TCVN

TIÊU CHUẨN QUỐC GIA

DỰ THẢO

TCVN 12212:2026

ISO/IEC 17825:2024

Xuất bản lần 2

CÔNG NGHỆ THÔNG TIN - KỸ THUẬT AN TOÀN - CÁC PHƯƠNG PHÁP KIỂM ĐỊNH ĐỂ GIẢM THIỂU CÁC LỚP TẤN CÔNG KHÔNG XÂM LẤN CHO CÁC MÔ-ĐUN MẬT MÃ

Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu

TCVN 12212:2026 hoàn toàn tương đương với ISO/IEC 17825:2024.

TCVN 12212:2026 do Ban Cơ yếu Chính phủ biên soạn, Bộ trưởng Bộ Quốc phòng đề nghị, Ủy ban tiêu chuẩn đo lường chất lượng quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Việc kiểm định yêu cầu các hằng số được xác định, vốn được dẫn xuất từ một phân tích dựa trên các tiên đề của vấn đề an toàn. Các mức đảm bảo an toàn bị ràng buộc với việc kiểm định và các rủi ro còn lại. Cách tiếp cận kiểm định có thể được đặc tả như sau:

a) Tính vững chắc của kiểm định

1) Một mô tả hình thức của kiểm định hộp kín thực nghiệm cung cấp tính vững chắc, trong bối cảnh của cuộc tấn công, vì việc kiểm định tuân theo một phương pháp luận đã được chấp nhận.

2) Việc áp dụng phương pháp luận không đảm bảo rằng tất cả các tấn công khả thi được đề cập. Kiểm định cho phép phát hiện điểm yếu trong một hệ thống; do đó, kiểm định làm tăng độ tin cậy vào khả năng của hệ thống để chống lại một loạt các tấn công mô phỏng. Hình thức luận được triển khai cho phép phát hiện các điểm yếu và kết quả là một mức hợp lý được chứng thực bởi các kiểm thử.

3) Mức đảm bảo có thể đạt được với phương pháp luận trong tiêu chuẩn này là mức "được kiểm soát" thuộc mức tin cậy "hợp lý", là mức thấp đến trung bình. Mức cao là không thể đạt được do cách tiếp cận hộp kín. Ý nghĩa của "hợp lý" được xác định bởi ngưỡng rủi ro của khách hàng. Người kiểm định xác định mức độ hợp lý, phù hợp với một mục tiêu mức an toàn.

4) Kiểm định được dẫn dắt bởi một chiến lược, vốn cho phép sự minh bạch trong phương pháp luận và các kết quả.

5) Phương pháp luận có tính đặc thù cho từng lớp thiết bị. Tiêu chí đạt/không đạt cần phải xem xét đến lớp thiết bị đang được kiểm định. Ví dụ, tiêu chí dành cho các thiết bị có hành vi tất định (tức là thuần phần cứng) và các thiết bị có ngăn xếp phần mềm phức tạp nên khác nhau.

6) Kiểm định an toàn là một "sự đánh giá" khi dựa trên các phép đo có nhiễu hoặc khi người kiểm thử không có toàn quyền kiểm soát mô-đun đang được kiểm thử (IUT).

b) Tính lặp lại (theo TCVN ISO/IEC 17025:2017, 7.2.2.4)

Tính lặp lại (Repeatability) nghĩa là thu được kết quả tương tự từ cùng một phương pháp luận (tức là được lặp lại), trong khi tính tái tạo được (Reproducibility) nghĩa là thu được kết quả tương tự từ phương pháp luận tương tự. Đánh giá an toàn là một đánh giá dựa trên các phép đo có nhiễu, trên IUT mà hành vi của nó có thể không hoàn toàn nằm trong tầm kiểm soát của người kiểm định. Trong tiêu chuẩn này, có một điều kiện tiên quyết là IUT phải là một hộp kín (closed-box), có thể hoạt động theo cách bất định (ít nhất là các thành phần bên trong của nó – do việc ngẫu nhiên hóa có chủ đích nào đó được sử dụng như một biện pháp bảo vệ). Hơn nữa, phép kiểm thử chỉ có thể được thực hiện dựa trên các quan sát và phát hiện bên ngoài. Do đó, mục tiêu là ghi lại một quy trình kiểm định chính thức và minh bạch, trong đó các kiểm thử độc lập có thể được tái tạo với các kết quả dự kiến tương tự (càng nhiều càng tốt, trong các giới hạn hợp lý). Các phương pháp luận là tương tự nhau (ví dụ: được thực hiện bởi hai người kiểm định) ở chỗ chúng cho ra kết quả tương tự.

c) Chi phí kiểm định

1) Mục tiêu là dành nỗ lực đúng mức cho kiểm định ở một mức độ đảm bảo nhất định. Hiệu quả chi phí của việc kiểm định có dính líu trực tiếp đến việc đảm bảo một mức độ an toàn nhất định. Chi phí kiểm định bao gồm, nhưng không giới hạn ở:

i. Mức độ chuyên môn và kinh nghiệm: Hệ quả/sự dính líu của việc sử dụng một quy trình đã được chính thức hóa (không phụ thuộc vào IUT). Người kiểm định cần có kỹ năng và năng lực.

ii. Thời gian: Thời gian trôi qua để thu thập dữ liệu, mặc dù quy trình được tự động hóa.

iii. Thiết bị: Tác động chi phí của thiết bị được đề cập trong TCVN 14192-1:2024 ISO/IEC 20085-1:2019 (các yêu cầu) và TCVN 14192-2:2024 ISO/IEC 20085-2:2020 (hiệu chuẩn).

2) Tiêu chuẩn này nhằm giữ chi phí vừa phải. Mức độ đảm bảo sẽ đạt đến một ngưỡng nhất định khi số lượng dấu vết được ghi nhận vượt qua một con số nhất định. Mức đảm bảo không tăng đáng kể thêm khi vượt quá ngưỡng đó. Phương pháp luận được quy định không thể vượt quá một mức đảm bảo nhất định do thiết kế của nó.

Các tuyên bố sau đây áp dụng như một hệ quả của phương pháp được sử dụng:

d) Kiểm định hộp kín giới hạn phương pháp luận này chỉ kiểm thử rò rỉ mà không tính đến các đặc điểm cụ thể của việc triển khai thuật toán (ví dụ: các đặc thù triển khai, chẳng hạn như thực thi song song các phép toán mật mã không liên quan, hoặc các biện pháp đối phó, chẳng hạn như che giấu ngẫu nhiên, triển khai số học trường trong mật mã đường cong elliptic).

e) Kiểm định chỉ xem xét rò rỉ trong quá trình kiểm thử các phép toán mật mã sử dụng khóa. Theo thiết kế, quá trình này không tìm kiếm các nguồn rò rỉ tiềm ẩn khác (ví dụ: Phát xạ trong quá trình truyền khóa qua bus nội bộ).

f) Các kết quả phụ thuộc vào tập dữ liệu và chất lượng thiết bị sử dụng trong quá trình thu thập. Những kẻ tấn công có tài nguyên lớn hơn vẫn có thể khai thác các đường tấn công được kiểm thử bởi phương pháp luận này, ngay cả khi chúng đã vượt qua bài kiểm tra, nhờ vào việc tăng cường tài nguyên và nỗ lực.

g) Các tấn công tinh vi hơn có thể được áp dụng và thành công. Các tấn công tinh vi hơn đề cập đến các tấn công khác với các tấn công thông thường, ví dụ như các tấn công dành riêng cho các mật mã phi đối xứng (xem 9.2).

h) Mỗi ứng dụng cụ thể hoặc phiên bản API của mô-đun mật mã cũng yêu cầu một đánh giá bổ sung ngoài các bài kiểm tra chung trong tiêu chuẩn này. Các lĩnh vực đánh giá như vậy cần bao gồm các mối đe dọa sử dụng mô-đun phi tham số đặc thù cho ứng dụng, chẳng hạn như phân tích lưu lượng, thao túng thứ tự logic hoặc phạm vi của các hoạt động bên ngoài.

Trong tiêu chuẩn này, các yêu cầu được đánh số. Theo quy ước, các yêu cầu được dán nhãn [CC.NN], trong đó CC đại diện cho số điều (ví dụ: 06 có nghĩa là Điều 6) và NN đại diện cho vị trí yêu cầu trong Điều (ví dụ: yêu cầu đầu tiên của Điều 6 được gọi là [06.01]). Mục đích của các yêu cầu được dán nhãn là để dễ dàng tạo ra các tài liệu thể hiện sự tuân thủ tiêu chuẩn này và khả năng truy xuất nguồn gốc của chúng đối với người kiểm thử.

Công nghệ thông tin - Kỹ thuật an toàn – Các phương pháp kiểm định giảm thiểu các lớp tấn công không xâm lấn cho các mô-đun mật mã

Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các chỉ số kiểm thử để giảm thiểu tấn công không xâm lấn nhằm xác định sự phù hợp các yêu cầu được quy định trong TCVN 11295:2016 (ISO/IEC 19790:2012) cho các mức an toàn 3 và 4. Các chỉ số kiểm thử này được liên kết với các chức năng an toàn được đề cập trong TCVN 11295:2016 (ISO/IEC 19790:2012). Kiểm định được tiến hành tại ranh giới đã xác định của mô-đun mật mã và tại các đầu vào/đầu ra có sẵn ở ranh giới đó.

Tiêu chuẩn này nhằm được sử dụng kết hợp với TCVN 12211:2018 (ISO/IEC 24759:2017) để chứng minh sự phù hợp với TCVN 11295:2016 (ISO/IEC 19790:2012).

CHÚ THÍCH: TCVN 12211:2018 (ISO/IEC 24759:2017) quy định các phương pháp kiểm thử được các phòng thí nghiệm kiểm định sử dụng để đánh giá liệu mô-đun mật mã có tuân thủ các yêu cầu được quy định trong TCVN 11295:2016 (ISO/IEC 19790:2012) và các chỉ số kiểm thử (test metrics) được quy định trong tiêu chuẩn này cho từng chức năng an toàn liên quan được đề cập trong TCVN 11295:2016 (ISO/IEC 19790:2012) hay không.

Phương pháp kiểm thử được triển khai trong tiêu chuẩn này là cách tiếp cận "nhấn-nút" hiệu quả, tức là các bài kiểm thử này đáng tin về mặt kỹ thuật, có thể lặp lại đợc và có chi phí vừa phải.

2 Tài liệu viện dẫn

Các tài liệu sau đây được viện dẫn trong văn bản theo cách mà một phần hoặc toàn bộ nội dung của chúng cấu thành các yêu cầu của tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả các sửa đổi, bổ sung nếu có).

TCVN 11295:2016 (ISO/IEC 19790:2012), Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu an toàn cho mô-đun mật mã.

TCVN 12211:2018 (ISO/IEC 24759:2017), Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu kiểm định cho 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

phân tích kênh kề nâng cao

advanced side-channel analysis

ASCA

Việc khai thác nâng cao các kênh kề tức thời phát xạ từ một thiết bị mật mã, dựa trên sự phụ thuộc của các kênh này vào dữ liệu đang được xử lý và phép toán đang được thực thi, nhằm mục đích khôi phục lại các tham số bí mật.

3.2

Phân tích điện năng tương quan

correlation power analysis

CPA

Phân tích mà tại đó hệ số tương quan được sử dụng trong phương pháp thống kê.

3.3

Lớp tham số an toàn trọng yếu

critical security parameter class

Lớp CSP

Lớp mà một *tham số an toàn trọng yếu* (3.3) được phân lớp vào.

VÍ DỤ: Các khóa mật mã, dữ liệu xác thực chẳng hạn như các mật khẩu, các mã PIN, dữ liệu xác thực sinh trắc học.

3.4

phân tích vi sai điện từ

differential electromagnetic analysis

DEMA

Phân tích của các biến thiên đối với trường điện từ phát xạ từ một mô-đun mật mã, sử dụng các phương pháp thống kê trên một số lượng lớn các giá trị phát xạ điện từ được đo để xác định xem giả thuyết về các tập con được phân chia của một tham số bí mật có chính xác hay không, nhằm mục đích trích xuất thông tin có tương quan với hoạt động của chức năng an toàn.

3.5

phân tích vi sai điện năng

differential power analysis

DPA

Phân tích sự biến thiên trong mức tiêu thụ điện năng của một mô-đun mật mã, nhằm mục đích trích xuất thông tin tương quan với tính toán mật mã.

3.6

phân tích điện từ

electromagnetic analysis

EMA

Phân tích trường điện từ phát xạ từ một mô-đun mật mã là kết quả của sự chuyển mạch logic, nhằm mục đích trích xuất thông tin tương quan với tính toán của chức năng an toàn và sau đó là giá trị của các tham số bí mật chẳng hạn như các khóa mật mã.

3.7

Mô-đun đang được kiểm thử

implementation under test

IUT

Mô-đun được kiểm thử dựa trên các phương pháp không xâm lấn

3.8

phân tích điện năng

power analysis

PA

Phân tích mức tiêu thụ điện năng của một mô-đun mật mã, nhằm mục đích trích xuất thông tin tương quan với hoạt động của chức năng an toàn và sau đó là các giá trị của các tham số bí mật chẳng hạn như các khóa mật mã.

3.9

phân tích kênh kề

side-channel analysis

SCA

Khai thác sự việc rằng các kênh kề tức thời do một thiết bị mật mã phát xạ phụ thuộc vào dữ liệu mà thiết bị này xử lý dữ liệu và vào phép toán mà nó thực hiện để khôi phục lại các tham số bí mật.

3.10

tấn công va chạm kênh kề

side-channel collision attack

loại mạnh của *phân tích kênh kề* (3.9) thường kết hợp rò rỉ từ các điểm thời gian khác nhau, làm chúng vốn dĩ nhị biến.

3.11

phân tích điện từ đơn giản

simple electromagnetic analysis

SEMA

Phân tích trực tiếp (chủ yếu dựa trên quan sát) các mẫu thực thi lệnh hoặc các hoạt động của mạch logic, thu được thông qua việc giám sát những biến thiên trong trường điện từ phát xạ từ một mô-đun mật mã, nhằm mục đích làm lộ ra các đặc điểm và cách thức triển khai của các thuật toán mật mã và sau đó là các giá trị của những tham số bí mật.

3.12

phân tích điện năng đơn giản

simple power analysis

SPA

Phân tích trực tiếp (chủ yếu dựa trên quan sát) các mẫu thực thi lệnh (hoặc việc thực thi các lệnh riêng biệt), trong mối liên quan đến mức tiêu thụ năng lượng điện của một mô-đun mật mã, nhằm mục đích trích xuất thông tin tương liên với một phép toán mật mã.

3.13

phân tích thời lượng

timing analysis

TA

Phân tích các biến thiên của thời gian phản hồi hoặc thực thi của một hoạt động trong một chức năng an toàn, có thể tiết lộ tri thức về tham số an toàn hoặc có liên quan đến tham số đó chẳng hạn như một khóa mật mã hoặc số PIN.

4 Ký hiệu và thuật ngữ viết tắt

ASCA	advanced side-channel analysis	phân tích kênh kề nâng cao
AES	advanced encryption standard	tiêu chuẩn mã hóa tiên tiến
CPA	correlation power analysis	phân tích điện năng tương quan

CSP	critical security parameter	tham số an toàn trọng yếu
DEMA	differential electromagnetic analysis	phân tích vi sai điện từ
DES	data encryption standard	tiêu chuẩn mã hóa dữ liệu
DLC	discrete logarithm cryptography	mật mã dựa trên logarit rời rạc
DPA	differential power analysis	phân tích vi sai điện năng
DSA	digital signature algorithm	thuật toán chữ ký số
ECC	elliptic curve cryptography	mật mã đường cong elliptic
ECDSA	elliptic curve digital signature algorithm	thuật toán chữ ký số dựa trên đường cong elliptic
EM	Electromagnetic	điện từ
EMA	electromagnetic analysis	phân tích điện từ
HMAC	keyed-hashing message authentication code	mã xác thực thông báo dựa trên hàm băm có khóa
IFC	integer factorization cryptography	mật mã dựa trên phân tích số nguyên
IUT	implementation under test	mô-đun đang được kiểm thử
MAC	message authentication code	mã xác thực thông báo
PA	power analysis	phân tích điện năng
PC	personal computer	máy tính cá nhân
PCB	printed circuit board	bảng mạch in
PKCS	public-key cryptography standards	các tiêu chuẩn mật mã khóa công khai
RBG	random bit generator	bộ sinh bit ngẫu nhiên
RNG	random number generator	bộ sinh số ngẫu nhiên
RSA	Rivest Shamir Adleman	Tên của hệ mã do ba nhà toán học Rivest, Shamir và Adleman phát minh
SCA	side-channel analysis	phân tích kênh kề
SEMA	simple electromagnetic analysis	phân tích điện từ đơn giản
SHA	secure hash algorithm	thuật toán băm an toàn
SNR	signal to noise ratio	tỉ số tín hiệu trên nhiễu
SPA	simple power analysis	phân tích điện năng đơn giản
USB	universal serial bus	chuẩn kết nối tuần tự đa dụng
TA	timing analysis	phân tích thời lượng
.	multiplication symbol	ký hiệu phép nhân

5 Bố cục tiêu chuẩn

Điều 6 quy định các phương pháp tấn công không xâm lấn mà một mô-đun mật mã phải chống lại để phù hợp với TCVN 11295:2016 (ISO/IEC 19790:2012).

Điều 7 quy định các phương pháp kiểm thử tấn công không xâm lấn.

Điều 8 quy định các phương pháp kiểm thử cho việc phân tích kênh kề đối với các hệ mật khóa đối xứng.

Điều 9 quy định các phương pháp kiểm thử cho việc phân tích kênh kề đối với các hệ mật khóa phi đối xứng.

Tiêu chuẩn này phải được sử dụng cùng với TCVN 12211:2018 (ISO/IEC 24759:2017) để chứng minh sự tuân thủ TCVN 11295:2016 (ISO/IEC 19790:2012).

