

- Việc thực hiện các hàm chuyển đổi trạng thái và đầu ra phải được kiểm tra sự phù hợp với các thông số kỹ thuật của chúng và so với các bài kiểm tra đáp án đã biết.

Các thuộc tính quan trọng của RBG tất định được xác định sẽ phải đánh giá, trong một loạt các tình huống tấn công, cung cấp đầu ra mà kẻ tấn công bị giới hạn về mặt tính toán không thể phân biệt được với dữ liệu ngẫu nhiên được phân phối lý tưởng. Kẻ tấn công bị giới hạn về mặt tính toán theo nghĩa này là kẻ tấn công không thể thực thi thêm nhiều tính toán trong một số hoạt động mật mã đơn giản (ví dụ: tính toán băm trên một khối thông điệp) so với được chỉ ra bởi mức an toàn được xác nhận của RBG.

Các đặc tính sau đây thường phải được kiểm thử:

- Độ an toàn phía sau và độ an toàn phía trước có thể được hiển thị theo các giả định mật mã tiêu chuẩn. Khả năng dự đoán độ bền và độ an toàn phía trước nâng cao cần được kiểm tra trong các bộ tạo bit sẽ được đánh giá với mục đích sử dụng chúng trong các ứng dụng mật mã tùy ý hoặc nếu ứng dụng tiêu thụ cần các thuộc tính này. Trong hai thuộc tính này, độ an toàn phía trước nâng cao là bắt buộc để đánh giá trong tiêu chuẩn này nếu RBG được sử dụng trong các ứng dụng tùy ý; khả năng dự đoán độ bền chỉ là bắt buộc giữa các lần thay mầm mới, nhưng nói chung là một đặc tính rất mong muốn đạt được giữa các lần gọi RBG khác nhau.

- Việc thay mầm mới và (tùy chọn) cung cấp đủ entropy để hỗ trợ các đảm bảo an toàn mật mã được xác nhận theo điểm trước đó.

- Kiểm tra chất lượng được thực hiện trên tất cả các thành phần của RBG. Điều này là quan trọng nhất đối với cơ chế tạo mầm và thay mầm mới; kiểm tra chất lượng của thành phần xác định có thể được thực hiện một lần khi khởi động bằng cách xử lý một số vectơ kiểm thử.

Bảo vệ khỏi tấn công kênh kề và các cuộc tấn công phát hiện lỗi có tầm quan trọng như nhau đối với thành phần tất định và bất định.

Nếu mục tiêu an toàn cho RBG yêu cầu mức an toàn cho RBG theo TCVN 11295:2016 (ISO 19790:2012) thì việc đánh giá kênh kề ở mức tối thiểu phải bao gồm các phương pháp kiểm thử

và đánh giá áp dụng được đưa ra trong TCVN 12212:2018 (ISO/IEC 17825:2016). Nếu không có mức an toàn theo theo tiêu chuẩn TCVN 11295:2016 (ISO 19790:2012) được tuyên bố trong mục tiêu an toàn, sau đó đánh giá viên có thể xác định mức an toàn áp dụng từ các điều kiện hoạt động đã nêu và mục đích sử dụng của RBG và sử dụng mức an toàn đó làm cơ sở để đánh giá giảm thiểu kênh kề.

8.2 Tổng quan về cấu trúc của bộ tạo bit ngẫu nhiên tất định

Về mặt cấu trúc, không có sự khác biệt cơ bản giữa DRBG và NRBG. Do đó, tất cả các nhận xét và yêu cầu của điều khoản 6.3.2 và điều khoản 6.3.3 được áp dụng không thay đổi. Về yêu cầu đánh giá, sự khác biệt giữa DRBG và NRBG là một trong những điểm nhấn mạnh: DRBG là bộ tạo bit ngẫu nhiên mà việc thay mầm mới không được diễn ra liên lục; do đó, tính an toàn của chúng hoàn toàn dựa trên các giả định về độ phức tạp tính toán. Điều này có những hậu quả sau:

- Không giống như đối với bộ tạo bit ngẫu nhiên bất định, một vài ứng dụng có thể chấp nhận các sai xót nhỏ thống kê trong các số ngẫu nhiên đầu ra mà không cần đến các biện pháp an toàn nêu trên, việc sử dụng các cơ chế mật mã mạnh trong bộ tạo bit ngẫu nhiên là bắt buộc đối với các bộ tạo bit ngẫu nhiên tất định. Đánh giá viên phải đảm bảo rằng độ an toàn phía sau, độ an toàn phía trước và độ an toàn phía trước nâng cao của DRBG có thể được chứng minh là có hiệu lực theo các giả định mật mã tiêu chuẩn nếu mầm của DRBG cung cấp đủ entropy. Ngay cả những điểm yếu đã được hiểu rõ của việc xây dựng DRBG cũng phải được xử lý một cách thận trọng nhất. Không có sai lệch thống kê nào có thể được chứng minh được theo kinh nghiệm trong đầu ra số ngẫu nhiên được coi là có thể chấp nhận được đối với DRBG.

- Việc không thay mầm mới liên tục cũng có nghĩa là cần phải đặc biệt chú ý đến sự cần thiết phải đảm bảo rằng khởi tạo mầm có chất lượng cao. Do đó, độc lập với các tuyên bố an toàn do nhà cung cấp đưa ra trong mục tiêu an toàn, DRBG phải được tạo mầm với ít nhất 120-bit Entropy theo Shannon và phải có trạng thái bên trong ít nhất 200-bit. Nếu một trong hai điều kiện này không được đáp ứng, báo cáo đánh giá sẽ ghi lại điều này, nhưng vẫn có thể chấp nhận tất cả các yêu cầu an toàn do nhà cung cấp đưa ra.

- Một điều bắt buộc lưu ý là giá trị gốc cũng như các lần lặp tiếp theo của giá trị trạng thái bên trong đều không được để kẻ tấn công nắm được. Mặc dù bộ tạo bit ngẫu nhiên bất định thường sẽ có một số khả năng khôi phục từ sự trạng thái thỏa hiệp, nhưng điều này không đúng với bộ tạo bit ngẫu nhiên tất định.

9 Kiểm tra sự phù hợp của DRBG

9.1 Tổng quan

Các mục tiêu kiểm thử sự phù hợp đối với DRBG được nêu trong điều khoản 7. Nói chung, tất cả các nhận xét được đưa ra trong điều khoản 7 đều được áp dụng. Vì lý do này, phần đó sẽ chỉ chỉ ra một số vấn đề trong tài liệu của thiết kế RBG cần được đặc biệt chú ý khi đánh giá DRBG.

