PHƯƠNG PHÁP TẤN CÔNG PHÂN TÍCH NĂNG LƯỢNG ĐƠN GIẢN LÊN HỆ MẬT DỰA TRÊN ĐƯỜNG CONG ELLIPTIC

TS. Đinh Quốc Tiến, ThS. Nguyễn Ngọc Vĩnh Hảo, ThS. Bùi Đức Chính
Viện Khoa học - Công nghệ mật mã

Tấn công phân tích năng lượng đơn giản (Simple Power Analysis - SPA) là một dạng tấn công kênh kề được sử dụng phổ biến trong lĩnh vực thám mã. Tấn công này khai thác mối quan hệ tuyến tính giữa năng lượng tiêu thụ và các quá trình thực thi của thuật toán mật mã nhằm tìm ra khóa lưu trữ trong thiết bị. Bài báo này trình bày kết quả thực hiện tấn công SPA lên phép nhân điểm phương pháp nhị phân của mật mã đường cong Elliptic (Elliptic Curve Cryptography - ECC). Tấn công được thực hiện thông qua việc phân tích và nhận dạng các phép tính cơ bản khi thuật toán thực thi trên phần cứng.

ECC được giới thiệu vào năm 1985 như một hệ mật khóa công khai thay thế cho các hệ mật khóa công khai cũ như DSA, RSA [2] [3]. Do có nhiều ưu điểm so với các hệ mật khóa công khai trước đó, nên ECC được ứng dụng ngày càng nhiều trong thực tế. ECC được chứng minh là an toàn trên lý thuyết. Tuy nhiên, ECC có thể bị tấn công kênh kề khi triển khai bằng phần cứng.

Một trong các dạng tấn công kênh kề thường được sử dụng trên ECC là tấn công phân tích năng lượng. Tấn công này dựa trên mối tương quan giữa năng lượng tiêu thụ và các quá trình tính toán bên trong của thiết bị mật mã. Có nhiều dạng tấn công phân tích năng lượng khác nhau, trong đó tấn công SPA có thể thực hiện chỉ với một lần đo năng lượng tiêu thụ của thiết bị. Bài báo này chứng minh tính hiệu quả của SPA lên phép nhân điểm phương pháp nhị phân của ECC. Chương trình tấn công sẽ sử dụng một dấu vết năng lượng (Power Trace) để tìm khóa được lưu trong kit Arduino Uno. Kit này có một vi điều khiển 8 bit Atmega328p để thực thi firmware phép nhân điểm của ECC.

Phép nhân điểm trên ECC

Để thực hiện tấn công phân tích năng lượng SPA, cần hiểu thuật toán mật mã đang chạy trên kit. Trong bài báo này, phép nhân điểm của ECC chạy trên kit được lựa chọn như sau:

Về phép nhân điểm

Phép nhân điểm là phép tính cơ bản của ECC. Giả sử có điểm P trên đường cong Elliptic, kết quả Q của phép nhân điểm P với khóa K là phép cộng K lần của điểm P vào chính nó và ký hiệu $Q = KP$. Để tính KP có thể thực hiện theo phép tính Nhân đôi và Cộng (Double and Add) dựa trên biểu diễn nhị phân của khóa $K = (k_{n-1},...,k_0)_2$, trong đó k_{n-1} là bit lớn nhất của K. Phép nhân điểm phương pháp nhị phân theo hệ số giảm dần có dạng như sau [4]:

$input: k = (k_{n-1}, ..., k_0)_2, P \in E(F_p), k_{n-1} = 1$

$output: Q = KP$

– –

$1. Q \leftarrow P$

$2.\ for\ i = n-2\ downto\ 0\ do$

$2.1.\ Q \leftarrow 2Q$

$2.2. \text{if}\ (k_i = 1)\ then\ Q \leftarrow Q + P$

$3. return(Q)$

Thông thường, nếu khóa K được tạo đủ mạnh thì số bit "1" trong K sẽ xấp xỉ bằng $n/2$. Khi đó, số phép tính cần thực hiện của thuật toán trên sẽ gồm có $n/2$ phép cộng điểm và n phép nhân đôi điểm.

