(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0052301**

(51)[2021.01] **G06F 21/00**

(13) **B**

(21) 1-2022-05520

(22) 30/08/2022

(45) 27/10/2025 451

(43) 25/11/2022 416A

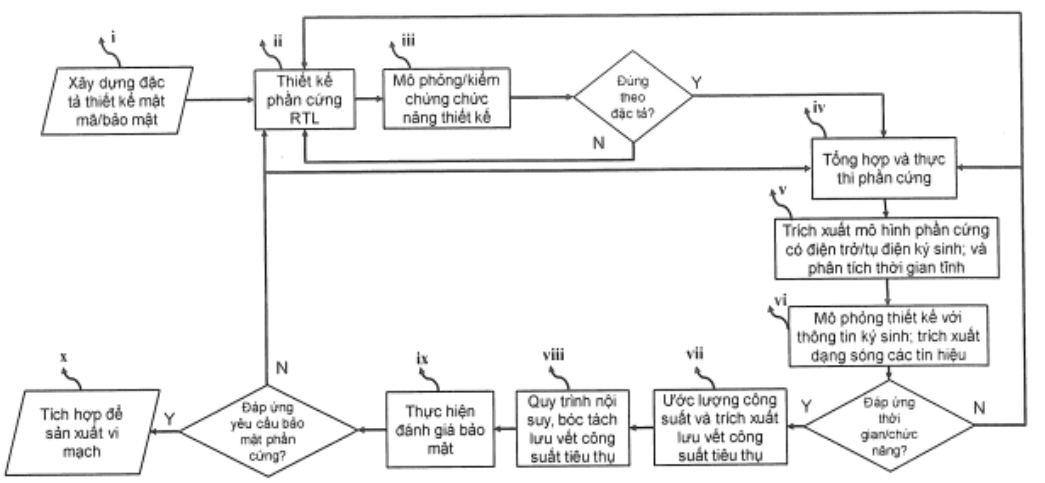
(73) VIỆN CÔNG NGHỆ THÔNG TIN, ĐẠI HỌC QUỐC GIA HÀ NỘI (VN)
Nhà E3, 144 Xuân Thủy, quận Cầu Giấy, Hà Nội

(72) Bùi Duy Hiếu (VN); Trần Xuân Tú (VN).

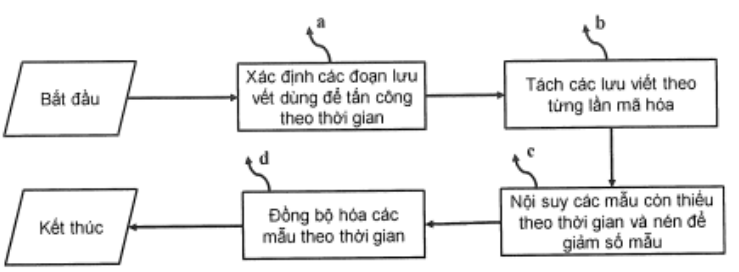
(54) QUY TRÌNH ĐÁNH GIÁ MỨC ĐỘ BẢO MẬT CỦA PHẦN CỨNG DỰA TRÊN LƯU VẾT ƯỚC LƯỢNG CÔNG SUẤT TIÊU THỤ

(21) 1-2022-05520

(57) Sáng chế đề cập đến quy trình đánh giá mức độ bảo mật của phần cứng dựa trên lưu vết ước lượng công suất tiêu thụ được thực hiện theo các bước sau: (i) xây dựng đặc tả thiết kế mật mã/bảo mật; (ii) thiết kế phần cứng dưới dạng chuyển dịch thanh ghi (RTL); (iii) mô phỏng/kiểm chứng chức năng của thiết kế; (iv) tổng hợp và thực thi phần cứng thiết kế; (v) trích xuất các thông tin trở kháng và dung kháng ký sinh dựa trên kết quả ở bước (iv) và phân tích thời gian tĩnh: kiểm tra các đáp ứng về mặt thời gian của thiết kế so với đặc tả và các ràng buộc; (vi) mô phỏng thiết kế với các thông tin ký sinh và trích xuất dạng sóng của các tín hiệu; (vii) ước lượng công suất tiêu thụ và trích xuất lưu vết ước lượng công suất tiêu thụ; (viii) nội suy và bóc tách các lưu vết công suất tiêu thụ; (ix) thực hiện đánh giá bảo mật dựa trên lưu vết ước lượng công suất tiêu thụ thu thập được ở bước (viii); và (x) tích hợp thiết kế vào hệ thống để sẵn sàng sản xuất vi mạch.



Hình 1



Hình 2

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến quy trình đánh giá mức độ bảo mật của phần cứng dựa trên việc phân tích lưu vết ước lượng công suất tiêu thụ của thiết kế phần cứng.

Tình trạng kỹ thuật của sáng chế

Các thuật toán bảo mật thường được đánh giá thông qua mức độ an toàn dựa trên thuật toán và các nghiên cứu lý thuyết dựa trên cấu trúc của thuật toán. Việc này nhằm đảm bảo thuật toán không có các lỗ hổng bảo mật trong quá trình thiết kế có thể bị khai thác để tìm ra khóa bí mật. Việc tìm ra khóa bí mật sử dụng trong các thuật toán này thường tốn rất nhiều thời gian và cần lượng dữ liệu và tính toán lớn. Tuy nhiên, trong quá trình thực thi thuật toán trên các hệ thống phần mềm và phần cứng, các thông tin kênh kề (side-channel information) như công suất tiêu thụ hay phát xạ điện từ trường có thể được sử dụng để tìm ra khóa bí mật. Tấn công sử dụng thông tin kênh kề đang là vấn đề nhức nhối trong lĩnh vực bảo mật.

Các thuật toán bảo mật dữ liệu như thuật toán AES (tiêu chuẩn mã hoá nâng cao - advanced encryption standard) đã được chứng minh là có mức độ an toàn cao, có nghĩa là nó không có lỗ hổng bảo mật về mặt thiết kế thuật toán. Tuy nhiên, kẻ tấn công vẫn có thể khai thác các thông tin rò rỉ trong quá trình thuật toán được chạy bằng phần mềm hoặc phần cứng kết hợp với các thông tin thu thập được để tìm ra chìa khóa bí mật trong một khoảng thời gian cho phép. Ví dụ, kẻ tấn công có thể tìm ra khóa bí mật dùng để mã hóa dữ liệu sử dụng thuật toán AES trên các vi điều khiển AVR của hãng Atmel bằng cách thu thập lưu vết công suất tiêu thụ của khoảng hơn 100 lần mã hóa và các giá trị lối ra của quá trình mã hóa. Toàn bộ quá trình tấn công này có thể được thực hiện trong vòng vài phút với các dụng cụ thông thường. Trong khi đó, các phương pháp tấn công truyền thống vào mặt thuật toán như tấn công vét cạn (Brute Force) có thể mất nhiều năm. Điều này cho thấy tầm quan trọng trong việc đánh giá mức độ bảo mật của các thực thi thuật toán mã hóa trên phần cứng và phần mềm trước các tấn công sử dụng thông tin kênh kề.

Các tấn công sử dụng thông tin kênh kề có thể được thực hiện bằng các thu thập các thông tin kênh kề như thông tin về thời gian chạy thuật toán, thông tin truy cập bộ nhớ đệm (cache) hay các lưu vết công suất tiêu thụ và lưu vết phát xạ điện từ trường. Đối với các thiết kế phần cứng của các thuật toán bảo mật, thông tin kênh kề hay được sử dụng là thông tin về các lưu vết công suất tiêu thụ hoặc phát xạ điện từ trường.

Thông thường, thiết kế phần cứng của các thuật toán bảo mật cần trải qua toàn bộ quy trình thiết kế bao gồm các bước như sau:

Xây dựng đặc tả thiết kế;

Xây dựng bản mô tả phần cứng dưới dạng chuyển dịch thanh ghi (RTL);

Kiểm tra/kiểm chứng thiết kế RTL để đảm bảo thiết kế hoạt động như đặc tả;

Tổng hợp và thực thi phần cứng thiết kế trên các công nghệ ASIC (Application-Specific Integrated Circuit) hoặc FPGA (Field Programmable Logic Array);

Trích xuất thông tin về trở kháng và dung kháng ký sinh;

Phân tích thời gian/công suất tiêu thụ;

So sánh sự tương đồng về mạch điện và bố trí linh kiện (Layout-Versus-Schematic) và kiểm tra luật thiết kế (Design-Rule-Check);

Sản xuất vi mạch hoặc nạp lên kit FPGA;

Chạy thuật toán trên phần cứng đã chế tạo và thu thập lưu vết công suất tiêu thụ và dữ liệu;

Thực hiện các đánh giá về mức độ bảo mật của phần cứng sử dụng lưu vết công suất tiêu thụ.

