A THRESHOLD SIGNATURE SCHEME ON ELLIPTIC CURVE IN EDWARDS FORM

Nguyen Van Nghi*, Dinh Tien Thanh, Do Manh Hung Anh, Nguyen Tan Dat, Dang Hoang Hanh Nguyen
Academy of Cryptography Techniques

ARTICLE INFO

Received: 03/11/2023
Revised: 01/12/2023
Published: 01/12/2023

KEYWORDS

Threshold Signature
Elliptic Curve
Edward
ECDSA
TS-EdDSA

ABSTRACT

Nowadays, digital signature methods play a crucial role in ensuring information security in computer networks by offering services such as authentication, integrity, and non-repudiation. In addition to typical digital signature standards such as RSA, ECDSA, or EdDSA, cryptographers also develop and introduce a number of special signature schemes for practical applications, such as threshold signature schemes, blind signature schemes, etc. The threshold signature scheme, in particular, is a group-oriented digital signature scheme that has been implemented in industries including blockchain technology and e-commerce and is currently garnering considerable attention. The objective of this paper is to propose a threshold signature scheme that offers both strong security and efficient computational cost when implemented on Elliptic curves in Edwards form. We analyze the security of the proposed scheme against known attacks, comparing the security and computational cost with other existing schemes in recent years. The result of the article is a threshold digital signature scheme with good potential for practical application in e-commerce systems and Blockchain technology.

MỘT LƯỢC ĐỒ CHỮ KÝ SỐ NGƯỠNG TRÊN ĐƯỜNG CONG ELLIPTIC DẠNG EDWARD

Nguyễn Văn Nghị*, Đinh Tiến Thành, Đỗ Mạnh Hùng Anh, Nguyễn Tấn Đạt, Đặng Hoàng Hạnh Nguyên
Học viện Kỹ thuật mật mã

THÔNG TIN BÀI BÁO

Ngày nhận bài: 03/11/2023
Ngày hoàn thiện: 01/12/2023
Ngày đăng: 01/12/2023

TỪ KHÓA

Lược đồ ký số ngưỡng
Đường cong elliptic
Edward
ECDSA
TS-EdDSA

TÓM TẮT

Ngày nay, lược đồ chữ ký số cung cấp các dịch vụ an toàn thông tin quan trọng như dịch vụ xác thực, toàn vẹn và chống chối bỏ trong hệ thống mạng máy tính. Ngoài các chuẩn chữ ký số điển hình như RSA, ECDSA hay EdDSA thì các nhà mật mã học còn phát triển và đưa ra một số dạng lược đồ chữ ký đặc biệt ứng dụng trong thực tế như lược đồ chữ ký số ngưỡng, lược đồ chữ ký số mù, lược đồ chữ ký số vòng... Trong đó, lược đồ chữ ký số ngưỡng là một lược đồ chữ ký số hướng nhóm đang được quan tâm nhiều và đã áp dụng vào trong các lĩnh vực như thương mại điện tử hay công nghệ Blockchain. Mục tiêu của bài báo này là đề xuất một lược đồ chữ ký số ngưỡng có độ an toàn cao và chi phí tính toán tốt trên đường cong elliptic dạng Edward. Để đạt được các mục tiêu này thì chúng tôi sử dụng phương pháp nghiên cứu là phân tích sự an toàn của lược đồ đề xuất trước các tấn công đã biết, so sánh sự an toàn và chi phí tính toán với các lược đồ khác trong những công bố những năm gần đây. Kết quả thu được của bài báo là một lược đồ chữ ký số ngưỡng có tiềm năng tốt để áp dụng vào thực tế trong các hệ thống thương mại điện tử và công nghệ Blockchain.

DOI: https://doi.org/10.34238/tnu-jst.9143

* Corresponding author. *Email: nghinv@actvn.edu.vn*

1. Giới thiệu

Ngày nay, hệ thống mạng máy tính đang được ứng dụng rất rộng rãi trong mọi lĩnh vực của đời sống con người như giải trí, học tập, hội họp trực tuyến, ngân hàng, thương mại điện tử... Việc đảm bảo các dịch vụ an toàn thông tin như bí mật, xác thực, toàn vẹn, chống chối bỏ có vai trò quan trọng và rất cấp thiết trong hoạt động của các dịch vụ mạng phổ biến hiện nay.

Lược đồ chữ ký số là một dạng thuật toán mật mã khóa công khai có khả năng cung cấp được dịch vụ xác thực, toàn vẹn và chống chối bỏ cho các dịch vụ mạng. Các chuẩn chữ ký số đang được ứng dụng phổ biến trên hệ thống mạng hiện nay là RSA, ECDSA hay EdDSA. Tuy nhiên thực tế hiện nay còn yêu cầu thêm về chữ ký số như giấu được thông tin bản rõ hay chữ ký số đại diện cho nhóm người dùng vì vậy các nhà mật mã học còn nghiên cứu và đưa ra các dạng lược đồ chữ ký đặc biệt như lược đồ chữ ký số ngưỡng, lược đồ chữ ký số mù [1] – [5]. Lược đồ chữ ký số ngưỡng là một trong các lược đồ chữ ký số hướng nhóm người dùng được phát triển và đã có những ứng dụng trên thực tế như công nghệ Blockchain, ngân hàng hay thương mại điện tử.

