Xây dựng lược đồ chữ ký số an toàn từ các lược đồ định danh

Võ Tùng Linh

***Tóm tắt*— Trong tài liệu [3], khi trình bày về phương pháp xây dựng lược đồ chữ ký số dựa trên các lược đồ định danh chính tắc nhờ phép biến đổi Fiat-Shamir, tác giả đã chỉ ra "điều kiện đủ" để nhận được một lược đồ chữ ký số an toàn dưới tấn công sử dụng thông điệp được lựa chọn thích nghi là lược đồ định danh chính tắc phải an toàn dưới tấn công bị động. Tuy nhiên, tác giả của [3] chưa chỉ ra "điều kiện cần" đối với các lược đồ định danh chính tắc nhằm đảm bảo tính an toàn cho lược đồ chữ ký số được xây dựng. Do đó, trong bài báo này, chúng tôi hoàn thiện kết quả của [3] bằng việc chỉ ra điều kiện đủ đó cũng chính là điều kiện cần.**

***Abstract*— In [3], the author shows that, in order to the digital signature scheme Π' resulting from the Fiat-Shamir transform applied to a canonical identification scheme Π is existentially unforgeable under chosen-message attack then a "sufficient" condition is that the scheme Π has to be secure against a passive attack. However, the author of [3] has not shown the "necessary" conditions for the canonical identification schemes to ensure security of the digital signature scheme Π'. In this paper, we complete this result by showing that sufficient condition is also necessary.**

***Từ khóa:* Lược đồ định danh; lược đồ chữ ký số; phép biến đổi Fiat-Shamir.**

***Keywords*: Identification scheme; signature scheme; Fiat-Shamir transform.**

I. GIỚI THIỆU

Một phương pháp hiệu quả để xây dựng các lược đồ chữ ký số an toàn là sử dụng kỹ thuật biến đổi từ một lược đồ định danh có tính chất mật mã tốt. Phương pháp được giới thiệu lần đầu bởi Amos Fiat và Adi Shamir trong [2] nên phép biến đổi được gọi là Phép biến đổi Fiat-Shamir, và dần trở thành một phương pháp phổ biến, một trong những công cụ để nhận được các lược đồ chữ ký số an toàn. Ý tưởng chính đằng sau phép biến đổi Fiat-Shamir là người ta chứng minh trong một lược đồ định danh chạy chính lược đồ đó để sinh một giá trị thách thức bằng cách áp dụng một hàm băm lên thông điệp đầu tiên, sau đó tính một giá trị phúc đáp thích hợp. Nếu hàm băm được mô hình hóa như một bộ tiên tri ngẫu nhiên thì thách thức được sinh bởi hàm băm đó là "ngẫu nhiên thực sự", do đó sẽ khiến kẻ tấn công (không biết các giá trị bí mật) khó khăn trong việc tìm kiếm một bản ghi chấp nhận được khi muốn mạo danh người chứng minh trong một lần thực thi trung thực lược đồ. Bằng việc đưa cả thông điệp vào trong đầu vào hàm băm, một bản ghi chấp nhận được sẽ góp phần tạo nên chữ ký trên thông điệp. Ta sẽ cụ thể hóa ý tưởng này trong các phần sau.

Với việc xây dựng lược đồ chữ ký số từ lược đồ định danh sử dụng phép biến đổi Fiat-Shamir, câu hỏi đặt ra là: "Lược đồ định danh cần thỏa mãn những điều kiện (tối thiểu) nào để đảm bảo tính an toàn cho lược đồ chữ ký số được xây dựng". Trong bài báo này, theo các kết quả nghiên cứu chính từ các tài liệu [1, 3] chúng tôi sẽ chỉ ra một cách chi tiết về các điều kiện cần thiết đối với lược đồ định danh sao cho đảm bảo được tính an toàn của lược đồ chữ ký số xây dựng lên từ nó chống lại các tấn công lựa chọn thông điệp.

Đóng góp của nhóm tác giả: Trong tài liệu [3], tác giả đã chỉ ra rằng, để lược đồ chữ ký số Π' nhận được từ lược đồ định danh Π qua phép biến đổi Fiat-Shamir không thể bị giả mạo tồn tại dưới tấn công sử dụng thông điệp được lựa chọn thích nghi thì một "điều kiện đủ" là lược đồ Π phải an toàn dưới các tấn công bị động. Trong bài báo này, với Mệnh đề 1, chúng tôi hoàn thiện kết quả này bằng cách chỉ ra điều kiện đó cũng chính là một "điều kiện cần" để đảm bảo cho lược đồ chữ ký số Π' an toàn. Mặc dù kết luận tương tự đã được chỉ ra trong [1], tuy nhiên ở đây kỹ thuật chứng minh chúng tôi sử dụng là thống nhất với cách trình bày của tài liệu [3], khác với kỹ thuật sử dụng trong [1].

Bài báo được nhận ngày 1/12/2018. Bài báo được nhận xét bởi phản biện thứ nhất vào ngày 11/12/2018 và được chấp nhận đăng vào ngày 18/12/2018. Bài báo được nhận xét bởi phản biện thứ hai vào ngày 14/12/2018 và được chấp nhận đăng vào ngày 28/12/2018.

Bố cục của bài báo: Mục II chúng tôi trình bày định nghĩa các lược đồ định danh cùng với độ an toàn hình thức của chúng dưới các tấn công bị động. Mục III trình bày về phương pháp xây dựng lược đồ chữ ký số từ các lược đồ định danh chính tắc qua phép biến đổi Fiat-Shamir cùng với kết quả chính về điều kiện cần và đủ để lược đồ chữ ký số thu được là an toàn. Cuối cùng là Mục Kết luận.