Tuy nhiên, nếu thực hiện toàn bộ các bước này thì tiêu tốn rất nhiều thời gian và tiền bạc, đặc biệt là các thiết kế sử dụng công nghệ ASIC. Bởi vì, thời gian sản xuất vi mạch (từ khi hoàn thành thiết kế để gửi đi chế tạo) khá lâu với chi phí lớn và nếu phát hiện ra vấn đề bảo mật phần cứng, các vi mạch đó có thể không được sử dụng cho các ứng dụng cần mức độ bảo mật cao như thẻ ngân hàng, căn cước công dân điện tử, các ứng dụng cho an ninh và quân sự.

Bản chất kỹ thuật của sáng chế

Để giải quyết vấn đề kỹ thuật nêu trên, sáng chế đề xuất quy trình đánh giá mức độ bảo mật của phần cứng dựa trên lưu vết ước lượng công suất tiêu thụ trước khi gửi đi chế tạo, nhằm mục đích tìm ra các lỗ hổng về bảo mật phần cứng sớm hơn. Quy trình này có thể giúp phát hiện sớm các lỗ hổng bảo mật của thiết kế phần cứng từ đó tiết kiệm được chi phí sản xuất và kiểm thử vi mạch sau chế tạo.

Để đạt được mục đích nêu trên, sáng chế đề xuất quy trình đánh giá mức độ bảo mật của phần cứng dựa trên lưu vết ước lượng công suất tiêu thụ được thực hiện theo các bước sau:

(i) xây dựng đặc tả thiết kế mật mã/bảo mật: dựa vào thuật toán và các yêu cầu của hệ thống, người thiết kế đề ra các chỉ tiêu kỹ thuật cần đạt, bao gồm các chức năng của hệ thống và thông số bao gồm tần số hoạt động, thông lượng cần đạt, công suất tiêu thụ và diện tích thiết kế;

(ii) thiết kế phần cứng dưới dạng chuyển dịch thanh ghi (RTL): dựa trên đặc tả thiết kế, xây dựng kiến trúc phần cứng của thiết kế và xây dựng mã nguồn dưới dạng chuyển dịch thanh ghi (RTL) để có thể tổng hợp thành phần cứng;

(iii) mô phỏng/kiểm chứng chức năng của thiết kế: kiểm tra lại thiết kế có được thiết kế đúng với đặc tả đã đề ra ở bước (i) hay không, trong đó:

nếu kết quả mô phỏng/kiểm chứng chức năng đáp ứng được các yêu cầu đề ra trong bước (i) thì thực hiện các bước tiếp theo,

ngược lại, nếu kết quả mô phỏng/kiểm chứng chức năng không đáp ứng được các yêu cầu đề ra trong bước (i) thì người thiết kế phải điều chỉnh lại thiết kế đã thực hiện ở bước (iii);

(iv) tổng hợp và thực thi phần cứng thiết kế: mã nguồn dưới dạng RTL được thực hiện ở bước (ii) sẽ được chuyển thành các cổng lô-gic và bố trí linh kiện (layout) của mạch trên công nghệ chế tạo lựa chọn;

(v) trích xuất các thông tin trở kháng và dung kháng ký sinh dựa trên kết quả ở bước (iv) và phân tích thời gian tĩnh: kiểm tra các đáp ứng về mặt thời gian của thiết kế so với đặc tả và các ràng buộc;

(vi) mô phỏng thiết kế với các thông tin ký sinh và trích xuất dạng sóng của các tín hiệu: mô phỏng thiết kế với các thông tin vật lý bao gồm độ trễ của

các tín hiệu trong các điều kiện khác nhau, kết quả mô phỏng là dạng sóng của các tín hiệu được lưu lại để tiến hành ước lượng công suất tiêu thụ và trích xuất lưu vết công suất tiêu thụ, trong đó:

nếu kết quả mô phỏng chạy đúng với đặc tả đã xây dựng ở bước (i), thì thực hiện các bước tiếp theo,

ngược lại, nếu kết quả mô phỏng không chạy đúng với đặc tả đã xây dựng ở bước (i) thì cần xác định lỗi gặp phải để quay lại bước (ii) hoặc bước (iv), cụ thể như sau:

nếu lỗi gặp phải là các vi phạm về mặt thời gian ảnh hưởng đến tần số hoạt động của thiết kế, thì quay lại bước (iv) để tối ưu lại thiết kế,

nếu lỗi gặp phải là các lỗi về mặt chức năng hoặc bước (iv) không thể giải quyết được, tức là một lỗi về mặt kiến trúc, thì quay lại bước (ii) để thiết kế lại kiến trúc của khối phần cứng;

(vii) ước lượng công suất tiêu thụ và trích xuất lưu vết ước lượng công suất tiêu thụ: sử dụng công cụ ước lượng công suất tiêu thụ để ước lượng công suất tiêu thụ của mạch dựa vào các thông tin trong thư viện công nghệ;

(viii) nội suy và bóc tách các lưu vết công suất tiêu thụ thu được ở bước (vii) do các lưu vết công suất tiêu thụ thu được ở trong bước (vii) chưa thể sử dụng ngay để đánh giá mức độ bảo mật của phần cứng;

(ix) thực hiện đánh giá bảo mật dựa trên lưu vết ước lượng công suất tiêu thụ thu thập được ở bước (viii):

sử dụng kỹ thuật phân tích công suất tiêu thụ vi sai và phân tích công suất tiêu thụ tương quan để tìm ra khóa bí mật của thuật toán mã hóa, dựa trên một giả định về khóa bí mật, hai kỹ thuật phân tích này cho đánh giá giả định là đúng hoặc sai, theo đó nếu thiết kế không để lộ khóa bí mật khi áp dụng hai kỹ thuật phân tích này với các giả định khóa khác nhau, thì hệ thống được coi là có thể chống lại các tấn công dùng lưu vết công suất tiêu thụ; hoặc

sử dụng kỹ thuật đánh giá rò rỉ dùng véc-tơ kiểm tra để chỉ ra bước nào trong thuật toán làm rò rỉ thông tin từ lưu vết công suất tiêu thụ, phương pháp này sử dụng hàm T-Test trong xác suất thống kê để tính toán hệ số t theo thời gian với phương trình như sau:

$$t = \frac{\mu_0^2 - \mu_1^2}{\sqrt{\frac{s_0^2}{n_0} - \frac{s_1^2}{n_1}}}$$

trong đó:

μ_0 là giá trị trung bình của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 0,

μ_1 là giá trị trung bình của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 1,

s_0 là phương sai của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 0,

s_1 là phương sai của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 1,

n_0 là tổng số mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 0,

n_1 là tổng số mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 1,

nếu hệ số $|t| > 4,5$ có nghĩa là có rò rỉ thông tin từ thiết kế, có thể phân biệt giữa các giả định đúng và giả định sai dựa vào hàm T-Test, trong đó:

nếu kết quả đánh giá mức độ bảo mật đạt yêu cầu, thì chuyển sang bước tiếp theo,

nếu kết quả đánh giá mức độ bảo mật chưa đạt yêu cầu, thì phải thực hiện lại quy trình thiết kế ở các bước (ii) hoặc bước (iv), cụ thể như sau:

nếu kết quả phân tích lưu vết công suất tiêu thụ sử dụng các kỹ thuật phân tích công suất tiêu thụ vi sai, phân tích công suất tiêu thụ tương quan không thể khôi phục khóa bí mật hoặc đánh giá rò rỉ công suất dùng véc-tơ kiểm tra không có sự rò rỉ thông tin với hệ số $|t| < 4,5$, thì chuyển sang các bước tiếp theo;

đối với các thiết kế không yêu cầu tính bảo mật phần cứng cao, kết quả phân tích lưu vết công suất tiêu thụ không cho phép khôi phục khóa bí mật nhưng chấp nhận có rò rỉ thông tin, tức là một số điểm hệ số $|t| > 4,5$;

đối với các thiết kế yêu cầu tính bảo mật phần cứng cao, thực hiện phân tích lưu vết công suất tiêu thụ sử dụng các hàm bậc cao;

đối với các thiết kế vi phạm các yêu cầu về bảo mật phần cứng, hiệu chỉnh lại quá trình tổng hợp phần cứng và tối ưu lô-gic ở bước (iv), khi việc này không giải quyết được vấn đề, thay đổi lại ở mức kiến trúc ở bước (ii); và

(x) tích hợp thiết kế vào hệ thống để sẵn sàng sản xuất vi mạch.

