Mối liên hệ giữa tính nhận biết tiền ảnh và một số tính chất mật mã khác của hàm băm

Nguyễn Tuấn Anh, Triệu Quang Phong

***Tóm tắt*—Hàm băm và các tính chất xung quanh nó luôn là một chủ đề rất được quan tâm. Sau các thuộc tính cơ bản của hàm băm như một chiều, kháng va chạm,… thì một số tính chất khác đã được xem xét, trong đó có tính nhận biết tiền ảnh (PrA). Trong bài báo này, chúng tôi khảo sát mối liên hệ giữa tính PrA và một số tính chất mật mã khác của hàm băm. Ngoài việc tổng hợp các kết quả đã có, chúng tôi đưa ra và phân tích các mối quan hệ mới. Kết quả thu được giúp hiểu rõ hơn về mối liên hệ giữa một số tính chất mật mã của hàm băm và thuận tiện hơn trong việc lựa chọn hàm băm phù hợp trong các ứng dụng mật mã.**

***Abstract*—The hashing function and its properties have always been an very interesting topic. Apart from the basic properties of hashing functions such as one-way, collision resistance,... the preimage awareness (PrA) also gradually gets more interesting. In this paper, we examine the relationship between PrA and some other cryptographic properties of the hash function. In addition to synthesizing existing results, we develop and analyze new relationships. The results provide a better understanding of the relationship between some of the cryptographic properties of hash function and the more convenience in choosing the right hash function in cryptographic applications.**

Từ khóa—bộ tiên tri giả ngẫu nhiên, tính nhận biết tiền ảnh, tính nhận biết tiền ảnh yếu, tính nhận biết tiền ảnh bị hạn chế.

Keywords—Pseudo-random oracle; preimage awareness, weak preimage awareness, bounded preimage awareness.

I. GIỚI THIỆU

Nhiều hàm băm sử dụng trong các ứng dụng mật mã đều được phân tích trong mô hình bộ tiên tri ngẫu nhiên. Không may, các hàm băm thông dụng hiện nay, bao gồm họ hàm SHA, đều sử dụng cấu trúc lặp Merkle-Damgård (được củng cố) với một hàm nén lại không thể sử dụng được như một bộ tiên tri ngẫu nhiên ngay cả khi hàm nén của nó được giả sử là lý tưởng [1]. Điều này dẫn đến sự không liên kết giữa lý thuyết và thực hành: mặc dù không có tấn công nào lên các ứng dụng cụ thể mà sử dụng các hàm băm hiện có được biết đến, nhưng cũng không có đảm bảo an toàn nào ngay cả khi hàm nén là lý tưởng. Để giải quyết cho vấn đề này, đã có hai cách tiếp cận được đề xuất.

Vào năm 2004, Maurer và các cộng sự đã đề xuất khái niệm bộ tiên tri giả ngẫu nhiên (Pseudo-Random Oracle – PrO) trong [2], sau đó nó được chấp nhận cho các hàm băm bởi Coron trong [3]. Khái niệm này thường được áp dụng cho các hàm H^P có sử dụng các thành phần được kết nối thông qua bộ tiên tri P. Ví dụ, có thể giả sử rằng hàm nén của một hàm băm được tạo ra từ một mã pháp lý tưởng hay một bộ tiên tri ngẫu nhiên. Trong mô hình như vậy, việc giả thiết kẻ tấn công có quyền truy cập vào bộ tiên tri P là hợp lý. Ý nghĩa thực tế quan trọng nhất của tính chất PrO là mọi ứng dụng mà dùng H^P như là một hàm băm đều có độ an toàn như khi H^P được giả thiết là một bộ tiên tri ngẫu nhiên. Điều này có nghĩa là có thể chứng minh độ an toàn của ứng dụng trong mô hình bộ tiên tri ngẫu nhiên và sau đó thay thế bộ tiên tri bởi một mô hình hàm băm H^P "thực tế hơn".

Vào năm 2009, Dodis và cộng sự [1] đã đề xuất khái niệm có tên gọi là nhận biết tiền ảnh (Preimage Awareness – PrA). Tính nhận biết tiền ảnh thỏa mãn ba yêu cầu: tính tự nhiên, độ an toàn đủ thuyết phục cho các ứng dụng quan trọng, có thể xây dựng được bằng cách sử dụng cấu trúc Merkle-Damgård (được củng cố) khi hàm nén đủ mạnh. Sau đó, một số tính chất liên

Bài báo được nhận ngày 19/02/2021. Bài báo được nhận xét bởi phản biện thứ nhất ngày 19/4/2021 và được chấp nhận đăng ngày 23/4/2021. Bài báo được nhận xét bởi phản biện thứ hai ngày 11/6/2021 và được chấp nhận đăng ngày 15/6/2021.

quan được đề xuất: tính nhận biết tiền ảnh yếu (Weak Preimage Awareness – WPrA) [1], tính nhận biết tiền ảnh mạnh (Strong Preimage Awareness – SPrA) [4] và tính nhận biết tiền ảnh bị hạn chế (Bounded Preimage Awareness – BPrA) [5]. Trong khi WPrA dùng để chứng minh một hàm băm là PrA nếu như nó đã WPrA và CR (kháng va chạm – Collision Resistance), thì SPrA và BPrA là các khái niệm làm chặt hơn tính PrA được đề xuất bởi Buldas và các cộng sự.

Bên cạnh đó, tính chất PrA và các biến thể của nó cũng đã được sử dụng để đánh giá độ an toàn của các lược đồ chữ ký ít phụ thuộc khóa [4] và lược đồ BLT [6] trong hạ tầng KSI. Trong đó, [4] chỉ ra cận an toàn của các lược đồ này phụ thuộc vào tính chất mà hàm băm được sử dụng đạt được. Cụ thể, hàm băm được sử dụng trong các lược đồ chữ ký ít phụ thuộc khóa yêu cầu thỏa mãn một trong các tính chất CR, PrA, SPrA, BPrA hoặc RO (độ dài đầu ra của hàm băm giảm dần đối với các tính chất này); trong lược đồ chữ ký BLT yêu cầu hàm băm PrO hoặc RO hoặc đồng thời tính hàm giả ngẫu nhiên (Pseudo-Random Function – PRF) và BPrA.

Vì vậy, việc nghiên cứu các tính chất PrA cũng như mối liên hệ giữa chúng là vấn đề cần thiết trong việc xây dựng các hàm băm sử dụng trong các ứng dụng thích hợp. Tuy nhiên, chỉ có một vài mối quan hệ được chỉ ra trong các tài liệu [4] và [1]. Nội dung này sẽ được trình bày chi tiết trong Bảng 1. Trong đó, bảng được đọc theo chiều ngang, dấu "✓" nghĩa là suy ra được, dấu "**×**" nghĩa là không suy ra được, dấu "**-**" nghĩa là chưa nghiên cứu được, MĐ là Mệnh đề, ĐL là Định lý và ĐN là Định nghĩa. Các kết quả được in đậm là kết quả của nhóm tác giả.

