Một cải tiến cận an toàn kháng va chạm cho lược đồ Hirose trong mô hình mã pháp lý tưởng

Trần Hồng Thái, Hoàng Đình Linh

***Tóm tắt*— Trong số các hàm nén dựa trên mã khối, có 3 hàm nén độ dài khối kép nổi tiếng đạt được độ an toàn kháng va chạm và kháng tiền ảnh tối ưu (lần lượt lên đến 2^n và 2^{2n} truy vấn) đó là Abreast-DM, Tandem-DM và lược đồ Hirose. Gần đây đã có một số lược đồ mới được đề xuất, tuy nhiên các chứng minh độ an toàn đều dựa trên các kết quả đã có đối với 3 lược đồ trên. Trong đó, lược đồ Hirose đạt được cận an toàn kháng va chạm và kháng tiền ảnh tốt hơn 2 lược đồ còn lại. Ngoài ra nó còn hiệu quả hơn khi chỉ sử dụng một lược đồ khoá duy nhất cho 2 mã khối cơ sở. Trong bài báo này, chúng tôi đưa ra một cận an toàn kháng va chạm chặt hơn cho lược đồ Hirose. Kết quả khi áp dụng với mã khối có độ dài khối 128 bit và độ dài khoá 256 bit, ví dụ như AES-256, đó là không có một kẻ tấn công bất kỳ nào thực hiện ít hơn $2^{126.73}$ truy vấn có thể tìm được một va chạm cho hàm nén Hirose với xác suất lớn hơn 1/2.**

***Abstract*— Among the compression functions based on block ciphers, there are three well-known double-block-length compression functions that achieve collision and preimage resistance security (up to 2^n and 2^{2n}, respectively) that are Abreast-DM, Tandem-DM and Hirose scheme. Recently, several new schemes have been proposed, but the security proofs are based on the results available for the three schemes above. In particular, the Hirose Scheme that achieves impact resistance and preimage resistance is better than the other two schemes. In addition, it is more efficient to use only a single key scheme for 2 base block ciphers. In this paper, we give a more secure collision resistance for the Hirose scheme. The result when applied to block ciphers with a 128-bit block length and a 256-bit key length, such as AES-256, is that no attacker make less than $2^{126.73}$ queries can find a collision for Hirose compression function with a probability greater than 1/2.**

***Từ khóa:* lược đồ Hirose, hàm nén độ dài khối kép, mã pháp lý tưởng, độ an toàn kháng va chạm, độ an toàn kháng tiền ảnh.**

***Keywords*: – Hirose scheme, double-block-length compression function, ideal cipher, collision resistance, preimage resistance.**

Bài báo được nhận ngày 8/8/2019. Bài báo được nhận xét bởi phản biện thứ nhất vào ngày 05/9/2019 và được chấp nhận đăng vào ngày 16/9/2019. Bài báo được nhận xét bởi phản biện thứ hai vào ngày 06/9/2019 và được chấp nhận đăng vào ngày 12/10/2019.

I. GIỚI THIỆU

Các hàm băm mật mã nhận một thông báo đầu vào có độ dài bất kỳ và trả về một xâu bit đầu ra có độ dài cố định. Đã có nhiều cấu trúc được sử dụng cho việc băm các thông báo có độ dài thay đổi mà trong đó lặp lại một hàm nén có kích thước cố định, như là cấu trúc Merkle-Damgård, khung HAIFA, cấu trúc Sponge... Hàm nén cơ sở có thể được xây dựng từ các thành phần hỗn tạp hoặc dựa trên chính các nguyên thuỷ mật mã như mã khối. Gần đây các cấu trúc hàm nén dựa trên mã khối thu hút được nhiều sự quan tâm, vì nhiều hàm băm chuyên dụng đã cho thấy các điểm yếu về độ an toàn.

Cách tiếp cận chung nhất là xây dựng một hàm nén $2n$ bit sang n bit sử dụng 1 phép gọi mã khối n bit, được gọi là hàm nén độ dài khối đơn (single block length - SBL). Tuy nhiên, một hàm nén như vậy có thể bị tổn thương trước các tấn công va chạm vì có độ dài đầu ngắn. Ví dụ, ta có thể thực hiện thành công tấn công ngày sinh lên một hàm nén dựa trên AES-128 chỉ dùng xấp xỉ 2^{64} truy vấn. Điều này đã thúc đẩy các nghiên cứu về các hàm nén độ dài khối kép (double block length - DBL), là các hàm nén có đầu ra gấp đôi độ dài của mã khối cơ sở.

Các hàm nén độ dài khối kép có thể chia thành hai lớp:

- Lớp thứ nhất là các hàm nén sử dụng mã khối cơ sở có kích cỡ khoá là n bit, tức là $E:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, ký hiệu là lớp

DBL^n. Một số hàm nén thuộc lớp 1 là MDC-2, MDC-4 [1], cấu trúc MJH [2, 3], lược đồ Parrallel-DM [4], lược đồ PBGV [5], lược đồ LOKI DBH [6], lược đồ của Mennink [7] và một cấu trúc đưa ra bởi Jetchev cùng đồng sự [8]. Trong đó chỉ có MJH và lược đồ của Mennink được chứng minh là đạt độ an toàn kháng va chạm tối ưu, tuy nhiên vẫn chưa đạt độ an toàn kháng tiền ảnh tối ưu.