Trong vòng khoảng 5 năm trở lại đây thì đã có rất nhiều các công bố đề xuất về lược đồ chữ ký số ngưỡng dựa trên các chuẩn chữ ký số như RSA, ECDSA hay EdDSA hoặc một số dạng lược đồ chữ ký số khác như BLZ hay Schnorr. Cụ thể có thể kể đến như: các lược đồ chữ ký số ngưỡng dựa trên RSA trong [6] – [8], các lược đồ chữ ký số ngưỡng dựa trên ECDSA như trong [9], [10], các lược đồ chữ ký số ngưỡng dựa trên EdDSA/Schnorr như trong [11] – [14].

Số lượng các công bố về lược đồ chữ ký số ngưỡng dựa trên chuẩn ECDSA và EdDSA chiếm đa số điều này được lý giải do khi sử dụng tham số có cùng độ an toàn với chuẩn RSA thì ECDSA và EdDSA có độ dài khóa ngắn hơn và hiệu năng tốt hơn [15]. Tuy nhiên, trong các công bố [9], [10] thì các lược đồ chữ ký số ngưỡng đề xuất bị ảnh hưởng bởi tấn công gây lỗi lên bộ tạo số giả ngẫu nhiên hoặc tấn công tiêm lỗi lên quá trình sinh tham số bí mật trong quá trình ký số [11] - [14]. Đồng thời trong các công bố [9] - [14] cũng chưa đề cập đến vấn đề an toàn xoắn của đường cong sử dụng trong lược đồ ký số ngưỡng.

Trong bài báo này chúng tôi đề xuất một lược đồ chữ ký số ngưỡng trên đường cong elliptic dạng Edward. Lược đồ chữ ký số đề xuất của chúng tôi khắc phục được các điểm yếu về tấn công gây lỗi lên bộ tạo số giả ngẫu nhiên hoặc tiêm lỗi lên quá trình sinh số bí mật trong quá trình ký số. Đồng thời lược đồ đề xuất có chi phí tính toán và hiệu năng tốt do sử dụng đường cong ellipitic dạng Edward [15].

Bài báo có bố cục như sau: Sau phần 1 giới thiệu, bài báo đưa ra khái niệm về lược đồ chữ ký số ngưỡng, cũng như mô tả chi tiết về lược đồ chữ ký số ngưỡng đề xuất trong phần 2. Phần 3 là sự phân tích về độ an toàn của lược đồ đề xuất trước các tấn công đã biết và so sánh về sự an toàn cũng như chi phí tính toán với các lược đồ chữ ký số ngưỡng đã công bố trong thời gian gần đây. Cuối cùng là phần kết luận và các tài liệu tham khảo của bài báo.

2. Vấn đề nghiên cứu

2.1. Giới thiệu về lược đồ chữ ký số ngưỡng

Năm 1987, Desmedt lần đầu tiên đưa ra khái niệm các hệ mật hướng nhóm trong việc truyền thông an toàn của nhóm người dùng. Và lược đồ ký số ngưỡng được phát triển từ ý tưởng các hệ mật hướng nhóm này. Trong năm 1990, Desmedt và Frankel đã đề xuất một lược đồ ký số ngưỡng và một lược đồ chia sẻ bí mật dựa trên hệ mật RSA với 2 đặc điểm cơ bản như sau [5]:

- Đối với nhóm người dùng có N người thì chỉ cần ít nhất t người dùng ($t < N$) cộng tác với nhau để tạo ra một chữ ký hợp lệ cho cả nhóm người dùng.
- Bất kỳ ai đóng vai trò là người xác minh thì đều có thể sử dụng khóa công khai của nhóm để xác minh chữ ký nhóm mà không cần xác định danh tính của người ký.

Khái niệm lược đồ ký số ngưỡng

Một tập hợp N người dùng sử dụng hệ mật khoá công khai gồm các thành phần: (M, K, E, D, H, t) trong đó: M là không gian rõ, K là không gian khoá gồm 2 thành phần là (pk là

khoá công khai và sk là khoá bí mật), E là quá trình mã hoá, D là quá trình giải mã, H là hàm băm, t là ngưỡng (số người cần tập hợp đủ). Lược đồ ký số ngưỡng được định nghĩa bởi ba quá trình là: sinh khoá, ký số, kiểm tra chữ ký số.