6 Các phương pháp tấn công không xâm lấn

Điều này quy định các phương pháp tấn công không xâm lấn cần phải được giải quyết [06.01] để đảm bảo sự tuân thủ tiêu chuẩn TCVN 11295:2016 (ISO/IEC 19790:2012).

Các tấn công không xâm lấn sử dụng các kênh kề (thông tin thu được từ việc triển khai vật lý của một hệ mật) do mô-đun đang được kiểm thử (IUT) phát xạ, chẳng hạn như:

- Mức tiêu thụ điện năng của IUT,
- Phạt xạ điện từ của IUT,
- Thời gian tính toán của IUT.

Số lượng các kênh kề khả dĩ có thể tăng lên trong tương lai (ví dụ: phát xạ phô-tôn, phát xạ âm thanh).

Để phân loại các tấn công một cách hình thức hơn, một hình thức luận cho phép làm nổi bật các mối quan hệ giữa các tấn công khác nhau và cung cấp một phương pháp có hệ thống để mô tả một tấn công mới.

Một tấn công được mô tả theo cách thức sau:

<KKK>-<YYY>-<XXX>-<ZZZ>-<TTT>

KKK đề cập đến bậc của tấn công (ví dụ: “2O” cho tấn công bậc hai).

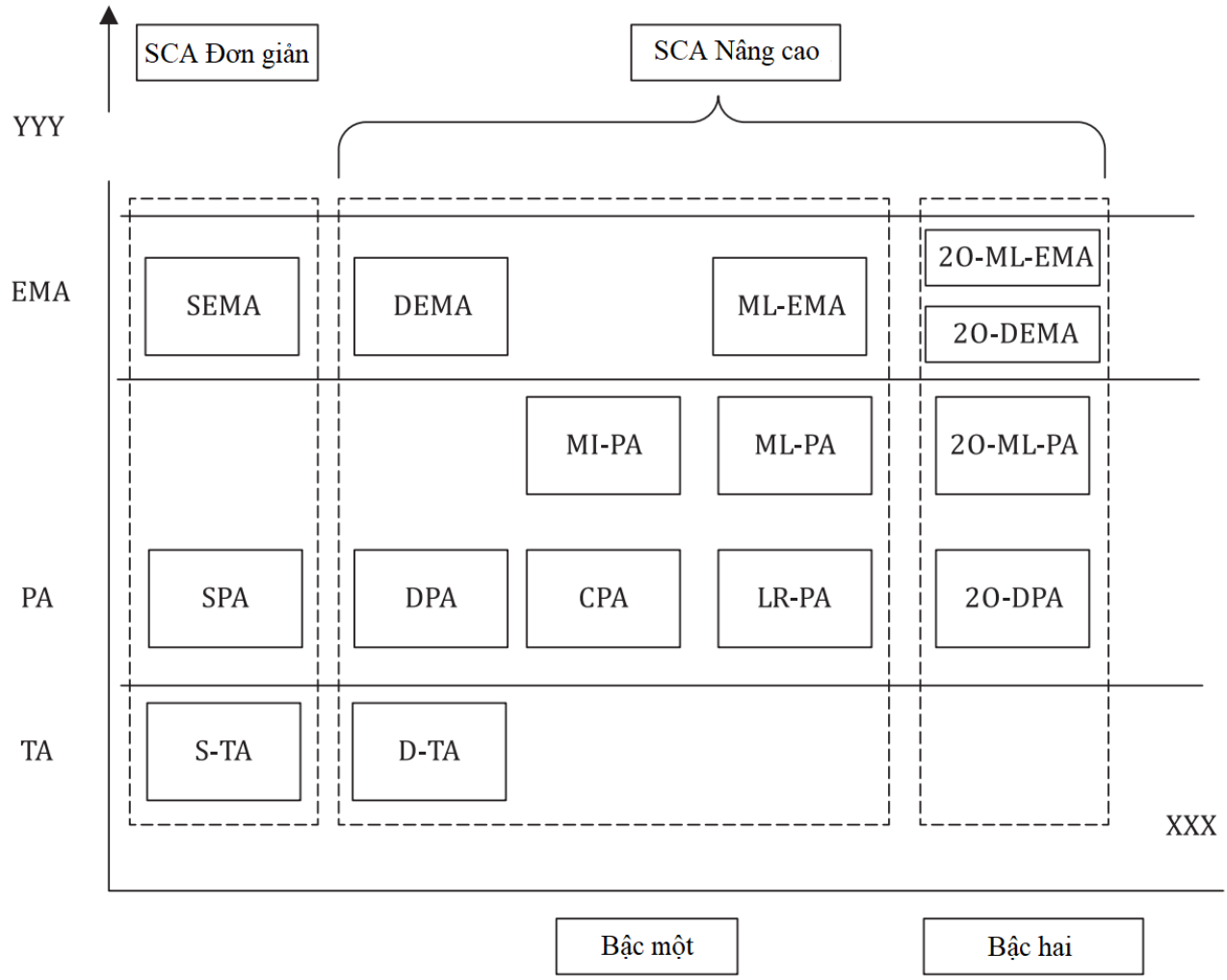
YYY đề cập đến phương pháp xử lý thống kê được sử dụng trong tấn công (ví dụ: “S” cho đơn giản (simple), “C” cho tương quan (correlation), “MI” cho thông tin tương hỗ (mutual), “ML” cho hợp lý cực đại (maxmimum likelihood), “D” cho hiệu số trung bình (difference), “LR” cho hồi quy tuyến tính (linear regression), v.v.).

CHÚ THÍCH 1: Các phương pháp xử lý thống kê khác có thể được chèn vào, như "dOC" tương ứng với một phương pháp xử lý tương quan khai thác các moment bậc d (ví dụ, thu được bằng cách nâng mỗi điểm mục tiêu trong các vết lên lũy thừa *d*, hoặc bằng cách kết hợp *d* điểm trên mỗi vết trước khi xử lý tương quan).

XXX đề cập đến loại kênh kề được quan sát: ví dụ: “PA” cho phân tích điện năng, “EMA” cho phân tích điện từ, “TA” cho phân tích thời gian, v.v.

ZZZ có thể đề cập đến đặc tính tấn công có lập hồ sơ (“P”) hoặc không lập hồ sơ (“UP”) của tấn công. Đây là tùy chọn và giá trị mặc định là “UP”.

TTT đề cập đến hướng của tấn công (ví dụ: “V” cho dọc, “H” cho ngang, “R” cho hình chữ nhật).



Hình 1 - Phân loại các tấn công không xâm lấn

CHÚ THÍCH 2: Thay vì chỉ chia phân tích kênh kề nâng cao (ASCA) thành các trường hợp đơn biến và đa biến, việc phân loại vẫn có thể được tinh chỉnh bằng cách tách các tấn công dựa trên "bộ phân biệt biến số" (tập trung vào một mô men cụ thể của phân bố của biến mục tiêu) khỏi các tấn công dựa trên "bộ phân biệt pdf" (bộ phân biệt phân tích không xâm lấn yêu cầu đầu vào là một đánh giá của hàm mật độ xác suất rò rỉ khi biết khóa bí mật). Loại đầu tiên bao gồm ASCA dựa trên kỹ thuật tương quan hoặc trên các kỹ thuật hồi quy tuyến tính. Loại thứ hai bao gồm một số ví dụ như các tấn công khả năng tối đa và các tấn công thông tin tương hỗ.

CHÚ THÍCH 3: Các phương pháp tấn công phân tích điện năng đơn giản (SPA) và phân tích điện từ đơn giản (SEMA) bao gồm một số mở rộng của các tấn công SPA và SEMA cơ bản (tức là tấn công mẫu). Các phương pháp tấn công phân tích điện năng vi sai (DPA) và phân tích điện từ vi sai (DEMA) bao gồm một số mở rộng của các tấn công DPA và DEMA cơ bản [tức là phân tích điện năng tương quan (CPA) và các tấn công DPA bậc cao hơn]. Việc kiểm thử chúng không bắt buộc trong tiêu chuẩn này.

Phân loại các tấn công không xâm lấn được minh họa trong Hình 1. Phạm vi áp dụng của tiêu chuẩn này tập trung vào các tấn công bậc một, tức là hai cột đầu tiên của Hình 1. Các tấn công không xâm lấn mới nổi và các kênh kề được mô tả trong Phụ lục D nhưng hiện không áp dụng như phương pháp kiểm thử bắt buộc trong tiêu chuẩn này.

Các biến được sử dụng trong mô tả ASCA là:

A xử lý mật mã

C xử lý quan sát

D số lượng dự đoán

d_C bậc đa biến

d_D bậc đa biến

d_o chiều của quan sát

F hàm, tức là thao tác

h quan sát

i chỉ số

K khóa bí mật

k_1 khóa con 1

k_2 khóa con 2

M mô hình rò rỉ

N số lượng quan sát

o_i khoảng quan sát

(o_i)_i khoảng quan sát thứ i

pred_i dự đoán

t_i lần lặp thứ i của thời gian

x1_i lần lặp thứ i của x1

x2_i lần lặp thứ i của x2

X dữ liệu đã biết

ASCA được mô tả theo các bước sau:

1) Đo N khoảng quan sát *o_i* liên quan đến một xử lý mật mã *A* được tham số hóa bởi một đầu vào đã biết *X* và một khóa bí mật *K*.
2) (Tùy chọn) Chọn một mô hình rò rỉ *M* cho sự rò rỉ của thiết bị.
3) (Tùy chọn) Chọn một xử lý quan sát *C* (mặc định *C* được đặt là chức năng đồng nhất).
4) Đặt tất cả các giả thuyết h về giá trị của *K* hoặc một phần của *K*.
5) Chọn giả thuyết có kiểm thử thống kê lớn nhất làm khóa có khả năng cao nhất.

CHÚ THÍCH 4: Các quan sát *o_i* có thể là đơn biến hoặc đa biến. Trong trường hợp đa biến, mỗi tọa độ của *o_i*, khi được xem như một vector, tương ứng với một thời điểm *t_i* khác nhau. Chiều của *o_i* được ký hiệu là *d_o* trong phần còn lại của chú thích này.

CHÚ THÍCH 5: Trong các tấn công va chạm kênh kề chống lại các mã khối, bước thứ hai được bỏ qua và bước thứ ba chỉ đơn giản bao gồm việc lựa chọn một điểm trong các vết o_i. Sau đó, giả thuyết h thường tương ứng với một giả thuyết về hiệu ($k_1 - k_2$) của hai phần của khóa đích K (ví dụ: hai khóa con trong một thực thi mã khối). Cuối cùng, các dự đoán được suy ra từ các quan sát (*o_i*)_*i* và hiệu *h*. Ví dụ, nếu tấn công nhắm vào thao tác của một giá trị $F(x_1\_i+k_1)$ [tức là $C(o\_i)$ tương ứng với phần quan sát liên quan đến thao tác của $F(x_1\_i+k_1)$], thì tấn công sẽ trích xuất từ các *o_i* các quan sát trong quá trình thao tác của các giá trị khác $F(x_2\_i+k_2)$. Các quan sát đó sẽ được sắp xếp lại sao cho $x_2\_i - x_1\_i = h$. Khi đó *h_i* tương ứng với phần quan sát liên quan đến thao tác của $F(x_2\_i+k_2) = F(x_1\_i+k_1)$ nếu *h* là đúng. Để xác thực giả thuyết, một hệ số tương quan thường được sử dụng cho *D*. Ngoài ra, tất cả các tấn công được mô tả trong Điều 6 có thể là dọc, ngang hoặc hình chữ nhật (tức là cả ngang và dọc). Một tấn công được gọi là dọc nếu mỗi quan sát o_*i* tương ứng với một xử lý thuật toán khác nhau. Nếu tất cả các o_*i* đều có cùng một thuật toán xử lý, thì tấn công được gọi là ngang. Nếu một số o_*i* chia sẻ cùng một thuật toán xử lý trong khi một số o_*i* khác thì không, thì tấn công được gọi là hình chữ nhật. Các tấn công cổ điển được quy định trong tài liệu là dọc và phương thức hoạt động này do đó sẽ được định nghĩa là phương thức mặc định. Ví dụ về các tấn công được thực hiện ở chế độ ngang có thể được tìm thấy trong Thư mục tài liệu tham khảo [43] và [44].

CHÚ THÍCH 6: Một cơ quan phê duyệt có thể sửa đổi, thêm hoặc xóa các phương pháp tấn công không xâm lấn, sự liên kết với các chức năng an toàn (xem Bảng C.1) và các chỉ số kiểm thử giảm thiểu tấn công không xâm lấn được quy định trong tiêu chuẩn này.

7 Các phương pháp kiểm thử tấn công không xâm lấn

7.1 Tổng quan

Điều này giới thiệu tổng quan về các phương pháp kiểm thử tấn công không xâm lấn đối với các phương pháp tấn công không xâm lấn tương ứng được quy định trong Điều 6.

7.2 Chiến lược kiểm thử

Mục đích của kiểm định tấn công không xâm lấn là để đánh giá xem một mô-đun mật mã sử dụng các kỹ thuật giảm thiểu tấn công không xâm lấn liệu có thể cung cấp khả năng kháng lại các tấn công tại mức an toàn mong muốn không. Không có chương trình kiểm định được chuẩn hóa có thể đảm bảo bảo vệ hoàn toàn chống lại các tấn công. Thay vào đó, các chương trình có hiệu quả xác nhận rằng đã có đủ sự cẩn trọng đã được thực hiện trong việc thiết kế và triển khai các biện pháp giảm thiểu tấn công không xâm lấn.

Các tấn công không xâm lấn khai thác độ lệch tiềm ẩn trong các đại lượng vật lý được đo theo cách không xâm lấn trên hoặc xung quanh IUT. Độ lệch thống kê này được sinh ra và phụ thuộc vào thông tin bí mật mà các tấn công hướng đến. Để biết chi tiết hơn, xem Thư mục tài liệu tham khảo [16]. Độ lệch có thể không dễ nhận thấy nhưng thường ổn định. Trong tiêu chuẩn này, thông tin thiên lệch phụ thuộc vào thông tin bí mật được gọi là rò rỉ, từ đây về sau. Một thiết bị có thể không đạt một hoặc nhiều kiểm thử nếu bằng chứng thí nghiệm cho thấy thông tin rò rỉ vượt quá các ngưỡng rò rỉ cho phép. Điều này ngụ ý rằng sự rò rỉ chứng tỏ có một lỗ hổng tiềm ẩn. Ngược lại, các tấn công không đạt và kiểm thử đạt trừ khi quan sát thấy rò rỉ. Phép kiểm thử sự tồn tại của rò rỉ được gọi là phân tích rò rỉ (leakage analysis), từ đây về sau.

Mục đích là thu thập và phân tích các phép đo bên trong các giới hạn kiểm định xác định chẳng hạn như số lượng dạng sóng tối đa thu thập, thời gian kiểm thử đã trôi qua và xác định mức độ của rò rỉ thông tin CSP. Bởi vậy, các giới hạn kiểm thử và các ngưỡng rò rỉ tạo thành các tiêu chí kiểm thử. Thời gian thu thập tối đa cũng phải được giới hạn [07.01]. Các giá trị cho mức an toàn 3 và 4 được trình bày chi tiết trong Phụ lục A.

Xét đến thử nghiệm tấn công thời lượng. Nếu kiểm thử cho thấy thời gian tính toán có sự lệch so với CSP thì IUT không đạt. Đối với DPA, nếu kiểm định cho thấy mức tiêu thụ điện năng trong các quá trình liên quan đến CSP bị lệch so với CSP thì IUT không đạt. Phương pháp kiểm định sử dụng kiểm định giả thuyết thống kê để xác định khả năng tồn tại của độ lệch. Do đó, tiêu chuẩn này cung cấp một ngưỡng rò rỉ theo ý nghĩa thống kê. Kiểm định sẽ không đạt nếu một độ lệch vượt quá ngưỡng rò rỉ. Các điều kiện đạt/không đạt đối với mức an toàn mong muốn được đưa ra trong Phụ lục A.

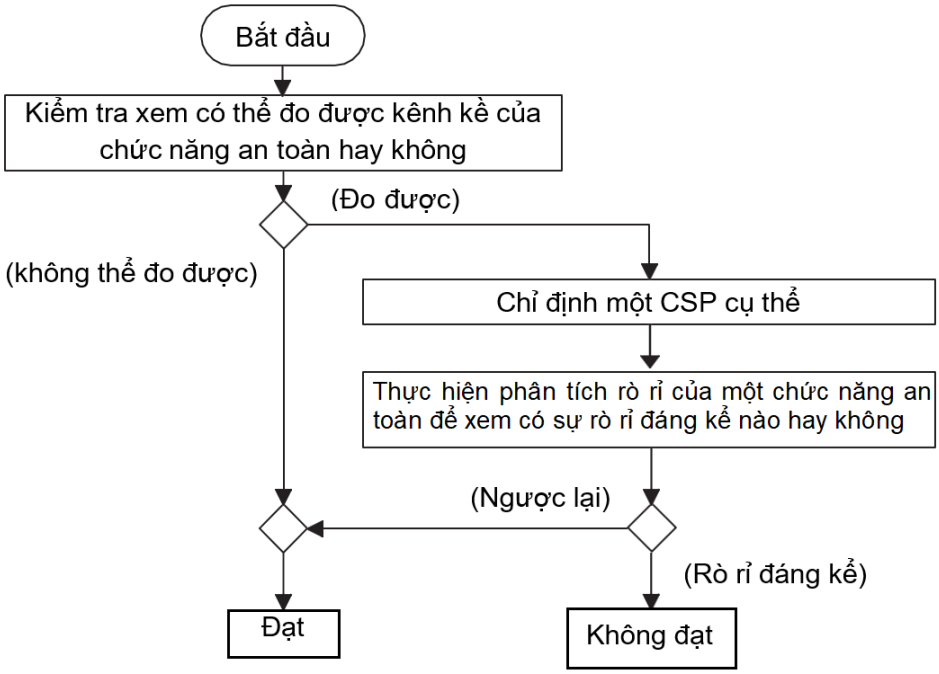
7.3 Lưu đồ phân tích kênh kề

7.3.1 Luồng kiểm định lõi

Người kiểm thử thu thập dữ liệu đo lường từ IUT và áp dụng một tập hợp các kiểm thử thống kê trên dữ liệu đã thu thập. Xem Phụ lục B để biết các yêu cầu đối với thiết bị đo lường. Kiểm thử lõi đề cập đến việc kiểm định cho một chức năng an toàn duy nhất với một lớp tham số an toàn trọng yếu (CSP) duy nhất, trong đó các lớp CSP bao gồm khóa mật mã, dữ liệu sinh trắc học hoặc mã PIN. Nếu một số chức năng an toàn xử lý nhiều hơn một lớp CSP, việc phân tích rò rỉ cho mọi lớp CSP áp dụng sẽ được thực hiện cho mỗi chức năng an toàn.

