# Phân tích 64 lược đồ hàm nén trong mô hình hàm băm dựa trên mã khối

**Nguyễn Văn Long, Hoàng Đình Linh**

***Tóm tắt*— Cấu trúc cho các hàm băm lặp dựa trên mã khối đã được nghiên cứu, trong đó kích thước giá trị băm bằng kích cỡ khối và kích cỡ khóa đã được quan tâm nghiên cứu rộng rãi. Bài báo này, chúng tôi chi tiết 64 lược đồ theo mô hình tổng quát được đề xuất bởi B. Preneel và các đồng sự, dựa trên 5 tấn công cơ bản. Chi tiết hóa phân loại lược đồ theo số lượng các biến đầu vào và thực hiện đánh giá độ an toàn của một trong số các lược đồ an toàn theo quan điểm thám mã vi sai.**

***Abstract*— Constructions for hash functions based on a block cipher have been studied where the size of the hashcode is equal to the block length of the block cipher and where the key size is approximately equal to the block length. In this paper, we have analyzed in more detail 64 general model schemes which has been represented by B. Preneel et al. using five basic attacks. An classification of these schemes also have been done in more detail by considering linear transformations of the inputs. More over, we have investigated the security for one of the secure schemes under the differential cryptanalysis, others are similar.**

***Từ khóa— hàm băm; hàm nén; mã khối.***

## I. GIỚI THIỆU

Các hàm băm mật mã là một ánh xạ thực hiện biến đổi một đầu vào có độ dài bất kỳ thành một xâu có kích thước cố định và phải đảm bảo các yêu cầu về mật mã. Hàm băm được ứng dụng nhiều trong lĩnh vực an toàn thông tin như chữ ký số, xác thực thông báo, tạo chuỗi giả ngẫu nhiên…. Tùy vào mục đích sử dụng mà hàm băm được thiết kế có thể có hoặc không có khóa. Tuy nhiên một hàm băm mật mã $H:V^* \to V_n$ an toàn phải đảm bảo 3 tính chất bắt buộc, đó là:

*Tính một chiều:* Theo đó độ phức tạp để tìm tiền ảnh $M \in V^*$ đối với giá trị băm *h* cho trước là $2^n$.

*Tính kháng va chạm:* Có nghĩa là độ phức tạp để tìm hai thông điệp khác nhau $M, M' \in V^*$, sao cho $H(M) = H(M')$ là $2^{n/2}$.

*Tính kháng tiền ảnh thứ 2:* Tức là với thông điệp $M \in V^*$ cho trước, độ phức tạp tìm thông điệp $M' \in V^*$ thỏa mãn $H(M) = H(M')$ là $2^n$.

Trong [1, 2], Merkle và Damgard nghiên cứu một cách độc lập và đưa ra một cấu trúc lặp (được gọi là cấu trúc Merkle-Damgard) cho phép xây dựng hàm băm lặp an toàn kháng va chạm dựa trên một hàm nén kháng va chạm [13, 14]. Trong thiết kế các hàm băm lặp theo cấu trúc này, hạt nhân quan trọng chính là hàm nén. Có nhiều nguyên lý thiết kế hàm nén như xây dựng dựa trên mã khối, mã dòng, đại số modular, lý thuyết chaotic [3]… Tuy nhiên, hàm nén trên cơ sở mã khối được sử dụng nhiều trong các thiết kế hàm băm mật mã, bởi tính an toàn có thể chứng minh của mã khối có thể áp dụng trong chứng minh an toàn của hàm băm, cũng như lợi thế của mã khối có thể sử dụng trong việc thực thi tại nhiều môi trường khác nhau.

Trong bài báo này, chúng tôi phân tích chi tiết các lược đồ đã được trình bày trong nghiên cứu của Preneel và cộng sự [4]. Sau đó tiến hành phân loại các lược đồ này, thực hiện phân tích các lược đồ an toàn theo quan điểm thám mã vi sai mà trong đó nhóm tác giả chỉ nêu ra chứ chưa được trình bày một cách chi tiết.

Bố cục những mục tiếp theo của bài báo được trình bày như sau: Mục II trình bày về mô hình tổng quát cơ sở thiết kế hàm nén dựa trên mã khối. Mục III trình bày các tấn công cơ bản và phân tích 64 lược đồ theo những tấn công cơ bản này và trình bày nguyên tắc phân loại các lược đồ theo số lượng các biến đầu vào của hàm nén. Theo quan điểm thám mã vi sai, 12 lược đồ an toàn nhận được sau khi phân loại sẽ được trình bày trong mục IV của bài báo. Cuối cùng là Mục Kết luận.

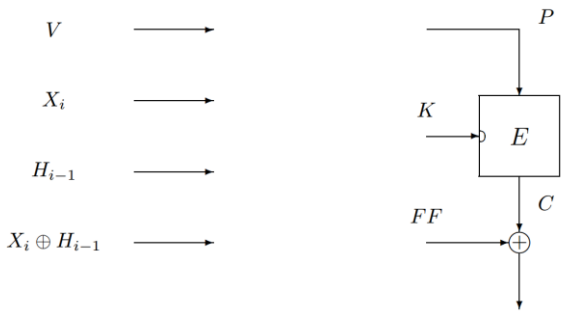
## II. MÔ HÌNH TỔNG QUÁT THIẾT KẾ HÀM NÉN DỰA TRÊN MÃ KHỐI

Trong mục này chúng tôi trình bày ý tưởng của mô hình thiết kế tổng quát của hàm nén dựa trên mã khối. Theo đó, mã khối với khóa bí mật *K* tác động lên khối bản rõ *X* được ký hiệu là $E(K, X)$, trong đó $K, X \in V_n$. Phép giải mã tương ứng khi giải mã bản mã *C* được ký hiệu là $D(K, C)$. Trong mô hình đang xét, nếu không có giải thích bổ sung, sẽ coi như các mã khối là không có điểm yếu. Đầu vào của hàm băm lặp $H:V^* \to V_n$ được chia thành *t* khối từ $X_1$ đến $X_t$.

Hàm băm lặp có thể được mô tả như sau:

$$H_i = f\left(X_i, H_{i-1}\right), i = 1,2,...,t \qquad (1)$$

Ở đây $f$ là hàm nén, $H_0$ chính là véc tơ khởi tạo *IV*, tùy thuộc vào mỗi lược đồ có *IV* khác nhau, và $H_t$ là giá trị băm.