II. ĐỊNH NGHĨA LƯỢC ĐỒ ĐỊNH DANH VÀ ĐỘ AN TOÀN

Trước khi định nghĩa lược đồ định danh là gì, ta xét một kịch bản mà trong đó người tham gia P (gọi là *người chứng minh*) muốn thuyết phục người tham gia khác, ký hiệu V (gọi là *người xác minh*), rằng anh ta chính là P như đã khẳng định. Cụ thể hơn, ta có thể thấy tình huống này nảy sinh trong các trường hợp chẳng hạn như *P* và V chưa bao giờ gặp nhau trước đó, hoặc P và V liên lạc qua một kênh truyền thông (nhưng không mặt-đối-mặt với nhau) và V muốn đảm bảo rằng mình đang liên lạc với P chứ không phải là một kẻ mạo danh nào đó. Để cho sự đảm bảo này có ý nghĩa thì rõ ràng phải có một số thông tin để phân biệt P với những người khác, nếu không thì bất kỳ ai cũng có thể giả mạo là P. Một giải pháp để P có thể thuyết phục những người xác minh tiềm năng là, P thiết lập một khóa công khai pk mà tất cả những người xác minh (tiềm năng) đều được biết, sau đó sử dụng một khóa bí mật tương ứng với khóa công khai này, P chạy một trường hợp cụ thể của lược đồ mà được gọi là *lược đồ định danh* để thuyết phục người xác minh V tin rằng mình chính là người mà được đại diện bởi khóa công khai pk.

Định nghĩa 1 ([3, Định nghĩa 8.1]). *Một* ***lược đồ định danh*** *bao gồm ba thuật toán thời gian đa thức, xác suất* $(\mathrm{Gen}, \mathrm{P}, \mathrm{V})$ *sao cho*

- ***Thuật toán sinh khóa*** *ngẫu nhiên Gen nhận đầu vào là tham số an toàn k và trả về một cặp khóa* $(\mathrm{pk}, \mathrm{sk})$*, trong đó* pk *được gọi là* ***khóa công khai*** *và* sk *được gọi là* ***khóa bí mật.***
- P *và* V *là các thuật toán tương tác với nhau.* ***Thuật toán chứng minh*** P *nhận đầu vào là khóa bí mật* sk *và* ***thuật toán xác minh*** V *nhận đầu vào là khóa công khai* pk*. Kết thúc quá trình tương tác,* V *đưa ra một bit b với* $b = 1$ *có nghĩa là "chấp nhận" và* $b = 0$ *có nghĩa là "bác bỏ".*

Các thuật toán $(\mathrm{Gen}, \mathrm{P}, \mathrm{V})$ *phải thỏa mãn yêu cầu là, với mọi k và với mọi đầu ra* $(\mathrm{pk}, \mathrm{sk})$ *của* $\mathrm{Gen}(1^k)$:

$$\Pr[\langle \mathrm{P}(\mathrm{sk}), \mathrm{V}(\mathrm{pk}) \rangle = 1] = 1.$$

Cặp thuật toán (P, V) *cùng với các hoạt động tương tác giữa chúng được gọi là* ***giao thức định danh****.*

Một lược đồ định danh được nói là *an toàn kháng lại các tấn công bị động* nếu kẻ tấn công sẽ khó có thể mạo danh được P kể cả khi nó có khả năng nghe trộm nhiều lần thực thi quá trình tương tác giữa P và một người xác minh trung thực V. Trước khi định nghĩa chính thức khái niệm an toàn này, chúng tôi giới thiệu một bộ tiên tri $\mathrm{Trans}_{\mathrm{sk},\mathrm{pk}}(\cdot)$ mà không cần đầu vào, sẽ trả về một bản ghi (tức là tất cả các thông điệp đã được gửi và nhận) của một lần thực thi trung thực $\langle \mathrm{P}(\mathrm{sk}), \mathrm{V}(\mathrm{pk}) \rangle$ của lược đồ định danh. Ta sẽ mô hình hóa mỗi nỗ lực nghe trộm của kẻ tấn công bằng một truy vấn đến bộ tiên tri này. Chú ý rằng nếu P, V được ngẫu nhiên hóa thì Trans cũng được ngẫu nhiên hóa và do vậy mỗi lần gọi sẽ trả về một bản ghi (có thể) khác so với những lần trước. Cũng cần lưu ý thêm rằng, ở đây ta giả thiết Trans sẽ *chỉ* trả về các thông điệp mà kẻ nghe trộm có thể thu thập được, hay cụ thể hơn, các trạng thái trong của các bên tham gia không được chứa trong thông tin trả về bởi Trans.

Định nghĩa 2 ([3, Định nghĩa 8.2]). *Một lược đồ định danh* $(\mathrm{Gen}, \mathrm{P}, \mathrm{V})$ *là* ***an toàn kháng lại các tấn công bị động****, hay còn gọi là* ***an toàn một cách bị động****, nếu xác suất dưới đây là không đáng kể với mọi kẻ tấn công PPT (thời gian đa thức, xác suất)* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$:

$$\Pr\left[\begin{matrix}(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}(1^k) \\ s \leftarrow \mathcal{A}_1^{\mathrm{Trans}_{\mathrm{sk},\mathrm{pk}}(\cdot)}(\mathrm{pk})\end{matrix} : \langle \mathcal{A}_2(s), \mathrm{V}(\mathrm{pk}) \rangle = 1\right].$$

Để hiểu rõ hơn Định nghĩa 2, ta hình dung kẻ tấn công trong định nghĩa trên thực hiện tấn công theo hai "giai đoạn": giai đoạn đầu tiên, kẻ tấn công nghe trộm nhiều lần thực thi lược đồ, tức là $\mathcal{A}_1$ được truy cập vào bộ tiên tri Trans, và đưa ra một thông tin trạng thái s nào đó; giai

đoạn thứ hai, kẻ tấn công sử dụng s để cố gắng mạo danh P.

