Phân tích, đánh giá hiệu quả các phương pháp mặt nạ chống tấn công DPA cho AES trên Smart Card

Nguyễn Thanh Tùng

***Tóm tắt*—Mặt nạ sử dụng giá trị ngẫu nhiên để che giá trị trung gian của thuật toán là phương pháp hiệu quả chống tấn công DPA. Có nhiều giải pháp mặt nạ cho thuật toán AES với mức độ an toàn và hiệu quả khác nhau. Bài báo phân tích, đánh giá ưu, nhược điểm, khả năng ứng dụng của các giải pháp này khi thực thi trên Smart Card. Đồng thời, đề xuất kỹ thuật mặt nạ nhúng, triển khai ứng dụng, đánh giá hiệu quả và khả năng chống tấn công DPA trên Smart Card.**

***Abstract*—Masking with the use of random values to mask the algorithm's intermediate value is an effective method to prevent DPA attacks. There are many masking solutions for AES algorithm with different levels of safety and effectiveness. The article analyzes and assesses advantages and disadvantages, the applicability of these solutions when implemented on Smart Card. Also, proposes embedded mask techniques, application deployment, evaluation of the effectiveness and resistance to DPA attacks on Smart Card.**

Từ khóa—Tấn công phân tích năng lượng vi sai; AES; thẻ thông minh; mặt nạ nhúng; FREM.

Keywords—Differential power analysis attack; AES; Smart Card; Embedded mask; FREM.

I. GIỚI THIỆU

Tấn công phân tích năng lượng vi sai (Difference Power Analysis attack - DPA attack) là loại tấn công khai thác năng lượng của thiết bị mật mã dựa vào kết quả sai khác giữa dữ liệu giả định và giá trị năng lượng thực tế đo được để tìm khóa bí mật [1], [7]. Với ưu điểm hiệu quả cao, không xâm lấn, giá thành rẻ, tấn công DPA là nguy cơ tiềm tàng ảnh hưởng đến sự an toàn của các thiết bị mật mã [1], [2], [9]. Khi tìm được khóa mật, kẻ tấn công có thể truy cập trái phép, giải mã, tạo chữ ký giả, giả mạo thông báo, nhân bản thiết bị…

Bài báo được nhận ngày 08/6/2020. Bài báo được nhận xét bởi phản biện thứ nhất ngày 11/8/2020 và được chấp nhận đăng ngày 11/8/2020. Bài báo được nhận xét bởi phản biện thứ hai ngày 04/8/2020 và được chấp nhận đăng ngày 04/8/2020.

Để chống tấn công DPA thì phải làm cho năng lượng tiêu thụ của thiết bị độc lập với giá trị trung gian thực của thiết bị. Kỹ thuật mặt nạ thực hiện che các giá trị trung gian của thuật toán bằng các giá trị ngẫu nhiên là giải pháp hiệu quả chống được tấn công DPA [3], [4]. Theo cách che giá trị trung gian, có thể chia kỹ thuật mặt nạ thành 4 loại: mặt nạ cố định, mặt nạ đầy đủ, mặt nạ nhân, mặt nạ biến đổi số học [14]. Bài báo phân tích, đánh giá phương pháp mặt nạ (Phần II), đề xuất thuật toán AES chống tấn công DPA dựa trên kỹ thuật mặt nạ nhúng (Phần III), xây dựng thực nghiệm đánh giá các phương pháp chống tấn công DPA lên AES trên Smart Card (Phần IV).

II. PHÂN TÍCH, ĐÁNH GIÁ PHƯƠNG PHÁP MẶT NẠ

Phương pháp mặt nạ che các giá trị trung gian của thuật toán bằng các giá trị ngẫu nhiên. Mặt nạ phải đảm bảo yêu cầu che được hết tất cả giá trị trung gian, phải tính trước, giám sát, làm chủ được sự hoạt động của mặt nạ và gỡ bỏ mặt nạ ở cuối quá trình tính toán.

Các loại mặt nạ cho thuật toán AES về cơ bản đều sử dụng phép tính XOR để gắn mặt nạ cho giá trị trung gian của thuật toán [9], [14]. Tuy nhiên, trong hoạt động SubBytes của AES có phép nghịch đảo là biến đổi phi tuyến nên không thể sử dụng phép XOR để gắn mặt nạ [8]. Vì vậy, các giải pháp công bố đều tập trung nghiên cứu, giải quyết mặt nạ cho biến đổi này. Các loại mặt nạ cố định thường tính trước giá trị mặt nạ cho cả bảng thế, mặt nạ nhân biến đổi phép kết hợp về phép nhân, mặt nạ biến đổi số học lại biểu diễn dữ liệu trên trường $GF(2^2)$ để thực hiện nghịch đảo.

