HNUE JOURNAL OF SCIENCE DOI: 10.18173/2354-1059.2019-0010
Natural Sciences 2019, Volume 64, Issue 3, pp. 82-88
This paper is available online at http://stdb.hnue.edu.vn

MẶT NẠ NHÂN CHỐNG TẤN CÔNG DPA LÊN AES TRÊN SMART CARD

Nguyễn Thanh Tùng[1] và Trần Ngọc Quý[2]
[1]*Trung tâm Thực hành Kĩ thuật Mật mã, Học viện Kĩ thuật Mật mã*
[2]*Khoa Điện tử Viễn thông, Học viện Kĩ thuật Mật mã*

Tóm tắt: Mặt nạ là giải pháp hữu hiệu để chống tấn công phân tích năng lượng vi sai (DPA). Mặt nạ phải che được tất cả giá trị trung gian của thuật toán khi hoạt động mật mã. Việc thay thế mặt nạ đầy đủ bằng mặt nạ nhân giải quyết được vấn đề dung lượng, thời gian (nhất là với những thiết bị có tài nguyên hạn chế). Bài báo trình bày phương pháp sử dụng mặt nạ nhân chống tấn công DPA cho thuật toán AES trên Smart Card.

Từ khóa: DPA, AES, 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 thực hiện khai thác năng lượng của thiết bị mật mã để tìm ra khóa mã. Quá trình tấn công thực hiện 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 [1-3].

Tấn công phân tích năng lượng vi sai (Diffirence Power Analysis - DPA) tấn công lên giá trị trung gian của thuật toán khi hoạt động mật mã để tìm khóa bí mật. DPA sẽ thành công nếu giá trị trung gian mà kẻ tấn công thu được có liên quan với bản rõ và khóa của thuật toán. Kĩ thuật mặt nạ sử dụng giá trị ngẫu nhiên để che các giá trị trung gian này, làm cho năng lượng tiêu thụ độc lập với giá trị trung gian của thiết bị khi hoạt động.

Bài báo *"Một giải pháp chống tấn công DPA hiệu quả"* [2] đã trình bày sơ đồ mặt nạ đây 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. Để giải quyết vấn đề này, bài báo đề xuất phương pháp mặt nạ nhân bao gồm hai loại: mặt nạ nhân thích nghi và mặt nạ nhân đơn giản chống tấn công DPA lên thuật toán AES trên Smart Card, đồng thời đánh giá về tính an toàn và hiệu năng của các lược đồ đề xuất.

2. Nội dung nghiên cứu

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

AES 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 [4-6]. Smart Card

Ngày nhận bài: 12/3/2019. Ngày sửa bài: 19/3/2019. Ngày nhận đăng: 26/3/2019.
Tác giả liên hệ: Nguyễn Thanh Tùng. Địa chỉ e-mail: tungkmm@gmail.com

thực thi AES được sử dụng rộng rãi trên nhiều lĩnh vực như an ninh quốc gia, truyền thông, tài chính, ngân hang.

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 [7, 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. 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 lí. 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 "thật" của thuật toán [5].

Tùy theo từng thuật toán mà có thể sử dụng mặt nạ boolean, mặt nạ arithmetic hay kết hợp [9].

- Mặt nạ boolean che giá trị v bằng giá trị ngẫu nhiên m với phép tính: $v_m = v \oplus m$

Hàm boolean có dạng: $f(v \oplus m) = f(v) \oplus f(m)$, hàm này có thể dễ dàng tính toán, thay đổi giá trị và gỡ bỏ mặt nạ.

- Mặt nạ arithmetic che giá trị v bằng giá trị ngẫu nhiên m qua các phép tính:

+ Mặt nạ cộng: $v_m = v + m \ (mod\ n)$

+ Mặt nạ nhân: $v_m = v \times m \ (mod\ n)$

Mod n theo mod của thuật toán mật mã.

Yêu cầu khi thực hiện mặt nạ gồm:

- Mặt nạ phải được tính trước;

- Mặt nạ phải che được tất cả các giá trị trung gian của thuật toán;

- Mặt nạ phải được gỡ bỏ tại đầu ra để thuật toán hoạt động bình thường.

