# Kết quả thực thi tấn công phân tích bức xạ điện từ đối với thẻ thông minh

**Trần Ngọc Quý, Phùng Văn Quyền**

***Tóm tắt*— Tấn công phân tích điện từ là một dạng tấn công kênh kề có thể được sử dụng để khôi phục thông tin bí mật của thiết bị mật mã thông qua bức xạ điện từ phát xạ ra từ thiết bị. Hiệu quả của tấn công phụ thuộc nhiều vào chất lượng của bức xạ điện từ đo được bởi hệ thống đo và phương pháp mô hình bức xạ điện từ sử dụng trong quá trình tấn công khôi phục khóa. Trong bài báo này, nhóm tác giả sẽ trình bày quy trình thực hiện các phương pháp tấn công phân tích bức xạ điện từ và các kết quả thực nghiệm tấn công lên smartcard trong đó có đánh giá sự ảnh hưởng của hệ thống đo, mô hình bức xạ điện từ đến hiệu quả của tấn công.**

***Abstract*— Electromagnetic analysis attack is a form of side channel attack that can be used to reveal secret information of a cryptographic device by examination of electromagnetic radiations. The effectiveness of EMA has a large dependences on the quality of the electromagnetic radiation measured by the measuring system and how the EM traces are simulated during the key recovery procedures. In this paper, we propose the practical procedure for electromagnetic analysis attack methods and the experimental results of EMA on smartcard that implemented AES algorithm, including assessing the influence of measuring system, radiation leakage model on effectiveness of attacks.**

***Từ khóa— tấn công phân tích điện từ; tấn công kênh kề; rò rỉ thông tin từ bức xạ điện từ.***

***Keywords— Electromagnetic analysis; side channel attack; EM leakage.***

## I. GIỚI THIỆU

Thẻ thông minh được sử dụng trong nhiều ứng dụng liên quan đến bảo mật như nhận dạng cá nhân, thẻ thanh toán ngân hàng và bảo mật máy tính. Để đảm bảo an toàn cho các ứng dụng các thuật toán và giao thức mật mã thường được cài đặt trên thẻ. Về mặt toán học, các thuật toán và giao thức này đã được chứng minh là an toàn, tuy nhiên hệ thống vẫn có thể bị phá vỡ vì các thông tin bí mật của thẻ thông minh có thể được tìm thấy bằng cách sử dụng các tấn công kênh kề, chẳng hạn như tấn công phâ n tích thời gian [1], tấn công phân tích tiêu thụ điện năng [2, 15, 16, 17], cũng như các cuộc tấn công phân tích điện từ (EMA) [3, 18, 19].

Tấn công EMA được thực hiện bằng cách phân tích các bức xạ EM thu được từ thiết bị bởi các công cụ thống kê để tìm khóa của thiết bị. Một số kỹ thuật tấn công EMA hiệu quả như tấn công phân tích điện từ vi sai (DEMA) [3] và tấn công phân tích điện từ tương quan (CEMA) [4, 5] được sử dụng phổ biến để phân tích bức xạ EM của thiết bị mật mã bởi phân tích vi sai và phân tích tương quan, qua đó trích xuất được các thông tin về khóa của thiết bị.

Trong các nghiên cứu gần đây, tấn công EMA đã được tiến hành trên nhiều nền tảng, thuật toán. Năm 2001, một tấn công EMA thực tế đầu tiên được Gandolfi và cộng sự [3] thực hiện, các tác giả đã mô tả cách sử dụng tín hiệu kênh kề là bức xạ EM để tấn công cho ba loại chip CMOS khác nhau. Agrawal và cộng sự [4] đã có thể phân loại các loại bức xạ EM thành hai dạng là bức xạ có chủ ý và các bức xạ bị điều chế bởi một số sóng mang. Bằng cách sử dụng các dạng bức xạ EM trên, các tác giả đã tấn công các thuật toán DES, RSA và COMP128 được

Bài báo được nhận ngày 21/8/2023. Bài báo được nhận xét bởi phản biện thứ nhất vào ngày 05/9/2023 và được chấp nhận đăng vào ngày 10/10/2023. Bài báo được nhận xét bởi phản biện thứ hai vào ngày 05/9/2023 và được chấp nhận đăng vào ngày 06/09/2023.

cài đặt trên thẻ thông minh và các thiết bị phần cứng thực thi SSL. Vào năm 2013, Montminy và cộng sự [6] đã thực hiện tấn công DEMA thành công đối với AES được cài đặt trên bộ vi xử lý 32 bit. Longo và cộng sự [7] vào năm 2015 đã tiến hành những phân tích chuyên sâu về bức xạ EM trên bo mạch phát triển sử dụng các vi điều khiển ARM. Mục tiêu của tấn công là đối với AES được cài đặt mềm, sử dụng thư viện OpenSSL, trên lõi ARM và AES đã được cứng hóa bởi bộ đồng xử lý mật mã trên ARM NEON. Gebotys và cộng sự [8] tiến hành thực thi các tấn công trên các ứng dụng thực tế được cài đặt trên thiết bị PDA có sử dụng thuật toán AES và ECC. Các tác giả khai thác thông tin của bức xạ EM sử dụng kỹ thuật biểu đồ tần số - thời gian để có được cả thông tin về tần số và thời gian của bức xạ EM.

Trong hầu hết các nghiên cứu về EMA sử dụng các tấn công phổ biến DEMA hoặc CEMA. Với các công bố hiện tại chỉ mô tả nguyên tắc tấn công mà chưa đưa ra các quy trình thực tế để thực hiện. Hơn nữa, việc so sánh hiệu quả của DEMA và CEMA cũng vẫn chưa được công bố. Vì vậy, trong bài báo này nhóm tác giả trình bày chi tiết quy trình thực nghiệm các phương pháp tấn công DEMA, CEMA cũng như so sánh hiệu quả của chúng dựa trên đánh giá mô hình ước lượng rò rỉ bức xạ EM. Do bức xạ EM của các thiết bị thường yếu và chịu nhiều ảnh hưởng bởi nhiễu [3] nên hệ thống đo bức xạ EM trong đó có các đầu đo EM có ảnh hưởng lớn đến hiệu quả của tấn công. Vấn đề này cũng được xem xét trong bài báo này thông qua những kết quả thực nghiệm cụ thể.