A. Mặt nạ cố định

Phương pháp mặt nạ cố định FiM (Fix Mask) sử dụng q bộ mặt nạ cố định, lựa chọn ngẫu nhiên một bộ m_k trong tập các giá trị $\{m_0, \dots, m_{q-1}\}$ của q bộ để che dữ liệu đầu vào, che các giá trị trung gian trong quá trình mã hóa. Bảng dữ liệu cho S-box được tính trước, lưu trên

bộ nhớ cố định. Giá trị mặt nạ này được gỡ ra ở cuối lược đồ mã hóa [5].

Bảng dữ liệu cho S-box được kết hợp giữa q bộ mặt nạ và dữ liệu. Bảng này được tính trước và lưu trên bộ nhớ cố định. Với mỗi mặt nạ m_k cho 1 giá trị S-box S_k, được tính:

$$S_k[x] = S[x \oplus m_k] \oplus m_k,$$

$$\text{với } k \in \{0, .., q-1\}.$$

Tại AddRoundKey thực hiện phép tính:

$$(Ti,j \oplus m_k) \oplus Ki,j = (Ti,j \oplus Ki,j) \oplus m_k$$

Trong đó, T_{ij} là byte thứ j của trạng thái hiện tại trong vòng i, K_{ij} là byte khóa vòng.

Hoạt động ShiftRows biến đổi vị trí của byte của trạng thái vì vậy nó không thay đổi giá trị mặt nạ.

Với việc các mặt nạ lựa chọn ngẫu nhiên m_k của q bộ đã tính trước, thì kẻ tấn công không thể xác định được tham số cần thiết để khám phá dữ liệu và khóa được thuật toán. Phương pháp FiM đã che được tất cả giá trị trung gian của thuật toán bằng bộ mặt nạ ngẫu nhiên, có thể bảo đảm an toàn cho thuật toán AES trước tấn công DPA.

Tuy nhiên, do quá trình thực thi đòi hỏi nhiều thời gian và tốn 01 byte bộ nhớ cho mỗi mặt nạ, 256 byte bộ nhớ cho S-box nên FiM không phù hợp để ứng dụng với thiết bị có tài nguyên hạn chế như Smart Card [4]-[6].

B. Mặt nạ đầy đủ

Phương pháp mặt nạ đầy đủ FuM (Full Mask) sử dụng 06 mặt nạ khác nhau gồm:

02 mặt nạ m và m', để mặt nạ cho đầu vào và đầu ra của biến đổi SubBytes được tính dựa trên bảng tra cứu mặt nạ cho hộp thế S-box theo công thức:

$$Sm\,(x \oplus m) = S(x) \oplus m')$$

04 mặt nạ (m'_1, m'_2, m'_3, m'_4) được tính từ phép toán MixColumns cho (m_1, m_2, m_3, m_4) theo công thức:

$$MixColumns\,(m_1, m_2, m_3, m_4) = (m'_1, m'_2, m'_3, m'_4)$$

Khởi đầu mỗi vòng, che bản rõ d với các giá trị m'_i (m'_1, m'_2, m'_3, m'_4), che khóa k với mặt nạ (là kết quả phép XOR giữa m'_i và m). Biến đổi AddRoundKey thực hiện phép XOR giữa bản rõ và khóa.

Giá trị trung gian $(d \oplus k)$ được mặt nạ theo công thức:

$$(d \oplus m'_i) \oplus (k \oplus m \oplus m'_i) = (d \oplus k) \oplus m$$

Tiếp theo, tại biến đổi SubBytes, thực hiện che giá trị trung gian theo bảng S-box mặt nạ $Sm\,(x \oplus m) = S(x) \oplus m')$. Sau bước này, giá trị trung gian được che với mặt nạ m'.

Sau biến đổi ShiftRows, mặt nạ m' vẫn được giữ nguyên.

Trước MixColumns, tiến hành che bằng các mặt nạ m_i với m_1 tại hàng đầu tiên, sang m_2 tại hàng thứ 2, sang m_3 tại hàng thứ 3 và sang m_4 tại hàng thứ 4.

Biến đổi MixColumns thay đổi các mặt nạ m_i thành m'_i với $i = 1, \ldots, 4$. Lúc này giá trị trung gian được che với m'_i. Giá trị này được sử dụng để làm đầu vào cho các biến đổi của vòng tiếp theo cho đến vòng cuối cùng.