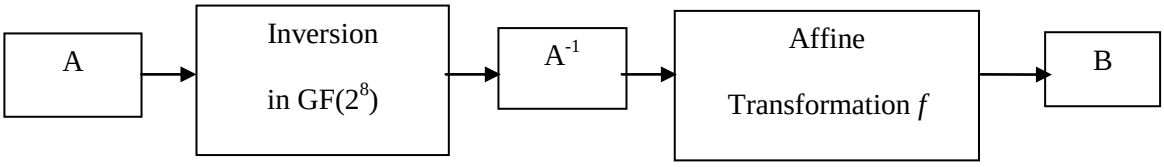
Các phép biến đổi của thuật toán AES có cả hàm Boolean và hàm Arithmetic, các phép AddRounKeys, MixColumns, ShiftRows là các phép biến đổi tuyến tính nên dễ dàng sử dụng mặt nạ Boolean.

Biến đổi SubBytes thực hiện hai phép tính (phép nghịch đảo và phép biến đổi affine), Hình 2. Phép nghịch đảo là phép biến đổi phi tuyến ($f^{-1}(x \oplus m) \neq f^{-1}(x) \oplus f^{-1}(m)$). Vì vậy, việc thực hiện mặt nạ cho biến đổi này sẽ khó khăn, phức tạp, hơn nữa an toàn của thuật toán AES cũng phụ thuộc nhiều vào phần phi tuyến này.

2.2. Mặt nạ nhân chống tấn công DPA lên AES trên Smart Card

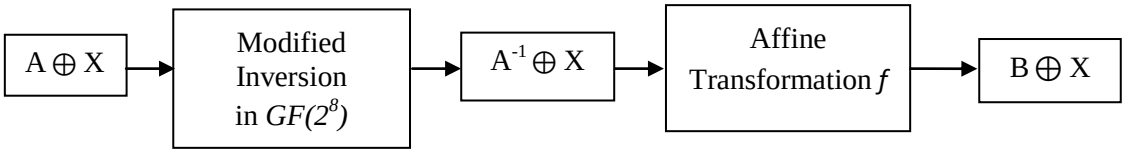
Bài báo sử dụng tính chất của phép nhân nghịch đảo trên trường hữu hạn theo công thức: $f^{-1}(x \times m) = (x \times m)^{-1} = f^{-1}(x) \times f^{-1}(m)$ để đề xuất mặt nạ nhân cho thuật toán AES trên Smart Card.

Biến đổi SubBytes của AES được thể hiện tại Hình 1.



Hình 1. Biến đổi SubBytes trong AES

Khi thực hiện mặt nạ, cần phải biến đổi phù hợp để phép nghịch đảo. Biến đổi SubBytes cải tiến được thể hiện tại Hình 2.



Hình 2. Biến đổi SubByte cải tiến

2.2.1. Mặt nạ nhân thích nghi

Để có kết quả biến đổi trong phép Modified Inversion in $GF(2^8)$ tại Hình 2 (từ giá trị A ⊕ X thành A^{-1} ⊕ X), mặt nạ nhân thích nghi sử dụng thêm giá trị ngẫu nhiên Y, thuật toán như sau:

Algorithm 1: ***Mặt nạ nhân thích nghi***

INPUT: A ⊕ X, X, Y

OUTPUT: Inv(A) + X,

1: (A ⊕ X) / x Y

2: (A ⊕ X) x Y / ⊕ (X x Y)

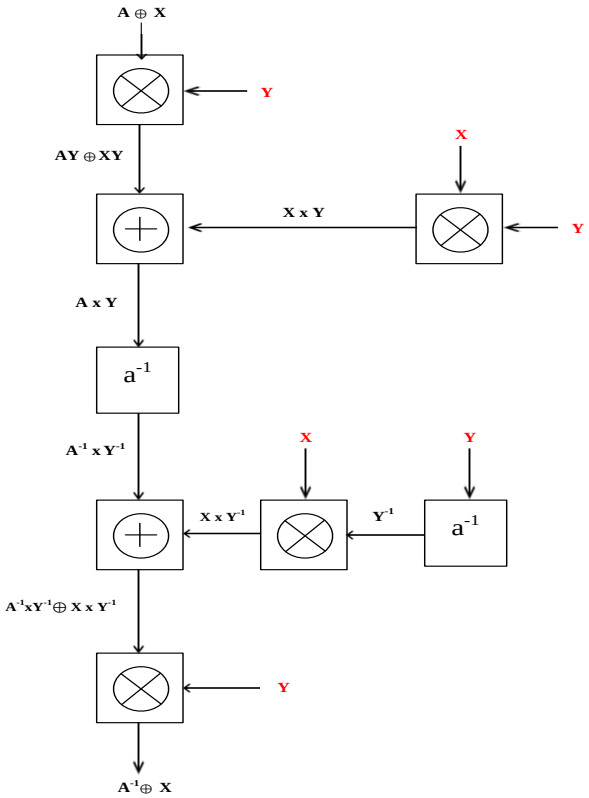
3: X x Y / $^{-1}$

4: A^{-1} x Y^{-1} / ⊕ (X x Y^{-1})

5: (A^{-1} x Y^{-1}) + (X x Y^{-1}) / x Y

6: (A^{-1} ⊕ X)

Sơ đồ mặt nạ nhân thích nghi được biểu diễn tại Hình 3.



