Độ an toàn chứng minh được của lược đồ chữ ký FIAT-SHAMIR dựa trên ý tưởng của POINTCHEVAL

Triệu Quang Phong, Võ Tùng Linh

Tóm tắt— **Trong bài báo này, chúng tôi phân tích độ an toàn "chứng minh được" đối với lược đồ chữ ký Fiat-Shamir dựa theo cách chứng minh độ an toàn cho các lược đồ chữ ký của Pointcheval. Cụ thể hơn, trong mô hình "bộ tiên tri ngẫu nhiên", với giả thiết rằng bài toán phân tích nhân tử là khó giải, có thể chỉ ra rằng tính an toàn của lược đồ chữ ký Fiat-Shamir được đảm bảo. Độ an toàn của lược đồ chữ ký này sẽ được phân tích theo hai kịch bản: tấn công không sử dụng thông điệp và tấn công sử dụng thông điệp được lựa chọn thích nghi. Trong kiểu tấn công đầu, tác giả Pointcheval và cộng sự đã chỉ ra rằng, nếu lược đồ chữ ký Fiat-Shamir là không an toàn dưới kiểu tấn công này, thì bài toán phân tích nhân tử sẽ giải được trong thời gian đa thức. Ở kiểu tấn công sau, nếu bộ ký của lược đồ chữ ký có thể bị mô phỏng theo một phân bố không phân biệt được, thì chúng ta có thể thu được kết quả tương tự như trong kiểu tấn công trước.**

Abstract— **In this paper, we analyze the "provable" security for Fiat-Shamir signature scheme based on the security proof methods of Pointcheval for signature schemes. In particular, in the "random oracle" model, assuming that the factorization problem is intractable, we can show that the security of Fiat-Shamir scheme is guaranteed. The security of this signature scheme will be analyzed in two scenarios: the no-message attack and the adaptively chosen message attack. In the former, Pointcheval and his partner proved that if the Fiat-Shamir signature scheme is unsecure against the no-message attack, then the factorization problem can be solved in polynomial time. In the latter, if the signer of signature scheme can be simulated with an indistinguishable distribution, then we will obtain the same result as the previous attack.**

Từ khóa— Lược đồ chữ ký; an toàn chứng minh được; bộ tiên tri ngẫu nhiên; tấn công không sử dụng thông điệp; tấn công sử dụng thông điệp được lựa chọn thích nghi.

I. GIỚI THIỆU

Trong lĩnh vực mật mã khóa công khai, hướng nghiên cứu nhằm cung cấp độ an toàn "có thể chứng minh" cho các giao thức mật mã đang được quan tâm và triển khai rộng rãi. Trong phạm vi của độ an toàn tính toán, các chứng minh đã được đưa ra trong khung tiệm cận theo lý thuyết độ phức tạp. Chúng là những suy dẫn tính toán qua lại giữa các vấn đề được định nghĩa chặt chẽ theo lý thuyết số như bài toán phân tích nhân tử, bài toán logarit rời rạc hay bài toán tìm căn bậc hai.

Trong [2], [3], các tác giả đã chứng minh chi tiết về độ an toàn của lược đồ chữ ký Schnorr và một phiên bản của lược đồ chữ ký El Gamal trước hai kịch bản tấn công sử dụng máy Turing thời gian đa thức xác suất: tấn công *không sử dụng thông điệp* và tấn công *sử dụng thông điệp được lựa chọn thích nghi*. Trong [2], độ an toàn cho lược đồ chữ ký Fiat-Shamir trước tấn công không sử dụng thông điệp đã được chứng minh và đưa ra nhận xét về độ an toàn của lược đồ chữ ký này trước tấn công sử dụng thông điệp được lựa chọn thích nghi nhưng không chứng minh (nhận xét 6 trong [2]).

Trong bài báo, dựa trên phương pháp lập luận của Pointcheval và cộng sự, chúng tôi phát biểu nhận xét này dưới dạng Mệnh đề 6, Hệ quả 7 và các chứng minh chi tiết cho chúng. Theo đó, kết quả đã thu được là độ an toàn của lược đồ chữ ký Fiat-Shamir trong mô hình bộ tiên tri ngẫu nhiên được đảm bảo nhờ tính khó giải của bài toán phân tích nhân tử.

Bố cục của bài báo gồm: Mục II trình bày các kiến thức cơ sở: mô tả lược đồ chữ ký Fiat-Shamir, các tấn công được sử dụng trong bài, khái niệm về mô hình bộ tiên tri ngẫu nhiên, phân bố không phân biệt được và hai Bổ đề quan trọng là hai phiên bản của Bổ đề phân nhánh. Mục III trình bày việc áp dụng Bổ đề phân nhánh trên lược đồ chữ ký Fiat-Shamir và chỉ ra độ an toàn cho lược đồ này. Cuối cùng là kết luận.

