MỘT PHƯƠNG PHÁP HIỆU QUẢ CHỐNG TẤN CÔNG DPA LÊN AES TRÊN SMART CARD

Nguyễn Thanh Tùng[1] và Bùi Văn Dương[2]

[1]*Trung tâm Thực hành Kĩ thuật Mật mã, Học viện Kĩ thuật Mật mã*

[2]*Lớp AT13i, Học viện Kĩ thuật Mật mã*

Tóm tắt: Mặt nạ kết hợp trên trường mở rộng giải quyết được vấn đề an toàn và có hiệu năng phù hợp với những thiết bị có tài nguyên hạn chế. Bài báo trình bày cơ sở lý thuyết, phương pháp tính toán, nghịch đảo trên trưởng mở rộng đồng thời đề xuất sơ đồ mặt nạ cho thuật toán AES trên Smart Card chống tấn công DPA.

Từ khóa: DPA, AES, trường mở rộng, mặt nạ, giá trị trung gian, Smart Card.

1. Mở đầu

Tấn công phân tích năng lượng là một loại tấn công kênh kề, không xâm lấn. Kẻ tấn công khai thác năng lượng của thiết bị mật mã để tìm ra khóa mã. Quá trình tấn công với việc đo và phân tích tiêu thụ điện năng không cần chi phí lớn nhưng đặc biệt hiệu quả, các thiết bị mật mã khi đối mặt với tấn công phân tích năng lượng thường không bị hư hại và các tham số không bị thay đổi nên rất khó có thể nhận biết thiết bị đang bị tấn công [1, 8].

Bài báo *"Một giải pháp chống tấn công DPA hiệu quả"* [2] đã trình bày sơ đồ mặt nạ đầy đủ chống tấn công DPA trên AES, tuy nhiên, sơ đồ mặt nạ đầy đủ cần số lượng lớn về bộ nhớ và thời gian, không phù hợp với các thiết bị nhỏ như Smart Card.

Bài báo "*Mặt nạ nhân chống tấn công DPA lên AES trên Smart Card"* [3] đề xuất phương pháp mặt nạ nhân bao gồm: mặt nạ nhân thích nghi và mặt nạ nhân đơn giản chống tấn công DPA lên thuật toán AES trên Smart Card; Mặt nạ nhân với sự gọn nhẹ đã giải quyết được vấn đề hiệu suất, tuy nhiên phương pháp này lại đối mặt với kiểu tấn công giá trị zero (khi bản rõ và khóa như nhau).

Để khắc phục các vấn đề nêu trên, chúng tôi đề xuất phương pháp mặt nạ cho AES qua các phép biến đổi gồm: biểu diễn các giá trị trung gian trên trường $GF(2^8)$ như mở rộng bậc 2 của trường $GF(2^4)$, nhúng trường sang vành, thực hiện phép mũ thay thế nghịch đảo và chiếu ngược lại. Giải pháp đề xuất đã khắc phục được điểm yếu của mặt nạ nhân trước tấn công giá trị zero, đồng thời giảm được đáng kể dung lượng, chi phí cho thiết bị so với mặt nạ đầy đủ, phù hợp cài đặt, thực thi thuật toán AES trên Smart Card chống tấn công DPA.

2. Nội dung nghiên cứu

2.1. Phương pháp mặt nạ chống tấn công DPA lên thuật toán AES trên Smart Card

AES [4, 5, 7] là một mã khối, có độ dài khối bằng 128 bit và các độ dài khóa bằng 128, 192 hay 256 bit. Với thiết kế sử dụng các phép thay thế và hoán vị nên AES có thể kháng được tấn công, tạo ưu thế về tốc độ, dung lượng và đơn giản trong thiết kế và được đánh giá là hệ mã mạnh. Smart Card thực thi AES được sử dụng rộng rãi trên nhiều lĩnh vực như an ninh quốc gia, truyền thông, tài chính, ngân hàng….

Tấn công DPA khai thác năng lượng tiêu thụ thực tế của thiết bị mật mã dựa vào giá trị trung gian mà nó xử lý trong quá trình thực hiện thuật toán mật mã. Dù được đánh giá là hệ mã mạnh, kháng được các loại tấn công đã biết, nhưng AES vẫn không kháng được tấn công DPA. Với chiến lược thu vết năng lượng tiêu thụ, xây dựng tập giá trị trung gian giả định, phân tích, so sánh qua đó khai thác được khóa bí mật của thuật toán, DPA đã thám thành công khóa của thuật toán AES qua 13 vết năng lượng [6, 8].