Vòng cuối không thực hiện phép biến đổi MixColumns. Tại điểm kết thúc của vòng cuối cùng, giá trị dữ liệu lúc này được che với mặt nạ m' (giá trị có được sau bước SubBytes và ShiftRows của mỗi vòng). Lúc này, khóa vòng cuối được che bởi mặt nạ m', khi thực hiện phép AddRoundKey cuối cùng nhận được bản mã (không mặt nạ). Như vậy, mặt nạ đã được gỡ bỏ tại đầu ra của thuật toán để giải mã.

Với việc sử dụng mặt nạ che cho tất cả giá trị trung gian của thuật toán AES, FuM đảm bảo an toàn, chống được tấn công DPA lên thuật toán AES.

Tuy nhiên, cũng như FiM, phương pháp FuM đòi hỏi nhiều thời gian và phải tính mặt nạ cho S-box, mặt nạ đầy đủ cho các vòng của thuật toán và cho lược đồ khóa. Phương pháp FuM sẽ tốn khoảng 8.000 bytes bộ nhớ. Như vậy, phương pháp FuM không phù hợp với với các thiết bị có tài nguyên hạn chế như Smart Card [2], [9].

C. Mặt nạ nhân

Dựa vào tính chất nghịch đảo của phép nhân theo công thức:

$$f^{-1}(x \times m) = (x \times m)^{-1} = f^{-1}(x) \times f^{-1}(m),$$

phương pháp mặt nạ nhân MM (Multiplicatve Mask) thực hiện các tích toán, biến đổi sao cho phép kết hợp mặt nạ trước khi nghịch đảo là phép

nhân, đảm bảo yêu cầu gỡ mặt nạ ở đầu ra để thuật toán hoạt động bình thường [3], [14].

Phương pháp mặt nạ nhân có hai lược đồ chính là mặt nạ nhân thích nghi và mặt nạ nhân cải tiến.

a) MM thích nghi

Để có kết quả biến đổi trong phép nghịch đảo cải tiến trên trường $GF(2^8)$ (chuyển từ giá trị A $\oplus$ X thành $A^{-1} \oplus X$), lược đồ MM sử dụng thêm giá trị ngẫu nhiên Y (Hình 1).

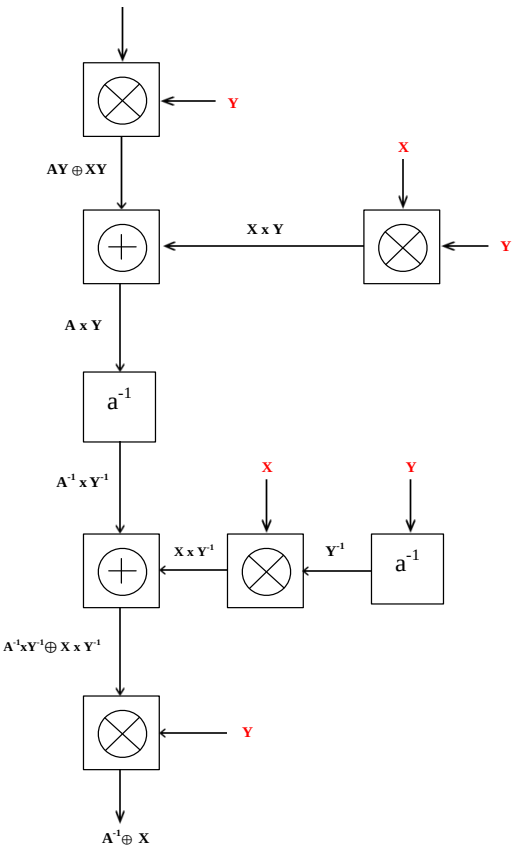
Sơ đồ MM thích nghi gồm các bước:

1/ Sinh giá trị ngẫu nhiên Y (8 bits), nhân giá trị đầu vào (A $\oplus$ X) với Y.

2/ Lấy giá trị Y nhân với giá trị mặt nạ X sau đó thực hiện phép tính XOR.

3/ Thực hiện nghịch đảo A x Y trong trường $GF(2^8)$.