II. CÁC KIẾN THỨC CƠ SỞ

A. Mô tả lược đồ chữ ký Fiat-Shamir

Trong một lược đồ chữ ký, mỗi người sử dụng công bố một khóa công khai K_p trong khi giữ riêng một khóa bí mật K_s. Một chữ ký của người sử dụng trên thông điệp m là một giá trị phụ thuộc vào m, khóa công khai và khóa bí mật của người sử dụng theo cách mà bất kỳ người nào cũng có thể kiểm tra sự hợp lệ chỉ bằng khóa công khai.

Tuy nhiên, sẽ khó khăn để giả mạo một chữ ký của người sử dụng khi không biết khóa bí mật của người này. Lược đồ chữ ký Fiat-Shamir được mô tả như sau [1]:

- Thuật toán sinh khóa: Cho một tham số an toàn k, thuật toán chọn hai số nguyên tố lớn p và q, giữ bí mật chúng. Tính tích $N = pq$ và định nghĩa một hàm băm ngẫu nhiên f với đầu ra k bit. Sau đó, chọn một số ngẫu nhiên $s \in \mathbb{Z}/N\mathbb{Z}$ và công khai bình phương của nó $v = s^2 mod\ N$. Ở đây, N và f được công khai còn s được giữ bí mật.
- Thuật toán ký: để ký một thông điệp m, người ta tạo ra k số ngẫu nhiên, $r_i \in \mathbb{Z}/N\mathbb{Z}$ với $i = 1, \dots, k$, tính bình phương tương ứng của chúng $x_i = r_i^2 mod\ N$ cũng như thách thức $h = (e_1 \dots e_k) = f(m, x_1, \dots, x_k)$. Từ những dữ liệu này, người ta tạo $y_i = r_i s^{e_i} mod\ N$ và đưa ra $\sigma_1 = (x_1, \dots, x_k)$ và $\sigma_2 = (y_1, \dots, y_k)$. Chữ ký là tổ hợp/bộ ba (σ_1, h, σ_2).
- Thuật toán xác minh: Đối với một thông điệp cho trước m và một chữ ký $\sigma_1 = (x_1, \dots, x_k)$, $h = (e_1 \dots e_k)$ và $\sigma_2 = (y_1, \dots, y_k)$, thuật toán xác minh sẽ kiểm tra xem liệu $h = f(m, \sigma_1)$ và $y_i^2 = x_i v^{e_i} mod\ N$ với mọi i hay không.

Trong những bộ ba (σ_1, h, σ_2) đó, σ_1 được chọn ngẫu nhiên đều từ một tập có số phần tử lớn. Cụ thể hơn, có thể giả sử rằng với mỗi $\sigma_1^{(0)}$ cụ thể, khi thực hiện quá trình ký đối với thông điệp m thì xác suất $\sigma_1^{(0)}$ xuất hiện ở đầu ra là không đáng kể. Thật vậy, trong lược đồ chữ ký Fiat-Shamir, chúng ta thấy rằng: $\sigma_1 = (x_1, x_2, \dots, x_k)$, với $x_i = r_i^2$, $\forall i \in \{1, 2, \dots, k\}$, trong đó $r_i \in_R \mathbb{Z}/N\mathbb{Z}$ với $i = 1, \dots, k$; vì một số chính phương $mod\ N$ có không quá bốn căn bậc hai, do đó, xác suất để σ_1 nhận một giá trị cụ thể là không vượt quá $4^k \cdot N^{-k}$, một lượng không đáng kể.

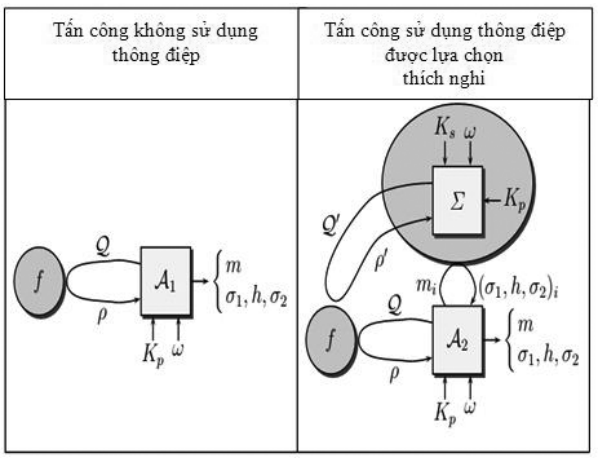
Ngoài ra, chúng ta cũng cần chú ý rằng, một *truy vấn* được yêu cầu lên hàm băm f sẽ có dạng (m, σ_1).