BẢNG 1. MỐI QUAN HỆ GIỮA PRA VÀ CÁC TÍNH CHẤT LIÊN QUAN

	RO	**PrO**	**BPrA**	**PrA**	**WPrA**	**CR**
RO	✓	-	✓ **(MĐ 5)**	✓ (ĐL3)	✓	✓
PrO	-	✓	-	✓ **(MĐ 6)**	✓	✓ **(BĐ1)**
BPrA	-	-	✓	✓ (ĐN3)	✓	✓
PrA	× **(MĐ4)**	× (NX1)	- (NX2)	✓	✓ **(MĐ 2)**	✓ (ĐL1)
WprA	×	×	×	× **(MĐ 3)**	✓	× (ĐN)
CR	×	×	×	× **(MĐ 1)**	-	✓
CR+WPrA	×	×	×	✓ (ĐL2)	✓	✓

Đóng góp. Trong bài báo này, chúng tôi đã đánh giá một số mối quan hệ giữa các tính chất liên quan đến tính PrA của hàm băm: Tồn tại hàm CR nhưng không phải là PrA, một hàm là PrA thì nó là WPrA, tồn tại hàm WPrA nhưng không phải là PrA, tồn tại hàm PrA nhưng không phải là RO, một hàm là RO thì nó là BPrA, tính PrO suy ra được tính CR và tính PrA. Các kết quả này cùng với các kết quả đã có được tổng hợp trong Bảng 1.

Cấu trúc bài báo. Sau phần mở đầu, trong Phần II chúng tôi trình bày lại các định nghĩa, khái niệm cần thiết. Tiếp theo, Phần III nhắc lại và làm rõ một số kết quả trước đó. Trong Phần IV đưa ra và chứng minh các mối quan hệ giữa tính PrA và các tính chất liên quan. Cuối cùng, Phần cuối trình bày một số kết luận.

II. KHÁI NIỆM

Khi S là một tập, $x \xleftarrow{\$} S$ nghĩa là phần tử x được lấy đều từ tập S. Ta viết $x \xleftarrow{\$} \mathcal{A}$ để ký hiệu việc thuật toán $\mathcal{A}$ chạy với nguồn ngẫu nhiên tươi mới và gán đầu ra của nó là x. Ký hiệu $\{0,1\}^*$ là tập các thông điệp có độ dài bất kỳ nhưng hữu hạn. Với $M \in \{0,1\}^*$, ta viết $M_1, \ldots, M_l \xleftarrow{d} M$, trong đó $l = \lceil |M|/d \rceil$; M_i là chuỗi con d bit thứ i của M, với $1 \le i \le l-1$; và $1 \le |M_l| \le d$.

Với mọi thuật toán f, ta viết $\mathrm{Time}(f)$ là thời gian chạy tối đa để tính $f(x)$ với mọi chuỗi x trong miền xác định.

Bộ tiên tri ngẫu nhiên (RO). Bộ tiên tri ngẫu nhiên đơn giản là một hàm được chọn ngẫu nhiên đều từ tập tất cả hàm trên các miền xác định. Nó lấy đầu vào là một chuỗi nhị phân và đưa ra ngẫu nhiên một chuỗi nhị phân. Ta ký hiệu $H \in RF_{Dom,Rng}$ là một hàm được chọn ngẫu nhiên đều trên không gian các hàm đi từ Dom đến Rng.

Nguyên thủy lý tưởng. Định nghĩa tổng quát của khái niệm này được trình bày trong tài liệu [1] dựa theo khái niệm *Máy Turing tương tác* (Interactive Turing Machine). Tuy nhiên, ta có thể hình dung, nguyên thủy lý tưởng như là một hộp đen, bộ tiên tri ngẫu nhiên, hàm ngẫu nhiên, hoán vị ngẫu nhiên hoặc một mã pháp lý tưởng. Ở đây, mã pháp lý tưởng được hiểu như sau. Mã khối là một ánh xạ $E:\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ sao cho $E(K,\cdot)$ là một hoán vị với mọi $K \in \{0,1\}^k$, trong đó k,n là các số tự nhiên. Xét $\mathrm{BC}(k,n)$ là tập các mã khối như vậy. Một mã pháp lý tưởng $C_{k,n} = (E,D)$ với hai giao diện tương ứng thực thi một mã khối được chọn ngẫu nhiên từ $\mathrm{BC}(k,n)$ và nghịch đảo của nó.

Bộ tiên tri giả ngẫu nhiên (PrO). Đây là một khái niệm áp dụng cho các hàm H^P là hàm mà các thành phần của nó được kết nối thông qua bộ tiên tri P. Ví dụ, ta có thể giả sử rằng hàm nén của một hàm băm được làm từ một mã pháp lý tưởng hay một bộ tiên tri ngẫu nhiên. Khi đó, P chính là hàm nén và H là hàm băm. Trong mô hình như vậy, việc giả thiết kẻ tấn công có quyền truy cập vào bộ tiên tri P là hợp lý. Hơn nữa, H^P đôi khi cũng được sử dụng như một khối kiến trúc trong các giao thức mật mã mà các chứng minh an toàn của nó giả sử rằng H^P được thay thế bởi một bộ tiên tri ngẫu nhiên thực sự Ω. Để sự thay thế này là đúng, ta cần giả thiết rằng H^P là một bộ tiên tri giả ngẫu nhiên.

Định nghĩa 1 (Definition 5, [6]) (PrO). *Ta nói rằng H^P là bộ tiên tri giả ngẫu nhiên (S,t')-an toàn nếu tồn tại một bộ mô phỏng $\mathcal{S}$ thời gian t', sao cho với mọi bộ phân biệt D thời gian t ta có:*

$$\mathrm{Adv}^{\mathrm{pro}}(H^P,D) = \left|\Pr\left[D^{H^P,P}=1\right] - \Pr\left[D^{\Omega,\mathcal{S}^\Omega}=1\right]\right| \le \frac{t}{S}.$$

Chú ý trong định nghĩa trên, Ω là bộ tiên tri ngẫu nhiên và $\mathcal{S}$ không biết các truy vấn đến Ω nhưng có quyền truy cập đến Ω để mô phỏng P, ta ký hiệu là $\mathcal{S}^P$. Ở đây, P là bộ tiên tri mà H được kết nối đến. Để làm rõ nhận xét này, ta xét ví dụ trong cấu trúc Merkle-Damgård với giá trị khởi tạo IV cố định. Xét trường hợp kẻ tấn công truy vấn lên Ω và $\mathcal{S}$. Với thông điệp $x_1\|x_2$, nếu kẻ tấn công truy vấn (IV,x_1) lên $\mathcal{S}$ thu được $u_1 = \mathcal{S}(IV,x_1)$ thì sau đó với truy vấn (u_1,x_2) lên $\mathcal{S}$, giá trị được trả về $u_2 = \mathcal{S}(u_1,x_2)$ có thể được tính bằng cách gọi lên Ω, tức là $\mathcal{S}(u_1,x_2) = \Omega(x_1\|x_2)$. Tuy nhiên, nếu kẻ tấn công truy vấn x_1 lên Ω thu được u_1', sau đó truy vấn (u_1',x_2) lên $\mathcal{S}$ thì giá trị được trả về $u_2' = \mathcal{S}(u_1',x_2)$ không thể được mô phỏng bởi $\Omega(x_1\|x_2)$, bởi vì $\mathcal{S}$ chỉ biết x_2 không biết truy vấn x_1 đã được hỏi đến Ω.

