A SCHNORR-BASED ZERO-KNOWLEDGE PROOF SCHEME ON ELLIPTIC CURVE

Nguyen Van Nghi*, Lai Thi Thu Van, Ha Nhu Tuan, Le Minh Hieu, Le Thi Bich Hang
Academy of Cryptography Techniques

ARTICLE INFO

Received: 11/5/2023
Revised: 20/6/2023
Published: 20/6/2023

KEYWORDS

Zero-Knowledge Proof
Interactive ZKP
Non-Interactive ZKP
Cryptography
Elliptic Curve

ABSTRACT

A cryptographic method known as Zero-Knowledge Proof, or ZKP for short, was introduced to the public for the first time in the 1990s. ZKP has been extensively implemented in practice over the past decade, such as in blockchain technology and authentication systems, as well as incorporated into other cryptographic algorithms. The majority of these ZKP schemes are mathematically founded on finite fields. In this paper, we propose a Schnorr-based ZKP scheme on Elliptic curves. This approach has high security and better performance than the Schnorr-based ZKP scheme on the finite field. Moreover, its security enhancements are superior to those of other Schnorr-based ZKP algorithms on the Elliptic curve. These results are argued on the basis of the mathematical theory of published and experimental works in the Python programming language. Therefore, it can be concluded that this ZKP scheme has tremendous potential for implementation in client-side authentication systems and in Blockchain technology.

MỘT LƯỢC ĐỒ BẰNG CHỨNG KHÔNG TIẾT LỘ TRI THỨC KIỂU SCHNORR TRÊN ĐƯỜNG CONG ELLIPTIC

Nguyễn Văn Nghị*, Lại Thị Thu Vân, Hà Như Tuấn, Lê Minh Hiếu, Lê Thị Bích Hằng
Học viện Kỹ thuật mật mã

THÔNG TIN BÀI BÁO

Ngày nhận bài: 11/5/2023
Ngày hoàn thiện: 20/6/2023
Ngày đăng: 20/6/2023

TỪ KHÓA

Bằng chứng không lộ tri thức
ZKP có tương tác
ZKP không tương tác
Mật mã học
Đường cong Elliptic

TÓM TẮT

Zero-Knowledge Proof (ZKP) - bằng chứng không lộ tri thức là một dạng kỹ thuật mật mã được công bố đầu tiên từ thập niên 90 của thế kỷ trước. Tuy nhiên, trong vòng 10 năm trở lại đây thì ZKP mới được ứng dụng phổ biến trong thực tế như: công nghệ Blockchain, hệ thống xác thực và kết hợp vào các thuật toán mật mã khác. Các lược đồ ZKP đang sử dụng này thì đa phần có cơ sở toán học trên trường hữu hạn có chi phí triển khai lớn và tốc độ chậm. Trong bài báo này, chúng tôi đề xuất một lược đồ ZKP kiểu Schnorr với cơ sở toán học dựa trên đường cong Elliptic. Mục tiêu giải pháp ZKP đề xuất trên Elliptic này có độ an toàn cao và hiệu năng tốt hơn so với lược đồ ZKP kiểu Schnorr trên trường hữu hạn, đồng thời có thêm một số cải tiến tốt hơn về mặt bảo mật so với các phiên ZKP kiểu Schnorr đã công bố khác trên đường cong Elliptic. Các kết quả này được lập luận dựa trên phương pháp nghiên cứu cơ sở lý thuyết toán học của các công trình đã công bố và thực nghiệm bằng ngôn ngữ lập trình python. Qua đó kết luận rằng đây là lược đồ ZKP rất có tiềm năng áp dụng vào thực tế trong các hệ thống xác thực và trong công nghệ Blockchain.

DOI: https://doi.org/10.34238/tnu-jst.7920

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

1. Giới thiệu

ZKP là một trong những khái niệm trừu tượng và cũng rất hấp dẫn của mật mã hiện đại. Thuật ngữ Zero Knowledge hay tri thức không lần đầu được công bố bởi nhóm tác giả Shafi Goldwasser và các cộng sự vào năm 1985 [1]. Hiểu đơn giản thì ZKP là cơ chế cho phép bên thứ nhất chứng minh mình biết một thông tin bí mật với bên thứ hai và không cho bên thứ hai tìm hiểu được bất kỳ điều gì về thông tin bí mật này. Vì có sự tương tác của hai bên liên lạc cho nên lược đồ ZKP còn được gọi là giao thức ZKP. Tuy đã được công bố từ lâu nhưng trong vòng 10 năm trở lại đây thì ZKP mới được ứng dụng phổ biến trong thực tế, cụ thể như: ứng dụng trong các hệ thống xác thực/định danh, trong công nghệ Blockchain, tích hợp trong các thuật toán mật mã...