2.1.1. Quá trình sinh khóa

Lược đồ ký mã thực hiện sinh các khóa sau:
- Sinh ngẫu nhiên khóa bí mật của nhóm người dùng sk
- Tính khóa công khai của nhóm người dùng pk từ khóa bí mật
- Sinh khoá riêng của người thứ i trong nhóm là pk_i sao cho $\sum_{i=1}^{N} sk_i = sk$.

2.1.2. Quá trình ký số

Đầu vào: Các tham số: thông điệp m, khóa bí mật của người dùng i là sk_i.
Đầu ra: Chữ ký cho thông điệp m của người dùng i trong nhóm người dùng.
1) Tính $r = H(m)$ với H là hàm băm mật mã.
2) Tính chữ ký số của người dùng i đối với thông điệp m là: $s_i = E(sk_i, r)$.

2.1.3. Quá trình kiểm tra chữ ký

Đầu vào: thông điệp m, khóa công khai pk và t chữ ký số của t người dùng khác nhau trong nhóm (với $t \leq N$).
Đầu ra: Chữ ký của nhóm người dùng là hợp lệ hoặc không hợp lệ.
1) Tính chữ ký số của nhóm người dùng cho thông điệp m là $s = \sum_{i=1}^{t} s_i$
2) Kiểm tra chữ ký số s bằng khóa công khai pk và đưa ra thông điệp chữ ký của nhóm người dùng là hợp lệ hoặc không hợp lệ.

2.2. Chuẩn chữ ký số EdDSA

Chuẩn chữ ký số EdDSA là một chuẩn chữ ký số mới dựa trên đường cong elliptic dạng Edward được công bố trong RFC 8032 năm 2016. Chuẩn chữ ký số EdDSA cũng bao gồm ba quá trình là sinh khóa, ký số và kiểm tra chữ ký số.

Tham số miền trong chuẩn chữ ký số 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) Chuẩn EdDSA sử dụng một đường cong elliptic trên trường hữu hạn $\mathbb{F}_p$ với p là nguyên tố mạnh.

2) Một số nguyên dương b thỏa mãn $2^{b-1} > p$. Khóa công khai của EdDSA có độ lớn chính xác b bit, còn chữ ký EdDSA có độ lớn chính xác $2b$ bit.

3) Một hàm băm mật mã H với đầu ra có độ lớn 2b bit.

4) Một phần tử $a \in \mathbb{F}_p$ thỏa mãn $a \neq 0$ và a là một số chính phương trong $\mathbb{F}_p$.

5) Một phần tử $d \in \mathbb{F}_p$ thỏa mãn d không phải là số chính phương trong $\mathbb{F}_p$.

6) Một điểm cơ sở $B \neq (0,1) \in E(\mathbb{F}_p) = \{(x,y), \mathbb{F}_p \times \mathbb{F}_p : ax^2 + y^2 = 1 + dx^2y^2\}$ gồm các điểm xác định trên trường hữu hạn $\mathbb{F}_p$ của đường cong Edwards xoắn E: $\mathrm{ax}^2 + y^2 = 1 + dx^2y^2$.

7) Một số nguyên tố lẻ l thỏa mãn $lB = \mathrm{O}$ với O là điểm vô cực, gọi là bậc của đường cong.

2.2.1. Quá trình sinh khóa

Chuẩn chữ ký số EdDSA thực hiện sinh các khóa sau:
- Sinh ngẫu nhiên khóa bí mật của người dùng là số nguyên sk: $1 < sk < l$
- Tính khóa công khai của người dùng là điểm $pk = sk \times B$

2.2.2. Quá trình ký số

Đầu vào: Các tham số: thông điệp m, khóa bí mật của người dùng sk
Đầu ra: Chữ ký cho thông điệp m của người dùng.

1) Tính $r = H(H(sk)||m)\ mod\ l$ với H là hàm băm mật mã.
2) Tính điểm $R = r \times B$
3) Tính $h = H(R||pk||m)\ mod\ l$
4) Tính giá trị $s = (\ r + h \times sk)\ mod\ l$
5) Đầu ra là chữ ký số $\{R, s\}$

2.2.3. Quá trình kiểm tra chữ ký

Đầu vào: thông điệp m, khóa công khai pk và chữ ký số $\{R, s\}$ của người dùng cho thông điệp m.

Đầu ra: Chữ ký của người dùng cho thông điệp m là hợp lệ hoặc không hợp lệ.

1) Tính $h = H(R||pk||m)\ mod\ l$
2) Tính điểm $P1 = s \times B$
3) Tính điểm $P2 = R + h \times pk$
4) So sánh $P1 = P2$, nếu bằng nhau đưa ra thông điệp chữ ký của người dùng là hợp lệ và ngược lại là không hợp lệ.