Về lựa chọn đường cong ECC

Nhóm tác giả sử dụng Elliptic NIST P-256, bởi đây là đường cong được sử dụng nhiều trong thực tế. Đường cong này có các tham số như sau [5]:

Phương trình đường cong:

$y^2 = x^3 - 3x +$
41058363725152142129...
32612978004726840911...
44410159937255548352...
56314039467401291

Số prime:

$p =$ 1157920892103562487626...
974469494075735300861 4...
341529031419553363 1308...
867097853951

Bậc của đường cong:

$n =$ 1157920892103562487626...
974469494075735299969 5...
522413576034242225906 1...
068512044369

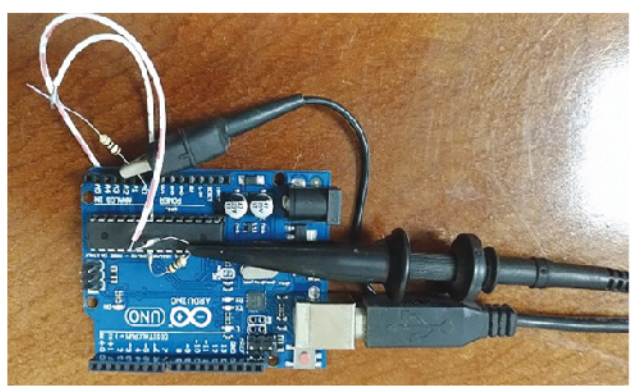
Điểm gốc:

$G =$ (48439561293906451759052 58...
525279791420276294952604 17...
47995844080717082404635286;
36134250956749795798585127...
91958788195661110667298501...
50718771982535684144051 09)

Thiết lập phép đo năng lượng tiêu thụ

Đầu tiên, kit Arduino Uno thực hiện phép nhân điểm với khóa được lưu sẵn trong bộ nhớ của kit. Cùng lúc, máy tính yêu cầu máy thu R&S®ESR đo năng lượng tiêu thụ khi mô-đun mật mã hoạt động. Kết thúc phép đo, dấu vết năng lượng thu được sẽ được gửi lên máy tính điều khiển để phân tích tìm khóa bằng SPA.

Kit Arduino Uno là có một vi điều khiển 8 bit Atmega328p đóng vai trò là module mật mã. Kit này hoạt động với clock là 16 Mhz, điện áp 5V. Kit có một bộ nhớ Flash 32KB đủ để lưu firmware thực thi phép nhân điểm phương pháp nhị phân cho NIST P-256. Vị trí đo năng lượng tiêu thụ trên kit được biểu diễn trên Hình 1.



Hình 1. Vị trí kết nối của đầu dò với các chân nguồn và đất của vi điều khiển Atmeg328p

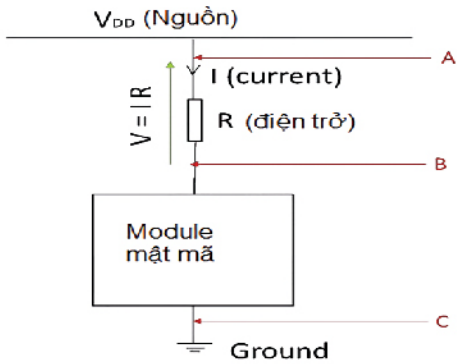
Để đo năng lượng tiêu thụ của kit trực tiếp là điều không thể với thiết bị đo này. Vì vậy, cần đo thông qua giá trị gián tiếp (Hình 3) là công suất tiêu thụ P_{VDK} của mô-đun mật mã. Giá trị này được tính như sau:

$$P_{VDK} = V_{DD}^2 / R \quad (1)$$

Trong đó: V_{DD} là điện áp nguồn của vi điều khiển, R là trở kháng của vi điều khiển hoặc của một điện trở trên đường nguồn. Nếu R không đổi, thì năng lượng tiêu thụ sẽ tỷ lệ thuận với điện áp V_{DD}.