- Lớp thứ hai là các hàm nén sử dụng mã khối cơ sở có kích cỡ khoá là 2*n* bit, tức là $E:\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^n$, ký hiệu là lớp DBL^{2n}. Một số hàm nén thuộc lớp thứ 2 như Tandem-DM [9] và Abreast-DM [9], lược đồ Hirose [10], hàm nén loại I của Stam [11] và các thiết kế tổng quát của Hirose [12] và Özen cùng Stam [13]. Tất cả các hàm nén trên đều cung cấp đảm bảo độ an toàn va chạm tối ưu (lên đến 2^n truy vấn), các hàm nén Tandem-DM, Abreast-DM và lược đồ Hirose còn được chứng minh thêm là kháng tiền ảnh tối ưu (lên đến 2^{2n} truy vấn). Trong đó, lược đồ Hirose đạt được cận an toàn kháng va chạm và kháng tiền ảnh tốt nhất trong 3 lược đồ trên.

Bài báo này đưa ra một cải tiến cận an toàn kháng va chạm chặt hơn cho lược đồ Hirose. Phần còn lại của bài báo có bố cục như sau: Mục II trình bày một số khái niệm cơ sở về mô hình mã pháp lý tưởng. Mục III nhắc lại một số cận an toàn đã được phân tích đối với hai lược đồ hàm nén Abreast-DM và Tandem-DM. Mục IV phân tích độ an toàn đối với hàm nén Hirose, trong đó chúng tôi đưa ra một cận an toàn kháng va chạm chặt hơn cho lược đồ hàm nén Hirose. Cuối cùng là kết luận ở Mục V.

II. MỘT SỐ KHÁI NIỆM CƠ SỞ

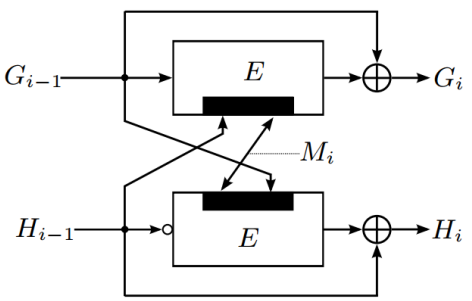
Một mã khối là một hàm $E:\{0,1\}^m\times\{0,1\}^n\to\{0,1\}^n$ sao cho $E(K,\cdot)$ là một hoán vị trên $\{0,1\}^n$ với mỗi $K\in\{0,1\}^m$. Chúng ta gọi *m* là độ dài khoá và *n* là độ dài khối của mã khối *E*. Thông thường ta viết $E_K(X)$ thay vì $E(K,X)$ với $K\in\{0,1\}^m, X\in\{0,1\}^n$. Ký hiệu hàm $E_K^{-1}(\cdot)$ là nghịch đảo của $E_K(\cdot)$.

Mô hình mã pháp lý tưởng. Với *m*, *n* nguyên dương, ký hiệu:

$$BC(m,n)=\left\{\begin{matrix}E:\{0,1\}^m\times\{0,1\}^n\to\{0,1\}^n\mid\forall K\in\{0,1\}^m,\\ E_K(\cdot)\text{ là một hoán vị trên }\{0,1\}^n\end{matrix}\right\}.$$

Trong mô hình mã pháp lý tưởng, một mã khối *E* được chọn ngẫu nhiên đều từ $BC(m,n)$. Cho phép 2 kiểu truy vấn $E_K(X)$ hoặc $E_K^{-1}(Y)$ với $X,Y\in\{0,1\}^n, K\in\{0,1\}^m$, *X*, *Y* và *K* lần lượt được gọi là bản rõ, bản mã và khoá. Câu trả lời của một truy vấn ngược $E_K^{-1}(Y)$ là $X\in\{0,1\}^n$ thoả mãn $E_K(X)=Y$. Trong phạm vi bài báo này, chúng ta chỉ xét trường hợp $m=2n$ và đặt $N=2^n$.

Hàm nén Abreast-DM và Tandem-DM đã được đề xuất tại EUROCRYPT '92 bởi Xuejia Lai và James L. Massey [9]. Các hàm nén này sử dụng kết hợp 2 lược đồ hàm nén đơn Davies-Meyer lần lượt như Hình 1 và Hình 2. Mô tả chi tiết của các lược đồ này lần lượt được đưa ra trong Định nghĩa 1 và Định nghĩa 2.

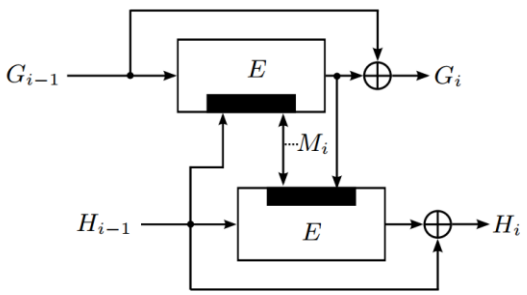


Hình 1. Hàm nén Abreast-DM, trong đó "◦" ký hiệu phép bù bit.