2.3. Đề xuất lược đồ chữ ký số ngưỡng TS-EdDSA

Dựa trên chuẩn chữ ký số EdDSA thì trong phần này của bài báo chúng tôi đề xuất một lược đồ ký số ngưỡng là TS-EdDSA. Lý do lựa chọn chuẩn ký số EdDSA vì chuẩn này có độ bảo mật cao và hiệu năng tốt hơn khi so với chuẩn ECDSA, điều này được khẳng định trong [15]. Tuy nhiên, trong lược đồ TS-EdDSA đề xuất chúng tôi có sử dụng tham số miền đường cong là Edward448 và hàm băm H là SHAKE256 để có độ an toàn cao (được thảo luận trong mục 3.2.1 của bài báo này).

Tham số miền lược đồ ký số ngưỡng TS-EdDSA

- Phương trình đường cong $ax^2 + y^2 = 1 + dx^2y^2\ mod\ p$
- Số modulo $p = 2^{448} - 2^{224} - 1$ là số nguyên tố mạnh theo RFC7748.
- Các tham số đường cong $a\ =\ 1$ và $d\ =\ -39081$
- Hàm băm mật mã H là SHAKE256.
- Số nguyên b = 456.
- Điểm cơ sở B có tọa độ: (224580040295924300187604334099896036246789641632564134246125461686950415467406032909029192869357953282578032075146446173674602635247710, 298819210078481492676017930443930673437544040154080242095928241372331506189835876003536878655418784733982303233503462500531545062832660).
- Bậc $l\ =\ 2^{446}$- 138180668098951153520073867485154268803366924748821786098945475038 85

Tiếp theo, chúng tôi mô tả 3 quá trình sinh khóa, ký số và kiểm tra chữ ký số của lược đồ ký số ngưỡng TS-EdDSA cho nhóm N người dùng với ngưỡng ký số là t $(t \leq N)$.

2.3.1. Quá trình sinh khóa

Lược đồ ký mã thực hiện sinh các khóa sau:

- Sinh ngẫu nhiên khóa bí mật của nhóm người dùng sk
- Tính khóa công khai của nhóm người dùng $pk = sk \times B$
- Sinh khoá bí mật của người thứ i trong nhóm là sk_i sao cho $\sum_{i=1}^{N} sk_i = sk$.

2.3.2. Quá trình ký số

Đầu vào: Các tham số: thông điệp m, khóa bí mật của người dùng sk

Đầu ra: Chữ ký cho thông điệp m của người dùng i trong nhóm

1) Nhóm người dùng tính $r = H(sk||H(m)||time)\ mod\ l$ với $time$ là tem thời gian và sinh N phần r_i sao cho $\sum_{i=1}^{N} r_i = r$ (áp dùng cho $t\ =\ N$, trường hợp $t < N$ cần áp dụng lược đồ chia sẻ bí mật Shamir).
2) Nhóm người dùng tính điểm $R = r \times B$

3) Tiếp theo nhóm người dùng tính giá trị $h = H(R||pk||H(m))\ mod\ l$ và gửi h, r_i cho người dùng thứ i trong nhóm qua một kênh an toàn.
4) Người dùng thứ i tiến hành tính $R_i = r_i \times B$
5) Người dùng thứ i tính giá trị $s_i = (\ r_i + h \times sk_i)\ mod\ l$
6) Đầu ra là chữ ký số $\{R_i, s_i\}$ của người dùng thứ i cho thông điệp m.

2.2.3. Quá trình kiểm tra chữ ký

Đầu vào: thông điệp m, khóa công khai pk của nhóm người dùng và t chữ ký $\{R_i, s_i\}$ của t người dùng khác nhau trong nhóm (trường hợp này $t = N$) cho thông điệp m.

Đầu ra: Chữ ký của nhóm người dùng cho thông điệp m là hợp lệ hoặc không hợp lệ.

Các bước tính toán quá trình kiểm tra chữ ký được thực hiện tại bên kiểm tra thứ ba là:

1) Người kiểm tra nhận được t chữ ký $\{R_i, s_i\}$ của t người dùng khác nhau trong nhóm (trường hợp này $t = N$) cho thông điệp m thì sẽ tính được giá trị chữ ký $s = \sum_{i=1}^{t} s_i\ mod\ l$ của nhóm người dùng cho thông điệp m.
2) Tính được $R = \sum_{i=1}^{t} R_i$
3) Tính $h = H(R||pk||H(m))\ mod\ l$
4) Tính điểm $P1 = s \times B$
5) Tính điểm $P2 = R + h \times pk$
6) So sánh $P1 = P2$, nếu bằng nhau đưa ra thông điệp chữ ký của nhóm người dùng là hợp lệ và ngược lại là không hợp lệ.

Lưu ý:

- Trường hợp $t < N$ có thể áp dụng lược đồ chia sẻ bí mật Shamir hoặc lược đồ chia sẻ bí mật Feldman VSS để chia sẻ các mảnh r_i, sk_i tới cho người dùng trong nhóm. Chi tiết cách thức triển khai xem trong [13].