B. Mô hình bộ tiên tri ngẫu nhiên

Trên thực tế, một lược đồ chữ ký số cần sử dụng một hàm băm f, chẳng hạn như SHA-3. Việc sử dụng hàm băm ban đầu có thể với mục đích muốn ký một thông điệp dài với một chữ ký ngắn. Và yêu cầu đối với hàm băm là phải có các tính chất mật mã đủ mạnh, cụ thể là tính kháng va chạm, kháng tiền ảnh và kháng tiền ảnh thứ hai. Người ta nhận ra rằng, hàm băm là một thành phần cơ bản trong quá trình phân tích độ an toàn của các lược đồ chữ ký số. Tuy nhiên, để thực sự cung cấp một chứng minh an toàn như vậy, một số tác giả đã đề cập tới việc sử dụng giả thiết f là một hàm ngẫu nghiên, nghĩa là với k là độ dài bit giá trị đầu ra của f, thì giá trị của f đưa ra đối với mỗi truy vấn mới sẽ được chọn ngẫu nhiên đều từ không gian $\{0,1\}^k$.Với giả thiết này, chúng ta sử dụng mô hình tương ứng, gọi là "mô hình bộ tiên tri ngẫu nhiên". Trong mô hình này, hàm băm có thể được xem như một bộ tiên tri tạo ra một giá trị ngẫu nhiên cho mỗi truy vấn mới. Nếu một truy vấn được yêu cầu hai lần thì sẽ nhận được các câu trả lời giống nhau. Các chứng minh trong mô hình này chỉ ra rằng, toàn bộ thiết kế của một lược đồ chữ ký sẽ đảm bảo độ an toàn khi được cung cấp một hàm băm có tính chất mật mã đủ mạnh như đã đề cập ở trên.

C. Các kịch bản tấn công

Chúng ta chỉ xem xét hai kịch bản khác nhau liên quan đến máy Turing thời gian đa thức với xác suất tấn công không sử dụng thông điệp và tấn công sử dụng thông điệp được lựa chọn thích nghi (xem Hình 1).



Hình 1. Kịch bản tấn công liên quan đến máy Turing thời gian đa thức xác suất

Trong kiểu tấn công đầu, kẻ tấn công chỉ biết khóa công khai của người ký, còn trong kiểu tấn công sau, anh ta có thể tự động yêu cầu người sử dụng hợp pháp ký thông điệp bất kỳ, sử dụng người ký như một bộ tiên tri (oracle). Hơn nữa, đối với dạng tấn công sử dụng thông điệp được lựa chọn thích nghi, chúng ta sẽ cần mô tả một bộ mô phỏng có thể của người ký hợp lệ và sử dụng nó.

Trong đó, Σ là bộ ký trong thuật toán ký và hai kẻ tấn công $\mathcal{A}_1, \mathcal{A}_2$ là các máy Turing thời gian đa thức xác suất, với băng ngẫu nhiên ω ở đầu vào. Bên cạnh đó, Q (hoặc Q') là truy vấn của kẻ tấn công (hoặc bộ ký) tới bộ tiên tri ngẫu nhiên f

và các câu trả lời nhận được là ρ (hoặc ρ'). Ngoài ra, cặp thông điệp chữ ký hợp lệ mới $(m, \sigma_1, h, \sigma_2)$ thu được sau tấn công được gọi là một *giả mạo tồn tại*.

D. Tính không thể phân biệt được của hai phân bố xác suất

Phân bố không phân biệt được có một lưu ý rằng, một hàm số $f(k)$ là *không đáng kể* theo k, nếu với mọi đa thức p thì $f(k) \leq 1/|p(k)|$, với k đủ lớn; ngược lại, $f(k)$ là *đáng kể*.

Định nghĩa 1 [3, Definition 6]. *Gọi δ^0 và δ^1 là hai phân bố xác suất. Một bộ phân biệt $\mathcal{D}$ là một máy Turing thời gian đa thức xác suất, với băng ngẫu nhiên ω, đưa vào ρ, trả lời 0 hoặc 1. Một lợi thế của $\mathcal{D}$ tương ứng với hai phân bố δ^0 và δ^1 được định nghĩa như sau:*

$$Adv(\mathcal{D}, \delta^0, \delta^1) = \frac{1}{2} \times \left| \underset{\rho \in \delta^0}{E}[\mathcal{D}(\omega, \rho)] - \underset{\rho \in \delta^1}{E}[\mathcal{D}(\omega, \rho)] \right|.$$

Hai phân bố δ^0 và δ^1 là không phân biệt được theo đa thức nếu không tồn tại bất kỳ bộ phân biệt $\mathcal{D}$ với một lợi thế đáng kể nào.

Hai phân bố δ^0 và δ^1 là không phân biệt được theo thống kê nếu

$$\sum_{y} \left| \underset{\rho \in \delta^0}{Pr}[\rho = y] - \underset{\rho \in \delta^1}{Pr}[\rho = y] \right|$$

là không đáng kể.