9.2 Kiểm thử

9.2.1 Tài liệu thiết kế

Trong trường hợp của DRBG, tài liệu thiết kế được trình theo các yêu cầu nêu trong điều khoản 7 phải cung cấp bằng chứng về việc đạt được độ an toàn phía trước, độ an toàn phía sau và độ an toàn phía trước nâng cao dựa trên các giả định tiêu chuẩn về độ cứng mật mã. Ngoài ra, thiết kế phải xem xét các cuộc tấn công kênh kề và tấn công tiêm lỗi chống lại các hàm tạo đầu ra và hàm chuyển đổi trạng thái cũng như bảo vệ tính bí mật của trạng thái bên trong một cách đáng tin cậy. Các yêu cầu về tài liệu và mục tiêu thiết kế của nguồn ngẫu nhiên được sử dụng để tạo mầm như trong điều khoản 7.

CHÚ THÍCH 1: Việc tiêu chuẩn này đề cập cụ thể đến các điểm trên liên quan đến bộ tạo bit ngẫu nhiên tất định không có nghĩa là chúng không được xem xét khi đánh giá bộ tạo bit ngẫu nhiên lai ghép theo điều khoản 7. Về nguyên tắc, các điểm giống nhau áp dụng để đánh giá các phần tất định của tất cả các bộ tạo bit ngẫu nhiên lai ghép.

CHÚ THÍCH 2: Độ an toàn phía trước nâng cao được theo quan điểm hoàn toàn là phân tích mật mã có thể đạt được bởi các cấu trúc có hàm chuyển đổi trạng thái mạnh, nhưng làm rò rỉ một phần trạng thái bên trong đầu ra; ví dụ: hãy tưởng tượng một cấu trúc bọt biển (sponge) dựa trên một

ánh xạ ngẫu nhiên tùy ý thay vì một hoán vị như thành phần mật mã cốt lõi. Tuy nhiên, cần lưu ý rằng các cấu trúc làm rò rỉ một phần trạng thái bên trong mà không được hậu xử lý nó có thể mang lại tính ngẫu nhiên xấu ngay lập tức nếu kẻ tấn công có thể điều khiển trạng thái bên trong, ví dụ: bằng cách áp dụng một cuộc tấn công lỗi. Ngoài ra, các cuộc tấn công kênh kề có thể trở nên dễ dàng hơn nếu có rò rỉ trạng thái, vì đối phương có thể thiết kế, ví dụ: các nguồn mẫu với dữ liệu đã biết một phần cho thiết bị chính xác đang bị tấn công. Do đó, việc bổ sung an toàn mật mã bảo vệ chống rò rỉ một phần trạng thái được khuyến khích trong các thiết kế DRBG.

9.2.2 Phân tích entropy của mầm

Nhà cung cấp sẽ cung cấp phân tích entropy của mầm. Các yêu cầu đối với phân tích này được xác định trong điều khoản 7.

Nhà cung cấp phải cung cấp mô hình ngẫu nhiên của nguồn entropy nếu sử dụng nguồn entropy vật lý chuyên dụng và chỉ định các thử nghiệm thống kê phù hợp để thu được giới hạn cận dưới đáng tin cậy về lượng entropy được thu thập. Nếu việc thay mầm mới được thực hiện từ một nguồn entropy phi vật lý, thì phải gửi lập luận phỏng đoán theo điều khoản 6.2.5 để hỗ trợ cho tuyên bố về entropy đối với quá trình tạo mầm. Hơn nữa, tuyên bố đối với entropy được cung cấp bởi quá trình khởi tạo mầm phải được chỉ rõ và phải được chứng minh bằng cách sử dụng mô hình ngẫu nhiên hoặc giới hạn cận dưới của phỏng đoán của entropy đã thu thập được thực hiện bởi nhà cung cấp. Yêu cầu về entropy cho các quá trình thay mầm mới được yêu cầu nếu chúng có liên quan đến các yêu cầu an toàn cho cấu trúc tổng thể. Ngoài ra, một cơ sở lập luận phải được cung cấp cho thấy rằng kết quả của lần khởi tạo không thể quan sát hoặc suy luận bằng cách khác với chi phí thực tế có thể xảy ra bởi kẻ tấn công và bất kỳ lần thay mầm mới nào sau đó đều đáp ứng các yêu cầu tương tự, ít nhất là chúng quan trọng đối với các yêu cầu an toàn được đưa ra bởi nhà cung cấp.

Ngoài bất kỳ yêu cầu an toàn nào được đưa ra cho quá trình tạo mầm, nhà cung cấp cũng sẽ đưa ra yêu cầu an toàn cho đầu ra DRBG. Cơ sở lý luận sẽ được cung cấp cho thấy rằng theo các giả định mật mã tiêu chuẩn, các yêu cầu an toàn cho đầu ra DRBG sẽ được đáp ứng nếu điều kiện tương tự được đáp ứng trong quá trình tạo mầm. Về nguyên tắc, quá trình tạo mầm được phép sai lệch đáng kể so với nguồn ngẫu nhiên lý tưởng miễn là đáp ứng các điều kiện nói trên.

10 Phương pháp kiểm thử

10.1 Yêu cầu chung

Để thực hiện đánh giá nhất quán cho cả NRBG và DRBG, khuyến nghị nên sử dụng sơ đồ đánh số sau. Điều này cũng sẽ đảm bảo khả năng yêu cầu truy xuất nguồn gốc đầy đủ và yêu cầu kiểm thử.

10.2 Yêu cầu của nhà cung cấp

Các yêu cầu của nhà cung cấp được đánh số trong khung sau:

VE<requirement_number>. <assertion_sequence_number>.<sequence_number>

- requirement number: đề cập đến điều mục kiểm thử sự phù hợp và chỉ điều khoản phụ cho NRBG và DRBG;

- assertion sequence: có nghĩa là thứ tự trong chỉ điều khoản phụ;

- sequence number: có nghĩa là thuyết minh chi tiết được cung cấp.

10.3 Yêu cầu kiểm thử

Các yêu cầu kiểm thử được đánh số và cung cấp các danh sách kiểm thử được thực hiện bởi đánh giá viên hoặc kiểm thử viên.