- Việc phân phối các giá trị R, r_i, sk_i tới cho người dùng trong nhóm thì lược đồ đề xuất sử dụng một máy chủ tập trung được quản lý bởi quản trị nhóm người dùng và phân phối các giá trị này tới người dùng thông qua kênh truyền bảo mật SSL/TLS. Trường hợp khác hoàn toàn có thể kết hợp lược đồ đề xuất với các lược đồ phân phối khóa khác như FROST trong [11], MPC Rescure trong [13] hoặc MPC ZKP trong [14].

3. Kết quả và bàn luận

Trong phần này, chúng tôi đưa ra phân tích về tính đúng đắn và sự an toàn của lược đồ chữ ký số ngưỡng đề xuất. Đồn thời, phần này cũng đưa ra kết quả so sánh các vấn đề an toàn và chi phí tính toán của lược đồ đề xuất với một số công bố khác trong 5 năm gần đây.

3.1. Phân tích tính đúng đắn của lược đồ ký số ngưỡng đề xuất

Tính đúng đắn của lược đồ được đảm bảo khi phương trình $s = \sum_{i=1}^{t} s_i\ mod\ l$ luôn đúng. Thật vậy, trường hợp $t = N$ ta luôn có:

$$\sum_{i=1}^{t} s_i = \sum_{i=1}^{N} s_i = s_1 + s_2 + .. + s_N = (\ r_1 + h \times sk_1) + (\ r_2 + h \times sk_2) + \cdots + (\ r_N + h \times sk_N)$$

$$= (\ r_1 + r_2 + \cdots + r_N) + h(sk_1 + sk_2 + \cdots + sk_N) = r + h \times sk = s.$$

Đối với trường hợp $t < N$ thì phương trình $s = \sum_{i=1}^{t} s_i\ mod\ l$ vẫn đúng do tính đúng đắn của lược đồ chia sẻ bí mật Shamir.

3.2. Phân tích sự an toàn của lược đồ chữ ký số ngưỡng đề xuất

Vấn đề an toàn của lược đồ chữ ký số ngưỡng đề xuất được xem xét thông qua các tấn công như sau: một là tấn công dựa trên lý thuyết toán học, hai là tấn công liên quan đến quá trình cài đặt, triển khai giao thức và cuối cùng là tấn công bằng máy tính lượng tử.

3.2.1. Tấn công dựa trên lý thuyết toán học

Việc tấn công dựa trên lý thuyết toán học vào lược đồ chữ ký số ngưỡng đề xuất có thể thực hiện theo hai hướng là giải bài toán logarit rời rạc trên đường cong elliptic hoặc tấn công giả mạo thông điệp dựa trên phá vỡ hàm băm mật mã sử dụng trong lược đồ.

- Trong lược đồ ký số ngưỡng đề xuất, kẻ tấn công tiến hành chặn bắt được các giá trị khóa công khai của nhóm người dùng là pk và điểm R (tính từ các giá trị R_i thu được trên kênh truyền) và tiến hành dự đoán các giá trị khóa bí mật sk và giá trị bí mật r. Cụ thể các bài toán cần giải đối với kẻ tấn công sẽ là: bài toán logarit rời rạc trên đường cong elliptic. Đây được xem là một bài toán khó và không có khả năng giải trong khoảng thời gian đa thức nếu các tham số đường cong được lựa chọn là an toàn. Chúng ta có Bảng 1 là khuyến nghị của Viện tiêu chuẩn quốc gia Hoa Kỳ NIST trong việc lựa chọn kích thước tham số cho các thuật toán mật mã cơ bản tương ứng thời điểm sử dụng được đưa ra năm 2020 [16].

Bảng 1. *Khuyến nghị NIST về tham số khóa cho các thuật toán mật mã*

Năm sử dụng	Độ bảo mật	ECDLP (độ dài p theo bit)	RSA/DH (độ dài n/p theo bit)	Hàm băm
2019-2030 và lâu hơn nữa	128	256	3072	SHA2-256 SHA3-256
2019-2030 và lâu hơn nữa	192	384	7680	SHA2-384 SHA3-384
2019-2030 và lâu hơn nữa	256	512	15360	SHA2-512 SHA3-512

Số liệu trên Bảng 1 cho thấy rằng lược đồ đề xuất sử dụng đường cong Edward448 có số modulo $p \sim 448$ bit nằm trong mức độ bảo mật từ 192 đến 256, thì được dự đoán là an toàn để sử dụng tới năm 2030 và lâu hơn nữa dựa theo sự phát triển năng lực tính toán của máy tính hiện nay.

- Để giả mạo thông điệp trong lược đồ đề xuất thì kẻ tấn công có thể sử dụng tấn công nghịch lý ngày sinh và tấn công gặp nhau ở giữa để phá vỡ hàm băm SHAKE256. Hàm băm SHAKE256 là một phiên bản của hàm băm SHA3-256, nên theo Bảng 1 thì hàm băm này cũng được dự đoán là an toàn để sử dụng tới năm 2030 và lâu hơn nữa.