4/ Từ đây, muốn có $A^{-1} \oplus X$, thực hiện 3 bước:



Hình 1. Sơ đồ MM thích nghi

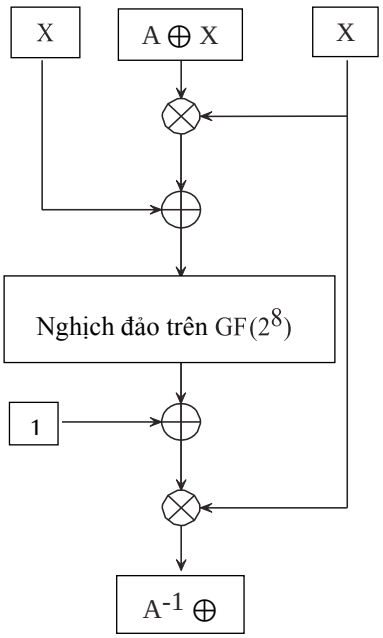
- Nghịch đảo giá trị Y
- Nhân Y^{-1} với mặt nạ X
- Thực hiện phép tính XOR giữa $(A \times Y)^{-1}$ và $X \times Y^{-1}$

5/ Nhân với Y

Kết quả thu được $A^{-1} \oplus X$ [12].

b) MM cải tiến

Để giải quyết vấn đề dung lượng, khả năng tính toán cho phù hợp với thuật toán AES trên Smart Card, sơ đồ MM cải tiến không sử dụng giá trị ngẫu nhiên Y, các biến đổi của sơ đồ được biểu hiện ở Hình 2.



Hình 2. Sơ đồ MM cải tiến

Thực hiện phép nghịch đảo qua 2 bước:

- Từ đầu vào giá trị $A \oplus X$ tính giá trị $A^{-1} \oplus X^{-1}$
- Biến đổi $A^{-1} \oplus X^{-1}$ thành giá trị $A^{-1} \oplus X$ [13].

Tuy đơn giản, đảm bảo yêu cầu về bộ nhớ cho Smart Card nhưng mặt nạ nhân lại phải đối mặt với tấn công giá trị zero khi bản rõ p trùng với khoá k, khi đó $p \oplus k = 0$, lúc này giá trị "0" không che được bằng cách nhân với giá trị mặt nạ ngẫu nhiên.

D. Mặt nạ biến đổi số học

Mặt nạ biến đổi số học AtM (Arithmetic Transform Mask) thực hiện biến đổi dữ liệu đầu vào trên trường $GF(2^8)$ sang trường $GF(2^4)$ và sang $GF(2^2)$ để thực hiện nghịch đảo (trong trường $GF(2^2)$ phép nghịch đảo tương đương với phép bình phương với: $(x^{-1} = x^2)$.

Lúc này, có thể ứng dụng phép tính XOR để che mặt nạ cho các giá trị trung gian, sau đó chuyển về trường $GF(2^8)$ để thực hiện các hoạt

động khác theo khuôn dạng của thuật toán [13], [14].

Phương pháp AtM che được hết giá trị trung gian, tuy nhiên với việc phải biến đổi, hạ bậc trường nhiều lần, biểu diễn dữ liệu trên các cấu trúc toán học khác nhau, thực hiện nhiều giá trị mặt nạ khác nhau đã làm tăng đáng kể thời gian thực thi và dung lượng của thiết bị, giải pháp này cũng chưa thật phù hợp để cài đặt, thực thi trên Smart Card chống tấn công DPA [12], [14].

Như vậy, các phương pháp mặt nạ được công bố trên không đủ điều kiện cả về an toàn và hiệu năng để chống tấn công DPA cho thuật toán AES thực thi trên thiết bị Smart Card. Để khắc phục những hạn chế đó, bài báo đề xuất giải pháp chống tấn công dựa trên kỹ thuật mặt nạ nhúng. Đề xuất thực hiện cụ thể đối với thuật toán AES, thực thi trên môi trường Smart Card.

III. THUẬT TOÁN AES CHỐNG TẤN CÔNG DPA DỰA TRÊN MẶT NẠ NHÚNG

Để đảm bảo cả về an toàn và hiệu năng cho thuật toán AES trên Smart Card chống tấn công DPA, bài báo đề xuất thuật toán AES mới sử dụng phương pháp mặt nạ nhúng, triển khai thực nghiệm tấn công DPA trên thiết bị Smart Card.