Từ định nghĩa trên, dễ dàng suy ra đẳng thức sau:

$$\Pr_{\substack{\omega \\ c \in \{0,1\} \\ \rho \in \delta^c}}[\mathcal{D}(\omega, \rho) = c] = \frac{1}{2} \pm Adv(\mathcal{D}, \delta^0, \delta^1).$$

Do đó, nếu lợi thế là không đáng kể, câu trả lời về kết quả của phân biệt giống như kết quả của việc tung đồng xu.

Chúng ta giả thiết rằng, bộ ký Σ có thể bị mô phỏng theo một *phân bố không phân biệt được* nếu tồn tại một bộ mô phỏng S mà hai phân bố xác suất lần lượt trên không gian chữ ký được tạo bởi S và Σ là không phân biệt được theo đa thức. Khi đó, cũng có thể nói S mô phỏng Σ theo một *phân bố không phân biệt được*.

Ngoài ra, ở [3] nêu ra nhận xét rằng nếu hai phân bố là *không phân biệt được theo thống kê* thì chúng là *không phân biệt được theo đa thức*. Thực vậy, khẳng định này nhận được bằng việc sử dụng bất đẳng thức sau:

$$\begin{aligned} 2 \times Adv(\mathcal{D}, \delta^0, \delta^1) &= \left| \underset{\rho \in \delta^0}{E}[\mathcal{D}(\omega, \rho)] - \underset{\rho \in \delta^1}{E}[\mathcal{D}(\omega, \rho)] \right| \\ &= \left| \Pr_{\rho \in \delta^0}[\mathcal{D}(\omega, \rho) = 1] - \Pr_{\rho \in \delta^1}[\mathcal{D}(\omega, \rho) = 1] \right| \\ &= \left| \Pr_{\rho \in \delta^0}[\rho \in \mathcal{D}^{-1}(\omega, 1)] - \Pr_{\rho \in \delta^1}[\rho \in \mathcal{D}^{-1}(\omega, 1)] \right| \\ &\leq \sum_{y} \left| \underset{\rho \in \delta^0}{Pr}[\rho = y] - \underset{\rho \in \delta^1}{Pr}[\rho = y] \right|. \end{aligned}$$

E. Hai phiên bản của bổ đề phân nhánh

Trong phần này, chúng ta sẽ phát biểu lại hai bổ đề quan trọng, là hai phiên bản của Bổ đề phân nhánh. Trong đó phiên bản thứ nhất (Bổ đề phân nhánh 1) được sử dụng để chứng minh Định lý 5 và phiên bản thứ hai (Bổ đề phân nhánh 2) được sử dụng để chứng minh Hệ quả 7. Các bổ đề này sử dụng "tấn công phát lại bộ tiên tri" (oracle replay attack): bằng việc lặp lại đa thức lần tấn công với cùng băng ngẫu nhiên và một bộ tiên tri khác, chúng ta nhận được hai chữ ký hợp lệ (σ_1, h, σ_2) và $(\sigma_1, h', \sigma_2')$, sao cho $h \neq h'$ đối với thông điệp m. Điều này giúp chứng minh tính an toàn của một lược đồ chữ ký trong mô hình bộ tiên tri ngẫu nhiên. Trước tiên, chúng ta sẽ nhắc lại bổ đề xác suất sau.

Bổ đề 2 (Bổ đề tách) [2, Lemma 4]. *Gọi $A \subset X \times Y$, sao cho $\Pr[(x, y) \in A] \geq \varepsilon$, thì tồn tại $\Omega \subset X$, sao cho:*

i) $Pr\ [x \in \Omega] \geq \varepsilon/2$,

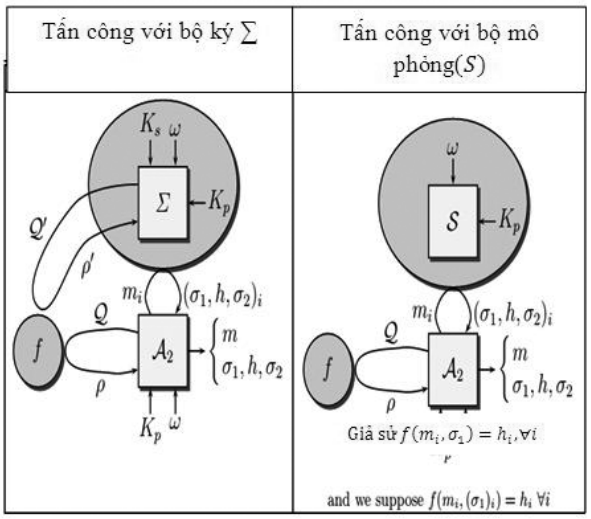
ii) bất cứ $\alpha \in \Omega$, $\Pr[(\alpha, y) \in A] \geq \varepsilon/2$.

Để chứng minh bổ đề này, ý tưởng chính là xây dựng một tập con Ω của X thỏa mãn tính chất "tốt" (theo điều kiện (ii)) và chứng minh tính đáng kể của Ω, nghĩa là chứng minh Ω thỏa mãn điều kiện (i). Bổ đề này là công cụ chính để chứng minh hai phiên bản của Bổ đề phân nhánh được phát biểu dưới đây.