TE<requirement_number>.<assertion_sequence_number>.<sequence_number>

Trong đó: <requirement_number>, <assertion_sequence_number> và <sequence_number> được định nghĩa trong điều khoản 9.2.

Phụ lục A

(Tham khảo)

Phương pháp thông kê chung

A.1 Yêu cầu chung

Phụ lục này mô tả các ví dụ về các thủ tục và mô hình thống kê chung và các ví dụ về thiết kế RNG và mô hình ngẫu nhiên phổ biến cho các phần khác nhau của tiêu chuẩn này (ví dụ: Kiểm tra chi bình phương (chi-square), ...). [25] [26] [27] [28]

A.2 Thử nghiệm thống kê

A.2.1 Nhận xét chung

Các bài thử nghiệm thống kê được sử dụng để đánh giá RBG phải được điều chỉnh cho phù hợp với mô hình ngẫu nhiên của nguồn và được thực hiện bằng cách sử dụng giai đoạn tạo bit ngẫu nhiên mục tiêu thông qua mô hình ngẫu nhiên.

Nhà cung cấp phải xác định thêm các thử nghiệm thống kê sẽ phát hiện ra các lỗi hoặc điều kiện entropy không đủ. Đánh giá viên sẽ kiểm tra sự phù hợp do nhà cung cấp cung cấp về tính đúng đắn và đầy đủ, kiểm tra xem các thử nghiệm thống kê được đề xuất sẽ phát hiện một cách đáng tin cậy các điều kiện lỗi phù hợp được xác định hay không và thực hiện kiểm thử để xác định xem nguồn ngẫu nhiên có cung cấp lượng entropy cần thiết hay không. Trong trường hợp RBG bất định không có thành phần biến đổi an toàn bằng mật mã, ngoài ra, chúng sẽ được kiểm tra xem phân phối của các số ngẫu nhiên đầu ra có gần với mức lý tưởng hay không. Các yêu cầu để đạt được thuộc tính PTG.2 của Tài liệu tham khảo [7] có thể đóng vai trò là hướng dẫn cung cấp thông tin.

A.2.2 Kiểm thử cơ bản

Ngoài ra, thử nghiệm thống kê cơ sở phải được thực hiện trên cả các số ngẫu nhiên thô (hay nói chung là giai đoạn tạo số ngẫu nhiên mục tiêu thông qua mô hình ngẫu nhiên) cũng như các số ngẫu nhiên đầu ra. Bất kỳ phát hiện nào mâu thuẫn với các tuyên bố an toàn hoặc không tương thích với mô hình ngẫu nhiên sẽ dẫn đến việc các tuyên bố an toàn được đề cập sẽ bị từ chối.

Bộ thử nghiệm cơ bản được khuyến nghị là Quy trình kiểm thử A và Quy trình kiểm thử B của tài liệu tham khảo [7].

A.2.3 Kiểm tra chất lượng và kiểm tra tổng số lỗi

Các bài kiểm tra chất lượng phải được thực hiện trực tuyến và phải được thiết kế để phát hiện các lỗi về entropy đủ để đe dọa bất kỳ tuyên bố an toàn nào được đưa ra đối với RBG. Bản chất của các bài kiểm tra chất lượng phải được xác định bằng cách kiểm thử tất cả các chế độ lỗi phù hợp về mặt kỹ thuật của RBG.

Kiểm tra tổng số lỗi sẽ phải xác thực tổng số lỗi của nguồn nhiễu. Sau sự cố toàn bộ nguồn nhiễu bị lỗi, RBG sẽ không xuất ra các bit ngẫu nhiên nếu bất kỳ thuộc tính an toàn nào được yêu cầu cho các bit ngẫu nhiên này đã bị ảnh hưởng bởi sự cố của nguồn ngẫu nhiên. Trong trường hợp bị lỗi, việc phát hiện ra lỗi có thể xảy ra với khả năng cao ở bất kỳ lần gọi nào tiếp theo của RBG.

Một lần nữa, loại thử nghiệm thống kê được sử dụng ở đây phụ thuộc vào việc kiểm thử tất cả các trường hợp hợp lý về mặt kỹ thuật sẽ dẫn đến RBG dừng cấp entropy.

A.2.4 Các cân nhắc khác

Các thử nghiệm thống kê được thực hiện trong quá trình đánh giá RBG nên được thực hiện trong một số trường hợp độc lập của thiết bị và trong các điều kiện hoạt động khác nhau để kiểm tra các giả định tuyên bố về entropy do nhà cung cấp đưa ra là hợp lệ cho toàn bộ vùng hoạt động của thiết bị được kiểm thử.

A.3 Ví dụ về mô hình ngẫu nhiên

A.3.1 Tổng quan

Trong phần tiếp theo, một số ví dụ đơn giản về mô hình ngẫu nhiên được giới thiệu. Theo điều khoản 3.26, mô hình ngẫu nhiên của một nguồn ngẫu nhiên là một mô tả một phần toán học về các thuộc tính dự kiến thống kê của nguồn cho phép suy ra các tuyên bố entropy nếu mô hình ngẫu nhiên được kết hợp với dữ liệu kiểm thử thích hợp. Do đó, nhà cung cấp có các nhiệm vụ sau:

- Tìm một nhóm phân phối chứa phân phối thực của nguồn ngẫu nhiên.

- Biểu thị bằng cách sử dụng các đối số dựa trên các chi tiết kỹ thuật của nguồn entropy mà họ phân phối được đề xuất được mong đợi một cách hợp lý để chứa phân phối thực được tạo ra bởi nguồn ngẫu nhiên.

- Cho thấy họ phân bố bị hạn chế đủ để cho phép xác định entropy được tạo ra dựa trên các phương pháp thống kê, ví dụ: ước lượng tham số.

- Lựa chọn các thử nghiệm thống kê thích hợp cũng như nêu tuyên bố về entropy cho nguồn.

A.3.2 Chú thích

- Thông thường, họ phân bố có thể được đặc trưng bởi một hoặc một số tham số.

- Có vẻ hợp lý khi yêu cầu mô hình ngẫu nhiên giả định tính cố định, vì nếu không, đối với các RBG trong thế giới thực, việc xác minh mô hình ngẫu nhiên có thể trở nên quá khó khăn. Tuy nhiên, bất cứ khi nào tuyên bố về tính ổn định được đưa ra, tất nhiên nó sẽ được hỗ trợ bởi các lập luận kỹ thuật dựa trên thiết kế của RBG đang được nghiên cứu.

