MỘT GIẢI PHÁP CHỐNG TẤN CÔNG DPA HIỆU QUẢ

Nguyễn Thanh Tùng*

Tóm tắt: *Tấn công phân tích năng lượng thực hiện lên giá trị trung gian của thuật toán mật mã để tìm khóa bí mật. Với việc sử dụng các giá trị ngẫu nhiên để che giá trị trung gian, làm cho năng lượng tiêu thụ của thiết bị độc lập với giá trị trung gian của thuật toán, masking (mặt nạ) là một giải pháp hữu hiệu để chống loại tấn công này. Bài báo trình bày phương pháp mặt nạ cho thuật toán AES chống tấn công DPA.*

Từ khóa: Tấn công DPA, AES, Mặt nạ.

1. ĐẶT VẤN ĐỀ

Trong những năm gần đây, việc phân tích các thuật toán mật mã để khai phá thông tin bí mật qua kênh kề ngày càng được quan tâm và đầu tư nghiên cứu. Nhiều kỹ thuật tấn công kênh kề lên các thiết bị mật mã đã được nghiên cứu, giới thiệu. Những dạng tấn công kênh kề điển hình có thể kể đến là tấn công phân tích timming, tấn công phân tích lỗi, tấn công phân tích điện - từ trường, tấn công phân tích âm thanh, tấn công phân tích nhiệt độ và tấn công phân tích năng lượng.

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. Quy trình tấn công được thực hiện bằng việc đo và phân tích tiêu thụ năng lượng không cần chi phí lớn nhưng đặc biệt hiệu quả [1], [2], [10].

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.

Tấn công phân tích năng lượng được chia thành hai loại: Tấn công phân tích năng lượng đơn giản (Simple Power Analysis – SPA) và tấn công phân tích năng lượngvi sai (Difference Power Analysis –DPA) [10]. Kỹ thuật tấn công SPA khai thác mối quan hệ giữa lệnh đang thực hiện và hình dáng vết tiêu thụ năng lượng. Việc phân tích thực hiện trên trục thời gian. Tấn công DPA khai thác mối quan hệ giữa dữ liệu được xử lý và năng lượng tiêu thụ, dùng các kỹ thuật thống kê, so sánh... để tìm khóa bí mật của thuật toán.

Trước thực tế và khả năng của tấn công phân tích năng lượng tiêu thụ lên thiết bị mã hóa, đã có một số nghiên cứu về giải pháp chống tấn công, tập trung vào các phương pháp ẩn, mặt nạ…

Mục đích của Ẩn là loại bỏ tương quan giữa năng lượng tiêu thụ và giá trị trung gian của thuật toán qua việc ngẫu nhiên hóa hoặc san để thiết bị tiêu thụ mức năng lượng bằng nhau trong mỗi chu kỳ hoạt động. Có thể thực hiện Ẩn bằng việc chèn thêm hoặc xáo trộn thứ tự hoạt động của các phép biến đổi trong thuật toán.

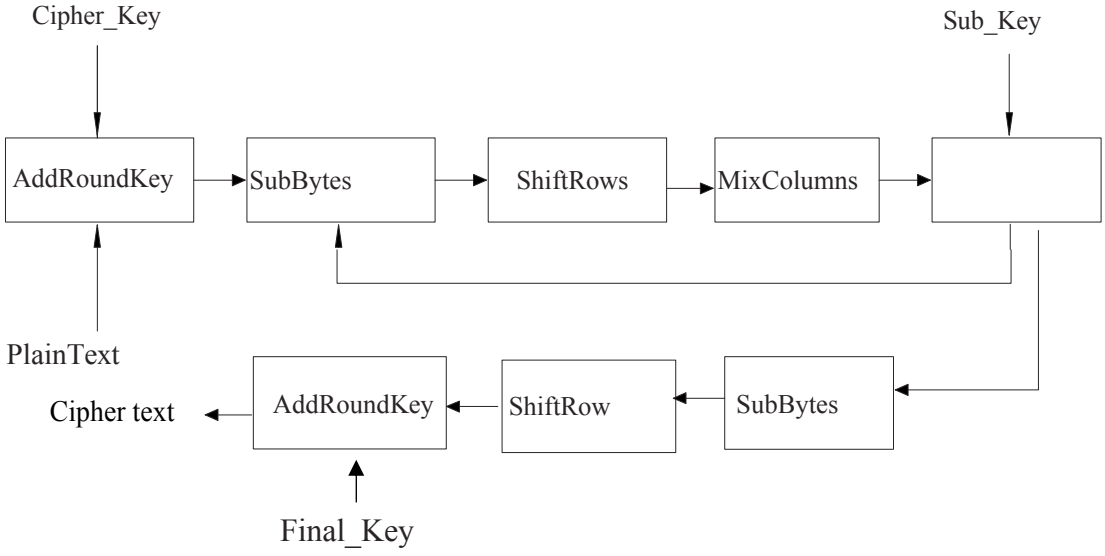
Mặt nạ là phương pháp chống tấn công với mục đích làm cho năng lượng tiêu thụ độc lập (kể cả khi dữ liệu phụ thuộc vào năng lượng tiêu thụ của thiết bị). Kỹ thuật mặt nạ sử dụng giá trị ngẫu nhiên để che các giá trị trung gian của thuật toán mật mã. Mặt nạ phải che được tất cả giá trị trung gian của thuật toán trong suốt thời gian thực vì giá trị trung gian tức thời được tính dựa trên giá trị trung gian trước đó.