Phương pháp kiểm thử yêu cầu lặp lại các kiểm thử lõi với các lớp CSP khác nhau cho đến khi xảy ra kết quả không đạt đầu tiên hoặc tất cả các lớp CSP đều đạt. Nếu một kiểm thử lõi không thể tiếp tục do IUT giới hạn số lượng thao tác lặp lại, kết quả được tính là đạt và kiểm thử lõi được tiếp tục với lớp CSP tiếp theo.

Kiểm thử lõi được trình bày trong Hình 2. Khung công việc kiểm thử khả năng kháng kênh kề được mô tả trong Hình 3. Phân tích rò rỉ cho TA được trình bày trong Hình 4, đối với SPA/SEMA trong Hình 5 và đối với DPA/DEMA trong Hình 6.



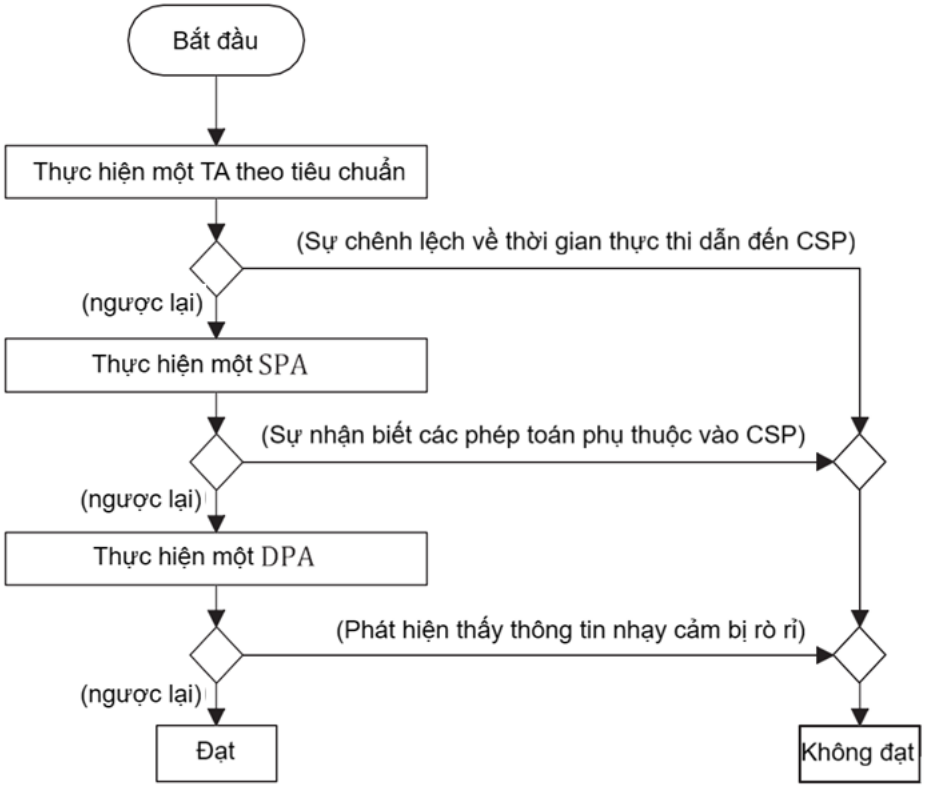
Hình 2 — Luồng kiểm thử lõi

Hình 2 cho thấy luồng của một bài kiểm thử lõi. Đầu tiên, tài liệu của nhà cung cấp được xác minh đối với lớp CSP được chỉ định. Thứ hai, tính thực tiễn của việc đo lường các đặc tính vật lý được xác định. Nếu không thể thực hiện phép đo, kết quả kiểm thử là đạt. Phòng kiểm định phải [07.02] cung cấp lý do giải thích tại sao kênh kề không thể đo lường được. Một danh sách các lý do được chấp nhận để một phòng thí nghiệm đánh giá một kênh kề là không thể đo lường được được đưa ra trong Phụ lục G. Thứ ba, một tập hợp các CSP do phòng kiểm định xác định được cấu hình vào IUT. Cuối cùng, phần cốt lõi của bài kiểm thử lõi, tức là việc phân tích, được trình bày trong các Hình 3, 4, 5, 6, 7, 8, và D.1, được thực hiện và rò rỉ đáng kể sẽ được quan sát thấy hoặc không.

7.3.2 Khung công việc kiểm định kháng kênh kề

Như đã giải thích trong 7.3.4, 7.3.5 và 7.3.6, phòng thử nghiệm sẽ [07.03] kiểm tra độ an toàn của IUT chống lại TA, SPA và DPA.

Kiểm định tuần tự của ba tấn công dẫn đến khung tấn công được mô tả trong Hình 3. Phòng thí nghiệm kiểm định nên tuân theo thứ tự các bước thực hiện. Ví dụ, SPA chỉ có thể được kiểm thử nếu TA đạt.



Hình 3 —Khung công việc kiểm thử kháng kênh kề

Phương pháp luận được đề xuất để đánh giá khả năng kháng tấn công kênh kề không đòi hỏi phải trích xuất toàn bộ khóa mới có thể kết luận thiết bị không đạt: Một IUT có thể bị đánh giá không đạt nếu có thể chứng minh được rằng có một lượng đáng kể thông tin nhạy cảm bị rò rỉ. Tuy nhiên, cần lưu ý rằng mục đích chính của tiêu chí đạt/không đạt là IUT chỉ có thể bị đánh giá không đạt nếu có nguy cơ tiết lộ thông tin CSP/thông tin nhạy cảm.

7.3.3 Thông tin nhà cung cấp phải cung cấp

Nhà cung cấp phải [07.04] cung cấp thông tin sau về các thuật toán và biện pháp đối phó được triển khai trong IUT:

a) các thuật toán mật mã được triển khai.

b) thiết kế của triển khai.

c) các điều kiện/chế độ sử dụng mà tại đó IUT dễ bị ảnh hưởng bởi phân tích kênh kề.

Hơn nữa, phòng thử nghiệm phải [07.05] có khả năng sửa đổi CSP và bản mã khi thực hiện thử nghiệm kênh kề.

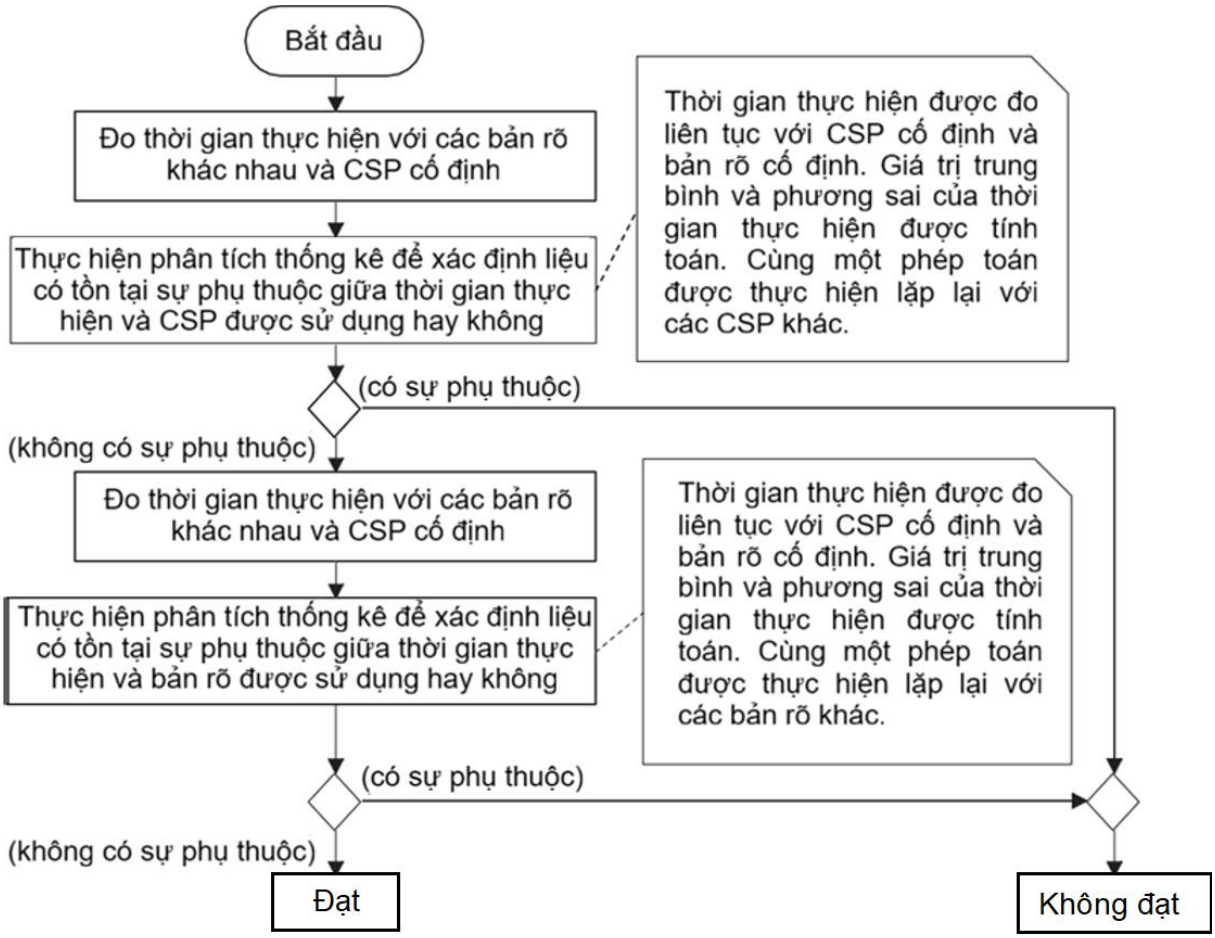
Khi thực hiện phân tích kênh kề, thông thường thực hiện căn chỉnh tín hiệu sao cho các vết khác nhau có thể được so sánh tại cùng một thời điểm trong quá trình tính toán mật mã. Để phục vụ mục đích kiểm định kênh kề, nhà cung cấp nên cung cấp cho phòng thí nghiệm kiểm định tín hiệu đồng bộ tốt nhất tương ứng với thời điểm bắt đầu của hoạt động mật mã. Ví dụ, trong chế độ kiểm định, thiết bị có thể cung cấp một điểm kích hoạt bên ngoài để chỉ ra thời điểm bắt đầu và kết thúc của phép toán mật mã. Nếu không có thông tin về thời điểm bắt đầu và kết thúc này, phòng thí nghiệm kiểm định nên áp dụng các kỹ thuật tiêu chuẩn dựa trên xử lý tín hiệu và đối sánh tín hiệu. Trong các trường hợp các vết được căn chỉnh tốt tại lúc bắt đầu của phép toán mật mã, phòng thí nghiệm có thể được yêu cầu sử dụng kỹ thuật đối sánh tín hiệu tiêu chuẩn để cải thiện việc căn chỉnh tại các giai đoạn nội bộ cụ thể của thuật toán; số lượng và các vị trí của các điểm căn chỉnh này do phòng thí nghiệm kiểm định quy định.

Sau đó, nhà cung cấp nên cung cấp một chức năng cho phép phòng thử nghiệm:

d) đồng bộ hóa các phép đo của mình;

e) kiểm tra chất lượng các phép đo của mình (xem 7.3.6 để biết thêm chi tiết).

7.3.4 Phân tích rò rỉ TA

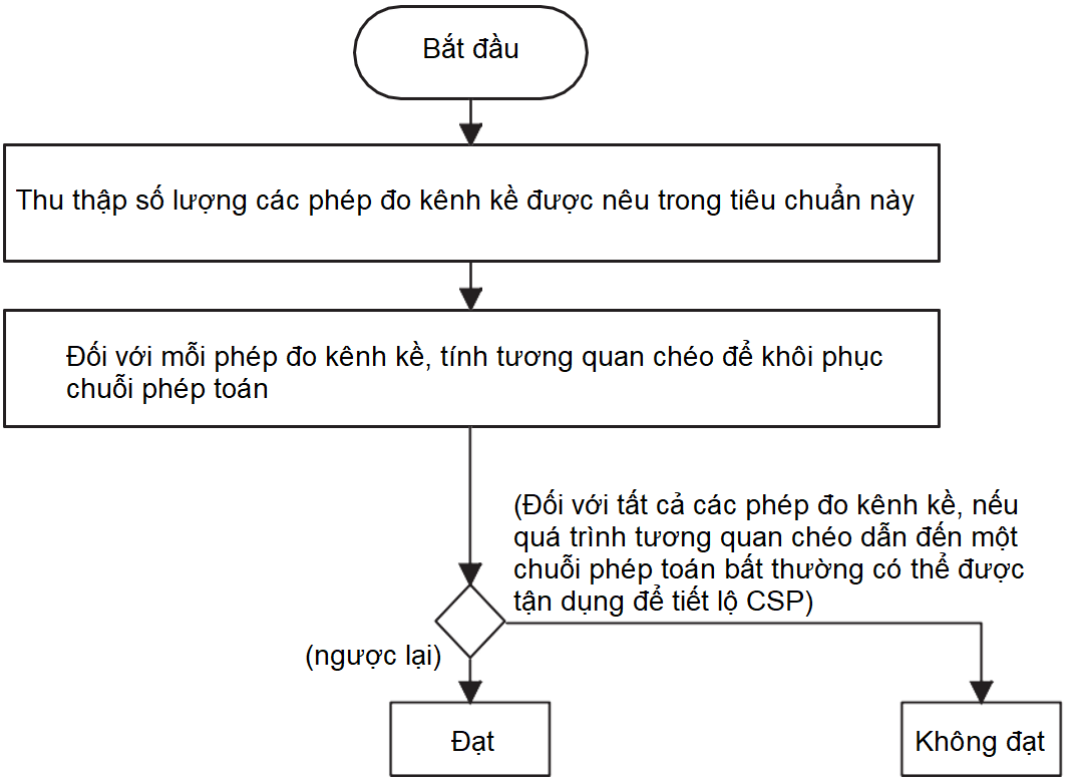


Hình 4 — Phân tích rò rỉ đối với các tấn công thời lượng

Hình 4 chỉ ra luồng phân tích rò rỉ đối với các tấn công thời lượng. Luồng có thể được chia làm hai giai đoạn. Đối với giai đoạn thứ nhất, các thời gian thực thi đối với một số CSP khác nhau và bản rõ cố định được đo đạc. Nếu thời gian thực thi được đo không chỉ ra sự phụ thuộc với CSP được sử dụng thông qua phân tích thống kê thì kiểm định tiếp tục sang giai đoạn thứ hai. Ngược lại, kiểm thử không đạt. Đối với giai đoạn hai, các thời gian thực thi với một số văn bản khác nhau và một CSP cố định được đo. Nếu thời gian thực thi được đo không chỉ ra sự phụ thuộc với văn bản đã sử dụng thì kiểm thử đạt. Ngược lại, kiểm thử không đạt. Nếu thời gian thực thi khó đo thì cần sử dụng một giá trị dung sai ε bằng một chu kỳ xung của con chip mục tiêu. Để so sánh hai giá trị thời gian (hay hai giá trị thời gian trung bình) T1 và T2, phép kiểm định đạt nếu $|T1 - T2| < \varepsilon$ và ngược lại là không đạt. Phân tích thời gian [07.07] phải được thực hiện với số lượng phép đo đủ. Các yêu cầu chi tiết đối với mức an toàn 3 và 4 được nêu trong Phụ lục A.