Đánh giá viên phải xác minh rằng mô hình ngẫu nhiên phù hợp với thiết kế của nguồn. Họ phải xác minh thêm rằng các phương pháp thống kê do nhà cung cấp đề xuất để đưa ra ước tính entropy phù hợp với mục đích đó và cho kết quả đáng tin cậy. Ngoài ra, phải kiểm tra xem tuyên bố về entropy do nhà cung cấp đưa ra có được thiết kế đáp ứng trong mọi điều kiện hoạt động hay không. Cuối cùng, đầu ra entropy dự kiến từ toàn bộ thiết bị, với bất kỳ quá trình hậu xử lý tiếp theo nào có thể được thực hiện trước khi xuất dữ liệu cho các ứng dụng tiêu thụ, sẽ được coi là phù hợp với cấu hình tấn công mà RBG sẽ được đánh giá.

Rõ ràng là một số bước của quá trình này có thể phụ thuộc vào chi tiết của việc thực hiện. Các ví dụ sau đây nhằm cho thấy một số bước trong số này có thể ảnh hưởng như thế nào đến quá trình đánh giá một nguồn ngẫu nhiên. Chúng không nhằm giải quyết tất cả các mối quan tâm có thể có hoặc đề xuất các thiết kế sẵn sàng để triển khai như trong các ứng dụng quan trọng về an toàn.

Trong Tài liệu tham khảo [14], một phương pháp ước lượng được đề xuất tích lũy giá trị trung gian của số tần số.

A.3.3 Ký hiệu và quy ước

Trong A.2.4. các biến ngẫu nhiên được biểu thị bằng chữ hoa và giá trị của một thực nghiệm tương ứng được biểu thị bằng chữ thường. Quy ước tương tự cũng áp dụng cho chuỗi các biến ngẫu nhiên biến thiên tương ứng: ở đây vị trí trong chuỗi sẽ được biểu thị bằng chỉ số, tức là A_i là phần tử thứ i trong chuỗi các biến ngẫu nhiên $A_1, A_2, \ldots, A_i, \ldots$, và A_i sẽ là nhận thức tương ứng. Các biến ngẫu nhiên trong phụ lục này có giá trị thực trừ khi có chỉ định khác. Các hàm của một biến thực duy nhất t được biểu thị bằng các chữ cái viết thường, ví dụ: $f(t)$. Ký hiệu tương tự cũng được sử dụng khi f là một hàm ngẫu nhiên của một biến thực (phụ thuộc vào kết quả của các sự kiện ngẫu nhiên).

Tất cả các biểu thức toán học được hiển thị ở dạng nghiêng.

Trong phần tiếp theo, chỉ các bộ tạo bit ngẫu nhiên hoàn toàn vật lý mới được xem xét, vì trọng tâm của điều này là đưa ra các ví dụ về việc sử dụng mô hình ngẫu nhiên trong việc đánh giá chất lượng của một nguồn entropy chứ không phải trong hậu xử lý.

A.3.4 Ví dụ

* Ví dụ 1: Tạo bit ngẫu nhiên dựa trên việc tung đồng xu.

Trong thiết lập tung đồng xu cổ điển, một đồng xu được kiểm thử viên tung lên không trung và sau đó bắt lấy đồng xu. Sau đó, kiểm thử viên sẽ đọc xem đồng xu rơi xuống mặt sấp hay mặt ngửa. Thử nghiệm này được giả định rằng đồng xu sẽ bắt đầu lại sau mỗi lần tung lên.

Mô hình ngẫu nhiên: Một mô hình ngẫu nhiên hợp lý của quá trình này là giả định rằng kết quả tung đồng xu sẽ độc lập và được phân phối giống hệt nhau *B (1, p)* như được mô tả trong Tài liệu tham khảo [7]. Entropy tối thiểu mà người ta có thể hy vọng thu thập được từ thử nghiệm sau mỗi lần tung đồng xu có thể được xác định bằng cách phân bổ lấy mẫu cho một lượng lớn các kiểm thử viên. Đối với mỗi kiểm thử viên, người ta có thể sử dụng một số tần suất đơn giản để suy ra giá trị có khả năng xảy ra nhất của p hoặc một đánh giá thận trọng của p. Do đó, mô hình ngẫu nhiên trong trường hợp này xác định phân phối một họ tham số.

Cơ sở lập luận của mô hình ngẫu nhiên như sau:

Phân tích vật lý của hệ thống đang được khảo sát như trong Tài liệu tham khảo [8] cho thấy rằng kết quả của việc tung đồng xu, về nguyên tắc là xác định, rất nhạy cảm với các điều kiện ban đầu. Vì những người thực hiện thử nghiệm trên người sẽ không dự tính thay đổi các điều kiện ban đầu làm thay đổi kết quả một cách có hệ thống, nên sẽ hợp lý khi cho rằng hệ thống không có bộ nhớ. Mặc dù khuynh hướng của việc tung đồng xu có thể khác nhau giữa kiểm thử viên này với kiểm thử viên khác, nhưng cũng hợp lý để kỳ vọng rằng ít nhất trong khoảng thời gian ngắn, sự phân bổ của thử nghiệm tung đồng xu với một đối tượng duy nhất sẽ không thay đổi. Do đó, giả định IID là hợp lý.

Các nhận xét sau đây là theo thứ tự nếu tình huống này được sử dụng như một phương pháp tương tự để đánh giá một RBG thực:

a) Trong một ví dụ trong thế giới thực, người làm thử nghiệm là con người sẽ được thay thế bằng một chiếc máy và chiếc máy đó sẽ tạo ra một dòng bit rất dài trong vòng đời của nó. Sau đó, nó sẽ không hợp lý khi kỳ vọng một số thuộc tính không cố định lâu dài do, ví dụ, lão hóa. Đây không phải là vấn đề nếu (các) tham số của phân phối thực vẫn nằm trong phạm vi phân phối thích hợp, tức là các phân phối hỗ trợ xác nhận entropy.

b) Ví dụ như đã cho hoàn toàn bỏ qua vấn đề chuyển đổi tín hiệu tương tự sang tín hiệu số của các sự kiện ngẫu nhiên được đề cập. Quá trình này cũng có thể không hoàn toàn đáng tin cậy trong một ví dụ trong thế giới thực và cũng có thể dễ bị ảnh hưởng bởi thiết bị lão hóa nhưng trong ví dụ này sẽ không thay đổi đáng kể kết luận.