Tính kháng va chạm (CR). Cố định các tập $Dom \subseteq \{0,1\}^*$ và Rng. Xét $\mathcal{A}$ là một kẻ tấn công đưa ra một cặp $x,x' \in Dom$. Xét P là một nguyên thủy lý tưởng. Hàm băm $H^P: Dom \to Rng$ được gọi là S-an toàn kháng va chạm nếu với mọi kẻ tấn công $\mathcal{A}$ thời gian t:

$$\mathrm{Adv}^{\mathrm{cr}}_{H,P}(\mathcal{A}) = \Pr\left[(x,x') \xleftarrow{\$} \mathcal{A}^P \;\middle|\; \begin{matrix} H^P(x) = H^P(x'), \\ x \neq x' \end{matrix}\right] \le \frac{t}{S}$$

trong đó xác suất được lấy trên các lựa chọn ngẫu nhiên được sử dụng bởi $\mathcal{A}$ và nguyên thủy P.

Tính nhận biết tiền ảnh (PrA). Ta có thể hiểu đơn giản hàm H là nhận biết tiền ảnh nếu một kẻ tấn công $\mathcal{A}$ biết được x là tiền ảnh của z, thì có thể bằng một cách nào đó tính $H(x) = z$. Cụ thể, giả sử H là một hàm băm được xây dựng từ một nguyên thủy lý tưởng P. Xét trường hợp sau: Một kẻ tấn công $\mathcal{A}$ đưa ra một điểm z thuộc miền giá trị, có thể sau khi tương tác với bộ tiên tri P. Bộ trích xuất sau đó được chạy trên hai đầu vào: z và *chuỗi tư vấn* (advice string) α. Chuỗi α gồm tất cả lần truy vấn của $\mathcal{A}$ cho đến nay lên P và câu trả lời tương ứng. Bộ trích xuất sử dụng các mảng toàn cục Q (ban đầu là $\perp$ ở mọi vị trí) và V (ban đầu để trống). Q được sử dụng để ghi lại các tham số đầu vào cho $\mathcal{E}$; V được sử dụng để lưu trữ tất cả các giá trị được trích xuất thành công tương ứng với các đầu vào của $\mathcal{E}$. Bộ trích xuất đưa ra một giá trị x trong miền xác định của H sao cho $H^P(x) = z$ hoặc đưa ra $\perp$ trong trường hợp $\mathcal{E}$ không tìm được x nào như vậy. Sau đó, $\mathcal{A}$ tiếp tục và cố gắng đưa ra một tiền ảnh x' sao cho $H^P(x') = z$ nhưng $x \neq x'$. Nói một cách hình thức, nếu không có một kẻ tấn công nào có thể làm như vậy với xác suất cao, thì H là nhận biết tiền ảnh. Ta gọi các truy vấn lên P là truy vấn nguyên thủy, truy vấn lên $\mathcal{E}$ là truy vấn trích xuất.

$\text{Exp}^{\text{pra}}_{H,P,\mathcal{E},\mathcal{A}}$	Bộ tiên tri $\mathbf{P}(m)$	Bộ tiên tri $\mathbf{Ex}(z)$
$x \leftarrow \mathcal{A}^{P,\text{Ex}}$ $z \leftarrow H^P(x)$ If $Q[z] = 1$ và $V[z] \neq x$ return 1 else return 0	$c \leftarrow P(m)$ $\alpha \leftarrow \alpha \| (m, c)$ Return c	$Q[z] \leftarrow 1$ $V[z] \leftarrow \mathcal{E}(z, \alpha)$ Return $V[z]$

Hình 1. Thí nghiệm về tính nhận biết tiền ảnh PrA.

Định nghĩa 2 (Definition 2, [4]). *Một hàm H^P có mức nhận biết tiền ảnh (PrA) S-an toàn nếu tồn tại một bộ trích xuất hiệu quả $\mathcal{E}$, sao cho với mọi bên đối kháng $\mathcal{A}$ hoạt động trong thời gian t, thì:*

$$\text{Adv}^{\text{pra}}_{H,P,\mathcal{E}}(\mathcal{A}) = \Pr\left[\text{Exp}^{\text{pra}}_{H,P,\mathcal{E},\mathcal{A}} = 1\right] \leq \frac{t}{S}.$$

Tính nhận biết tiền ảnh yếu (WPrA). Khái niệm WPrA được định nghĩa đơn giản bằng cách chỉnh sửa thí nghiệm PrA trong Hình 1, sao cho bộ trích xuất khi được truy vấn ảnh z có thể trả về một tập các tiền ảnh tiềm năng (thay vì chỉ một tiền ảnh). Kẻ tấn công thắng nếu như đưa ra được một tiền ảnh x sao cho $H^P(x) = z$ và x không nằm trong tập mà bộ trích xuất trả về. Chú ý, bộ trích xuất được gọi là bộ trích xuất đa điểm $\mathcal{E}^+$. Ta gọi $\mathcal{E}^+$ là trung thực nếu với mọi $z \in Rng$ và chuỗi tư vấn thì:

$$\Pr[\forall x \in \mathcal{X}. H^P(x) = z : \mathcal{X} \leftarrow \mathcal{E}^+(z, \alpha)] = 1.$$

Tính nhận biết tiền ảnh bị hạn chế (BPrA). Khái niệm mới này giả định sự tồn tại của bộ trích xuất PrA bị chặn theo nghĩa với các chuỗi truy vấn có thể tính toán được hiệu quả α, số lượng đầu ra z sao cho $\mathcal{E}(z, \alpha) \neq \perp$ không vượt quá số lượng truy vấn trong α.

Định nghĩa 3 (Tính BPrA) (Definition 8, [5]). *Một hàm $H^P : \{0,1\}^{2n} \to \{0,1\}^n$ có mức nhận biết tiền ảnh bị hạn chế (BPrA) S-an toàn nếu nó có mức nhận biết tiền ảnh (PrA) S-an toàn, và với mọi kẻ tấn công $\alpha \leftarrow \mathcal{A}^P$ chạy trong thời gian t đưa ra một danh sách P-truy vấn α, thì xác suất để $|\{z : \mathcal{E}(z, \alpha) \neq \perp\}| > |\alpha|$ không vượt quá $t^2/2^n$, trong đó $\mathcal{E}$ là bộ trích xuất từ điều kiện PrA.*

III. Các kết quả đã có

Theo các tài liệu [4] và [1], có thể thu được một số kết quả, bao gồm: PrA suy ra CR, WPrA+CR suy ra PrA, và RO suy ra PrA. Do khuôn khổ của bài viết có hạn, nhóm tác giả chỉ nhắc lại các kết quả trên mà không đi vào chứng minh chi tiết của chúng. Hơn nữa, để thống nhất về mặt ký hiệu, nhóm tác giả sẽ sử dụng $A \Rightarrow B$ để ký hiệu tính chất A suy ra tính chất B, và $A \not\Rightarrow B$ để biểu thị tính chất A không đủ để suy ra tính chất B.