Như vậy, đối với tấn công theo lý thuyết toán học với các tham số đường cong Edward448 và SHAKE256 được sử dụng thì lược đồ đề xuất được coi là an toàn sử dụng tới năm 2030 và lâu hơn nữa.

3.2.2. Tấn công liên quan đến vấn đề cài đặt

Đối với lược đồ đề xuất thì tấn công liên quan vấn đề cài đặt có thể xem xét hai tấn công phổ biến như sau: tấn công lên quá trình sinh tham số bí mật r và tấn công dựa trên tính chất an toàn xoắn của đường cong sử dụng.

- Đối với tấn công lên quá trình sinh tham số bí mật r thì tồn tại hai tấn công chính là: cài đặt bộ sinh số giả ngẫu nhiên tồn tại lỗ hổng và tấn công tiêm lỗi.

+ Trong [17] khẳng định tồn tại các cuộc tấn công vào quá trình sinh các số giả ngẫu nhiên trên với việc cài đặt bộ sinh số có lỗ hổng bảo mật trên phần cứng hay phần mềm và kẻ tấn công sẽ biết được giá trị sinh này. Tuy nhiên, lược đồ đề xuất sử dụng hàm băm SHAKE256 trong sinh giá trị r điều này chống lại được tấn công cài đặt bộ sinh số giả ngẫu nhiên có lỗ hổng theo khẳng định trong [17].

+ Trong [18], khẳng định có thể thực hiện các cuộc tấn công tiêm lỗi vào hàm băm trong sử dụng sinh số ngẫu nhiên, tuy nhiên lược đồ đề xuất có khả năng chống được tấn công này do sử dụng tem thời gian là một đầu vào hàm băm trong quá trình sinh số r và điều này được khẳng định trong [18].

- Đối với tấn công gây lỗi dựa trên cài đặt thang Montgomery trong dạng đường cong xoắn hay tấn công dựa trên tính chất an toàn xoắn: Trong [19] khẳng định rằng các đường cong Weistrass và Edward đều có thể được chuyển đổi sang dạng đường cong Edward xoắn và tiến hành tấn công gây lỗi quá trình tính toán phép cộng và nhân điểm dựa trên cài đặt thang Montgomery để có thể giải bài toán logarit rời rạc một cách tối ưu hơn và phá vỡ được các lược đồ ký số trên đường cong elliptic. Trong [20] khẳng định đường cong Edward448 là an toàn xoắn (twist-security) tức là chống được tấn công này.

3.2.3. Tấn công dựa trên máy tính lượng tử

Theo [21] thì các hệ mật dựa trên bài toán logarit rời rạc đều bị ảnh hưởng bởi tấn công trên máy tính lượng tử, cụ thể là thuật toán Shor. Cũng trong [21] đưa ra số lượng qubit tối thiểu giải bài toán logarit rời rạc trên đường cong elliptic và trên trường hữu hạn theo độ bảo mật tương đương độ dài tham số khóa hay số modulo như Bảng 2.

Bảng 2. *Số lượng Qubits cần thiết cho máy tính lượng tử để giải bài toán logarit rời rạc và phân tích số nguyên*

Độ bảo mật	#Qubits để giải bài toán logarit rời rạc trên elliptic	#Qubits cho giải bài phân tích số nguyên
112	2042	4098
192	2330	6146
256	3484	15362

Lược đồ đề xuất dựa trên bài toán logarit rời rạc trên đường cong elliptic vì vậy bị ảnh hưởng bởi tấn công Shor trên máy tính lượng tử, tuy nhiên theo Bảng 2 thì khi lựa chọn tham số cho các giao thức đề xuất có độ bảo mật từ 128 bit trở lên thì yêu cầu máy tính lượng tử hỗ trợ từ 2000 qubit trở lên. Tính tới thời điểm này tức năm 2023 thì điều này chưa khả thi và theo khuyến nghị của cơ quan mật mã của Đức năm 2023 trong tài liệu [22] thì khi lựa chọn tham số cho lược đồ đề xuất có độ bảo mật từ 128 bit thì lược đồ có thể sử dụng đến 2028 hoặc lâu hơn nữa có sự xem xét của máy tính lượng tử.

3.3. So sánh vấn đề an toàn của lược đồ ký số ngưỡng đề xuất với một số công bố khác

Phần này, chúng tôi đưa ra Bảng 3 so sánh về vấn đề an toàn của lược đồ đề xuất với một số lược đồ chữ ký số ngưỡng trong các công bố khác.