Không chỉ hiệu số các giá trị trung bình, mà cả các giá trị phương sai cần được tính toán để có thể phát hiện rò rỉ tấn công thời gian bậc hai. Thực vậy, các tấn công thời lượng bậc hai là các mối đe dọa thực tế. [58]

7.3.5 Phân tích rò rỉ SPA/SEMA



Hình 5 — Phân tích rò rỉ SPA (SEMA)

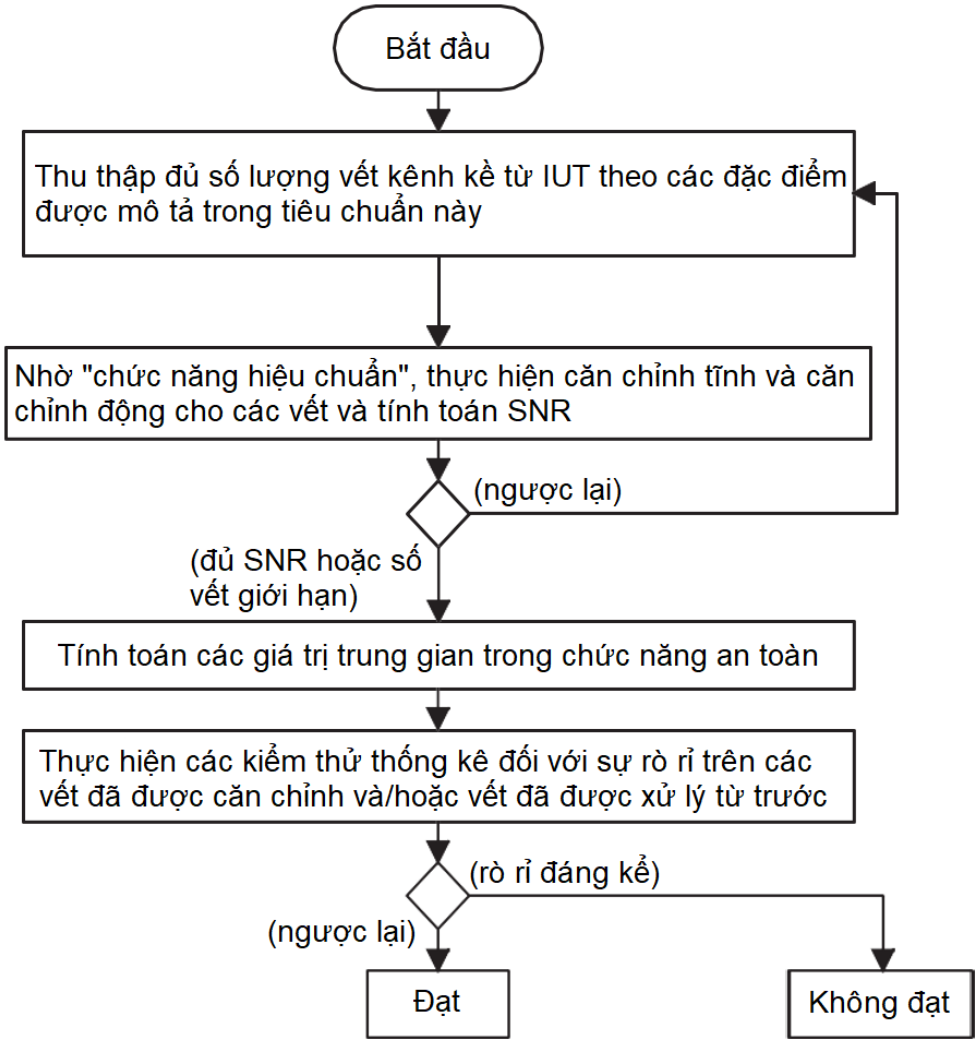
Hình 5 chỉ ra luồng phân tích rò rỉ SPA/SEMA. Luồng có thể được chia thành hai giai đoạn.

Đầu tiên, phòng thí nghiệm kiểm định phải [07.08] thu thập số lượng phép đo kênh kề liên quan đến mức an toàn mong muốn, như được chỉ định trong Phụ lục A.

Mật mã phi đối xứng lặp đi lặp lại sử dụng các phép toán sơ cấp. Đối với RSA các phép toán này là mô-đun bình phương (ký hiệu là “S”) và phép toán nhân (ký hiệu là “M”). Đối với ECC, chúng là các phép toán nhân đôi và cộng điểm. Vì khóa có thể nhận được từ bậc của các phép toán, phòng thí nghiệm kiểm định phải phân biệt được các phép toán này là điều quan trọng. Khi các phép đo kênh kề có thể bị nhiễu (xem Phụ lục E đối với tiêu chí chất lượng cho các thiết lập đo lường), thì khó có thể nhận diện các phép toán này một cách trực quan. Một phương pháp tốt để nhận biết phép toán lặp được gọi là “tương quan chéo”. Phương pháp này cũng giúp loại bỏ được đánh giá chủ quan từ phòng thí nghiệm kiểm định. Khi tương quan là yếu đến mức không có công bố rõ ràng được đưa ra thì phòng thí nghiệm kiểm định có thể sắp đặt một phân tích cụm.

Đối với tất cả các phép đo kênh kề, nếu quá trình tương quan chéo dẫn đến một dãy hoạt động bất thường mà dẫn đến CSP thì kết quả kiểm định là không đạt. Mục quan trọng cần lưu ý là IUT chỉ có thể không đạt nếu CSP đã được tiết lộ từ dãy phép toán bất thường.

7.3.6 Phân tích rò rỉ DPA/SEMA



Hình 6 — Phân tích rò rỉ DPA (DEMA)

Hình 6 chỉ ra luồng phân tích rò rỉ DPA/DEMA. Phòng thí nghiệm kiểm định phải [07.09] thu thập đủ các vết. Phương pháp để tính toán số lượng vết cần thiết được phác thảo trong Hình 7 và được trình bày chi tiết trong Phụ lục A. Kết quả được thể hiện cho biết có quan sát thấy rò rỉ đáng kể hay không. Trong trường hợp nghi ngờ, cần sử dụng hộp rõ hoặc hộp trắng để làm rõ sự không rõ ràng (xem Thư mục tài liệu tham khảo [45]). Thực vậy, nếu phép kiểm định là kiểm định t (Student's t-test) thì không phải tất cả các rò rỉ đều là thông tin nhạy cảm: thông thường, các vi phạm kiểm định khả thi phát sinh từ các biến không phải CSP, chẳng hạn như bản rõ hay bản mã của một mã khối (xem Phụ lục H). Do đó, dựa trên phân tích của tài liệu IUT, có thể xác định được xem các vi phạm kiểm thử có phụ thuộc vào CSP hay không. Các nội dung tương tự được áp dụng cho Hình 6.

Theo nguyên tắc chung, giả định rằng các phép toán mật mã luôn được thực hiện tại cùng một thời điểm trong mỗi phép đo (tiêu thụ hay phát xạ). Tuy nhiên, các nhà phát triển có khả năng tích hợp các đồng hồ nội bộ làm thay đổi tần số phép toán hoặc giới thiệu ngẫu nhiên trạng thái chờ không tính toán trong quá trình thực thi các thuật toán, khiến thời gian không còn là hằng số và các tính toán mật mã không được thực hiện tại cùng một thời điểm. Điều này dẫn đến các sai lệch căn chỉnh thường gặp trong tập vết, khiến phân tích trở nên khó khăn và tốn kém hơn nhiều xét về số lượng các vết cần xử lý. Những thay đổi so với hành vi ban đầu này là các biện pháp đối phó được triển khai bởi những người phát triển để chống lại khả năng thu thập thông tin qua các kênh kề, phá vỡ các giả thuyết đặc trưng cho các tấn công đã biết.

Trong các triển khai mật mã không áp dụng các biện pháp đối phó cụ thể, sự sai lệch căn chỉnh phát sinh từ các lỗi trong cấu hình phép đo, sự khác biệt giữa các miền xung nhịp, hiện tượng tranh chấp băng thông, sự gián đoạn OS, v.v., tại thời điểm bắt đầu thu thập mức tiêu thụ (hoặc phát xạ) điện năng. Trong trường hợp này, các vết có thể được căn chỉnh nếu sự không chắc chắn có thể được xác định khi thực hiện phép đo, bằng cách dịch chuyển các vết đo một cách thích hợp. Quá trình này được gọi là "căn chỉnh tĩnh". Sự không chắc chắn này cũng có thể được giảm thiểu hoặc ít nhất là tạo thuận lợi cho việc căn chỉnh nếu có (hoặc tồn tại) một tín hiệu kích hoạt báo hiệu khi phép toán bắt đầu.

Khi quá trình triển khai chủ động đưa vào các khoảng trễ thời gian ngẫu nhiên hoặc thay đổi tần số xung nhịp, việc căn chuyển tĩnh không thể căn chỉnh hoàn toàn các vết đo. Trong trường hợp này, cái được gọi là căn chỉnh động được áp dụng bằng cách đối sánh các đoạn của các vết đo với các mức dịch chuyển khác nhau và thực hiện lấy mẫu phi tuyến đối với các vết đo. Sau quá trình này, các phần khác nhau dọc theo các vết được đưa về cùng vị trí. (ví dụ, vị trí của các vòng khác nhau trùng khớp trong tất cả các vết).

Nhà cung cấp nên hợp tác với phòng thí nghiệm kiểm định bằng cách triển khai trong IUT một chức năng giúp cho phòng thí nghiệm kiểm định đồng bộ các dạng sóng (bằng cách cung cấp một tín hiệu kích hoạt báo hiệu thời điểm bắt đầu phép toán mật mã) và đánh giá chất lượng của các phép đo kênh kề. Nhà cung cấp nên cung cấp một chức năng tương ứng với từng biện pháp đối phó. Chức năng này cũng có thể hỗ trợ việc kiểm thử các phương pháp giảm nhiễu từ bên ngoài (lọc theo miền tần số, tính giá trị trung bình, v.v...). Chức năng này có thể đơn giản là việc xử lý/lưu trữ một biến công khai đã biết (không nhạy cảm) trong IUT (ví dụ, thành phần e của khóa công khai RSA). Phòng thí nghiệm kiểm định nên truy xuất giá trị đã biết này.

Nếu tỉ số tín hiệu trên nhiễu (SNR) của phần các phép đo kênh kề tương ứng với quá trình xử lý của giá trị đã biết này là đủ cao thì phòng thí nghiệm kiểm định có thể thực hiện các kiểm định.

Nếu phần của vết đo kênh kề tương ứng với quá trình xử lý giá trị đã biết này có tỷ số tín hiệu trên nhiễu (SNR) đủ cao Nếu không, phòng thí nghiệm kiểm định cần tìm ra một cách để cải tiến chất lượng của các phép đo của nó trước khi thực hiện các kiểm định.

Các điều kiện tiền xử lý trong phân tích vi sai được nêu trong Phụ lục A phải được [07.10] thỏa mãn.

Phòng thí nghiệm kiểm định khi đó phải [07.11] tính toán các giá trị trung gian của chức năng an toàn. Điều này có thể thực hiện được vì phòng thí nghiệm kiểm định thu thập các phép đo kênh kề sử dụng một tập hợp véc tơ kiểm thử đã được xác định trước. Các véc tơ kiểm thử này được phòng thí nghiệm kiểm định lựa chọn cẩn thận bằng các phương pháp như phương pháp đầu vào được lựa chọn (xem Phụ lục F) nhằm bộc lộ và cô lập các rò rỉ tiềm ẩn.

Bước cuối cùng bao gồm thực hiện các kiểm thử thống kê đối với việc rò rỉ trên các vết đo đã được căn chỉnh và/hoặc tiền xử lý. Phòng thí nghiệm kiểm định nên áp dụng một kiểm thử thống kê đơn giản (ví dụ: phép kiểm thử Welch) đối với nhiều bộ dữ liệu được xác định trước để phát hiện rò rỉ thông tin nhạy cảm qua kênh kề

Điều 8 và Điều 9 lần lượt mô tả các hướng dẫn đánh giá khả năng chống chịu đối với tấn công kênh kề của các hệ mật mã đối xứng và hệ mật mã phi đối xứng.

8 Phân tích kênh kề của các hệ mật khóa đối xứng

8.1 Tổng quan

Điều này tập trung vào phân tích kênh kề của các hệ mật khóa đối xứng. Khung công việc mô tả trên Hình 3 được sử dụng. Khả năng chống chịu các tấn công tính thời lượng, phân tích kênh kề đơn giản và phân tích kênh kề vi sai phải được đánh giá. [08.01].

8.2 Các tấn công tính thời gian

Đối với các hệ mật khóa đối xứng (phần mềm), mối đe dọa duy nhất được biết đến liên quan đến các tấn công định thời bộ nhớ đệm, cụ thể là các tấn công thời gian bộ nhớ đệm. [50] Chúng dựa trên các tính chất vi kiến trúc của CPU (ví dụ kiến trúc bộ nhớ đệm, bộ dự báo phân nhánh). Các tấn công bộ nhớ

đệm khai thác hành vi bộ nhớ đệm (tức là thống kê trúng/trượt bộ nhớ đệm) của các hệ thống mật mã. Kiến trúc bộ nhớ đệm làm rò rỉ thông tin về các mẫu truy cập bộ nhớ. Thời gian thực hiện là nguồn rò rỉ (trượt bộ nhớ đệm mất nhiều thời gian thực hiện hơn so với trúng bộ nhớ đệm). Các hệ thống mật mã có các mẫu truy cập bộ nhớ phụ thuộc. Một khi các mẫu truy cập được trích xuất thì phòng thí nghiệm kiểm định có thể khôi phục khóa bí mật.

Nếu IUT là một cài đặt phần mềm/phần sụn của các hệ mật khóa đối xứng và nếu IUT chứa bộ nhớ đệm thì phòng thí nghiệm kiểm định có thể kiểm thử IUT đối với các tấn công thời lượng theo khung công việc được mô tả trong Thư mục tài liệu tham khảo [50]. Trong trường hợp ngược lại, kết quả kiểm định là đạt.

8.3 SPA/SEMA

8.3.1 Các tấn công lên quá trình dẫn xuất khóa

Đối với các hệ mật khóa đối xứng, mối đe dọa duy nhất đã biết liên quan đến các tấn công SPA hoặc SEMA là quá trình dẫn xuất khóa (lược đồ khóa). Nếu phòng thí nghiệm kiểm định có thể xác định các trọng số Hamming của các giá trị trung gian xảy ra trong một hệ mật khóa đối xứng, khóa có thể bị suy ra. Ví dụ, đối với AES, [53] phòng thí nghiệm kiểm định có thể sử dụng các mối quan hệ phụ thuộc giữa các byte của các khóa vòng bên trong lược đồ khóa AES để làm giảm đi số lượng các giá trị khóa có thể. Sau đó khóa được xác định bằng cách sử dụng một cặp bản rõ - bản mã đã biết.

Nếu IUT chứa quá trình dẫn xuất khóa thì phòng thí nghiệm kiểm định có thể thử áp dụng một số phương pháp đã biết để trích xuất ra khóa (ví dụ: Thư mục tài liệu tham khảo [53] cho AES) hoặc bất kỳ phương pháp liên quan nào khác.

8.3.2 Các tấn công va chạm kênh kề

Các tấn công va chạm kênh kề cũng sử dụng thực tế là các phép đo kênh kề của IUT phụ thuộc vào dữ liệu đã được xử lý. Các chức năng an toàn mật mã bao gồm một số bước để sinh ra các giá trị trung gian từ giá trị đầu vào và khóa mật mã. Nếu các giá trị trung gian trở thành cùng giá trị đối với các giá trị đầu vào khác nhau thì tiêu thụ điện năng hoặc phát xạ điện từ thu được sẽ khá tương đồng. Kiểu “va chạm” này có thể được khai thác để làm giảm đi không gian khóa (xem Thư mục tài liệu tham khảo [38] đến [42]).

Phòng thí nghiệm kiểm định có thể đánh giá xem IUT có nhạy cảm đối với các tấn công va chạm kênh kề như vậy không bằng cách tuân theo một khung công việc đã biết (ví dụ Thư mục tài liệu tham khảo [39] cho AES) hoặc bất kỳ phương pháp có liên quan nào khác.

8.4 DPA/DEMA

Việc kiểm thử thống kê phải [08.02] được thực hiện theo những quy trình sau. Các vết kênh kề được chia thành hai tập con sao cho thông tin nhạy cảm đang được xử lý có sự khác biệt đáng kể giữa hai tập con.[20] Việc phân chia này là khả thi vì các thuật toán mật mã được thực hiện với các tham số và dữ liệu đã biết, và tất cả các trạng thái trung gian đều đã biết.

Nếu các vết kênh kề trong hai tập con khác biệt về mặt thống kê với độ tin cậy cao, thì xuất hiện rò rỉ thông tin và thiết bị không đạt (sự rò rỉ phải nằm trong ranh giới nhạy cảm, xem Phụ lục H). Ngược lại, sự rò rỉ thông tin hoặc là không xuất hiện hoặc là đã bị triệt tiêu.

Công cụ thống kê được sử dụng là kiểm thử t-Welch. Một giá trị dương hoặc giá trị âm lớn của của kiểm thử t thống kê giá trị T (được định nghĩa dưới đây) tại một thời điểm cho thấy một mức độ tin cậy cao rằng giả thuyết không (tức là giá trị trung bình của hai tập con bằng nhau) là không chính xác. Mức tin cậy là tùy ý trong khoảng 0 đến 1, nhưng thường được chọn gần 1, cho thấy độ tin cậy cao dựa trên các tiêu chí mong muốn, chẳng hạn như 0,99 (hoặc 99%). Mức tin cậy xác định giá trị ngưỡng C cho ngưỡng dương và ngưỡng âm (+C/-C) đối với T theo phân phối t. Ví dụ, mức tin cậy 99,99% tương ứng với C = 3,9 và 99,999% tương ứng với C = 4,5.

Để kiểm soát các trường hợp dương tính giả, các hiệu chỉnh bội là cần thiết. Trong tiêu chuẩn này, hiệu chỉnh Bonferroni được ưu tiên. Theo đó, mức ý nghĩa cho từng phép kiểm thử thu được bằng cách chia mức ý nghĩa tổng thể mong muốn α cho số lượng phép kiểm thử m, tức là $\alpha_{\text{per-test}} = \frac{\alpha}{m}$.

Đối với mỗi thuật toán, các hiệu chỉnh bội phải [08.03] được thực hiện, mỗi hiệu chỉnh nhắm vào một loại rò rỉ khác nhau. Hình 7 mô tả quy trình kiểm định thống kê chung.

Trước khi thực hiện kiểm thử thống kê, phòng thí nghiệm kiểm định phải [08.04] quy định các tham số như kích thước hiệu ứng được chuẩn hóa, tỷ lệ dương tính giả α, tỷ lệ âm tính giả β, v.v… Các giá trị ví dụ cho α và β có thể là α=0,05, α=0,00001, β=0,05, v.v. Người kiểm thử cũng phải [08.05] thực hiện các hiệu chỉnh bội để có được mức ý nghĩa cho mỗi phép kiểm thử. Sau đó, người kiểm thử phải [08.06] tính toán số lượng các vết $N = N_A + N_B$ cần thiết cho bài kiểm thử.