Lưu ý rằng, năng lượng tiêu thụ là công suất tiêu thụ theo thời gian. Như vậy, việc đo trực tiếp

năng lượng tiêu thụ được thay thế bằng bài báo đo điện áp trên vi điều khiển khi kit hoạt động.



Hình 2. Sơ đồ vị trí đo của đầu dò và điện trở dùng trong phép đo

Như sơ đồ Hình 2, có thể đo điện áp giữa điểm A và điểm B hoặc đo giữa điểm B và điểm C. Cả hai cách đo này đều đưa ra được giá trị điện áp tỷ lệ thuận với năng lượng tiêu thụ trong quá trình hoạt động của vi điều khiển Atmega328p. Từ đây về sau sẽ dùng khái niệm năng lượng tiêu thụ để chỉ kết quả đo điện áp.

Thông thường, phép đo được thực hiện tại các tần số là hài của tần số clock. Qua thực nghiệm thấy rằng, kết quả đo dấu vết năng lượng tốt nhất quan sát được tại tần số 47.9 MHz.

Kết quả đo cho thấy được có thể phân biệt giữa các lần thực thi phép nhân điểm được thực hiện trên kit.

Phân tích khóa với SPA

Tấn công SPA trên ECC cần thực hiện hai giai đoạn: Tìm đặc điểm các phép tính ECC trong dấu vết năng lượng và nhận dạng đặc điểm.

Giai đoạn 1: Tìm đặc điểm các phép tính ECC trong dấu vết năng lượng

Cần biết rằng, phép nhân điểm là kết quả của một chuỗi các phép cộng điểm và nhân đôi điểm. Khi thực thi trên kit, mỗi phép tính này sẽ tiêu tốn khoảng thời gian khác nhau. Giả sử có hai điểm trên đường cong Elliptic $P=(P_x,P_y), Q=(Q_x,Q_y)$ và $P \neq -Q$, các phép tính cơ bản trên ECC được biểu diễn như sau:

Phép cộng điểm:

$$\begin{aligned} S &= (S_x, S_y) = P+Q \\ \lambda &= \frac{P_y - Q_y}{P_x - Q_x} \\ S_x &= \lambda^2 - P_x - Q_x \\ S_y &= \lambda(Q_x - S_x) - Q_y \end{aligned} \quad (2)$$

Phép nhân đôi điểm:

$$\begin{aligned} D &= (D_x, D_y) = 2P \\ \lambda &= \frac{3(P_x - 1)}{2P_y} \\ D_x &= \lambda^2 - 2P_x \\ D_y &= \lambda(P_x - D_x) - P_y \end{aligned} \quad (3)$$

Qua hai công thức trên có thể suy ra số phép tính cơ bản cần dùng trong mỗi phép tính nhân đôi/cộng điểm, được mô tả trong Bảng 1 dưới đây.