Hình 1. Mô hình tổng quát thiết kế hàm nén dựa trên mã khối

Trong mô hình thiết kế tổng quát của hàm nén dựa trên mã khối *E*, chúng tôi đưa ra mã khối có hai đầu vào là khóa *K* và bản rõ *P* và một đầu ra *C* (như Hình 1). Ta có thể chọn đầu vào là một trong bốn giá trị: $X_i, H_{i-1}, X_i \oplus H_{i-1}$ và hằng số *V*. Ta cũng có thể điều chỉnh bằng một phép FF (feedforward) lên đầu ra *C* bởi phép cộng XOR giá trị *C* với một trong bốn giá trị ở trên. Các tham số như vậy sẽ tạo ra tổng cộng $4^3 = 64$ lược đồ khác nhau. Trong các phần sau, để không làm mất tính tổng quát ta sẽ giả thiết rằng $V = 0$.

## III. PHÂN TÍCH 64 LƯỢC ĐỒ THEO CÁC TẤN CÔNG CƠ BẢN

Để thực hiện phân tích 64 lược đồ nhận được từ mô hình tổng quát, đầu tiên chúng ta xem xét năm tấn công cơ bản. Tư tưởng chính của phần này chúng tôi dựa trên tài liệu [4].

### *A. Các tấn công cơ bản*

*Tấn công trực tiếp (Direct attack) (ký hiệu là D):* Cho trước $H_{i-1}$ và $H_i$, nếu dễ dàng tìm được $X_i$ thỏa mãn (1) khi đó ta nói lược đồ bị tấn công trực tiếp.

*Tấn công hoán vị (Permutation attack) (ký hiệu là P):* Nếu $H_i$ có thể được biểu diễn dưới dạng $H_i = H_{i-1} \oplus f'\left(X_i\right)$, với $f'$ là hàm một chiều, thì lược đồ bị tấn công hoán vị. Khi đó giá trị $X_i$ không thể khôi phục từ $H_{i-1}$ và $H_i$, nhưng giá trị băm lại độc lập với thứ tự các khối thông báo. Thật vậy, gọi *H* là giá trị băm, ta có:

$$H = H_0 \oplus \bigoplus_{i=1}^{t} f' \ X_i$$

Khi đó nếu ta thay đổi thứ tự các khối thông báo thì giá trị băm không thay đổi. Như vậy việc tìm va chạm và nghịch ảnh thứ 2 là dễ dàng. Đây là một tấn công tầm thường, vì $H_i$ chỉ phụ thuộc tuyến tính vào $H_{i-1}$.

*Tấn công thuận (Forward attack) (ký hiệu là F):* Cho trước $H_{i-1}, H'_{i-1}$ và $X_i$ (chú ý là $H_i$ cố định), nếu dễ dàng tìm được $X'_i$ sao cho $f\left(X'_i, H'_{i-1}\right) = f\left(X_i, H_{i-1}\right) = H_i$, khi đó ta nói lược đồ bị tấn công thuận.

*Tấn công ngược (Backward attack) (ký hiệu là B):* Cho trước $H_i$, nếu dễ dàng tìm được cặp $\left(X_i, H_{i-1}\right)$ sao cho $f\left(X_i, H_{i-1}\right) = H_i$, thì khi đó ta nói lược đồ bị tấn công ngược.

*Tấn công điểm bất động (Fixed point attack) (ký hiệu FP):* Nếu dễ dàng tìm được $H_{i-1}$ và $X_i$ sao cho $f\left(X_i, H_{i-1}\right) = H_{i-1}$, thì ta nói lược đồ bị tấn công điểm bất động.

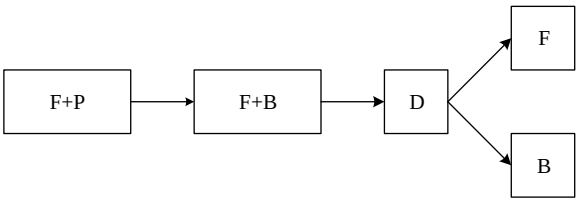
Quan hệ của các tấn công này cũng rất quan trọng: nếu lược đồ nào có thể bị tấn công D thì cũng có thể bị tấn công B và F, nhưng ngược lại thì không đúng. Thật vậy, giả sử lược đồ bị tấn công D, tức là cho trước $H_{i-1}$ và $H_i$, khi đó theo định nghĩa tấn công D, ta dễ dàng tìm được $X_i$ thỏa mãn $f\left(X_i, H_{i-1}\right) = H_i$. Trong trường hợp này nếu cho trước $H_i$, ta chọn một giá trị $H_{i-1}$ và áp dụng tấn công D để thu được $X_i$. Vậy ta dễ dàng tìm được một cặp $\left(X_i, H_{i-1}\right)$ sao cho $f\left(X_i, H_{i-1}\right) = H_i$, hay nói cách khác lược đồ bị tấn công B. Tương tự, nếu cho trước $H_{i-1}, H'_{i-1}$ và $X_i$ khi đó ta có thể tính được $H_i$. Bây giờ áp dụng tấn công D khi đã biết trước $H'_{i-1}$ và $H_i$, khi đó ta dễ dàng tính được $X'_i$. Vậy lược đồ bị tấn công F.

Trong trường hợp lược đồ bị tấn công P, thì người ta cũng có thể áp dụng tấn công B bằng việc chọn khối $X_i$ trước và sau đó tính $H_{i-1}$.

Và nếu có thể thực hiện cả tấn công B và F hoặc cả F và P được thì tấn công D cũng có thể xảy ra. Thật vậy, giả sử không thể thực hiện tấn công D. Trong trường hợp này, vì có thể thực hiện tấn công F dẫn đến giá trị ba đầu vào đều là hằng số hoặc bằng $X_i \oplus H_{i-1}$. Mặt khác, nếu ta có thể

thực hiện tấn công B hoặc P, thì ta có thể tìm được một cặp $(X_i, H_{i-1})$ thỏa mãn $f(X_i, H_{i-1}) = H_i$. Thực tế, trong trường hợp này ta có thể xác định được $X_i \oplus H_{i-1}$, sau đó với $H_{i-1}$ cho trước, ta tính được $X_i$ tương ứng, trái với giả thiết ban đầu là không thực hiện được tấn công D.