Các ký hiệu sau được sử dụng:

N_A, N_B là kích thước của các tập con A và B;

N là kích thước mẫu, bằng $N_A + N_B$;

μ_A là trung bình của tất cả các vết trong nhóm A;

μ_B là trung bình của tất cả các vết trong nhóm B;

σ_A là độ lệch chuẩn mẫu của tất cả các vết trong nhóm A;

σ_B là độ lệch chuẩn mẫu của tất cả các vết trong nhóm B;

T là $\frac{(\mu_A - \mu_B)}{\sqrt{\frac{\sigma_A^2}{N_A} + \frac{\sigma_B^2}{N_B}}}$;

α là mức ý nghĩa (hoặc dương tính giả);

β là âm tính giả;

d là kích thước hiệu ứng được chuẩn hóa.

Đối với trường hợp đơn giản của kiểm thử *t* với các kích thước mẫu bằng nhau, công thức cho kích thước mẫu cần thiết có thể được biểu thị theo kích thước hiệu ứng được chuẩn hóa, như trong Công thức (1):

$$N = 4 \cdot \frac{\left(Z_{\alpha/2} + Z_{\beta}\right)^2}{d^2} \quad (1)$$

Ngoài kiểm định t, có thể sử dụng NICV (Phương sai giữa các lớp được chuẩn hóa, hay còn gọi là hệ số xác định).[60][61] Các ưu điểm là:

a) nó có thể là đa bit;

b) nó có thể so sánh được giữa các triển khai, vì nó nằm trong khoảng từ 0 đến 1;

c) nó liên quan đến hệ số tương quan Pearson ρ theo công thức $0 \le \rho^2 \le \text{NICV} \le 1$;

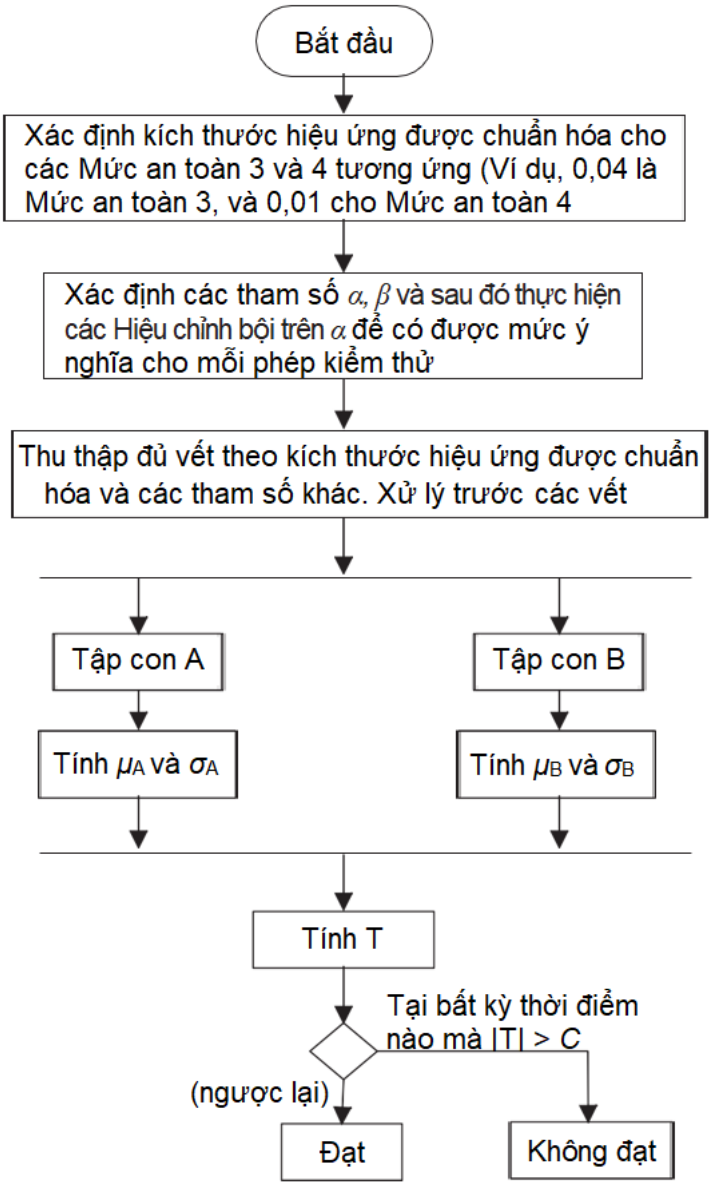
d) nó tổng quát hóa một cách tự nhiên cho rò rỉ bậc cao.

Hướng dẫn về việc lựa chọn các tham số α (alpha) và β (beta) như sau:

Giá trị của beta nên được đặt ở mức thấp, vì mục đích chính của phân tích kênh kề là để phát hiện một lỗ hổng (tiềm ẩn); một sự rò rỉ không nên bị bỏ sót bằng cách nới lỏng ràng buộc đối với beta.

Mặt khác, việc lựa chọn alpha linh hoạt hơn. Bằng cách thận trọng (alpha thấp), người kiểm thử cần ít phân tích các trường hợp dương tính giả hơn (mặc dù phải trả giá bằng việc thu thập nhiều vết hơn).

Ngược lại, với alpha lớn hơn, cần thực hiện một số kiểm tra thủ công (để xác minh liệu một rò rỉ tiềm năng có thật hay chỉ là một hiện tượng giả), nhưng cần ít vết hơn.



Hình 7 — Quy trình kiểm thử thống kê tổng quát

9 ASCA trên mật mã phi đối xứng

9.1 Tổng quan

Điều này tập trung vào phân tích kênh kề đối với các hệ mật khóa phi đối xứng.

Các thuật toán phi đối xứng có thể thực hiện ba nhiệm vụ khác nhau: chữ ký số, mã hóa và thỏa thuận khóa. Như được chỉ ra trên Bảng C.1, các thuật toán phi đối xứng được sử dụng nhiều nhất là RSA và các hệ mật đường cong elliptic (ECC).

Đối với chữ ký số, mã hóa hay thỏa thuận khóa, hoạt động chủ yếu là tính toán các:

a) Phép lũy thừa mô-đun trong trường hợp của RSA; đó là phép tính m^d mod n đối với số nguyên m bất kỳ, khóa bí mật d và một số nguyên n, và

b) Phép nhân vô hướng đường cong elliptic trong trường hợp của ECC; tức là tính $d \cdot p$ đối với một điểm trên đường cong elliptic cho trước và khóa bí mật d.

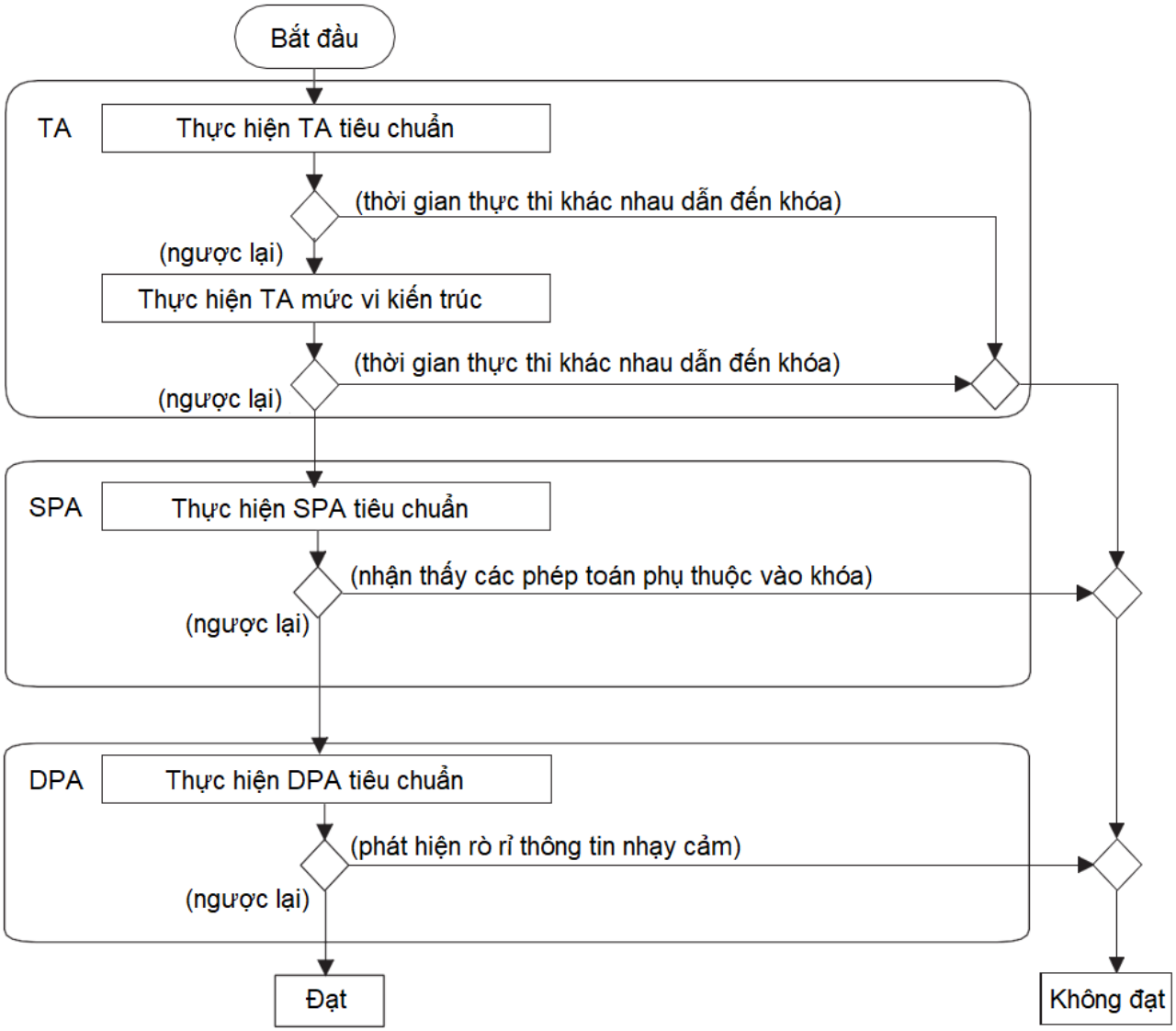
Có nhiều khả năng để tính lũy thừa mô-đun và phép nhân vô hướng đường cong elliptic. Các thuật toán lũy thừa trong thực tế phụ thuộc vào cách biểu diễn các số nguyên và các phép toán số học mô-đun.

CHÚ THÍCH Các triển khai thuật toán lũy thừa thực tế cũng phụ thuộc vào hiệu suất, độ phức tạp, tính gọn nhẹ và mức an toàn được hướng đến, và đó là kết quả của sự đánh đổi cần thiết.

Khung công việc mô tả trong Hình 3 được sử dụng. Khả năng kháng các tấn công tính thời gian, phân tích kênh kề đơn giản và phân tích kênh kề vi sai phải [09.01] được đánh giá.

Về ECC, một khảo sát toàn diện của các tấn công kênh kề sẵn có trong Thư mục tài liệu tham khảo [59].

9.2 Khung công việc kiểm thử kháng kênh kề chi tiết



Hình 8 — Khung công việc kiểm thử khả năng kháng của kênh kề dành cho các hệ mật khóa phi đối xứng

So với các hệ mật khóa đối xứng, có nhiều phương thức hơn để tấn công các hệ mật khóa phi đối xứng do sự đa dạng về cấu trúc và số học nền tảng. Hình 8 mô tả khung công việc kiểm thử khả năng kháng của kênh kề dành cho các hệ mật khóa phi đối xứng. Các kiểm thử an toàn nhằm mục đích kiểm tra tính an toàn chống lại các tấn công thông thường như TA, SPA, DPA. Các tấn công tinh vi hơn như Markov SPA, địa chỉ-bit DPA và tấn công nhân đôi được nêu trong Phụ lục D. Cơ quan phê duyệt có thẩm quyền có thể chọn thực hiện các bài kiểm thử an toàn chống lại các tấn công này hay không. Mỗi dạng tấn công nêu trên là tấn công chuyên biệt nhắm vào các hệ mật mã phi đối xứng.

9.3 Các tấn công thời lượng

9.3.1 Tổng quan

Theo quy định tại Hình 8, phòng thí nghiệm kiểm định nên đánh giá độ an toàn của các hệ mật khóa phi đối xứng chống lại phương pháp phân tích thời lượng tiêu chuẩn và phân tích thời lượng vi kiến trúc.

9.3.2 Phân tích thời lượng tiêu chuẩn

Do các hệ mật khóa phi đối xứng tính toán các phép toán phụ thuộc vào khóa và có thể sử dụng các phép toán toán học cơ bản với các tính toán biến thiên thời gian (ví dụ: phép nhân mô-đun), chúng có thể bị tổn thương bởi tấn công thời lượng. Phần sau đây diễn tả chi tiết phương pháp được mô tả trong Thư mục tài liệu tham khảo [2] để tấn công RSA với tấn công thời lượng.

Trong Thư mục tài liệu tham khảo [2] các tấn công được thực hiện trên một IUT mà cài đặt:

- Phép nhân mô-đun (phương pháp Montgomery) chỉ rõ các biến thiên thời gian tính toán;

- Chương trình lũy thừa “bình phương và nhân” theo tiêu chuẩn cho phép các biến thiên này có thể bị khai thác.

Kết quả của mỗi phép nhân nằm trong khoảng [0, 2N-1], trong đó N là giá trị tuyệt đối.

Đối với chương trình lũy thừa, IUT tính một bước nhân khi bit của khóa bí mật hiện tại *d_I* bằng 1. Nếu kết quả của bước nhân lớn hơn *N*, một phép trừ cho *N* sẽ được tính.

Trong Thư mục tài liệu tham khảo [2], phòng thí nghiệm kiểm định phải [09.02] có tri thức về các bit khóa bí mật *d_k*-1 đến *d_k-i*+1 khi tấn công *d_k*. Biết được đoạn thông điệp, giá trị trung gian sau bước bình phương (được gọi là *s*) tại vòng lặp *k-i* được tính. Có thể xác định được liệu phép trừ trong bước nhân có cần thiết hay không.

Cuộc tấn công dựa trên một oracle. Oracle là một bản sao của IUT, trong đó người kiểm thử có thể thay đổi CSP. Phòng thí nghiệm kiểm định phải [09.03]:

a) ký số với cùng (*d, N*) đối với nhiều thông điệp ngẫu nhiên;

b) giả định rằng *d_k-i* = 1;

c) xây dựng hai tập thông điệp phụ thuộc vào việc là phép trừ có xảy ra (tập *A*) hay không (tập *B*) trong quá trình nhân.

Trong trường hợp:

- *d_k-i* = 0, các thời gian toàn cục đối với các tập *A* và *B* là không phân biệt được về mặt thống kê (phân tách là dựa trên một phép nhân mà nó không xảy ra);

- *d_k-i* = 1, các thời gian toàn cục đối với các tập *A* và *B* chứng tỏ một sự khác biệt thống kê liên quan đến phép trừ không bắt buộc (phép nhân có xảy ra).

Các phép đo thời gian thừa nhận hoặc bác bỏ oracle. Phòng thí nghiệm kiểm định phải [09.04] tính giá trị trung bình của khoảng thời gian toàn cục đối với mỗi tập con <*A*> (tương ứng <*B*>) là khoảng thời gian toàn cục trung bình đối với các thông điệp A(B). Tiêu chí oracle như sau:

- Nếu <*A*> - <*B*>> 0 thì oracle đã đúng (*d_k-i* = 1);

- Nếu <*A*> - <*B*> = 0 thì oracle đã sai (*d*[*k-i*] = 0).

Nếu phòng thí nghiệm kiểm định cuối cùng cũng khôi phục được toàn bộ khóa bằng phương pháp này (từ Thư mục tài liệu tham khảo [2]) hoặc bằng bất kỳ phương pháp nào khác có liên quan, kết quả kiểm thử là không đạt. Ngược lại, kết quả kiểm thử là đạt.

CHÚ THÍCH RSA PKCS#1 v2.1, DSA và ECDSA không dễ bị tấn công trước các phương pháp phân tích thời lượng chuẩn vì:

- phần đệm (padding) được sử dụng cho RSA PKCS#1 v2.1 mang tính xác suất và kẻ tấn công không thể dự đoán được các giá trị trung gian;

- DSA và ECDSA lần lượt sử dụng một số mũ phù du và vô hướng, do đó kẻ tấn công không thể nhắm mục tiêu vào một bit cụ thể.

9.3.3 Phân tích thời lượng vi kiến trúc

Các hệ mật khóa phi đối xứng (dạng phần mềm) cũng bị tổn thương đối với các tấn công vi kiến trúc. Kênh kề này phát sinh bởi khả năng dự đoán nhánh có chung trên tất cả các CPU hiện đại. Hình phạt trả giá (các chu kỳ xung nhịp tăng thêm) cho một nhánh bị dự đoán sai có thể được sử dụng để phân tích mật mã của các nguyên thủy mật mã có sử dụng một luồng chương trình phụ thuộc vào dữ liệu. Thế nên các hệ mật khóa phi đối xứng (dạng phần mềm) có thể dễ bị tấn công bởi cái gọi là “Phân tích dự đoán nhánh” [52]. Phòng thí nghiệm kiểm định cần kiểm thử IUT chống lại các tấn công thời lượng (vi kiến trúc) theo khung công việc được mô tả trong Thư mục tài liệu tham khảo [52], hoặc bất kỳ phương pháp có liên quan nào khác.

9.4 SPA/SEMA

Đối chiếu với Hình 8, phòng thí nghiệm kiểm định phải [09.05] đánh giá mức độ an toàn của các hệ mật khóa phi đối xứng chống lại SPA tiêu chuẩn.

Do các hệ mật khóa phi đối xứng thực hiện một dãy các phép toán phụ thuộc vào khóa, bản chất dễ bị tổn thương trước SPA/SEMA “tiêu chuẩn”

Đối với mọi các phép đo kênh kề, nếu tương quan chéo dẫn đến một dãy phép toán bình thường, chẳng hạn, với một RSA (Ở đây “M” biểu diễn một phép toán nhân và “S” một phép toán bình phương):

- “MMMMMM…”
- “MSMSMS…”

thì kết quả kiểm thử là đạt.