Bổ đề 3 (Bổ đề phân nhánh 1) [2, Lemma 2]. *Gọi $\mathcal{A}$ là một máy Turing thời gian đa thức xác suất, chỉ cho trước dữ liệu công khai như đầu vào. Nếu $\mathcal{A}$ có thể tìm được một chữ ký hợp lệ $(m, \sigma_1, h, \sigma_2)$ với xác suất đáng kể, thì với một xác suất đáng kể, một sự phát lại của máy này với cùng băng ngẫu nhiên và một bộ tiên tri khác sẽ đưa ra hai chữ ký hợp lệ $(m, \sigma_1, h, \sigma_2)$ và $(m, \sigma_1, h', \sigma_2')$ sao cho $h \neq h'$.*

Chú ý rằng, bổ đề trên dành cho kiểu tấn công chỉ sử dụng dữ liệu công khai ở đầu vào, hay tấn công không sử dụng thông điệp.

Kết quả sau đây sẽ chỉ ra rằng, nếu bộ ký Σ có thể bị mô phỏng theo một phân bố xác suất không phân biệt được bởi một bộ mô phỏng S, thì bổ đề phân nhánh trên cũng có thể áp dụng được trong tấn công sử dụng thông điệp được lựa chọn thích nghi để thu được hai chữ ký hợp lệ $(m, \sigma_1, h, \sigma_2)$ *và* $(m, \sigma_1, h', \sigma_2')$, sao cho $h \neq h'$, với xác suất đáng kể, trong thời gian đa thức.



Hình 2. Kịch bản tấn công sử dụng thông điệp được lựa chọn thích nghi

Bổ đề 4 (Bổ đề phân nhánh 2) [3, Lemma 4]. *Gọi $\mathcal{A}$ là máy Turing thời gian đa thức xác suất mà đầu vào chỉ lấy các dữ liệu công khai. Chúng ta ký hiệu Q và R tương ứng là số các truy vấn mà $\mathcal{A}$ có thể hỏi đến bộ tiên tri ngẫu nhiên và bộ ký. Giả sử rằng, với thời gian đa thức, $\mathcal{A}$ tạo ra, với xác suất đáng kể, một chữ ký hợp lệ $(m, \sigma_1, h, \sigma_2)$.*

Nếu bộ ba (σ_1, h, σ_2) có thể bị mô phỏng mà không biết khóa bí mật, với một xác suất phân bố không phân biệt được, thì một sự phát lại của tấn công $\mathcal{A}$, cùng những tương tác với bộ ký được mô phỏng, đưa ra hai chữ ký hợp lệ $(m, \sigma_1, h, \sigma_2)$ và $(m, \sigma_1, h', \sigma_2')$ sao cho $h \neq h'$, với một xác suất đáng kể, trong thời gian đa thức.

Ở đây các ký hiệu là hoàn toàn giống như trong Hình 1, ngoại trừ việc có thêm các truy vấn đến bộ mô phỏng S.

III. ĐỘ AN TOÀN CỦA LƯỢC ĐỒ CHỮ KÝ FIAT-SHAMIR

A. Tấn công không sử dụng thông điệp lên lược đồ chữ ký Fiat-Shamir

Từ Bổ đề phân nhánh 1, chúng ta thu được kết quả sau đây trong mô hình bộ tiên tri ngẫu nhiên.

Định lý 5 [2, Theorem 5]. *Xem xét một tấn công không sử dụng thông điệp trong mô hình bộ tiên tri ngẫu nhiên. Nếu một giả mạo tồn tại trong lược đồ chữ ký Fiat-Shamir là có thể với xác suất đáng kể, thì phân tích nhân tử của RSA modulus có thể được thực hiện trong thời gian đa thức.*

Chứng minh. Gọi $N \in \mathbb{N}$ là số nguyên để phân tích thừa số. Chúng ta chọn $s \in_R \mathbb{Z}/N\mathbb{Z}$, và gọi $v = s^2 mod\ N$. Dễ thấy, xác suất thu được $s = 0\ mod\ N$ là $1/N$ không đáng kể. Mặt khác, nếu ta thu được s ngẫu nhiên thỏa mãn $N > \gcd(s, N) > 1$, thì việc phân tích N có thể thực hiện trong thời gian đa thức. Do đó, để đảm bảo trường hợp chung, giả sử s ngẫu nhiên thu được thỏa mãn $\gcd(s, N) = 1$, điều này tương đương với $\gcd(v, N) = 1$.

