MỘT BIẾN THỂ AN TOÀN CHỨNG MINH ĐƯỢC CỦA LƯỢC ĐỒ CHỮ KÝ SỐ EdDSA

Đinh Tiến Thành[1*], Võ Tùng Linh[2]

Tóm tắt: *Bài báo đề xuất lược đồ chữ ký số R-EdDSA, là một biến thể ngẫu nhiên hóa của lược đồ EdDSA. Với giả thiết hàm băm H được mô hình hóa như một bộ tiên tri ngẫu nhiên và bài toán khó logarit rời rạc trên đường cong elliptic. Bài báo đã chứng minh rằng, lược đồ chữ ký số R-EdDSA không thể bị giả mạo tồn tại dưới các tấn công lựa chọn thông điệp thích nghi.*

Từ khóa: Lược đồ chữ ký số EdDSA; Lược đồ R-EdDSA; Phép biến đổi Fiat-Shamir; An toàn chứng minh được; Đường cong Edwards xoắn.

1. 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 [3] 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 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 được chấp nhận 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 được chấp nhận sẽ góp phần tạo nên chữ ký trên thông điệp. Ta sẽ cụ thể hóa ý tưởng này trong các phần sau.

Lược đồ chữ ký EdDSA được giới thiệu lần đầu vào năm 2012 trong tài liệu [1] xây dựng trên đường cong ký hiệu Curve25519, một đường cong Edwards xoắn với $a=-1, d=-121665/121666$ định nghĩa trên đường hữu hạn $\mathbb{F}_q$ với $q=2^{255}-19$, là một biến thể của lược đồ chữ ký số Schnorr. Sau đó, các tác giả công bố tài liệu [2], trong đó mở rộng việc mô tả lược đồ EdDSA cho các đường cong elliptic dạng Edwards xoắn với các tham số hợp lý. Đến năm 2017, lược đồ chữ ký số EdDSA được ban hành như một chuẩn Internet [4].

Mặc dù lược đồ chữ ký số EdDSA, theo [4] được đánh giá là một lược đồ chữ ký số an toàn, có hiệu suất thực hiện cao đối với nhiều nền tảng khác nhau, có lợi thế kháng lại tấn công kênh kề… Tuy nhiên, cho đến nay vẫn chưa có một chứng minh lý thuyết về độ an toàn chứng minh được của lược đồ chữ ký số EdDSA.

Với mục tiêu xây dựng một lược đồ chữ ký số mà vẫn giữ nguyên được "hầu hết" các ưu điểm của lược đồ EdDSA, đồng thời chỉ ra độ an toàn chứng minh được, bài báo trình bày một biến thể của lược đồ EdDSA bằng cách ngẫu nhiên hóa qua trình sinh chữ ký (lược đồ chữ ký số R-EdDSA) và chỉ ra tính an toàn chứng minh được của lược đồ biến thể này trong mô hình bộ tiên tri ngẫu nhiên.

2. CƠ SỞ TOÁN HỌC

2.1. Lược đồ định danh

Một lược đồ định danh được định nghĩa một cách hình thức như sau:

Định nghĩa 1 ([5, Định nghĩa 8.1]). Một lược đồ định danh bao gồm ba thuật toán thời gian đa thức, xác suất (*Gen*, *P*, *V*) sao cho:

- Thuật toán sinh khóa ngẫu nhiên ***Gen*** nhận đầu vào là tham số san toàn κ và trả về một cặp khóa (*pk*, *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" $b'=0$ có nghĩa là "bác bỏ".

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

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

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

Rõ ràng, một lược đồ định danh chính là một phương thức để người tham gia P (gọi là *người chứng minh*) thuyết phục người tham gia khác, ký hiệu V (gọi là *người xác minh*), rằng anh ta chính là P như đã khẳng định.

Một lược đồ định danh được gọi 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 anh ta 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 $\mathbf{Trans}_{sk,pk}(.)$ 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 $\langle P(sk),V(pk)\rangle$ 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 nhập 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 ([5, Định nghĩa 8.2])**.** Một lược đồ định danh (*Gen*, *P*, *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) $\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)$.

$$\Pr\left[\begin{matrix}(pk)\leftarrow Gen(1^{\kappa})\\ state\leftarrow \mathcal{A}_1^{Tran_{sk,pk}(.)}(pk)\end{matrix}:\langle \mathcal{A}_2(state),V(pk)\rangle=1\right]$$

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 sau đó sẽ cố mạo danh P trước người xác minh (trung thực) nào đó.