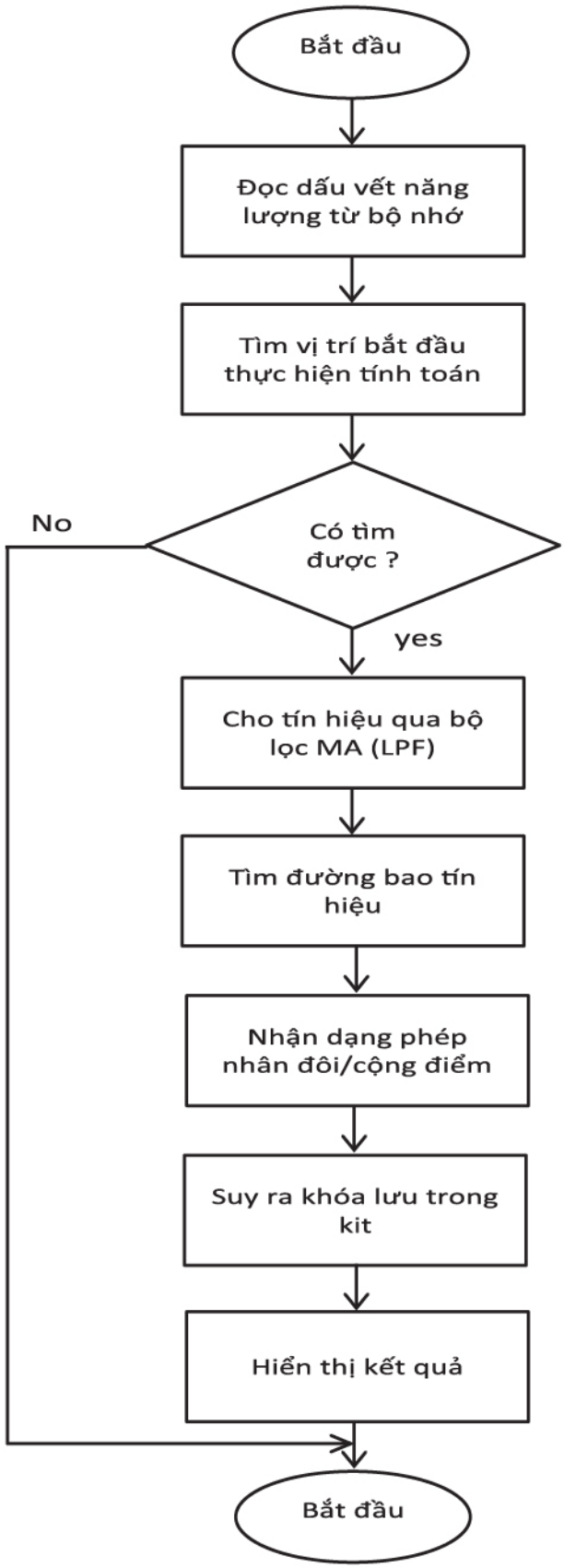
Bảng 1. Thời gian thực thi các phép tính cơ bản trên ECC [6]

Tên phép tính	Số lượng phép tính cơ bản	Ước lượng thời gian tính (chu kỳ clock)
Phép cộng		206
Phép trừ		273
Phép nhân		15803
Phép nghịch đảo		12790
Phép cộng điểm	1 phép nghịch đảo, 6 phép trừ, 2 phép nhân	64524
Phép nhân đôi điểm	1 phép nghịch đảo, 4 phép trừ, 4 phép nhân	95857

Giai đoạn 2: Nhận dạng đặc điểm

Để tính toán bộ chuỗi khóa, cần nhận dạng đặc điểm của hai phép tính cơ bản của ECC trong toàn bộ dấu vết năng lượng thu được. Chương trình nhận dạng được viết trong Matlab với lưu đồ thuật toán như Hình 3.

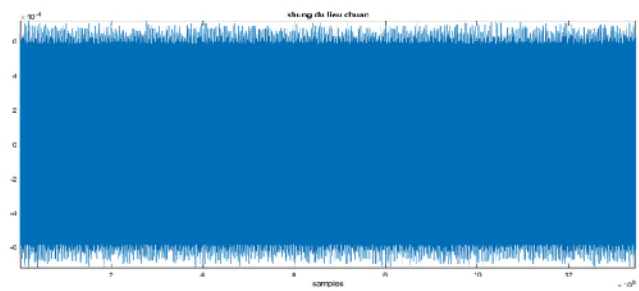
Các bước của lưu đồ trong Hình 3 thực hiện như sau:



Hình 3. Lưu đồ thuật toán chương trình phân tích khóa trên dấu vết năng lượng thu được

Bước 1. Đọc dữ liệu đo năng lượng tiêu thụ do máy thu ESR gửi về.