Theo một phương án của sáng chế, đặc tả thiết kế mật mã/bảo mật tại bước (i) còn bao gồm yêu cầu về mức độ bảo mật và bảo mật ở mức phần cứng gồm có khả năng chống lại một số loại tấn công vào phần cứng bao gồm tấn công sử dụng lưu vết công suất tiêu thụ hay sử dụng lưu vết điện từ trường hoặc tấn công bằng cách gây lỗi hệ thống.

Theo một phương án của sáng chế, các kỹ thuật được dùng để đánh giá bảo mật dựa trên lưu vết ước lượng công suất tiêu thụ tại bước (ix) bao gồm phân tích công suất tiêu thụ vi sai (Differential Power Analysis), phân tích công suất tiêu thụ tương quan (Corrational Power Analysis), đánh giá rò rỉ dùng véc-tơ kiểm tra (Test Vector Leakage Assessment).

Bước (viii) nội suy và bóc tách các lưu vết ước lượng công suất tiêu thụ bao gồm các công đoạn sau:

(a) xác định các đoạn lưu vết ước lượng công suất tiêu thụ dùng để tấn công theo thời gian để loại bỏ các đoạn lưu vết ước lượng công suất tiêu thụ không sử dụng nhằm mục tiêu giảm số lượng dữ liệu cần xử lý và tăng tốc độ tính toán;

(b) tách các đoạn lưu vết công suất tiêu thụ theo từng lần mã hóa;

(c) nội suy các mẫu còn thiếu theo thời gian và nén để giảm số mẫu: lưu vết ước lượng công suất tiêu thụ chỉ lưu những thời điểm có công suất tiêu thụ thay đổi nên dữ liệu không dàn đều theo thời gian, trong đó thực hiện việc nội suy các điểm còn thiếu đảm bảo các lưu vết ước lượng công suất tiêu thụ có cùng số điểm dữ liệu;

(d) đồng bộ hóa các mẫu để tăng hiệu quả của bài đánh giá. Nếu các mẫu không đồng bộ về mặt thời gian, số lượng lưu vết cần dùng để thực hiện đánh giá tăng lên nhiều lần.

Theo một phương án của sáng chế, tại công đoạn (c) của bước (viii) áp dụng kỹ thuật nén để giảm số điểm dữ liệu từ đó giảm số lượng dữ liệu cần lưu trữ và tăng tốc độ xử lý.

Mô tả vắn tắt các hình vẽ

Hình 1 là lưu đồ minh hoạ quy trình đánh giá mức độ bảo mật của phần cứng sử dụng lưu vết ước lượng công suất tiêu thụ theo sáng chế.

Hình 2 là lưu đồ minh hoạ quá trình nội suy, bóc tách các lưu vết công suất tiêu thụ của quy trình đánh giá mức độ bảo mật của thiết kế phần cứng sử dụng lưu vết ước lượng công suất tiêu thụ theo một phương án của sáng chế.

Hình 3 là đồ thị minh hoạ lưu vết công suất tiêu thụ theo các chu kỳ mã hóa thu được từ quá trình ước lượng công suất tiêu thụ của quy trình đánh giá mức độ bảo mật của thiết kế sử dụng lưu vết ước lượng công suất tiêu thụ theo sáng chế.

Hình 4 là đồ thị minh hoạ lưu vết công suất tiêu thụ với các mốc thời gian không đều lấy từ công cụ ước lượng công suất tiêu thụ của quy trình đánh giá mức độ bảo mật của thiết kế sử dụng lưu vết ước lượng công suất tiêu thụ theo sáng chế.

Hình 5 là đồ thị minh hoạ lưu vết công suất tiêu thụ sau khi sử dụng kỹ thuật nội suy với các mốc thời gian đều của quy trình đánh giá mức độ bảo mật của thiết kế sử dụng lưu vết ước lượng công suất tiêu thụ theo sáng chế.

Hình 6 là đồ thị minh hoạ lưu vết công suất tiêu thụ sau khi được đồng bộ hóa để sẵn sàng sử dụng cho bước đánh giá của quy trình đánh giá mức độ bảo mật thiết kế sử dụng lưu vết ước lượng công suất tiêu thụ theo sáng chế.

Mô tả chi tiết sáng chế

Theo Hình 1, sáng chế đề xuất quy trình đánh giá mức độ bảo mật phần cứng của thiết kế dựa trên lưu vết ước lượng công suất tiêu thụ được thực hiện theo các bước sau:

Bước (i): xây dựng đặc tả thiết kế mật mã/bảo mật: dựa vào thuật toán và các yêu cầu của hệ thống, người thiết kế đề ra các chỉ tiêu kỹ thuật cần đạt, bao gồm các chức năng của hệ thống và thông số như tần số hoạt động, thông lượng cần đạt, công suất tiêu thụ và diện tích thiết kế.

Các chức năng của thiết kế được chuyển thành các tham số có thể định lượng được thông qua các công cụ đánh giá trong các bước tiếp theo. Đối với

thiết kế phần cứng, một số tham số cần được cụ thể hóa bao gồm diện tích phần cứng tối đa cho phép của thiết kế, tần số hoạt động cực đại, thông lượng xử lý, các giao diện Vào/Ra, độ trễ xử lý và công suất tiêu thụ. Dựa trên các tham số này, Bước (ii) sẽ chọn các kiến trúc và giải pháp kỹ thuật để đáp ứng được các yêu cầu trong bản đặc tả. Bước xây dựng đặc tả có thể được thực hiện sử dụng các công cụ soạn thảo văn bản hoặc công cụ trình diễn mà chưa cần sử dụng đến các công cụ kỹ thuật. Các yêu cầu trong bản đặc tả sẽ ảnh hưởng đến các bước tiếp theo trong quy trình thiết kế đặc biệt là việc lựa chọn kiến trúc phần cứng.

Theo một phương án của sáng chế, đối với các hệ thống cần mức độ an toàn cao, bên cạnh các yêu cầu của hệ thống, đặc tả thiết kế còn bao gồm yêu cầu về mức độ bảo mật và bảo mật ở mức phần cứng như có khả năng chống lại một số loại tấn công vào phần cứng như tấn công sử dụng lưu vết công suất tiêu thụ hay sử dụng lưu vết điện từ trường hoặc tấn công bằng cách gây lỗi hệ thống. Nội dung của sáng chế này tập trung vào các tấn công phần cứng sử dụng lưu vết công suất tiêu thụ và có thể mở rộng ra các tấn công sử dụng lưu vết bức xạ điện từ trường.

Bước (ii): Thiết kế phần cứng dưới dạng chuyển dịch thanh ghi RTL. Người thiết kế dựa trên đặc tả thiết kế, xây dựng kiến trúc phần cứng của thiết kế và xây dựng mã nguồn dưới dạng chuyển dịch thanh ghi (RTL) để có thể tổng hợp thành phần cứng.

Trong bước này, người thiết kế sử dụng các kiến thức về điện tử số và các ngôn ngữ lập trình để tạo ra các kiến trúc phần cứng nhằm đáp ứng các yêu cầu được đưa ra trong đặc tả của thiết kế. Bản đặc tả của thiết kế sẽ được chuyển thành mô hình mô phỏng sử dụng ngôn ngữ miêu tả phần cứng như VHDL, Verilog, SystemVerilog hoặc các ngôn ngữ miêu tả phần cứng khác. Mô hình dưới dạng các ngôn ngữ miêu tả phần cứng của bản đặc tả thiết kế sẽ được mô phỏng để đánh giá về mặt chức năng, ước lượng thông lượng và độ trễ của thiết kế dựa trên tần số hoạt động và số chu kỳ cần dùng để thực hiện các chức năng của bản thiết kế. Mô hình dưới dạng RTL có thể được tổng hợp thành phần cứng sử dụng các công cụ tổng hợp phần cứng.