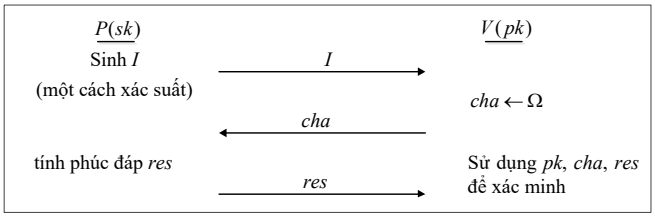
Tiếp theo, chúng tôi trình bày định nghĩa về một lớp các lược đồ định danh 3-pha với một số tính chất đặc trưng, gọi là lược đồ định danh chính tắc.

Định nghĩa 3 (Lược đồ định danh chính tắc, [5]). 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" *cha* được gửi bởi V, và phúc đáp cuối cùng *res* được gửi bởi P.

- Ta giả thiết thách thức *cha* được chọn đều từ một tập Ω nào đó (nói chung, $\Omega = \{\Omega_K\}$ phụ thuộc vào tham số an toàn κ, 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 các hiệu quả xem liệu V đã chấp nhận sau lần thực thi đó hay chưa. Ta nói (pk, I, cha, res) là một bản ghi được 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, cha, res) là một bản ghi được 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 P(*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 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 minh họa bởi hình 1 dưới đây.



Hình 1. *Lược đồ định danh chính tắc.*

2.2. Phép biến đổi Fiat-Shamir

Trong [3], các tác giả Amos Fiat và Adi Shamir đã đề xuất một phương pháp xây dựng lược đồ chữ ký số từ các lược đồ định danh, gọi là *Phép biến đổi Fiat-Shamir*. Chi tiết của phương pháp này được mô tả như sau:

Phép biến đổi Fiat-Shamir ([5, Const.8.1])

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

Sinh khóa: Chạy $Gen(1^\kappa)$ để sinh cặp khóa công khai/bí mật tương ứng là (*pk*, *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 *P*(*sk*) để sinh một thông điệp khởi tạo *I;*
- Tính *cha* = *H*(*I*, *M*);
- Tính câu phúc đáp thích hợp *res* cho "thách thức" *cha* với việc sử dụng *P*(*sk*);
- Đưa ra chữ ký là (*I*, *res*).

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

- Tính *cha* = *H*(*I*, *M*);
- Chấp nhận chữ ký nếu và chỉ nếu (*pk*, *I*, *cha*, *res*) là một bản ghi được chấp nhận.

2.3. Mối liên hệ giữa độ an toàn của lược đồ định danh và lược đồ chữ ký số

Ký hiệu $\Pi = (Gen, P, V)$ là một lược đồ định danh chính tắc 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 chính tắc Π phải thỏa mãn các điều kiện gì. Định lý dưới đây

sẽ trả lời các câu hỏi đó.

Định lý 1 ([5, Định lý 8.1]). Cho Π = (Gen, P, V) là một lược đồ định danh chính tắc 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.

Bây giờ, chúng tôi nhắc lại 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** và tiêu chuẩn **mạnh đặc biệt.** Cụ thể**,** tiêu chuẩn này được định nghĩa như sau.

Định nghĩa 4 ([5, Định nghĩa 8.3]). Một lược đồ định danh Π là không lộ tri thức cho người xác minh trung thực 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:

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

và

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

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

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

$$\Pr\left[\begin{matrix}(\mathrm{pk},\mathrm{sk})\leftarrow\mathrm{Gen}(1^K)\\ (\mathrm{I},c_1,r_1,c_2,r_2)\leftarrow\mathrm{A}(\mathrm{pk})\end{matrix} : \begin{matrix}c_1\neq 2\\ \text{và}\\ (\mathrm{pk},\mathrm{I},c_1,r_1),(\mathrm{pk},\mathrm{I},c_2,r_2)\\ \text{đều là các bản ghi được chấp nhận}\end{matrix}\right]$$

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 chính tăc.

Định lý 2 ([5, Định lý 8.2]). Giả sử lược đồ định danh chính tắc 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 A = (A_1, A_2), ta có:

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

với hàm không đáng kể $\mu(.)$ nào đó. Cụ thể hơn, nếu $|\Omega_\kappa| = \omega(poly(\kappa))$ thì Π là an toàn kháng lại các tấn công bị động.