Định lý 1. (PrA⇒CR) (Theorem 3.1, [1]). *Xét P là một nguyên thủy lý tưởng và $H^P : Dom \to Rng$ là một hàm băm. Xét $\mathcal{E}$ là một bộ trích xuất. Xét $\mathcal{A}$ là một kẻ tấn công CR lên hàm H sử dụng tối đa q_p truy vấn đến P. Khi đó, tồn tại $\mathcal{B}$ là một kẻ tấn công PrA sao cho:*

$$\text{Adv}^{\text{cr}}_{H}(\mathcal{A}) \leq \text{Adv}^{\text{pra}}_{H,P,\mathcal{E}}(\mathcal{B}).$$

Trong đó, $\mathcal{B}$ chạy với thời gian của $\mathcal{A}$ cộng với $\mathcal{O}(q_p) + \text{Time}(H)$, sử dụng tối đa q_p truy vấn nguyên thủy, và một truy vấn trích xuất.

Định lý 2 (WPrA+CR⇒PrA) (Lemma 3.4, [1]). *Xét P là một nguyên thủy lý tưởng và $H^P : Dom \to Rng$ là một hàm băm. Xét $\mathcal{E}^+$ là một bộ trích xuất đa điểm trung thực bất kỳ. Khi đó, tồn tại một bộ trích xuất $\mathcal{E}$ sao cho với mọi kẻ tấn công $\mathcal{A}$ phá tính PrA thực hiện q_e truy vấn trích xuất đều tồn tại kẻ tấn công $\mathcal{B}$ phá tính WPrA và kẻ tấn công $\mathcal{C}$ phá tính CR thỏa mãn:*

$$\text{Adv}^{\text{pra}}_{H,P,\mathcal{E}}(\mathcal{A}) \leq \text{Adv}^{\text{wpra}}_{H,P,\mathcal{E}^+}(\mathcal{B}) + \text{Adv}^{\text{cr}}_{H,P}(\mathcal{C}).$$

Trong đó, $\mathcal{B}$ thực hiện số truy vấn giống $\mathcal{A}$ và có thời gian chạy bằng thời gian chạy của $\mathcal{A}$ cộng với $\mathcal{O}(q_e)$. Kẻ tấn công $\mathcal{C}$ thực hiện q_p truy vấn và có thời gian chạy là $t + q_e Time(\mathcal{E}^+)$. Bộ trích xuất $\mathcal{E}$ có thời gian chạy giống $\mathcal{E}^+$.

Định lý 3 (Theorem 3.2, [1]) (RO⇒PrA). *Cố định $Dom \subseteq \{0,1\}^*$ và $n > 0$, xét $P = RF_{Dom,n}$. Khi đó hàm băm $H^P(x) = P(x)$ là PrA. Cụ thể, tồn tại một bộ trích xuất $\mathcal{E}$ sao cho với mọi kẻ tấn công $\mathcal{A}$ thực hiện tối đa q_p truy vấn tới P và q_e truy vấn trích xuất ta có:*

$$\text{Adv}^{\text{pra}}_{H,P,\mathcal{E},\Pi}(\mathcal{A}) \leq \frac{q_p q_e}{2^n} + \frac{q_p^2}{2^n}.$$

Chú ý rằng, bộ trích xuất $\mathcal{E}$ trong Định lý 3 được xác định như sau: Giả sử kẻ tấn công thực hiện các truy vấn nguyên thủy x_i và nhận được câu trả lời tương ứng là y_i.

Thuật toán $\mathcal{E}(z_j, \alpha)$:

Gán $\alpha \leftarrow (x_1, y_1), \dots, (x_k, y_k)$ với k là chỉ số cao nhất của truy vấn nguyên thủy trước thời điểm truy vấn z_j lên bộ trích xuất.

For $i = 1$ to k

If $y_i = z_j$ then $\mathcal{X} \leftarrow x_i$

If $\mathcal{X} = \emptyset$ then return $\perp$

else return phần tử đầu tiên của $\mathcal{X}$.

IV. Một số mối liên hệ mới liên quan đến tính PrA

Trong phần này, chúng tôi sẽ đưa ra một số mối quan hệ mới giữa tính PrA và các tính chất mật mã liên quan.

A. Liên hệ giữa tính PrA và CR

Mệnh đề 1 (CR⇏PrA). *Tồn tại một hàm CR nhưng không phải là PrA.*

Chứng minh. Xét hàm $H^P: \{0,1\}^{2n} \to \{0,1\}^n$ là một hàm CR, Pre (preimage resistance – tính kháng tiền ảnh) và kháng không điểm (không tồn tại một kẻ tấn công nào có thể tìm được x sao cho $H^P(x) = 0$ với xác suất đáng kể). Xét hàm $H_1^P: \{0,1\}^{2n} \to \{0,1\}^n$ được xác định như sau: $H_1^P(0) = 0$ với xác suất là $1/2$, $H_1^P(x) = H^P(x)$ với $x \neq 0$. Khi đó, ta sẽ chứng minh H_1^P là một hàm CR nhưng không phải là PrA. Trước hết ta xem xét xác suất sau: $\Pr[H_1^P(x) = H_1^P(y)]$, với $x \neq y$. Nếu $x, y \neq 0$ thì $\Pr[H_1^P(x) = H_1^P(y)] = \Pr[H^P(x) = H^P(y)]$. Nếu $x = 0$ hoặc $y = 0$, giả sử $y = 0$ xác suất để $H_1^P(x) = H_1^P(0)$ chính là xác suất tìm không điểm hoặc tìm tiền ảnh. Tuy nhiên, hàm H^P là CR, Pre và kháng không điểm nên xác suất xảy ra hai trường hợp trên là rất nhỏ. Do đó, hàm H_1^P là CR.