Phân tích về quan hệ giữa các tấn công này được tác giả trình bày trong luận văn năm 2003 [12], ở đây đưa ra những lập luận chi tiết hơn bằng các công thức cụ thể. Hình 2 dưới đây minh họa quan hệ thứ tự của các tấn công trên:




Hình 2. Quan hệ thứ tự của các tấn công

*B. Đánh giá 64 lược đồ*

BẢNG 1. CÁC TẤN CÔNG LÊN 64 LƯỢC ĐỒ
(CÁC LƯỢC ĐỒ ĐƯỢC ĐÁNH SỐ THEO CHỈ SỐ TRÊN)

| **FF** | **K** | **P** | | | |
|---|---|---|---|---|---|
| | | $X_i$ | $H_{i-1}$ | $X_i \oplus H_{i-1}$ | $V$ |
| $V$ | $X_i$ | -[1] | B[17] | B[33] | -[49] |
| | $H_{i-1}$ | D[2] | -[18] | D[34] | -[50] |
| | $X_i \oplus H_{i-1}$ | B[3] | B[19] | F[35] | F[51] |
| | $V$ | -[4] | -[20] | D[36] | -[52] |
| $X_i$ | $X_i$ | -[5] | B[21] | B[37] | -[53] |
| | $H_{i-1}$ | √[6] | D[22] | √[38] | D[54] |
| | $X_i \oplus H_{i-1}$ | FP[7] | FP[23] | B[39] | B[55] |
| | $V$ | -[8] | D[24] | B[40] | -[56] |
| $H_{i-1}$ | $X_i$ | P[9] | FP[25] | FP[41] | P[57] |
| | $H_{i-1}$ | B[10] | -[26] | D[42] | -[58] |
| | $X_i \oplus H_{i-1}$ | FP[11] | FP[27] | B[43] | B[59] |
| | $V$ | D[12] | -[28] | D[44] | -[60] |
| $X_i \oplus H_{i-1}$ | $X_i$ | P[13] | FP[29] | FP[45] | P[61] |
| | $H_{i-1}$ | √[14] | D[30] | √[46] | D[62] |
| | $X_i \oplus H_{i-1}$ | B[15] | B[31] | F[47] | F[63] |
| | $V$ | P[16] | D[32] | F[48] | D[64] |

Trên cơ sở mô hình tổng quát, chúng ta xác định được 64 lược đồ được đánh số thứ tự bởi chỉ số trên như trong Bảng 1. Trong Bảng này các tấn công được biểu thị bằng chữ cái đầu, còn ký hiệu "-" có nghĩa là hàm nén $f$ là yếu, là trường hợp tầm thường. Nếu hàm nén không bị tấn công nào trong 5 tấn công, thì được ký hiệu bởi "√".

Từ bảng thống kê theo [4] ta có Mệnh đề 1. Kết quả của Mệnh đề 1 có thể coi là một cách phân loại lược đồ theo từng dạng tấn công. Ngoài ra trong [4] nhóm tác giả chỉ đưa ra kết quả tổng hợp theo các tấn công, nhưng không phân tích chi tiết. Phần chứng minh Mệnh đề dưới đây chính là phân tích chi tiết bằng công thức cụ thể mà được đưa vào để giải thích rõ hơn về độ an toàn của mỗi lược đồ trước các tấn công cơ bản.

Trên cơ sở thống kê từ Bảng 1, chúng ta sẽ nhận được 7 lớp các lược đồ như sau:

**Mệnh đề 1.** *Trong số 64 lược đồ theo mô hình tổng quát của Preneel, chúng ta chia thành các lớp như sau*:

*Lớp a: Có* 15 *lược đồ là hiển nhiên yếu, đó là các lược đồ:* 1, 4, 5, 8, 18, 20, 26, 28, 49, 50, 52, 53, 56, 58, 60.

*Lớp b: Có* 13 *lược đồ bị tấn công D, đó là các lược đồ:* 2, 12, 22, 24, 30, 32, 34, 36, 42, 44, 54, 62, 64.

*Lớp c: Có* 5 *lược đồ bị tấn công P, đó là các lược đồ:* 9, 13, 16, 57, 61.

*Lớp d: Có* 5 *lược đồ bị tấn công F, đó là các lược đồ*: 35, 47, 48, 51, 63.

*Lớp e: Có* 14 *lược đồ bị tấn công B, đó là các lược đồ:* 3, 10, 15, 17, 19, 21, 31, 33, 37, 39, 40, 43, 55, 59.

*Lớp f: Có* 8 *lược đồ bị tấn công FP, đó là các lược đồ:* 7, 11, 23, 25, 27, 29, 41, 45.

*Lớp g: Có* 4 *lược đồ không bị tấn công nào, đó là các lược đồ*: 6, 14, 38, 46.

*Chứng minh.* Trong chứng minh này, chúng tôi xem xét phân tích chi tiết một số lược đồ đại diện cho mỗi tấn công, là các lược đồ được đề xuất và sử dụng trong các chế độ hoặc trong các thiết kế mà đã được trình bày trong các tài liệu. Các lược đồ khác có thể được phân tích theo cách tiếp cận tương tự.

*Trong Lớp a, chọn lược đồ đại diện là Lược đồ 1*

**Lược đồ 1.** $P = X_i, K = X_i, FF = V = 0$, khi đó $H_i = E(X_i, X_i)$, giá trị xích thứ $i$ không phụ thuộc vào giá trị xích thứ $i-1$. Do đó, giá trị băm chỉ phụ thuộc vào khối bản rõ thứ t. Dễ dàng thực hiện được các tấn công tìm va chạm, tìm tiền ảnh và tiền ảnh thứ 2. Kết luận, lược đồ 1 là hiển nhiên yếu.

*Trong Lớp b, chọn lược đồ đại diện là Lược đồ 24*

**Lược đồ 24. (CFB).** Với việc lựa chọn các tham số $P = H_{i-1}, K = V = 0, FF = X_i$, khi đó biểu thức của hàm nén có dạng

$$H_i = E(0, H_{i-1}) \oplus X_i .$$

Dễ thấy rằng biểu thức này tương ứng với chế độ CFB trong mã khối. Với lược đồ này dễ thấy rằng có thể thực hiện tấn công D. Thật vậy, với $H_i, H_{i-1}$ ta tính được $X_i = H_i \oplus E(0, H_{i-1})$.

*Trong Lớp c, chọn lược đồ đại diện là Lược đồ 9*

**Lược đồ 9.** $P = X_i, K = X_i, FF = H_{i-1}$, khi đó $H_i = E(X_i, X_i) \oplus H_{i-1}$. Dễ thấy

$$H_i = H_{i-1} \oplus f'(X_i)$$

do vậy có thể thực hiện tấn công P.

*Trong Lớp d, chọn lược đồ đại diện là Lược đồ 35*

**Lược đồ 35.** Với các tham số $P = X_i \oplus H_{i-1}$, $K = X_i \oplus H_{i-1}, FF = V = 0$, khi đó biểu thức hàm nén là: $H_i = E(X_i \oplus H_{i-1}, X_i \oplus H_{i-1})$. Dễ thấy có thể thực hiện tấn công F.