2. TẤN CÔNG DPA LÊN AES

Tấn công DPA xác định khóa bí mật của thiết bị mật mã dựa trên các vết năng lượng ghi được khi thiết bị thực hiện mã hóa hoặc giải mã các khối dữ liệu khác nhau. Tấn công DPA phân tích tiêu thụ năng lượng tại thời điểm hoạt động của thuật toán có liên quan đến khóa mã.

2.1. Thuật toán AES

AES là thuật toán mã hóa tiên tiến được sử dụng rộng rãi trên nhiều lĩnh vực như an ninh quốc gia, truyền thông, tài chính, ngân hàng….



Hình 1. *Luồng biến đổi của thuật toán AES.*

AES [12] có cấu trúc dạng SPN, xử lý với kích cỡ khối 128 bit, với kích thước khóa là 128, 192 hay 256 bit. Hoạt động của thuật toán như sau: Tại thời điểm bắt

đầu phép mã hóa, dữ liệu rõ đầu vào được ghi vào mảng trạng thái. Sau phép cộng khóa vòng khởi đầu, mảng trạng thái được biến đổi bằng cách thực thi một hàm vòng liên tiếp với các phép biến đổi AddRoundKey (), SubByte (), ShiftRow (), MixColumn () và với số lần vòng lặp là 10, 12 hoặc 14 (phụ thuộc vào độ dài khóa là 128, 192 hay 256 bit), tất cả các vòng trong lược đồ mã hóa giống nhau, chỉ trừ vòng cuốicùng không có phép biến đổi MixColumns(). Trạng thái cuối cùng được chuyển thành đầu ra (bản mã). Luồng biến đổi của thuật toán AES được biểu diễn tại hình 1.

2.2. Tấn công DPA lên AES

a. Kỹ thuật tấn công

Tấn công DPA lên AES thực hiện theo một chiến thuật bao gồm 5 bước.

Bước 1: Bước đầu tiên trong tấn công DPA là lựa chọn, xác định vị trí tấn công. Đối với thuật toán AES chọn vị trí tấn công tại đầu ra của Sbox vòng đầu tiên (giá trị trung gian phụ thuộc vào khóa mã).

Bước 2: Đo năng lượng tiêu thụ của thiết bị mật mã khi mã hóa dữ liệu và xây dựng thành ma trận năng lượng tiêu thụ.

Bước 3: Tính các giá trị trung gian giả định khi thiết bị thực hiện thuật toán với các khóa giả thiết.

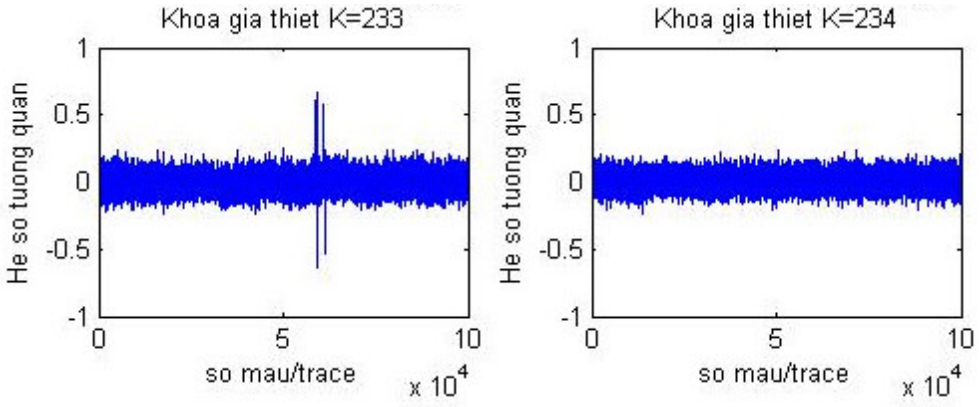
Bước 4: Ánh xạ giá trị trung gian giả định thành năng lượng tiêu thụ giả định.