Mặt khác, H_1^P không phải PrA. Thật vậy, kẻ tấn công chỉ cần thực hiện truy vấn $z = 0$ lên bộ trích xuất và không cần thực hiện bất kỳ truy vấn nguyên thủy nào. Khi đó, bộ trích xuất sẽ trả về $\perp$ vì chuỗi $\alpha = \emptyset$. Khi đó anh ta đưa ra $x = 0$ là tiền ảnh của $z = 0$. ■

B. Liên hệ giữa tính PrA và WPrA

Mệnh đề 2 (PrA⇒WPrA). *Một hàm PrA thì sẽ thỏa mãn tính WPrA.*

Chứng minh. Giả sử H^P là một hàm thỏa mãn tính PrA với bộ trích xuất $\mathcal{E}$. Ta xét bộ trích xuất đa điểm chính là $\mathcal{E}$. Khi đó hàm H^P cũng sẽ là một hàm WPrA. ■

Mệnh đề 3 (WPrA⇏PrA). *Tồn tại một hàm WPrA nhưng không phải là PrA.*

Chứng minh. Xét

$$H^P: \{0,1\}^{2n} \to \{0,1\}^n$$

là một hàm PrA. Xét

$$H_1^P: \{0,1\}^{2n+1} \to \{0,1\}^{n+1}$$

$$x \| a \mapsto H^P(x) \| 1$$

với $a \in \{0,1\}$.

Sau đây ta sẽ chứng minh H_1^P là hàm WPrA nhưng không phải là PrA.

Do H^P là một hàm PrA, suy ra tồn tại một bộ trích xuất hiệu quả $\mathcal{E}$. Khi đó, xét bộ trích xuất đa điểm $\mathcal{E}^+$ của hàm H_1^P như sau: với giá trị cam kết $z = z_1 \| c$ lên $\mathcal{E}^+$ ($c \in \{0,1\}$) và chuỗi tư vấn α, bộ trích xuất $\mathcal{E}^+$ như sau: nếu $c = 0$ thì $\mathcal{E}^+(z, \alpha)$ trả về $\perp$; nếu $c = 1$ thì $\mathcal{E}^+$ chạy $\mathcal{E}(z_1, \alpha)$ thu được $\perp$ hoặc x, sau đó $\mathcal{E}^+$ trả về $\perp$ hoặc $x \| 0$ và $x \| 1$, tương ứng. Tiếp theo, ta sẽ chứng minh rằng H_1^P là WPrA. Gọi $\mathcal{A}$ là kẻ tấn công bất kỳ lên tính WPrA của H_1^P. Xét $\mathcal{B}$ là kẻ tấn công lên tính PrA của H^P mà sử dụng $\mathcal{A}$ như một chương trình con như sau: nếu $\mathcal{A}$ truy vấn nguyên thủy thì $\mathcal{B}$ cũng thực hiện truy vấn nguyên thủy và trả về cho $\mathcal{A}$. Nếu $\mathcal{A}$ thực hiện truy vấn trích xuất thì $\mathcal{B}$ sử dụng $\mathcal{E}$ để xây dựng $\mathcal{E}^+$ như được mô tả ở trên. Giả sử sau khi tương tác với P và bộ trích xuất, $\mathcal{A}$ đưa ra tiền ảnh $x^* = x_1^* \| a$ (với $a \in \{0,1\}$) cho giá trị cam kết z^* thỏa mãn $x^* \neq \mathcal{E}^+(z^*, \alpha)$. Khi đó, $z^* = z_1^* \| 1$ và z_1^* đã được truy vấn lên $\mathcal{E}$ (theo cách xây dựng của $\mathcal{E}^+$). Do đó, $\mathcal{B}$ đưa ra x_1^* là tiền ảnh của z_1^* và $x_1^* \neq \mathcal{E}(z_1^*, \alpha)$ do $x^* \neq \mathcal{E}^+(z^*, \alpha)$. Tuy nhiên, H^P là một hàm PrA. Suy ra điều này là mâu thuẫn. Vì vậy H_1^P là WPrA.

Ngoài ra, $H_1^P(x\|0) = H_1^P(x\|1)$ nên H_1^P không thỏa mãn tính CR. Do đó H_1^P không đạt tính PrA. ■

C. Liên hệ giữa tính PrA, BPrA với tính RO và PrO

Mệnh đề 4 (PrA⇏RO). *Tồn tại một hàm là PrA nhưng không phải là RO.*

Chứng minh. Xét hàm $H^P:\{0,1\}^{2n}\to\{0,1\}^n$ là PrA và kháng không điểm. Xét hàm H_1^P được xác định như sau: $H_1^P(0)=0$, $H_1^P(x)=H^P(x)$ với $x\neq 0$. Khi đó H_1^P là PrA nhưng không phải là RO.

Trước hết ta chứng minh H_1^P là PrA. Do H^P là PrA suy ra tồn tại một bộ trích xuất hiệu quả $\mathcal{E}$. Ta xét $\mathcal{E}'$ là bộ trích xuất của H_1^P như sau: $\mathcal{E}'(0,\alpha)=0$, $\mathcal{E}'(z,\alpha)=\mathcal{E}(z,\alpha)$ với $z\neq 0$. Giả sử kẻ tấn công $\mathcal{A}$ đưa ra (x^*,z^*) thỏa mãn $H_1^P(x^*)=z^*$ và $x^*\neq\mathcal{E}'(z^*,\alpha)$ với xác suất đáng kể. Nếu $z^*=0$ thì $x^*\neq 0$, tức là kẻ tấn công phải tìm $x^*\neq 0$ sao cho $H^P(x)=0$ với xác suất đáng kể. Mâu thuẫn với giả thiết kháng không điểm. Nếu $z^*\neq 0$, thì $x^*\neq 0$ vì nếu $x^*=0$ thì $z^*=H_1^P(x^*)=0$. Mặt khác, do $H_1^P(x^*)=z^*$ và $x^*\neq\mathcal{E}'(z^*,\alpha)$ nên ta có $H^P(x^*)=z^*$ (do $H^P(x^*)=H_1^P(x^*)$) và $x^*\neq\mathcal{E}(z^*,\alpha)$ (do cách xây dựng của $\mathcal{E}'$). Khi đó, ta có thể xây dựng một kẻ tấn công $\mathcal{B}$ lên tính PrA của H^P mà đưa ra (x^*,z^*) sao cho $H^P(x^*)=z^*$ và $x^*\neq\mathcal{E}(z^*,\alpha)$ với xác suất đáng kể. Mâu thuẫn với giả thiết H^P là PrA. Vì vậy H_1^P là PrA.

Tiếp theo ta chứng minh H_1^P không phải là RO. Điều này được suy ra từ định nghĩa của H_1^P. ■

Mệnh đề 5 (RO⇒BPrA). *Cố định $Dom\subseteq\{0,1\}^*$ và $n>0$, xét $P=RF_{Dom,n}$. Khi đó hàm băm $H^P(x)=P(x)$ là BPrA. Cụ thể, tồn tại một bộ trích xuất $\mathcal{E}$ sao cho với mọi kẻ tấn công $\mathcal{A}$ thực hiện tối đa q_e truy vấn tới P và q_e truy vấn trích xuất ta có:*

$$\mathrm{Adv}^{\mathrm{bpra}}_{H,P,\mathcal{E},\Pi}(\mathcal{A})\leq\frac{q_pq_e}{2^n}+\frac{q_p^2}{2^n}.$$