Phương pháp mặt nạ nhúng FREM (Field Ring Embeded Mask) là sự kết hợp của quá trình tính toán, biến đổi trên trường mở rộng, nhúng vào vành, xử lý trên vành và chiếu ngược lại. Mục đích của phương pháp là giải quyết vấn đề nghịch đảo trong biến đổi SubBytes của thuật toán AES. Với đầu vào là giá trị trung gian đã được mặt nạ:

$$f(a) \oplus f(m), a, m \in GF(2^8), f: GF(2^8) \rightarrow GF((2^4)^2)$$

đầu ra là giá trị trung gian đã nghịch đảo với giá trị mặt nạ:

$$f(a^{-1}) \oplus f(m),$$

Với phép ánh xạ giá trị dữ liệu trên trường $GF((2^4)^2)$, thành giá trị tính toán trên vành $GF(2^4)[x]/PQ$, qua phép ánh xạ ngẫu nhiên ρ sao cho:

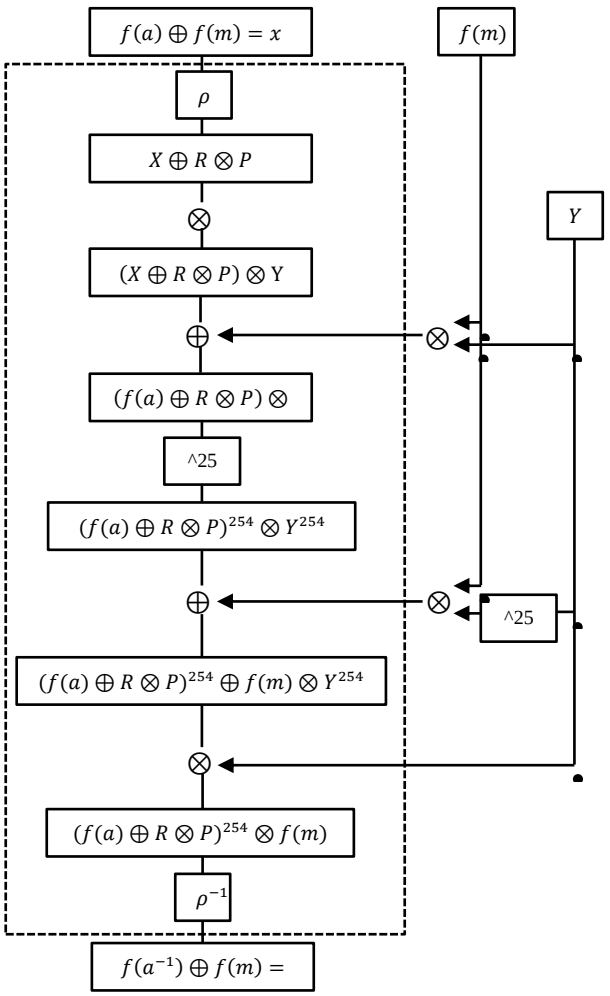
$$\rho(X) = X \oplus RP \bmod PQ$$

thì một giá trị "0" trên trường $GF(2^8)$ được ánh xạ lên 2^k giá trị ngẫu nhiên có thể trong R.

Phương pháp này tăng độ phức tạp tính toán, chống tấn công giá trị zero [4], [11].

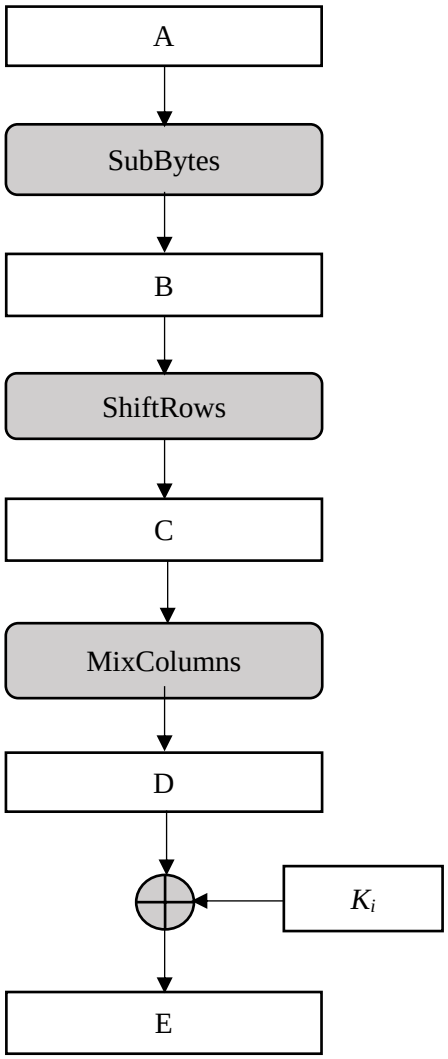
Phép ánh xạ từ giá trị (a $\oplus$ m) thành giá trị $f(a) \oplus f(m)$ = X trong khung FREM gồm các phép tính:

- Chuyển giá trị X sang giá trị X $\oplus$ $R \otimes P$
- Nhân với giá trị ngẫu nhiên 8 bit Y
- Cộng giá trị thu được với tích (Y $\otimes$ $f(m)$) qua đó triệt tiêu được giá trị $f(m)$
- Thực hiện phép mũ 254
- Cộng giá trị thu được với $Y^{254} \otimes f(m)$
- Nhân giá trị thu được với Y
- Thực hiện phép ánh xạ ngược từ vành sang trường để thu về $f(a^{-1}) \oplus f(m)$.