CHÚ THÍCH 1 Thay vì các khóa và đầu vào ngẫu nhiên, phòng thí nghiệm kiểm định có thể chọn các khóa và đầu vào cụ thể:

- Khóa: ngẫu nhiên, 0x80…01, 0xff…ff, 0xaa…aa (dạng nhị phân: 1010 1010 …).
- Đầu vào: ngẫu nhiên, trọng số Hamming thấp, trọng số Hamming cao.

Trong một hệ mật phi đối xứng, các bit của số mũ/vô hướng có ảnh hưởng lớn đến kiểu phép toán hay dữ liệu được thao tác. Các khóa cụ thể có thể giúp phân biệt được sự khác nhau phụ thuộc vào bit hiện tại, ví dụ, phân biệt bình phương với nhân (nhân đôi từ cộng điểm đối với ECC), phân biệt dữ liệu di chuyển cụ thể cho luôn luôn bình phương và nhân (luôn nhân đôi và cộng điểm đối với ECC), sử dụng không đúng các hướng dẫn nhảy phụ thuộc vào bit hiện tại, v.v…

CHÚ THÍCH 2: Một IUT sử dụng một số biện pháp đối phó với SPA/SEMA như “thuật toán nhân đôi và cộng nguyên tử” có thể rò rỉ trọng số Hamming của khóa bí mật. Trong một số điều kiện thì nó là đủ để làm rò rỉ toàn bộ khóa [57]. Phòng thí nghiệm kiểm định khi đó có thể tùy chọn tuân theo phương pháp luận được đề xuất trong Thư mục tài liệu tham khảo [57].

9.5 DPA/DEMA

Đối chiếu với Hình 8, phòng thí nghiệm kiểm định phải [09.06] đánh giá độ an toàn của các hệ mật khóa phi đối xứng chống lại DPA tiêu chuẩn.

Trong trường hợp tổng quát, phép kiểm thử kháng DPA/DEMA đối với các hệ mật khóa phi đối xứng là tương tự với các hệ mật khóa đối xứng ngoại trừ việc tồn tại nhiều các mô hình rò rỉ hơn.

DSA và ECDSA có thể bị tổn thương bởi một DPA/DEMA đặc thù khi khóa bí mật được nhân với một số đã biết.

Khi khóa bí mật d được sử dụng để nhân với r, trong trường hợp này, kẻ tấn công có thể thực hiện DPA/DEMA trong quá trình tính toán $d \cdot r$.

Một phép nhân thường được thực hiện từng từ một. Mô hình rò rỉ có thể là trọng số Hamming của từ đầu tiên của *d* (*d*[0]) nhân với từ đầu tiên của *r* (*r*[0]), tức là HW(*d*[0]· *r*[0]).

Như mã hóa đối xứng, thực hiện kiểm thử t với giả thuyết đúng và giả thuyết sai ngẫu nhiên. Các kiểm thử có thể được thực hiện với các kích thước kiến trúc khác nhau: 8, 16, 32 và 64.

Không cần thiết phải thực hiện phép kiểm thử này với tất cả các từ của *d*. Có thể rút ra kết luận rằng các từ khác cũng được phục hồi giống như vậy trong trường hợp thành công và các từ khác cũng được bảo vệ trong trường hợp thất bại.

PHỤ LỤC A
(Quy định)
Các thước đo đạt/không đạt của việc kiểm thử đối với các biện pháp chống tấn công không xâm lấn

A.1 Giới thiệu

Phụ lục này quy định các thước đo kiểm thử và tiêu chí đạt/không đạt đối với từng tổ hợp giữa phương pháp tấn công và chức năng an toàn tương ứng được liệt kê trong Bảng C.1.

Trong phụ lục này, các thước đo kiểm thử được cung cấp theo thời gian thu thập dữ liệu, thời gian phân tích và lượng dữ liệu. Việc lựa chọn các giới hạn đối với thời gian thu thập dữ liệu, thời gian phân tích và lượng dữ liệu cần xem xét đến loại thiết bị được kiểm thử. Các tập dữ liệu được sử dụng khi kiểm thử một thiết bị đơn chip đơn giản có khả năng sẽ nhỏ hơn các tập dữ liệu cần thiết để thực hiện phân tích có ý nghĩa đối với các thiết bị phức tạp, chẳng hạn như hệ thống trên chip (System-On-Chip - SoC) phức tạp. Các giới hạn được quy định trong phụ lục này phù hợp hơn đối với các thiết bị đơn chip đơn giản.

Tham chiếu hiệu năng cho quá trình phân tích tính toán được quy định thông qua cấu hình của máy tính tham chiếu do cơ quan phê duyệt chỉ định, nhằm bảo đảm tiêu chí công bằng trong việc đánh giá thời gian phân tích.

Các độ đo kiểm thử và tiêu chí đạt/không đạt do cơ quan phê duyệt ban hành có thể thay thế toàn bộ nội dung của phụ lục này.

A.2 Mức an toàn 3

A.2.1 Giới hạn thời gian

Thời gian lấy mẫu tối đa cần là không nhiều hơn 6 giờ đối với mỗi kiểm định sơ cấp đối với mức an toàn 3. Khi giới hạn này đạt đến thì phép đo sẽ được kết thúc thậm chí cả khi số các đo đạc không đáp ứng tối đa được chỉ định. Dãy tổng thể thời gian nhận được cần là không nhiều hơn 72 giờ.

A.2.2 SPA và SEMA

Để hoàn thành bài kiểm thử SPA hoặc SEMA ở mức an toàn 3, bộ dùng để kiểm thử được quy định phải thu thập:

— 11 dạng sóng sử dụng các mẫu dữ liệu đầu vào, mỗi dạng sóng bao gồm một CSP và văn bản rõ được cung cấp bởi bộ kiểm thử (1 mẫu dữ liệu đầu vào được xác định trước được sử dụng cho đầu vào cùng một cặp dữ liệu; 1 cặp được xác định trước và 4 cặp dữ liệu ngẫu nhiên được sử dụng cho các đầu vào cặp dữ liệu khác nhau).

Để phân tích tương ứng với một bit CSP, độ phân giải của mỗi dạng sóng là 100 điểm hoặc lớn hơn

Mức độ tương đồng của các vết đo thu được trong một phép kiểm thử lõi được đánh giá bằng cả phương pháp quan sát trực quan và phép kiểm thử thống kê. Để đạt yêu cầu đối với phép kiểm thử lõi, kết quả của cả hai phương pháp đánh giá phải đạt. Trong trường hợp ngược lại, phép kiểm thử được xác định là không đạt.

A.2.3 DPA và DEMA

Để hoàn thành bài kiểm thử DPA hoặc DEMA ở mức an toàn 3, bộ kiểm thử được cung cấp phải thu thập:

- Các dạng song N của một kiểu của rò rỉ kênh kề từ các mẫu dữ liệu đầu vào khác nhau đối với mỗi CSP trong một tập các CSP được cung cấp. Trong đó N được tính theo Công thức (1), với d = 0,04.

Nếu mức rò rỉ được tính toán được xác định là đáng kể so với mức rò rỉ được định nghĩa trong tài liệu, thì kiểm định không đạt. Ngược lại Kiểm định đạt.

A.2.4 Phân tích thời gian

Để hoàn thành kiểm thử phân tích thời gian ở mức an toàn 3, bộ kiểm thử được cung cấp sẽ thu thập:

- 1 000 phép đo thời gian cho CSP ngẫu nhiên và một bản rõ xác định trước cho khối đo đạc đầu tiên, và

- 1 000 phép đo thời gian cho CSP được xác định trước và bản rõ ngẫu nhiên cho khối đo đạc thứ hai.

A.2.5 Các điều kiện tiền xử lý trong phân tích lượng vi sai

Để hoàn thành phân tích phát xạ hay điện năng vi sai tại mức an toàn 3, các yếu tố sau có thể áp dụng:

- Một tín hiệu đồng bộ hóa có sẵn báo hiệu tín hiệu bắt đầu của hoạt động mật mã.

- Làm giảm nhiễu sẽ được thực hiện [A.01] bởi người kiểm định tính giá trị trung bình của các vết khác nhau (10 hoạt động mật mã cần được tiến hành đối với cùng một tập các đầu vào để thu được chỉ một vết).

A.2.6 Điều kiện đạt / không đạt

a) Nếu các vết thu được bằng cách sử dụng tín hiệu đánh dấu không được sắp xếp từ những lần thực hiện khác nhau các bài kiểm định sẽ đạt và kiểm thử thống kê cho thuật toán mật mã sẽ không được thực hiện [A.02].

b) Nếu các vết thu được bằng cách sử dụng tín hiệu đánh dấu được sắp xếp thì giá trị trung bình sẽ được tính toán và kết quả sẽ là kết quả thu được từ kiểm định thống kê áp dụng cho thuật toán mật mã và các vết.

A.3 Mức an toàn 4

A.3.1 Giới hạn thời gian

Thời gian lấy mẫu tối đa cần là không nhiều hơn 24 giờ đối với mỗi kiểm định sơ cấp đối với mức an toàn 4. Khi giới hạn này đạt đến thì phép đo sẽ được kết thúc thậm chí cả khi số các đo đạc không đáp ứng tối đa được chỉ định. Dãy tổng thể thời gian nhận được cần là không nhiều hơn 288 giờ

A.3.2 SPA và SEMA

Để hoàn thành bài kiểm thử SPA hoặc SEMA ở mức an toàn 4, bộ kiểm thử được cung cấp phải thu thập:

- 21 dạng sóng sử dụng các mẫu dữ liệu đầu vào, mỗi dạng sóng bao gồm một CSP và bản rõ được cung cấp bởi bộ kiểm thử (1 mẫu dữ liệu đầu vào được xác định trước được sử dụng cho đầu vào cùng một cặp dữ liệu; 5 cặp được xác định trước và 15 cặp dữ liệu ngẫu nhiên được sử dụng cho các đầu vào cặp dữ liệu khác nhau).

Đối với phân tích từng bit CSP, độ phân giải của mỗi dạng sóng là 1 000 điểm trở lên.

Tính tương tự của các vết tổng hợp đối với kiểm định lõi sẽ được kiểm tra cả trực quan và với một kiểm định thống kê. Để thỏa mãn kiểm định lõi, cả hai các kết quả kiểm định cần là đạt. Kiểm định sẽ không đạt nếu ngược lại.

A.3.3 DPA và DEMA

Để hoàn thành bài kiểm thử DPA hoặc DEMA ở mức an toàn 4, bộ kiểm thử được cung cấp phải thu thập:

- N dạng sóng của một một kiểu của rò rỉ kênh kề từ các mẫu dữ liệu đầu vào khác nhau đối với mỗi CSP trong một tập các CSP được cung cấp. Trong đó N được tính theo Công thức (1), với d = 0,01.

Nếu mức rò rỉ được tính toán được xác định là đáng kể so với mức rò rỉ được định nghĩa trong tài liệu, thì kiểm định sẽ không đạt. Ngược lại Kiểm định đạt.

A.3.4 Phân tích thời gian

Để hoàn thành kiểm định phân tích tính thời gian tại mức an toàn 4, bộ kiểm định được cung cấp cần thu thập:

- 10.000 phép đo thời gian cho các CSP ngẫu nhiên và một bản rõ xác định trước đối với khối đo đạc đầu tiên, và

- 10.000 phép đo thời gian cho CSP được xác định trước và bản rõ ngẫu nhiên đối với khối đo đạc thứ hai.

A.3.5 Các điều kiện tiền xử lý trong phân tích lượng vi sai

Để hoàn thành phân tích phát xạ hay điện năng vi sai tại mức an toàn 4, ngoài các các nhân tố được chỉ định đối với mức an toàn 3, có thể áp dụng những Mục sau:

- Làm giảm nhiễu sẽ được thực hiện bởi người kiểm định bằng cách áp dụng một phân tích phổ và lọc các vết theo tần số (bộ lọc băng thông phù hợp với tần số hoạt động của mô-đun).

- Căn chỉnh động và tĩnh sẽ được thực hiện để loại bỏ các sắp xếp sai xuất phát từ bất kỳ biện pháp đối phó trực tiếp nào hoặc từ các lỗi cấu hình phép đo khi bắt đầu thu thập mức tiêu thụ điện năng (hoặc phát xạ).

A.3.6 Điều kiện đạt / không đạt

Áp dụng bộ lọc theo tần số.

a) Nếu các vết đưa ra kết luận về độ trễ tính thời gian ngẫu nhiên hay biến thiên tần số xung sao cho chúng không thể được sắp xếp đầy đủ với một căn chỉnh tĩnh thì kiểm định đạt và kiểm định thống kê đối với thuật toán mật mã sẽ không được thực hiện.

b) Nếu căn chỉnh tĩnh thành công thì sẽ nhận được kết quả từ việc kiểm định thống kê được áp dụng cho các thuật toán mật mã, các vết được lọc và được sắp xếp.

PHỤ LỤC B
(Tham khảo)
Yêu cầu đối với thiết bị đo lường

B.1 Tổng quan

Phụ lục này cung cấp các yêu cầu và thông tin chung về các đặc tính thu nhận tín hiệu.[20] Một số yêu cầu này không cần thiết để đáp ứng trong một số tình huống, miễn là tỷ lệ tín hiệu trên nhiễu đủ (xem 7.3.6). Ví dụ, có thể thực hiện các tấn công hiệu quả ở tốc độ lấy mẫu thấp hơn nhiều khi đồng hồ mẫu được đồng bộ hóa,[63] hoặc khi rò rỉ ở tần số thấp hơn nhiều phổ biến với các thuật toán mã khóa công khai.[64]

B.2 Tốc độ

a) Độ rộng băng thông tối thiểu của 50% tốc độ xung nhịp thiết bị đối với các cài đặt phần mềm và ít nhất 80% tốc độ xung nhịp đối với các cài đặt phần cứng.

b) [B.02] sẽ có khả năng thu thập mẫu tại 5 × băng thông.

B.3 Độ phân giải

a) Phải có [B.03] độ phân giải lấy mẫu tối thiểu 8 bit.

B.4 Khả năng

a) Phải có đủ bộ nhớ [B.04] để thu toàn bộ tín hiệu cần thiết cho kiểm thử và phân tích.

B.5 Đầu đo

Đầu đo là cần thiết để đo các dòng IUT.

Nếu kênh kề được sử dụng là tiêu thụ điện năng của IUT thì điện trở cần được đặt giữa dòng VCC cung cấp IUT và IUT. Phòng thí nghiệm kiểm định cần [B.06] chọn điện trở có giá trị cao nhất cho phép IUT hoạt động.

Nếu kênh kề được sử dụng là phát xạ điện từ của IUT thì khảo nghiệm từ trường gần cần được sử dụng [B.07], miễn là băng thông của phép khảo nghiệm ít nhất là băng thông của tốc độ xung IUT.

PHỤ LỤC C
(Tham khảo)
Các hàm an toàn kết hợp

Trong tấn công mục tiêu, các phương pháp tấn công không xâm lấn được đặc tả trong Điều 6 kết hợp với các chức năng an toàn cụ thể sử dụng các CSP bị mục tiêu tấn công. Các chức năng an toàn được liệt kê trong TCVN 11295:2016 (ISO/IEC 19790:2012), Phụ lục C, D và E.

Các kết hợp được chỉ ra trong Bảng C.1. Các tấn công không xâm lấn khác và các kết hợp khác giữa các phương pháp tấn công và các chức năng an toàn có thể tồn tại nhưng cách chống lại chúng chưa được đề cập trong tiêu chuẩn này.

Mục này không loại trừ việc sử dụng các tấn công không xâm lấn được cơ quan phê duyệt phê duyệt.

Danh sách các tấn công không xâm lấn và các kết hợp khác từ cơ quan phê duyệt có thể thay thế toàn bộ phụ lục này.

Hàm an toàn		**Các phương pháp tấn công không xâm lấn**		
		SPA/SEMA	**DPA / DEMA**	**TA**
Khóa đối xứng	AES	A[16]	A [16]	A[50]
	Triple-DES	A[24]	A[15]	A[23]
	Mã dòng	A[63]	A[63]	A[63]
Khóa phi đối xứng	RSA nguyên thủy (Bọc khóa)	A[15]	A[15]	A[1]
	RSA PKCS # 1 v1.5	A15]	A[15]	A[1]
	RSA PKCS # 1 v 2.1	A[15]	NKR	NKR
	DSA	A[59]	A[59]	A[59]
	ECDSA	A[59]	A[59]	A[59]
Các cơ chế băm	SHA	A[16]	A[65]	NKR
RNG và RBG	Tất định	A[16]	NKR	NKR
	Bất định	A[16]	NKR	NKR
Cơ chế xác thực dữ liệu	HMAC	A[16]	A[65]	NKR
Sinh khóa	Mật mã khóa đối xứng	A[15]	NKR	NKR
	RSA	A[59]	NKR	A[1]
	ECDSA	A[59]	NKR	A[1]
Dẫn xuất khóa từ khóa khác		NKR	NKR	A[66]
Dẫn xuất khóa từ mật khẩu		NKR	NKR	A[66]
Thiết lập khóa	DLC	A[59]	NKR	NKR

	IFC	A[59]	NKR	NKR
Các cơ chế xác thực hoạt động	Mã PIN / Mật khẩu	A[16]	A[65]	NKR
	Khóa	NKR	NKR	NKR
	Sinh trắc học	NKR	NKR	NKR

Viết tắt

A Áp dụng được

NKR Không có tài liệu tham khảo

CHÚ THÍCH 1 Áp dụng được có nghĩa là các chức năng an toàn là nhạy cảm với các đang tấn công này trong tài liệu đã phát hành.