Bảng 3. *So sánh vấn đề an toàn của một số lược đồ chữ ký số ngưỡng trên đường cong elliptic*

Lược đồ chữ ký số ngưỡng	Dựa trên bài toán ECLDP theo chuẩn ECDSA hoặc EdDSA/Schnorr		Tấn công lên quá trình cài đặt			Tấn công bằng máy tính lượng tử
	ECDSA	EdDSA /Schnorr	Cài đặt bộ sinh số ngẫu nhiện tồn tại lỗ hổng [17]	Tấn công tiêm lỗi lên hàm băm sinh số ngẫu nhiên [18]	Tấn công dựa trên tính chất an toàn xoắn (twist security) [20]	
Trong [9]	Có	Không	Có	Không	Tồn tại	Có
Trong [10]	Có	Không	Có	Không	Tồn tại	Có
Trong [11]	Không	Có	Có	Không	Tồn tại	Có
Trong [12]	Không	Có	Không	Có	Tồn tại	Có

Lược đồ chữ ký số ngưỡng	Dựa trên bài toán ECLDP theo chuẩn ECDSA hoặc EdDSA/Schnorr		Tấn công lên quá trình cài đặt			Tấn công bằng máy tính lượng tử
Trong [13]	Không	Có	Không	Có	Tồn tại	Có
Trong [14]	Không	Có	Không	Tồn tại	Tồn tại	Có
Lược đồ đề xuất	Không	Có	Không	Không	Không	Có

Trong Bảng 3, thì các lược đồ ký số ngưỡng được xem xét có thể bị ảnh hưởng bởi các tấn công ở ba mức là: không, có và tồn tại. Đối với mức "không" thì các lược đồ không bị ảnh hưởng bởi tấn công, ở mức "có" thì các lược đồ chắc chắn bị ảnh hưởng bởi các tấn công, còn mức "tồn tại" là có thể bị ảnh hưởng bởi tấn công đang xem xét tùy thuộc vào đường cong mà lược đồ đó sử dụng.

Như vậy, dễ thấy rằng lược đồ của chúng tôi đề xuất chống được tất cả các tấn công lên quá trình cài đặt đã đề cập trong mục 3.2 và tốt hơn tất cả các lược đồ đang so sánh.

3.3. So sánh chi phí tính toán của lược đồ đề xuất với một số công bố khác

Trong phần này, chúng tôi đưa ra so sánh về chi phí tính toán của lược đồ đề xuất so với các lược đồ khác trong các công trình đã công bố trong khoảng 5 năm gần đây. Chi phí tính toán của các giao thức tại các bên liên lạc sẽ được đo bởi số các phép tính như: Elliptic Curve Point Multiplication (ECPM) – phép nhân điểm, Elliptic Curve Point Addition (ECPA) – Phép cộng điểm, Modular Inversion (MI) – Phép nghịch đảo, Modular Multiplication (Mul) – Phép nhân, Modular Addition (Add) – Phép cộng, One-way hash function (Hash) – Băm mật mã. Trong Bảng 4 là số liệu chi phí tính toán chúng tôi tính được đối với quá trình ký số và kiểm tra ký số trong một số lược đồ chữ ký số ngưỡng trên đường cong elliptic đối với một người dùng trong nhóm và không tính chi phí đối với các cách thức phân phối khóa (trong bảng chỉ đưa ra tên cách thức phân phối khóa). Quá trình phân phối khóa ký hiệu là KD (Key Distribution).

Bảng 4. *Chi phí tính toán của một số lược đồ chữ ký số ngưỡng*

Lược đồ	Quá trình	ECPM	ECPA	MI	Mul	Add	Hash	KD
Trong [9] và [10]	Ký	1	0	0	2	1	1	Máy chủ tập trung
	Kiểm tra	2	1	1	2	t đến N	1	
Trong [11] và [12]	Ký	1	0	0	1	1	1	FROST
	Kiểm tra	1	0	0	1	t đến N	1	
Trong [13]	Ký	2	0	0	1	1	2	ZKP
	Kiểm tra	2	1	0	0	t đến N	1	
Trong [14]	Ký	2	0	0	1	1	4	Rescure
	Kiểm tra	2	1	0	0	t đến N	2	
Lược đồ đề xuất	Ký	2	0	0	1	1	3	Máy chủ tập trung
	Kiểm tra	2	1	0	0	t đến N	1	

Số liệu Bảng 4 cho thấy lược đồ đề xuất có chi phí tính toán gần như tương đồng với các lược đồ chữ ký số ngưỡng dựa trên EdDSA/Schnorr đã công bố khác.

4. Kết luận

Bài báo đã đề xuất được một lược đồ chữ ký số ngưỡng trên đường cong elliptic Edward448. Với độ an toàn cao và chi phí triển khai thấp đã được chứng minh và so sánh với một lược chữ ký số ngưỡng khác đã công bố, thì lược đồ đề xuất rất có tiềm năng trong triển khai ứng dụng thực tế như thương mại điện tử hoặc công nghệ Blockchain.