Từ các định lý 1 và định lý 2, ta có hệ quả sau đây:

Hệ quả 1. Cho $\Pi = (Gen, P, V)$ *là một lược đồ định danh chính tắc 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 là hiển nhiên từ các định lý 1 và định lý 2. □

3. BIẾN THỂ CỦA LƯỢC ĐỒ CHỮ KÝ SỐ EDDSA

3.1. Lược đồ chữ ký số R-EdDSA

Trong mục này mô tả một phiên bản ngẫu nhiên hóa của lược đồ chữ ký số EdDSA, gọi là lược đồ chữ ký số R-EdDSA. Thực tế, việc "ngẫu nhiên hóa" lược đồ chữ ký số EdDSA là ngẫu nhiên hóa quá trình sinh chữ ký bằng cách thêm một thành phần ngẫu nhiên vào quá trình sinh khóa bí mật tức thời cho mỗi lần ký.

Các tham số miền và quy tắc ghi mã của lược đồ R-EdDSA

Lược đồ chữ ký số R-EdDSA sử dụng các tham số miền và quy tắc ghi mã thỏa mãn các yêu cầu giống như đối với lược đồ chữ ký số EdDSA trong [4]. Cụ thể như sau:

1. Một số nguyên tố mạnh *p*. lược đồ R-EdDSA sử dụng một đường cong elliptic trên trường hữu hạn $\mathbb{F}_p$;
2. Một số nguyên dương b thỏa mãn $2^{b-1} > p$. Khóa công khai của R-EdDSA cố độ lớn chính xác *b* bit, còn chữ ký R-EdDSA có độ lớn chính xác $2b$ bit;
3. Một quy tắc ghi mã *(b-1)*-bit các phần tử của trường mã hữu hạn $\mathbb{F}_p$;
4. Một hàm băm mật mã *H* với đầu ra có độ lớn $2b$ bit;
5. Một số nguyên dương $c \in \{2,3\}$ các giá trị vô hướng bí mật của lược đồ R-EdDSA là bội của 2^c;
6. Một số nguyên dương *n* thỏa mãn $c \le n \le b$. Các giá trị vô hướng bí mật của lược đồ R-EdDSA có độ lớn chính xác *(n+1)* bit với bit cao nhất (vị trí 2^n) luôn được thiết lập bằng 1 và *c* bit thấp nhất được thiết lập bằng 0;
7. Một phần tử $a \in \mathbb{F}_p$ thỏa mãn $a \neq 0$ và *a* là một số chính phương trong $\mathbb{F}_p$;
8. Một phần tử $d \in \mathbb{F}_p$ thỏa mãn *d* không phải là số chính phương trong $\mathbb{F}_p$;
9. Một điểm $B \neq (0,1) \in E(\mathbb{F}_p) = \{(x,y), \mathbb{F}_p \times \mathbb{F}_p : ax^2 + y^2 = 1 + dx^2y^2\}$ gồm các điểm xác định trên trường hữu hạn $\mathbb{F}_p$ của đường cong Edwards xoắn $E : \mathrm{a}x^2 + y^2 = 1 + dx^2y^2$;
10. Một số nguyên tố lẻ *l* thỏa mãn $lB = 0$ và $2^c l = \#E(\mathbb{F}_p)$;
11. Một số nguyên $S \in \{0,1,...,l-1)$ được ghi mã thành một xâu có độ lớn *b* bit, ký hiệu là $\underline{S}$;
12. Mỗi điểm $P = (x,y) \in E(\mathbb{F}_p)$ được ghi mã thành một xâu có độ lớn *b* bit, ký hiệu $\underline{P}$, bằng cách nối xâu kết quả ghi mã *(b-1)* bit của giá trị tọa độ *y* với bit 1 nếu tọa độ *x* là âm, ngược lại thì nối với bit 0.

Dưới đây chúng tôi mô tả 3 thuật toán sinh khóa, sinh chữ ký và xác minh chữ ký của lược đồ chữ ký số R-EdDSA.

Thuật toán sinh khóa R-EdDSA

1. Sinh ngẫu nhiên một khóa bí mật (dài hạn) R-EdDSA là một số nguyên *k* có độ lớn *b* bit.
2. Tính $H(k) = (h_0, h_1, ..., h_{2b-1})$.
3. Tính $s = 2^n + \sum_{c \le i < n} 2^i h_i$.
4. Tính $A = sB$ trên đường cong elliptic *E*.
5. Khóa công khai (dài hạn) R-EdDSA là kết quả ghi mã $\underline{A}$ của điểm *A*.