Một số mô hình chỉ mô tả chức năng đơn thuần, có thể được mô phỏng để đánh giá về chức năng nhưng không thể tổng hợp thành phần cứng. Trong trường hợp này, người thiết kế tiếp tục phân tích và chuyển chúng thành mô

hình dưới dạng RTL để có thể thực thi thành phần cứng. Trong bước này, các mô hình miêu tả chức năng dần dần được chuyển thành các mô hình RTL để sẵn sàng chuyển thành phần cứng trong Bước (iv) sau khi đã được mô phỏng và kiểm chứng về mặt chức năng.

Đối với các thiết kế có khối mật mã hoặc bảo mật bằng phần cứng có yêu cầu về bảo mật ở mức phần cứng, người thiết kế phải thêm các giải pháp chống lại các tấn công về mặt bảo mật phần cứng. Một số giải pháp có thể được áp dụng trong bước này. Một số giải pháp khác có thể được áp dụng trong Bước (iv). Một số giải pháp có thể là sự kết hợp của các phương án kể trên. Việc đánh giá sớm mức độ bảo mật phần cứng được thực hiện trong Bước (ix).

Bước (iii): Mô phỏng/kiểm chứng chức năng của thiết kế. Bước này kiểm tra lại thiết kế có được thiết kế đúng với đặc tả đã đề ra ở Bước (i) hay không.

Trong bước này, người thiết kế sử dụng các công cụ mô phỏng phần cứng để mô phỏng và kiểm chứng thiết kế để đảm bảo mô hình dưới dạng RTL hoạt động đúng như đặc tả đã xây dựng ở Bước (i). Môi trường mô phỏng thiết kế được thiết lập với các mô hình tham chiếu để đảm bảo hệ thống hoạt động đúng như mong muốn. Kết quả chạy mô phỏng mô hình RTL của thiết kế sẽ được so sánh với kết quả từ mô hình tham chiếu của thiết kế để đưa ra quyết định như được đề cập dưới đây. Để chứng minh thiết kế hoạt động đúng như đặc tả, thiết kế cần được mô phỏng với nhiều chuỗi dữ liệu đầu vào khác nhau. Ở một khía cạnh khác, các dữ liệu này có thể là dữ liệu ngẫu nhiên được kiểm soát trong quá trình mô phỏng.

Nếu các giải pháp bảo mật phần cứng được thực thi dưới dạng mô hình RTL, bước mô phỏng và kiểm chứng chỉ có thể kiểm tra về mặt chức năng của thiết kế. Người thiết kế phải đảm bảo, các giải pháp bảo mật phần cứng không làm thay đổi chức năng ban đầu của thiết kế. Đánh giá về mức độ bảo mật được thực hiện tại Bước (ix).

Nếu kết quả mô phỏng/kiểm chứng chức năng đáp ứng được các yêu cầu đề ra trong Bước (i) thì thực hiện các bước tiếp theo. Ngược lại, nếu kết quả mô phỏng/kiểm chứng chức năng không đáp ứng được các yêu cầu đề ra trong Bước (i) thì người thiết kế phải điều chỉnh lại thiết kế đã thực hiện ở Bước (ii).

Việc thực hiện đưa ra quyết định tại bước này phụ thuộc vào các thông tin nhận về từ quá trình mô phỏng như kết quả mô phỏng mô hình RTL giống với

kết quả từ mô hình tham chiếu và mức độ bao phủ của dữ liệu kiểm chứng đạt 100%.

Ở một khía cạnh khác, độ bao phủ của dữ liệu kiểm chứng có thể đạt mức từ 90% đến 95%. Nếu các kết quả không đạt, cần quay lại bước (ii) hoặc điều chỉnh kịch bản kiểm tra hoặc tăng số lượng dữ liệu chạy mô phỏng.

Bước (iv): Tổng hợp và thực thi phần cứng thiết kế. Trong bước này, mã nguồn dưới dạng RTL được thực hiện ở Bước (ii) sẽ được chuyển thành các cổng lô-gic và bố trí linh kiện (layout) của mạch trên công nghệ chế tạo lựa chọn.

Bước này sử dụng các công cụ tổng hợp phần cứng để thực hiện việc chuyển từ mã nguồn dưới dạng RTL thành phần cứng dưới dạng các cổng lô-gic và danh sách kết nối sử dụng thư viện tế bào chuẩn của một công nghệ chế tạo. Thiết kế dưới dạng cổng lô-gic và danh sách kết nối tiếp tục được công cụ thực thi phần cứng chuyển thành dạng bố trí linh kiện (layout). Quá trình tổng hợp phần cứng có thể không thực hiện được nếu mã nguồn chưa ở dưới dạng mô hình RTL. Quá trình thực thi phần cứng thành dạng bố trí linh kiện (layout) để gửi đi chế tạo cần sử dụng các luật thiết kế của nhà sản xuất. Bước tổng hợp và thực thi phần cứng cũng tạo ra các báo cáo về diện tích thiết kế, độ trễ của thiết kế, đáp ứng các tiêu chí về mặt thời gian, tần số hoạt động v.v... Các báo cáo này có thể được sử dụng để tối ưu thiết kế và hiệu chỉnh thiết kế để đáp ứng đặc tả được xây dựng trong Bước (i).

Một số giải pháp bảo mật phần cứng có thể được thực thi tại bước này bằng cách tác động trực tiếp vào thiết kế sau khi đã tổng hợp phần cứng hoặc quá trình thực thi phần cứng. Việc tác động vào thiết kế sau khi đã tổng hợp và thực thi phần cứng có thể làm sai lệch các chức năng ban đầu của thiết kế. Do vậy, Bước (vi) kiểm tra thiết kế sau khi tổng hợp và thực thi phần cứng bằng công cụ mô phỏng phần cứng với thông tin về độ trễ gây ra bởi các phần tử ký sinh được trích xuất trong Bước (v).

Bước (v): Trích xuất các thông tin trở kháng và dung kháng ký sinh dựa trên kết quả ở Bước (iv) và phân tích thời gian tĩnh.

Bước này kiểm tra các đáp ứng về mặt thời gian của thiết kế so với đặc tả và các ràng buộc. Phân tích thời gian tĩnh là một bước quan trọng trong quy trình để đảm bảo thiết kế không có lỗi về mặt thời gian. Để thực hiện phân tích

thời gian tĩnh một cách chính xác, các thông tin về trở kháng và dung kháng ký sinh của kết quả bố trí linh kiện (layout) cần được trích xuất dựa trên thông tin ký sinh của công nghệ chế tạo. Dựa trên thông tin về trở kháng và dung kháng ký sinh, độ trễ của các tín hiệu trong thiết kế có thể được tính toán một cách chính xác trong các điều kiện làm việc khác nhau. Đáp ứng thời gian trong bước này được tính toán chính xác hơn các báo cáo về thời gian trong Bước (iv). Ngoài ra, công cụ phân tích thời gian tĩnh cũng có thể phân tích tính toàn vẹn của các tín hiệu trước sự ảnh hưởng của các can nhiễu trong vi mạch. Kết quả của bước này là mô hình độ trễ dựa của thiết kế dựa trên các phần tử ký sinh. Các mô hình độ trễ trong các điều kiện khác nhau được dùng trong mô phỏng ở Bước (vi) để thu được các dạng sóng của tín hiệu trong hệ thống.

Bước (vi): Mô phỏng thiết kế với các thông tin ký sinh và trích xuất dạng sóng của các tín hiệu. Bước này thực hiện mô phỏng thiết kế với các thông tin vật lý như độ trễ của các tín hiệu trong các điều kiện khác nhau. Kết quả mô phỏng là dạng sóng của các tín hiệu được lưu lại để tiến hành ước lượng công suất tiêu thụ và trích xuất lưu vết công suất tiêu thụ.

Nếu kết quả mô phỏng chạy đúng với đặc tả đã xây dựng ở bước (i), thì thực hiện các bước tiếp theo. Ngược lại, nếu kết quả mô phỏng không chạy đúng với đặc tả đã xây dựng ở bước (i) thì cần xác định lỗi gặp phải để quay lại bước (ii) hoặc bước (iv), cụ thể như sau:

nếu lỗi gặp phải là các vi phạm về mặt thời gian ảnh hưởng đến tần số hoạt động của thiết kế, có thể quay lại bước (iv) để tối ưu lại thiết kế;

nếu lỗi gặp phải là các lỗi về mặt chức năng hoặc bước (iv) không thể giải quyết được, tức là có lỗi về mặt kiến trúc, cần phải quay lại bước (ii) để thiết kế lại kiến trúc của khối phần cứng.