Hình 3. Sơ đồ FREM cho thuật toán AES

So sánh lược đồ thuật toán AES (Hình 4) và thuật toán AES ứng dụng kỹ thuật FREM (Hình 5), có thể thấy hai lược đồ có các bước biến đổi tương tự nhau. Điểm khác nhau là, thuật toán AES ứng dụng FREM thay thế biến đổi SubBytes bằng các biến đổi FREM và AFFINE.



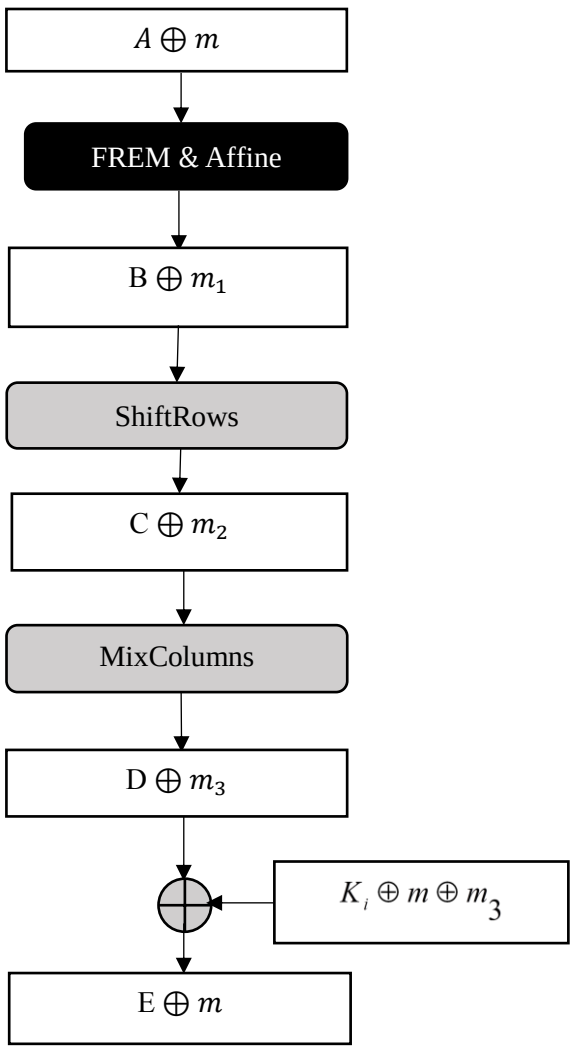
Hình 4. Lược đồ thuật toán AES

Quan sát lược đồ thuật toán AES ta thấy các giá trị trung gian A, B, C, D, E (Hình 4) chưa được mặt nạ, mã thám sẽ tấn công DPA lên các giá trị trung gian này để khai thác khóa bí mật của thuật toán.

Sau khi thực hiện mặt nạ cho thuật toán AES ứng dụng kỹ thuật mặt nạ nhúng FREM, các giá trị trung gian A, B, C, D, E đều được che bởi mặt nạ m, m_1, m_3, m_3 (Hình 5).

Đối chiếu với các yêu cầu của mặt nạ gồm: mặt nạ phải che các giá trị trung gian của thuật toán bằng các giá trị ngẫu nhiên; mặt nạ phải tính trước, phải được giám sát; khi thực thi phải làm chủ được sự hoạt động của mặt nạ và phải gỡ bỏ mặt nạ ở cuối quá trình tính toán.

Như vậy, kỹ thuật FREM đảm bảo an toàn cho thuật toán AES trước tấn công DPA, đồng thời đảm bảo các yêu cầu khi thực thi mặt nạ.