Để chống được 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. Tấn công DPA hoạt động dựa trên việc năng lượng tiêu thụ của thiết bị mật mã phụ thuộc vào giá trị trung gian v mà nó xử lý. Khi che giá trị trung gian v với mặt nạ m (ngẫu nhiên) thì giá trị trung gian mà kẻ tấn công thu được v_m độc lập với v, vì vậy năng lượng tiêu thụ của v_m cũng độc lập với năng lượng tiêu thụ của v. Do vậy, kẻ tấn công không khai thác chính xác được giá trị trung gian "thực" của thuật toán [6].

Tùy theo từng thuật toán với các phép tính thực hiện mà có thể sử dụng mặt nạ Boolean, mặt nạ Arithmetic hay kết hợp [8].

Thuật toán AES có sử dụng cả hàm Boolean và hàm Arithmetic, các phép AddRounKeys, MixColumns, ShiftRows là các biến đổi tuyến tính nên dễ dàng sử dụng mặt nạ Boolean để che. Riêng biến đổi SubBytes thực hiện hai phép tính (nghịch đảo và biến đổi affine). Phép nghịch đảo là phép biến đổi phi tuyến ($f^{-1}(x \oplus m) \neq f^{-1}(x) \oplus f^{-1}(m)$) nên không thể sử dụng phép tính Boolean để mặt nạ. Các giải pháp đã và đang được nghiên cứu, đề xuất đều tập trung vào mặt nạ cho phép biến đổi này.

Lược đồ mặt nạ đầy đủ [2] sử dụng mặt nạ S-Box, $S_m(x \oplus m) = S(x) \oplus m$, tuy nhiên phương pháp đòi hỏi thiết bị phải có tài nguyên lớn không phù hợp với Smart Card.

Lược đồ mặt nạ nhân [3] sử dụng tính chất nghịch đảo của phép nhân trên trường hữu hạn theo công thức: $f^{-1}(x \text{ x } m) = (x \text{ x } m)^{-1} = f^{-1}(x) \text{ x } f^{-1}(m)$ để tính toán, nghịch đảo. Lược đồ này đã giải quyết được vấn đề hiệu năng, tuy nhiên mặt nạ nhân lại phải đối mặt với tấn công giá trị zero (khi bản rõ và bản khóa bằng nhau dẫn đến giá trị trung gian bằng "0" – không có nghịch đảo).

Với những đánh giá trên, bài báo đề xuất phương pháp mới vừa chống được tấn công DPA, tấn công giá trị zero, đồng thời có hiệu năng phù hợp với thiết bị tài nguyên hạn chế như Smart Card.

2.2 Đề xuất sơ đồ mask hiệu quả chống tấn công DPA lên AES trên Smart Card

2.2.1. Cơ sở lý thuyết

a. Biến đổi trên trường hữu hạn

Biểu diễn trường $GF(2^8)$ như một trường mở rộng bậc 2 của trường $GF(2^4)$ theo công thức:

$$a \cong a_h x + a_l, \quad a_h, a_l \in GF(2^4) \tag{1}$$

Phép biến đổi $f: GF(2^8) \to GF((2^4)^2)$ được định nghĩa:

$$f(a) = a_h x + a_l \tag{2}$$

Phép biến đổi $f^{-1}: GF((2^4)^2) \to GF(2^8)$ được định nghĩa như sau:

$$f^{-1}(a_h x + a_l) = a \tag{3}$$

Đa thức bất khả quy của $f(a)$ lúc này là đa thức bất khả quy bậc hai $P(x)$:

$$P(x) = x^2 + \{1\}x + \{e\} \tag{4}$$

Với $\{e\} \in GF(2^4)$ sao cho $P(x)$ nguyên tố [11].