Thuật toán sinh chữ ký R-EdDSA

Để ký một thông điệp *M* với khóa bí mật *k*, ta thực hiện như sau:

1. Sinh ngẫu nhiên giá trị $m \in \mathbb{Z}_l$.
2. Tính $r = H(m, h_b, ..., h_{2b-1}, M) \in \{0,1,...2^{2b} - 1\}$. Ở đây, *r* được xem như một số nguyên thuộc $\{0,1,...2^{2b} - 1\}$.
3. Tính $R = rB$ trên đường cong elliptic *E* và ghi mã điểm *R* thành $\underline{R}$.

4. Tính $h = H(\underline{R}, \underline{A}, M)$.
5. Tính $S = (r + hs) \bmod l$ và ghi mã giá trị này dưới dạng $\underline{S}$.
6. Đưa ra chữ ký trên thông điệp M với khóa bí mật k là xâu $(\underline{R}, \underline{S})$ có độ lớn $2b$ bit.

Thuật toán xác minh chữ ký R-EdDSA

Để xác minh chữ ký $(\underline{R}, \underline{S})$ được tạo ra trên thông điệp M với khóa bí mật k, người xác minh sử dụng khóa công khai $\underline{A}$ tương ứng và thực hiện như sau:

1. Khôi phục và kiểm tra các điểm A, R thuộc đường cong elliptic E từ $\underline{A}$, $\underline{R}$ và số nguyên $S \in \{0,1,...l-1\}$ từ $\underline{S}$.
2. Tính $h = H(\underline{R}, \underline{A}, M)$.
3. Kiểm tra hệ thức $2^c SB = 2^c R + 2^c hA$ trên đường cong elliptic E. Nếu đúng thì "chấp nhận" chữ ký, ngược lại thì "không chấp nhận" chữ ký.

Rõ ràng, với chữ ký được sinh một cách đúng đắn theo thuật toán sinh chữ ký R-EdDSA, từ $lB = 0$ trên đường cong elliptic E và $h = H(\underline{R}, \underline{A}, M) \bmod l$, ta có

$$\begin{aligned} 2^c R + 2^c hA &= 2^c (rB) + 2^c (hs)B \\ &= 2^c ((r + hs) \bmod l)B \\ &= 2^c SB \end{aligned}$$

3.2. So sánh lược đồ R-EdDSA với một số biến thể khác của lược đồ EdDSA

Trong tài liệu [6], tác giả Trevor Perrin đã đưa ra hai biến thể của lược đồ chữ ký số EdDSA, ký hiệu là VEdDSA và VXEdDSA. Điểm tương đồng giữa các lược đồ chữ ký số mô tả trong [6] và lược đồ R-EdDSA của chúng tôi, mặc dù việc nghiên cứu là độc lập với nhau, là đều đưa thêm yếu tố ngẫu nhiên vào việc tính khóa bí mật tức thời mỗi lần ký. Tuy nhiên, với các lược đồ VEdDSA và VXEdDSA, thành phần ngẫu nhiên là một dữ liệu ngẫu nhiên an toàn có độ lớn 64 byte, còn trong lược đồ R-EdDSA chúng tôi lựa chọn giá trị ngẫu nhiên là một số ngẫu nhiên có độ lớn b-bit theo tham số b được sử dụng. Hơn nữa, khi tính giá trị bí mật tức thời, các lược đồ trong [6] đưa cả giá trị vô hướng bí mật s vào trong hàm băm, khác với việc sử dụng một phần chuỗi băm đầu ra của khóa bí mật k như trong lược đồ EdDSA và R-EdDSA.

Một điều quan trọng là, mặc dù cũng xây dựng các biến thể ngẫu nhiên hóa của lược đồ chữ ký số EdDSA nhưng tác giả của [6] không chỉ ra độ an toàn chứng minh được của các biến thể đó. Còn với lược đồ R-EdDSA, trong phần tiếp theo, chúng tôi chỉ ra lược đồ này là an toàn chứng minh được trong mô hình bộ tiên tri ngẫu nhiên.

4. ĐỘ AN TOÀN CHỨNG MINH ĐƯỢC CỦA LƯỢC ĐỒ CHỮ KÝ SỐ R-EDDSA TRONG MÔ HÌNH BỘ TIÊN TRI NGẪU NHIÊN

Mục tiêu của phần này là chúng tôi chỉ ra độ an toàn chứng minh được của lược đồ R-EdDSA trong mô hình bộ tiên tri ngẫu nhiên (ROM). Ý tưởng của chúng tôi là xây dựng một lược đồ định danh chính tắc mà từ nó ta nhận được lược đồ chữ ký số R-EdDSA qua việc áp dụng phép biến đổi Fiat-Shamir. Sau đó chỉ ra lược đồ định danh chính tắc đã xây dựng thỏa mãn các điều kiện của định lý 2.