CHÚ THÍCH 2 Không có tài liệu tham khảo có nghĩa là các chức năng an toàn không được biết là dễ bị nhạy cảm với các dạng tấn công này trong tài liệu công khai, không có nghĩa là các tấn công không áp dụng được.

CHÚ THÍCH 3 Một cài đặt HMAC có thể bị tổn hại bằng áp dụng DPA/DEMA, tuy nhiên, mã khối dựa trên MAC sẽ được bao hàm bởi AES và/hoặc DES bội ba.

CHÚ THÍCH 4 RSA PKCS # 1 v1.5 có thể bị xâm phạm bằng cách áp dụng DPA / DEMA có thể bị tổn hại bằng áp dụng DPA/DEMA bởi vì đệm thông báo được sử dụng là tất định.

CHÚ THÍCH 5 Các tấn công thời gian trên RSA PKCS # 1 v2.1 1 là không thực hành được bởi vì đệm thông báo được sử dụng là bất định. RSA PKCS#1 v2.1 không thể bị tổn hại bằng áp dụng DPA/DEMA bởi vì đệm thông báo được sử dụng là xác suất (các số ngẫu nhiên khác nhau được sử dụng cho mỗi chữ ký mới của thông báo).

CHÚ THÍCH 6 Có hai phép toán trong DSA (tương ứng là ECDSA) liên quan đến khóa bí mật hay khóa (bí mật) phù du:

- Phép lũy thừa mô-đun (nhân vô hướng) của một giá trị bí mật với một tham số đã biết. Phép toán này bị tổn thương đối với phân tích kênh kề đơn giản và các tấn công lượng sai nằm ngang.

- Phép nhân mô-đun của một giá trị đã biết và khóa bí mật. Nếu phép nhân được cài đặt theo cách mà số nhân là khóa bí mật và phép nhân được thực hiện với một biến thể của thuật toán nhị phân thì cài đặt này là về mặt nguyên tắc bị tổn thương đối với phân tích kênh kề.

CHÚ THÍCH 7 SHA có thể được sử dụng đối với băm mật khẩu, ví dụ: trong hàm dẫn xuất khóa dựa trên mật khẩu, vì thế trong trường hợp này một SHA không được bảo vệ chống lại SPA/SEMA hay DPA/DEMA cũng có thể dẫn đến mật khẩu.

CHÚ THÍCH 8 Các định nghĩa SPA/SEMA, DPA/DEMA và TA trong phụ lục này tổng quát hơn so với các định nghĩa trong Điều 6. Đặc biệt, DPA/DEMA trong phụ lục này bao gồm các EMA và PA nâng cao trong Hình 1.

PHỤ LỤC D
(Tham khảo)
Các tấn công khả thi

D.1 Tổng quan

Phụ lục này liệt kê các tấn công không xâm lấn và các kênh kề mà các phép đo kiểm định đạt/không đạt còn chưa được định nghĩa

D.2 Tấn công mẫu

Tấn công mẫu sử dụng thực tế là tiêu thụ điện năng hay phát xạ điện từ của IUT phụ thuộc vào dữ liệu được xử lý. Hành vi này được đặc trưng bởi cái gọi là “mẫu” và dữ liệu được xử lý kể cả IUT nếu có, có thể được nhận biết bằng cách so sánh khớp với mẫu (xem Thư mục tài liệu tham khảo [35-37]).

Một khi mẫu được xây dựng thì tấn công này sẽ là tấn công mạnh nhất ít nhất là về mặt lý thuyết. Tuy nhiên, để xây dựng mẫu đối khi các mẫu mở được cần đến cho phép những người kiểm định đưa vào hàng loạt các giá trị khác nhau. Cũng được biết rằng trong đó còn có biến thiên nào đó trong các mẫu tổng hợp phụ thuộc vào hoạt phiên của IUT. Do đó, tính ứng dụng được và các phép đo kiểm định đạt/không đạt không được định nghĩa trong tài liệu này.

D.3 Tấn công va chạm kênh kề

Tấn công va chạm kênh kề cũng sử dụng thực tế là tiêu thụ điện năng hay phát xạ điện từ của IUT phụ thuộc vào dữ liệu được xử lý. Các chức năng an toàn mật mã sẽ bao gồm một số bước để sinh ra các giá trị trung gian từ giá trị đầu vào và khóa mật mã. Nếu các giá trị trung gian trở thành như nhau về giá trị đối với các giá trị đầu vào khác nhau thì tiêu thụ điện năng hay phát xạ điện từ tổng hợp có thể là hoàn toàn tương tự. Kiểu “va chạm” này có thể được khai thác để làm suy giảm không gian khóa (xem Thư mục tài liệu tham khảo [38-42]).

D.4 Các tấn công tinh vi vào mật mã phi đối xứng

D.4.1 Tấn công nhân đôi

Trong một số trường hợp, phòng thí nghiệm kiểm thử có thể gửi các vectơ đầu vào cụ thể đến IUT cho phép truy xuất khóa bằng SPA/ SEMA bằng cách sử dụng một số lượng nhỏ dạng sóng. Đó là nguyên tắc " tấn công nhân đôi".

Tấn công nhân đôi dựa trên thực tế là các giá trị trung gian tương tự được thao tác khi làm việc với điểm P và điểm kép của nó (được ký hiệu $^{[2]}$P), như được thể hiện trong Thư mục tài liệu tham khảo [54]. Nếu phòng thí nghiệm kiểm thử có thể xác định các hoạt động nhân đôi điểm với dữ liệu giống hệt nhau trong hai phép đo kênh kề, nó có thể suy ra các giá trị bit khóa. Trong điều kiện lý tưởng, tấn công này chỉ cần hai phép đo kênh kề. Nếu phòng thí nghiệm lấy chìa khóa, kết quả kiểm thử đã không thành công.

CHÚ THÍCH: ECDSA không dễ bị tấn công nhân đôi vì điểm cơ sở đã được cố định.

D.4.2 Markov SPA / SEMA

Một số biện pháp đối phó SPA/SEMA dẫn đến chuỗi các hoạt động có thể mang lại đủ thông tin để lấy khóa. "Markov SPA/SEMA" sau đó có thể cho phép xóa sự phụ thuộc giữa trình tự và khóa.

Nếu tương quan chéo dẫn đến các dãy phép toán không bình thường và nếu liên kết giữa các thao tác không bình thường này và khóa không rõ ràng trong quan sát đầu tiên thì phòng thí nghiệm kiểm định có thể áp dụng các tấn công cụ thể để cuối cùng khôi phục được khóa. Phòng thí nghiệm kiểm định có thể ví dụ đối mặt với một phép lũy thừa mô-đun được ngẫu nhiên hóa có sai sót (tương ứng là phép nhân vô hướng) và khi đó nó có thể sử dụng những điểm yếu đã biết để cuối cùng khôi phục được khóa bằng cách xét thuật toán lũy thừa (hay phép nhân vô hướng) như là một quá trình Markov trong Thư mục tài liệu tham khảo [51] về ECC hoạt động theo bốn bước:

- Giai đoạn tính trước: Tìm mô hình Markov. Phòng thí nghiệm kiểm định cần phải tính các xác suất điều kiện đối với các dãy bit và các dãy các phép toán được thực hiện.

- Giai đoạn thu thập dữ liệu: Phòng thí nghiệm kiểm định cần phải suy ra dãy các phép toán bình phương và nhân (nhân đôi và cộng điểm).

- Giai đoạn phân tích dữ liệu: Phòng thí nghiệm kiểm định cần phân tách dãy thành một số các dãy con.

- Giai đoạn kiểm thử khóa: Phòng thí nghiệm kiểm định cần phải kiểm tra tất cả các khóa có thể bằng bản mã đã biết.

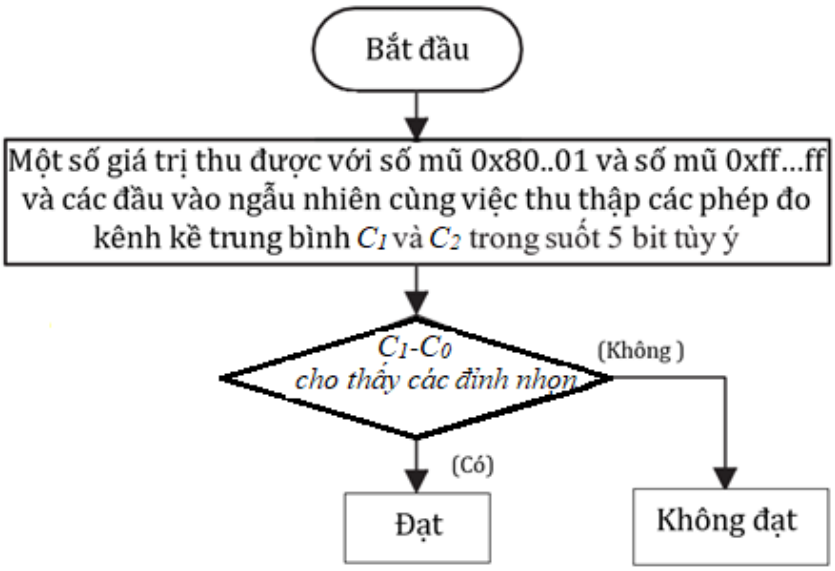
Phòng thí nghiệm kiểm định cần kiểm định IUT chống lại SPA/SEMA (đặc biệt khi quan hệ giữa các bit của khóa và các phép toán là khó tìm) tuân theo khung công việc được mô tả trong Thư mục tài liệu tham khảo [51], hoặc một phương pháp liên quan khác bất kỳ. Nếu nó khôi phục được khóa thì kết quả kiểm định là Thất bại.

D.4.3 DPA/DEMA địa chỉ-bit

DPA/DEMA địa chỉ-bit [14] khai thác thực tế là các địa chỉ bên trong của các vị trí thanh ghi hay bộ nhớ là kiểu khác của dữ liệu được xử lý bởi CPU. Từ đó các phép đo kênh kề của hai đoạn của một thuật toán mà trong đó cùng một câu lệnh truy cập các địa chỉ khác nhau sẽ là ít tương quan hơn nếu lệnh đó truy cập đến cùng một địa chỉ. Tấn công là dễ dàng hơn nếu số các vị trí thanh ghi hay bộ nhớ được truy cập trong quá trình thuật toán phụ thuộc vào các bit của khóa bí mật là nhỏ.

Kẻ tấn công tính các phép đo kênh kề trung bình đối với hai khóa đã biết: 0xfff...f và 0x80...01. Nếu hiệu của hai giá trị trung bình (c_0 và c_1) chỉ ra các đỉnh nhọn thì các bít khóa rò rỉ và vì vậy kết quả kiểm định là thất bại (xem Hình D.1).

CHÚ THÍCH: DSA và ECDSA là không bị tổn thương đối với DPA/DEMA địa chỉ - bit bởi vì chúng sử dụng số mũ phù du và số vô hướng tương ứng.



Hình D.1 - DPA / DEMA bit địa chỉ

D.5 SPA/ SEMA đã tinh chỉnh

Liên quan đến ECC nếu các tọa độ xạ ảnh được sử dụng trong một IUT thì chúng có thể được sử dụng để làm ngẫu nhiên dữ liệu trung gian; SPA/SEMA chuẩn như được mô tả trong các điều trước không thể được sử dụng trực tiếp. Tuy nhiên, dưới giả thuyết rằng khóa bí mật là không ngẫu nhiên, khai thác các tính chất của các gọi là các điểm đặc biệt có thể dẫn đến một tấn công.[55] Một điểm đặc biệt *P0* (không bằng vô hạn) là một điểm có tính chất là một trong các tọa độ affine hay xạ ảnh là 0. Từ đó, ngẫu nhiên hóa của các tọa độ xạ ảnh không ảnh hưởng đến tính chất này và tính chất đặc biệt của điểm này vì vậy có thể được lấy từ một vài phép đo kênh kề bằng cách lấy trung bình trên các phép đo.

Trong Thư mục tài liệu tham khảo [56], một phần mở rộng của tấn công trong Thư mục tài liệu tham khảo [55] được mô tả. Tấn công mở rộng này là dựa trên quan sát rằng thậm chí khi một điểm không có tọa độ 0 thì một số giá trị trung gian xảy ra trong quá trình cộng điểm (hay nhân đôi điểm) cũng có thể là 0.

Phòng thí nghiệm kiểm định có thể kiểm thử IUT đối chọi lại SPA/SEMA đã tinh chỉnh theo khung công việc được mô tả trong Thư mục tài liệu tham khảo [55] và / hoặc [56] hay phương pháp liên quan bất kỳ nào khác. Nếu nó khôi phục được CSP thì kết quả kiểm định là không đạt.

ECDSA là giao thức mật mã duy nhất dựa trên các đường cong elliptic trong tiêu chuẩn này. Bởi vậy SPA/SEMA đã tinh chỉnh là không thể áp dụng được bởi vì điểm cơ sở là cố định.

D.6 Sử dụng các kênh kề khả thi mới

Số lượng các kênh kề khả thi có thể tăng lên trong tương lai (ví dụ các phát xạ phô-tôn [49] phát xạ âm thanh). Tại thời điểm viết tiêu chuẩn này, chưa có đủ kiến thức về các kênh kề mới này để định nghĩa một độ đo đạt/không đạt.

D.7 Thay đổi thời lượng do tiêu thụ điện năng

Vì một thiết bị tiêu thụ nhiều lượng điện năng khác nhau, điện áp bên trong của thiết bị sẽ thay đổi một chút. Tín hiệu tương tự được thu được khi sử dụng điện trở Shunt để đo DPA/ SPA.

Các biến thể tương tự về điện áp gây ra sự thay đổi về thời lượng của tín hiệu bên trong, có thể được thu bằng cách sử dụng bộ chuyển đổi thời gian sang kỹ thuật số (TDC) để xuất ra tín hiệu tương tự như vết năng lượng.[67] Vết năng lượng này có thể được coi là phép đo SPA/DPA cho mục đích kiểm định đạt/không đạt, bao gồm cả việc áp dụng các bài kiểm thử SNR trong 7.3.6.

PHỤ LỤC E
(Tham khảo)
Tiêu chí chất lượng cho thiết lập đo lường

E.1 Nhiễu điện tử

E.1.1 Nhiễu của nguồn cung cấp điện

Để làm giảm nhiễu sinh ra bởi nguồn cung cấp điện, một nguồn cung cấp điện ổn định cao cần được sử dụng. IUT cần phải không bao giờ được cấp điện trực tiếp bởi một máy tính PC (ví dụ: qua cổng USB).

E.1.2 Nhiễu của bộ tạo xung nhịp

Là nguồn cung cấp điện năng, một xung nhịp phải có tính ổn định. Một mặt, không thể đòi hỏi các đơn vị triển khai cung cấp một xung nhịp nội bộ ổn định theo thời gian vì nó có thể là một cách để làm mất đồng bộ các thực hiện và do đó trở thành một biện pháp đối phó với các kênh kề. Mặt khác, xung nhịp nội bộ có biên độ ổn định là bắt buộc vì một xung nhịp không ổn định có thể mang đến các hiệu ứng ghép. Nói chung, tín hiệu xung nhịp dạng hình sin nên được ưu tiên hơn so với tín hiệu xung nhịp dạng hình chữ nhật. Chất lượng của bộ tạo xung nhịp (ví dụ bộ dao động tinh thể) cần được đánh giá.

E.1.3 Phát xạ truyền dẫn và bức xạ

Ngoại trừ đối với IUT, các thành phần khác có mặt trong bảng IUT có thể mang đến các phát xạ truyền dẫn và vì vậy mang đến nhiễu trong các phép đo kênh kề. Lý tưởng là thiết lập phép đo cần được xây dựng với hai PCB: Một bảng đo đạc và một bảng giao diện. Bảng đo đạc chỉ chứa thiết bị bị tấn công và mạch đo điện năng. Bảng giao diện quan tâm đến liên lạc với máy tính PC. Hai bảng này lý tưởng là cách ly bởi các mắc nối từ hoặc quang trong các đường liên lạc. Các nguồn phát xạ truyền dẫn bởi vậy được tối thiểu hóa.

Tác động của phát xạ bức xạ đối với thiết lập phép đo có thể được làm giảm đi bằng lá chắn. PCB đặc trưng cho thiết bị bị tấn công có thể được đặt trong lồng Paraday. Các đường liên lạc và đo đạc được nối đến thiết bị bị tấn công cần phải được che chắn hay mắc nối tương ứng.

E.1.4 Nhiễu lượng tử hóa

Nhiễu này là hậu quả của chuyển đổi tương tự sang số được thực hiện bởi máy hiện sóng. Độ phân giải bắt buộc là 8 bit. Trong trường hợp này, hiệu ứng của nhiễu lượng tử hóa là điển hình nhỏ hơn nhiều so với hiệu ứng của các dạng khác của nhiễu.

E.2 Nhiễu chuyển mạch

Tham chiếu đến nhiễu chuyển mạch như là biến thiên của các phép đo kênh kề được gây ra bởi các tế bào không liên quan đến tấn công. Ví dụ, trong phân tích kênh kề của một cài đặt phần cứng AES 128 bit, chúng ta tập trung vào kênh kề được phát xạ bởi một phần của IUT (ví dụ một SBox). Tuy nhiên, nếu nhiều phần của IUT phát xạ các kênh kề tại cùng một lúc thì kẻ tấn công buộc phải phân biệt rõ tất cả các phần để khôi phục phần của IUT khi lựa chọn nó để tấn công. Phát xạ kênh kề của tất cả các phần khác của thiết bị là “nhiễu” từ quan điểm của kẻ tấn công.

Vì rằng tiêu thụ điện năng của IUT kênh kề toàn cục và phát xạ điện từ (EM) của IUT là kênh kề cục bộ nên EM cần được ưu tiên để xác nhận hợp lệ kháng kênh kề.