b. Tính toán nghịch đảo

Nghịch đảo trên trường mở rộng bất kỳ $GF((2^n)^m)$ tương đương với phép lấy mũ theo công thức:

$$a^{-1} = \left(a^{2^{m.n}-2}\right) (mod\ P), a \in\ GF((2^n)^m) \tag{5}$$

Trong $GF((2^4)^2)$, phép nghịch đảo có thể tính [12], với $P(x)$ từ (4):

$$a^{-1} = a^{254}\ \left(mod\ P(x)\right), a \in\ GF((2^4)^2) \tag{6}$$

c. Nhúng trường vào vành và chiếu ngược từ vành sang trường

Ta biểu diễn trường mở rộng $GF((2^4)^2)$ như vành đa thức biến x với hệ số thuộc $GF(2^4)$ có modulo là đa thức bất khả quy $P(x)$ tại (4). Cho $Q(x)$ là một đa thức bất khả quy bậc k với hệ số thuộc $GF(2^4)$, nguyên tố cùng nhau với $P(x)$. Ta có $GF((2^4)^2)$ là một trường con của vành $\mathcal{R} = GF(2^4)[x]/PQ$, $\mathcal{R}$ đẳng cấu với $GF((2^4)^2) \times GF((2^4)^k)$ qua phép đẳng cấu $U \to (U_P, U_Q)$, với hai tọa độ U_p, U_Q được định nghĩa bởi $U_P = U\ mod\ P(x)$ và $U_Q = U\ mod\ Q(x)$ [10].

Để chống tấn công giá trị zero lên sơ đồ mặt nạ nhân (giá trị zero ("0") xuất hiện khi byte bản rõ bằng byte khóa), ta sử dụng phép ánh xạ ngẫu nhiên $\rho: GF((2^4)^2)\ \to \mathcal{R}$ được định nghĩa như sau:

$$\rho(X) =\ X\ +\ RP\ mod\ PQ \tag{7}$$

Với R là đa thức ngẫu nhiên bậc nhỏ hơn k (k bit) và có hệ số thuộc $GF(2^4)$, $\rho(X)$ là một giá trị ngẫu nhiên trên $\mathcal{R}$. Khi thực hiện phép ánh xạ này mỗi giá trị "0" trên $GF((2^4)^2)$ được ánh xạ sang 2^k giá trị ngẫu nhiên trên vành $\mathcal{R}$. Như vậy, với việc có thể điều chỉnh k, khi thực hiện phép tính này sẽ tăng độ phức tạp tính toán khi thực hiện tấn công zero. Với bất kì giá trị nào của R, ta có thể ánh xạ ngược lại trường mở rộng $GF((2^4)^2)$ với phép ánh xạ $\rho'(U) = U\ mod\ P(x)$ loại bỏ giá trị ngẫu nhiên R vì $RP\ \equiv 0\ mod\ P$.

d. Xử lý trên vành

Đối với phép nhân và cộng trừ trên $\mathcal{R}$, ta xử lý tương đương với phép nhân và cộng trừ đa thức với đa thức bất khả quy $P(x)Q(x)$. Vì vành đóng với các phép tính và đẳng cấu với $GF((2^4)^2) \times GF((2^4)^k)$ nên thực hiện các phép tính trong vành tương đương với việc thực hiện các phép tính lên hai tọa độ trong đẳng cấu của nó.

Theo lý thuyết tính toán nghịch đảo (6), việc tính phần tử nghịch đảo trong trường cũng tương đương việc lấy mũ 254, phù hợp để triển khai trên vành bởi $\mathcal{R}$ tồn tại phép nhân nhưng không tồn tại phép nghịch đảo. Việc tác động lên $\mathcal{R}$ cũng tương đương với việc tác động lên hai tọa độ trong đẳng cấu $GF((2^4)^2) \times GF((2^4)^k)$ của $\mathcal{R}$.