Với $X_i, H_{i-1}, H'_{i-1}$ ta tính được

$$X'_i = X_i \oplus H_{i-1} \oplus H'_{i-1},$$

khi đó

$$f(X'_i, H'_{i-1}) = E(X'_i \oplus H'_{i-1}, X'_i \oplus H'_{i-1}) = E(X_i \oplus H_{i-1}, X_i \oplus H_{i-1}) = H_i .$$

*Trong Lớp e, chọn lược đồ đại diện là Lược đồ 17*

**Lược đồ 17. (Rabin).** Đây là lược đồ được đề xuất bởi Rabin (năm 1978) [11]. Tuy nhiên Merkle đã chỉ ra một tấn công B là có thể áp dụng lên lược đồ này và từ đây có thể xây dựng một tấn công tìm tiền ảnh. Bây giờ chúng sẽ xem xét tấn công B lên lược đồ 17. Với các tham số $P = H_{i-1}, K = X_i, FF = V = 0$, khi đó biểu thức của hàm nén có dạng $H_i = E(X_i, H_{i-1})$ và lược đồ dễ bị tấn công bởi tấn công B. Thật vậy, cho trước $H_i$ ta thực hiện giải mã $H_i$ với khóa *K* bất kỳ để thu được $H_{i-1}$. Ta có:

$$X_i = K, H_{i-1} = D(K, H_i) .$$

*Trong Lớp f, chọn lược đồ đại diện là Lược đồ 25*

**Lược đồ 25. (Davies-Mayer).** Đây là lược đồ được đề xuất trong [5]. Lược đồ này bị tấn công FP. Thật vậy, với các tham số $P = H_{i-1}$, $K = X_i, FF = H_{i-1}$. Khi đó, biểu thức của hàm nén sẽ có dạng $H_i = E(X_i, H_{i-1}) \oplus H_{i-1}$. Với khóa *K* bất kỳ, ta chọn $X_i = K$, khi đó vì $H_{i-1} = H_i = D(K, 0)$. Khi đó, $f(X_i, H_{i-1}) = E(K, D(K, 0)) \oplus D(K, 0) = D(K, 0) = H_{i-1}$.

Cần phải nói thêm rằng, lược đồ Davies-Meyer được sử dụng trong thiết kế nhiều hàm băm hiện đại như SHAvite-3 [18], họ hàm băm SHA [13], MD5 [12]… mặc dù nó bị tấn công FP. Lý do lược đồ này vẫn được sử dụng nhiều là bởi tấn công FP có thể bị kháng lại khi sử dụng một vài tham số mở rộng, ví dụ như giá trị #bits là số bit được băm cho đến thời điểm hiện tại trong khung HAIFA [14].

*Trong Lớp g, chọn lược đồ đại diện là Lược đồ 14*

**Lược đồ 14. (Miyaguchi-Preneel).** Lược đồ Miyaguchi-Preneel được xây dựng trong thiết kế hàm băm N-hash [10]. Đây cũng là lược đồ được sử dụng trong thiết kế hàm nén của nhiều hàm băm hiện đại như Whirepool [11], GOST R 34.11-2012 [15]… Với những tham số $P = X_i$, $K = H_{i-1}, FF = X_i \oplus H_{i-1}$, hàm nén có dạng $H_i = E(H_{i-1}, X_i) \oplus X_i \oplus H_{i-1}$ có khả năng kháng lại toàn bộ 5 tấn công trên. Để làm sáng tỏ điều này, một lập luận tương tự được sử dụng như khi phân tích lược đồ Matyas-Meyer-Oseas. Thật vậy, giả sử phản chứng có thể thực hiện tấn công FP. Khi đó, ta có thể tìm được $H_{i-1}$ và $X_i$ thỏa mãn $E(H_{i-1}, X_i) = X_i$. Do đó, ta thấy rằng phép mã hóa không phụ thuộc vào khóa và bản mã thu được bằng chính bản rõ. Suy ra mã khối sử dụng là yếu, trái với giả thiết.

Giả sử phản chứng, có thể thực hiện tấn công F. Tức là khi cho trước $X_i, H_{i-1}, H'_{i-1}$ ta dễ dàng tính được $X'_i$ thỏa mãn

$$f(X_i, H_{i-1}) = f(X'_i, H'_{i-1}) .$$

Hay

$$H_i = E(H'_{i-1}, X'_i) \oplus X'_i \oplus H'_{i-1} .$$

Khi đó $E(H'_{i-1}, X'_i) = H_i \oplus H'_{i-1} \oplus X'_i$. Tuy nhiên, ta việc giải phương trình trên là "khó" khi mã khối là không có điểm yếu, nên không thể thực hiện tấn công F. Kéo theo, ta không thể thực hiện tấn công D và đồng thời cũng không thể thực hiện được tấn công B. Thật vậy, giả sử phản chứng ta có thể thực hiện tấn công B. Khi đó, với $H_i$ cho trước, ta có thể dễ dàng tính được cặp $(X_i, H_{i-1})$ thỏa mãn:

$$E(H_{i-1}, X_i) \oplus X_i \oplus H_{i-1} = H_i .$$

Theo giả thiết, mã khối sử dụng là không có điểm yếu, khi đó việc xác định cặp $(X_i, H_{i-1})$ thỏa mãn điều kiện trên là không dễ dàng. Vậy không áp dụng được tấn công B. Kéo theo cũng không áp dụng được tấn công P .□

***Chú ý*:** Phần này nhằm nói về một số lược đồ thuộc các lớp khác nhau mà có ứng dụng trong các thiết kế thực tế.

Ngoài lược đồ 17, trong Lớp e còn có lược đồ 19 do Bitzer đề xuất được xem xét trong tài liệu số [15] với mục đích thiết kế xây dựng thuật toán chữ ký số. Tuy nhiên trong [7] Winternitz đã chỉ ra lược đồ này cũng chịu tấn công B.

Ngoài lược đồ 14, trong Lớp g còn có lược đồ số 6 do nhóm tác giả S. Matyas, C. Meyer, J. Oseas đề xuất năm 1985 trong [6] với mục đích xây dựng hàm một chiều mạnh thỏa mãn các yêu cầu mật mã.