Bài báo được tổ chức như sau: Phần II cung cấp thông tin cơ bản về bức xạ EM và cơ sở của việc rò rỉ thông tin thông qua EM. Phần III mô tả phương pháp, quy trình thực hiện tấn công DEMA và CEMA. Phần IV trình bày kết quả thực nghiệm tấn công DEMA và CEMA cho thuật toán AES-128 được cài đặt trên thẻ thông minh. Phần V là kết luận bài báo và thảo luận các vấn đề mở.

## II. Rò rỉ thông tin từ bức xạ EM

### A. *Bức xạ EM từ thiết bị CMOS*

Các chip VLSI hiện nay thường được thiết kế dựa trên các cổng logic CMOS. Trong các thiết bị CMOS, tất cả các hoạt động được xử lý dưới sự điều khiển của tín hiệu đồng hồ và cạnh lên hoặc cạnh xuống của đồng hồ sẽ kích hoạt tất cả các cổng chuyển đổi trạng thái logic. Do đặc tính chuyển mạch của các cổng logic trong các vi mạch số, cường độ dòng điện khi vi mạch hoạt động thường ở dạng dòng xung có giá trị thay đổi tại thời điểm có sự chuyển mạch của các cổng logic tương ứng với sườn lên hoặc sườn xuống của tín hiệu đồng hồ. Cường độ dòng điện là một hàm của điện áp đầu ra, có thể được biểu diễn dưới dạng: $i(t) = C_L.\frac{dv(t)}{dt}$ [9].

Theo phương trình Maxwell trong lý thuyết trường điện từ, dòng điện biến đổi theo thời gian trong mạch sẽ tạo ra trường điện từ. Điện trường và từ trường tương tác với nhau, lan truyền từ mạch điện ra không gian dưới dạng sóng điện từ. Quá trình này diễn ra cùng với sự truyền năng lượng, được gọi là bức xạ điện từ [4]. Do đó, các vi mạch số sẽ tạo ra một lượng lớn bức xạ điện từ khi hoạt động. Đặc biệt là các thành phần như bộ điều khiển, ALU và bus, trong đó trạng thái của chúng thay đổi phụ thuộc vào đối tượng điều khiển, phép toán thực hiện, hay dữ liệu được chuyển trên bus. Tất cả các thao tác này hoạt động dưới sự điều khiển của tín hiệu đồng hồ. Có một số mối liên hệ giữa những thông tin trạng thái này và tín hiệu bức xạ điện từ. Bằng cách sử dụng mối quan hệ tương quan và phân tích mối quan hệ giữa chúng, có thể lấy dữ liệu từ các thành phần này và đó chính là sự rò rỉ thông tin từ thiết bị thông qua bức xạ điện từ.

Bức xạ EM có thể được phân thành hai loại: bức xạ EM trực tiếp và bức xạ EM gián tiếp. Những loại này xuất phát từ những lý do khác nhau và có đặc tính truyền tải khác nhau.

*Bức xạ điện từ trực tiếp.* Các thành phần logic trong mạch thay đổi trạng thái một cách đồng bộ trong khi thực thi các phép toán và được

điều khiển bởi đồng hồ hệ thống. Thông thường, logic 0 đại diện cho dòng điện mức thấp và logic 1 đại diện cho dòng điện mức cao. Sự thay đổi đột ngột của dòng điện trong các thành phần logic dẫn đến bức xạ EM trực tiếp. Những bức xạ này có thành phần tần số cao và thường có thể được phát hiện bằng đầu đo trường gần đặt gần chip. Để có được bức EM trực tiếp tốt có thể cần phải tiến hành mở vỏ chip [3,5].

*Bức xạ điện từ gián tiếp.* Bức xạ EM gián tiếp đôi khi bị các nhà thiết kế chip bỏ qua vì chúng là kết quả của hiệu ứng ghép nối giữa các thành phần khác nhau trên chip. Các bức xạ gián tiếp là các tín hiệu điều chế bởi nguồn sóng mang mạnh nhất chính tín hiệu đồng hồ của mạch điện. Chúng được tạo ra do sự truyền tín hiệu điện giữa các thành phần được đã được tích hợp trong trên cùng một chip và ở đó mỗi thành phần có thể coi như một ăng-ten phát. Ví dụ, tín hiệu EM từ bus dữ liệu có thể bị điều chế bởi sóng mang mạnh là tín hiệu đồng hồ chủ của hệ thống và điều này làm độ lớn của bức xạ EM tăng lên. Loại tín hiệu này được gọi là tín hiệu điều chế biên độ, nhưng đôi khi bức xạ EM có thể ở dạng tín hiệu điều chế tần số khi bức xạ EM của bus dữ liệu được điều chế bởi một sóng mang có độ lớn nhỏ. Hơn nữa, đối với những chip có thành thành phần tương tự [10], tín hiệu được điều chế sẽ rò rỉ đến phần tương tự trên chip. Ở phần tương tự, khối RF điều chế lại tín hiệu EM và gửi nó qua ăng-ten. Vì lý do này, bức xạ EM gián tiếp có thể được phát hiện ở khoảng cách xa hơn nhiều so với bức xạ EM trực tiếp.

### *B. Mô hình rò rỉ thông tin từ bức xạ EM*

Do tín hiệu EM tỷ lệ thuận với dòng điện nên mô hình rò rỉ để ước lượng mức tiêu thụ điện năng trong DPA cũng có thể được áp dụng để ước lượng cho bức xạ EM. Trong bài báo gốc của Kocher [2], mô hình rò rỉ kênh kề được sử dụng dựa trên trọng số Hamming (HW) của bit hoặc byte dữ liệu mà người tấn công cố gắng dự đoán. Mô hình này, được gọi là mô hình rò rỉ HW, cho rằng bit 0 không dẫn đến bức xạ EM, trong khi bit 1 liên quan đến một lượng bức xạ EM đáng kể. Do đó, các chuyển đổi 0 → 0 và 1 → 0 được coi là không dẫn đến bức xạ EM; các chuyển đổi 0 → 1 và 1 → 1 được cho là sinh ra bức xạ EM. Trên thực tế, mô hình này không hoàn toàn chính xác với thực tế, ngoại trừ trong trường hợp mức logic của thanh ghi dữ liệu được thiết lập trước là 0 trước khi được cập nhật, bởi trong trường hợp này khoảng cách Hamming (HD) bằng với HW của nó.