Trước tiên, chúng tôi xây dựng một lược đồ định danh Π như mô tả dưới đây. Các tham số sử dụng trong lược đồ định danh này giống như các tham số của lược đồ R-EdDSA.

Lược đồ định danh Π = (*Gen*, *P*, *V*)

Sinh khóa *Gen*: Sinh ngẫu nhiên khóa bí mật k có độ lớn b-bit, tính $H(k) = (h_0, h_1, ..., h_{2b-1})$ và $s = 2^n + \sum_{c \le i < n} 2^i h_i$. Tính $A = sB$ trên đường cong elliptic E và ghi mã thành $\underline{A}$. Cặp khóa bí mật/công khai là $(k, \underline{A})$.

Thông điệp khởi tạo của người chúng minh P: Chọn ngẫu nhiên $m \leftarrow \mathbb{Z}_l$, tính

$$r = H(m, h_b, ...h_{2b-1}, text),$$

sau đó gửi thông điệp khởi tạo $I = (\underline{R}, \underline{A})$ đến người xác minh V, trong đó, $\underline{R}$ là kết quả ghi mã của điểm $R = rB$ trên đường cong elliptic E. Ở đây *text* là thông tin tùy chọn, có thể là một thông điệp M, hoặc định danh của người chứng minh, hoặc một số thứ tự, v.v.

Thách thức của người xác minh V: Chọn ngẫu nhiên đều $T \leftarrow \{0,1,...,2^{2b}-1\}$ và gửi T tới người chứng minh P như là một giá trị thách thức.

Phúc đáp của người chứng minh P: Tính $S = (r + Ts) \bmod \ell$ với $s = 2^n + \sum_{c \le i < n} 2^i h_i$, ghi mã thành $\underline{S}$ và gửi $\underline{S}$ tới người xác minh V như là phúc đáp của mình đối với thách thức T.

Tiêu chuẩn chấp nhận: Người xác minh V khôi phục R, S, A từ $\underline{R}$, $\underline{A}$, $\underline{S}$ và chấp nhận $((\underline{R}, \underline{A}), T, \underline{S})$ là bản ghi tương ứng với khóa công khai $\underline{A}$ nếu và chỉ nếu R, A là các điểm của đường cong elliptic E, T, $S \in \mathbb{Z}_\ell$ và

$$2^c SB - 2^c TA = 2^c R$$

trên đường cong elliptic E.

Dễ thấy, lược đồ định danh $\Pi = (Gen, P, V)$ là một lược đồ định danh chính tắc.

Nhận xét 1. Dễ thấy rằng, bằng cách áp dụng phép biến đổi Fiat-Shamir lên lược đồ định danh chính tắc Π, ta nhận được lược đồ chữ ký số R-EdDSA.

Định lý dưới đây chỉ ra lược đồ định danh chính tắc $\Pi = (Gen, P, V)$ thỏa mãn tiêu chuẩn không lộ tri thức cho người xác minh trung thực và tính mạnh đặc biệt.

Định lý 3. *Giả sử hàm H được mô hình hóa như một bộ tiên tri ngẫu nhiên. Lược đồ định danh chính tắc Π = (Gen, P, V) thỏa mãn tiêu chuẩn không lộ tri thức cho người xác minh trung thực. Hơn nữa, nếu bài toán logarit rời rạc trên đường cong elliptic E được giả thiết là khó thì lược đồ Π cũng thỏa mãn tiêu chuẩn mạnh đặc biệt.*

Chứng minh. Trước tiên chúng tôi chứng minh rằng, với hàm băm H được mô hình hóa như một bộ tiên tri ngẫu nhiên, lược đồ định danh chính tắc Π thỏa mãn tiêu chuẩn không lộ tri thức cho người xác minh trug thực. Để thực hiện điều này, chúng tôi xây dựng một thuật toán ***Sim*** với mô tả như sau:

Thuật toán Sim:

Thuật toán được cho trước hàm băm H (như một bộ tiên tri ngẫu nhiên), khóa công khai $\underline{A}$ với $A=sB$ và một thách thức T được chọn ngẫu nhiên đều từ $\{0,1,….,2^{2b}-1\}$.

1. Chọn ngẫu nhiên đều $t \leftarrow \mathbb{Z}_\ell$ và tính $S = H(t) \bmod \ell$.
2. Tính $R = SB - TA$ trên đường cong elliptic E.
3. Đưa ra bản ghi (I, T, S) với $I = (\underline{R}, \underline{A})$.