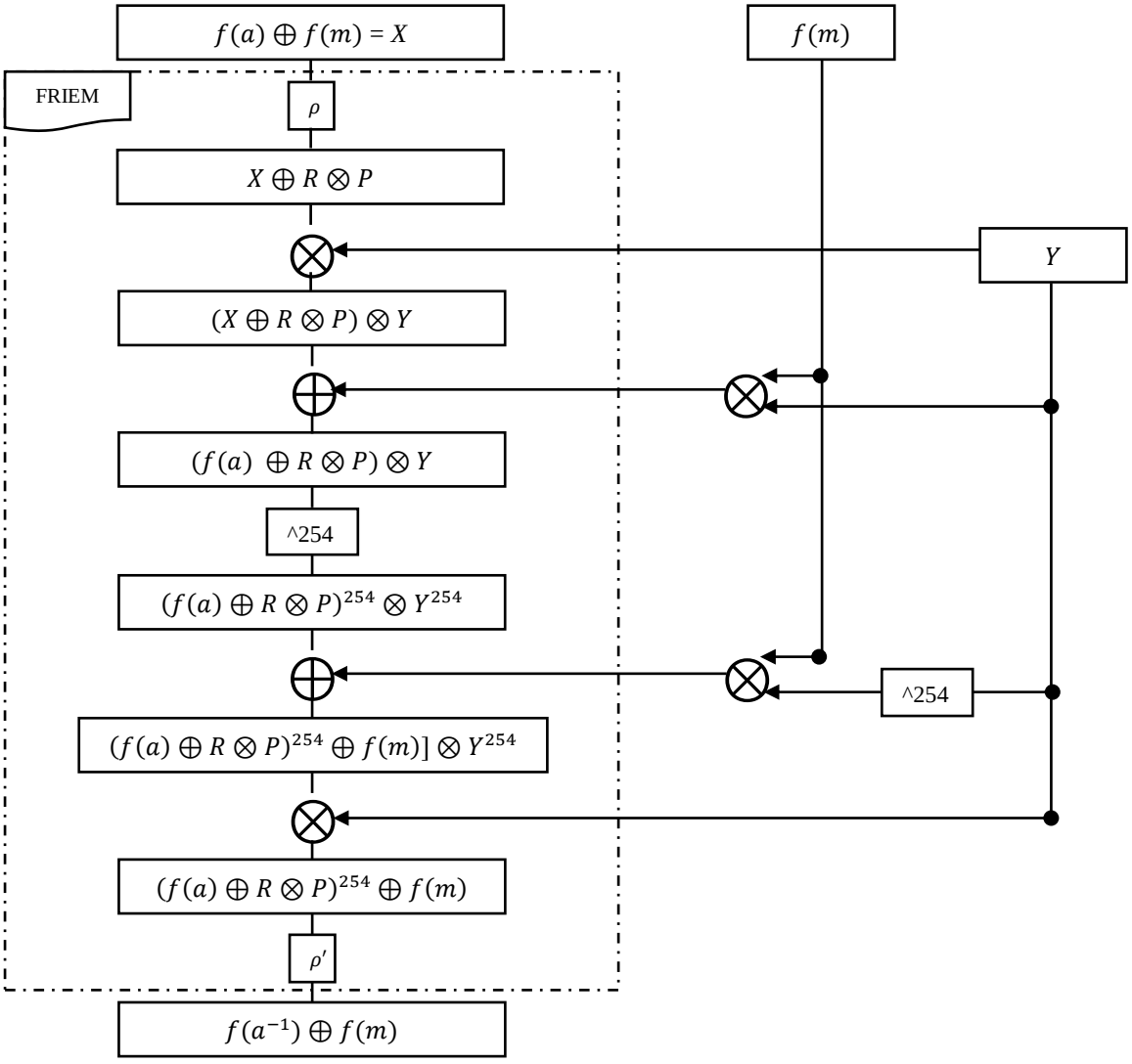
Định nghĩa phép ánh xạ $F: \mathcal{R} \to \mathcal{R}, F(U) = U^i \ mod \ PQ$. Để $U_Q = U \ mod \ Q$ không trở thành phần tử đơn vị sau phép biến đổi F, cần chọn i phù hợp với từng giá trị k. Với $k = 8$, $U_Q^{254} \equiv 1 \ mod \ Q$, nên chọn $i = 509$. Với $k \neq 8$, chọn $i = 254$, $F: F(U) = U^{254}$.

Bởi tồn tại đẳng cấu $U \to (U_P, U_Q)$, $F(U) = F(U_P, U_Q) = (U_P^{254}, U_Q^{254})$, F tác động lên U_P tương đương phép lấy nghịch đảo.

2.2.2. Đề xuất FRIEM chống tấn công DPA lên AES trên SmartCard

a. Sơ đồ đề xuất

Phương pháp FRIEM (Field Ring Inversion 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 $f(a) \oplus f(m), a, m \in GF(2^8), f: GF(2^8) \to GF((2^4)^2)$, đầu ra là giá trị trung gian đã nghịch đảo với giá trị mặt nạ $f(a^{-1}) \oplus f(m)$, (Hình 1).