*C. Các lớp tương đương theo số lượng biến đầu vào*

Trong mục này chúng tôi sẽ trình bày chi tiết ý tưởng phân loại các lược đồ thành các lớp tương đương được trình bày trong [4]. Theo đó, một lớp các lược đồ nhận được từ một lược đồ bởi biến đổi tuyến tính của các biến đầu vào được gọi là một lớp tương đương. Cụ thể các lược đồ sẽ được phân loại theo số lượng biến đầu vào độc lập của hàm nén. Mục đích của việc phân loại này là xem xét các lớp lược đồ theo số lượng các biến đầu vào tổng quát.

***Nhóm 1:*** Hàm nén phụ thuộc vào 2 biến đầu vào

Có 7 lớp tương đương mà hàm nén phụ thuộc vào 2 biến đầu vào độc lập là $X_i$ và $H_{i-1}$. Như vậy, trong mỗi lớp này sẽ có 6 phần tử vì có 6 ma trận $2\times 2$ khả nghịch trên trường GF(2), cụ thể như sau:

- Lớp 1: $FF = P, P \neq K$ . Xét lược đồ đại diện cho lớp này như sau:

$$f(X_i, H_{i-1}) = E(H_{i-1}, X_i) \oplus X_i \qquad (2)$$

và các lược đồ thông qua lần lượt 6 phép biến đổi tuyến tính $A_1, \ldots, A_6$ lên các biến:

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, A_5 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, A_5 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Ví dụ, với ma trận $A_1$ ta sẽ nhận được chính biểu thức hàm nén là (2). Đây là phép biến đổi đồng nhất.

Với ma trận $A_2$ ta có:

$A_2 (X_i\, H_{i-1})^T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} X_i \\ H_{i-1} \end{pmatrix} = \begin{pmatrix} H_{i-1} \\ X_i \end{pmatrix}$ ta suy ra lược đồ tương đương với lược đồ đại diện là $f(X_i, H_{i-1}) = E(X_i, H_{i-1}) \oplus H_{i-1}$. Các lược đồ còn lại được lập tương tự, dựa trên các phép biến đổi tuyến tính theo các ma trận còn lại.

Vậy các lược đồ thuộc lớp này là:

- $f(X_i, H_{i-1}) = E(H_{i-1}, X_i) \oplus X_i$

(lược đồ 6).

- $f(X_i, H_{i-1}) = E(X_i, H_{i-1}) \oplus H_{i-1}$ (lược đồ 25).

- $f(X_i, H_{i-1}) = E(H_{i-1} \oplus X_i, X_i) \oplus X_i$

(lược đồ 7).

- $f(X_i, H_{i-1}) = E(H_{i-1}, H_{i-1} \oplus X_i) \oplus H_{i-1} \oplus X_i$

(lược đồ 46).

- $f(X_i, H_{i-1}) = E(X_i \oplus H_{i-1}, H_{i-1}) \oplus H_{i-1}$

(lược đồ 27).

- $f(X_i, H_{i-1}) = E(X_i, X_i \oplus H_{i-1}) \oplus X_i \oplus H_{i-1}$

(lược đồ 45).

Tương tự như vậy ta sẽ nhận được các lớp còn lại của nhóm 1 như sau:

- Lớp 2: $FF = K, P \neq K$. Các lược đồ thuộc lớp này là: 21, 37, 10, 42, 15, 31.
- Lớp 3: $P = K, FF \neq P$. Các lược đồ thuộc lớp này là: 9, 13, 22, 30, 39, 43.

BẢNG 2. PHÂN LOẠI 64 LƯỢC ĐỒ THÀNH CÁC LỚP TƯƠNG ĐƯƠNG THEO SỐ LƯỢNG BIẾN ĐẦU VÀO

| Nhóm | Lớp | Đặc trưng của lớp | Lược đồ số | *n* | Tấn công | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | - | D | P | B | F | FP | √ |
| 1 | 1 | $FF = P, P \neq K$ | 6, 7, 25, 27, 45, 46 | 6 | | | | | | 4 | 2 |
| | 2 | $FF = K, P \neq K$ | 10, 15, 21, 31, 37, 42 | 6 | | 2 | | 4 | | | |
| | 3 | $P = K, FF \neq P$ | 9, 13, 22, 30, 39, 43 | 6 | | 2 | 2 | 2 | | | |
| | 4 | $FF = P \oplus K, P \neq K$ | 11, 14, 23, 29, 38, 41 | 6 | | | | | | 4 | 2 |
| | 5 | $FF = V, P \neq K$ | 2, 3, 17, 19,, 33, 34 | 6 | | 2 | | 4 | | | |
| | 6 | $P = V, FF \neq K$ | 54, 55, 57, 59, 61, 62 | 6 | | 2 | 2 | 2 | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 7 | $K=V, FF\neq P$ | 12, 16, 24, 32, 40, 44 | 6 | | 4 | 1 | 1 | | | |
| 2 | 8 | $FF=P=K$ | 5, 26, 47 | 3 | 2 | | | | 1 | | |
| | 9 | $FF=V, P=K$ | 1, 18, 35 | 3 | 2 | | | | 1 | | |
| | 10 | $P=V, FF=K$ | 53, 58, 63 | 3 | 2 | | | | 1 | | |
| | 11 | $K=V, FF=P$ | 8, 28, 48 | 3 | 2 | | | | 1 | | |
| | 12 | $FF=P=V$ | 49, 50, 51 | 3 | 2 | | | | 1 | | |
| | 13 | $FF=K=V$ | 4, 20, 36 | 3 | 2 | 1 | | | | | |
| | 14 | $P=K=V$ | 56, 60, 64 | 3 | 2 | 1 | | | | | |
| 3 | 15 | $FF=P=K=V$ | 52 | 1 | 1 | | | | | | |
| **Tổng số** | | | | 64 | 15 | 14 | 5 | 13 | 5 | 8 | 4 |

• Lớp 4: $FF=P\oplus K, P\neq K$. Các lược đồ thuộc lớp này là: 14, 11, 23, 29, 38, 41.

• Lớp 5: $FF=V, P\neq K$. Các lược đồ thuộc lớp này là: 2, 17, 3, 19, 33, 34.

• Lớp 6: $P=V, FF\neq K$. Các lược đồ thuộc lớp này là: 54, 55, 57, 59, 61,62.

• Lớp 7: $K=V, FF\neq P$. Các lược đồ thuộc lớp này là: 24, 40, 12, 44, 16, 32.