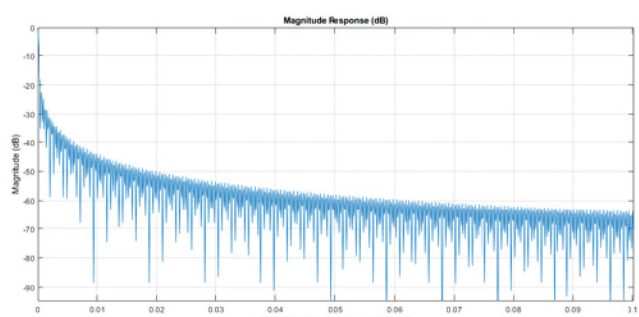
Bước 2. Tìm vị trí thực hiện phép nhân điểm trong dấu vết năng lượng thu được. Một khung trượt kích thước N = 100 mẫu được sử dụng để tìm vị trí bắt đầu và kết thúc phép nhân điểm (Hình 4).



Hình 4. Kết quả tìm khung dữ liệu tương ứng với phép nhân điểm

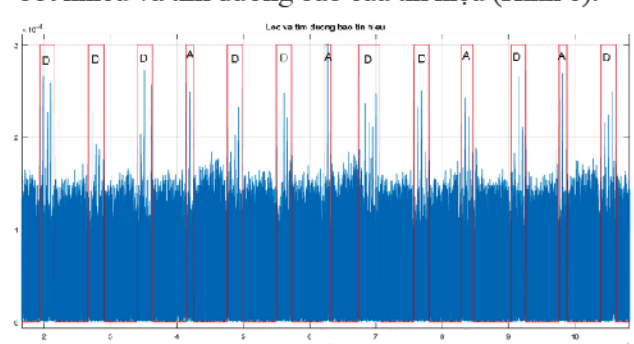
Bước 3. Nếu tìm được vị trí bắt đầu thì chuyển sang lọc dữ liệu. Nếu không tìm thì kết thúc chương trình.

Bước 4. Lọc dữ liệu tìm nền nhiễu với bộ lọc trung bình động (Moving Average - MA) có độ rộng W = 10001, mẫu có đáp ứng tần số như Hình 5.



Hình 5. Đáp ứng tần số của bộ lọc

Bước 5. Từ kết quả của Bước 4, thực hiện loại bỏ bớt nhiễu và tìm đường bao của tín hiệu (Hình 6).



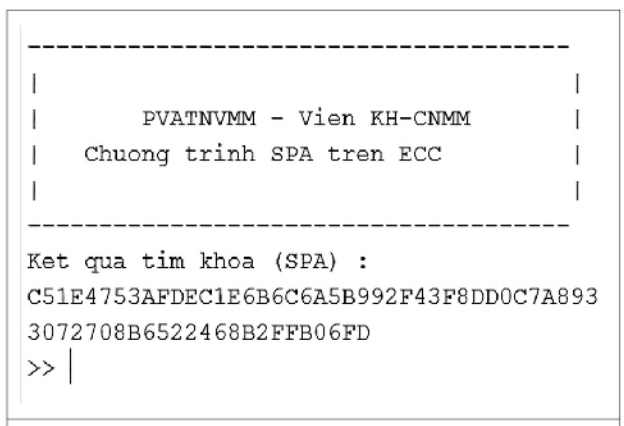
Hình 6. Kết quả lọc và tìm đường bao tín hiệu của một đoạn tín hiệu

Bước 6. Dựa trên biên độ và độ rộng của xung tín hiệu, tìm phép nhân đôi điểm và cộng điểm. Giá trị độ rộng các xung này phụ thuộc vào nhiều yếu tố như tốc độ clock, cách lập trình mô-đun mật mã. Qua thực nghiệm nhận thấy, với kit Arduino Uno, độ rộng xung D (phép nhân đôi điểm) ~ 8.5 ms, độ rộng xung A (phép nhân đôi điểm) ~ 5 ms.