Hình 1: Sơ đồ FRIEM cho thuật toán AES

Phép ánh xạ từ giá trị (a $\oplus$ m) thành giá trị $f(a) \oplus f(m)$ = X được thực hiện theo công thức (2).

Trong khung FRIEM gồm các phép tính:

- Chuyển giá trị X sang giá trị X $\oplus$ $R \otimes P$ theo công thức (7)

- Nhân với giá trị ngẫu nhiên 8 bít Y

- Cộng giá trị thu được với tích (Y X $f(m)$) qua đó triệt tiêu được giá trị $f(m)$

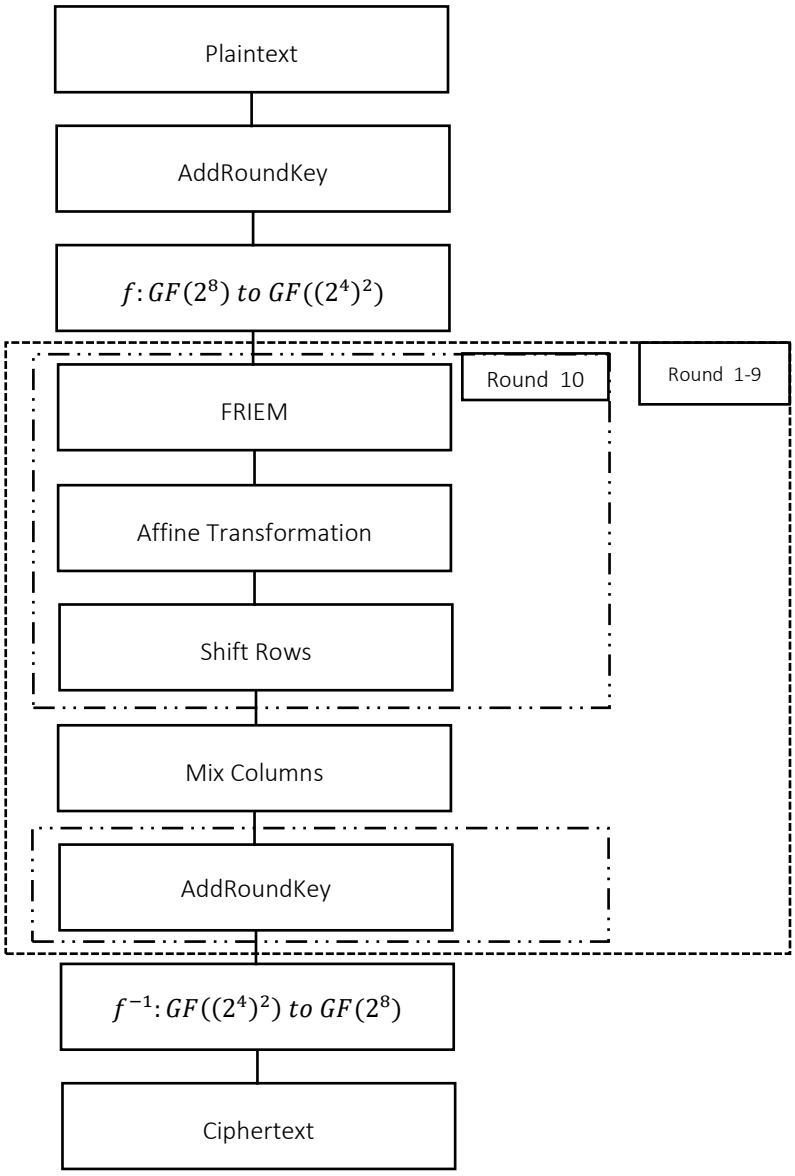
- Thực hiện phép mũ 254 theo công thức (6)

- 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 $f(a^{-1}) \oplus f(m)$ theo công thức (3)

Thuật toán AES sử dụng mặt nạ FRIEM được thực thi theo sơ đồ Hình 2, trong đó khối FRIEM được trình bày tại phần trên.