Định nghĩa 1 (Definition 2, [14]). *Cho* $F^{ADM}:\{0,1\}^{2n}\times\{0,1\}^n\to\{0,1\}^{2n}$ *là một hàm nén thoả mãn* $(G_i,H_i)=F^{ADM}(G_{i-1},H_{i-1},M_i)$ *trong đó* $G_i,H_i,M_i,G_{i-1},H_{i-1}\in\{0,1\}^n$. F^{ADM} *sử dụng một mã khối E có độ dài khoá 2n bit và độ dài khối n bit như sau:*

$$\begin{cases}G_i=G_{i-1}\oplus E_{H_{i-1}\|M_i}(G_{i-1})\\ H_i=H_{i-1}\oplus E_{M_i\|G_{i-1}}(\bar{H}_{i-1})\end{cases}$$

trong đó $\bar{H}$ *là ký hiệu phép bù bit của H.*

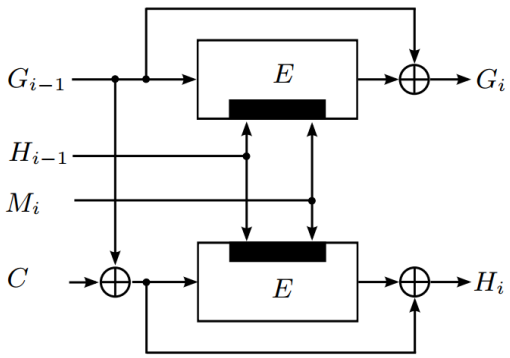


Hình 2. Hàm nén Tandem-DM

Định nghĩa 2 (Definition 16, [14]). *Cho* $F^{TDM}:\{0,1\}^{2n}\times\{0,1\}^{n}\to\{0,1\}^{2n}$ *là một hàm nén thoả mãn* $(G_i,H_i)=F^{TDM}(G_{i-1},H_{i-1},M_i)$ *trong đó* $G_i,H_i,M_i,G_{i-1},H_{i-1}\in\{0,1\}^{n}$. F^{TDM} *sử dụng một mã khối E có độ dài khoá 2n bit và độ dài khối n bit như sau:*

$$\begin{cases} W_i = E_{H_{i-1}\|M_i}(G_{i-1}) \\ G_i = G_{i-1}\oplus E_{H_{i-1}\|M_i}(G_{i-1}) = G_{i-1}\oplus W_i \\ H_i = H_{i-1}\oplus E_{M_i\|W_{i-1}}(H_{i-1}) \end{cases}$$

Tại FSE'06, Hirose [10] đã đề xuất hàm nén độ dài khối kép F^{Hirose}. Hàm nén được minh hoạ trong Hình 3 và được mô tả chi tiết trong Định nghĩa 3.



Hình 3. Hàm nén Hirose, C là một hằng số

Định nghĩa 3 (Definition 15, [14]). *Cho* $F^{Hirose}:\{0,1\}^{2n}\times\{0,1\}^{n}\to\{0,1\}^{2n}$ *là một hàm nén thoả mãn* $(G_i,H_i)=F^{Hirose}(G_{i-1},H_{i-1},M_i)$ *trong đó* $G_i,H_i,M_i,G_{i-1},H_{i-1}\in\{0,1\}^{n}$. F^{Hirose} *sử dụng một mã khối E có độ dài khoá 2n bit và độ dài khối n bit như sau:*

$$\begin{cases} G_i = G_{i-1}\oplus E_{H_{i-1}\|M_i}(G_{i-1}) \\ H_i = G_{i-1}\oplus C\oplus E_{H_{i-1}\|M_i}(G_{i-1}\oplus C) \end{cases}$$

trong đó $C\in\{0,1\}^{n}\setminus\{0^{n}\}$ *là một hằng số.*

Lợi thế kháng va chạm và kháng tiền ảnh. Gọi $F:\{0,1\}^{3n}\to\{0,1\}^{2n}$ là một hàm nén dựa trên một mã khối lý tưởng $E\in BC(2n,n)$, và A là một kẻ tấn công thông tin-lý thuyết với bộ tiên tri truy cập đến E hoặc E^{-1}.

Thí nghiệm $\mathbf{Exp}_{\mathrm{A}}^{Coll}$

$E\xleftarrow{\$}BC(2n,n)$

$\mathrm{A}^{E,E^{-1}}$ cËp nhËt Q

Nếu $\exists A\neq A', B$ sao cho

$A\Rightarrow_{\mathrm{Q}} B$ và $A'\Rightarrow_{\mathrm{Q}} B$

thì trả về 1

nếu không trả về 0

Hình 4a. Thí nghiệm tìm va chạm

Khi đó ta thực hiện thí nghiệm $\mathbf{Exp}_{\mathrm{A}}^{Coll}$ như mô tả trong Hình 4a, để định lượng độ an toàn kháng va chạm của F. Thí nghiệm sẽ lưu lại các truy vấn mà kẻ tấn công A thực hiện vào một lịch sử truy vấn Q. Một bộ $(X,K,Y)\in$Q nếu A hỏi $E_K(X)$ và thu được câu trả lời Y hoặc hỏi $E_K^{-1}(Y)$ và thu được câu trả lời X. Với $A\in\{0,1\}^{3n}, B\in\{0,1\}^{2n}$ ký hiệu $A\Rightarrow_{\mathrm{Q}} B$ nếu tồn tại một cặp truy vấn $(X_1,K_1,Y_1),(X_2,K_2,Y_2)\in$Q sao cho A có tính toán $F(A)=B$ sử dụng cặp truy vấn trên.

Khi đó lợi thế tìm va chạm của A được định nghĩa là

$$Adv_F^{Coll}(\mathrm{A})=\Pr\left[\mathbf{Exp}_{\mathrm{A}}^{Coll}=1\right].$$

Xác suất lấy trên mã khối E ngẫu nhiên. Với $q>0$, chúng ta định nghĩa $Adv_F^{Coll}(q)$ là giá trị lớn nhất của $Adv_F^{Coll}(\mathrm{A})$ trên tất cả các kẻ tấn công A thực hiện q truy vấn.