Hình 3. Sơ đồ mặt nạ nhân thích nghi

2.2.2. Mặt nạ nhân đơn giản

Để tiếp tục giải quyết vấn đề dung lượng, bài báo đề xuất mặt nạ nhân đơn giản. Mặt nạ nhân đơn giản không sử dụng giá trị ngẫu nhiên Y, thuật toán như sau:

Algorithm 2: ***Mặt nạ nhân đơn giản cho biến đổi SybBytes()***

INPUT: $A \oplus X$, X

OUTPUT: $Inv(A) \oplus X$,

1: $(A \oplus X)$ / x X

2: $(A \oplus X) \times X$ / $\oplus (X \times X)$

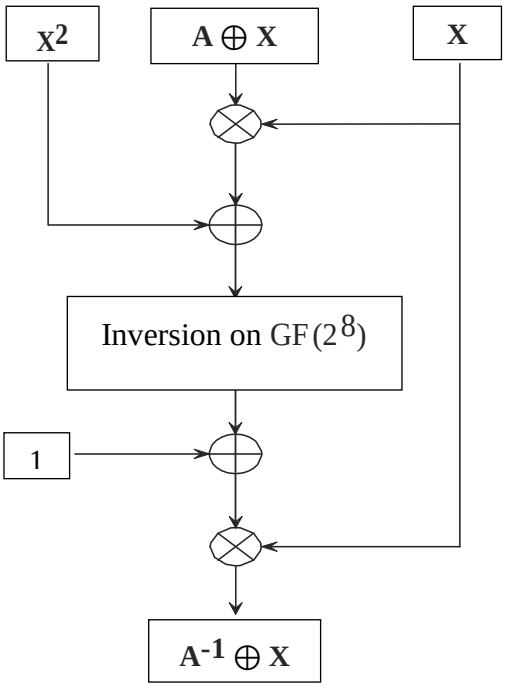
3: $A \times X$ / $^{-1}$

4: $A^{-1} \times X^{-1}$ / $\oplus 1$

5: $(A^{-1} \times X^{-1}) \oplus 1$ / x X

6: $A^{-1} \oplus X$

Sơ đồ mặt nạ nhân đơn giản cho SubByte được biểu diễn tại Hình 4



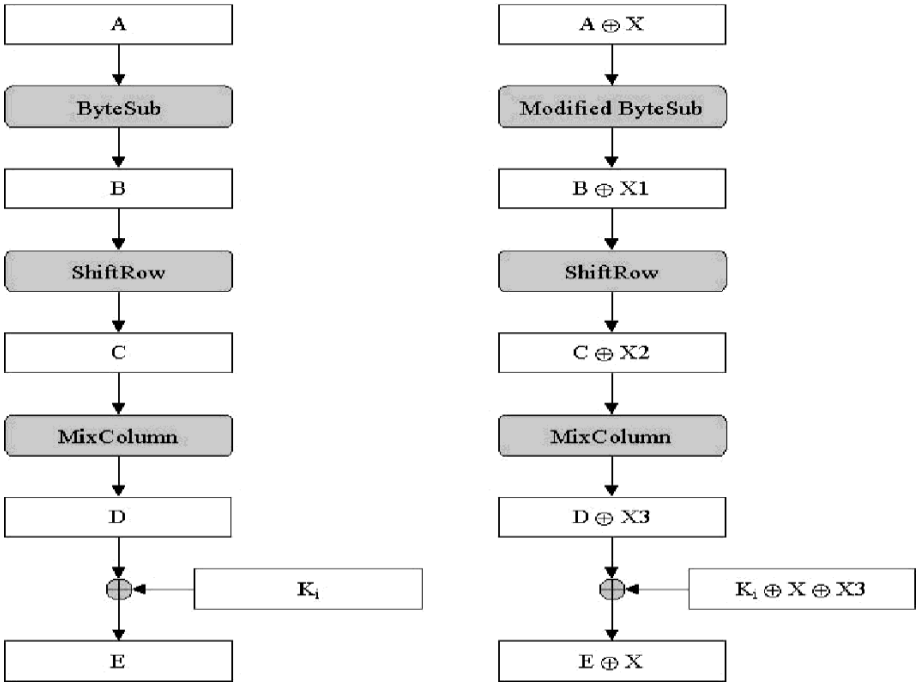
Hình 4. Sơ đồ mặt nạ nhân đơn giản

2.3. Vấn đề an toàn và hiệu năng của mặt nạ nhân

2.3.1. Vấn đề an toàn

** An toàn lí thuyết*

Sự khác nhau giữa một vòng AES chưa thực hiện giải pháp mặt nạ và vòng AES đã thực hiện mặt nạ được thể hiện ở Hình 5.