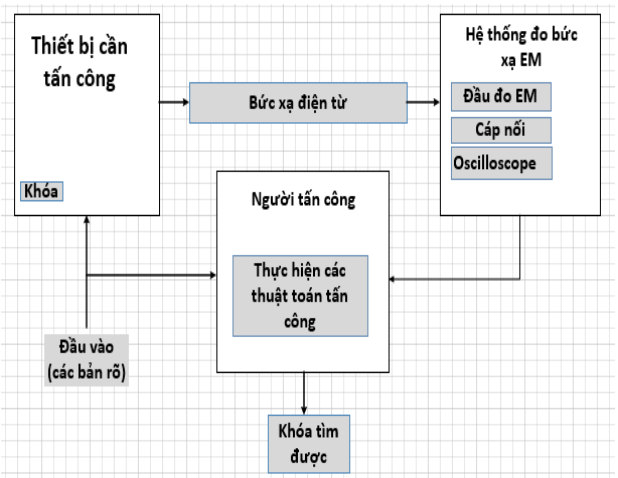
Vì vậy, mô hình rò rỉ HW có thể được cải thiện bằng cách xem xét trạng thái chuyển mạch thay vì trạng thái đầu ra của cổng logic[11]: các chuyển đổi 0 → 0 và 1 → 1 không dẫn đến bức xạ EM; chuyển tiếp 0 → 1 và 1 → 0 sinh ra bức xạ EM. Mô hình rò rỉ này được gọi là mô hình rò rỉ HD. Một mô hình khác có thể sử dụng để ước lượng bức xạ EM như mô hình rò rỉ phân biệt sự chuyển trạng thái chỉ từ 0→1 hoặc ngược lại được nghiên cứu trong [12], nhưng kết quả thu được tương tự với kết quả khi sử dụng với mô hình HD.

## III. TẤN CÔNG PHÂN TÍCH BỨC XẠ ĐIỆN TỪ

Phân tích các vết bức xạ điện từ của thiết bị thực hiện khai thác các thông tin bí mật trong thiết bị giống với việc phân tích vết điện năng tiêu thụ và đã được mô tả tổng quan trong [13]. Thay vì phân tích các vết điện năng tiêu thụ đo được từ thiết bị, người tấn công EMA sử dụng một đầu đo điện từ để thu thập các vết bức xạ điện từ. Tấn công sử dụng thông tin kênh kề là các vết bức xạ EM có ưu điểm hơn tấn công phân tích điện năng tiêu thụ là bởi các vết EM có thể thu được mà không cần tác động vào mạch điện của thiết bị. Tài liệu [14] của Mulder giới thiệu tổng quan về dạng tấn công phân tích bức xạ điện từ.

Hệ thống thực hiện tấn công kênh kề sử dụng bức xạ EM gồm ba thành phần chính: thiết bị cần tấn công, hệ thống đo vết EM và người thực thi tấn công như được mô tả trên Hình 1. DUT là một thiết bị mật mã lưu trữ khóa và thực hiện thuật toán mã hóa. Trong quá trình DUT thực thi tính toán, nó làm rò rỉ thông tin kênh kề dưới dạng bức xạ điện từ mà hệ thống đo có thể thu

thập được. Bức xạ điện từ thu thập được có thể được coi là vết EM và được người tấn công sử dụng để dự đoán khóa của DUT.




Hình 1. Mô hình thực hiện tấn công EMA

Nguyên lý thực hiện EMA có thể được mô tả như sau: Thiết bị mật mã lưu trữ khóa, thực thi thuật toán mật mã với $M$ bản rõ đầu vào đã biết $p_i$ $(i = 1, \dots, M)$. Mỗi khi thiết bị thực thi mã hóa với một bản rõ $p_i$, một vết EM được thu thập bởi hệ thống đo và được ký hiệu là $x_i(t)$. Khi $x_i(t)$ được lưu trữ trên máy tính nó được thể hiện là một véc-tơ với $t = 1,2, \dots, N$. Người tấn công lựa chọn một điểm tấn công trên thuật toán mã. Điểm tấn công được lựa chọn là điểm mà thuật toán mật mã có giá trị trung gian là một hàm có sự phụ thuộc vào bản rõ đầu vào $p_i$ và $k$ là một phần nhỏ của khóa. Một phần nhỏ của khóa ở đây có ý nghĩa là việc thực hiện các kỹ thuật thống kê đối với các vết EM là có thể thực hiện được.

Để thực thi tấn công, người tấn công phải có thể dự đoán được rò rỉ kênh kề tại giá trị trung gian tấn công. Việc này được thực hiện bằng cách sử dụng một mô hình rò rỉ bức xạ EM như HW hoặc HD. Gọi $L_{k,i}$ là rò rỉ kênh kề giả định đối với bản rõ đầu vào $p_i$ và một giả thiết về khóa $k$. Người tấn công, sẽ tính bức xạ điện từ giả định với các bản rõ đầu vào $p_i$ và tất cả các giá trị có thể có của $k$. Giả sử rằng, với giá trị khóa giả thiết là đúng với khóa thực hiện trong thiết bị $k = k^c$, sẽ tồn tại một mối quan hệ thống kê giữa bức xạ điện từ dự đoán $L_{k,i}; i = 1{:}M$ và bức xạ điện từ thực tế đo được $x_i(t); i = 1{:}M$ tại một điểm $t$ chưa biết. Để phát hiện sự phụ thuộc này và xác định được giá trị khóa $k$ mà thiết bị sử dụng, thời điểm thiết bị xử lý giá trị trung gian tấn công thì người tấn công sẽ sử dụng một kiểm tra thống kê hay còn gọi là bộ quyết định. Dựa trên kỹ thuật thống kê mà bộ quyết định sử dụng là tính vi sai hay tương quan mà chúng ta có hai phương pháp tấn công phân tích bức xạ điện từ tương ứng là tấn công phân tích bức xạ điện từ vi sai (DEMA) và tấn công phân tích bức xạ điện từ tương quan (CEMA) sẽ được trình bày sau đây.