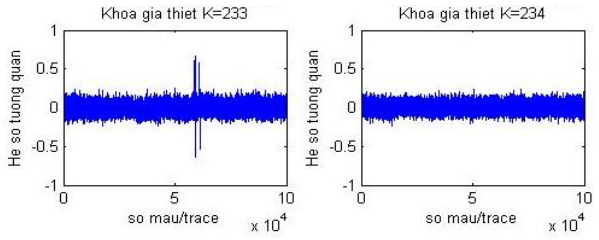


Hình 5. Lược đồ thuật toán AES sử dụng FREM

IV. THỰC NGHIỆM ĐÁNH GIÁ CÁC PHƯƠNG PHÁP CHỐNG TẤN CÔNG DPA LÊN AES TRÊN SMART CARD

Để đánh giá kết quả, bài báo thực hiện tấn công DPA lên các thuật toán AES-128, AES với FiM, FuM, MM, AtM và thuật toán AES với FREM cài đặt trên Smart Card Atmega168PA. Thiết bị gồm vi xử lý Microchip picoPower 8-bit AVR RISC, bộ nhớ flash 16KB, 512B EEPROM, 20 KB SRAM.

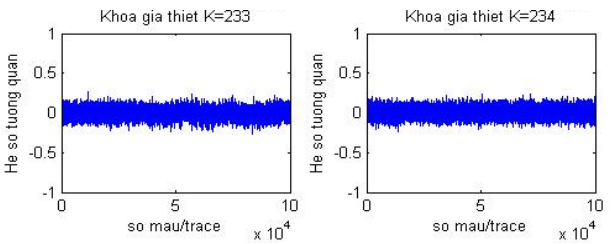
Kết quả đối với AES-128 khi thực hiện tấn công DPA khi thu thập trên 480 bản rõ, với độ dài mỗi vết là 10.000 mẫu, thu được kết quả tấn công thành công với biểu đồ vi sai có gai nhọn tương ứng với khóa đúng của thuật toán. Trong trường hợp này là khóa đúng 233. Biểu đồ vi sai với khóa đúng 233 và khóa 234 được thể hiện ở Hình 6.



Hình 6. Biểu đồ vi sai tấn công DPA lên AES-128

Khi tấn công lên AES-128 có thực hiện FuM, MM, AtM với kỹ thuật, thiết bị và phạm vi tương tự thì không phát hiện được khóa đúng, không có gai nhọn ở biểu đồ vi sai.

Tiếp theo, bài báo thực hiện tấn công DPA lên thuật toán AES-128 cài đặt kỹ thuật mặt nạ nhúng FREM với kỹ thuật, thiết bị và phạm vi tương tự. Kết quả biểu đồ vi sai cũng không xuất hiện gai nhọn (Hình 7). Qua đó khẳng định, trong tình huống này DPA không tấn công thành công lên AES FREM.



Hình 7. Biểu đồ vi sai tấn công DPA lên AES có FREM

Kết quả thực thi các sơ đồ mặt nạ, thời gian và dung lượng các bộ nhớ khi thực thi các sơ đồ được thể hiện qua Bảng 1.

BẢNG 1. SO SÁNH CÁC SƠ ĐỒ THỰC THI MẶT NẠ

Sơ đồ thực thi	Thời gian tại 3,58 MHz	Bộ nhớ ROM (bytes)	Bộ nhớ RAM (bytes)
AES bình thường	18,1 ms	730	42
AES có FuM	78,3 ms	3795	4250
AES có AtM	58,7 ms	1752	121
AES có MM	37,8 ms	732	46
AES có FREM	25,5 ms	734	48

Theo kết quả ở Bảng 1, các sơ đồ AES có FuM, AtM tốn nhiều tài nguyên, không phù hợp với dung lượng của thiết bị có tài nguyên hạn chế như Smart Card.

Sơ đồ AES có FREM tốn 734 bytes ROM và 48 bytes RAM. Như vậy, hiệu năng của thuật toán AES có FREM phù hợp với dung lượng của thiết bị Smart Card hiện nay.

V. KẾT LUẬN

Bài báo đã đánh giá các phương pháp mặt nạ chống tấn công DPA. Phương pháp cố định FiM và mặt nạ đầy đủ FuM có độ an toàn cao nhưng tốn nhiều tài nguyên (do phải tính trước và lưu mặt nạ cho bảng thế), không phù hợp với Smart Card.

Phương pháp mặt nạ nhân MM sử dụng tính chất nghịch đảo của phép nhân để mặt nạ, bảo đảm được tài nguyên cho thiết bị nhưng không kháng được tấn công giá trị zero.

Phương pháp mặt nạ biến đổi số học AtM sử dụng phép bình phương trên trường $GF(2^2)$, thay thế phép nghịch đảo đảm bảo an toàn, chống được tấn công zero nhưng lại gây hiệu ứng cả về thời gian và tài nguyên, không phù hợp với thiết bị có tài nguyên hạn chế như Smart Card.