Ta có thể chứng minh được thuật toán ***Sim*** thỏa mãn yêu cầu như trong định nghĩa 4. Để có điều này, ta sẽ chỉ ra thuật toán ***Sim*** mô tả một cách hoàn hảo một lần thực thi thật sự của lược đồ định danh chính tắc Π ứng với khóa công khai $\underline{A}$ đã cho (tương ứng với khóa bí mật k) và một thách thức $T \in_R \{0,1,...,2^{2b}-1\}$.

Thật vậy, trong một lần thực thi thực sự của lược đồ định danh Π với cặp khóa bí mật/công khai $(k, \underline{A})$ ta có:

$$R = (H(m, h_b, ..., h_{2b-1}, text) \bmod \ell) B$$

và

$$S = \left(H(m, h_b, ..., h_{2b-1}, \text{text}) + T(2^n + \sum_{c \le i < n} 2^i h_i) \right) \bmod \ell$$

trong đó, các giá trị h_i được xác định từ $H(k) = (h_0, h_1, ..., h_{2b-1})$, m được chọn ngẫu nhiên

trong $\mathbb{Z}_\ell$, T được chọn ngẫu nhiên đều từ $\{0,1,\ldots, 2^{2b}\text{-}1\}$ và *text* là một thành phần tùy chọn. Để so sánh, ta xét các giá trị tương ứng trong một lần thực thi thuật toán ***Sim***

$$\begin{aligned} R &= (H(t) \bmod \ell)B - TA \\ &= ((H(t) - Ts) \bmod \ell)B \end{aligned} \qquad (\text{vì } A = sB)$$

và $$S = H(t) \bmod l$$

với t được chọn ngẫu nhiên đều từ $\mathbb{Z}_l$. Khi đó, với giả thiết hàm băm H được mô hình hóa như một bộ tiên tri ngẫu nhiên, T được chọn nhẫu nhiên đều trong $\{0,1,\ldots, 2^{2b}\text{-}1\}$ và các điểm B, $A=sB$ được cố định trước trên đường cong eliptic E, ta suy ra phân bố xác suất của (R, S) trong cả hai trường hợp là không thể phân biệt được về mặt tính toán. Nói cách khác, ta không thể phân biệt được (R, S) là nhận được từ thuật toán ***Sim*** hay từ một lần thực thi thật sự của lược đồ định danh Π. Điều này kéo theo phân phân bố xác suất của bản ghi $((\underline{R}, \underline{A}), T, \underline{S})$ là không thể phân biệt được về mặt tính toán trong cả trường hợp thuật toán ***Sim*** và một lần thực thi thực sự của lược đồ định danh Π.

Để chỉ ra những lập luận trên là đúng, một cách cụ thể ta sẽ ước lượng phân bố xác suất đầu ra (R, S) của thuật toán ***Sim*** và một lần thực thi thực sự lược đồ định danh Π. Đối với đại lượng R, lược đồ định danh Π tính theo công thức

$$R = \left(H\left(m, h_b, \ldots, h_{2b-1}, text\right) \bmod l\right)B,$$

còn thuật toán ***Sim*** tính R theo công thức

$$R = \left(H(t) \bmod l\right)B - TA = \left((H(t) - Ts) \bmod l\right)B,$$

trong đó T được chọn ngẫu nhiên đều từ $\{0,1,\ldots, 2^{2b}\text{-}1\}$ độc lập với hàm băm H, $t \in_R \mathbb{Z}_l$ và s là giá trị cho trước. Do điểm B đã cố định trước nên để so sánh phân bố của R được đưa ra bởi hai thuật toán trên, ta chỉ cần ước lượng xác suất để $H\left(m, h_b, \ldots, h_{2b-1}, text\right) \bmod l$ và $\left(H(t) - Ts\right) \bmod l$ cho cùng một giá trị trong $\mathbb{Z}_l$.