Nếu một kẻ tấn công $\mathcal{A}_1$ có thể phá vỡ lược đồ chữ ký Fiat-Shamir, theo Bổ đề phân nhánh 1, thì có thể thu được hai chữ ký hợp lệ $(m, \sigma_1, h, \sigma_2)$ *và* $(m, \sigma_1, h', \sigma_2')$ sao cho $h \neq h'$. Từ đó, ta thu được i sao cho $h_i \neq h'_i$. Giả sử $h_i = 0$ và $h'_i = 1$, chúng ta nhận được $y_i^2 = x_i\ mod\ N$ và $y'^2_i = vx_i mod\ N$. Theo lập luận đối với v như trên, ta thực hiện tương tự đối với x_i, như vậy có thể giả sử rằng $\gcd(x_i, N) = 1$. Khi đó, ta gọi $z = y'_i y_i^{-1} mod\ N$, thì $z^2 = v = s^2 mod\ N$.

Ta thu được s và z là hai căn bậc hai của $v\ mod\ N$ sau tấn công. Từ đó $z^2 - v^2 = 0\ mod\ N$, hay $(z - s)(z + s) = 0\ mod\ N$. Nếu $z \neq \pm s$, thì $N > \gcd(z - s, N) > 1$, bởi vì, nếu $\gcd(z - s, N) = 1$ thì $z + s = 0\ mod\ N$ (sẽ là vô lý). Như vậy, chúng ta có thể thu được nhân tử của N bằng thuật toán Euclid, nếu $z \neq \pm s$. Mặt khác, do thuật toán không phân biệt s với những nghiệm khác, mà một phần tử v nguyên tố cùng nhau với N là số chính phương theo $mod\ N$, sẽ có đúng bốn căn bậc hai, nên chúng ta có thể kết luận rằng, với xác suất $1/2$, $\gcd(z - s, N)$ cung cấp một thừa số của N.

B. Tấn công sử dụng thông điệp được lựa chọn thích nghi lên lược đồ chữ ký Fiat-Shamir

Trong phần này, chúng tôi sử dụng ý tưởng chứng minh độ an toàn cho lược đồ chữ ký Schnorr theo Bổ đề 5 trong [3] của Pointcheval để chứng minh cho Nhận xét 6 trong [2] về độ an toàn của lược đồ chữ ký Fiat-Shamir trước tấn công sử dụng thông điệp được lựa chọn thích nghi. Trước tiên, ta có khẳng định sau:

Mệnh đề 6. *Bộ ký* Σ *trong lược đồ chữ ký Fiat-Shamir có thể bị mô phỏng theo một phân bố không phân biệt được.*

Chứng minh. Đầu tiên, chúng ta sẽ đưa ra một mô phỏng S để tạo ra các chữ ký thỏa mãn điều kiện xác minh của lược đồ Fiat-Shamir. Tiếp theo, chứng minh S là một mô phỏng "tốt", nghĩa là, bộ ký Σ bị mô phỏng bởi S theo một phân bố không phân biệt được.

Chúng ta bắt đầu xây dựng mô phỏng S như sau: để mô phỏng một chữ ký của thông điệp m, lấy $(e_1 e_2 \dots e_k)$ là xâu ngẫu nhiên có độ dài k bit và k số $y_i \in_R \mathbb{Z}/N\mathbb{Z}$, với $i \in \{1,2,\dots,k\}$. Chúng ta cần đưa ra k số x_i sao cho $y_i^2 = x_i v^{e_i}$, với $i \in \{1,2,\dots,k\}$. Theo như lập luận trong chứng minh của Định lý 5, ta có thể coi v nguyên tố cùng nhau với N. Do đó, có thể lấy $x_i = y_i^2 v^{-e_i}$, với $i \in \{1,2,\dots,k\}$. Như vậy, chúng ta thu được bộ ba (σ_1, h, σ_2) với $\sigma_1 = (x_1, x_2, \dots, x_k)$, $h = (e_1 e_2 \dots e_k)$ và $\sigma_2 = (y_1, y_2, \dots, y_k)$, là một chữ ký thỏa mãn điều kiện xác minh $y_i^2 = x_i v^{e_i}$, với $i \in \{1,2,\dots,k\}$.

Tiếp theo, chúng ta sẽ chứng minh S có khả năng mô phỏng Σ theo một phân bố không phân biệt được. Thật vậy, gọi A là không gian các chữ ký được tạo ra bởi Σ, ta có:

$$A = \left\{ (\sigma_1, h, \sigma_2) \;\middle|\; \begin{array}{c} \frac{r_i \in_R \mathbb{Z}}{N\mathbb{Z}}, \ \forall i \in \{1,\dots,k\} \\ h = (e_1 e_2 \dots e_k) \in_R \{0,1\}^k \\ \sigma_1 = (x_1, x_2, \dots, x_k), x_i = r_i^2 mod N \\ \sigma_2 = (y_1, y_2, \dots, y_k), \quad y_i = r_i s^{e_i} mod N \end{array} \right\}$$

dễ thấy, số chữ ký trong không gian A là $N^k \cdot 2^k$ (tính cả trường hợp trùng nhau) do không gian A được sinh ra trực tiếp bởi việc lấy $h \in_R \{0,1\}^k$ và các $r_i \in \mathbb{Z}/N\mathbb{Z}$, với $i = 1 \dots k$ và có $N^k \cdot 2^k$ bộ $(h, r_1, r_2, \dots, r_k)$ bằng cách lấy ngẫu nhiên như vậy.