***Nhóm 2:*** Hàm nén chỉ phụ thuộc vào 1 biến đầu vào:

Có 7 lớp tương đương mà hàm nén phụ thuộc vào một biến độc lập duy nhất. Mỗi lớp có 3 phần tử vì có 3 đầu vào có thể là $X_i, H_{i-1}$ và $X_i\oplus H_{i-1}$. Khi thay đổi vai trò (ví dụ lược đồ "Y" chỉ phụ thuộc vào biến $X_i$, khi thay $X_i$ bằng biến $H_{i-1}$ hoặc $X_i\oplus H_{i-1}$) ta sẽ nhận được một lược đồ tương ứng. Bằng phân tích đơn giản và thống kê theo Bảng 1 ta có các lớp tương đương sau:

• Lớp 8: $FF=P=K$. Các lược đồ thuộc lớp này là: 5, 26, 47.

• Lớp 9: $FF=V, P=K$. Các lược đồ thuộc lớp này là: 1, 18, 35.

• Lớp 10: $P=V, FF=K$. Các lược đồ thuộc lớp này là: 53, 58, 63.

• Lớp 11: $K=V, FF=P$. Các lược đồ thuộc lớp này là: 8, 28, 48.

• Lớp 12: $FF=P=V, K\neq P$. Các lược đồ thuộc lớp này là: 49, 50, 51.

• Lớp 13: $FF=K=V, P\neq K$. Các lược đồ thuộc lớp này là:4, 20, 36.

• Lớp 14: $P=K=V, FF\neq P$. Các lược đồ thuộc lớp này là: 56, 60, 64.

***Nhóm 3:*** Hàm nén chỉ đơn giản là một hằng số:

Có 1 lớp tương đương mà hàm nén đơn giản chỉ là hằng số và lớp này cũng chỉ có duy nhất một phần tử.

• Lớp 15: $FF=P=K=V$. Lược đồ 52 thuộc lớp này.

Theo cách phân loại ở trên ta có số liệu tổng hợp (Bảng 2). Trong bảng, *n* là số lượng các lược đồ trong lớp. Để đặc trưng hóa một lớp, một quan hệ sẽ được cho giữa bản rõ *P*, khóa *K* và biến *FF*.

Như vậy chỉ 4 trong 64 lược đồ là an toàn và đại diện của chúng là các lược đồ S. Matyas, C. Meyer, J. Oseas (số 6, Bảng 1), Miyaguchi-Preneel (số 14), số 38 và số 46. Ngoài ra có 8 lược đồ chỉ dễ bị tấn công bởi Tấn công điểm bất động. Như phân tích trong phần chứng minh của mệnh đề 1 ở mục trước, tấn công điểm bất động có thể được loại bỏ một cách dễ dàng bởi một số cấu trúc sửa đổi, cho nên có thể coi 12 lược đồ là an toàn trong tổng số 64 lược đồ có thể của hàm nén.

## IV. THÁM MÃ VI SAI LÊN CÁC LƯỢC ĐỒ HÀM NÉN AN TOÀN

Trong [4] Preneel và cộng sự có đưa ra bình luận về thám mã vi sai lên 12 lược đồ an toàn như trong Bảng 3 dưới đây. 12 lược đồ này nhận được trong phần phân loại theo số lượng các biến đầu vào của hàm nén trong Mục III.

BẢNG 3. CÁC TÍNH CHẤT CỦA 12 LƯỢC ĐỒ AN TOÀN THEO CÁC BIẾN SỬ DỤNG TRONG THÁM MÃ VI SAI

| **TT** | **Lược đồ số** | **Biểu thức hàm nén** | **Các biến** |
|---|---|---|---|
| 1 | 6 | $H_i=E(H_{i-1}, X_i)\oplus X_i$ | $X_i$ |
| 2 | 46 | $H_i=E(H_{i-1}, X_i\oplus H_{i-1})\oplus \oplus X_i\oplus H_{i-1}$ | $X_i$ |
| 3 | 14 | $H_i=E(H_{i-1}, X_i)\oplus X_i\oplus H_{i-1}$ | $X_i$ |
| 4 | 38 | $H_i=E(H_{i-1}, X_i\oplus H_{i-1})\oplus X_i$ | $X_i$ |
| 5 | 25 | $H_i=E(X_i, H_{i-1})\oplus H_{i-1}$ | $H_{i-1}$ |
| 6 | 45 | $H_i=E(X_i, X_i\oplus H_{i-1})\oplus \oplus X_i\oplus H_{i-1}$ | $H_{i-1}$ |

| | | | |
|---|---|---|---|
| 7 | 29 | $H_i = E(X_i, H_{i-1}) \oplus X_i \oplus H_{i-1}$ | $H_{i-1}$ |
| 8 | 41 | $H_i = E(X_i, X_i \oplus H_{i-1}) \oplus H_{i-1}$ | $H_{i-1}$ |
| 9 | 7 | $H_i = E(X_i \oplus H_{i-1}, X_i) \oplus X_i$ | $X_i, H_{i-1}$ |
| 10 | 27 | $H_i = E(X_i \oplus H_{i-1}, H_{i-1}) \oplus \oplus H_{i-1}$ | $H_{i-1}$ |
| 11 | 11 | $H_i = E(X_i \oplus H_{i-1}, X_i) \oplus H_{i-1}$ | $X_i, H_{i-1}$ |
| 12 | 23 | $H_i = E(X_i \oplus H_{i-1}, H_{i-1}) \oplus X_i$ | $X_i, H_{i-1}$ |

Bảng 3 chỉ đưa ra các biến, nhưng không chỉ ra cách tác động lên chúng để có thể thu được những quan hệ vi sai phù hợp. Trong phạm vi của mục này chúng tôi sẽ phân tích cụ thể cách tác động này để tìm ra biểu thức va chạm cho hàm nén. Nhưng trước tiên chúng tôi đưa vào các tấn công va chạm sau:

*Tấn công tìm kiếm va chạm* (*search-collison attack*). Cho hàm băm $H: V^* \mapsto V_n$. Tìm hai thông điệp khác nhau $M, M' \in V^*$ thỏa mãn $H(M) = H(M')$. Cặp $\{M, M'\}$ gọi là cặp va chạm của hàm *H*.

*Tấn công giả va chạm* (*pseudo-collision attack*). Tìm hai thông điệp khác nhau $M, M' \in V^*$ và hai giá trị $IV, IV' \in V_n$ thỏa mãn $H(IV, M) = H(IV', M')$. Khi đó cặp $\{(IV, M), (IV', M')\}$ gọi là cặp giả va chạm của hàm *H*.

*Tấn công gần va chạm* (*near-collision attack*). Tìm hai thông điệp khác nhau $M, M' \in V^*$ thỏa mãn $H(M) + H(M')$ có trọng số Hamming nhỏ.