Lợi thế tìm tiền ảnh của A được định nghĩa tương tự sử dụng thí nghiệm $\mathbf{Exp}_{\mathrm{A}}^{Pre}$ được mô tả trong Hình 4b. Kẻ tấn công A chọn một giá trị ảnh mục tiêu $B\in\{0,1\}^{2n}$ trước khi thực hiện các truy vấn. Lợi thế tìm tiền ảnh của A được định nghĩa là

$$Adv_F^{Pre}(\mathrm{A})=\Pr\left[\mathbf{Exp}_{\mathrm{A}}^{Pre}=1\right].$$

Thí nghiệm $\mathbf{Exp}_{\mathrm{A}}^{Pre}$

$E \xleftarrow{\$} BC(2n,n)$

A chän $B \in \{0,1\}^{2n}$

$\mathrm{A}(B)^{E,E^{-1}}$ cËp nhËt Q

Nếu $\exists A$ sao cho $A \Rightarrow_{\mathrm{Q}} B$

thì trả về 1

nếu không trả về 0

Hình 4b. Thí nghiệm tìm tiền ảnh

Xác suất lấy trên mã khối E ngẫu nhiên. Với $q > 0$, chúng ta định nghĩa $Adv_F^{Pre}(q)$ là giá trị lớn nhất của $Adv_F^{Pre}(\mathrm{A})$ trên tất cả các kẻ tấn công A thực hiện q truy vấn.

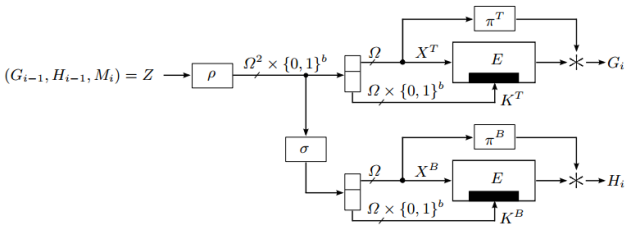
Hai lược đồ Abreast-DM và Hirose nằm trong một lớp các hàm nén tổng quát có tên gọi là hàm nén độ dài khối kép tuần hoàn (cyclic double block length).

Định nghĩa 4 (Definition 6, [14]). *Cho* $(\Omega,*)$ *là một nhóm,* $N = |\Omega|$. *Gọi* $F^{CYC}: \Omega^2 \times \{0,1\}^b \to \Omega^2$ *là một hàm nén thoả mãn* $(G_i, H_i) = F^{CYC}(G_{i-1}, H_{i-1}, M_i)$ *trong đó* $G_{i-1}, H_{i-1}, G_i, H_i \in \Omega$ *và* $M_i \in \{0,1\}^b, b > 0$. *Cho* $E \in BC\left(\Omega, \Omega \times \{0,1\}^b\right)$ *là một mã khối;* ρ *và* σ *là các hoán vị trên* $\Omega^2 \times \{0,1\}^b$ *và* π^T, π^B *là các hoán vị trên* Ω. *Đặt* $Z := (G_{i-1}, H_{i-1}, M_i) \in \Omega^2 \times \{0,1\}^b$. *Khi đó* $X^T, X^B \in \Omega, K^T, K^B \in \Omega \times \{0,1\}^b$ *thoả mãn* $(X^T, K^T) = \rho(Z)$ *và* $(X^B, K^B) = \sigma(\rho(Z))$. *Khi đó* F^{CYC} *chứa mã khối E được biểu diễn như sau:*

$$\begin{cases} G_i = E_{K^T}(M^T) * \pi^T(X^T) \\ H_i = E_{K^B}(M^B) * \pi^B(X^B) \end{cases}$$

trong đó tính toán đưa ra G_i *thường được gọi là hàng trên và tính toán* H_i *được gọi là hàng dưới.*

Hàm nén F^{CYC} được minh hoạ như trong Hình 5.



Hình 5. Hàm nén tuần hoàn

$(G_i, H_i) = F^{CYC}(Z), Z = (G_{i-1}, H_{i-1}, M_i)$

Định nghĩa 5 (Definition 7, [14]). *Cho* σ *là một song ánh trên tập S trong đó* $S := \Omega^2 \times \{0,1\}^b$. *Gọi ID là ánh xạ đồng nhất trên S. Hàm* σ^k *được định nghĩa là* $\sigma^k := \sigma \circ \sigma^{k-1}$ *với* $k > 0$ *và* $\sigma^0 := ID$.

(i) Cố định một phần tử $s \in S$. *Bậc của s được định nghĩa là* $|s| = \min_{r \geq 1}(\sigma^r(s) = s)$, *tức là* $|s|$ *là giá trị nhỏ nhất (lớn hơn 0) thoả mãn* $\sigma^{|s|}(s) = s$.

(ii) Nếu có một giá trị $c \in \mathrm{N}^*$ *thoả mãn* $\forall s \in S: |s| = c$, *ta nói rằng thứ tự của ánh xạ* σ, *được ký hiệu là* $|\sigma|$, *bằng c, tức là* $|\sigma| = c$. *Nếu không tồn tại c như vậy thì* $|\sigma| := 0$. *Chú ý rằng nếu* $|\sigma| > 0$ *thì bậc của* σ *bằng bậc của một phần tử bất kỳ được chọn từ S.*

Định nghĩa 6 (Definition 8, [14]). *Cho* F^{CYC}, ρ, σ *như được định nghĩa trong Định nghĩa 4. Nếu* $|\sigma| \geq 2$ *thì* F^{CYC} *được gọi là hàm nén độ dài khối kép tuần hoàn (CDBL) với độ dài chu kỳ là* $|\sigma|$.