Bây giờ ta đi xét trường hợp mà ở giai đoạn hai, kẻ tấn công - ký hiệu tương ứng là $\mathcal{A}_2$, được phép truy cập đến bộ tiên tri Trans ngay cả khi đang nỗ lực để mạo danh P (vậy nên, nếu lược đồ định danh là một giao thức 3-pha thì $\mathcal{A}_2$ có thể quyết định truy vấn tới bộ tiên tri Trans giữa pha thứ hai và pha thứ ba). Để chỉ ra độ an toàn trong trường hợp này cũng được suy ra từ độ an toàn trong Định nghĩa 2, ta giả sử $\mathcal{A}$ là một chiến lược tấn công mà việc truy vấn tới bộ tiên tri Trans được thực hiện cả trước và trong quá trình tương tác của kẻ tấn công với V (tức là ở đây không có sự phân chia quá trình tấn công thành hai giai đoạn phân biệt), và sẽ chỉ ra sự tồn tại một chiến lược tấn công $\mathcal{A}' = (\mathcal{A}'_1, \mathcal{A}'_2)$ mà đạt được thành công với cùng xác suất giống như $\mathcal{A}$ nhưng không truy vấn đến bộ tiên tri Trans trong suốt giai đoạn thứ hai của nó. Gọi $q = q(k)$ là biên trên (đa thức) của số lượng các truy vấn được thực hiện bởi $\mathcal{A}$ tới bộ tiên tri Trans. Khi đó ta cho $\mathcal{A}'$ hoạt động như sau: $\mathcal{A}'_1$ thực hiện q truy vấn tới Trans để nhận được một dãy các bản ghi $t_1, \dots, t_q$. Đầu ra của $\mathcal{A}'_1$ là $s = t_1, \dots, t_q$. Trong giai đoạn thứ hai, $\mathcal{A}'_2$ chỉ cần chạy $\mathcal{A}$ và chuyển tiếp các thông điệp đến/đi từ V; mỗi khi $\mathcal{A}$ thực hiện truy vấn thứ i của nó tới Trans thì truy vấn này được trả lời bởi $\mathcal{A}'_2$ với bản ghi t_i mà nó đã nhận được. Rõ ràng $\mathcal{A}'_2$ không thực hiện việc truy vấn tới Trans nhưng $\mathcal{A}'$ thành công trong việc giả mạo P với cùng xác suất như $\mathcal{A}$ đã thực hiện.

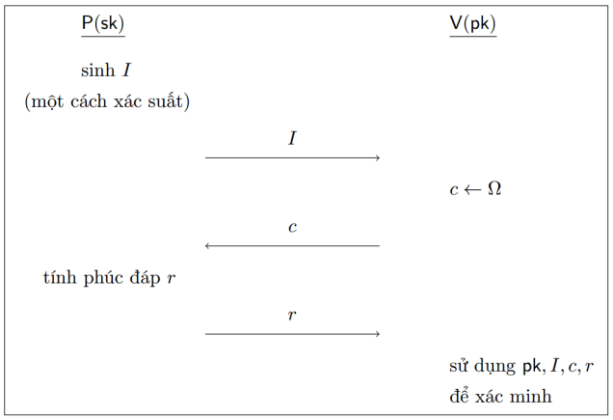
Cần chú ý thêm rằng độ an toàn bị động là một khái niệm an toàn khá yếu. Với định nghĩa độ an toàn này, lược đồ định danh không được bảo vệ kháng lại những kẻ tấn công mà đóng vai trò như người xác minh (và do đó có thể tương tác với P trong những lần thực thi lược đồ) và có thể hành động một cách không trung thực như những người xác minh cần phải làm, và rồi sau đó chúng sẽ cố mạo danh P trước người xác minh (trung thực) nào đó.

Để kết thúc mục này, chúng tôi trình bày định nghĩa về một lớp các lược đồ định danh 3-pha với một số tính chất đặc trưng, gọi là *lược đồ định danh chính tắc*.

Định nghĩa 3 (Lược đồ định danh chính tắc, [3]). *Một lược đồ định danh thỏa mãn các phát biểu dưới đây thì được gọi là một* ***lược đồ định danh chính tắc****:*

- *Giao thức định danh* (P, V) *là một giao thức 3-pha, tức là một lần thực thi giao thức bao gồm một thông điệp khởi tạo I được gửi bởi* P*, một "thách thức" c được gửi bởi* V*, và phúc đáp cuối cùng r được gửi bởi* P.
- *Ta giả thiết thách thức c được chọn đều từ một tập* Ω *nào đó. (Nói chung,* $\Omega = \Omega_k$ *phụ thuộc vào tham số an toàn k, và cũng có thể phụ thuộc vào khóa công khai* pk*.) Điều này hàm ý rằng bất kỳ ai được cho bản ghi của một lần thực thi giao thức (cùng với khóa công khai* pk *của* P*) đều có thể xác định một cách hiệu quả xem liệu* V *đã chấp nhận sau lần thực thi đó hay chưa. Ta nói* (pk, I, c, r) *là một* ***bản ghi chấp nhận*** *nếu* V *chấp nhận lần thực thi của giao thức mà cho kết quả là bản ghi đó. (Khi không lo có sự mập mờ về* pk*, ta viết* (I, c, r) *là một bản ghi chấp nhận.)*
- *Ta giả thiết rằng thông điệp đầu tiên của giao thức là "không suy biến" theo nghĩa: với mỗi khóa bí mật sk và một thông điệp cố định* $\hat{I}$ *bất kỳ, xác suất để* $\mathrm{P}(\mathrm{sk})$ *đưa ra* $I = \hat{I}$ *như thông điệp đầu tiên là không đáng kể. Cụ thể hơn, điều này có nghĩa là xác suất để thông điệp đầu tiên I lặp lại trong đa thức lần thực thi của giao thức là không đáng kể. (Chú ý rằng yêu cầu này có thể dễ dàng được thỏa mãn đối với bất kỳ một lược đồ định danh 3-pha nào bằng cách cho P gửi thêm một chuỗi ngẫu nhiên k-bit (mà sẽ được bỏ qua bởi* V*) như là một phần trong thông điệp đầu tiên của nó.)*

Một lược đồ định danh chính tắc được mô tả như trong Hình 1.



Hình 1. Lược đồ định danh chính tắc

III. XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ TỪ CÁC LƯỢC ĐỒ ĐỊNH DANH SỬ DỤNG PHÉP BIẾN ĐỔI FIAT-SHAMIR

Từ đây, do chỉ đề cập tới các lược đồ định danh chính tắc nên để đơn giản, khi không có giải thích gì thêm thì thuật ngữ "lược đồ định danh" được hiểu là "lược đồ định danh chính tắc".