Ứng dụng trong các hệ thống xác thực và định danh: việc sử dụng ZKP trong các hệ thống xác thực giúp người dùng chứng minh thông tin định danh bí mật cá nhân với máy chủ và không cho máy chủ biết cụ thể thông tin này là gì [2] – [4]. Trên thực tế khi sử dụng mật khẩu như thông tin bí mật để xác thực thường dễ bị lộ do độ dài ngắn và tính ngẫu nhiên kém nên khi kết hợp với ZKP thì các hệ thống xác thực có thể khắc phục được các điểm yếu này.

Ứng dụng trong công nghệ Blockchain: nổi bật có thể kể đến các dự án tiền mã hóa như ZCash, MINA, ZKSync, StarkWawe [5]. Việc sử dụng ZKP giúp các dự án Blockchain này đảm bảo tính riêng tư của giao dịch, kích thước khối nhỏ và khả năng mở rộng quy mô mạng lưới tốt hơn.

Ứng dụng trong các thuật toán mật mã khác như: giao thức trao đổi khóa SRP, giao thức trao đổi khóa JPAKE, giao thức trao đổi khóa DragonFly, lược đồ ký số mù DSA, lược đồ ký số hậu lượng tử Pinic [6], [7].

Các lược đồ ZKP đang được sử dụng trong các ứng dụng thực tế hiện nay có thể chia 3 nhóm: Nhóm 1 dựa trên cơ sở toán học là việc tính toán dựa trên trường hữu hạn như: lược đồ ZKP Schnorr, lược đồ ZKP Fiat-Shamir [2], [3]. Nhóm 2 dựa trên mạch phần cứng như lược đồ ZKP ZK-SNARK [8], lược đồ ZKP ZK-STARK [9]. Nhóm 3 dựa trên tính toán trên đường cong Elliptic như trong [10].

Bài báo này tập trung vào các lược đồ ZKP trên đường cong Elliptic, cụ thể các lược đồ ZKP kiểu Schnorr trên đường cong Elliptic. Mục tiêu của bài báo là đề xuất một lược đồ ZKP kiểu Schnorr trên đường cong Elliptic mà có cơ chế xác thực hai chiều và chống lỗi cài đặt trong bộ sinh số ngẫu nhiên. Các lỗi này đã tồn tại trong lược đồ ZKP kiểu Schnorr trên trường hữu hạn và trong một số lược đồ ZKP kiểu Shnorr trên đường cong Elliptic trong [10]. Các mục tiêu này được đưa ra dựa trên hoạt động lược đồ đề xuất và việc so sánh cơ sở lý thuyết các công trình đã công bố trong [2], [10], [11]. Đồng thời nhóm tác giả còn cài đặt thực nghiệm lược đồ ZKP đề xuất bằng ngôn ngữ lập trình python để đánh giá hiệu năng so với lược đồ trên trường hữu hạn.

Bài báo này được bố cục theo 4 mục chính: sau phần 1 giới thiệu, phần 2 đưa ra vấn đề và phương pháp nghiên cứu chính. Phần 3 trình bày chi tiết về hoạt động lược đồ ZKP kiểu Schnorr trên đường cong Elliptic mà chúng tôi đề xuất. Đồng thời trong phần này chúng tôi xem xét các tính chất, vấn đề an toàn, hiệu năng của lược đồ ZKP đề xuất dựa trên cơ sở lý thuyết toán học và kết quả triển khai thực nghiệm của giải pháp. Cuối cùng là phần kết luận và tài liệu tham khảo được tham chiếu trong bài báo.

2. Vấn đề và phương pháp nghiên cứu

2.1. Tổng quan về ZKP

2.1.1. Khái niệm và tính chất của ZKP

Trong [2] và [3], nhóm tác giả đưa ra rằng: ZKP là phương pháp mà một bên P (bên chứng minh – Prover) có thể chứng minh với bên còn lại V (người xác minh – Verifier) rằng P biết một giá trị x tồn tại, mà không cần tiết lộ bất kỳ thông tin nào cho V về giá trị x này. ZKP được thực hiện bởi sự tương tác giữa hai bên liên lạc nên có thể gọi là giao thức.

ZKP có thể hoạt động được khi thỏa mãn ba tính chất là [2], [3]: Completeness, Soundness, Zero-Knowledge.