Chứng minh. Từ Định lý 3 ta có H^P là một hàm PrA với bộ trích xuất $\mathcal{E}$ được định nghĩa như sau Định lý 3. Bây giờ ta chỉ cần chứng minh rằng, với mọi kẻ tấn công $\mathcal{A}$ chạy trong thời gian t và đưa ra một danh sách P-truy vấn α thì xác suất để $|\{z:\mathcal{E}(z,\alpha)\neq\perp\}|>|\alpha|$ không vượt quá $t^2/2^n$. Thật vậy, giả sử các P-truy vấn là $(x_1,y_1),\dots,(x_{q_e},y_{q_e})$. Khi đó, các giá trị cam kết z mà thỏa mãn điều kiện $\mathcal{E}(z,\alpha)\neq\perp$ thì $z=y_i$ với $i\in\{1,\dots,q_e\}$ nào đó. Do đó, $|\{z:\mathcal{E}(z,\alpha)\neq\perp\}|\leq q_e=|\alpha|$, hay xác suất để $|\{z:\mathcal{E}(z,\alpha)\neq\perp\}|>|\alpha|$ bằng 0. ■

Mệnh đề 6 (PrO⇒PrA). *Xét hàm băm $H^P:\{0,1\}^*\to\{0,1\}^n$ được xây dựng dựa trên nguyên thủy lý tưởng P thỏa mãn tính chất PrO. Khi đó, H^P là một hàm PrA. Hơn nữa tồn tại bộ trích xuất hiệu quả $\mathcal{E}$ sao cho với mọi $\mathcal{A}$ là một kẻ tấn công phá tính PrA của H^P thực hiện tối đa q_p truy vấn nguyên thủy và tối đa q_e truy vấn trích xuất thì luôn tồn tại một kẻ tấn công $\mathcal{B}$ phá vỡ tính PrO của H^P thực hiện cùng số truy vấn nguyên thủy, truy vấn trích xuất với $\mathcal{A}$ và 1 truy vấn cấu trúc thỏa mãn:*

$$\mathrm{Adv}^{\mathrm{pra}}_{H^P,P,\mathcal{E}}(\mathcal{A})\leq\mathrm{Adv}^{\mathrm{pro}}_{H^P,P}(\mathcal{B})+\frac{1}{2^n}.$$

Chứng minh. Trước khi chứng minh mệnh đề này ta cần bổ đề sau.

Bổ đề 1 (PrO⇒CR). *Một hàm băm $H^P:\{0,1\}^*\to\{0,1\}^n$ được xây dựng dựa trên nguyên thủy lý tưởng P đạt tính PrO thì sẽ thỏa mãn tính CR. Hơn nữa với mọi $\mathcal{A}$ là một kẻ tấn công tìm kiếm va chạm của H^P thực hiện tối đa q truy vấn thì luôn tồn tại một kẻ tấn công phá vỡ tính PrO của H^P thực hiện cùng số truy vấn nguyên thủy và 1 truy vấn cấu trúc sao cho:*

$$\mathrm{Adv}^{\mathrm{cr}}_{H^P,P}(\mathcal{A})\leq\mathrm{Adv}^{\mathrm{pro}}_{H^P,P}(\mathcal{B})+\frac{1}{2^n}.$$

Chứng minh (Bổ đề 1). Xét $\mathcal{A}$ là một kẻ tấn công bất kỳ lên tính CR của H^P. Giả sử $\mathcal{A}$ tìm được một va chạm của H^P bằng cách truy vấn lên nguyên thủy P, tức là $\mathcal{A}$ tìm được x và x' sao cho $H^P(x)=H^P(x')=z$. Ta xây dựng $\mathcal{B}$ là một kẻ tấn công lên tính PrO của hàm H^P mà sử dụng $\mathcal{A}$ như một chương trình con như sau:

- $\mathcal{B}$ chạy $\mathcal{A}$. Nếu $\mathcal{A}$ thực hiện các truy vấn nguyên thủy thì $\mathcal{B}$ cũng thực hiện các truy vấn của mình lên bộ tiên tri của anh ta.
- $\mathcal{A}$ đưa ra x và x'. $\mathcal{B}$ thực hiện các truy vấn cấu trúc là x và x'. Nếu kết quả thu được là giống nhau thì $\mathcal{B}$ đưa ra 1, ngược lại đưa ra 0.

Đối với trường hợp $\mathcal{B}$ được sử dụng bộ tiên tri là (H^P,P) thì ta xác định được:

$$\Pr\left[\mathcal{B}^{H^P,P}=1\right]=\mathrm{Adv}^{\mathrm{cr}}_{H^P,P}(\mathcal{A}).$$

Đối với trường hợp $\mathcal{B}$ được sử dụng bộ tiên tri là (Ω, S^{Ω}) thì ta xác định được:

$$\Pr\left[\mathcal{B}^{\Omega,S^{\Omega}} = 1\right] = \Pr[\mathcal{A} \text{ tìm được va chạm của } \Omega\,].$$

Điều này có nghĩa rằng kẻ tấn công khi sử dụng các truy vấn lên S^{Ω} có thể tìm được x và x' sao cho $\Omega(x) = \Omega(x')$. Tuy nhiên, xét về mặt bản chất Ω là một bộ tiên tri ngẫu nhiên nên xác suất để $\Omega(x) = \Omega(x')$ là rất nhỏ, chỉ bằng $1/2^n$. ■

Quay trở lại chứng minh Mệnh đề 6.

Với mọi đầu vào x, ta định nghĩa α_x là tập các P-truy vấn cần thiết để H^P tính x. Với mọi α là tập các P-truy vấn, ta định nghĩa H^{α} là một hàm giống như H^P, nhưng thay vì thực hiện các P-truy vấn thì câu trả lời được suy ra từ α. Khi đó, H^{α} chỉ được định nghĩa cho x mà $\alpha_x \subseteq \alpha$. Ta ký hiệu D_{α} là tập những x như vậy, nó được gọi là tập xác định của H^{α}. Tập giá trị R_{α} được định nghĩa là $H^{\alpha}(D_{\alpha})$. Ta xây dựng bộ trích xuất $\mathcal{E}$ với đầu vào là truy vấn trích xuất là z_j:

Thuật toán $\mathcal{E}(z_j, \alpha)$:

Gán $\alpha \leftarrow (x_1, y_1), \ldots, (x_k, y_k)$ với k là chỉ số cao nhất của P-truy vấn trước thời điểm truy vấn z_j lên bộ trích xuất.

If $z_j \in R_{\alpha}$ then $\mathcal{X} \leftarrow \{x | H^{\alpha}(x) = z_j\}$
else $\mathcal{X} \leftarrow \emptyset$
If $\mathcal{X} = \emptyset$ then retutn $\perp$
else return phần tử đầu tiên của $\mathcal{X}$.

Tiếp theo, ta sẽ xác định lợi thế thành công của một kẻ tấn công $\mathcal{A}$ trong việc phá vỡ tính PrA của hàm băm H^P qua giả thiết H^P là một hàm PrO. Tức là, với bộ trích xuất hiệu quả $\mathcal{E}$, ta sẽ tính xác suất để $\mathcal{A}$ tìm được $z = H^P(x)$ mà $x \notin \mathcal{E}(z, \alpha)$.