A. Phép biến đổi Fiat-Shamir

Trong [2], Amos Fiat và Adi Shamir đã đề xuất một phương pháp xây dựng lược đồ chữ ký số từ các lược đồ định danh như sau:

Phép xây dựng 1: Phép biến đổi Fiat-Shamir

Cho $\Pi = (\mathrm{Gen}, \mathrm{P}, \mathrm{V})$ là một lược đồ định danh, trong đó các thách thức của người xác minh được chọn đều từ Ω. Gọi $H: \{0,1\}^* \longrightarrow \Omega$ là một hàm băm.

Sinh khóa: Chạy $\mathrm{Gen}(1^k)$ để sinh cặp các khóa công khai/bí mật tương ứng là $(\mathrm{pk}, \mathrm{sk})$.

Sinh chữ ký: Để ký một thông điệp m với khóa bí mật sk, ta thực hiện các hoạt động sau:

- Chạy thuật toán chứng minh $\mathrm{P}(\mathrm{sk})$ để sinh một thông điệp khởi tạo I.
- Tính $c = H(I, m)$.
- Tính câu phúc đáp thích hợp r cho "thách thức" c với việc sử dụng $\mathrm{P}(\mathrm{sk})$.
- Đưa ra chữ ký là (I, r).

Xác minh chữ ký: Để xác minh chữ ký (I, r) trên thông điệp m ứng với khóa công khai pk, ta thực hiện:

- Tính $c = H(I, m)$.
- Chấp nhận chữ ký nếu và chỉ nếu (pk, I, c, r) là một bản ghi chấp nhận.

Tính đúng đắn của lược đồ chữ ký số Π được xây dựng qua phép biến đổi Fiat-Shamir ở trên là dễ dàng suy ra từ tính đúng đắn của lược đồ định danh Π ban đầu.

Bây giờ, giả sử lược đồ định danh Π có thêm tính chất là dựa vào khóa công khai pk, một thách thức tùy ý c, và phúc đáp r tùy ý, việc tính một cách tất định (trong thời gian đa thức) thông điệp khởi tạo I sao cho (pk, I, c, r) là một bản ghi chấp nhận là hoàn toàn có thể. Khi đó, với tính chất này của Π ta có một biến thể của phép biến đổi Fiat-Shamir để xây dựng lược đồ chữ ký số Π' từ Π như sau ([3, Phép xây dựng 8.2]):

Phép xây dựng 2: Một biến thể của phép biến đổi Fiat-Shamir

Sinh khóa: Chạy $\mathrm{Gen}(1^k)$ để sinh cặp khóa công khai/bí mật $(\mathrm{pk}, \mathrm{sk})$.

Sinh chữ ký: Để ký một thông điệp m với việc sử dụng khóa bí mật sk, thực hiện như sau:

- Chạy thuật toán chứng minh $\mathrm{P}(\mathrm{pk})$ để sinh một thông điệp khởi tạo I.
- Tính $c = H(I, m)$.
- Tính câu phúc đáp thích hợp r để trả lời "thách thức" c bằng cách sử dụng $\mathrm{P}(\mathrm{pk})$.
- Đưa ra chữ ký là (c, r).

Xác minh chữ ký: Để kiểm tra chữ ký (c, r) trên thông điệp m sử dụng khóa công khai pk, thực hiện như sau:

- Tính một cách tất định I' sao cho (pk, I', c, r) là một bản ghi chấp nhận. Nếu không tồn tại I' như vậy thì bác bỏ chữ ký.
- Chấp nhận chữ ký nếu $c = H(I', m)$.

Mối quan hệ giữa hai Phép xây dựng trình bày ở trên được thể hiện qua nhận xét dưới đây.

Nhận xét 1. Giả sử ta nhận được chữ ký (I, r) từ Phép xây dựng 1. Khi đó, dễ thấy là ta có thể chuyển đổi chữ ký này thành chữ ký trên m nhận được qua Phép xây dựng 2 bằng cách đưa ra chữ ký (c, r) với $\mathrm{c} = \mathrm{H}(\mathrm{I}, \mathrm{m})$, và dễ thấy chữ ký này vượt qua được thuật toán xác minh trong Phép xây dựng 2 bằng cách lấy $\mathrm{I}' = \mathrm{I}$. Ngược lại, giả sử ta nhận được chữ ký hợp lệ (c, r) trên m qua Phép xây dựng thứ 2. Khi đó sử dụng thuật toán xác minh chữ ký ta tính được I' sao cho $(\mathrm{pk}, \mathrm{I}', \mathrm{c}, \mathrm{r})$ là bản ghi chấp nhận và

$c = H(I', m)$. Đưa ra chữ ký (I', r), thì rõ ràng chữ ký vượt qua được thuật toán xác minh của Phép xây dựng 1, nên được chấp nhận là chữ ký trên m được tính nhờ Phép xây dựng 1. Do các chữ ký nhận được từ hai Phép xây dựng có thể chuyển đổi lẫn nhau nên suy ra lược đồ chữ ký số Π' nhận được từ Phép xây dựng 2 cũng đạt được tính chất an toàn như lược đồ chữ ký số nhận được từ Phép xây dựng 1.

B. Điều kiện cần và đủ cho độ an toàn của lược đồ chữ ký số xây dựng từ các lược đồ định danh

Ký hiệu $\Pi = (Gen, P, V)$ là một lược đồ định danh và Π' là lược đồ chữ ký số nhận được qua việc áp dụng Phép biến đổi Fiat-Shamir lên Π. Một câu hỏi tự nhiên là, để lược đồ chữ ký số Π' an toàn dưới các tấn công sử dụng thông điệp được lựa chọn thích nghi thì lược đồ định danh Π phải thỏa mãn các điều kiện gì. Định lý dưới đây sẽ trả lời cho câu hỏi đó.