### A. *Tấn công DEMA*

Tấn công DEMA dựa trên tấn công DPA được đề xuất bởi Kocher [2]. DEMA sử dụng kỹ thuật thống kê là tính vi sai hay cụ thể là tính vi sai giữa hai giá trị trung bình (DoM) để kiểm tra sự phụ thuộc giữa các rò rỉ kênh kề. Kiểm tra DoM chia tập vết EM thành hai tập con $S_{1k} = x_i(t)|L_{k,i} = \delta$ và $S_{0k} = x_i(t)|L_{k,i} \neq \delta$ dựa trên giá trị rò rỉ kênh kề ước lượng $L_{k,i}$. Ví dụ, khi tập trung vào một bit đơn $L_{k^c,i} \in \{0,1\}$, chúng ta có thể phân chia tập vết theo $L_{k,i} = 1$ hay $L_{k,i} = 0$. Kế đến, giá trị trung bình của từng tập vết được tính và độ lệch giữa các giá trị trung bình bày được xác định và gọi là vết vi sai. Với khóa giả thiết $k = k^c$ là đúng với khóa được thực thi trên thiết bị, ước lượng về $L_{k,i}$ là đúng và việc phân chia các EM thành hai tập tương ứng với hai giá trị khác nhau của $L_{k,i}$. Khi đó, sẽ tồn tại một đỉnh trên vết vi sai còn gọi là gai tại đúng thời điểm khi giá trị trung gian tấn công được thiết bị thực hiện. Với các khóa giả thiết $k \neq k^c$, việc phân chia tập vết là ngẫu nhiên và kết quả là vết vi sai sẽ bằng phẳng. Do đó, giá trị đúng của $k$ có thể được xác định là giá trị $k$ mà tồn tại các gai, phân biệt được trên vết vi sai. Như vậy, bộ quyết định của DEMA sẽ tính (1) cho tất cả các khóa giả thiết của $k$ và lựa chọn khóa giả thiết đúng nhất theo (2).

$$\mathcal{D}_k = mean\left(x_i(t)\middle|L_{k,i} = \delta\right) - mean\left(x_i(t)\middle|L_{k,i} \neq \delta\right) \quad (1)$$

$$(k^c, t^*) = \underset{k}{argmax}(\mathcal{D}_k(t)) \quad (2)$$

**Thuật toán 1:** Tấn công DEMA

**Đầu vào:**

$p_{i,l}$: các bản rõ $i = 1, \dots, M; l = 1{:}16$

$\boldsymbol{x}_{i,j}$ : các vết EM $i = 1, \dots, M; j = 1, \dots, N$

$b_s$ : vị trí bít tấn công.

**Đầu ra:**

$k_l^c, t_l^*$: 16 byte khóa đúng, thời điểm các khóa được xử lý; $l = 1{:}16$

*1: for1* $l = 1{:}16$
*2:* $for2\ \ k = 1{:}\mathbb{K}\ do$
*3:* $for3\ \ i = 1{:}M\ do$
*4:* $z_{i,k} = f(p_{i,l}, k)$
*5:* $L_{i,k} = bitget(z_{i,k}, b_s)$
*6:* $S_{1,k} = \{x_{i,j}\} | L_{i,k} == 1$
*7:* $S_{0,k} = \{x_{i,j}\} | L_{i,k} == 0$
*8:* $endfor3$
*9:* $endfor2$
*10:* $for4\ k = 1{:}\mathbb{K}\ do$
*11:* $\mathcal{D}_{k,j} = mean(S_{1,k}) \ - mean(S_{0,k})$
*12:* $endfor4$
*13:* $return\ (k_l^c, t_l^*) = \underset{k,j}{argmax}(\mathcal{D}_{k,j})$
14: $endfor1$

Dựa trên nguyên tắc của DEMA, nhóm tác giả đề xuất quy trình thực hiện thực tế đối với DEMA theo Thuật toán 1. Để chuẩn bị thực hiện tấn công, cần chuẩn bị dữ liệu phục vụ tấn công là các bản rõ đầu vào của thuật toán và các vết EM thu được khi thiết bị thực thi thuật toán với các bản rõ đầu vào này. Với mỗi byte khóa cần tấn công được thể hiện bởi tham số $l$ tại dòng 1 của Thuật toán 1, các bước sau được thực thi:

*Bước 1*: Đối với tất cả các khóa giả thuyết, sắp xếp các vết EM thành hai nhóm $S_{0k}$ và $S_{1k}$ theo các giá trị rò rỉ giả thuyết $L_{i,k}$ là 1 hoặc 0. Hàm $bitget(z_{i,k}, b_s)$ lấy lại giá trị của một bit trong $z_{i,k}$ với vị trí $b_s$. $z_{i,k}$là giá trị trung gian được tính bằng hàm lựa chọn $f(p_i, k)$. Để tấn công tìm ra giá trị khóa, $f$ được chọn để có thể tính toán với các giá trị liên quan đến bản rõ đầu vào đã biết và một phần của toàn bộ khóa. Ví dụ: $f$ thường là phép tính đầu ra S-hộp của thuật toán mật mã.

*Bước 2*: Tính các vết vi sai $\mathcal{D}_k$ cho tất cả các khóa giả thiết.

*Bước 3*: Chọn $k$; $(k = 0{:}255)$ sao cho $\mathcal{D}_k$ có giá trị lớn nhất là khóa đúng và thời gian tương ứng để thiết bị xử lý khóa đó theo dòng 13 của Thuật toán 1.

*B. Tấn công CEMA*

Tấn công CEMA dựa trên tấn công CPA được đề xuất trong [11]. Người tấn công xem xét mối tương quan giữa các vết EM thực tế và giá trị EM giả định được tính toán bằng một mô hình rò rỉ bức xạ. Bộ quyết định của CEMA sử dụng hệ số tương quan Pearson như trong (3) để kiểm tra về mối quan hệ tuyến tính giữa hai biến $x_i(t)$ và $L_{i,k}$. Bộ quyết định tính toán biểu thức (3) với tất cả các giá trị giả thiết của khóa $k$ và chọn một khóa giả thiết là đúng nhất theo (4). Dựa trên nguyên tắc CEMA, chúng tôi đề xuất quy trình CEMA thực tế như mô tả bởi Thuật toán 2.

$$\rho_k(t) = \frac{cov(x_i(t), L_{i,k})}{\sigma(x_i(t))\sigma(L_{i,k})}; với\ i = 1{:}M; t = 1{:}N \quad (3)$$

$$(k^c, t^*) = \underset{k,t}{argmax}(\rho_k(t)) \quad (4)$$

Tương tự như tấn công DEMA, đầu vào của tấn công CEMA cũng là các bản rõ, các vết EM tương ứng khi thiết bị thực thi mã hóa cho các bản rõ này, và mô hình rò rỉ kênh kề $L$. Với mỗi byte cần tấn công, các bước sau được thực hiện:

*Bước 1:* Với tất cả các khóa giả thiết, giá trị bức xạ EM giả thiết $h_{i,k}$ được tính bởi một mô hình rò rỉ bức xạ điện từ $L$ và hàm lựa chọn $f(p_i, k)$. $f$ được chọn giống với tấn công DEMA và $L$ có thể chọn là HW hay HD.