Đặt $$2^{2b} = u.l + v,$$

với $1 \le u \in \mathbb{Z}$ và $0 \le v \le l-1$. Do $H(.) \in \left\{0,1,\ldots,2^{2b-1}\right\}$, ta dễ dàng chỉ ra được:

- Với mọi $0 \le i \le v-1$,

$$p_i = \Pr\left[H(m, h_b, \ldots, h_{2b-1,} text) \bmod l = i\right] = \frac{u+1}{2^{2b}}$$

- Với mọi $v \le j \le l-1$,

$$p_j = \Pr\left[H\left(m, h_b, \ldots, h_{2b-1,} text\right) \bmod l = j\right] = \frac{u}{2^{2b}}$$

Trong khi đó, với mọi $0 \le z \le l-1$ ta có

$$\begin{aligned} P_z &= \Pr\left[\left(H\left(t\right) - Ts\right), \bmod l = z\right] \\ &= \sum_{w=0}^{l-1} \Pr\left[H\left(t\right) \bmod l = w\right] \cdot \Pr\left[Ts \bmod l = \left(z+w\right) \bmod l\right] \\ &= \sum_{w=0}^{v-1} \Pr\left[H\left(t\right) \bmod l = w\right] \cdot \Pr\left[Ts \bmod l = \left(z+w\right) \bmod l\right] \\ &+ \sum_{w=v}^{l-1} \Pr\left[H\left(t\right) \bmod l = w\right] \cdot \Pr\left[Ts \bmod l = \left(z+w\right) \bmod l\right] \\ &= \frac{u+1}{2^{2b}} \sum_{w=0}^{v-1} \Pr\left[Ts \bmod l = \left(z+w\right) \bmod l\right] + \frac{u}{2^{2b}} \sum_{w=v}^{l-1} \Pr\left[Ts \bmod l = \left(z+w\right) \bmod l\right] \end{aligned}$$

$$= \frac{u}{2^{2b}} + \frac{1}{2^{2b}} \sum_{w=0}^{v-1} \Pr\left[Ts \bmod l = (z+w) \bmod l \right]$$

Lấy hiệu các xác suất ở trên, ta nhận được hai loại gái trị sai khác để cho thuật toán ***Sim*** và một lần thực thi lược đồ Π đưa ra cùng một đầu ra R là

- Với mọi $0 \le i \le v-1$

$$s_i = | p_z - p_i | = \frac{1}{2^{2b}} \left(1 - \sum_{w=0}^{v-1} \Pr\left[Ts \bmod l = (i+w) \bmod l \right] \right)$$

$$= \frac{1}{2^{2b}} \sum_{w=v}^{l-1} \Pr\left[Ts \bmod l = (i+w) \bmod l \right],$$

- Với mọi $v \le j \le l-1$,

$$s_j = | p_z - p_j | = \frac{1}{2^{2b}} \sum_{w=0}^{v-1} \Pr\left[Ts \bmod l = (j+w) \bmod l \right]$$

Dễ thấy rằng, với tham số b, l của lược đồ R-EdDSA được lựa chọn đủ lớn theo tiêu chuẩn an toàn của các tham số đường cong eliptic thì cả hai loại sai khác xác suất này đều là không đáng kể so với các xác suất p_i, p_j và p_z. Điều này chỉ ra, về mặt tính toán thì phân bố xác suất của đầu ra R trong trường hợp thuật toán ***Sim*** và trong một lầm thực thi thật sựi lược đồ Π là không thể phân biệt được.

Chứng minh tương tự ta cũng nhận được kết luận như trên đối với đầu ra S, và do đó thu được khẳng định rằng, phân bố xác suất của bản ghi $((\underline{R}, \underline{A}), T, \underline{S})$ là không thể phân biệt được về mặt tính toán trong cả hai trường hợp thuật toán ***Sim*** và một lần thực thi thật sự lược đồ định danh chính tắc Π.

Như vậy, lược đồ định danh chính tắc Π là thỏa mãn tiêu chuẩn không lộ tri thức cho người xác minh trung thực.

Để chứng minh Π thỏa mãn tiêu chuẩn mạnh đặc biệt, với giả thiết bài toán ECDLP là khó giải, ta suy ra từ điểm A được khôi phục lại từ khóa công khai $\underline{A}$ và điểm cơ sơ B, ta không thể tính được giá trị s thỏa mãn $A = sB$ trên đường cong elliptic E.

Bây giờ, giả thiết phản chứng rằng, lược đồ định danh chính tắc Π không thỏa mãn tiêu chuẩn mạnh đặc biệt. Điều này có nghĩa là tồn tại hai bản ghi được chấp nhận $((\underline{R}, \underline{A}), T_1, \underline{S}_1)$ và $((\underline{R}, \underline{A}), T_2, \underline{S}_2)$ với $T_1 \ne T_2 \in_R \{0,1,...,2^{2b}-1\}$. Khi đó, từ tiêu chuẩn chấp nhận của lược đồ định danh Π, ta có

$$2^c S_1 B - 2^c T_1 A = 2^c R = 2^c S_2 B - 2^c T_2 A$$

Với $A = sB$, ta nhận được

$$(S_1 - S_2) B = s(T_1 - T_2) B$$

Vì $T_1 \ne T_2, T_1, T_2 \in \{0,1,...,2^{2b}-1\}$ nên xác suất để $T_1 \bmod l = T_2 \bmod l$ là không đáng kể, do đó, ta tính được

$$s = (S_1 - S_2)(T_1 - T_2)^{-1} \bmod l$$

Điều này mâu thuẫn với giả thiết bài toán ECDLP là khó, và do vậy, lược đồ Π phải thỏa mãn tiêu chuẩn mạnh đặc biệt.