c) Trong ví dụ tung đồng xu, những người thực hiện thử nghiệm đã qua đào tạo, tất nhiên có thể kiểm soát kết quả (ví dụ: nhà ảo thuật, xem Tài liệu tham khảo [8]). Ví dụ trong thế giới thực, khả năng kẻ tấn công có thể làm xuất hiện các trạng thái của hệ thống mà trong thực tế sẽ không bao giờ xảy ra một cách tình cờ và có thể liên quan đến hành vi giả ngẫu nhiên mạnh trên một phần của nguồn entropy (tức là các cuộc tấn công gây lỗi) sẽ luôn là đã cân nhắc và nghiên cứu nghiêm túc. Phân phối quy nạp có thể vẫn nằm trong họ phân phối, được chỉ định bởi mô hình ngẫu nhiên hoặc có thể nằm bên ngoài (ví dụ: một số giá trị xác định trong mô hình IID). Nếu các cuộc tấn công lỗi có liên quan đến mục tiêu đánh giá thì các hiện tượng đó sẽ được phát hiện. Nếu cần thiết, ngoài các thử nghiệm nhằm phát hiện các vấn đề thống kê trong các số ngẫu nhiên thô, việc giám sát vật lý thông qua các cảm biến thích hợp có thể là một lựa chọn để ngăn ngừa sự thiếu sót trong tính ngẫu nhiên được tạo ra do các cuộc tấn công lỗi hoặc sự cố vật lý tự nhiên của nguồn entropy. Hiện tượng thứ hai nên được phát hiện bằng kiểm tra tổng số lỗi, có thể được nhận biết bằng các cảm biến vật lý.

* Ví dụ 2: Tạo bit ngẫu nhiên bằng cách sử dụng diode nhiễu.

Trong ví dụ này (được lấy từ Tài liệu tham khảo [15]) đầu ra của hai diode nhiễu được so sánh và khuếch đại sự khác nhau. Đầu ra của bộ khuếch đại sau đó được gửi đến một mạch so sánh (Schmitt Trigger), tức là một thành phần tạo ra tín hiệu nhị phân về cơ bản, chuyển từ trạng thái "0" sang trạng thái "1" nếu điện áp đầu vào vượt quá "ngưỡng cao" U_h và chuyển đổi từ trạng thái "1" sang trạng thái "0" nếu điện áp đầu vào giảm thấp hơn "ngưỡng thấp" U_l. Một dãy hai mạch đa hài ổn định kép (flip-flops) đếm modulo số lần chuyển đổi giữa "0 - 1" của Schmitt Trigger. Số lần chuyển đổi giữa "0 - 1" của Schmitt Trigger tại thời điểm t sau khi bắt đầu thử nghiệm sẽ được ký hiệu là $c(t)$; trạng thái của flip-flop lưu trữ tại thời điểm t do đó được cho bởi $c(t)\ mod\ 2$. Bit kết quả
$b_i := c(t_i)\ mod\ 2$ được đọc ra tại các điểm trong thời gian $t_i := i/f$ được xác định bởi đồng hồ bên ngoài, trong đó f là tần số của đồng hồ và $s := 1/f$ là thời gian trôi qua trong một chu kỳ đồng hồ. Bit b_i là chuỗi đầu ra liên tục của số ngẫu nhiên RBG vật lý thuần túy.

Mô hình ngẫu nhiên: Mô hình ngẫu nhiên của RBG này được phân tích trong Tài liệu tham khảo [15] coi như nguồn entropy cơ bản, thời gian chờ giữa các lần chuyển đổi tiếp theo của flipflop lưu trữ, tức là giữa các lần chuyển đổi giữa "0 - 1" tiếp theo của Schmitt Trigger. Biểu thị bằng $t'_1, t'_2, t'_3, ...$ các thời điểm mà chuyển đổi "0 - 1" của Schmitt Trigger xảy ra và đặt $d_i := t'_i - t'_{i-1}$, trong đó theo quy ước $t'_0 = 0$. Sau đó d_i được xác định bởi hoạt động của các diode nhiễu: sau khi Schmitt Trigger đã hoàn thành quá trình chuyển đổi giữa "0 - 1", đầu ra từ bộ khuếch đại trước tiên cần đẩy Schmitt Trigger từ trạng thái bật sang trạng thái tắt và sau đó trở lại trạng thái bật một lần nữa.

Trong tài liệu tham khảo [15], các D_i được coi là các biến ngẫu nhiên có giá trị thực. Các biến ngẫu nhiên tương ứng D_i được giả định là cố định và tuân theo sự tổng quát hóa phù hợp của định lý giới hạn trung tâm cho các biến phụ thuộc, ví dụ như hệ quả của việc thỏa mãn điều kiện pha trộn mạnh được xác định trong Tài liệu tham khảo [15]. Có thể giả định thêm rằng Di không xác định. Cuối cùng, cần có một giả định kỹ thuật về sự tồn tại của mô men tuyệt đối thứ ba.

Đặt $\mu := E(D_1)$ và σ là phương sai tổng quát của vectơ vô hạn $(D_1, D_2, ...)$, người ta nhận được rằng nếu s lớn so với μ và nếu σ không quá thấp so với μ thì số $C := C((k+1)s) - C(ks)$ của việc chuyển đổi Schmitt Trigger giữa hai bản cập nhật của mạch flip-flop lưu trữ sau khi chuẩn hóa có thể được phân phối chuẩn gần đúng. Điều này ngụ ý rằng $C \bmod 2$ sẽ có xu hướng phân phối đồng đều. Sự pha trộn mạnh mẽ của D_i ngụ ý rằng trong trường hợp này, các bản cập nhật tiếp theo của flip-flop lưu trữ sẽ độc lập.

Mục tiêu của mô hình ngẫu nhiên là thu được ước lượng về entropy của các số ngẫu nhiên đầu ra. Trong trường hợp hiện tại, đối số nêu trên đã gợi ý rằng khi s đi đến vô cùng ít nhất là trong giới hạn mong đợi một phân phối lý tưởng của các bit đầu ra. Hơn nữa, tốc độ hội tụ đến phân bố lý tưởng sẽ chủ yếu phụ thuộc vào tỷ lệ s/μ và μ/σ. Thật vậy, theo giả thiết hội tụ đến chuẩn tắc, bản thân sự phân bố của các bit đầu ra sẽ phụ thuộc vào hai đại lượng này; do đó, mô hình ngẫu nhiên cho phép lấy ra một họ hai tham số của các phân phối được mong đợi là gần đúng với phân phối thực của các bit ngẫu nhiên được tạo ra tốt. Lấy mẫu phân bố D_i cho phép tính được hai tham số với độ chính xác cao nếu biết s. Tham khảo tài liệu tham khảo [15] để biết thêm chi tiết.