*Bước 2:* Tính tương quan giữa giá trị bức xạ EM giả thiết và giá trị EM thực tế bởi công thức tương quan Pearson như ở dòng 9 của Thuật toán 2.

*Bước 3:* Quyết định khóa đúng: Lựa chọn giá trị $k$ đúng nhất tương ứng với giá trị lớn nhất của hệ số tương quan Pearson và thời điểm thiết bị xử lý khóa này như mô tả ở dòng 12 của Thuật toán 2.

**Thuật toán 2:** Tấn công CEMA

**Đầu vào:**

$p_{i,l}$: các bản rõ $i = 1, \dots, M; l = 1{:}16$

$\boldsymbol{x}_{i,j}$ : các vết EM $i = 1, \dots, M; j = 1, \dots, N$

$L$ : mô hình rò rỉ bức xạ EM.

**Đầu ra:**

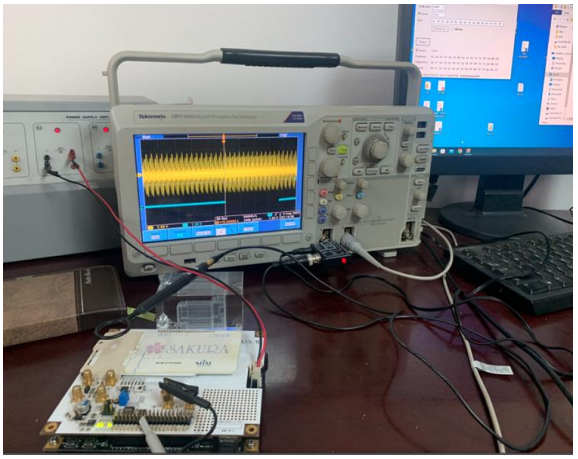
$k_l^c, t_l^*$: 16 byte khóa đúng, thời điểm các khóa được xử lý; $l = 1{:}16$

1: $for1\ l = 1{:}16$
2: $for2\ k = 1{:}\mathbb{K}\ do$
3: $for3\ i = 1{:}M\ do$
4: $h_{i,k} = L\big(f(p_i, k)\big);$
5: $endfor3$
6: $endfor2$
7: $for4\ k = 1{:}\mathbb{K}\ do$
8: $for5\ j = 1{:}N\ do$
9: $r_{k,j} = \frac{\sum_{i=1}^{M}(h_{i,k}-\bar{h}_k).(t_{i,j}-\bar{t}_j)}{\sqrt{\sum_{i=1}^{M}(h_{i,k}-\bar{h}_k)^2.\sum_{i=1}^{M}(t_{i,j}-\bar{t}_j)^2}}$
10: $endfor5$
11: $endfor4$
12: $return\ (k_l^c, t_l^*) = \underset{k,j}{argmax}\big(r_{k,j}\big)$
13: $endfor1$

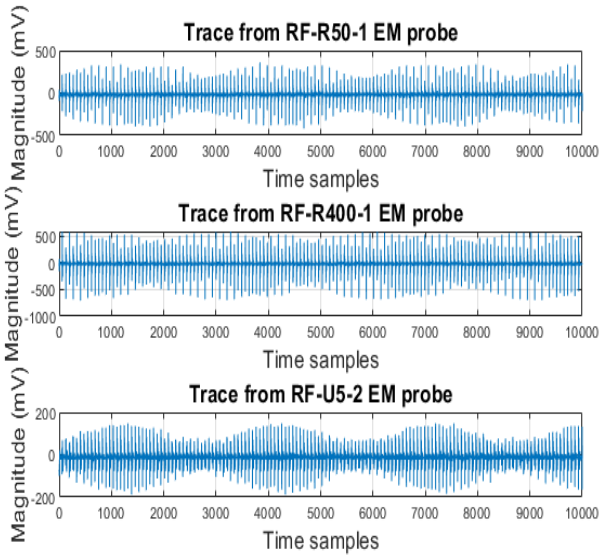
## IV. THỰC NGHIỆM

Trong phần này, nhóm tác giả trình bày kết quả thực nghiệm khi tiến hành các cuộc tấn công DEMA và CEMA đối với AES-128. Hình 2 mô tả môi trường thử nghiệm, AES-128 được cài đặt mềm trên thẻ thông minh Atmega8515 và thẻ thông minh này được điều khiển bởi bo mạch SAKURA-G/W. Tần số xung nhịp hoạt động của thẻ thông minh là 3,57 MHz. Đầu đo Langer EM được kết nối với máy hiện sóng (Tektronix DPO-3052) để đo bức xạ EM ở tốc độ lấy mẫu 100Mhz. Để đánh giá chất lượng các đầu đo đến hiệu quả của các tấn công chúng tôi sử dụng 03 bộ vết EM được thu thập bằng ba đầu dò EM: RF-R50-1, đặt cách thẻ thông minh 3 cm, RF-R400-1, đặt cách thẻ thông minh 5 cm và đặt RF-U5-2 trên bề mặt của thẻ thông minh. Đây là các đầu đo trường gần thụ động để đo từ trường từ 30 MHz đến 3 GHz trên thẻ thông minh. Đầu dò RF-R400-1 và RF-R50-1 có thể phát hiện bức xạ điện từ từ khoảng cách xa hơn. Với độ phân giải cao hơn, đầu dò RF-U5-2 được thiết kế để phát hiện các nguồn EM chính xác hơn. Hình 3 mô tả một vết EM điển hình trong mỗi bộ vết EM.

Các thuật toán tấn công được cài đặt và thực hiện sử dụng phần mềm MATLAB 2017b chạy trên máy tính cá nhân. Khả năng thực hiện tấn công và hiệu quả của tấn công được đánh giá như sau: (1) Khả năng khôi phục khóa đúng: Để xác nhận rằng các tấn công có thể khôi phục được khóa đúng được sử dụng bởi AES-128, nhóm tác giả đã biểu diễn vết vi sai hoặc tương quan của tất cả các khóa giả thiết. Một tấn công được coi là thành công nếu trong các vết vi sai hoặc tương quan tồn tại một vết có xuất hiện các gai đủ lớn có thể phân biệt được với các giá trị còn lại; (2) Hiệu quả của tấn công là số lượng vết $N_a$ sử dụng cho tấn công để tấn công có thể khôi phục được khóa đúng. Để xác định $N_a$, vi sai hay hệ số tương quan sẽ được tính toán theo số vết tấn công sử dụng và $N_a$ là số vết EM để tấn công có thể phân biệt được giữa khóa đúng và khóa khác.