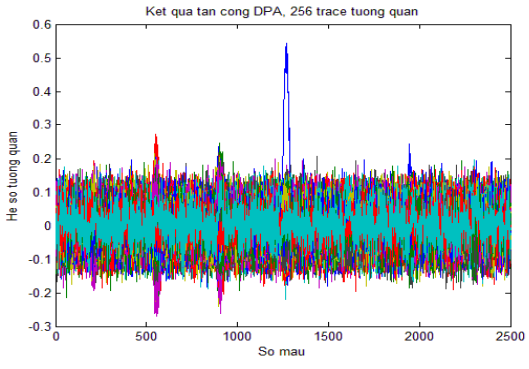


Hình 5. So sánh một vòng AES

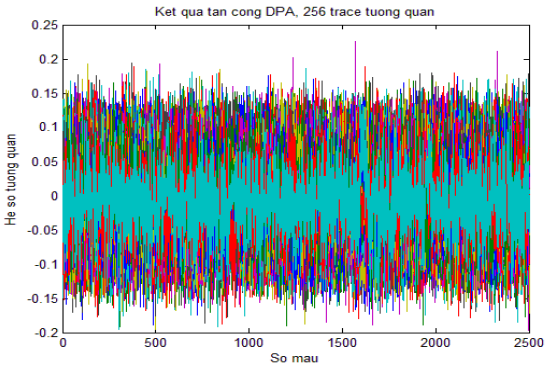
Theo sơ đồ Hình 5 thì từ điểm khởi đầu của thuật toán tới điểm cuối của thuật toán (từ A ⊕ X đến E ⊕ X) không có giá trị trung gian 'thật' nào xuất hiện. Giải pháp đã bảo vệ được thuật toán trước tấn công DPA.

** Kết quả thực nghiệm*

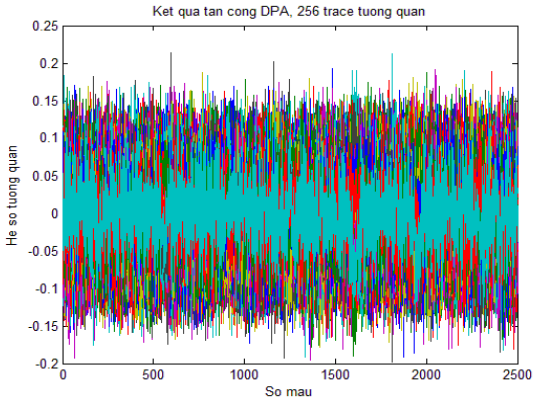
Thực thi trên Smart Card Atmega 8515, tiến hành cài đặt thuật toán AES-128 bình thường (Hình 6a), AES có mặt nạ đầy đủ (Hình 6b), AES có mặt nạ nhân thích nghi (Hình 6c) và AES có mặt nạ nhân đơn giản (Hình 6d). Cho thuật toán mã hóa với byte khóa bí mật k = 63. Quan sát cho thấy khi không thực thi mặt nạ, vết năng lượng thu được có đỉnh nhô cao, qua đó xác định được khóa bí mật của thuật toán (khóa 63). Khi tấn công DPA lên các sơ đồ mặt nạ, qua hình 6b, 6c, 6d không tìm thấy đỉnh nhô lên (tất cả khóa tương tự nhau). Vì vậy tấn công DPA không tìm được khóa đúng của thuật toán.