Đồng thời, bài báo trình bày kỹ thuật mặt nạ nhúng FREM. Thuật toán AES sử dụng kỹ thuật mặt nạ nhúng FREM với các lý thuyết biểu diễn trên trường mở rộng, nhúng trường sang vành, chiếu ngược lại, xử lý trên vành tăng độ phức tạp tính toán, chống tấn công giá trị zero. Lược đồ kết hợp mặt nạ đầy đủ và kỹ thuật mặt nạ nhúng FREM đã che được hết tất cả các giá trị trung gian của thuật toán, chống được tấn công DPA. Bên cạnh đó, lược đồ bảo đảm dung lượng để thực thi trên thiết bị có tài nguyên hạn chế như Smart Card.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Hồng Quang, "Phân tích tiêu thụ điện năng của thiết bị mật mã", Tạp chí nghiên cứu Khoa học và Công nghệ Quân sự, vol. 34 12/2014, pp 87-93, 2014.

[2] Nguyễn Thanh Tùng, "Một giải pháp chống tấn công DPA hiệu quả", Tạp chí nghiên cứu Khoa học và Công nghệ Quân sự, vol. 5/2017, pp 33-41, 2017.

[3] Nguyễn Thanh Tùng, Trần Ngọc Quý, "Mặt nạ nhân chống tấn công DPA lên AES trên Smart Card", Tạp chí nghiên cứu khoa học – Đại học Sư phạm Hà Nội, vol. 5/2019.

[4] Nguyễn Thanh Tùng, Bùi Văn Dương, "Một phương pháp hiệu quả chống tấn công DPA lên AES trên Smart Card", Tạp chí Nghiên cứu Khoa học và Công nghệ Quân sự, 2019.

[5] Kouichi Itoh, Masahiko Takenaka, and Naoya Torii, "DPA countermeasure based on the "masking method", In KwangjoKim, editor, ICISC**,** volume 2288 of Lecture Notes in Computer Science, Springer, 2001**.**

[6] Xiaoan Zhou, Juan Peng anh Liping Guo, "An Improved AES Masking Method Smartcard Implementation for Resisting DPA Attacks", International Journal of Computer Science, 2013.

[7] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis", proceedings of crypto 99, Lecture Notes in Computer Science, vol. 1666, Springer, pp. 388–397, 1999.

[8] National Institute of Standards and Technology (NIST). FIPS-197 "Advanced Encryption Standard", November, 2001.

[9] Stefan Mangard, Elisabeth Oswald, and Thomas Popp, "Power Analysis Attacks Revealing the Secrets of Smart Cards", Graz University of Technology Graz, 2007.

[10] Department of the Army Washington DC, "Basic Cryptanalysis" Field Manual 34-40-2, 1990.

[11] Jovan Dj. Golic, Christophe Tymen, **"**Multiplicative Masking and Power Analysis of AES Cryptographic Hardware and Embedded Systems – CHES 2002, vol. 2523 of Lecture Notes in Computer Science, pp. 198–212, Springer-Verlag, 2003.

[12] M. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks", Springer-Verlag Berlin Heidelberg, 2001

[13] Elena Trichina, Domenico De Seta, and Lucia Germani, "Simplified Adaptive Multiplicative Mask for AES", Cryptographic Design Center, Gemplus Technology R & DVia Pio Emanuelli 1, 00143 Rome, Italy, 2003.

[14] Johannes Wolkerstorfer, Elisabeth Oswald, and Mario Lamberger, "An ASIC Implementation of the AES Sboxes", Institute for Applied Information Processing and Communications, Graz University of Technology, Inffeldgasse 16a, A-8010 Graz, Austria, 2005.

[15] Christof Parr, "Effcient VLSI Architectures for Bit Parallel Computation in Galois Fields" ECE Department, Worcester Polytechnic Institute, 100 Institute Road, Worcester,MA 01609 USA, 1994.

[16] Johannes Blömer, Jorge Guajardo, and Volker Krummel, "Provably Secure Masking of AES", ResearchGate, 2004.

SƠ LƯỢC VỀ TÁC GIẢ

ThS. Nguyễn Thanh Tùng

Đơn vị công tác: Học viện Kỹ thuật mật mã

Email: tungkmm@gmail.com

Quá trình đào tạo: Nhận bằng Kỹ sư năm 2000, nhận bằng Thạc sĩ năm 2008 tại Học viện Kỹ thuật mật mã.

Hướng nghiên cứu hiện nay: Tấn công và chống tấn công lên thiết bị mật mã.