Bước 5: So sánh giá trị điện năng tiêu thụ giả định và giá trị năng lượng thu được, đánh giá kết quả và kết luận khóa bí mật tìm được.

b. Thực nghiệm tấn công DPA lên AES -128

Mô hình thực nghiệm gồm một Smartcard, nhận dữ liệu từ máy tính, mã hóa bằng thuật toán AES rồi trả lại kết quả về máy tính. Tần số clock là 11.0592MHz, nguồn điện 5V, cổng giao tiếp RS-232. Để đo năng lượng tiêu thụ của vi xử lý ta nối tiếp một điện trở 1Ω trên đường đất của nó. Điện áp rơi trên điện trở phản ánh năng lượng tiêu thụ của vi xử lý, được đo bằng digital oscilloscope có băng thông đầu vào 1GHz, độ phân giải 8 bits. Sử dụng tín hiệu DTR để trigger oscilloscope. Tốc độ trích mẫu là 250MS/s. Vết năng lượng tiêu thụ được oscilloscope ghi lại và truyền sang máy tính để phân tích. Cho smartcard mã hóa với 256 khóa giả thiết. Dùng hệ số tương quan để xác định khóa. Quan sát cho thấy khóa giả thiết 233 có tương quan lớn nhất (khoảng 0.7 - hình 2), được thể hiện là đỉnh nhô lên trên biểu

đồ vi sai ứng với khóa giả thiết 233 (các khóa khác không có đỉnh nhô lên). Vì vậy, có thể xác định khóa giả thiết 233 là khóa của thuật toán.



Hình 2. *Biểu đồ vi sai ứng với hai khóa giả thiết k =233 và k=234.*

Tấn công DPA thực hiện được vì năng lượng tiêu thụ của thiết bị mật mã phụ thuộc vào giá trị trung gian do thiết bị xử lý. Các nghiên cứu đã chứng minh có thể tấn công DPA thành công lên thuật toán AES trên Smartcard với chi phí và thời gian hợp lý [1], [2].

3. ĐỀ XUẤT GIẢI PHÁP MẶT NẠ CHO AES

Như đã phân tích ở trên, với khả năng ngày càng cao, đa dạng của mã thám, yêu cầu các thuật toán mật mã phải thực thi các giải pháp phòng chống. Để chống tấn công DPA lên AES thì phải làm cho năng lượng tiêu thụ của thiết bị độc lập với giá trị trung gian. Bài báo trình bày lý thuyết và đề xuất thực hiện giải pháp mặt nạ cho AES trên Smartcard.

3.1. Tổng quan về mặt nạ

Mặt nạ thực hiện che một giá trị *v* bằng một giá trị mặt nạ *m* theo công thức:

$$v_m = v * m \quad (1)$$

Mặt nạ Boolean: Thực hiện che giá trị trung gian *v* bằng giá trị *m* với phép Xor:

$$v_m = v \oplus m \ . \quad (2)$$

Mặt nạ toán học: Thực hiện che giá trị trung gian *v*bằng giá trị ngẫu nhiên *m* qua một phép toán (cộng hoặc nhân modular):

Phép cộng modular: $v_m = v + m \ (\mathrm{mod} n)$

Phép nhân modular: $v_m = v \times m \ (\mathrm{mod} n)$

Modular *n* tính theo moduler của thuật toán mật mã.

3.2. Đề xuất sơ đồ mặt nạ cho thuật toán AES

Để chống tấn công DPA lên AES phải thực hiện mặt nạ đầy đủ (che hết các giá trị trung gian), bài báo trình bày sơ đồ mặt nạ đầy đủ cho tất cả các phép biến đổi của thuật toán AES – 128 (hình 3).

a. Mặt nạ cho các phép biến đổi trong các vòng AES

AddRoundKey: Đầu tiên, che khóa *k* bằng mặt nạ, che bản rõ *d* bằng mặt nạ, quá trình Addroundkey kết hợp giữa các byte rõ *d* và các byte khóa *k* (đã được mặt nạ).