Từ đây, ta có hệ quả sau về tính an toàn của lược đồ chữ ký số R-EdDSA.

Hệ quả 2. *Với hàm băm H được mô hình hóa như một bộ tiên tri ngẫu nhiên và giả thiết bài toán logarit rời rạc trên đường cong elliptic là khó thì lược đồ chữ ký số R-EdDSA là không thể bị giả mạo tồn tại dưới các tấn công lựa chọn thông điệp thích nghi.*

Chứng minh. Theo nhận xét 1, ta có lược đồ chữ ký số R-EdDSA chính là lược đồ chữ ký số nhận được bằng cách áp dụng phép biến đổi Fiat-Shamir lên lược đồ định danh chính tắc Π.

Từ định lý 3 và các giả thiết về hàm băm H và bài toán ECDLP, ta có lược đồ định danh chính tắc Π thỏa mãn tiêu chuẩn không bị lộ tri thức cho người xác minh trung thực và tiêu chuẩn mạnh đặc biệt. Áp dụng định lý 2 suy ra lược đồ định danh chính tắc Π là an toàn kháng lại các tấn công bị động. Cuối cùng, áp dụng định lý 1 và hệ quả 1 ta nhận được khẳng định lược đồ chữ ký số R-EdDSA là không thể bị giả mạo tồn tại dưới các tấn công lựa chọn thông điệp thích nghi. □

5. KẾT LUẬN

Bài báo đã đề xuất lược đồ chữ ký số là biến thể ngẫu nhiên hóa của lược đồ chữ ký số EdDSA, gọi là lược đồ R-EdDSA và phân tích độ an toàn của lược đồ đề xuất. Các kết quả chỉ ra, với giả thiết hàm băm H được mô hình hóa như một bộ tiên tri ngẫu nhiên và giả thuyết bài toán khó logarit rời rạc trên đường cong elliptic thì lược đồ chữ ký số R-EdDSA là an toàn chứng minh được trong mô hình bộ tiên tri ngẫu nhiên. Ngoài ra, với các tham số an toàn được lựa chọn như đối với lược đồ chữ ký số EdDSA thì lược đồ R-EdDSA cũng đạt được các tính chất an toàn tương tự.

TÀI LIỆU THAM KHẢO

[1]. Daniel J Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo- Yin Yang. *"High-speedhigh-security signatures".* Journal of Cryptographic Engineering, 2(2):77-89, 2012.

[2]. Daniel J Bernstein, Simon Josefsson, Tanja Lange, Peter Schwabe, and Bo- Yin Yang. *"Eddsa for more curves".* Cryptology ePrint Archive, 2015.

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

[4]. Simon Josefsson and Ilari Liusvaara. *"Edwards-curve digital signature algorithm (EdDSA)".* Technical report, 2017.

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

[6]. Trevor Perrin. *"The XEdDSA and VXEdDSA signature schemes".* Specification. 2016.

ABSTRACT

A PROVABLE SECURE VARIANT OF THE EDDSA DIGITAL SIGNATURE SCHEME

This paper proposes a digital signature scheme, called R-EdDSA scheme, which is a randomized variant of the EdDSA scheme. Assuming the hash function H is modelled as a random oracle and the elliptic curve discrete logarithm problem is hard, we prove that the R-EdDSA digital signature scheme is existentially unforgeable under an adaptive chosen message attacks.

Keywords: EdDSA digital signature schemes; R-EdDSA schemes; Fiat-Shamir transform; Provable security; Twisted Edwards curves.

Nhận bài ngày 08 tháng 01năm 2020
Hoàn thiện ngày 20 tháng 02 năm 2020
Chấp nhận đăng ngày 10 tháng 4 năm 2020

Địa chỉ: [1]Học viện Kỹ thuật Mật mã;
[2]Viện Khoa học – Công nghệ mật mã.
*Email: thanhhvkt@yahoo.com.