Định lý 1 ([3, Định lý 8.1]). *Cho* $\Pi = (Gen, P, V)$ *là một lược đồ định danh mà an toàn kháng lại các tấn công bị động. Khi đó, nếu hàm băm H được mô hình hóa như một bộ tiên tri ngẫu nhiên thì lược đồ chữ ký số* Π' *nhận được từ việc áp dụng phép biến đổi Fiat-Shamir lên* Π *là không thể bị giả mạo tồn tại dưới các tấn công sử dụng thông điệp được lựa chọn thích nghi.*

Chứng minh. Ý tưởng chứng minh là, ta sẽ sử dụng một kẻ tấn công $\mathcal{A}'$ của lược đồ chữ ký số Π' để xây dựng một kẻ tấn công $\mathcal{A}$ tấn công vào lược đồ định danh. Kẻ tấn công $\mathcal{A}$ được cho khóa công khai pk cũng như được phép truy cập đến bộ tiên tri $\text{Trans}_{\text{pk,sk}}$, và tương tác với một người xác minh trung thực V. Chú ý rằng, như những lập luận đã trình bày phía dưới Định nghĩa 2, để không mất tính tổng quát, ta có thể giả thiết cho phép $\mathcal{A}$ được truy cập đến bộ tiên tri $\text{Trans}_{\text{pk,sk}}$ ngay cả trong quá trình tương tác với V.

Bây giờ, giả sử $\mathcal{A}'$ là một kẻ tấn công PPT đối với lược đồ Π'. Ta sẽ đưa ra một vài giả thiết đơn giản mà không làm mất đi tính tổng quát. Trước tiên, ta giả thiết $\mathcal{A}'$ chỉ thực hiện truy vấn đối với giá trị băm đã cho chỉ duy nhất một lần. Để đơn giản, khi $\mathcal{A}'$ được cho một chữ ký (I, r) trên thông điệp m thì đồng thời $\mathcal{A}'$ cũng được cho giá trị $H(I, m)$, do đó ta giả thiết $\mathcal{A}'$ không bao giờ truy vấn $H(I, m)$ sau khi đã nhận được chữ ký (I, r) trên m. Ta cũng yêu cầu, nếu $\mathcal{A}'$ đưa ra chữ ký giả mạo (I, r) trên thông điệp m, thì $\mathcal{A}'$ đã yêu cầu trước đó một truy vấn băm $H(I, m)$. Ta gọi truy vấn băm duy nhất này là *truy vấn băm đặc biệt*. Ký hiệu q_H là biên trên đa thức cho số lượng các truy vấn băm được thực hiện bởi $\mathcal{A}'$.

Tiếp theo ta mô tả kẻ tấn công PPT $\mathcal{A}$ lên lược đồ Π. Kẻ tấn công $\mathcal{A}$ được cho đầu vào là khóa công khai pk, được phép truy cập đến bộ tiên tri $\text{Trans}_{\text{pk,sk}}$, và có tương tác với người xác minh V. Hoạt động đầu tiên $\mathcal{A}$ thực hiện là đoán một chỉ số ngẫu nhiên $i \leftarrow \{1, \dots, q_H\}$. Chỉ số này đóng vai trò là phỏng đoán cho chỉ số của truy vấn băm đặc biệt (nếu có) sẽ được thực hiện bởi $\mathcal{A}'$. Sau đó, kẻ tấn công $\mathcal{A}$ chạy $\mathcal{A}'(\text{pk})$, và trả lời các truy vấn của $\mathcal{A}'$ như sau:

Truy vấn băm $H(I, m)$**:** Có hai trường hợp:

- Nếu đây là truy vấn thứ i đến H, thì $\mathcal{A}$ sẽ đưa ra phỏng đoán truy vấn này chính là truy vấn băm đặc biệt. $\mathcal{A}$ gửi I tới người xác minh trung thực V mà nó được phép tương tác, và nhận giá trị trả về là một thách thức c. Sau đó $\mathcal{A}$ gửi c cho $\mathcal{A}'$ như là câu phúc đáp ứng với truy vấn băm này. Ta gọi truy vấn băm trong trường hợp này là *truy vấn đã phỏng đoán*.
- Nếu đây không phải là truy vấn thứ i thì $\mathcal{A}$ chọn ngẫu nhiên một giá trị $c \leftarrow \Omega$ và gửi c về $\mathcal{A}'$ để phúc đáp truy vấn này.

Rõ ràng, trong cả hai trường hợp giá trị trả về mà $\mathcal{A}'$ nhận được đều có phân bố đều trong Ω.

Truy vấn ký $\text{Sign}_{\text{sk}}(m)$**:** $\mathcal{A}$ truy vấn tới bộ tiên tri $\text{Trans}_{\text{sk,pk}}$ và nhận được bản ghi (I, c, r). Nếu giá trị băm $H(I, m)$ đã được xác định trước đó thì $\mathcal{A}$ bỏ dở. Ngược lại, $\mathcal{A}$ gửi trả về chữ ký (I, r) cho $\mathcal{A}'$ (cùng với giá trị băm $H(I, m) = c$).

Nếu $\mathcal{A}'$ đưa ra một chữ ký hợp lệ $(\hat{I}, \hat{r})$ trên thông điệp $\hat{m}$, thì $\mathcal{A}$ kiểm tra xem truy vấn đã phỏng đoán $H(I, m)$ có bằng truy vấn đặc biệt $H(\hat{I}, \hat{m})$ hay không. Nếu chúng không bằng nhau, thì kết luận $\mathcal{A}$ bỏ dở. Ngược lại, $\mathcal{A}$ gửi $\hat{r}$ tới người xác minh V.

Chú ý rằng, với điều kiện $\mathcal{A}$ không bỏ dở trong khi thực thi và phỏng đoán của nó về truy

vấn đặc biệt là đúng, thì $\mathcal{A}$ thành công trong việc giả mạo người chứng minh trung thực. Lý do là bởi vì:

- Khi truy vấn đã phỏng đoán bằng với truy vấn đặc biệt, tức là $\mathcal{A}$ đã gửi $\hat{I}$ tới người xác minh, và nhận về thách thức $c = H(\hat{I}, \hat{m})$.
- $(\hat{I}, \hat{r})$ là một chữ ký hợp lệ trên $\hat{m}$ nếu $(\hat{I}, c, \hat{r})$ chính xác là một bản ghi chấp nhận.