Completeness (Tính hoàn thành): Nếu mệnh đề là đúng thì một người kiểm tra trung thực sẽ bị thuyết phục bởi một người chứng minh trung thực rằng mệnh đề đó là đúng.

Soundness (Tính hợp lý): Nếu người chứng minh là không trung thực thì họ không thể thuyết phục được người kiểm tra rằng mệnh đề đúng bằng cách dối trá.

Zero-Knowledge (Tính không tiết lộ tri thức): Nếu mệnh đề là đúng thì người kiểm tra chỉ biết là nó đúng và không thể biết được chính xác mệnh đề đó là gì.

2.1.2. Phân loại ZKP

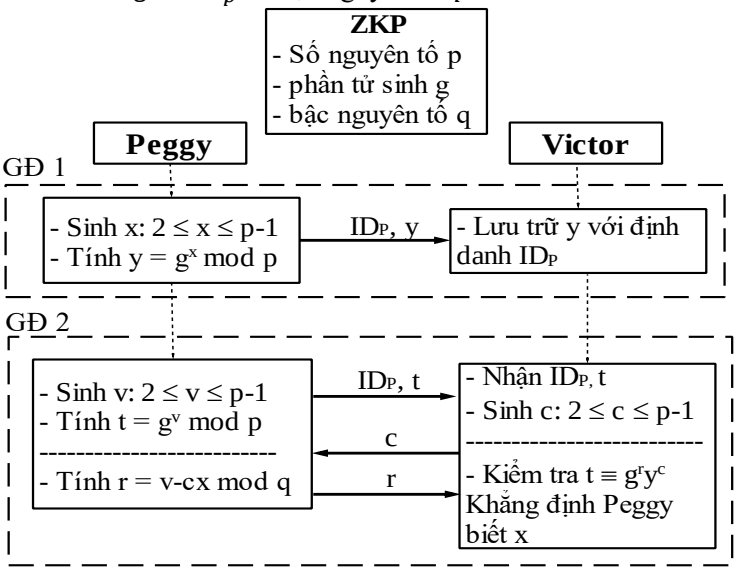
ZKP được phân loại thành 2 dạng chính là: Interactive ZKP và Non-Interactive ZKP.

Interactive ZKP (ZKP có tương tác): ở đây trong quá trình thực hiện ZKP thì cần có sự tương tác của cả hai phía Verifier và Prover.

Non-Interactive ZKP (ZKP không tương tác): trong quá trình thực hiện ZKP thì không cần sự tương tác phản hồi lại cho Prover từ phía Verifier.

2.2. Lược đồ Interactive ZKP kiểu Schnorr trên trường hữu hạn

Xem xét lược đồ Interatctive ZKP kiểu Schnorr dựa trên bài toán logarit rời rạc trên trường hữu hạn Z_p dựa trên ý tưởng từ lược đồ ký số Schnorr được trình bày trong hình 1 [2], [3]. Tham số chung thực hiện ZKP giữa hai người dùng Peggy (bên chứng minh) và Victor (bên xác minh) là số nguyên tố lớn p, phần tử sinh g của Z_p có bậc nguyên tố q.



Hình 1. *Quá trình kiểm tra chữ ký số Ed25519*

Ý nghĩa của giao thức ZKP là Peggy muốn chứng minh cho Victor rằng mình biết về giá trị x trong trường Z_p với p là số nguyên tố có phần tử sinh g và bậc nguyên tố lớn nhất q. Các bước thực hiện cụ thể như sau:

- Giai đoạn 1 – Đăng ký:

+ Peggy sinh giả ngẫu nhiên giá trị x: $2 \leq x \leq p-1$ và tính $y = g^x \bmod p$. Rồi gửi y tới Victor cùng với định danh ID_P của mình.

+ Victor sẽ lưu trữ giá trị y với định danh của Peggy vào cơ sơ dữ liệu để phục vụ cho việc xác minh trong giai đoạn 2. Chú ý giai đoạn 1 cần thực hiện trên kênh an toàn tránh việc bên thứ ba chặn bắt được giá trị y và giả mạo giá trị này.

- Giai đoạn 2 – Xác minh:

+ Peggy sinh giá trị v sao cho $2 \leq v \leq p-1$ và tính $t = g^v \ mod \ p$. Rồi gửi t tới Victor cùng với định danh ID_P của mình.