Phương pháp: từ kẻ tấn công $\mathcal{A}$ lên tính PrA bất kỳ, ta sẽ xây dựng được một kẻ tấn công $\mathcal{B}$ lên tính PrO mà sử dụng $\mathcal{A}$ như một chương trình con. Do $\mathcal{A}$ có quyền truy vấn lên bộ trích xuất $\mathcal{E}$, nên $\mathcal{B}$ cũng phải có quyền truy vấn bộ trích xuất để tạo môi trường tấn công cho $\mathcal{A}$. Khi $\mathcal{B}$ được tương tác với các bộ tiên tri (H^P, P) thì bộ trích xuất mà $\mathcal{B}$ truy vấn vào chính là $\mathcal{E}$. Khi $\mathcal{B}$ được tương tác với các bộ tiên tri (Ω, S^{Ω}) thì ta cần xây dựng một bộ trích xuất tương ứng cho trường hợp này. Ta ký hiệu bộ trích xuất này là $\mathcal{E}^{\Omega}$. Cách xây dựng của $\mathcal{E}^{\Omega}$ tương tự như $\mathcal{E}$. Trước hết ta cần một số ký hiệu sau:

- Với mọi đầu vào x, ta định nghĩa α_x^{Ω} là tập các truy vấn lên S^{Ω} cần thiết để đưa ra kết quả giống với $\Omega(x)$.
- Với mọi α là tập các truy vấn nguyên thủy, ta định nghĩa Ω^{α} là một bộ tiên tri giống như Ω, nhưng thay vì thực hiện các truy vấn thì câu trả lời được suy ra từ α.
- Khi đó, Ω^{α} chỉ được định nghĩa cho x mà $\alpha_x^{\Omega} \subseteq \alpha$. Ta ký hiệu D_{α}^{Ω} là tập những x như vậy, nó được gọi là tập xác định của Ω^{α}. Tập giá trị R_{α}^{Ω} được định nghĩa là $\Omega^{\alpha}(D_{\alpha}^{\Omega})$. Ta xây dựng bộ trích xuất $\mathcal{E}^{\Omega}$ với đầu vào là truy vấn trích xuất là z_j.

Thuật toán $\mathcal{E}^{\Omega}(z_j, \alpha)$:

Gán $\alpha \leftarrow (x_1, y_1), \ldots, (x_k, y_k)$ với k là chỉ số cao nhất của truy vấn nguyên thủy trước thời điểm truy vấn z_j lên bộ trích xuất.

If $z_j \in R_{\alpha}^{\Omega}$ then $\mathcal{X} \leftarrow \{x | \Omega^{\alpha}(x) = z\}$
else $\mathcal{X} \leftarrow \emptyset$
If $\mathcal{X} = \emptyset$ then return $\perp$
else return phần tử đầu tiên của $\mathcal{X}$.

Chú ý rằng, do H^P là một hàm PrO nên khi kết quả của phép truy vấn $\Omega(x)$ cũng bằng với việc lần lượt thực hiện các truy vấn nguyên thủy đến S^{Ω}. Do đó, bộ trích xuất $\mathcal{E}^{\Omega}$ cũng chỉ có tác dụng như $\mathcal{E}$ là trả lại tiền ảnh của giá trị cam kết mà giá trị này đã được tính trước đó. Vì vậy, nó không làm ảnh hưởng đến lợi thế phân biệt PrO.

Quay lại việc xây dựng một kẻ tấn công $\mathcal{B}$ (có quyền truy vấn lên bộ trích xuất $\mathcal{E}$ hoặc $\mathcal{E}^{\Omega}$ tùy thuộc vào các bộ tiên tri mà anh ta đang tương tác vào) lên tính PrO mà sử dụng $\mathcal{A}$ như một chương trình con như sau:

- $\mathcal{B}$ chạy $\mathcal{A}$. Nếu $\mathcal{A}$ thực hiện các truy vấn nguyên thủy thì $\mathcal{B}_2$ cũng thực hiện các truy vấn này lên bộ tiên tri của anh ta đồng thời lưu lại các cặp (truy vấn, câu trả lời) tạo thành chuỗi α. Nếu $\mathcal{A}$ thực hiện truy vấn trích xuất thì $\mathcal{B}$ dùng chuỗi α để truy vấn cùng lên bộ trích xuất ($\mathcal{E}$ hoặc $\mathcal{E}^{\Omega}$) để trả về cho $\mathcal{A}$.
- $\mathcal{A}$ đưa ra tiền ảnh x cho giá trị z. Kẻ tấn công truy vấn x lên H^P hoặc Ω, nếu giá trị trả về bằng z thì đưa ra 1, ngược lại thì đưa ra 0.

Tiếp theo, ta quay về đánh giá xác suất để $\mathcal{A}$ tìm được $z = H^P(x)$ mà $x \notin \mathcal{E}(z, \alpha)$ thông qua lợi thế của $\mathcal{B}$ tấn công lên tính PrO. Ta gọi bộ tiên tri trích xuất mà $\mathcal{A}$ được tương tác là $\mathcal{E}^*$ (có thể là $\mathcal{E}$ hoặc $\mathcal{E}^{\Omega}$), ký hiệu R_α^* là R_α hoặc R_α^{Ω} tương ứng khi với bộ tiên tri trích xuất $\mathcal{A}$ tương tác. Ta xét hai trường hợp sau:

(i) $z \in R_\alpha^*$, hay là $\mathcal{E}^*(z, \alpha) = x'$ với x' là một giá trị đầu vào nào đó. Điều này có nghĩa là kẻ tấn công $\mathcal{A}$ tìm được một va chạm của hàm băm H^P hoặc Ω. Tuy nhiên, theo Bổ đề 1 ta có:

$$\mathrm{Adv}^{\mathrm{pra}}_{H^P,P,\mathcal{E}}(\mathcal{A}) = \mathrm{Adv}^{\mathrm{cr}}_{H^P,P}(\mathcal{A}) \leq \mathrm{Adv}^{\mathrm{pro}}_{H^P,P}(\mathcal{B}) + \frac{1}{2^n}.$$

(ii) $z \notin R_\alpha^*$, hay là $\mathcal{E}^*(z, \alpha) = \perp$. Điều này có nghĩa là $\mathcal{E}$ không thể dùng thông tin trong chuỗi tư vấn α để suy ra được tiền ảnh của z. Mặt khác, kẻ tấn công $\mathcal{A}$ vẫn đưa ra được x sao cho $H^P(x) = z$.