Cơ sở lập luận: D_i có thể được giả định ít nhất là một phần ngẫu nhiên vì sự dao động trong đầu ra của các diode nhiễu bị chi phối bởi xung nhiễu. Việc sử dụng hai diode nhiễu như nhau kết hợp với một bộ so sánh chênh lệch loại bỏ phần lớn bất kỳ sự thay đổi đầu ra nào do các lý do xác định; ví dụ, nhiễu vật lý bởi các trường điện từ bên ngoài sẽ có xu hướng ảnh hưởng đến cả hai diode như nhau.

Xung nhiễu trong diode nhiễu sẽ không biểu hiện bất kỳ tác động nào đến bộ nhớ dài hạn. Sử dụng sự khác biệt về mức đầu ra của hai diode nhiễu độc lập về nguyên tắc sẽ giảm hơn nữa bất kỳ sự phụ thuộc nào ở mức diode; ngoài ra, điện áp đầu vào của bộ khuếch đại phải để hoàn thành chu kỳ khởi động bản cập nhật của flip-flop lưu trữ đầu tiên chéo U_l từ phía trên, sau đó chéo U_h từ bên dưới. Chuỗi sự kiện này, nếu được khởi động chủ yếu bởi đầu ra của các diode nhiễu, sẽ đủ xóa các hiệu ứng trễ - trong các diode cũng như Schmitt Trigger - để không tồn tại các mối tương quan chặt chẽ giữa D_i và D_{i+r} đối với bất kỳ $r > 1$. Giả định rằng D_i ở mức tách biệt vừa đủ có thể được coi là độc lập theo quan điểm thực tế là chính đáng.

Tính ổn định là hợp lý vì hành động ngẫu nhiên của hệ thống đang nghiên cứu được xác định bởi các hằng số hoạt động như điện áp đánh thủng của diode nhiễu, đặc tính điện tử của bộ so sánh và bộ khuếch đại và các thông số kỹ thuật của Schmitt Trigger. Vì chúng là bất biến ít nhất trong khoảng thời gian ngắn, nên phân phối chung của $(D_i, D_{i+1}, ..., D_{i+n})$ không nên phụ thuộc đáng kể vào i. Độ nhạy của đầu ra đối với các vi phạm về tính ổn định có thể xảy ra trong thời gian dài, chẳng hạn như do thiết bị cũ nên ở mức thấp sự phân bố D_i không thay đổi hoàn toàn do hệ quả (ví dụ như trong sự cố hoàn toàn của nguồn nhiễu).

Hơn nữa, với xấp xỉ gần đúng thì D_i phải được phân phối Poisson, bởi vì chúng là số lượng các sự kiện xảy ra ngẫu nhiên và ít nhất là gần đúng độc lập (nếu khoảng thời gian s giữa các lần lấy mẫu tiếp theo của thanh ghi lưu trữ đủ dài, sao cho trong phạm vi một thời gian cập nhật của bộ đếm cuối cùng, người ta kỳ vọng sẽ thấy nhiều lần giao nhau "0 - 1" của Schmitt Trigger). Do đó, sự tồn tại của phương tiện, phương sai và mô men cao hơn là không có vấn đề.

Nhận xét 1: Để mô hình này hợp lệ, nó phải được xác minh theo kinh nghiệm rằng xung nhiễu từ các diode nhiễu không bị chi phối bởi các nguồn xung nhiễu khác trong hệ thống, ví dụ: nhiễu bởi nhiệt độ từ bộ khuếch đại. Trong khi về nguyên tắc, cấu trúc được đưa ra có thể thành công trong việc thu thập đủ entropy nếu một nguồn nhiễu khác chiếm ưu thế đầu vào của Schmitt Trigger, câu hỏi nguồn nhiễu nào chi phối các đóng góp cho bộ đếm là rất quan trọng, chẳng hạn như để hiểu các cuộc tấn công vật lý, để kết hợp kiểm tra chất lượng và kiểm tra tổng số lỗi trong thiết kế cuối cùng và để đánh giá mô hình ngẫu nhiên. Ví dụ, nhiễu nhiệt từ bộ khuếch đại sẽ tuân theo một cấu hình nhiệt độ khác với nhiễu từ diode Zener.

Nhận xét 2: Một thiết kế chỉ có một diode nhiễu về nguyên tắc có thể được mô hình hóa theo cách tương tự. Tuy nhiên, khả năng chống lại các cuộc tấn công vật lý sẽ thấp hơn [15].

Nhận xét 3: Trong Tài liệu tham khảo [14], Phần 5, sự phân bố của D_i đã được nghiên cứu để triển khai bộ tạo bit thực tế được mô tả. Việc áp dụng công cụ ước lượng entropy có trong Tài liệu tham khảo [14], Phần 5, cho kết quả phân phối sẽ mang lại ước lượng entropy cho RBG là 0,9999-bit trên mỗi bit đầu ra. Điều quan trọng cần lưu ý là ước lượng entropy này chỉ áp dụng cho việc triển khai cụ thể được mô tả trong Tài liệu tham khảo [15]. Tuy nhiên, cùng một loại phân tích có thể được áp dụng cho một loạt các triển khai của cùng một thiết kế và thậm chí cho một loạt các thiết kế RBG phù hợp với mô hình ngẫu nhiên chung ở đây đang được thảo luận.

Nhận xét 4: Cần thận trọng hơn trong các tình huống khi không thể tin cậy được xấp xỉ D_i theo phân phối chuẩn, ví dụ như: trường hợp σ nhỏ so với μ hoặc μ không nhỏ hơn s nhiều. Có thể RBG mà mô hình ngẫu nhiên tổng quát được mô tả trong Tài liệu tham khảo [15] phù hợp sẽ trong tình huống như vậy vẫn tạo ra đầu ra entropy cao nhưng việc hiển thị điều này sẽ đòi hỏi phân tích toán học sâu hơn.