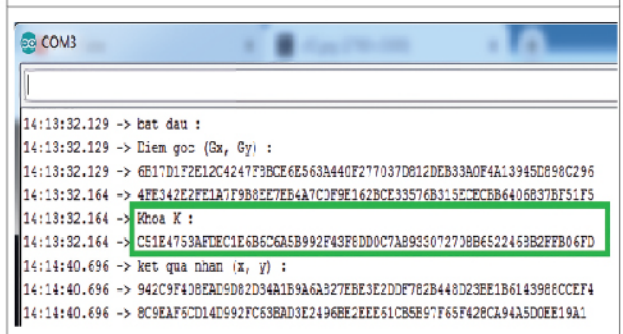
Bước 7. Kết hợp kết quả nhận dạng ở Bước 6, suy ra khóa được sử dụng trong phép nhân điểm bằng 2 nguyên tắc. Thứ nhất, nếu có một phép nhân đôi điểm thì là bit 0 của khóa. Thứ hai, nếu có phép nhân đôi đi kèm với phép cộng điểm thì là bit 1 của khóa.

Bước 8. Hiển thị kết quả và kết thúc chương trình

So sánh khóa phân tích bằng SPA (Hình 7.a) với khóa lưu trong kit (Hình 7.b) nhận thấy, chương trình đã phân tích đúng khóa dùng trong phép nhân điểm phương pháp nhị phân ECC.



a/



b/

Hình 7. Kết quả phân tích khóa của chương trình a/ và khóa lưu trong kit b/

Giải pháp chống tấn công SPA

Có nhiều biện pháp để chống lại tấn công SPA như: sử dụng thuật toán sao cho cân bằng năng lượng các quá trình tính toán trên kit (phương pháp Montgomery ladder), sử dụng phép tính phụ nhằm che đi sự khác biệt trong năng lượng tiêu thụ giữa nhân đôi và cộng điểm (phương pháp chống SPA của Coron) [1].

Phương pháp Montgomery ladder

$input: k = (k_{n-1},...,k_0)_2, P \in E(F_p), k_{n-1} = 1$
$output: Q = KP$

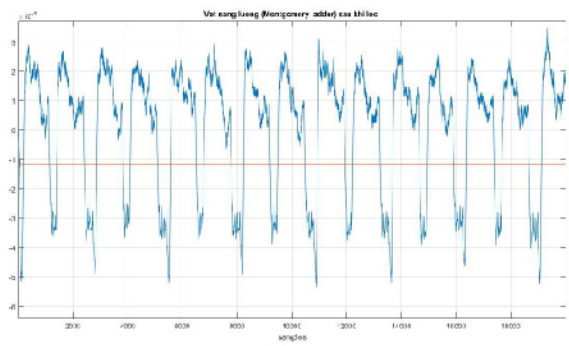
$1. R_0 \leftarrow 0$
$2. R_1 \leftarrow P$
$3.\ for\ i = n-1\ downto\ 0\ do$
  if $(k_i = 0)$ *then*
    3.1. $R_1 \leftarrow R_0 + R_1$
    3.2. $R_0 \leftarrow 2R_0$
  else
    3.3. $R_0 \leftarrow R_0 + R_1$
    3.4. $R_1 \leftarrow 2R_1$
$4. return(R_0)$

Phương pháp chống SPA của Coron

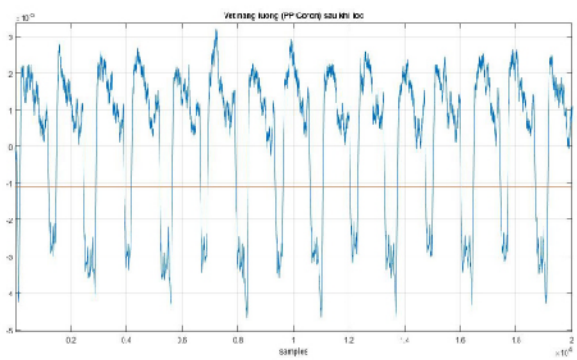
$input: k = (k_{n-1},...,k_0)_2, P \in E(F_p), k_{n-1} = 1$
$output: Q = KP$