Trong trường hợp hàm nén Abreast-DM và Hirose, ta có:

Hàm nén Abreast-DM:

$\Omega = \{0,1\}^n, b = n, \pi^T = ID, \pi^B(X) = \bar{X}, \rho = ID$ và $\sigma(G,H,M) = (\bar{H}, M, G)$. Hàm nén Abreast-DM có chu kỳ $|\sigma| = c = 6$.

Hàm nén Hirose:

$\Omega = \{0,1\}^n, b = n, \pi^T = \pi^B = ID, \rho = ID$ và $\sigma(G_{i-1}, H_{i-1}, M_i) = (G_{i-1} \oplus c, H_{i-1}, M_i)$. Hàm nén Hirose có chu kỳ $|\sigma| = 2$.

III. ĐỘ AN TOÀN CỦA CẤU TRÚC ABREAST-DM VÀ TANDEM-DM

Đã có nhiều kết quả nghiên cứu độc lập chỉ ra Abreast-DM và Tandem-DM đạt độ an toàn và kháng tiền ảnh tối ưu. Phần này nhắc lại một số kết quả tốt nhất đã có cho 2 lược đồ này đến nay theo hiểu biết của các tác giả.

Trong [15], Lee cùng đồng sự đã đưa ra cận an toàn kháng va chạm cho hàm nén Abreast-DM là

$$Adv_{ADM}^{Coll}(q) \le \frac{q}{\left(2^n - 6q\right)} + \frac{18q^2}{\left(2^n - 6q\right)^2}.$$

Tuy nhiên, trong [14] Fleischmann cùng đồng sự cũng đã độc lập đưa ra cận an toàn kháng va chạm cho hàm nén Abreast-DM chặt hơn như sau:

Định lý 1 (Theorem 1, [14]). *Cho* $F := F^{ADM}$ *như trong Định nghĩa 1 và n, q là các số tự nhiên với* $q < 2^{n-2.58}$. *Khi đó*

$$Adv_{ADM}^{Coll}(q) \le 18\left(\frac{q}{2^{n-1}}\right)^2.$$

Từ đó, ta có kết quả sau:

Hệ quả 1. *Cho* $F := F^{ADM}$ *như trong Định nghĩa 1 và n, q là các số tự nhiên với* $q \le 2^{n-3.58}$. *Khi đó*

$$Adv_{ADM}^{Coll}(q) \le \frac{1}{2} + o(1)$$

trong đó $o(1) \to 0$ *khi* $n \to +\infty$.

Chứng minh. Xét $18\left(\frac{q}{2^{n-1}}\right)^2 = \frac{1}{2}$ suy ra $q = \frac{2^{n-1}}{6} = 2^{n-1-\log_2 6} \approx 2^{n-3.58}$. Áp dụng Định lý 1 với $q \le 2^{n-3.58}$ suy ra điều phải chứng minh.

Hệ quả 1 có ý nghĩa đó là một kẻ tấn công bất kỳ thực hiện ít hơn $2^{n-3.58}$ truy vấn đến bộ tiên tri mã khối thì không thể tìm được một va chạm cho hàm nén Abreast-DM với một xác suất đáng kể (ở đây là lớn hơn bằng 1/2).

Trong [15] Lee và Kwon đã chỉ ra cận an toàn kháng tiền ảnh cho Abreast-DM là $Adv_{ADM}^{Pre}(q) \le 6q/\left(2^n - 6q\right)^2$. Tuy nhiên, cận này trở nên vô nghĩa khi $q \ge 2^n/6$. Sau đó, Fleichmann cùng đồng sự [16] đã cải tiến cận này. Kết quả được đưa ra trong Định lý 2.

Định lý 2 (Theorem 2, [16]). *Cho* $F^{ADM} : \{0,1\}^{3n} \to \{0,1\}^{2n}$ *là hàm nén dựa trên mã khối được mô tả như Hình 1. Cho* $\alpha > 0$ *là một số nguyên và N, q là các số tự nhiên thoả mãn* $N = 2^n$. *Khi đó*

$$Adv_{ADM}^{Pre}(q) \le \frac{16\alpha}{N} + \frac{8q}{N^2(N-2)} + 2\left(\frac{2eq}{\alpha N}\right)^{\alpha} + \frac{4q}{\alpha N}.$$

Hệ quả 2 (Corollary 2, [16]). *Ta có*

$$Adv_{ADM}^{Pre}\left(2^{2n-10}\right) \le 1/2 + o(1)$$

trong đó $o(1)$ *tiến đến 0 khi* $n \to \infty$.

Trong [17], Lee và đồng sự đã đưa ra cận kháng va chạm và kháng tiền ảnh cho Tandem-DM như sau:

Định lý 3 (Theorem 1, [17]). *Cho* $N = 2^n, q < N/2, N' = N - 2q$ *và một số nguyên* α *thoả mãn* $1 \le \alpha \le 2q$. *Khi đó*

$$Adv_{TDM}^{Coll}(q) \le 2N\left(\frac{2eq}{\alpha N'}\right)^{\alpha} + \frac{4q\alpha}{N'} + \frac{4q}{N'}.$$

Một ví dụ cho Định lý 3 là với $n = 128, q = 2^{120.87}$ và $\alpha = 16$ ta có

$$Adv_{TDM}^{Coll}\left(2^{120.87}\right) < 1/2.$$

Định lý 4 (Theorem 2, [17]). *Cho* $N = 2^n, q < N^2$ *và* $\alpha > 0$ *là một số nguyên. Thì*

$$Adv_{TDM}^{Pre\neq 0}(q) \le \frac{16\alpha}{N} + \frac{8q}{N^2(N-2)} + 2\left(\frac{2eq}{\alpha N}\right)^{\alpha} + \frac{4q}{\alpha N}.$$