*Tấn công gần giả va chạm* (*pseudo-near-collision attack*). Tìm hai thông điệp khác nhau $M, M' \in V^*$ hai giá trị $IV, IV' \in V_n$ thỏa mãn $H(IV, M) + H(IV', M')$ có trọng số Hamming nhỏ.

Trong [1, 2] đưa ra định lý về mối quan hệ giữa hàm băm lặp an toàn kháng va chạm trên cơ sở hàm nén kháng va chạm. Theo đó độ phức tạp tìm va chạm của hàm nén khi biết va chạm của hàm băm là tương đương nhau. Chính vì vậy việc xây dựng hàm nén an toàn kháng va chạm là rất quan trọng trong thiết kế hàm băm lặp. Trong [16] AlTawy và cộng sự đưa ra tấn công Rebound lên số vòng rút gọn của hàm nén sử dụng trong hàm băm GOST R 34.11-2012, trong đó sử dụng lược đồ Miyaguchi-Preneel (là một lược đồ an toàn), làm hạt nhân trong thiết kế hàm nén. Ngoài GOST R 34.11-2012, hàm băm Whirepool cũng sử dụng lược đồ này trong thiết kế hàm nén của mình và cũng giống như GOST R 34.11-2012, nó bị tấn công Rebound lên số vòng rút gọn. Mặt khác tấn công Rebound chính là tấn công dựa trên cơ sở thám mã vi sai. Đây chính là lý do vì sao trong mục này chúng tôi xem xét độ an toàn của các lược đồ theo quan điểm thám mã vi sai.

Bây giờ chúng tôi sẽ đưa ra biểu thức điều kiện cho quan hệ vi sai và biểu thức va chạm tương ứng cho hàm nén Miyaguchi-Prenell (lược đồ 14, Bảng 1). Hàm nén của lược đồ này có dạng

$$f(H, X) = E(H, X) \oplus X \oplus H$$

*Tấn công tìm kiếm va chạm:*

Xét biểu thức

$$f(H, X) \oplus f(H, X \oplus \Delta X) =$$
$$E(H, X) \oplus H \oplus X \oplus E(H, X \oplus \Delta X) \oplus$$
$$\oplus H \oplus X \oplus \Delta X =$$
$$E(H, X) \oplus E(H, X \oplus \Delta X) \oplus \Delta X$$

Trong biểu thức này ta thấy rằng nếu mã khối *E* có quan hệ vi sai $\Delta X \to \Delta X$, có nghĩa là

$$E(H, X) \oplus E(H, X \oplus \Delta X) = \Delta X \qquad (3)$$

Khi đó $f(H, X) \oplus f(H, X \oplus \Delta X) = 0$. Suy ra $f(H, X) = f(H, X \oplus \Delta X)$ chính là va chạm của hàm nén.

*Tấn công giả va chạm:*

Tấn công tìm kiếm giả va chạm trong một số tài liệu còn gọi là tấn công va chạm bắt đầu tự do. Trong kiểu tấn công này xét cả sai khác của khối bản rõ và của cả khóa (trong trường hợp này đóng vai trò là giá trị *H*). Theo đó ta xét biểu thức:

$$f(H, X) \oplus f(H \oplus \Delta H, X \oplus \Delta X) =$$
$$E(H, X) \oplus H \oplus X \oplus E(H \oplus \Delta H, X \oplus \Delta X) \oplus$$
$$\oplus H \oplus \Delta H \oplus X \oplus \Delta X$$
$$= E(H, X) \oplus E(H, X \oplus \Delta X) \oplus \Delta X \oplus \Delta H$$

Trong biểu thức này ta thấy rằng nếu mã khối *E* có quan hệ vi sai $\Delta H, \Delta X \to \Delta X \oplus \Delta H$, quan hệ này tương đương với biểu thức:

$$E\ H,X\ \oplus E\ H\oplus\Delta H,X\oplus\Delta X\ =\Delta X\oplus\Delta H \quad (4)$$

Khi đó chúng ta có

$$f\ H,X\ \oplus f\ H\oplus\Delta H,X\oplus\Delta X\ =0$$

Suy ra $f\ H,X\ =f\ H\oplus\Delta H,X\oplus\Delta X$ chính là giả va chạm của hàm nén.

*Tấn công gần va chạm:*

Lập luận tương tự như hai tấn công trên ta nhận được kết quả như sau: Nếu mã khối $E()$ có quan hệ vi sai $\Delta X\rightarrow\Delta E$, có nghĩa là

$$E\ H,X\ \oplus E\ H,X\oplus\Delta X\ =\Delta E \quad (5)$$

khi đó có

$$E\ H,X\oplus\Delta X\ \oplus X\oplus\ X\oplus\Delta X\ =$$
$$=\ E\ H,X\ \oplus H\oplus X\ \oplus\ \Delta X\oplus\Delta E$$

Nếu như $\Delta X\oplus\Delta E$ có trọng số nhỏ, khi đó $f\ H,X\ \oplus f\ H,X\oplus\Delta X\ =\Delta X\oplus\Delta E$ chính là gần va chạm của hàm nén.

*Tấn công gần giả va chạm:*

Bằng lập luận tương tự chúng ta có thể đưa ra được biểu thức quan hệ vi sai với mã khối $E()$ trong trường hợp tấn công tìm kiếm gần giả va chạm. Theo đó nếu mã khối $E()$ có quan hệ vi sai với khóa quan hệ $\Delta H,\Delta X\ \rightarrow\Delta E$, có nghĩa là chúng thỏa mãn biểu thức:

$$E\ H,X\ \oplus E\ H\oplus\Delta H,X\oplus\Delta X\ =\Delta E \quad (6)$$

khi đó có

$$E\ H\oplus\Delta H,X\oplus\Delta X\ \oplus$$
$$\oplus\ H\oplus\Delta H\ \oplus\ X\oplus\Delta X\ =$$
$$=\ E\ H,X\ \oplus H\oplus X\ \oplus\ \Delta X\oplus\Delta H\oplus\Delta E$$

Nếu như $\Delta X\oplus\Delta H\oplus\Delta E$ có trọng số nhỏ, khi đó biểu thức:

$$f\ H,X\ \oplus f\ H\oplus\Delta H,X\oplus\Delta X\ =\Delta X\oplus\Delta E$$

chính là gần giả va chạm của hàm nén.

Qua phân tích lược đồ Miyaguchi-Preneel trước thám mã vi sai theo 4 tấn công trong mục IV ta thấy rằng, nếu chỉ ra được sự tồn tại những quan hệ vi sai (3), (4), (5), (6) đối với mã khối $E$ với độ phức tạp nhỏ hơn $2^{n/2}$, thì khi đó có thể dễ dàng thực hiện 4 tấn công này lên hàm nén Miyaguchi-Preneel, hay nói cách khác hàm nén này là không an toàn trước thám mã vi sai.