Hình 2: Sơ đồ thuật toán AES sử dụng mặt nạ FRIEM

Các bước thực hiện như sau:

- Bản rõ đầu vào được cộng khóa tại bước AddRoundkey;

- Biến đổi giá trị trung gian về trường $GF((2^4)^2)$;

- Xử lý theo sơ đồ FRIEM;

- Thực hiện biến đổi Affine, ShiftRow, MixColumn và AddRoundkey trong trường $GF((2^4)^2)$;

- Ở vòng cuối cùng không có biến đổi MixColumn, sau khi ra khỏi vòng thực hiện đưa giá trị trung gian từ $GF((2^4)^2)$ về $GF(2^8)$;

- Trả bản mã ở đầu ra.

b. Đánh giá

- Vấn đề an toàn

Mặt nạ thực hiện che giá trị trung gian của thuật toán mật mã bằng giá trị ngẫu nhiên để chống tấn công DPA, vấn đề an toàn của mặt nạ đã được trình bày tại [13]. Để đảm bảo an toàn cho sơ đồ FRIEM đề xuất, phải chỉ ra các phép biến đổi của sơ đồ của đề xuất như thay đổi cách biểu diễn trên trường, nhúng vào, chiếu ngược lại và xử lý trên vành không ảnh hưởng đến sự an toàn của mặt nạ.

Với xử lý trên trường, Trichina trong bài báo đánh giá mặt nạ kết hợp [14] đã chỉ ra rằng việc đưa về $GF((2^4)^2)$ vẫn giữ nguyên được khả năng chống tấn công DPA của mặt nạ. Sơ đồ FRIEM bài báo đề xuất khác sơ đồ mặt nạ kết hợp ở cách xử lý Sbox với việc thêm phép nhúng trường để chống tấn công giá trị zero, nên phải chỉ ra tính an toàn của bước này.

Phép ánh xạ ρ: $\rho(X) = X + RP$ nhúng từ trường $GF((2^4)^2)$ sang $\mathcal{R}$, lúc này giá trị $X = f(a + m)$ trong đó f: $GF(2^8) \rightarrow GF((2^4)^2)$. Do f độc lập với giá trị trung gian $a \in GF(2^8)$ nên $\rho(X) = X + RP$ cũng độc lập với $f(a)$.

Các bước xử lý trên $\mathcal{R}$, tương tự như mặt nạ nhân thích nghi [3] với đầu vào $\rho(X) = X + RP$. Để đánh giá an toàn, ta chỉ ra 2 giá trị trung gian $(X + RP) \times Y$ và $(f(a) + RP) \times Y$ độc lập với $f(a)$ (với Y là giá trị ngẫu nhiên độc lập với $f(a)$ có phân bố đều trên $GF((2^4)^2)$).

Với giá trị trung gian $(X + RP) \times Y$, ta thấy: giá trị này độc lập với $f(a)$ bởi $X, X + RP, Y$ đều độc lập với $f(a)$.

Với giá trị trung gian thứ hai, $(f(a) + RP) \times Y$, có $f(a) + RP$ độc lập với $f(a)$ với $deg(RP) \geq deg(f(a))$, kéo theo $(f(a) + RP) \times Y$ cũng độc lập với $f(a)$ với Y độc lập với $f(a)$. Cả $(X + RP) \times Y$ và $(f(a) + RP) \times Y$ đồng thời có phân bố theo phân phối của $R \times Y$.

Như vậy, quá trình thực hiện phép nhúng từ trường $GF((2^4)^2)$ sang vành $\mathcal{R} = GF(2^4)[x]/P(x)Q(x)$, phép chiếu ngược lại và các bước xử lý trên $\mathcal{R}$ vẫn đảm bảo tính độc lập giữa giá trị xử lý và giá trị trung gian thực, đáp ứng yêu cầu mặt nạ. Qua đó có thể khẳng định sơ đồ FRIEM chống được tấn công DPA.

- Đánh giá hiệu năng

Việc thực thi các thuật toán mã hóa trên các hệ thống bit song song (bit-parallel) tỏ ra phù hợp với các thiết bị mật mã bởi ưu điểm chi phí thời gian thấp tuy nhiên đi cùng nhược điểm chi phí lưu trữ tốn kém hơn việc sử dụng các hệ thống tuần tự. Do đó, cần kiểm soát được chi phí lưu trữ này sao cho phù hợp với các thiết bị có dung lượng thấp như SmartCard, bên cạnh đó cũng phải kiểm soát được chi phí thực thi trong thiết kế của thuật toán để đảm bảo tính tối ưu.