Một ví dụ cho Định lý 4 là với $n = 128, q = 2^{245.99}$ và $\alpha = q^{1/2}/2$ ta có

$$Adv_{TDM}^{Pre\neq 0}\left(2^{245.99}\right) \le 0.498.$$

IV. ĐỘ AN TOÀN CỦA LƯỢC ĐỒ HIROSE

Một điều đáng chú ý đó là lược đồ Hirose được đề xuất sau hơn 10 năm so với thời điểm hai lược đồ Abreast-DM và Tandem-DM được đề xuất. Nhưng cũng phải đến gần đây các kết quả an toàn chứng minh được của cả 3 lược đồ này mới được đưa ra. Trong đó, các kết quả chỉ ra rằng lược đồ Hirose đạt được độ an toàn kháng va chạm và kháng tiền ảnh cao hơn hai lược đồ còn lại.

A. Độ an toàn kháng va chạm của lược đồ Hirose

Trong [14], Lee cùng đồng sự đã đưa ra kết quả sau:

Định lý 5 (Theorem 3, [14]). *(Độ an toàn kháng va chạm cho $|\sigma|=2$) cho $F:=F^{CYC}$ là một hàm nén tuần hoàn với chu kỳ $c=|\sigma|=2$ như trong Định nghĩa 6. Nếu $\pi^T=\pi^B$ thì $a=1$ nếu không $a=2$. Khi đó với $q>1$ và $2q<N$, ta có*

$$Adv_F^{Coll}(q)\le\frac{2aq^2}{(N-2q)^2}+\frac{2q}{N-2q}.$$

Áp dụng cho hàm nén Hirose ta có Hệ quả sau:

Hệ quả 3. *Cho $F^{Hirose}:\{0,1\}^{3n}\to\{0,1\}^{2n}$ là một hàm nén dựa trên mã khối được mô tả như Hình 3. Khi đó*

$$Adv_{Hirose}^{Coll}(q)\le 2q^2/(N-2q)^2+2q/(N-2q).$$

Chứng minh. Áp dụng Định lý 5 cho lược đồ Hirose với $|\sigma|=2,\pi_T=\pi_B$ ta có điều phải chứng minh.

Hệ quả 4. *Cho $F^{Hirose}:\{0,1\}^{3n}\to\{0,1\}^{2n}$ là một hàm nén dựa trên mã khối được mô tả như Hình 3. Khi đó với $q\le 2^{n-2.77}$ ta có*

$$Adv_{Hirose}^{Coll}(q)\le 1/2+o(1)$$

trong đó $o(1)$ tiến về 0 khi n tiến ra vô cùng.

Chứng minh. Trước tiên ta thấy rằng vế phải của Hệ quả 3 là một hàm đồng biến theo q với $q<N/2$. Xét

$$2q^2/(N-2q)^2+2q/(N-2q)=1/2.$$

Đặt $q/(2N-q)=t$ ta có phương trình bậc 2

$$2t^2+2t=1/2.$$

Phương trình có nghiệm dương là $t=\frac{-1+\sqrt{2}}{2}$. Trả lại biến $\frac{q}{N-2q}=\frac{-1+\sqrt{2}}{2}$ suy ra:

$$q=N\left(\frac{-1+\sqrt{2}}{2\sqrt{2}}\right)\approx 2^{n-2.77}.$$

Áp dụng Hệ quả 3, suy ra điều phải chứng minh.

Chứng minh của Định lý 5 có thể áp dụng cho trường hợp tổng quát của các lược đồ hàm nén tuần hoàn có $|\sigma|=2$. Tuy nhiên, chúng tôi đã xem xét và chứng minh lại đối với trường hợp cụ thể là lược đồ Hirose theo cách tiếp cận của [18] và đưa ra một cận tốt hơn so với hệ quả 5. Cụ thể chúng tôi đưa ra định lý sau:

Định lý 6. *Cho $F^{Hirose}:\{0,1\}^{3n}\to\{0,1\}^{2n}$ là một hàm nén dựa trên mã khối được mô tả như Hình 3. Khi đó*

$$Adv_{Hirose}^{Coll}(q)\le q(q-1)/(N-q)^2.$$

Chứng minh. Xét một kẻ tấn công A bất kỳ thực hiện q truy vấn lên mã khối E hoặc E^{-1} để tìm va chạm đối với hàm nén F^{Hirose}. A sẽ lưu một lịch sử truy vấn $Q:=\{Q_i\}_{i=1}^{q}$, trong đó $Q_i=(K_i,X_i,Y_i)$ thoả mãn $E_{K_i}(X_i)=Y_i$. Chú ý rằng A không bao giờ thực hiện lặp lại 1 truy vấn mà hắn đã biết câu trả lời. Chúng ta xét một kẻ tấn công A′ mô phỏng A nhưng đôi khi sẽ thực hiện thêm một truy vấn bổ sung lên bộ tiên tri E dưới một số điều kiện nào đó. Do đó, A′ là mạnh hơn A và ta chỉ cần tìm cận trên của xác suất thành công của A′ để đưa ra một va chạm cho hàm nén F^{Hirose}.