SubBytes: Thực hiện mặt nạ để che bảng tra cứu S-box.

ShiftRows: Biến đổi ShiftRows dịch chuyển các bytes trạng thái. Tất cả các bytes trạng thái được mặt nạ với giá trị không đổi. Vì vậy, hoạt động này không phải thực hiện mặt nạ.

MixColumns: Biến đổi MixColumns trộn các bytes từ các hàng khác nhau trong một cột. Để che hết giá trị trung gian, cần thực hiện mỗi dòng một mặt nạ, đồng thời chỉ cần thực hiện mặt nạ giống nhau cho các vòng.

Với các điều kiện trên, để thực hiện mặt nạ đầy đủ cho các giá trị trung gian của thuật toán AES, bài báo đề xuất sử dụng 06 mặt nạ độc lập gồm: hai mặt nạ *m* và *m'* che cho đầu vào và đầu ra của biến đổi SubBytes và 4 mặt nạ m_1, m_2, m_3, m_4 để che đầu vào của biến đổi MixColumns.

Quá trình chuẩn bị: Tính trước mặt nạ S-box và mặt nạ Mixcolumns như sau:

Mặt nạ bảng tra cứu S-box S_m được tính theo công thức:

$$S_m\,(x \oplus m) = S(x) \oplus m'. \qquad (3)$$

trong đó, m là mặt nạ đầu vào, m' là mặt nạ cho đầu ra S-box.

Giá trị mặt nạ đầu ra của phép biến đổi MixColumns theo công thức:

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

Quá trình thực hiện:

Bắt đầu mỗi vòng làm việc, 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 (đều đã được mặt nạ).

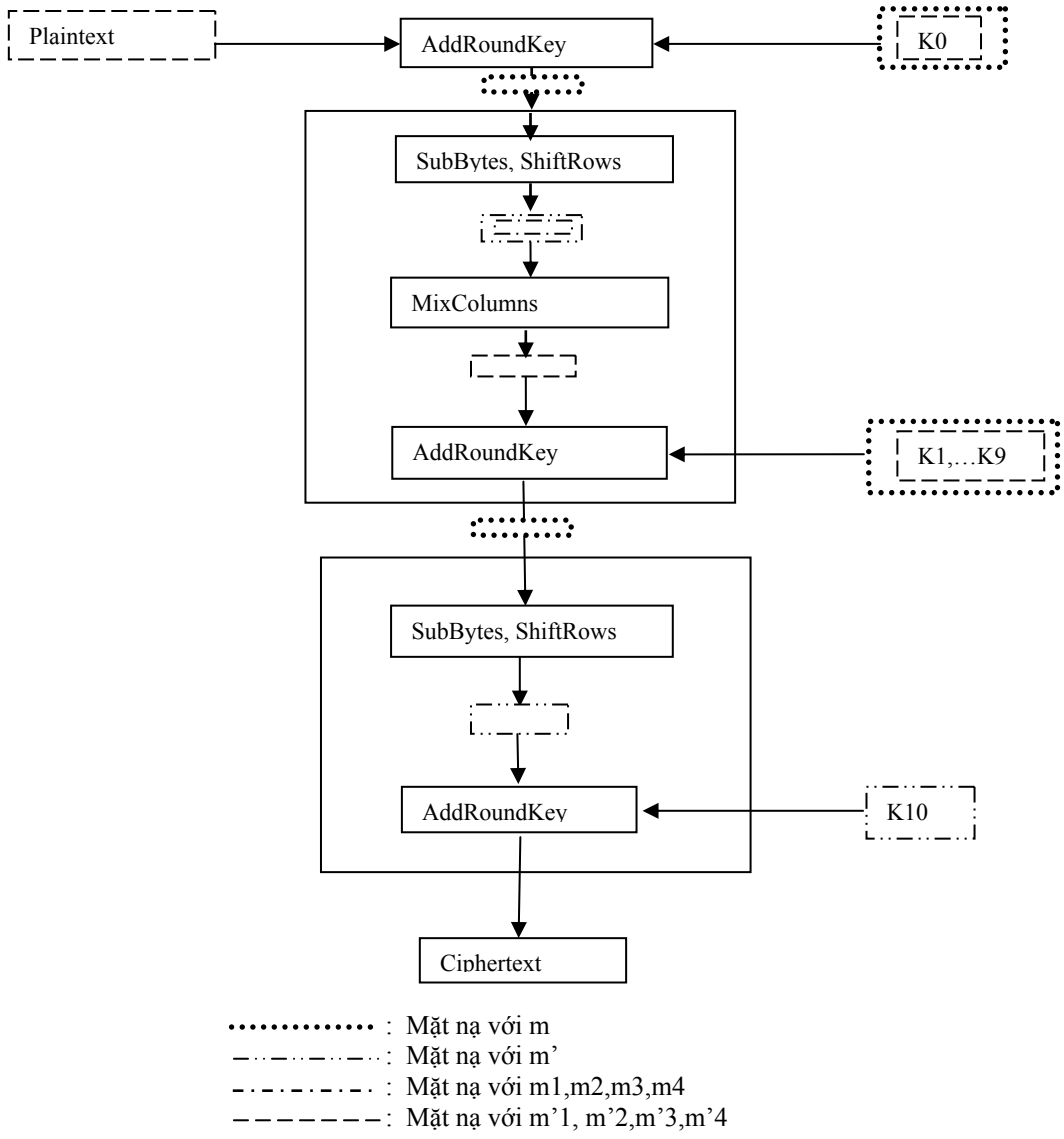
Giá trị trung gian $(d \oplus k)$ được mặt nạ theo công thức:

$$(d \oplus m'_i) \oplus (k \oplus m \oplus m'_i) = (d \oplus k) \oplus m. \qquad (4)$$

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

Sau biến đổi ShiftRows mặt nạ m' vẫn giữa 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 tư. Biến đổi MixColumns thay đổi các mặt nạ m_i thành m'_1 với i =1,…,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.



Hình 3. *Sơ đồ mặt nạ cho thuật toán AES – 128.*

Vòng cuối không thực hiện phép biến đổi MixColums. 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 ta được bản mã (không mặt nạ). Như vậy, mặt nạ đã được gỡ bỏ tại đầu ra của thuật toán để giải mã.

b. Mặt nạ cho lược đồ khóa:

Để bảo đảm an toàn, lược đồ khóa cũng phải được mặt nạ. Sử dụng lại các bytes mặt nạ *m* và *m'* cho tất cả các vòng.

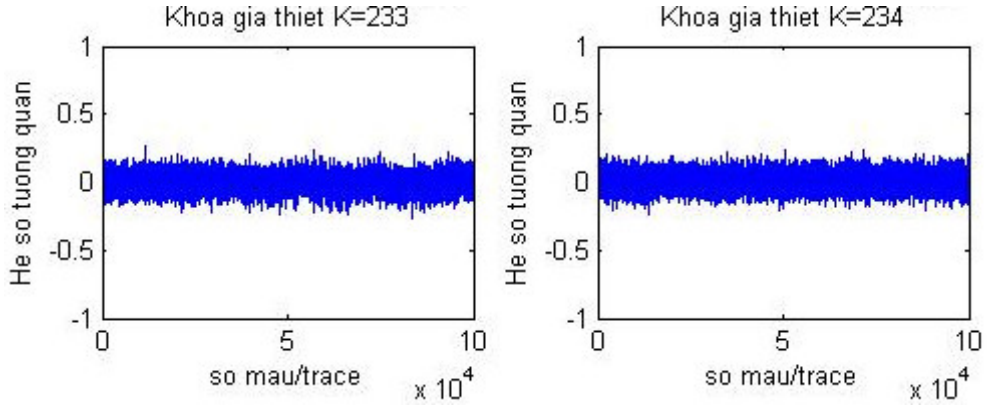
Bước thứ nhất của lược đồ khóa, khóa gốc (sử dụng cho khóa vòng đầu tiên) được mặt nạ với giá trị mặt nạ là $(m_i' \oplus m)$. Mặt nạ $m_i' \oplus m$ che cho các khoá vòng trừ cuối cùng được che bằng mặt nạ *m'*.

3.3. Đánh giá an toàn

a. Đánh giá an toàn lý thuyết

Tấn công DPA thực hiện được khi năng lượng tiêu thụ của thiết bị mật mã phụ thuộc vào giá trị trung gian do thiết bị xử lý. Khi một giá trị trung gian *v* được che bởi mặt *m*: $v_m = v \oplus m$ (m là một giá trị ngẫu nhiên), thì v_m độc lập với *v*, do đó, năng lượng tiêu thụ của v_m cũng độc lập với *v*. Vì vậy, mặt nạ xóa bỏ được mối liên hệ giữa năng lượng tiêu thụ và giá trị trung gian của thiết bị. Giải pháp đề xuất sử dụng 06 mặt nạ đã che được tất cả các giá trị trung gian, chống được tấn công DPA lên thuật toán.