Lượng nhiễu chuyển mạch cũng phụ thuộc vào tần số của tín hiệu xung được sử dụng để vận hành thiết bị mật mã. Nếu chẳng hạn, một tín hiệu xung cao được sử dụng đối với thiết bị bị tấn công thì có thể là các tín hiệu tiêu thụ điện năng của các chu kỳ xung liên tiếp đã cản trở lẫn nhau.

Theo nguyên tắc chung để làm giảm nhiễu chuyển mạch trong các vết điện năng, tần số xung cần được giảm đi đến mức mà nó dẫn đến các đỉnh tách biệt trong vết điện năng đối với mỗi đường biên xung. Điều này chỉ khả thi khi thiết bị cho phép hoạt động ở tần số xung thấp như vậy.

PHỤ LỤC F
(Tham khảo)
Phương pháp đầu vào được lựa chọn để thúc đẩy phân tích rò rỉ

F.1 Tổng quan

Một vấn đề thực tế trong phân tích rò rỉ DPA/ DEMA là số lượng lớn các vết (các dạng sóng) điện năng/EM để có được các kết quả kiểm định liên quan. Phụ lục này mô tả một cách tiếp cận khả thi gọi là “phương pháp đầu vào được lựa chọn” để kiểm định nghiêm ngặt rò rỉ kênh kề và làm giảm đáng kể số lượng cần thiết các vết điện năng/EM (xem Thư mục tài liệu tham khảo [46], [47], [48]).

F.2 Phác thảo phương pháp

Phương pháp thông thường sử dụng các văn bản đầu vào ngẫu nhiên vào mô-đun mật mã. Tập các văn bản là độc lập với giá trị đã cho của CSP. Kịch bản này là giống như kịch bản được tiến hành bởi các kẻ tấn công.

Tuy nhiên, nếu người kiểm định biết giá trị của CSP thì người kiểm định có thể lựa chọn một tập các văn bản “tốt” đối với phân tích rò rỉ đối với CSP đã biết. Sau đó, người kiểm thử vận hành mô-đun mật mã với CSP khi nhập các văn bản trong tập.

Ví dụ, để thực hiện kiểm thử rò rỉ cho AES khóa 128 bit của CPA đối với vòng cuối cùng (thứ 10), người kiểm thử:

a) tìm dữ liệu trung gian để được xử lý bởi vòng thứ mười với khoảng cách Hamming nhỏ trong tất cả các bộ tám bit hoặc khoảng cách Hamming lớn trong tất cả các bộ tám bit đối với các đầu ra sau đó;

b) chuyển đổi chúng thành văn bản đầu vào sử dụng CSP đã biết.

PHỤ LỤC G
(Tham khảo)
Nguyên nhân một kênh kề được đánh giá là không thể đo lường được

G.1 Mục đích

Phụ lục này cung cấp danh sách các ví dụ về các nguyên nhân tại sao phòng thí nghiệm có thể đánh giá một kênh kề là không thể đo lường được (xem G.2). Danh sách này không đầy đủ.

Mục này không ngăn cản cơ quan phê duyệt mở rộng danh sách.

Một danh sách các nguyên nhân từ cơ quan phê duyệt có thể thay thế phụ lục này.

G.2 Ví dụ

a) IUT sẽ được sử dụng trong khu vực hạn chế không có truy cập internet cũng như truy cập vật lý.

b) Các hoạt động mật mã của IUT không thể được kích hoạt.

PHỤ LỤC H
(Tham khảo)
Thông tin về vị trí rò rỉ liên quan đến thời gian thuật toán

H.1 Mục đích

Phụ lục này cung cấp danh sách các ví dụ về rò rỉ không nên được coi là nhạy cảm và không được quy kết là không đạt (xem H.2). Danh sách này không đầy đủ.

Mục này không ngăn cản cơ quan phê duyệt mở rộng danh sách.

Danh sách thời gian rò rỉ không nhạy cảm từ cơ quan phê duyệt có thể thay thế phụ lục này.

Thời gian rò rỉ nhạy cảm có nghĩa là rò rỉ trong ranh giới này đại diện cho một độ nhạy cảm. Rò rỉ có thể tồn tại tại một điểm trên thông tin nhạy cảm do cơ chế kiểm thử được đề xuất, nhưng rò rỉ này không phải là sự không đạt. Mục này thường thấy nhất khi khóa bí mật được tải hoặc gỡ bỏ từ lõi mật mã chẳng hạn. Phòng thí nghiệm kiểm định nên chỉ định thời gian rò rỉ nhạy cảm và chỉ rò rỉ trong ranh giới này mới là sự không đạt.

H.2 Ví dụ về thời gian rò rỉ không nhạy cảm

a) Các vòng bên ngoài của mật mã khối (ví dụ: 1/3 vòng AES đầu tiên/cuối cùng).

b) Các hoạt động tải khóa như khóa được tải từ thanh ghi nội bộ vào lõi mật mã.

c) Xử lý văn bản thuần túy hoặc văn bản mật mã của mật mã khối.

Thư mục tài liệu tham khảo

[1] Kocher P. C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, CRYPTO '96.

[2] Dhem J.-F., Koeune F., Leroux P.-A., Mestre P., Quisquater J.-J., Willems J.-L. A Practical Implementation of the Timing Attack, UCL Report, 1998.

[3] Schindler W. A Timing Attack against RSA with the Chinese Remainder Theorem, CHES '00.

[4] Walter C. D. Sliding Windows Succumbs to Big Mac Attack, CHES'01.

[5] Walter C. D., Thompson S. “Distinguishing Exponent Digits by Observing Modular Subtractions”, CT- RSA'01.

[6] Novak R. SPA-Based Adaptive Chosen-Ciphertext Attack on RSA Implementation, PKC'02.

[7] Schindler W. “Combined Timing and Power Attack”, PKC'02.

[8] den Boer B., Lemke K., Wiche G. A DPA Attack Against the Modular Reduction with a CRT Implementation of RSA, CHES2002.

[9] Klima V., Rosa T. Further Results and Considerations on Side Channel Attacks on RSA, CHES2002.

[10] Sakai Yasuyuki Kouichi Sakurai, On the Side Channel Attacks Against a Parallel Algorithm of the Exponentiation, SCIS2003.

[11] Hideyuki Miyake, Yuuki Tomoeda, Atsuhi Shimbo, Shinichi Kawamura, New timing attack against RSA implementation with Montgomery multiplication, SCIS2003 (Japanese).

[12] Masanobu Koike, Shinichi Kawamura, Tsutomu Matsumoto, Side-Channel Attacks on RSA Implementation in RNS Representation and Their Countermeasures, SCIS2003 (Japanese).

[13] Pierre-Alain Fouque, Gwénaelle Martinet, and Guillaume Poupard, Attacking Unbalanced RSA-CRT Using SPA, CHES2003.

[14] Itoh K., Izu T. Address-bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA, CHES2002.

[15] Kocher P., Jaffe J., Jun B., Differential Power Analysis, Springer-Verlag, CRYPTO 99. Springer-Verlag, 1999, pp. 388–97.

[16] Mangard S., Oswald E., Popp T. Power Analysis Attacks - Revealing the Secrets of Smartcards. Springer -Verlag, 2007

[17] Gandolfi K., Mourtel C., Olivier F. Electromagnetic Analysis: Concrete Results, CHES 2001. Springer-Verlag, 2001, pp. 251–61.

[18] Batina L., Hogenboom J., Mentens N., Moelans J., Vliegen J. Side-channel evaluation of FPGA implementations of binary Edwards curves, ICECS 2010. IEEE, 2010

[19] Katashita T., Hori Y., Sakane H., Satoh A. Side-Channel Attack Standard Evaluation Board SASEBO-W for Smartcard Testing, NIAT2011, 2011.

[20] Goodwill G., Jun B., Jaffe J., Rohatgi P. A testing methodology for side-channel resistance validation, NIAT2011, 2011.

[21] Jaffe J., Rohatgi P., Witteman M. Efficient side-channel testing for public key algorithms: RSA case study, NIAT2011, 2011.

[22] Robert McEvoy, Micheal Tunstall, Colin C. Murphy, William P. Marnane, Differential power analysis of HMAC based on SHA-2, and countermeasures, WISA'07.

[23] Mangard S., A Simple Power Analysis (SPA) Attack on Implementation of the AES Key Expanstion, LNCS 2587. Springer-Verlag, 2003, pp. 343–58.

[24] Messerges T.S., Dabbish E.A., Sloan R.H., Examining Smart-Card Security under the Threat of Power Analysis Attacks. IEEE Trans. Comput. 2002 May, 51 (5) pp. 541–552

[25] Bevan R., Knudsen E. Ways to Enhance DPA, International Converence on Information Security and Cryptology (ICISC 2002), LNCS 2587, pp.32342, Springer-Verlag, Dec. 2003.

[26] Waddle J., Wagner D. Towards Efficient Second-Order Power Analysis, CHES 2004, LNCS 3156. Springer-Verlag, 2004, pp. 1–15.

[27] Messerges T.S. Using Second-Order Power Analysis to Attack DPA Resistant Software, CHES 2000, LNCS 1965. Springer-Verlag, 2000, pp. 238–51.

[28] Brier E., Clavier C., Olivier F. Correlation Power Analysis with a Leakage Model, CHES 2004, LNCS 3156, pp. 16-29, Springer-Verlag, Aug. 2004.

[29] Le T., Clediere J., Canovas C., Robisson B., Serviere C., Lacoume J. A Proposition for Correlation Power Analysis Enhancement, CHES2006, LNCS 4249, pp. 14-186, Springer-Verlag, Oct. 2006.

[30] Gierlichs B., Lejla Batina, Pim Tuyls and Bart Preneel, Mutual Information Analysis, A Generic Side- Channel Distinguisher, CHES2008, LNCS 5154. Springer-Verlag, 2008, pp. 426–42.

[31] Batina Lejla, Gierlichs Benedikt, Prouff Emmanuel, Rivain Matthieu, Standaert François- Xavier, Veyrat-Charvillon Nicolas Mutual Information Analysis: a Comprehensive Study, Journal of Cryptology, Vol. 24, No. 2 (2011), pp 269-291, Springer-Verlag, 2011.

[32] Meynard O., Denis Réal, Florent Flament, Sylvain Guilley, Naofumi Homma, Jean-Luc Danger, Enhancement of simple electro-magnetic attacks by pre-characterization in frequency domain and demodulation techniques. DATE, 2011, pp. 1004–9.

[33] Doget Julien, Prouff Emmanuel, Rivain Matthieu, Standaert François-Xavier Univariate side channel attacks and leakage modeling, Journal of Cryptographic Engineering, Vol. 1, No. 2 (2011), pp 123-144, Springer-Verlag, 2011.

[34] Youssef Souissi, Nicolas Debande, Sami Mekki, Sylvain Guilley, Jean-Luc Danger and Ali Maalaoui, On the Optimality of Correlation Power Attack on Embedded Cryptographic Systems, WISTP2012.

[35] Chari S., Josyula R. Rao and Pankaj Rohatgi, Template Attacks, CHES2002, LNCS 2523. Springer- Verlag, 2002, pp. 51–62.

[36] Christian Rechberger and Elisabeth Oswald, Practical Template Attacks, LNCS 3325. Springer-Verlag, 2005, pp. 440–56.

[37] Agrawal D., Josyula R. Rao, Pankaj Rohatgi, and Kai Schramm. Templates as Master Keys, CHES 2005. Springer-Verlag, 2005, pp. 15–29.

[38] Schramm K., Thomas Wollinger, and Chiristof Paar, A New Class of Collision Attacks and its Application to DES, LNCS 2887. Springer, 2003, pp. 206–22.

[39] Schramm K., Gregor Leander, Patrick Felke, and Christof Paar. A Collision-Attack on AES combining Side Channel- and Differential-Attack. CHES 2004, LNCS 3156. Springer-Verlag, 2004, pp. 163–75.

[40] Ledig H., Frédéric Muller, and Frédéric Valette. Enhancing Collision Attacks, CHES 2004, LNCS 3156. Springer, 2004, pp. 176–90.

[41] Clavier C., Benoit Feix, Georges Gagnerot, Mylène Roussellet and Vincent Verneuil, Improved Collision-Correlation Power Analysis on First Order Protected AES, CHES 2004, LNCS 3156. Springer, 2004, pp. 176–90.

[42] Homma N., Miyamoto A., Aoki T., Satoh A., Shamir A., Comparative Power Analysis of Modular Exponentiation Algorithms. IEEE Trans. Comput. 2010 June, 59 (6) pp. 795–807

[43] Clavier C., Benoit Feix, Georges Gagnerot, Mylène Roussellet, Vincent Verneuil: Horizontal Correlation Analysis on Exponentiation. ICICS 2010: 46-61.

[44] Colin D., Walter: Sliding Windows Succumbs to Big Mac Attack. CHES, 2001, pp. 286–99.

[45] François-Xavier Standaert, Tal Malkin, Moti Yung: A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. EUROCRYPT 2009: 443-461.

[46] Kishikawa Takeshi, Saito Shohei, Tsuchiya Yuu, Toyama Tsuyoshi, Matsumoto Tsutomu How to Accelerate Side-Channel Security Evaluation, poster presentation at CHES 2012, Leuven, 09-12 Sept. 2012.

[47] Kishikawa Takeshi, Saito Shohei, Tsuchiya Yuu, Toyama Tsuyoshi, Matsumoto Tsutomu An Efficient Method of Strictly Evaluating Side-Channel Security, IEICE Technical Report, ISEC2012-56, Tokyo, 21 Sept. 2012.

[48] Kishikawa T., Matsumoto T. Applying Chosen-Input Method to Electromagnetic Side-Channel Analysis, The 30th Symposium on Cryptography and Information Security, 3E4-E, IEICE, Kyoto, Japan, Jan. 22- 25, 2013.

[49] Schlösser A., Dmitry Nedospasov, Juliane Krämer, Susanna Orlic and Jean-Pierre Seifert. Simple Photonic Emission Analysis of AES – Photonic side channel analysis for the rest of us. CHES, 2012, pp. 41– 57.

[50] Daniel J. Bernstein. Cache-Timing Attacks on AES. Available on cr.yp.to/antiforgery/cachetiming-20050414.pdf

[51] Oswald E., Enhancing Simple Power-Analysis Attacks on Elliptic Curve Cryptosystems. CHES, 2002, pp. 82–97.

[52] Aciiçmez O., Koç C.K., Seifert J.-P. Predicting Secret Keys via Branch Prediction. RSA Conference, Cryptographer's Track (CT-RSA) 2007. pp. 225-242.

[53] Mangard S., A Simple Power-Analysis (SPA) Attack on Implementation of the AES Key Expansion. ICISC 2002, LNCS 2587, pp. 343-358.

[54] Fouque P.-A., Valette F. The Doubling Attack – Why Upwards is Better than Downwards. CHES 2003, pp- 269-280.

[55] Goubin L., A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems. PKC, 2003, pp. 199–210.

[56] Akishita T., Takagi T. Zero-value point attacks on elliptic curve cryptosystem. In Information Security 2003, LNCS 2851, pp. 218–233.

[57] CathaLo J., Koeune F., Quisquater J.-J., A New Type of Timing Attack: Application to GPS. CHES, 2003, pp. 291–303.

[58] Jean-Luc Danger, Nicolas Debande, Sylvain Guilley and Youssef Souissi, "High-order Timing Attacks", Proceedings of the First Workshop on Cryptography and Security in Computing Systems, CS2 '14, ISBN: 978-1-4503-2484-7, Vienna, Austria, pages 7-12, ACM. Available at https://dl.acm.org/citation.cfm?id=2556316

[59] Danger J.-L., Guilley S., Hoogvorst P., Murdica C., Naccache D. "A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards", Journal of Cryptographic Engineering, volume 3, number 4, 2013, Springer Berlin Heidelberg, pages 241-265. Available at http://link.springer.com/ article/10.1007%2Fs13389-013-0062-6

[60] Bhasin S. Jean-Luc Danger, Sylvain Guilley and Zakaria Najm. "NICV: Normalized Inter-Class Variance for Detection of Side-Channel Leakage". International Symposium on Electromagnetic Compatibility, EMC'14, Tokyo, Japan.

[61] Bhasin S., Danger J.-L., Guilley S., Najm Z. "NICV: Normalized Inter-Class Variance for Detection of Side-Channel Leakage". Cryptology ePrint Archive, 2013. Available at https://eprint.iacr.org/2013/ 717

[62] Whitnall C., Oswald E. A Critical Analysis of ISO 17825 ('Testing Methods for the Mitigation of Non-invasive Attack Classes Against Cryptographic Modules'). ASIACRYPT 2019. LNCS, vol 11923: 256-284. Available at https://link.springer.com/chapter/10.1007%2F978-3-030-34618-8_9

[63] O'Flynn C., Chen Z., Synchronous Sampling and Clock Recovery of Internal Oscillators for Side Channel Analysis. Journal of Cryptographic Engineering volume 5, pages 53–69 (2015).

[64] Genkin D., Pachmanov L., Pipman I., Tromer E., Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation. CHES 2015, pp 207–228.

[65] Belenky Y., Dushar I., Teper V., Chernyshchyk H., Azriel L., Kreimer Y., First Full-Fledged Side Channel Attack on HMAC-SHA-2. In: Bhasin S., De Santis F., (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2021. Lecture Notes in Computer Science, vol 12910. Springer, Cham.

[66] Chuah C.W., Koh W.W. Timing Side Channel Attack on Key Derivation Functions. In: Kim, K., Joukov, N. (eds) Information Science and Applications 2017. ICISA 2017. Lecture Notes in Electrical Engineering, vol 424. Springer, Singapore.

[67] Schellenberg Falk, Dennis R.E. Gnad, Amir Moradi, and Mehdi B. Tahoori. An Inside Job: Remote Power Analysis Attacks on FPGAs. Design, Automation & Test in Europe Conference & Exhibition (DATE) 2018.

[68] ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories

[69] ISO/IEC 20085-1:2019, IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques

[70] ISO/IEC 20085-2:2020, IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 2: Test calibration methods and apparatus.