Kẻ tấn công A′ sẽ duy trì một danh sách L (được khởi tạo là rỗng) mô tả một đầu vào/đầu ra bất kỳ của hàm nén F^{Hirose} mà có thể tính được bởi kẻ tấn công A. Một phần tử $L\in\mathrm{L}$ là một bộ 4 giá trị $(K,X,Y,Y')\in\{0,1\}^{5n}$ trong đó $K\in\{0,1\}^{2n}, X\in\{0,1\}^{n}$ là đầu vào 3n bit của hàm nén thoả mãn $K=(H_{i-1},M)$ và $X=G_{i-1}$. Các giá trị n bit Y,Y' được cho bởi $Y=E_K(X)$ và $Y'=E_K(X\oplus C)$.

Danh sách được xây dựng như sau. Kẻ tấn công A sẽ thực hiện truy vấn thứ i lên E hoặc E^{-1} với $1\le i\le q$. Nếu là truy vấn lên E, kẻ tấn công sẽ thu được bộ 3 (K_i,X_i,Y_i) trong đó $E_{K_i}(X_i)=Y_i$. Nếu là truy vấn lên E^{-1}, kẻ tấn công vẫn thu được một bộ 3 (K_i,X_i,Y_i) nhưng là $E_{K_i}^{-1}(Y_i)=X_i$. Trong mỗi trường hợp đó, giá trị $X_i\oplus Y_i$ được xác định một cách ngẫu nhiên.

Bây giờ, A′ sẽ kiểm tra xem một phần tử $L=(K_i,X_i,*,*)$ hoặc $L'=(K_i,X_i\oplus C,*,*)$ có

trong danh sách L hay không, trong đó "*" là một giá trị tuỳ ý. Khi đó, chúng ta phân tích 2 trường hợp mà A′ gặp phải.

Trường hợp 1: Cả L và L' đều không có trong L. Khi đó A′ sẽ thực hiện một truy vấn xuôi $Y_i' = E_{K_i}(X_i \oplus C)$. Do hằng số C khác 0 nên giá trị của Y_i' xuất hiện ngẫu nhiên đều và độc lập với Y_i. Khi đó, đặt $L_i := (K_i, X_i, Y_i, Y_i')$ và thêm vào danh sách L.

Bây giờ chúng ta định nghĩa thế nào là một va chạm trong danh sách. Cố định 2 số nguyên a, b với $a \neq b$, sao cho $L_a = (K_a, X_a, Y_a, Y_a')$ là phần tử thứ a trong L và $L_b = (K_b, X_b, Y_b, Y_b')$ là phần tử thứ b trong L. Ta nói rằng L_a và L_b va chạm nếu một va chạm của hàm nén xảy ra sử dụng các kết quả truy vấn trong L_a và L_b. Sự kiện này xảy ra khi và chỉ khi một trong 2 điều kiện sau xảy ra.

(i) $Y_a \oplus X_a = Y_b \oplus X_b$ và $Y_a' \oplus X_a = Y_b' \oplus X_b$

(ii) $Y_a \oplus X_a = Y_b' \oplus X_b \oplus C$ và $Y_a' \oplus X_a = Y_b \oplus X_b \oplus C$

Đối với truy vấn thứ i có tối đa $i-1$ phần tử trong danh sách L có thể va chạm với L_i. Do đó, xác suất thành công của truy vấn thứ i lớn nhất là

$$\sum_{j=1}^{i-1} \frac{2}{(N-q)^2} = \frac{2(i-1)}{(N-q)^2}.$$

Vì kẻ tấn công A thực hiện tối đa q truy vấn, nên danh sách L không thể chứa nhiều hơn q phần tử (với mỗi truy vấn của kẻ tấn công A chỉ có thể thêm tối đa 1 phần tử vào danh sách L của A′). Do đó, xác suất thành công đối với q truy vấn là

$$\leq \sum_{i=1}^{q} \frac{2(i-1)}{(N-q)^2} = \frac{q(q-1)}{(N-q)^2}.$$

Trường hợp 2: Rõ ràng theo cách xây dựng, không thể xảy ra trường hợp chỉ có chính xác 1 trong 2 giá trị L và L' nằm trong L. Do đó, giả sử rằng cả hai giá trị này đều đã có trong L. Khi đó A′ sẽ bỏ qua truy vấn này vì chúng ta biết rằng A không có cơ hội chiến thắng, nếu không thì chúng ta đã đưa tấn công cho kẻ tấn công trước đó.

Vậy, xác suất để kẻ tấn công A′ thành công là:

$$Adv_{F^{Hirose}}^{Coll}(A') \leq \frac{q(q-1)}{(N-q)^2}.$$

Vì A là một kẻ tấn công bất kỳ thực hiện q truy vấn nên ta có

$$Adv_{Hirose}^{Coll}(q) \leq q(q-1)/(N-q)^2.$$

Hệ quả 5. *Cho* $F^{Hirose}: \{0,1\}^{3n} \to \{0,1\}^{2n}$ *là một hàm nén dựa trên mã khối được mô tả như hình 3. Khi đó với* $q \leq 2^{n-1.27}$ *ta có*

$$Adv_{Hirose}^{Coll}(q) \leq 1/2 + o(1)$$

trong đó $o(1)$ *tiến về 0 khi n tiến ra vô cùng.*

Chứng minh. Trước tiên ta thấy rằng vế phải của Định lý 6 là một hàm đồng biến theo q với $q < N$. Xét

$$q(q-1)/(N-q)^2 = 1/2.$$

Suy ra

$$q \approx N(\sqrt{2}-1) \approx 2^{n-1.27}.$$

Áp dụng Định lý 6, suy ra điều phải chứng minh.