Gọi B là không gian các chữ ký được tạo ra bởi S, ta có:

$$B = \left\{ (\sigma_1, h, \sigma_2) \;\middle|\; \begin{array}{c} \frac{y_i \in_R \mathbb{Z}}{N\mathbb{Z}}, \ \forall i \in \{1,\dots,k\} \\ h = (e_1 e_2 \dots e_k) \in_R \{0,1\}^k \\ \sigma_2 = (y_1, y_2, \dots, y_k) \\ \sigma_1 = (x_1, x_2, \dots, x_k), \ x_i = y_i^2 v^{e_i} \ mod \ N \end{array} \right\}$$

Tương tự như trên, chúng ta cũng có số chữ ký trong không gian B là $N^k \cdot 2^k$.

Do số chữ ký tạo ra từ Σ và S là như nhau, nên để chứng minh Σ có thể bị S mô phỏng theo một phân bố không phân biệt được, chúng ta sẽ chỉ ra rằng với chữ ký hợp lệ $(\sigma_1^{(0)}, h^{(0)}, \sigma_2^{(0)})$, trong đó,

$$\sigma_1^{(0)} = (x_1^{(0)}, x_2^{(0)}, \dots, x_k^{(0)},$$

$$h^{(0)} = \left(e_1^{(0)} e_2^{(0)} \dots e_k^{(0)}\right),$$

$$\text{và } \sigma_2^{(0)} = \left(y_1^{(0)}, y_2^{(0)}, \dots, y_k^{(0)}\right),$$

thì số lần xuất hiện của nó trong A và B là như nhau. Trước khi chứng minh điều này, chúng ta có đánh giá sau: Xét một số chính phương $b \ mod \ N$, nếu $b = 0 \ mod \ N$ thì b chỉ có duy nhất một căn bậc hai; nếu $N > gcd(b, N) > 1$ thì b có đúng 2 căn bậc hai; trường hợp còn lại, $gcd(b, N) = 1$ thì b sẽ có 4 căn bậc hai.

Nhờ nhận xét này, ta chia $\{1,2,\dots,k\}$ thành ba tập chỉ số I, J, L, trong đó: I là tập chỉ số sao cho $x_i^{(0)} = 0 \ mod \ N, \ \forall i \in I$; J là tập chỉ số sao cho $N > gcd\left(x_j^{(0)}, N\right) > 1, \ \forall j \in J$; L là tập chỉ số sao cho $gcd\left(x_l^{(0)}, N\right) = 1, \ \forall l \in L$.

Khi đó, xét trong quá trình ký: Với $i \in I$, số lần xuất hiện r_i để $r_i^2 = x_i^{(0)} mod N$ là 1; Với $j \in J$, số lần xuất hiện r_j để $r_j^2 = x_j^{(0)} \ mod \ N$ là 2; Với $l \in L$, số lần xuất hiện r_l để $r_l^2 = x_l^{(0)} mod N$ là 4; Số lần xuất hiện h để $h = h^{(0)}$ cũng là 1.

Do đó, số lần xuất hiện của chữ ký $(\sigma_1^{(0)}, h^{(0)}, \sigma_2^{(0)})$ trong A là $2^{|J|} \cdot 4^{|L|}$.

Tiếp theo, ta xét số lần $(\sigma_1^{(0)}, h^{(0)}, \sigma_2^{(0)})$ xuất hiện trong B (cùng với chú ý $gcd(v, N) = 1$): Số lần xuất hiện h để $h = h^{(0)}$ cũng là 1; *Với* $i \in I$, số lần xuất hiện y_i để $y_i^2 = x_i^{(0)} \cdot v^{e_i^{(0)}} \ mod \ N$ là 1; *Với* $j \in J$, số lần xuất hiện y_j để $y_j^2 = x_j^{(0)} \cdot v^{e_j^{(0)}} \ mod \ N$ là 2; *Với* $l \in L$, số lần xuất hiện y_l để $y_l^2 = x_l^{(0)} \cdot v^{e_l^{(0)}} \ mod \ N$ là 4.

Do đó, số lần xuất hiện của chữ ký $(\sigma_1^{(0)}, h^{(0)}, \sigma_2^{(0)})$ trong B cũng là $2^{|J|} \cdot 4^{|L|}$.