Nhận xét 5: Về mặt kiểm tra chất lượng và kiểm tra tổng số lỗi là một tùy chọn đáng đề cập cho một thiết kế như thế này ngoài các thử nghiệm thống kê trên các số ngẫu nhiên thô còn có các cảm biến vật lý giám sát các diode nhiễu, so sánh và khuếch đại để bảo vệ khỏi chống lại giả mạo hoặc hư hỏng thiết bị. Ngoài ra, số lần giao nhau "0 - 1" của Schmitt Trigger giữa các chu kỳ đồng hồ có thể được sử dụng để kiểm tra chất lượng, nếu nó có sẵn trực tuyến. Nhìn chung, các kiểm tra chất lượng và kiểm tra tổng số lỗi phải được điều chỉnh cho phù hợp với các đặc tính của mô hình ngẫu nhiên và các chế độ lỗi vật lý hợp lý của thiết bị. Việc điều chỉnh các kiểm tra chất lượng và lỗi chấp nhận được trong mô hình ngẫu nhiên bảo vệ khỏi việc sử dụng một mắt xích yếu trong họ các phân phối được sử dụng trong mô hình ngẫu nhiên; Hơn nữa, việc thích ứng với các chế độ lỗi chấp nhận được của thiết bị còn bổ sung thêm một số biện pháp bảo vệ chống lại các tình huống trong đó phân phối các số ngẫu nhiên thô không còn là một mắt xích trong các họ phân phối được chỉ định bởi mô hình ngẫu nhiên.

Ví dụ 3: Tạo số ngẫu nhiên dựa trên nguồn phóng xạ

Trong ví dụ này, bức xạ năng lượng cao phát ra tự phát từ một mẫu phóng xạ được sử dụng làm nguồn nhiễu vật lý. Trong phần tiếp theo, một phiên bản đơn giản hơn một chút được đưa ra trong Tài liệu tham khảo [7], điều khoản 2.4.1, ví dụ 4.

Lưu ý rằng ý tưởng sử dụng thời gian của các sự kiện phân rã trong nguồn phóng xạ để tạo bit ngẫu nhiên là khá cũ, xem ví dụ Tài liệu tham khảo [16]. Tuy nhiên, các phương pháp được sử dụng để suy ra từ thời gian thu được một chuỗi ký hiệu kỹ thuật số được phân bố gần như đồng đều giữa các phương pháp tiếp cận khác nhau. Cần nhấn mạnh rằng việc lựa chọn và phân tích một cơ chế số hóa thích hợp cũng quan trọng trong việc tạo ra mô hình ngẫu nhiên của RBG vật lý như việc lựa chọn nguồn entropy vật lý cuối cùng. Giải thích trong Tài liệu tham khảo [7] sử dụng các phương pháp và phân tích của Tài liệu tham khảo [17], Chương 4.2. Một nguồn phóng xạ được đặt gần bộ đếm Geiger gắn với máy tính. Bộ đếm Geiger gửi một tín hiệu đến máy tính bất cứ khi nào một sự kiện phân rã được phát hiện. Máy tính sử dụng đồng hồ bên trong để lấy thời gian của các sự kiện. Thời gian T_i giữa lần phát hiện thứ i và thứ $(i-1)$ được sử dụng làm điểm bắt đầu tạo bit ngẫu nhiên.

Nguồn phóng xạ được giả định là phân rã tự phát (tức là không có sự đóng góp nhiều của phản ứng dây chuyền hạt nhân hoặc phân rã do kích thích bên ngoài) với chu kỳ bán rã L vượt quá đáng kể thời gian tồn tại của RBG. Người ta cũng giả định rằng không có nguồn bức xạ bên ngoài thay đổi nào góp phần vào việc phát hiện các sự kiện phân rã ở một mức độ đáng kể. Trong một

mẫu phóng xạ đang bị phân rã tự phát, các sự kiện phân rã xảy ra trong mẫu một cách ngẫu nhiên với xác suất không đổi trên một đơn vị thời gian, vì vậy tất cả T_i sẽ độc lập và phân phối theo hàm mũ với tham số tốc độ: $\theta = ln(2)/L$.

Thật đơn giản để xác minh rằng đối với hai biến ngẫu nhiên độc lập và phân phối theo cấp số nhân X và Y với tham số tỷ lệ giống hệt nhau, biến ngẫu nhiên trong công thức (A.1):

$$Z := \frac{X}{X+Y} \qquad \text{(A.1)}$$

được phân bố đồng đều trong đoạn [0,1]. Do đó, với dãy T_i, nó được đặt như trong công thức (A.2):

$$Z_i := \frac{T_i}{T_i + T_{i+1}} \qquad \text{(A.2)}$$

để có được một chuỗi các biến ngẫu nhiên có giá trị dấu phẩy động độc lập lẫn nhau và phân bố đồng nhất, tất cả chúng đều được rút ra gần như đồng nhất từ [0,1].

Một số sai lệch sẽ xuất phát từ thực tế là T_i không phải là các biến liên tục mà là bộ đếm đồng hồ có hiệu lực và một vài lỗi đo lường như do thời gian chết của bộ đếm Geiger gây ra sau khi ghi lại một sự kiện. Tuy nhiên, nếu số lượng sự kiện phát hiện thấp so với chu kỳ đồng hồ và thời gian chết, thì chấp nhận giá trị gần đúng và Z_i ít nhất phải được phân bố độc lập và giống hệt nhau. Các sai lệch trong việc phân phối các số dấu phẩy động thu được, đưa ra các ước lượng chắc chắn về entropy, có thể được loại bỏ bằng cách hậu xử lý mật mã. Độ chệch dự kiến có thể được định lượng tốt dựa trên sự phân bố lý thuyết của T_i. Luôn luôn phải thực hiện so sánh giữa phân phối dự kiến và thực nghiệm của T_i.

Có thể giảm nhẹ độ chệch của phân phối dẫn xuất do các lý do sáng suốt bằng cách sử dụng công thức (A.3) thay vì công thức (A.2):

$$Z_i := \frac{T_i - \frac{1}{2}}{T_i + T_{i+1} - 1} \qquad \text{(A.3)}$$

cung cấp phân phối đều hơn cho đầu vào được phân phối theo hình học so với Công thức (A.2). Các giới hạn về độ lệch so với phân bố đều mà trong trường hợp này có thể được mong đợi do sử dụng T_i phân bố hình học có thể tìm thấy trong Tài liệu tham khảo [17], Chương 4.2, định lý 4.1.