Bước (vii): Ước lượng công suất tiêu thụ và trích xuất lưu vết ước lượng công suất tiêu thụ. Bước này sử dụng công cụ ước lượng công suất tiêu thụ để ước lượng công suất tiêu thụ của mạch dựa vào các thông tin trong thư viện công nghệ. Lưu vết công suất tiêu thụ có thể được tính toán dựa trên hoạt động của vi mạch. Do đó, kết quả mô phỏng thiết kế với thông tin về độ trễ có thể dựa sử dụng để tính toán công suất tiêu thụ tức thời dựa trên các hoạt động của từng cổng lô-gic. Sử dụng thông tin về độ trễ và công suất tiêu thụ của các cổng lô-gic cùng với độ trễ của các đường dây dẫn với trở kháng và dung kháng ký sinh,

công suất tiêu thụ tức thời có thể được ước lượng chính xác. Trong bước này, sử dụng công cụ ước lượng công suất, các lưu vết công suất tiêu thụ có thể được trích xuất để tiến hành đánh giá mức độ bảo mật. Sử dụng dạng sóng với thông tin độ trễ thu được trong Bước (vi) cùng với thư viện công nghệ, công cụ ước lượng công suất có thể tạo ra các lưu vết công suất tiêu thụ. Đối với mỗi điều kiện làm việc, cần thực hiện mô phỏng trong Bước (vi) để thu được dạng sóng cho điều kiện làm việc đó và cần thực hiện việc ước lượng công suất tiêu thụ theo điều kiện làm việc đó. Các lưu vết công suất tiêu thụ tại các điều kiện làm việc khác nhau sẽ được sử dụng để đánh giá mức độ bảo mật phần cứng.

Bước (viii): Nội suy và bóc tách các lưu vết công suất tiêu thụ. Lưu vết công suất tiêu thụ thu được ở trong Bước (vii) chưa thể sử dụng ngay để đánh giá mức độ bảo mật phần cứng. Bước nội suy và bóc tách lưu vết công suất tiêu thụ được thể hiện trong Hình 2.

Các lưu vết công suất tiêu thụ thu được ở Bước (vii) chỉ ghi lại công suất tiêu thụ tức thời tại thời điểm dạng sóng của tín hiệu thay đổi theo quá trình mô phỏng. Do vậy, dữ liệu của lưu vết công suất tiêu thụ bao gồm thời điểm mà công suất tiêu thụ thay đổi, và giá trị công suất tại thời điểm đó. Việc này dẫn tới các đoạn công suất trong mỗi lần chạy có thể khác nhau và không khớp về mặt thời gian giữa các điểm trong lưu vết công suất tiêu thụ. Do vậy, cần phải thực hiện các kỹ thuật để bóc tách và đồng bộ hóa về thời gian.

Đối với lưu vết công suất tiêu thụ chứa nhiều lần mã hóa/giải mã, lưu vết cho mỗi lần mã hóa/giải mã cần được cần được bóc tách thành lưu vết công suất tiêu thụ cho mỗi lần mã hóa/giải mã riêng biệt.

Đối với lưu viết công suất tiêu thụ của mỗi lần mã hóa riêng biệt, cần đảm bảo có cùng số điểm dữ liệu và đồng bộ hóa về thời gian. Các lưu vết công suất tiêu thụ dùng để đánh giá bảo mật phải cùng xuất phát tại một thời điểm, có số điểm dữ liệu giống nhau và đồng bộ hóa về mặt thời gian. Việc mất đồng bộ làm giảm hiệu quả của các bài đánh giá.

Theo phương án của sáng chế, lưu vết công suất tiêu thụ của mỗi lần mã hóa có thể được đồng bộ bằng cách nội suy các điểm còn thiếu theo độ phân giải thời gian chạy mô phỏng ở Bước (vi). Việc này đảm bảo các lưu vết công suất tiêu thụ của mỗi lần mã hóa bắt đầu tại cùng một mốc thời gian, có số điểm dữ liệu giống nhau và đồng bộ về mặt thời gian.

Việc nội suy này làm tăng số mẫu trong các lưu vết công suất tiêu thụ và làm tăng thời gian đánh giá. Theo phương án của sáng chế, số mẫu có thể được giảm xuống bằng cách áp dụng kỹ thuật nén để giảm số mẫu. Việc này rút ngắn thời gian đánh giá đáng kể mà không làm giảm hiệu quả của bài đánh giá.

Bước (ix): Thực hiện đánh giá bảo mật dựa trên lưu vết ước lượng công suất tiêu thụ thu thập được ở Bước (viii).

Lưu vết công suất tiêu thụ thu được ở Bước (viii) cùng với các dữ liệu mô phỏng như dữ liệu lối vào và dữ liệu thu được lối ra được sử dụng để đánh giá mức độ bảo mật phần cứng. Các giả định về chìa khóa bí mật có thể được xây dựng dựa vào dữ liệu lối vào hoặc dữ liệu lối ra của thiết kế. Các công cụ xác suất thống kê được sử dụng để loại bỏ những giả định sai dựa trên lưu vết công suất tiêu thụ.

Đối với các giả định ở mức từng bit, kỹ thuật phân tích vi sai có thể được áp dụng trên lưu vết công suất tiêu thụ để phân biệt giả định bit 0 hay bit 1.

Đối với các giả định ở mức byte, kỹ thuật ước lượng tương quan dùng hàm tương quan Pearson. Giả định đúng có giá trị tương quan với lưu vết ước lượng công suất tiêu cao hơn các giả định sai. Nhờ đó giúp phân biệt được khóa đúng và khóa sai theo từng byte.

Lưu vết công suất tiêu thụ thu được ở Bước (viii) và dữ liệu lối vào/lối ra của thiết kế được dùng với các công cụ xác suất thống kê để tìm ra khóa bí mật hoặc để đánh giá thông tin bí mật có bị rò rỉ hay không.

Đối với các thiết kế có thực thi các biện pháp bảo mật ở mức phần cứng, việc phân biệt giữa khóa bí mật thực tế giữa các giả định khó hơn rất nhiều, có thể cần thu thập một lượng rất lớn các lưu vết công suất tiêu thụ. Ngay cả khi có nhiều dữ liệu lưu vết công suất tiêu thụ, các hàm đánh giá cho thấy không có thông tin khóa bí mật bị rò rỉ hoặc không thể tìm ra khóa bí mật do có nhiều thông tin nhiễu.

Theo phương án của sáng chế, các kỹ thuật có thể được dùng để đánh giá bảo mật dựa trên lưu vết ước lượng công suất tiêu thụ bao gồm phân tích công suất tiêu thụ vi sai (Differential Power Analysis), phân tích công suất tiêu thụ tương quan (Corrational Power Analysis), đánh giá rò rỉ dùng véc-tơ kiểm tra (Test Vector Leakage Assessment). Đối với các ứng dụng thông thường, các phép đánh giá này có thể được tiến hành ở bậc một. Đối với các ứng dụng đòi

hỏi mức độ bảo mật cao, các phép đánh giá này có thể được thực hiện ở các bậc cao hơn như bậc hai, bậc ba, v.v... Các đánh giá ở bậc một sử dụng trực tiếp lưu vết công suất tiêu thụ thu được từ Bước (viii). Các đánh giá ở bậc cao sử dụng các biến đổi để ánh xạ lưu vết công suất tiêu thụ và dữ liệu lối vào/lối ra vào một không gian đa chiều để thực hiện đánh giá. Đánh giá ở các bậc cao có các tính toán phức tạp, lượng dữ liệu đa chiều lớn nên thời gian đánh giá chậm. Đầu tiên, các giả định được xây dựng dựa trên dữ liệu Vào/Ra và một mô hình công suất tiêu thụ. Có hai mô hình công suất tiêu thụ được sử dụng phổ biến hiện nay là mô hình trọng số Hamming và mô hình khoảng cách Hamming. Trong mô hình trọng số Hamming, công suất tiêu thụ được coi tỷ lệ với số bit 1 có trong chuỗi bit. Trong mô hình khoảng cách Hamming, công suất tiêu thụ được coi tỷ lệ với số lần chuyển từ bit 0 sang bit 1 hoặc bit 1 sang bit 0 của một tín hiệu.