Như vậy, chúng ta thu được kết quả A và B là hai phân bố đồng nhất (đây là trường hợp đặc biệt của hai phân bố không phân biệt được theo thống kê khi tổng độ lớn của các hiệu xác suất bằng 0 thay vì lượng không đáng kể). Do đó, theo Mục II.D thì S có thể mô phỏng Σ theo một phân bố không phân biệt được.

Với việc tồn tại bộ mô phỏng S được chỉ ra như trong Mệnh đề trên, ta nhận được hệ quả sau:

Hệ quả 7. *Xác định một tấn công sử dụng thông điệp được lựa chọn thích nghi trong mô hình bộ tiên tri ngẫu nhiên, nếu tồn tại trong lược đồ chữ ký Fiat-Shamir một giả mạo với xác suất đáng kể, thì phân tích nhân tử có thể được thực hiện trong thời gian đa thức.*

Chứng minh. Sử dụng Mệnh đề 6 vào Bổ đề 4, ta suy ra kẻ tấn công có thể nhận được hai chữ ký

hợp lệ $(m, \sigma_1, h, \sigma_2)$ và $(m, \sigma_1, h', \sigma_2')$ sao cho $h \neq h'$, với một xác suất đáng kể, trong thời gian đa thức. Khi đó, lập luận hoàn toàn như trong chứng minh của Định lý 5, ta chỉ ra được bài toán phân tích nhân tử là có thể giải được trong thời gian đa thức.

Như vậy, với giả thiết về tính khó giải của bài toán phân tích nhân tử, thì Hệ quả 7 chỉ ra lược đồ chữ ký Fiat-Shamir là an toàn trước tấn công sử dụng thông điệp được lựa chọn thích nghi.

IV. KẾT LUẬN

Bằng việc nghiên cứu, tìm hiểu độ an toàn "chứng minh được" của lược đồ chữ ký dựa trên ý tưởng chứng minh trong các bài viết của Pointcheval, cụ thể là việc tham khảo chứng minh độ an toàn trên lược đồ chữ ký Shnorr, chúng tôi đã chứng minh chi tiết cho [2, nhận xét 6] về độ an toàn của lược đồ chữ ký Fiat-Shamir trước tấn công sử dụng thông điệp được lựa chọn thích nghi. Để thực hiện điều này, chúng tôi đã phát biểu Mệnh đề 6 về sự tồn tại của một bộ mô phỏng cho bộ ký trong lược đồ này. Từ đó, kết hợp với [3, Bổ đề 4], chúng tôi thu được kết quả là lược đồ Fiat-Shamir an toàn trước tấn công sử dụng thông điệp được lựa chọn thích nghi trong mô hình bộ tiên tri ngẫu nhiên, với giả thiết về tính khó giải của bài toán phân tích nhân tử.

Tuy việc nghiên cứu mới chỉ xét trên đối tượng cụ thể là lược đồ chữ ký Fiat-Shamir, nhưng cũng đã cung cấp cách nhìn rõ hơn về vấn đề độ an toàn của các lược đồ chữ ký. Chúng tôi hy vọng sẽ tiến xa hơn trong việc nghiên cứu về độ an toàn cho lược đồ chữ ký theo hướng này.

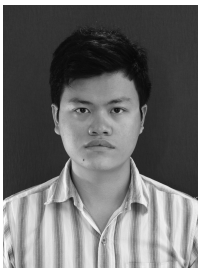
TÀI LIỆU THAM KHẢO

[1]. A. Fiat and A. Shamir. "How to Prove Yourself: practical solutions of identification and signature problems". In A. M. Odlyzko, editor, Advances in Cryptology - Proceedings of CRYPTO '86, vol. 263 of Lecture Notes in Computer Science, pp. 186-194, Santa Barbara, California, 1987. Springer-Verlag.

[2]. D. Pointcheval and J. Stern. "Security Proofs for Signature Schemes". In Eurocrypt'96, LNCS1070, pp. 387-398. Springer-Verlag, Berlin, 1996.

[3]. David Pointcheval and Jacques Stern. "Security Arguments for Digital Signatures and Blind Signatures", J. Cryptology, vol. 13, pp. 361-396, 2000.

SƠ LƯỢC VỀ TÁC GIẢ



CN. Triệu Quang Phong

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

E-mail: phongtrieu53@gmail.com

Tốt nghiệp ngành Toán học, Đại học Khoa học tự nhiên - Đại học Quốc gia Hà Nội năm 2014.

Hướng nghiên cứu hiện nay: Toán học, khoa học mật mã.

ThS. Võ Tùng Linh

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

E-mail: beathovenvn@gmail.com

Tốt nghiệp chuyên ngành Toán học, Đại học Khoa học tự nhiên - Đại học Quốc gia Hà Nội năm 2005. Nhận bằng Thạc sĩ Lý thuyết số và Đại số, Đại học Khoa học tự nhiên –Đại học Quốc gia Hà Nội năm 2014.

Hướng nghiên cứu hiện nay: Mật mã khóa công khai.