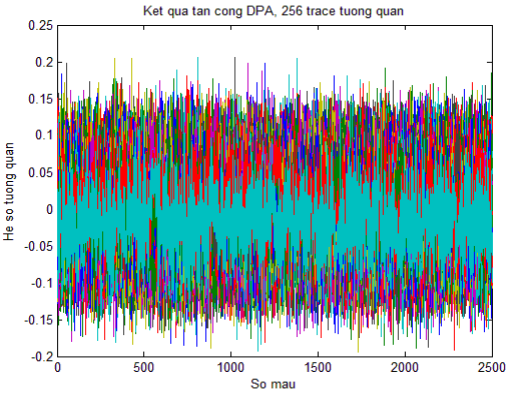


a. Tấn công DPA lên AES bình thường



b. Tấn công DPA lên AES có mặt nạ đầy đủ





c. Tấn công DPA lên AES có mặt nạ nhân thích nghi ***d. Tấn công DPA lên AES có mặt nạ nhân đơn giản***

Hình 6. Tấn công DPA lên AES

2.3.2. So sánh hiệu năng

Kết quả đánh giá về thời gian và dung lượng như sau:

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 mặt nạ đầy đủ	78, 3 ms	3795	4250
AES có mặt nạ nhân thích nghi	58,7 ms	1752	121
AES có mặt nạ nhân đơn giản	37,8 ms	1563	118

Theo kết quả ở Bảng 1, sơ đồ AES có mặt nạ đầy đủ (thực hiện các bảng mặt nạ cho hộp thế) [2] tốn 3795 bytes ROM và 4250 bytes RAM. Trong khi đó sơ đồ AES có mặt nạ nhân thích nghi (với sự xuất hiện của giá trị Y) tốn 1752 bytes ROM và 121 bytes RAM. Đặc biệt, sơ đồ AES thực hiện mặt nạ nhân đơn giản chỉ tốn 1563 bytes ROM và 118 bytes RAM. Hai sơ đồ mặt nạ nhân đã giải quyết được bài toán về dung lượng và thời gian khi thực hiện mặt nạ để chống tấn công DPA cho thuật toán AES trên Smart Card.

3. Kết luận

Bài báo trình bày lí thuyết và thực nghiệm phương pháp mặt nạ nhân cho thuật toán AES-128 trên Smart Card. Các sơ đồ mặt nạ đề xuất che các giá trị trung gian bằng các giá trị ngẫu nhiên chống được tấn công DPA lên thuật toán AES. Mặt nạ nhân thích nghi và mặt nạ nhân đơn giản bảo đảm các yêu cầu về dung lượng và thời gian cho thiết bị nhỏ, tài nguyên hạn chế như Smart Card.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Hồng Quang, 2014. *Phân tích tiêu thụ điện năng của thiết bị mật mã*. Tạp chí Nghiên cứu Khoa học và Công nghệ Quân sự, Vol. 34, tr. 87-93.

[2] Nguyễn Thanh Tùng, 2017. *Một giải pháp chống tấn công DPA hiệu quả*. Tạp chí Nghiên cứu Khoa học và Công nghệ Quân sự, số Đặc san tháng 5/2017, tr. 33-41.
[3] Stefan Mangard, Elisabeth Oswald and Thomas Popp, 2007. *Power Analysis Attacks Revealing the Secrets of Smart Cards.* Graz University of Technology Graz.
[4] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, 1997. *Handbook of Aplied Cryptology*, Crc Press Inc.
[5] D.R. Stinson, 1995. *Cryptography: Theory and Practice,* CRC Press, Inc.
[6] National Institute of Standards and Technology (NIST). *FIPS-197,* 2001. *Advanced Encryption Standard*, No. November/2001.
[7] P. Kocher, J. Jaffe and B. Jun, 1999. *Differential power analysis.* Proceedings of Crypto 99, Lecture Notes in Computer Science, Vol. 1666, Springer, pp. 388-397.
[8] Department of the Army Washington DC, 1990. *Basic Cryptanalysis.* Field Manual 34-40-2.
[9] J.-S. Coron and L. Goubin, 2000. *On Boolean and arithmetic masking against differential power analysis.* Springer-Verlag Berlin Heidelberg, pp. 231-237.

ABSTRACT

Multiplicative masking resistant to DPA on AES Smart Card implemention

Nguyen Thanh Tung[1] and Tran Ngoc Quy[2]

[1]*Department of Practice Cryptography Techniques, Academy of Cryptography Techniques*

[2]*Department of Electronics and Telecommunications, Academy of Cryptography Techniques*

Mask is an effective solution to countermeasure differential power analysis (DPA). The mask must cover all intermediate values of the algorithm. Multiplication mask solves the capacity and time issue (especially for devices with limited resources). The article presents the method of using multiplication mask resistant DPA attack for AES algorithm on Smart Card.

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