Dữ liệu giả định với mô hình công suất kết hợp với lưu vết công suất tiêu thụ có thể được dùng để tìm ra khóa bí mật bằng cách loại bỏ giả định sai.

Dữ liệu giả định với mô hình công suất kết hợp với lưu vết công suất tiêu thụ có thể được dùng để tìm ra việc rò rỉ thông tin về khóa bí mật thông qua các công cụ thống kê.

Sử dụng kỹ thuật phân tích công suất tiêu thụ vi sai và phân tích công suất tiêu thụ tương quan sẽ tìm ra khóa bí mật của thuật toán mã hóa, dựa trên một giả định về khóa bí mật, hai kỹ thuật phân tích này cho đánh giá giả định là đúng hoặc sai, theo đó nếu thiết kế không để lộ khóa bí mật khi áp dụng hai kỹ thuật phân tích này với các giả định khóa khác nhau, thì hệ thống được coi là có thể chống lại các tấn công dùng lưu vết công suất tiêu thụ; hoặc

Sử dụng kỹ thuật đánh giá rò rỉ dùng véc-tơ kiểm tra không tìm ra khóa bí mật mà chỉ ra bước nào trong thuật toán làm rò rỉ thông tin từ lưu vết công suất tiêu thụ, phương pháp này sử dụng hàm T-Test trong xác suất thống kê để tính toán hệ số t theo thời gian với phương trình như sau:

$$t = \frac{\mu_0^2 - \mu_1^2}{\sqrt{\frac{s_0^2}{n_0} - \frac{s_1^2}{n_1}}}$$

trong đó:

μ_0 là giá trị trung bình của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 0.

μ_1 là giá trị trung bình của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 1.

s_0 là phương sai của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 0.

s_1 là phương sai của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 1.

n_0 là tổng số mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 0.

n_1 là tổng số mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 1.

Hệ số $|t| > 4,5$ có nghĩa là có rò rỉ thông tin từ thiết kế, có thể phân biệt giữa các giả định đúng và giả định sai dựa vào hàm T-Test.

Nếu kết quả đánh giá mức độ bảo mật ở Bước (ix) này đạt yêu cầu, thì chuyển sang bước tiếp theo.

Nếu kết quả đánh giá mức độ bảo mật ở Bước (ix) này chưa đạt yêu cầu, thì phải thực hiện lại quy trình thiết kế ở các bước (ii) hoặc bước (iv), cụ thể như sau:

nếu kết quả phân tích lưu vết công suất tiêu thụ sử dụng các kỹ thuật phân tích công suất tiêu thụ vi sai, phân tích công suất tiêu thụ tương quan không thể khôi phục khóa bí mật hoặc đánh giá rò rỉ công suất dùng véc-tơ kiểm tra không có sự rò rỉ thông tin với hệ số $|t| < 4,5$, có thể chuyển sang các bước tiếp theo;

đối với các thiết kế không yêu cầu tính bảo mật phần cứng cao, kết quả phân tích lưu vết công suất tiêu thụ không cho phép khôi phục khóa bí mật nhưng chấp nhận có rò rỉ thông tin, tức là một số điểm hệ số $|t| > 4,5$;

đối với các thiết kế yêu cầu tính bảo mật phần cứng cao, thực hiện phân tích lưu vết công suất tiêu thụ sử dụng các hàm bậc cao;

đối với các thiết kế vi phạm các yêu cầu về bảo mật phần cứng, hiệu chỉnh lại quá trình tổng hợp phần cứng và tối ưu lô-gic ở bước (iv), khi việc này không giải quyết được vấn đề, thay đổi lại ở mức kiến trúc ở bước (ii).

Bước (x) tích hợp thiết kế vào hệ thống để sẵn sàng sản xuất vi mạch.

Hình 2 minh hoạ các công đoạn của bước nội suy và bóc tách các lưu vết ước lượng công suất tiêu thụ của quy trình theo một phương án của sáng chế, bao gồm các công đoạn sau:

Công đoạn (a): Xác định các đoạn lưu vết ước lượng công suất tiêu thụ dùng để tấn công theo thời gian để loại bỏ các đoạn lưu vết ước lượng công suất tiêu thụ không sử dụng nhằm mục tiêu giảm số lượng dữ liệu cần xử lý và tăng tốc độ tính toán.

Các đoạn lưu vết ước lượng công suất tiêu thụ dùng để tấn công có thể được xác định dựa vào thông tin về thời gian của từng lần mã hóa trong kết quả mô phỏng. Kịch bản kiểm tra của thiết kế có thể được sử dụng để xác định các đoạn lưu vết công suất tiêu thụ có chứa thông tin cần kiểm tra.

Bên cạnh đó, các kịch bản kiểm tra phần cứng thường hoạt động theo tính chu kỳ. Do vậy, việc xác định các đoạn lưu vết công suất tiêu thụ cần bóc tách cũng mang tính chu kỳ. Điểm khó là phải xác định đúng điểm bắt đầu của chu kỳ đầu tiên. Việc này có thể thực hiện dựa vào kết quả mô phỏng trong quy trình đánh giá mức độ bảo mật phần cứng dựa trên lưu vết ước lượng công suất tiêu thụ.

Công đoạn (b): Tách các đoạn lưu vết công suất tiêu thụ theo từng lần mã hóa.

Sau khi xác định được các mốc thời gian của lưu vết công suất tiêu thụ cần bóc tách. Việc tách các đoạn lưu vết công suất tiêu thụ theo từng lần mã hóa có thể được thực hiện bằng cách sử dụng các chu kỳ mã hóa hoặc các điểm thời gian đã xác định trong bước (i). Theo đó, mỗi đoạn lưu vết công suất tiêu thụ của một lần xử lý sẽ được tách riêng để sẵn sàng cho các bước xử lý tiếp theo. Hình 3 là một ví dụ về việc bóc tách các đoạn lưu vết công suất tiêu thụ theo chu kỳ của mỗi lần mã hóa. Theo đó, $t_{encrypt1}$ và $t_{encrypt2}$ lần lượt là các khoảng thời gian của lần mã hóa thứ nhất và thứ hai. Trong thực tế, các khoảng thời gian này đối với các thiết kế phần cứng thường bằng nhau.

Công đoạn (c): nội suy các mẫu còn thiếu theo thời gian và nén để giảm số mẫu: lưu vết ước lượng công suất tiêu thụ chỉ lưu những thời điểm có công suất tiêu thụ thay đổi nên dữ liệu không dàn đều theo thời gian, bước này thực hiện việc nội suy các điểm còn thiếu đảm bảo các lưu vết ước lượng công suất tiêu thụ có cùng số điểm dữ liệu.

Theo một phương án của sáng chế, áp dụng kỹ thuật nén để giảm số điểm dữ liệu từ đó giảm số lượng dữ liệu cần lưu trữ và tăng tốc độ xử lý.

Kết quả ước lượng công suất tiêu thụ chỉ lưu công suất tiêu thụ và thời gian công suất tiêu thụ thay đổi. Do vậy, các khoảng thời gian giữa các điểm có giá trị lưu vết công suất tiêu thụ t_1 và t_2 không đều nhau như trên Hình 4. Để các lưu vết công suất tiêu thụ có các mốc thời gian đều, kỹ thuật nội suy có thể được áp dụng. Hình 5 là một ví dụ về lưu vết công suất tiêu thụ trên Hình 4 được nội suy dùng hàm nội suy bậc 0. Theo đó, các điểm được nội suy nhận giá trị của điểm đo được ở phía trước. Khoảng thời gian giữa các điểm có lưu vết công suất tiêu thụ liên tiếp t_1, t_2, t_3, … bằng nhau. Các kỹ thuật nội suy khác cũng có thể được áp dụng nhưng sẽ tiêu tốn tài nguyên tính toán và bộ nhớ.