Đối với các phép biến đổi trên vành $\mathcal{R} = GF(2^4)[x]/P(x)Q(x)$, phép nhân có chi phí thực hiện phụ thuộc vào giá trị k được chọn. Phép nhân trên $\mathcal{R}$ sử dụng $(k + 1)^2$ phép nhân và tối thiểu $n^2 - 1$ phép cộng trên $GF(2^4)$, phép mũ 2^p có chi phí $(k + 1)k$ phép nhân hằng số, $(k + 1)p$ phép bình phương và k^2

phép cộng trên $GF(2^4)$. Về mặt bộ nhớ, các phép tính trong $GF(2^4)$ được thực hiện theo [12] sử dụng thêm nhiều biến nhớ tạm so với $GF(2)$. So sánh với các phép biến đổi trên $\mathcal{R}_{G\&T} = GF(2)[x]/P'(x)Q'(x)$, sự chênh lệch về số phép thực thi là không quá nhiều nhưng về mặt chi phí bộ nhớ là rõ rệt, tuy nhiên vì các phép tính trong $GF(2^4)$ có thể thực hiện trên hệ thống song song, do đó thời gian thực thi thấp hơn, vấn để chỉ là sử dụng cân đối sao cho vẫn đảm bảo được dung lượng cho phép.

Vì phụ thuộc vào giá trị k, việc chọn k để phù hợp với Smart Card rất quan trọng. Chọn k càng lớn tuy tốc độ thực thi chậm nhưng lại có sự an toàn lớn và ngược lại, do vậy cần chọn k phù hợp với tính chất sử dụng của thiết bị Smart Card.

3. Kết luận

Bài báo đã trình bày sơ đồ FRIEM cho thuật toán AES thực thi trên Smart Card. Các lý thuyết biểu diễn trên trường mở rộng, nhúng trường sang vành, chiếu ngược lại, xử lý trên vành đã cung cấp cơ sở đề bài báo xây dựng sơ đồ đảm bảo an toàn cho thuật toán AES trước tấn công DPA. Ngoài ra với việc xử lý trên trường mở rộng được dung lượng, phù hợp với thiết bị có tài nguyên hạn chế như Smart Card.

Bài báo cũng đã đánh giá vấn đề bảo đảm an toàn và hiệu năng của sơ đồ đề xuất. Các giá trị ngẫu nhiên kết hợp vào thuật toán làm cho giá trị trung gian mà kẻ tấn công thu được độc lập với giá trị trung gian "thực" của thiết bị. Các phép tính toán, biến đổi trên trường mở rộng để có thể xử lý song song (qua đó tiết kiệm được chi phí thực thi) phù hợp với thiết bị có tài nguyên hạn chế. Việc nhúng giá trị trên trường qua vành sẽ tăng được độ phức tạp tính toán, chống tấn công giá trị zero.

Với việc chống được tấn công giá trị zero, đảm bảo được hiệu năng, phù hợp với thiết bị Smart Card, đồng thời luôn bảo đảm cho các giá trị trung gian độc lập với năng lượng tiêu thụ, sơ đồ FRIEM đề xuất phù hợp để thực thi thuật toán AES trên Smart Card chống tấn công DPA.

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 tháng 12/2014, pp 87-93.*

[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 đặc san tháng 5/2017, pp 33-41.

[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 3 tháng 5 năm 2019.

[4] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, "*Handbook of aplied cryptology*", Crc Press Inc, 1997.

[5] D.R. Stinson, "*Cryptography: Theory and Practice",* CRC Press, Inc, 1995.

[6] 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.

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

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

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

[10] 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.

[11] 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

[12] 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.
[13] Johannes Blömer, Jorge Guajardo, and Volker Krummel, “Provably Secure Masking of AES”, ResearchGate, 2014
[14] Elena Trichina, “Combinational Logic Design For AES Sub-Byte Transformation On Masked Data”, 2003.

ABSTRACT

The Field Ring Inversion Embeded Mask (FRIEM) solve the safety and performance issues that are suitable for devices with limited resources. The paper presents the theoretical basis, method of calculation and inverse on the extension and proposed a mask diagram for the AES algorithm on Smart Card against DPA attack.

Keywords: DPA, AES, extended field, mask, intermediate value, Smart Card.

Nguyen Thanh Tùng[1], Bùi Văn Dương[2]
[1]*Trung tâm Thực hành Kĩ thuật Mật mã, Học viện Kĩ thuật Mật mã*
[2]*Lớp AT13i, Học viện Kĩ thuật Mật mã*

Keywords: DPA, AES, mask, intermediate value, Smart Card.