b. Đánh giá an toàn thực nghiệm



Hình 4. *Biểu đồ vi sai ứng với hai khóa giả thiết k =223 và k=224 (đã mặt nạ).*

Thực nghiệm tấn công DPA lên sơ đồ mặt nạ, biểu đồ vi sai (hình 4) cho thấy giá trị tương quan của khóa giả thiết 233 lúc này có giá trị khoảng 0.3 tương tự các

khóa khác (đã che được gai nhọn nhô lên so với thuật toán không thực hiện mặt nạ). Lúc này, thực hiện tấn công DPA không thể suy đoán ra giá trị khóa đúng của thuật toán.

Qua thực nghiệm cho thấy giải pháp đề xuất đã chống được tấn công DPA lên AES -128 trên Smartcard.

4. KẾT LUẬN

Tấn công DPA khai thác mối quan hệ giữa dữ liệu được xử lý và tiêu thụ điện năng. Loại tấn công này dựa vào nhiều phép đo và dùng thống kê để lọc bỏ nhiễu để tìm ra khóa bí mật của thiết bị mật mã. Bài báo đề xuất giải pháp chống tấn công DPA lên thiết bị mật mã. Giải pháp đề xuất sử dụng mặt nạ để che các giá trị trung gian của thuật toán mật mã. Qua đánh giá lý thuyết và thực nghiệm cho thấy sơ đồ mặt nạ đề xuất chống tấn công DPA đã loại bỏ sự phụ thuộc giữa dữ liệu và điện năng tiêu thụ, vì vậy, kẻ tấn công không thể sử dụng phân tích DPA để tìm ra khóa của thuật toán.

Tuy nhiên, với sự phát triển của phân tích mã (đặc biệt đối với các loại tấn công DPA bậc cao) thì sơ đồ mặt nạ không thể tuyệt đối an toàn. Hướng nghiên cứu tiếp là các sơ đồ mặt nạ an toàn, kết hợp với các giải pháp xáo trộn, chèn, ẩn, ngẫu nhiên hóa các hoạt động của thuật toán.

TÀI LIỆU THAM KHẢO

[1]. Nguyễn Hồng Quang, *"DPA, một dạng tấn công sidechannel hiệu quả"*, Tạp chí nghiên cứu Khoa học và Công nghệ Quân sự, 2013.

[2]. Nguyễn Hồng Quang, *"Trace năng lượng trong DPA"*, Tạp chí nghiên cứu Khoa học và Công nghệ Quân sự, 2013.

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

[4]. Christophe Clavier, Benoit Feix, Georges Gagnerot, *"Improved Collision-Correlation Power Analysis on First Order Protected AES"*, Ches, 2011.

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

[6]. Emmanuel Prouff, *"Side Channel Attacks against Block Ciphers Implementations and Countermeasures"*, Ches, 2013.

[7]. Hamad Marzouqi, Mahmoud Al-Qutayri, Khaled Salah, *"Review of gate-level differential power analysis and fault analysis countermeasures"*, IET Information Security, 2013.

[8]. Jun Wu, Yiyu Shi, and Minsu Choi,Senior Member, *"Measurement and Evaluation of Power Analysis Attacks on Asynchronous S-Box"*, IEEE Information Security, 2013.

[9]. Oscar Reparaz, Benedikt Gierlichs, Ingrid Verbauwhed, *"Selecting time samples for multivariate DPA"*, Leuven, Belgium, 2012.

[10]. 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.

[11]. S. Mangard, E. Oswald, F.-X. Standaert, *"One for all – all for one: unifying standard differential power analysis attacks"*, IEEE transactions on instrumentation and measurement, vol.61, no.10, 2012.

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

ABSTRACT

AN EFFICIENT SOLUTION GAINTS DPA ATTACKS

Anpower analysis attack implement on the intermediate value of the cryptographic algorithm to find the secret key. By using random values to mask the intermediate value and making the consumption power of device independent from the median value of algorithm, masking is an effective solution against the type of this attack. This paper presents the masking method for AES algorithms against DPA attacks.

Keywords: DPA attacks, AES, Mask.

Nhận bài ngày 14 tháng 02 năm 2017
Hoàn thiện ngày 15 tháng 3 năm 2017
Chấp nhận đăng ngày 01 tháng 5 năm 2017

Địa chỉ: Học viện Kỹ thuật Mật mã.
*Email: tungkmm@yahoo.com.