Hình 2. Môi trường thực nghiệm tấn công EMA

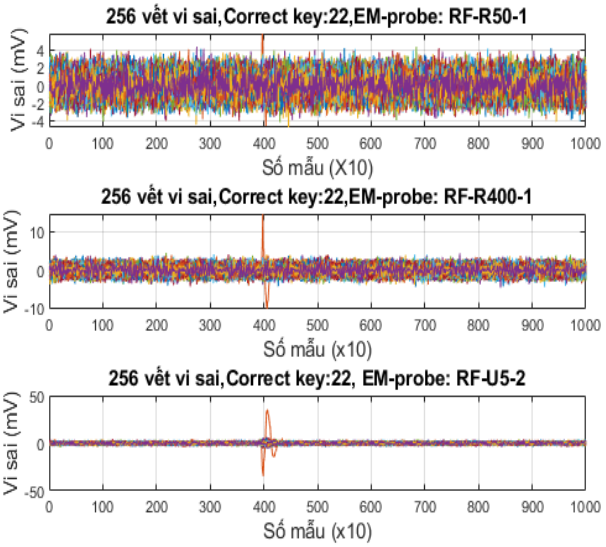



Hình 3. Các vết EM của thẻ thông minh Atmega 8515 khi thực thi AES-128

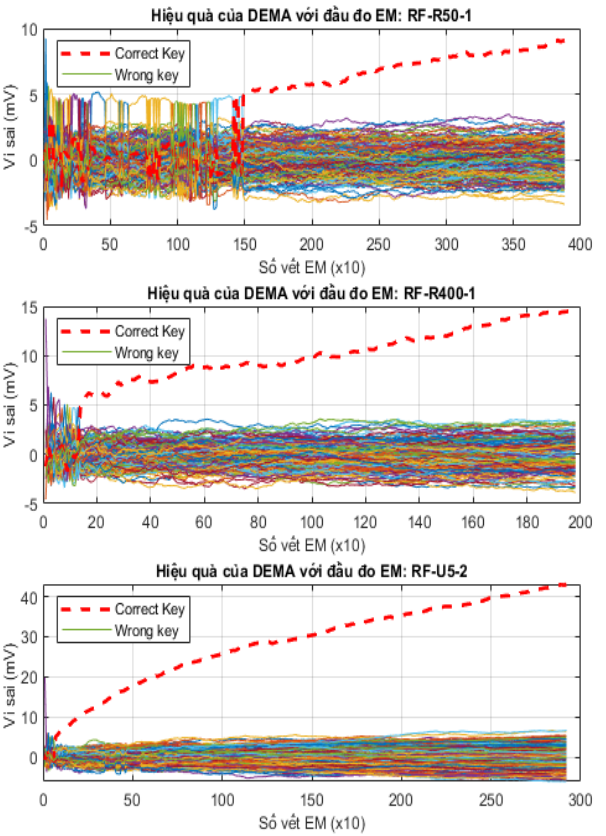
*A. Kết quả thực nghiệm tấn công DEMA*

Trong thử nghiệm tấn công DEMA, điểm tấn công được lựa chọn là đầu ra của S-hộp của AES, số vết EM sử dụng là 2.000, mỗi vết chứa 35.000 mẫu thời gian.

Kết quả tấn công đối với byte khóa đầu tiên được hiển thị trong Hình 4 cho các kịch bản sử dụng các đầu dò EM khác nhau. Từ vết vi sai của tất cả các khóa giả thiết của byte khóa đầu tiên, chỉ byte khóa có giá trị 22 xuất hiện gai và có thể phân biệt được với vết vi sai của các khóa giả giả thiết khác. Điều này chứng tỏ tấn công DEMA có thể khôi phục byte khóa đầu tiên của AES-128 khi sử dụng 2.000 dấu vết EM với cả ba đầu dò EM. Như vậy, dấu vết EM thu thập được chứa thông tin rò rỉ về khóa của thẻ thông minh và có thể bị khai thác bằng phương pháp tấn công DEMA.




Hình 4. Kết quả tấn công DEMA




Hình 5. Hiệu quả tấn công DEMA

Để đánh giá hiệu quả tấn công, chúng tôi thực hiện tấn công DEMA với số vết EM sử dụng tăng

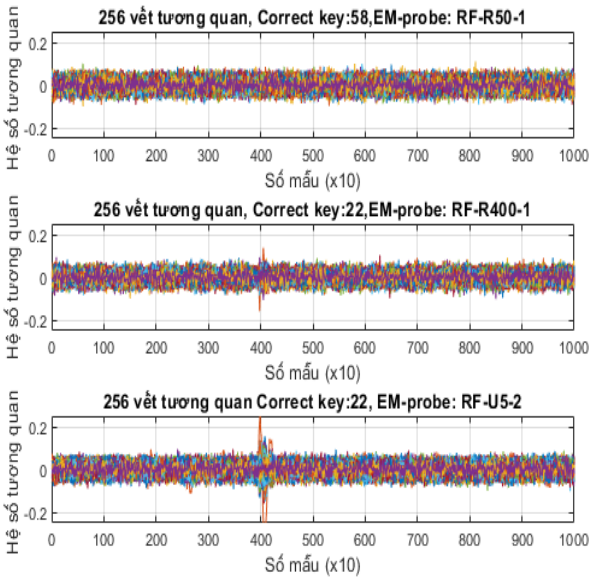
dần, kết quả giá trị vi sai của tất cả các khóa giả thiết được mô tả trên Hình 5. Từ hình vẽ này có thể thấy rằng, khi số vết EM tăng, giá trị vi sai của khóa đúng tăng dần và khi số vết tăng đến giá trị $N_a$ như mô tả ở Bảng 1 thì có thể phân biệt được khóa đúng và khóa sai, hay nói cách khác khi đó người tấn công có thể tìm ra khóa đúng của thẻ thông minh. Với giá trị $N_a$ mô tả trên Bảng 1, có thể kết luận rằng đầu dò RF-R 400-1 và RF-U5-2 có thể phù hợp với DEMA hơn RF-R 50-1.