$\mathcal{A}$ bỏ dở nếu, trong quá trình trả lời một truy vấn ký cho thông điệp m, $\mathcal{A}$ nhận được bản ghi (I, c, r) mà với nó truy vấn băm $H(I, m)$ đã được thực hiện bởi $\mathcal{A}'$. Vì lược đồ định danh Π được giả thiết là chính tắc (và vì thế thông điệp đầu tiên là không suy biến) nên xác suất để xảy ra trường hợp này là không đáng kể.

Giả sử $\mathcal{A}$ không bỏ dở trong quá trình thực thi, thì nó là một sự giả lập hoàn hảo cho $\mathcal{A}'$. Hơn nữa, phỏng đoán của $\mathcal{A}'$ về truy vấn đặc biệt là đúng với xác suất $1/q_H$ (và biến cố này độc lập với biến cố $\mathcal{A}'$ đưa ra một chữ ký giả mạo hợp lệ). Nếu $\mathcal{A}'$ thành công trong việc đưa ra một chữ ký hợp lệ với xác suất ε' thì $\mathcal{A}$ thành công trong việc giả mạo với xác suất $\varepsilon = (\varepsilon' - \mu(k))/q_H$ với $\mu(k)$ là một hàm nào đó mà không đáng kể theo k. Do lược đồ định danh Π là an toàn bị động, nên suy ra ta nhận được khẳng định cần chứng minh.

Định lý 1 đã cung cấp cho ta một "điều kiện đủ" để nhận được một lược đồ chữ ký số không thể bị giả mạo tồn tại dưới tấn công sử dụng thông điệp được lựa chọn thích nghi từ việc áp dụng phép biến đổi Fiat-Shamir lên các lược đồ định danh, đó là "lược đồ định danh phải an toàn kháng lại các tấn công bị động và hàm băm H phải được mô hình hóa như một bộ tiên tri ngẫu nhiên".

Tuy nhiên, không chỉ có vậy, với mệnh đề dưới đây, chúng tôi chỉ ra "điều kiện đủ" đưa ra ở Định lý 1 cũng chính là "điều kiện cần".

Mệnh đề 1. *Cho* $\Pi = (\mathrm{Gen}, \mathrm{P}, \mathrm{V})$ *là một lược đồ định danh. Giả sử hàm băm H được mô hình hóa như một bộ tiên tri ngẫu nhiên. Khi đó, nếu lược đồ chữ ký số* Π' *nhận được từ việc áp dụng phép biến đổi Fiat-Shamir lên lược đồ* Π *là không thể bị giả mạo tồn tại dưới tấn công sử dụng thông điệp được lựa chọn thích nghi thì lược đồ* Π *là an toàn tức là kháng lại được các tấn công bị động.*

Chứng minh. Ta sẽ sử dụng phương pháp phản chứng để chỉ ra điều cần chứng minh. Giả sử ngược lại rằng lược đồ chữ ký số Π' là không thể bị giả mạo tồn tại dưới tấn công sử dụng thông điệp được lựa chọn thích nghi, nhưng lược đồ định danh Π không an toàn dưới các tấn công bị động. Khi đó, tồn tại một kẻ tấn công $\mathcal{A}$ mà dựa vào khóa công khai có thể mạo danh người chứng minh P với xác suất đáng kể. Tất nhiên ở đây $\mathcal{A}$ được phép truy vấn một số lượng hữu hạn (đa thức) đến bộ tiên tri Trans để nhận được các bản ghi chấp nhận. Mục tiêu của ta là xây dựng một kẻ tấn công $\mathcal{A}'$ được phép truy cập đến bộ tiên tri ký $\mathrm{Sign}_{\mathrm{sk}}$ mà sử dụng $\mathcal{A}$ như một thủ tục con để giả mạo thành công chữ ký của lược đồ Π' với xác suất đáng kể.

Kẻ tấn công $\mathcal{A}'$ được xây dựng một cách đơn giản như sau: Để đưa ra một chữ ký giả mạo trên thông điệp m, trước tiên $\mathcal{A}'$ chạy $\mathcal{A}$ để sinh ra một thông điệp I. $\mathcal{A}'$ tính giá trị $c = H(I, m)$ và gửi trả về $\mathcal{A}$ như là giá trị thách thức của m. Do H được mô hình hóa như một bộ tiên tri ngẫu nhiên nên giá trị thách thức c mà $\mathcal{A}$ nhận được cũng được phân bố đều trong Ω như mọi giá trị thách thức khác do người xác minh chọn ngẫu nhiên đều từ Ω. Có thể lặp lại hoạt động của $\mathcal{A}'$ một số hữu hạn (đa thức) lần cho đến khi $\mathcal{A}$ đưa ra một câu phúc đáp r tương ứng với thông điệp I. Theo giả thiết thì (pk, I, c, r) sẽ là bản ghi chấp nhận vượt qua được bước kiểm tra của người xác minh V với xác suất đáng kể. Cuối cùng, $\mathcal{A}'$ đưa ra (I, r) như là chữ ký giả mạo trên thông điệp m. Rõ ràng, ngoại trừ với một xác suất nhỏ không đáng kể như sẽ chỉ ra dưới đây, (I, r) là một chữ ký hợp lệ trên thông điệp m nhận được từ bản ghi chấp nhận (pk, I, c, r). Như vậy $\mathcal{A}'$ đã tạo ra được chữ ký hợp lệ (I, r) trên thông điệp m với xác suất đáng kể mà không cần biết khóa bí mật.