$1. Q[0] \leftarrow P$
$2.\ for\ i = n-2\ downto\ 0\ do$
  2.1. $Q[0] \leftarrow 2Q[0]$
  2.2. $Q[1] \leftarrow Q[0] + P$
  2.3. $Q[0] \leftarrow Q[k_i]$
$3. return(Q)$

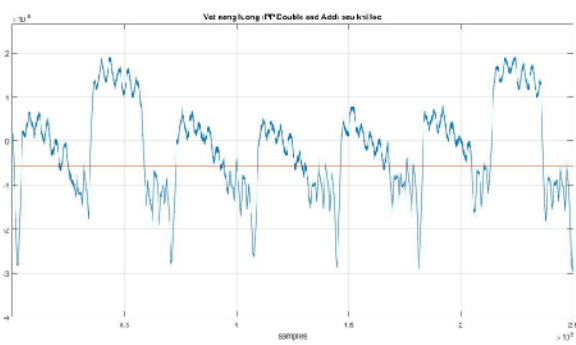
Kết quả đo năng lượng tiêu thụ trên kit khi sử dụng phương pháp Montgomery ladder và Coron so sánh với phương pháp Double and Add (đã trình bày trên) được biểu diễn trên Hình 8.



a/



b/



c/

Hình 8. Kết quả đo và phân tích vết năng lượng với phương pháp Montgomery ladder (a), phương pháp của Coron (b) và phương pháp Double and Add (c)

Có thể thấy rằng vệt năng lượng tiêu thụ trên Hình 8.a và b khác so với c. Điểm khác biệt lớn nhất là thời gian và biên độ của tín hiệu sau khi lọc. Ở Hình 8.a và b năng lượng kit dùng để tính phép nhân điểm với bit '0' và bit '1' của khóa là tương đương nhau cả về thời gian và biên độ. Còn Hình 8.c thấy rõ sự khác biệt khi tính bit '0' và bit '1'. Điều này đã được dự đoán từ cách triển khai thuật toán ở trên và được chứng minh thông qua kết quả đo năng lượng tiêu thụ. Nhờ đặc trưng này mà ECC với phương pháp Montgomery ladder và Coron chống được tấn công SPA.

Cần lưu ý rằng, các biện pháp này có thể bảo vệ ECC trước tấn công SPA, nhưng có thể không hiệu quả trước các tấn công phân tích năng lượng dạng khác như DPA, High-order DPA, các dạng tấn công chủ động.

Kết luận

Bài báo đã trình bày quá trình thực hiện tấn công SPA lên phương pháp nhân điểm phương pháp nhị phân của ECC. Thông qua phân tích và nhận dạng đặc điểm các phép tính cơ bản trên dấu vết năng lượng đã khôi phục được khóa lưu trong kit. Kết quả của bài báo cho thấy có sự mất an toàn của phép nhân điểm nhị phân ECC đối với tấn công phân tích năng lượng SPA. Thực nghiệm được thực hiện trên đường cong NIST P-256. Tuy nhiên, tấn công này có thể mở rộng cho đường cong bất kỳ.❖

TÀI LIỆU THAM KHẢO

1. Coron J. S., "Resistance against Diffrential Power Analysis for Elliptic Curve Cryptosystems", In Proceedings of CHES, 1999.
2. Miller V. S., "Use of Elliptic Curves in Cryptography", Proceedings of Crypto 85, LNCS 218, Berlin, 1986.
3. Koblitz N., "Elliptic Curve Cryptosystems, Mathematics of Computation", 1987.
4. Keke Wu, , Huiyun Li, Tingding Chen, "Simple Power Analysis on Elliptic Curve Cryptosystems and Countermeasures: Practical Work", Technical Report, 2003.
5. "FIPS PUB 186-4-federal information processing standards publication digital signature standard (DSS)", The National Institute of Standards and Technology (NIST), 2013.
6. Cockrum C.K., "Implementation of an Elliptic Curve Cryptosystem on an 8-bit Microcontroller", 2009.