Đối với các lược đồ khác, khi lập luận tương tự ta cũng thu được điều kiện quan hệ vi sai của mã khối, để từ đó có thể nhận được biểu thức tương ứng cho tấn công va chạm, tấn công giả va chạm, tấn công gần va chạm và tấn công gần giả va chạm. Bảng thống kê những điều kiện và biểu thức này có kích thước lớn nên chúng tôi không đưa vào nội dung bài báo.

## V. KẾT LUẬN

Nghiên cứu về các hàm nén dựa trên mã khối, các kết quả chính đạt được cụ thể như sau:

- Phân tích chi tiết 64 lược đồ hàm nén dựa trên mã khối theo mô hình tổng quát dựa trên 5 tấn công cơ bản.
- Phân tích chi tiết để phân loại lược đồ theo số lượng các biến đầu vào của hàm nén.
- Đưa ra biểu thức quan hệ vi sai (3), (4), (5) và (6) cho hàm nén Miyaguchi-Preneel để từ đó dễ dàng nhận được biểu thức va chạm, gần va chạm, giả va chạm và gần giả va chạm cho hàm nén này.

Kết quả phân tích theo 5 tấn công cơ bản đã chỉ ra 12 lược đồ là an toàn. Tuy nhiên trong bài báo này chúng tôi không đưa ra phân tích theo quan điểm thám mã vi sai cho toàn bộ 12 lược đồ an toàn mà chỉ phân tích cho lược đồ Miyaguchi-Preneel như là một lược đồ đại diện. Kết quả phân tích trước thám mã vi sai lên Miyaguchi-Preneel nói riêng và toàn bộ 12 lược đồ an toàn nói chung chỉ ra rằng nếu tồn tại quan hệ vi sai với độ phức tạp nhỏ hơn $2^{n/2}$, thì khi đó có thể dễ dàng thực hiện 4 tấn công này lên hàm nén tương ứng, hay nói cách khác hàm nén này là không an toàn trước thám mã vi sai.

## TÀI LIỆU THAM KHẢO

[1]. Damgård, I.B. "A design principle for hash functions", CRYPTO'89, 1989.

[2]. Merkle, R.C. "One way hash functions and DES"., CRYPTO'89, 1989.

[3]. P. Gauravaram. "Cryptographic Hash Functions Cryptanalysis, Design and Applications", Thesis, 2013. Information Security Institute, Queensland University of Technology.

[4]. B. Preneel, R. Govaerts, and J. Vandewalle, "Hash functions based on block ciphers: a synthetic approach", CRYPTO'1993, Lecture Notes in Computer Science 773, D. R. Stinson (ed.), Springer-Verlag, pp. 368-378, 1993.

[5]. M.O. Rabin, "Digitalized signatures," in "Foundations of Secure Computation," R. Lipton and R. DeMillo, Eds., Academic Press, New York, pp. 155-166, 1978.

[6]. D. Denning, "Digital signatures with RSA and other public-key cryptosystems". Communications ACM, vol. 27, pp. 388-392, April 1984.

[7]. R.S. Winternitz, "A secure one–way hash function built from DES," Proc. IEEE Symposium on Information Security and Privacy 1984, pp. 88-90, 1984.

[8]. R.S. Winternitz, "Producing a one-way hash function from DES", CRYPTO'83, D. Chaum, Ed., Plenum Press, New York, pp. 203-207, 1984.

[9]. S.M. Matyas, C.H. Meyer, and J. Oseas, "Generating strong one-way functions with cryptographic algorithm," IBM Techn. Disclosure Bull., vol. 27, no. 10A, pp. 5658-5659, 1985.

[10]. S. Miyaguchi, M. Iwata, and K. Ohta, "New 128-bit hash function," Proc. 4th International Joint Workshop on Computer Communications, Tokyo, Japan, July 13–15, pp. 279-288, 1989.

[11]. Dunkelman, O. and E. Biham. "A framework for iterative hash functions: Haifa". in 2nd NIST Cryptographich Hash Workshop, 2006.

[12]. Rivest, R., "The MD5 message-digest algorithm", 1992.

[13]. Eastlake, D. and P. Jones, "US secure hash algorithm 1 (SHA1"), RFC 3174, September, 2001.

[14]. Barreto, P. and V. Rijmen. "The Whirlpool hashing function". in First open NESSIE Workshop, Leuven, Belgium, 2000.

[15]. Preneel, B., "Analysis and design of cryptographic hash functions". Thesis, 2003, Citeseer.[16]. Dolmatov, V. and A. Degtyarev, "GOST R 34.11-2012: Hash Function", 2013.

[16]. Dolmatov, V. and A. Degtyarev," GOST R 34.11-2012: Hash Function", 2013.

[17]. AlTawy, R., Kircanski, A., and Youssef, A. M. "Rebound attacks on Stribog". In ICISC (2013), H.-S. Lee and D.-G. Han, Eds., vol. 8565 of Lecture Notes in Computer Science, Springer, pp. 175–188, 2013.

[18]. O. Dunkelman, E. Biham, "The AHAvite-3 Hash Function". Submission to NIST (Round 2) (2009): 113.

## SƠ LƯỢC VỀ TÁC GIẢ

**TS. Nguyễn Văn Long**

Đơn vị công tác: Viện Khoa học – Công nghệ Mật mã, Ban Cơ yếu Chính phủ, Hà Nội.

E-mail: nvlong.bcy@gmail.com.

Tốt nghiệp chuyên nghành An toàn thông tin các Hệ thống viễn thông, năm 2008 và nhận bằng Tiến sĩ chuyên ngành Các phương pháp bảo vệ thông tin, Học viện FSO, Liên bang Nga năm 2015.

Hướng nghiên cứu hiện nay: Khoa học mật mã, mã hóa đối xứng.

**CN. Hoàng Đình Linh**

Đơn vị công tác: Viện Khoa học – Công nghệ Mật mã, Ban Cơ yếu Chính phủ, Hà Nội.

E-mail: linhhd@bcy.gov.vn.

Tốt nghiệp chuyên ngành Toán học Đại học Khoa học tự nhiên ĐHQGHN chương trình Tiên tiến.

Hướng nghiên cứu hiện nay: Nghiên cứu, thiết kế, đánh giá độ an toàn chứng minh được của các thuật toán mã hóa đối xứng.