Công đoạn (d): Đồng bộ hóa các mẫu. Bước này thực hiện đồng bộ hóa các mẫu để tăng hiệu quả của bài đánh giá. Nếu các mẫu không đồng bộ về mặt thời gian, số lượng lưu vết cần dùng để thực hiện đánh giá tăng lên nhiều lần. Hình 6 là một ví dụ về các lưu vết công suất tiêu thụ được đồng bộ hóa. Các lưu vết công suất tiêu thụ của mỗi lần mã hóa cùng xuất phát tại một thời điểm. Các mẫu được điều chỉnh để xuất hiện tại các mốc thời gian đều nhau. Khoảng thời gian giữ các mẫu liên tiếp t_1, t_2, t_3, … bằng nhau. Sau khi được đồng bộ hóa, các lưu vết công suất tiêu thụ đã sẵn sàng để sử dụng cho các phép đánh giá về mức độ bảo mật phần cứng của thiết kế. Bước đồng bộ hóa rất quan trọng, giúp giảm số lưu vết cần dùng để đánh giá và tăng hiệu quả bài đánh giá.

Yêu cầu bảo hộ

1. Quy trình đánh giá mức độ bảo mật của phần cứng dựa trên lưu vết ước lượng công suất tiêu thụ bao gồm các bước sau:

(i) xây dựng đặc tả thiết kế mật mã/bảo mật: dựa vào thuật toán và các yêu cầu của hệ thống, người thiết kế đề ra các chỉ tiêu kỹ thuật cần đạt, bao gồm các chức năng của hệ thống và thông số bao gồm tần số hoạt động, thông lượng cần đạt, công suất tiêu thụ và diện tích thiết kế;

(ii) thiết kế phần cứng dưới dạng chuyển dịch thanh ghi (RTL): dựa trên đặc tả thiết kế, xây dựng kiến trúc phần cứng của thiết kế và xây dựng mã nguồn dưới dạng chuyển dịch thanh ghi (RTL) để có thể tổng hợp thành phần cứng;

(iii) mô phỏng/kiểm chứng chức năng của thiết kế: kiểm tra lại thiết kế có được thiết kế đúng với đặc tả đã đề ra ở bước (i) hay không, trong đó:

nếu kết quả mô phỏng/kiểm chứng chức năng đáp ứng được các yêu cầu đề ra trong bước (i) thì thực hiện các bước tiếp theo,

ngược lại, nếu kết quả mô phỏng/kiểm chứng chức năng không đáp ứng được các yêu cầu đề ra trong bước (i) thì người thiết kế phải điều chỉnh lại thiết kế đã thực hiện ở bước (ii);

(iv) tổng hợp và thực thi phần cứng thiết kế: mã nguồn dưới dạng RTL được thực hiện ở bước (ii) sẽ được chuyển thành các cổng lô-gic và bố trí linh kiện (layout) của vi mạch trên công nghệ chế tạo lựa chọn;

(v) trích xuất các thông tin về trở kháng và dung kháng ký sinh dựa trên kết quả ở bước (iv) và phân tích thời gian tĩnh: kiểm tra các đáp ứng về mặt thời gian của thiết kế so với đặc tả và các ràng buộc;

(vi) mô phỏng thiết kế với các thông tin ký sinh và trích xuất dạng sóng của các tín hiệu: mô phỏng thiết kế với các thông tin vật lý bao gồm độ trễ của các tín hiệu trong các điều kiện khác nhau, kết quả mô phỏng là dạng sóng của các tín hiệu được lưu lại để tiến hành ước lượng công suất tiêu thụ và trích xuất lưu vết công suất tiêu thụ, trong đó:

nếu kết quả mô phỏng chạy đúng với đặc tả đã xây dựng ở bước (i), thì thực hiện các bước tiếp theo,

ngược lại, nếu kết quả mô phỏng không chạy đúng với đặc tả đã xây dựng ở bước (i) thì cần xác định lỗi gặp phải để quay lại bước (ii) hoặc bước (iv), cụ thể như sau:

nếu lỗi gặp phải là các vi phạm về mặt thời gian ảnh hưởng đến tần số hoạt động của thiết kế, thì quay lại bước (iv) để tối ưu lại thiết kế,

nếu lỗi gặp phải là các lỗi về mặt chức năng hoặc bước (iv) không thể giải quyết được, tức là một lỗi về mặt kiến trúc, cần phải quay lại bước (ii) để thiết kế lại kiến trúc của khối phần cứng;

(vii) ước lượng công suất tiêu thụ và trích xuất lưu vết ước lượng công suất tiêu thụ: sử dụng công cụ ước lượng công suất tiêu thụ để ước lượng công suất tiêu thụ của mạch dựa vào các thông tin trong thư viện công nghệ;

(viii) nội suy và bóc tách các lưu vết công suất tiêu thụ thu được ở bước (vii) do các lưu vết công suất tiêu thụ thu được ở trong bước (vii) chưa thể sử dụng ngay để đánh giá mức độ bảo mật phần cứng;

(ix) thực hiện đánh giá bảo mật dựa trên lưu vết ước lượng công suất tiêu thụ thu thập được ở bước (viii):

sử dụng kỹ thuật phân tích công suất tiêu thụ vi sai và phân tích công suất tiêu thụ tương quan để tìm ra khóa bí mật của thuật toán mã hóa, dựa trên một giả định về khóa bí mật, hai kỹ thuật phân tích này cho đánh giá giả định là đúng hoặc sai, theo đó nếu thiết kế không để lộ khóa bí mật khi áp dụng hai kỹ thuật phân tích này với các giả định khóa khác nhau, thì hệ thống được coi là có thể chống lại các tấn công dùng lưu vết công suất tiêu thụ; hoặc

sử dụng kỹ thuật đánh giá rò rỉ dùng véc-tơ kiểm tra để chỉ ra bước nào trong thuật toán làm rò rỉ thông tin từ lưu vết công suất tiêu thụ, phương pháp này sử dụng hàm T-Test trong xác suất thống kê để tính toán hệ số t theo thời gian với phương trình như sau:

$$t = \frac{\mu_0^2 - \mu_1^2}{\sqrt{\frac{s_0^2}{n_0} - \frac{s_1^2}{n_1}}}$$

trong đó:

μ_0 là giá trị trung bình của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 0,

μ_1 là giá trị trung bình của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 1,

s_0 là phương sai của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 0,

s_1 là phương sai của các mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 1,

n_0 là tổng số mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 0,

n_1 là tổng số mẫu lưu vết công suất tiêu thụ tại thời điểm t_i với bit thứ j bằng 1,

nếu hệ số $|t| > 4,5$ có nghĩa là có rò rỉ thông tin từ thiết kế, có thể phân biệt giữa các giả định đúng và giả định sai dựa vào hàm T-Test, trong đó:

nếu kết quả đánh giá mức độ bảo mật đạt yêu cầu, thì chuyển sang bước tiếp theo,

nếu kết quả đánh giá mức độ bảo mật chưa đạt yêu cầu, thì phải thực hiện lại quy trình thiết kế ở các bước (ii) hoặc bước (iv), cụ thể như sau:

nếu kết quả phân tích lưu vết công suất tiêu thụ sử dụng các kỹ thuật phân tích công suất tiêu thụ vi sai, phân tích công suất tiêu thụ tương quan không thể khôi phục khóa bí mật hoặc đánh giá rò rỉ công suất dùng véc-tơ kiểm tra không có sự rò rỉ thông tin với hệ số $|t| < 4,5$, thì chuyển sang các bước tiếp theo,

đối với các thiết kế không yêu cầu tính bảo mật phần cứng cao, kết quả phân tích lưu vết công suất tiêu thụ không cho phép khôi phục khóa bí mật nhưng chấp nhận có rò rỉ thông tin, tức là một số điểm hệ số $|t| > 4,5$;

đối với các thiết kế yêu cầu tính bảo mật phần cứng cao, thực hiện phân tích lưu vết công suất tiêu thụ sử dụng các hàm bậc cao;

đối với các thiết kế vi phạm các yêu cầu về bảo mật phần cứng, hiệu chỉnh lại quá trình tổng hợp phần cứng và tối ưu lô-gic ở bước (iv), khi việc này không giải quyết được vấn đề, thay đổi lại ở mức kiến trúc ở bước (ii);

(x) tích hợp thiết kế vào hệ thống để sẵn sàng sản xuất vi mạch.

2. Quy trình đánh giá mức độ bảo mật của phần cứng dựa trên lưu vết ước lượng công suất tiêu thụ theo điểm 1, trong đó đặc tả thiết kế mật mã/bảo mật tại bước

(i) còn bao gồm yêu cầu về mức độ bảo mật và bảo mật ở mức phần cứng gồm có khả năng chống lại một số loại tấn công vào phần cứng bao gồm tấn công sử dụng lưu vết công suất tiêu thụ hay sử dụng lưu vết điện từ trường hoặc tấn công bằng cách gây lỗi hệ thống.