### B. *Kết quả tấn công CEMA*

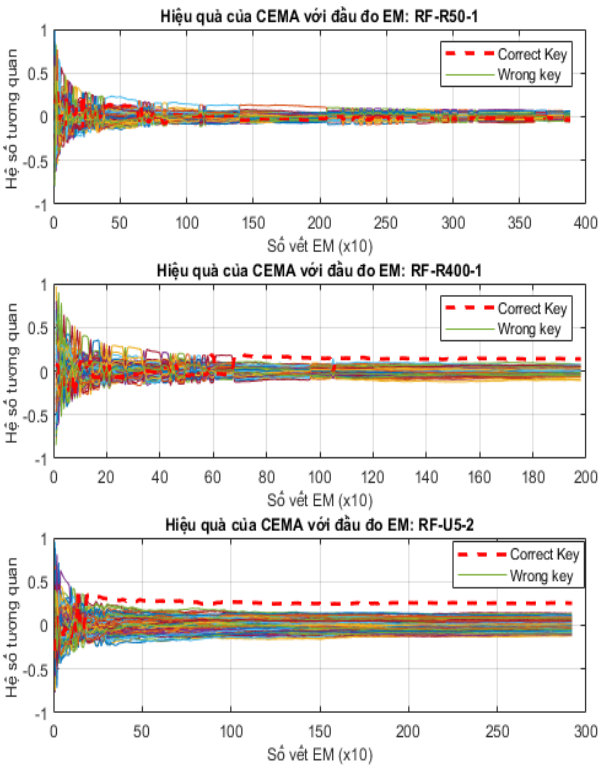
Đối với CEMA, các kịch bản tấn công được tiến hành giống như DEMA. Kết quả tấn công đối với byte khóa đầu tiên được hiển thị trong Hình 6 cho các kịch bản sử dụng các bộ vết EM khác nhau. Khi sử dụng đầu dò RF-R 50-1, khóa tìm thấy là 58, khác với khóa thực tế được sử dụng bởi thẻ thông minh, điều này chứng tỏ rằng trong trường hợp này, tấn công CEMA không thể tìm thấy khóa đúng. Mặt khác, chúng ta cũng thấy vết tương quan của tất cả các khóa giả thiết khá giống nhau và không xuất hiện các gai đủ lớn, không thể phân biệt được với nhau. Khi sử dụng đầu đo RF-R 400-1 và RF-U5-2, vết tương quan của khóa đúng 22 xuất hiện gai và có thể phân biệt được với vết tương quan của các khóa khác. Tuy nhiên, gai xuất hiện khi sử dụng RF-U5-2 lớn hơn, có thể phân biệt rõ ràng với các khóa khác. Điều này chứng tỏ tấn công CEMA có thể khôi phục được byte khóa đầu tiên của AES-128 khi sử dụng 2.000 dấu vết EM với 02 đầu dò EM là RF-R 400-1 và RF-U5-2. Do đó, vết EM được thu thập từ thẻ thông minh chứa thông tin rò rỉ về khóa của thẻ thông minh và có thể bị khai thác bằng phương pháp CEMA. Tuy nhiên, hiệu quả của tấn công phụ thuộc vào đầu đo EM được sử dụng.

BẢNG 1. HIỆU QUẢ CỦA TẤN CÔNG EMA

| Phương pháp | Đầu đo EM | | |
|---|---|---|---|
| | RF-R 50-1 | RF-R 400-1 | RF-U5-2 |
| DEMA | 1530 | 160 | 100 |
| CEMA | NA | 690 | 360 |




Hình 6. Kết quả tấn công CEMA




Hình 7. Hiệu quả của tấn công CEMA

Về hiệu quả tấn công, Hình 7 mô tả hệ số tương quan của tất cả các khóa giả thiết khi số lượng vết EM sử dụng cho tấn công tăng dần. Khi số lượng vết EM tăng đến giá trị $N_a$ như mô tả ở Bảng 1, có thể phân biệt được hệ số tương quan giữa khóa đúng và khóa sai. Vì vậy, tương tự như tấn công DEMA, sử dụng đầu rò RF-U5-2 yêu

cầu số lượng vết EM ít nhất là 360 và RF-R400-1 yêu cầu số lượng tối đa 690 vết EM để khôi phục khóa đúng thành công. Với đầu dò RF-50-1, không thể tìm thấy khóa đúng với số lượng vết EM sử dụng là 3.900. Hệ số tương quan của khóa đúng ẩn dưới nền của các khóa khác và không có xu hướng tăng theo số lượng vết EM, do đó có thể dự đoán rằng phương pháp CEMA sẽ không tìm thấy khóa chính xác khi sử dụng đầu đo RF-R50-1.

### *C. Thảo luận*

Từ kết quả thử nghiệm của các tấn công DEMA và CEMA được mô tả ở trên, có thể thấy rằng tấn công EMA của thẻ thông minh là có thể thực hiện được. Có sự rò rỉ giá trị bí mật của thuật toán mật mã khi nó được thực thi trên thẻ thông minh thông qua bức xạ điện từ. Với vết EM được thu thập từ thẻ thông minh sử dụng các đầu đo EM khác nhau, hiệu quả của tấn công DEMA tốt hơn CEMA vì nó yêu cầu số vết EM ít hơn để khôi phục thành công khóa đúng. Điều này có thể giải thích như sau, khi sử dụng CEMA, người tấn công sử dụng mô hình EM để tính toán các giá trị EM giả định tại thời điểm tấn công và mô hình này chỉ gần đúng với thực tế, trong khi ở DEMA, người tấn công chia dấu vết EM theo giá trị bit đầu ra của điểm tấn công là 1 hoặc 0. Thực nghiệm cho thấy hiệu quả của DEMA tốt hơn CEMA nên mô hình rò rỉ dựa trên bit đơn để mô tả vết EM mạnh hơn so với việc sử dụng mô hình HW để mô tả giá trị EM giả định. Nói cách khác, mô hình ước lượng EM theo HW có thể sử dụng nhưng vẫn cần nghiên cứu và xây dựng mô hình tốt hơn cho cuộc tấn công CEMA. Hơn nữa, từ kết quả thực nghiệm trên cho thấy hệ thống đo EM, đặc biệt là đầu đo EM có ảnh hưởng rất lớn đến hiệu quả tấn công. Loại đầu đo nên được sử dụng là đầu dò trường gần và được đặt trên bề mặt thẻ thông minh tại vị trí có chíp điều khiển.