B. Độ an toàn kháng tiền ảnh của lược đồ Hirose

Trong [15], Lee và Kwon đã chứng minh rằng $Adv_{Hirose}^{Pre}(q) \leq 2q/(N-2q)^2$, cận này trở nên vô nghĩa khi $q > N/2$. Sau đó, Fleischmann cùng đồng sự [16] đã đưa ra một cận cải tiến như sau:

Định lý 7 (Theorem 1, [16]). *Cho* $F^{Hirose}: \{0,1\}^{3n} \to \{0,1\}^{2n}$ *là một hàm nén dựa trên mã khối được mô tả như hình 3. Khi đó*

$$Adv_{Hirose}^{Pre}(q) \leq 8q/N^2 + 8q/N(N-2).$$

Đặc biệt, $Adv_{Hirose}^{Pre}(q)$ *bị chặn trên bởi xấp xỉ* $16q/N^2$.

V. KẾT LUẬN

Trong bài báo này, chúng tôi đã đưa ra và chứng minh một cận an toàn kháng va chạm chặt hơn cho lược đồ hàm nén Hirose. Trong đó, cận an toàn kháng va chạm mới của chúng tôi cho lược đồ Hirose (Định lý 6) là tốt hơn nhiều so với cận được đưa ra trong [14], và tiệm cận đến độ an toàn tối ưu ($\approx 2^{n-1.27}$).

Hướng nghiên cứu tiếp theo: Có thể thấy cả 3 lược đồ Abreast-DM, Tandem-DM và Hirose

đều sử dụng song song hai lược đồ Davies-Meyer và đạt độ an toàn tối ưu, do đó có thể hướng đến việc đề xuất và nghiên cứu độ an toàn của các lược đồ hàm nén mới sử dụng các lược đồ hàm nén đơn khác như lược đồ Matyas-Meyer-Oseas hoặc Miyaguchi–Preneel. Ngoài ra, việc xem xét độ an toàn của các lược đồ hàm nén trên trong mô hình mã pháp yếu (weak cipher model) cũng cần được nghiên cứu thêm.

TÀI LIỆU THAM KHẢO

[1]. Meyer, C.H. and Schilling, M. *Secure program load with manipulation detection code*. in *Proc. Securicom*. 1988.

[2]. Lee, J. and Stam, M. *MJH: A faster alternative to MDC-2*. in *Cryptographers' Track at the RSA Conference*. 2011. Springer.

[3]. Lee, J. and Stam, M., *MJH: a faster alternative to MDC-2.* Designs, Codes and Cryptography, 2015. **76**(2): p. 179-205

[4]. Hohl, W., et al. *Security of iterated hash functions based on block ciphers*. in *Annual International Cryptology Conference*. 1993. Springer.

[5]. Prencel, B., et al. *Collision-free hashfunctions based on blockcipher algorithms*. in *Security Technology, 1989. Proceedings. 1989 International Carnahan Conference on*. 1989. IEEE.

[6]. Brown, L., Pieprzyk, J., and Seberry, J. *LOKI—a cryptographic primitive for authentication and secrecy applications*. in *International Conference on Cryptology*. 1990. Springer.

[7]. Mennink, B. *Optimal collision security in double block length hashing with single length key*. in *International Conference on the Theory and Application of Cryptology and Information Security*. 2012. Springer.

[8]. Jetchev, D., Özen, O., and Stam, M. *Collisions are not incidental: A compression function exploiting discrete geometry*. in *Theory of Cryptography Conference*. 2012. Springer.

[9]. Lai, X. and Massey, J.L. *Hash functions based on block ciphers*. in *Workshop on the Theory and Application of of Cryptographic Techniques*. 1992. Springer.

[10]. Hirose, S. *Some plausible constructions of double-block-length hash functions*. in *International Workshop on Fast Software Encryption*. 2006. Springer.

[11]. Stam, M. *Blockcipher-based hashing revisited*. in *Fast Software Encryption*. 2009. Springer.

[12]. Hirose, S. *Provably secure double-block-length hash functions in a black-box model*. in *International Conference on Information Security and Cryptology*. 2004. Springer.

[13]. Özen, O. and Stam, M. *Another glance at double-length hashing*. in *IMA International Conference on Cryptography and Coding*. 2009. Springer.

[14]. Fleischmann, E., Gorski, M., and Lucks, S. *Security of cyclic double block length hash functions*. in *IMA International Conference on Cryptography and Coding*. 2009. Springer.

[15]. Lee, J. and Kwon, D., *The security of Abreast-DM in the ideal cipher model.* IEICE transactions on fundamentals of electronics, communications and computer sciences, 2011. **94**(1): p. 104-109

[16]. Armknecht, F., et al. *The preimage security of double-block-length compression functions*. in *International Conference on the Theory and Application of Cryptology and Information Security*. 2011. Springer.

[17]. Lee, J., Stam, M., and Steinberger, J.J.J.o.C., *The security of Tandem-DM in the ideal cipher model.* 2017. **30**(2): p. 495-518

[18]. Fleischmann, E., et al., *Weimar-DM: The Most Secure Double Length Compression Function.*

SƠ LƯỢC VỀ TÁC GIẢ

ThS. Trần Hồng Thái

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

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

Nhận bằng Kỹ sư năm 2000 và Thạc sĩ năm 2007 chuyên ngành Kỹ thuật mật mã, Học viện Kỹ thuật Mật mã.

Hướng nghiên cứu hiện nay: Nghiên cứu đánh giá độ an toàn của mã khối và hàm băm mật mã

CN. Hoàng Đình Linh

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

Email: hoangdinhlinh@bcy.gov.vn

Quá trình đào tạo: Nhận bằng cử nhân Toán học tại Đại học Khoa học tự nhiên - Đại học Quốc gia Hà Nội năm 2014.

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.