Cần lưu ý rằng, trong quá trình tấn công để mạo danh P, trước khi đưa ra phúc đáp r tương ứng với thách thức c và thông điệp I, kẻ tấn công $\mathcal{A}$ có thể thực hiện một số lượng hữu hạn (đa thức) các truy vấn đến bộ tiên tri $\mathrm{Trans}_{\mathrm{sk,pk}}$. Do đó ở đây ta cần mô tả chính xác cách mà $\mathcal{A}'$ giả lập việc truy vấn của $\mathcal{A}$ đến bộ tiên tri Trans. Cụ thể $\mathcal{A}'$ thực hiện như sau: Đối với truy vấn thứ i của $\mathcal{A}$ đến $\mathrm{Trans}_{\mathrm{sk,pk}}$, $\mathcal{A}'$ sẽ sinh ngẫu nhiên một thông điệp m_i, sau đó thực hiện truy vấn ký trên m_i đến bộ tiên tri ký. Kết quả

của việc truy vấn ký là $\mathcal{A}'$ sẽ nhận được chữ ký (I_i, r_i) trên thông điệp m_i. Khi đó, nếu $m = m_i$, hoặc m_i đã xuất hiện trong các truy vấn trước đó, hoặc $H(I, m) = H(I_i, m_i)$ thì $\mathcal{A}'$ bỏ dở. Ngược lại, $\mathcal{A}'$ sẽ gửi trả về cho $\mathcal{A}$ bản ghi chấp nhận $(\text{pk}, I_i, c_i, r_i)$ với $c_i = H(I_i, m_i)$ như là phúc đáp của lời truy vấn thứ i tới bộ tiên tri $\text{Trans}_{\text{sk,pk}}$. Và $\mathcal{A}$ sẽ sử dụng các bản ghi này trong nỗ lực mạo danh người chứng minh P.

Rõ ràng, do các thông điệp m, m_i được chọn ngẫu nhiên, và theo giả thiết hàm băm H được mô hình hóa như một bộ tiên tri ngẫu nhiên nên từ cách xây dựng $\mathcal{A}'$, ta thấy xác suất để $\mathcal{A}'$ bỏ dở các hoạt động là không đáng kể. Do đó suy ra, xác suất của $\mathcal{A}'$ đưa ra một chữ ký hợp lệ trên một thông điệp m mà không cần đến khóa bí mật sk sẽ xấp xỉ xác suất thành công của kẻ tấn công $\mathcal{A}$ trừ đi một lượng không đáng kể.

Ta mô tả kẻ tấn công $\mathcal{A}'$ được xây dựng từ kẻ tấn công $\mathcal{A}$ dưới dạng thuật toán như sau:

Kẻ tấn công $\mathcal{A}'$:

Kẻ tấn công $\mathcal{A}'$ được cho khóa công khai pk và được phép truy cập đến bộ tiên tri ký Sign_{sk}.

1. Sinh ngẫu nhiên một thông điệp m.
2. Chạy $\mathcal{A}(\text{pk})$ và thực hiện như sau:
   - Tính $c = H(I, m)$ và gửi c về cho $\mathcal{A}$ như là giá trị thách thức của người xác minh V.
   - Khi $\mathcal{A}$ thực hiện truy vấn thứ i đến bộ tiên tri $\text{Trans}_{\text{sk,pk}}$, thì trả lời như sau:
     - $\mathcal{A}'$ sinh ngẫu nhiên một thông điệp m_i và thực hiện truy vấn ký trên m_i đến bộ tiên tri ký Sign_{sk}, nhận về chữ ký hợp lệ (I_i, r_i) trên m_i.
     - Nếu $m = m_i$, hoặc m_i đã xuất hiện trong các truy vấn trước đó, hoặc $H(I, m) = H(I_i, m_i)$ thì $\mathcal{A}'$ bỏ dở. Ngược lại, $\mathcal{A}'$ gửi cho $\mathcal{A}$ bản ghi chấp nhận (pk, I_i, c_i, r_i) với $c_i = H(I_i, m_i)$.
3. Sau khi $\mathcal{A}$ đưa ra bản ghi chấp nhận (pk, I, c, r) thì $\mathcal{A}'$ đưa ra (I, r) như là chữ ký trên thông điệp m.

Tất cả các lập luận trên cho thấy, sử dụng kẻ tấn công $\mathcal{A}$ đối với lược đồ định danh Π như một thủ tục con, ta đã xây dựng được một kẻ tấn công $\mathcal{A}'$ mà có thể giả mạo chữ ký của lược đồ chữ ký số Π' với xác suất đáng kể. Điều này trái với giả thiết lược đồ chữ ký số Π' là không thể bị giả mạo tồn tại dưới các tấn công sử dụng thông điệp được lựa chọn thích nghi. Do vậy suy ra, lược đồ định danh Π phải an toàn kháng lại các tấn công bị động.

C. Điều kiện đủ cho tính an toàn bị động của các lược đồ định danh

Trong mục trước, với Định lý 1 và Mệnh đề 1, ta đã chỉ ra lược đồ chữ ký số Π' nhận được qua việc áp dụng Phép biến đổi Fiat-Shamir lên lược đồ định danh Π là không thể bị giả mạo tồn tại dưới các tấn công sử dụng thông điệp được lựa chọn thích nghi nếu và chỉ nếu Π là an toàn bị động. Trong mục này, chúng tôi trình bày hai tiêu chuẩn mà là điều kiện đủ để một lược đồ định danh đạt được độ an toàn bị động. Đó là tiêu chuẩn *không lộ tri thức cho người xác minh trung thực (HVKZ)* và tiêu chuẩn *mạnh đặc biệt.* Cụ thể các tiêu chuẩn này được định nghĩa chính thức như dưới đây.

Định nghĩa 4 ([3, Định nghĩa 8.3])**.** *Một lược đồ định danh* Π *là* ***không lộ tri thức cho người xác minh trung thực (HVZK)*** *nếu tồn tại một thuật toán PPT* Sim *sao cho các phân bố sau đây là không thể phân biệt được về mặt tính toán:*

$$\{(\text{pk}, \text{sk}) \leftarrow \text{Gen}(1^k) : (\text{sk}, \text{pk}, \text{Sim}(\text{pk}))\}$$

và

$$\{(\text{pk}, \text{sk}) \leftarrow \text{Gen}(1^k) : (\text{sk}, \text{pk}, \text{Trans}_{\text{sk,pk}})\}.$$

Nếu các phân bố trên là ***đồng nhất****, ta nói* Π *là không lộ tri thức cho người xác minh trung thực* ***hoàn hảo****.*

Định nghĩa 5 ([3, Định nghĩa 8.4])**.** *Một lược đồ định danh* Π *thỏa mãn tính chất* ***mạnh đặc biệt*** *nếu xác suất sau đây là không đáng kể đối với mọi thuật toán PPT* $\mathcal{A}$*:*

$$\Pr\left[\begin{array}{c}(\text{pk}, \text{sk}) \leftarrow \text{Gen}(1^k) \\ (I, c_1, r_1, c_2, r_2) \leftarrow \mathcal{A}(\text{pk}) \\ : \quad c_1 \neq c_2 \ \text{và} \\ (\text{pk}, I, c_1, r_1), (\text{pk}, I, c_2, r_2) \\ \text{đều là các bản ghi chấp nhận}\end{array}\right].$$

Định lý sau đây chỉ ra hai tiêu chuẩn trên là điều kiện đủ đảm bảo cho độ an toàn bị động của các lược đồ định danh.