## V. KẾT LUẬN

Trong bài báo này, nhóm tác giả đã nghiên cứu các phương pháp tấn công EMA và đưa ra quy trình thực tế để thực hiện tấn công phân tích bức xạ điện từ vi sai và tấn công phấn tích bức xạ điện tường tương quan. Nhóm cũng đã tiến hành thử nghiệm DEMA và CEMA để tìm ra khóa đúng của thẻ thông minh có cài đặt thực thi AES-128 dựa trên các bức xạ EM. Bức xạ EM có thể xem là nguồn tín hiệu kênh kề và có sự rò rỉ thông tin nhạy cảm của thẻ thông minh thông qua bức xạ EM nên các cuộc tấn công EMA có thể được sử dụng để tìm ra khóa của thiết bị. Bằng kết quả thực nghiệm, có thể khẳng định rằng tấn công DEMA hiệu quả hơn tấn công CEMA và hệ thống đo bức xạ EM, đặc biệt là đầu đo EM có ảnh hưởng lớn đến hiệu quả tấn công EMA. Nghiên cứu của nhóm đã chứng minh khả năng thực hiện các tấn công EMA đối với thẻ thông minh. Tuy nhiên, chủ đề này cần được nghiên cứu sâu hơn, rộng hơn. Các vấn đề sau có thể cần được quan tâm làm rõ đó là xây dựng cơ sở lý thuyết đánh giá sự rò rỉ thông tin từ bức xạ điện từ, khảo sát các tấn công EMA trên các nền tảng khác nhau, sử dụng các đầu đo EM khác nhau, thiết kế các đầu dò EM phù hợp với từng thiết bị cần đo và cuối cùng là nghiên cứu xây dựng các giải pháp phòng chống tấn công EMA nhằm đảm bảo an toàn cho thiết bị.

## LỜI CẢM ƠN

Nhóm tác giả xin chân thành cảm ơn Học viện Kỹ thuật Mật mã đã hỗ trợ kinh phí và trang thiết bị thí nghiệm để thực hiện công trình nghiên cứu này.

## TÀI LIỆU THAM KHẢO

[1]. P. Kocher, "Cryptanalysis of Diffie-Hellman, RSA, DSS, and other cryptosystems using timing attacks," in *International Advances in Cryptology Conference* , 1995.

[2]. P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *19th International Advances in Cryptology Conference*, 1999.

[3]. J-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," *E-smart*, pp. 200-210, 2001.

[4]. D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi, "The EM side-channel(s)," in *Cryptographic Hardware and Embedded Systems - CHES2002*, 2002.

[5]. K. Gandolfi, C. Mourtel, and F. Olivier,

"Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems*, 2001.

[6]. D. P. Montminy, R. O. Baldwin, M. A. Temple, and M. E. Oxley, "Differential electromagnetic attacks on a 32-bit microprocessor using software defined radio," *Information Forensics and Security*, vol. 8, no. 12, pp. 2101-2114, 2013.

[7]. J. Longo, E. D. Mulder, D. Page, and M. Tunstall, "Soc it to EM: electromagnetic side-channel attacks on a complex system-on-chip," *Cryptology ePrint Archive*, 2015.

[8]. C. H. Gebotys, S. Ho, and C. C. Tiu, "EM analysis of rijndael and ECC on a wireless java-based PDA," in *Cryptographic Hardware and Embedded Systems*, 2005.

[9]. Sung-Mo Kang,Yusuf Leblebic, CMOS Digital Integrated Circuits:Analysis and Design, *McGraw-Hill Science*, 2002.

[10]. Stephane Bronckers, Geert Van der Plas, and Yves Rolain, Substrate noise coupling in analog/RF circuits, *Artech House*, 2010.

[11]. Brier, E., Clavier, C., Olivier, F, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems*, 2014.

[12]. Peeters, E., Standaert, F.-X., Quisquater, J.-J, "Power and electromagnetic analysis: improved model, consequences and comparisons," Integration VLSI, vol. 40, pp. 52-60, 2007.

[13]. S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, Berlin: Springer-Verlag, 2007.

[14]. E. D. Mulder, Electromagnetic techniques and probes for side-channel analysis on cryptographic devices, PhD Thesis, 2010.

[15]. Kocher, P., Jaffe, J., Jun, B. et al. *Introduction to differential power analysis*. J Cryptogr Eng 1, 5–27 (2011).

[16]. Owen Lo, William J. Buchanan & Douglas Carson, Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA), Journal of Cyber Security Technology, 88-107, 2017.

[17]. Quy, T. N., Tung, N. T., Trung, D. Q., & Viet, D. H. (2022). Convolutional neural network based sidechannel attacks. *Journal of Science and Technology on Information Security*, *1*(15), 26-37. https://doi.org/10.54654/isj.v1i15.834.

[18]. Hảo, N. N. V., & Chính, B. Đức. (2020). Phương pháp phát nhiễu đồng bộ chống thu bức xạ kênh kề phát ra từ màn hình máy tính dựa trên công nghệ FPGA. *Journal of Science and Technology on Information Security*, *7*(1), 44-50.

[19]. Bui, C. D., Ngo, M. T., Nguyen, H. N. V., & Pham, T. M. (2020). Information leakage through electromagnetic radiation of PS/2 Keyboard. *Journal of Science and Technology on Information Security*, *10*(2), 51-60. https://doi.org/10.54654/isj.v10i2.67.

## SƠ LƯỢC VỀ TÁC GIẢ

**Trần Ngọc Quý**

Đơn vị công tác: Học viện Kỹ thuật Mật mã

Email: quytn@actvn.edu.vn

Quá trình đào tạo: Tốt nghiệp Đại học năm 2003 và Thạc sĩ chuyên ngành Điện tử Viễn thông năm 2006 tại Đại học Công nghệ, Đại học Quốc gia Hà Nội, Tiến sĩ Kỹ thuật Mật mã tại Học Viện Kỹ thuật Mật mã năm 2022.

Hướng nghiên cứu: An toàn phần cứng, Tấn công kênh kề, Chống tấn công kênh kề, Hệ thống IoT.

**Phùng Văn Quyền**

Đơn vị công tác: Học viện Kỹ thuật Mật mã

Email: quyenpv@actvn.edu.vn

Quá trình đào tạo: Tốt nghiệp Thạc sĩ chuyên ngành Tự động hóa tại Học viện Kỹ thuật Quân sự năm 2008.

Hướng nghiên cứu: An toàn IoT, hệ thống điều khiển tự động.