Nhận thấy rằng trong trường hợp $\mathcal{B}$ được truy vấn lên P và H^P thì khi đó:

$$\Pr\left[\mathcal{B}^{H^P,P} = 1\right] = \mathrm{Adv}^{\mathrm{pra}}_{H^P,P,\mathcal{E}}(\mathcal{A}).$$

Trong trường hợp $\mathcal{B}$ được truy vấn lên bộ tiên tri ngẫu nhiên Ω và bộ mô phỏng S, thì:

$$\Pr\left[\mathcal{B}^{\Omega,S^{\Omega}} = 1\right] = \Pr[\mathcal{A} \text{ tìm được tiền ảnh của } \Omega].$$

Tiếp theo, ta sẽ đánh giá xác suất để $\Omega(x) = z$. Chú ý rằng, $\mathcal{B}$ đưa ra x khi $\mathcal{A}$ đưa ra x. Nếu $\Omega(x) = z$ thì có nghĩa rằng $\mathcal{A}$ chỉ dựa trên các truy vấn lên S mà đưa ra được x sao cho $\Omega(x) = z$. Bộ mô phỏng S lại có quyền gọi lên bộ tiên tri Ω. Mặt khác, theo giả thiết ở trên, từ chuỗi α gồm các truy vấn và câu trả lời trước đó $\mathcal{B}$ (sử dụng bộ trích xuất $\mathcal{E}$) không thể tính được x. Vì vậy, S không thể truy vấn x lên bộ tiên tri Ω được. Do đó, giá trị x chưa được tính bởi bộ tiên tri Ω trước đó. Do đó, xác suất để $\Omega(x) = z$ là nhỏ, chỉ bằng $1/2^n$. Vì vậy, trong trường hợp này ta có:

$$\mathrm{Adv}^{\mathrm{pra}}_{H^P,P,\mathcal{E}}(\mathcal{A}) \leq \mathrm{Adv}^{\mathrm{pro}}_{H^P,P}(\mathcal{B}) + \frac{1}{2^n}.$$

Từ hai trường hợp trên, chúng ta có điều phải chứng minh. ■

Nhận xét 1. Một hàm PrA thì không nhất thiết có tích PrO. Thật vậy, theo Dodis và các cộng sự (Theorem 4.2, [1]) cấu trúc SMD (strengthened Merkle-Damgård) là bảo toàn tính PrA. Tuy nhiên, trong [3] (trang 9) Coron đã chứng minh rằng SMD lại không thỏa mãn tính PrO ngay cả khi hàm nén của nó là RO.

Nhận xét 2. Theo định nghĩa của BPrA, ngoài tính PrA ta cần thêm các điều kiện khác. Do đó, nếu một hàm PrA mà không thỏa mãn các điều kiện này thì hàm đó mang tính BPrA. Tuy nhiên, nhóm tác giả vẫn chưa tìm được ví dụ cho điều này.

Nhận xét 3. Hiện tại, nhóm tác giả vẫn chưa thể tìm hiểu được mối liên hệ giữa PrO và BPrA bởi vì cần phải có bộ trích xuất cụ thể để đánh giá.

KẾT LUẬN

Trong bài báo này, nhóm tác giả đã khảo sát một số mối quan hệ giữa các tính chất liên quan đến tính PrA của hàm băm. Trên cơ sở trình bày chi tiết cho một số tính chất đã được đề cập trong các tài liệu đã có, nhóm tác giả phát biểu và chứng minh cho Mệnh đề 1 về sự tồn tại của một hàm CR nhưng không có tính PrA; Mệnh đề 2 khẳng định rằng một hàm PrA thì có tính WPrA; Mệnh đề 3 về sự tồn tại một hàm WPrA nhưng không có tính PrA; Mệnh đề 4 về sự tồn tại một hàm là PrA nhưng không có tính RO; Mệnh đề 5 khẳng định một hàm có tính RO thì có tính BPrA; Bổ đề 1 khẳng định PrO suy ra CR và Mệnh đề 6 khẳng định một hàm PrO thì có tính PrA.

Qua bài báo này, chúng ta nhận thấy rằng họ hàm băm có cấu trúc Sponge (là PrO [7]) cùng với họ hàm băm $\mathcal{GOST}$ (là PrA [8]) sẽ phù hợp với lược đồ chữ ký ít phụ thuộc khóa. Trong khi lược đồ chữ ký BLT sẽ an toàn khi sử dụng hàm băm có cấu trúc Sponge.

Bên cạnh đó, bài báo này vẫn còn một số vấn đề tồn tại như chưa tìm được ví dụ về một hàm PrA nhưng không thỏa mãn BPrA, chưa tìm được mối liên hệ giữa BPrA với PrO. Vì vậy, hướng nghiên cứu tiếp theo của nhóm là giải quyết trọn vẹn vấn đề trên.

TÀI LIỆU THAM KHẢO

[1] Dodis, Y., T. Ristenpart, and T. Shrimpton. Salvaging Merkle-Damgård for practical applications. in Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2009. Springer.

[2] Maurer, U., R. Renner, and C. Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. in Theory of cryptography conference. 2004. Springer.

[3] Coron, J.-S., et al. Merkle-Damgård revisited: How to construct a hash function. in Annual International Cryptology Conference. 2005. Springer.

[4] Buldas, A. and R. Laanoja. Security proofs for hash tree time-stamping using hash functions with small output size. in Australasian Conference on Information Security and Privacy. 2013. Springer.

[5] Buldas, A., et al. Bounded pre-image awareness and the security of hash-tree keyless signatures. in International Conference on Provable Security. 2014. Springer.

[6] Buldas, A., R. Laanoja, and A. Truu, Security Proofs for the BLT Signature Scheme. IACR Cryptol. ePrint Arch., 2014. 2014: p. 696.

[7] Guido, B., et al., Cryptographic sponge functions. 2011.

[8] Седов, Г.К., Стойкость ГОСТ Р 34.11-2012 к атаке поиска прообраза и к атаке поиска коллизий. Математические вопросы криптографии, 2015. 6(2): p. 79-98.

[9] Trần Hồng Thái, Hoàng Đình Linh, "Một cải tiến cận an toàn kháng va chạm cho lược đồ Hirose trong mô hình mã pháp lý tưởng", Journal of Science and Technology on Information security, ISSN 2615-9570, Vol. 09, No. 01, 2019, pp. 29-36.

SƠ LƯỢC VỀ TÁC GIẢ

Nguyễn Tuấn Anh

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

Email: tuananhnghixuan@gmail.com

Quá trình đạo tạo: Tốt nghiệp Đại học Khoa học tự nhiên - Đại học Quốc gia Hà Nội, hệ Chính quy, chương trình Toán tài năng, chuyên ngành Toán học năm 2016.

Hướng nghiên cứu hiện nay: Nghiên cứu về độ an toàn chứng minh được của các lược đồ chữ ký số và các giao thức trao đổi khóa.

Triệu Quang Phong

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

Email: phongtrieu53@gmail.com

Quá trình đạo tạo: Tốt nghiệp Đại học Khoa học tự nhiên - Đại học Quốc gia Hà Nội, hệ Chính quy, chương trình Toán tài năng, chuyên ngành Toán học năm 2014.

Hướng nghiên cứu hiện nay: Nghiên cứu về độ an toàn chứng minh được của các lược đồ chữ ký số và các giao thức trao đổi khóa.