TÀI LIỆU THAM KHẢO/ REFERENCES

[1] A. Roy and S. Karforma, "A survey on digital signatures and its applications," *Journal of Computer and Information Technology*, vol.3, no.2, pp. 45-69, 2012.

[2] N. Asghar, *A Survey on Blind Digital Signatures*, University of Waterloo, ON, Canada, 2011.

[3] H. Kinkelin and F. Rezabek, "A Survey on Threshold Signature Schemes," in *Proceeding of Seminar IITM SS 20 - Network Architectures and Services, Informatics Technical University of Munich*, 2020, pp. 49-53.

[4] S. Josefsson and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)," RFC 8032, 2017. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8032. [Accessed Oct. 26, 2023].

[5] Y. Desmedt and Y. Frankel, "Threshold cryptosystems," in *Advances in Cryptology CRYPTO' 89 Proceedings*, Springer New York, 1990, pp. 307-315.

[6] S. Tang, "Simple Threshold RSA Signature Scheme Based on Simple Secret Sharing," in *Proceeding of International Conference on Computational and Information Science*, Springer, 2005, pp. 186-191.

[7] R. Gennaro, S. Halevi, H. Krawczyk, and T. Rabin, "Threshold RSA for Dynamic and Ad-Hoc Groups," in *Proceeding of Advances in Cryptology – EUROCRYPT 2008*, Springer, 2008, pp. 88-107.

[8] J. Dossogne, F. Lafitte, and D. V. Heule, "Secure and practical threshold RSA," in *Proceedings of the 6th International Conference on Security of Information and Networks*, Aksaray Turkey, 2013, pp. 79-85.

[9] Gennaro and S. Goldfeder, "Fast multiparty threshold ECDSA with fast trustless setup," In *Proceeding of ACM CCS 2018*, ACM Press, 2018, pp. 1179–1194.

[10] J. Doerner, Y. Kondi, E. Lee, and A. Shelat, "Threshold ECDSA from ECDSA Assumptions: The Multiparty Case," *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 1051-1066.

[11] Komlo and I. Goldberg, "Frost: flexible round-optimized schnorr threshold signatures," in *Proceeding of International Conference on Selected Areas in Cryptography*, Springer, 2020, pp. 34–65.

[12] F. Garillot, Y. Kondi, P. Mohassel, and V. Nikolaenko, "Threshold Schnorr with Stateless Deterministic Signing from Standard Assumptions," in *Advances in Cryptology — CRYPTO 2021*, Springer, 2021, pp. 26-28.

[13] M. Battagliola, R. Longo, A. Meneghetti, and M. Sala, "Provably Unforgeable Threshold EdDSA with an Offline Participant and Trustless Setup," *Mediterranean Journal of Mathematics*, vol. 20, no. 253, pp. 1-30, 2023.

[14] C. Bonte, N. P. Smart, and T. Tanguy, "Thresholdizing HashEdDSA: MPC to the rescue," in *International Journal of Information Security*, vol. 20, no. 6, pp. 879–894, 2021.

[15] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang, "High-speed high-security signatures," in *International Workshop on Cryptographic Hardware and Embedded Systems*, Springer, 2011, pp. 124–142.

[16] D. Giry, "Recommendation for Key Management," Special Publication 800-57 Part 1 Rev. 5, National Institute of Standards and Technology of America, May 2020. [Online]. Available: https://www.keylength.com/en/4/. [Accessed Oct. 14, 2023].

[17] V. N. Nguyen and Q. T. Do, "Attacks on elliptic curve digital signature algorithm related to the secret value k and proposed solutions to prevention," *Proceedings of the 15th National Conference on Fundamental and Applied Information Technology Research (FAIR)*, Ha Noi - Viet Nam, 2022, pp. 90-94.

[18] Romailler and Pelissier, "Practical Fault Attack against the Ed25519 and EdDSA Signature Schemes," *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2017, pp. 1-22.

[19] P. -A. Fouque, R. Lercier, D. Réal, and F. Valette, "Fault Attack on Elliptic Curve Montgomery Ladder Implementation," *2008 5th Workshop on Fault Diagnosis and Tolerance in Cryptography*, Washington, DC, USA, 2008, pp. 92-98, doi: 10.1109/FDTC.2008.15.

[20] T. T. Dinh, Q. T. Nguyen, V. S. Nguyen, and V. D. Nguyen, "An algorithm to select a secure twisted elliptic curve in cryptography," *Journal of Science and Technology on Information security*, no. 1 - CS15, pp. 17-25, 2022.

[21] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, "Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms," *Cryptology ePrint Archive*, no. 598, pp. 1-24, 2017.

[22] Federal Office for Information Security of Germany, "Recommendations and Key Lengths," TR02102-1 v2023-01, BSI, March 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html. [Accessed Oct. 14, 2023].