Nhận xét 1: Về nguyên tắc, lượng ngẫu nhiên được tạo ra bởi một RBG thuộc loại này có thể được suy ra khá chính xác từ các định luật vật lý đã hiểu rõ, đưa ra ước tính về số lượng các sự kiện phân rã thực tế xảy ra trong mẫu phóng xạ trên một đơn vị thời gian và một số thuộc tính cơ bản của thiết bị được sử dụng như: thời gian chết của bộ đếm Geiger, độ nhạy của thiết bị về tỷ lệ phần trăm tổng số sự kiện phân rã sẽ được phát hiện hoặc độ chính xác của đồng hồ được sử dụng cho các sự kiện thời gian. Tuy nhiên, toàn bộ chuỗi lập luận kết nối các sự kiện ngẫu nhiên với entropy của các số ngẫu nhiên thô vẫn còn dài và chứa các giả định mô hình hóa và đơn giản hóa cần được kiểm tra. Do đó, cần phải thử nghiệm thống kê RBG ngay cả khi có cơ sở lập luận thuyết phục hợp lý để kỳ vọng một phân phối số lượng cụ thể.

Nhận xét 2: Về nguyên tắc, một RBG loại này có thể hoạt động ngay cả khi không có nguồn phóng xạ, bằng cách sử dụng nền bức xạ thông thường. Tuy nhiên, trong trường hợp này, tốc độ bit thu được sẽ thay đổi theo thời gian và phân bố dự kiến của T_i không thể được mô tả trước.

Phụ lục B

(Tham khảo)

Kiểm tra tài liệu

Xem tài liệu tham khảo mục [25], [26] và [27] để biết các liên kết đến các tài liệu thử nghiệm được sử dụng cho các bài kiểm thử và đánh giá. Đây là một tập hợp các giá trị mà khi một thử nghiệm thống kê được áp dụng, sẽ thành công.

Tài liệu tham khảo

[1] National Institute of Standards and Technology. NIST Special Publication 800-22, Rev. 1a, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010. http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf

[2] National Institute of Standards and Technology. NIST Draft Special Publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, August 2012. http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf

[3] CISCO Entropy Sources – Practical Designs and Validation Challenges, Sonu Shankar and David McGrew, 2012. http://csrc.nist.gov/groups/ST/rbg_workshop_2012/shankar.pdf

[4] Analysis of the Linux Random Number Generator, Zvi Gutterman, Benny Pinkas, Tzachy Reinman, March 06, 2006. http://www.pinkas.net/PAPERS/gpr06.pdf.

[5] Network event detection with entropy measures, Eimann, Raimund E. A., 2008. https:/ researchspace.auckland.ac.nz/handle/2292/3427.

[6] ANSI X9.82-4-2011, Random Number Generation - Part 4: Random Bit Generator Constructions.

[7] BSI A proposal for: Functionality classes of random number generators, version 2.0, September 2011, Wolfgang Killmann, Werner Schindler https://www.bsi.bund.de/SharedDocs/Downloads/DEBSI/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_numbergenerators_e.pdf

[8] Dynamical Biases in the Coin Toss, Persi Diaconis, Susan Holmes, Richard Montgomery, Stanford University Department of Statistics Technical Report No. 2004-32, https:/ statistics.stanford.edu/sites/default/files/2004-32.pdf.

[9] Dokumentation und Analyse des Linux-Pseudozufallsgenerators, Stephan Müller, Gerald Krummeck, Mario Romsy, Version 3.8,2013 https://www.bsi.bund.de/DEBSI/Publikationen/Studien/LinuxRNG/index_htm.html

[10] Guessing and Entropy. James L. Massey, 1994 IEEE International Symposium on Information Theory, p. 204.

[11] A Hardware Random Number Generator, Thomas E. Tkacik, Proceedings Cryptographic Hardware and Embedded Systems 2002, LNCS 2523, p. 450-453.

[12] How to Predict the Output of a Hardware Random Number Generator, Markus Dichtl, Proceedings Cryptographic Hardware and Embedded Systems 2003, LNCS 2779, p. 181-188.

[13] Lubicz D. On classification of finite statistical tests Adv. In Math. of Comm. 1(4) : 509-524 (2007)

[14] Kim Y.-S., Yeom Y., Choi H.B., Online test based on mutual information for true random number generators. Journal of the Korean Mathematical Society. 2013, 50 (4)

[15] Killmann W., Schindler W. A Design for a Physical RNG with Robust Entropy Estimators, CHES 2008, LNCS 5154, pp. 146-163

[16] Rosenblatt M., A central limit theorem and a strong mixing condition. Proc. Natl. Acad. Sci.USA. 1956, 42 (1) pp. 43-47.

[17] Schmidt H., Quantum-Mechanical Random-Number Generator. J. Appl. Phys. 1970, 41 (2) pp. 462-468.

[18] Neuenschwander D., Probabilistic and statistical methods in cryptology: an introduction by selected topics. Springer Science & Business Media, Vol. 3028, 2004.

[19] Christian Cachin, Entropy Measures and Unconditional Security in Cryptography, Dissertation at ETH Zurich, 1997.

[20] Brown D., Formally Assessing Cryptographic Entropy: http://eprint.iacr.org/2011/

[21] Nguyen P.Q., Shparlinski I.E., The insecurity of the elliptic curve digital signature algorithm with partially known nonces. Des. Codes Cryptogr. 2003, 30 (2) pp. 201-217.

[22] Analysis of Random Number Generation in Virtual Environments https://www.bsi.bund.de/DE/Publikationen/Studien/ZufallinVMS/zufall-in-vms.html

[23] ISO/IEC 18367:2016, Information technology — Security techniques — Cryptographic algorithms and security mechanisms conformance testing.

[24] ISO/IEC 24759:2017, Information technology — Security techniques — Test requirements for cryptographic modules Statistical Test Suite (STS) 2.1.2 from 2014.
[25] A Statistical Test Suite for Random and Pseudorandom Number Generators for cryptographic Applications. SP 800-22 Rev1a. 2010. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a
[26] NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation. http://csrc.nist.gov/publications/drafts/800-90/ sp800-90b.pdf
[27] Killmann W., Schindler W. A proposal for: Functionality Classes and Evaluation Methodology for True (Physical) Random Number Generators, Version 3.1, English translation, 25.09.2001. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.html