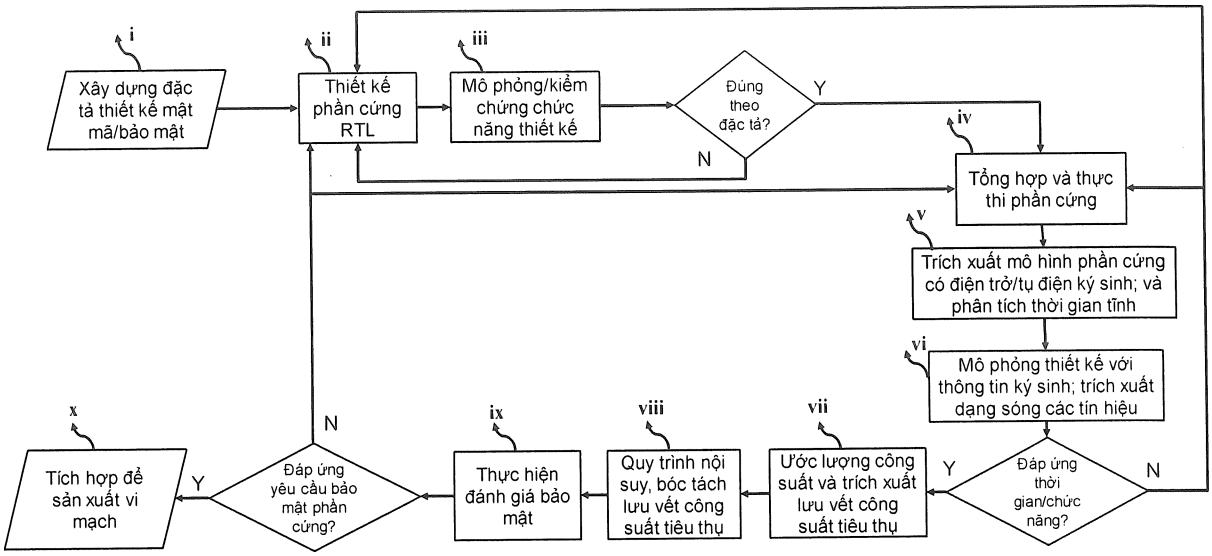
3. Quy trình đánh giá mức độ bảo mật phần cứng dựa trên lưu vết ước lượng công suất tiêu thụ theo điểm 1, trong đó bước (viii) nội suy và bóc tách các lưu vết ước lượng công suất tiêu thụ bao gồm các công đoạn sau:

(a) xác định các đoạn lưu vết ước lượng công suất tiêu thụ dùng để tấn công theo thời gian để loại bỏ các đoạn lưu vết ước lượng công suất tiêu thụ không sử dụng nhằm mục tiêu giảm số lượng dữ liệu cần xử lý và tăng tốc độ tính toán;

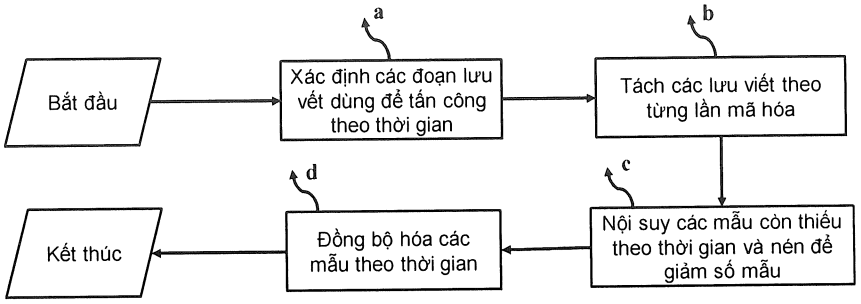
(b) tách các đoạn lưu vết công suất tiêu thụ theo từng lần mã hóa;

(c) nội suy các mẫu còn thiếu theo thời gian và nén để giảm số mẫu: lưu vết ước lượng công suất tiêu thụ chỉ lưu những thời điểm có công suất tiêu thụ thay đổi nên dữ liệu không dàn đều theo thời gian, trong đó thực hiện việc nội suy các điểm còn thiếu đảm bảo các lưu vết ước lượng công suất tiêu thụ có cùng số điểm dữ liệu;

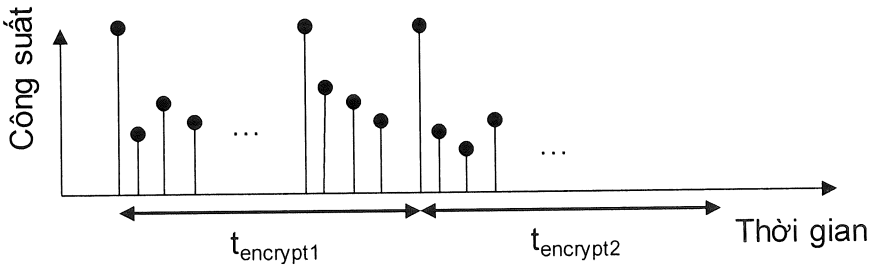
(d) đồng bộ hóa các mẫu để tăng hiệu quả của bài đánh giá, nếu các mẫu không đồng bộ về mặt thời gian, số lượng lưu vết cần dùng để thực hiện đánh giá tăng lên nhiều lần.



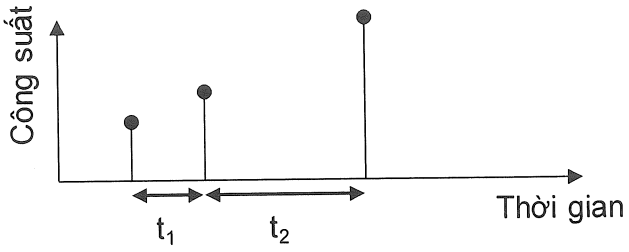
Hình 1



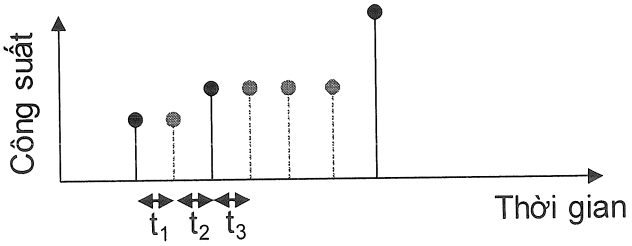
Hình 2



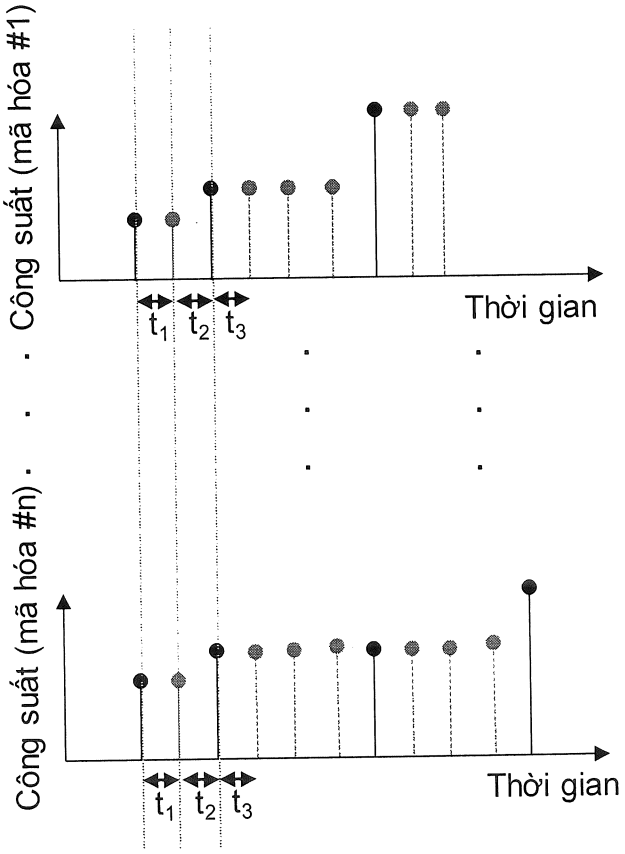
Hình 3



Hình 4



Hình 5



Hình 6