Định lý 2 ([3, Định lý 8.2])**.** *Giả sử lược đồ định danh* Π *là không lộ tri thức cho người xác minh trung thực và thỏa mãn tính chất mạnh đặc biệt. Khi đó với mọi kẻ tấn công* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *ta có:*

$$\Pr\left[\begin{matrix}(\mathrm{pk},\mathrm{sk}) \leftarrow \mathrm{Gen}(1^k) \\ s \leftarrow \mathcal{A}_1^{\mathrm{Trans}_{\mathrm{sk},\mathrm{pk}}(\cdot)}(\mathrm{pk}) \\ : \langle \mathcal{A}_2(\mathrm{pk}), \mathrm{V}(\mathrm{pk}) = 1\rangle\end{matrix}\right] - |\Omega_k|^{-1} \leq \mu(k)$$

với hàm không đáng kể $\mu(\cdot)$ *nào đó. Cụ thể hơn, nếu* $|\Omega_k| = \omega(\mathrm{poly}(k))$ *thì* Π *là an toàn kháng lại các tấn công bị động.*

Chứng minh. Chi tiết xem trong tài liệu đã dẫn.

Từ các Định lý 1 và Định lý 2 ta có hệ quả sau đây.

Hệ quả 1. *Cho* $\Pi = (\mathrm{Gen}, \mathrm{P}, \mathrm{V})$ *là một lược đồ định danh thỏa mãn các tiêu chuẩn như trong Định lý 2. Khi đó nếu hàm băm H được mô hình hóa như một bộ tiên tri ngẫu nhiên thì lược đồ chữ ký số* Π' *nhận được từ việc áp dụng phép biến đổi Fiat-Shamir lên* Π *là không thể bị giả mạo tồn tại dưới các tấn công sử dụng thông điệp được lựa chọn thích nghi.*

Chứng minh. Khẳng định này là hiển nhiên từ các Định lý 1 và 2.

IV. KẾT LUẬN

Trong bài báo này chúng tôi đã trình bày nội dung cơ bản về phương pháp xây dựng lược đồ chữ ký số từ các lược đồ định danh với việc sử dụng phép biến đổi Fiat-Shamir. Ngoài các định nghĩa và kết quả được trích dẫn từ tài liệu tham khảo [2], đóng góp của chúng tôi qua bài báo gồm có:

- Phát biểu và chứng minh Mệnh đề 1 về điều kiện cần của lược đồ định danh để đảm bảo cho lược đồ chữ ký xây dựng từ nó là an toàn.
- Chúng tôi đưa ra Hệ quả 1 như là một sự tổng kết về một số "điều kiện đủ" cho các lược đồ định danh để đảm bảo tính an toàn cho lược đồ chữ ký số được xây dựng từ nó. Đồng thời, trong bài báo, đã đưa ra Nhận xét 1 để chỉ ra sự tương đồng giữa Phép biến đổi Fiat-Shamir và biến thể của nó.

Hướng nghiên cứu tiếp theo: Việc xây dựng các lược đồ chữ ký số từ các lược đồ định danh là một trong số những phương pháp quan trọng, bao hàm nhiều khía cạnh tinh tế của mật mã hiện đại. Trong khuôn khổ một bài báo chúng tôi chưa đủ khả năng cũng như thời gian để trình bày một cách đầy đủ, chi tiết, sâu sắc về tất cả các khía cạnh mật mã của phương pháp xây dựng này, chẳng hạn như về các điều kiện cho lược đồ định danh để có các lược đồ chữ ký số đạt tính chất an toàn về phía trước cũng như về các lược đồ định danh cụ thể với các tính chất an toàn tốt, tiêu biểu là lược đồ Fiat-Shamir, lược đồ Schnorr, lược đồ Guillou-Quisquater,…. Ngoài ra, việc so sánh các tính chất an toàn giữa các lược đồ chữ ký số nhận được từ các lược đồ định danh qua phép biến đổi Fiat-Shamir với các lược đồ chữ ký số không được xây dựng dựa trên phép biến đổi này, (chẳng hạn như lược đồ RSA, ECDSA) cũng chưa được đề cập đến trong bài báo. Do đó các vấn đề này cần được tiếp tục nghiên cứu sâu hơn nữa.

TÀI LIỆU THAM KHẢO

[1]. Michel Abdalla, Jee Hea An, Mihir Bellare, and Chanathip Namprempre. "From identification to signatures via the Fiat-Shamir transform: Necessary and sufficient conditions for security and forward-security". IEEE Transactions on Information Theory, 54(8): pp.3631-3646, 2008.

[2]. Amos Fiat and Adi Shamir. "How to prove yourself: Practical solutions to identification and signature problems". In Advances in Cryptology - CRYPTO'86, pp. 186-194, Springer, 1986.

[3]. Jonathan Katz. "Digital signatures". Springer Science & Business Media, 2010.

SƠ LƯỢC VỀ TÁC GIẢ

ThS. Võ Tùng Linh

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

Email: vtlinh@gmail.com

Quá trình đào tạo: nhận bằng Cử nhân toán học năm 2005 và bằng Thạc sỹ toán học năm 2014.

Lĩnh vực nghiên cứu hiện nay: mật mã khóa công khai, mật mã đường cong elliptic.