+ Victor nhận các giá trị t và định danh ID_P của Peggy sẽ tìm được giá trị y tương ứng trong cơ sở dữ liệu đã lưu. Thực hiện sinh giá trị c sao cho $2 \leq c \leq p-1$ và gửi tới Peggy.

+ Tiếp theo, Peggy tính toán giá trị $r = (v - cx) \ mod \ p$ và gửi tới Victor.

+ Cuối cùng, Victor sẽ thực hiện so sánh giá trị t với $g^r y^c$ theo phương trình đồng dư $t \equiv g^r y^c \ mod \ p$. Nếu hai giá trị này giống nhau thì Victor sẽ khẳng định được rằng Peggy biết x, ngược lại thì không xác minh được Peggy có biết x hay không.

2.2.1. Xem xét kiểm tra các tính chất của lược đồ ZKP kiểu Schnorr trên trường hữu hạn

Completeness: Nếu Victor và Peggy là hai bên không bị giả mạo thì lược đồ hoàn thành khi hai giá trị t và $g^r.y^c$ là bằng nhau. Phân tích công thức tính giá trị: $g^r.y^c = g^{v-cx}.y^c = g^{(v-cx)}.g^{xc} = g^v =$ t. Như vậy, phương trình $t \equiv g^r y^c$ là chính xác hay lược đồ hoàn thành.

Soundness: Thấy rằng, Peggy không thể bị giả mạo vì phương trình $t \equiv g^r y^c$ diễn ra khi và chỉ khi Peggy biết giá trị x.

Zero-Knowledge: Trong giai đoạn 2 thì thấy rằng Peggy không cung cấp giá trị x hoặc p cho bên Victor để xác minh rằng Peggy biết x. Với kẻ tấn công thì chỉ biết giá trị t, c, r chặn bắt được trên kênh truyền, suy ra để tìm giá trị x này thì cần phải giải bài toán logarit rời rạc trên trường F_p để tìm v và đây là một bài toán khó không thể giải trong thời gian đa thức khi độ dài của p lớn.

2.2.2. Các điểm yếu bảo mật tồn tại của lược đồ

Lược đồ hình 1 tồn tại hai vấn đề bảo mật là: thiếu cơ chế xác thực hai chiều và bộ sinh số giả ngẫu nhiên.

Thiếu cơ chế xác thực hai chiều: Trong lược đồ hình 1 dễ thấy rằng Peggy không có cơ chế nào để xác thực được có chính xác là Victor đã gửi c cho mình hay không và chỉ có Victor xác thực được Peggy khi kiểm tra phương trình đồng dư $t \equiv g^r y^c$. Như vậy, từ việc thiếu cơ chế xác thực Victor có thể dẫn tới việc kẻ tấn công giả mạo Victor để thực thi lược đồ.

Việc sinh giá trị x và v ngẫu nhiên tại phía Peggy (máy trạm) có thể tồn tại cửa hậu hoặc chu kỳ sinh số nhỏ dẫn tới kẻ tấn công tìm được giá trị x và phá vỡ lược đồ. Ví dụ được đưa ra trong [14], [15] về hàm sinh số giả ngẫu nhiên tồn tại cửa hậu như sau:

- Trong [14] là hàm getRandomNumber1 luôn trả về giá trị 4.

```
int getRandomNumber1()
{
    return 4;
}
```

- Trong [15] là hàm *getRandomNumber2* luôn trả về một số trong đoạn $[1, 100]$, như vậy kẻ tấn công hoàn toàn có thể thử vét cạn giá trị x, v trong đoạn này để tìm được giá trị y.

```
int getRandomNumber()
{
    srand(time(NULL));
int res = 1+ rand() % 100;
return res;
}
```

2.3. Đề xuất lược đồ ZKP kiểu Schnorr trên đường cong Elliptic

Trong [10], các tác giả đã đưa ra một số lược đồ ZKP kiểu Schnorr trên Elliptic và được chuẩn hóa với tài liệu RFC 8235 của tổ chức Internet Engineering Task Force. Chúng tôi sẽ không đưa ra cụ thể hoạt động của lược đồ ở đây do độ dài bài báo có hạn, tuy nhiên chúng tôi khẳng định rằng các lược đồ trong [10] vẫn tồn tại hai điểm yếu về bảo mật như lược đồ hình 1 là thiếu cơ chế xác

thực hai chiều và lỗi cài đặt bộ sinh số giả ngẫu nhiên. Trong bài báo này, chúng tôi đề xuất lược đồ ZKP kiểu Schnorr để khắc phục điểm yếu bảo mật tồn tại này với các bước thực hiện được mô tả theo hình 2.

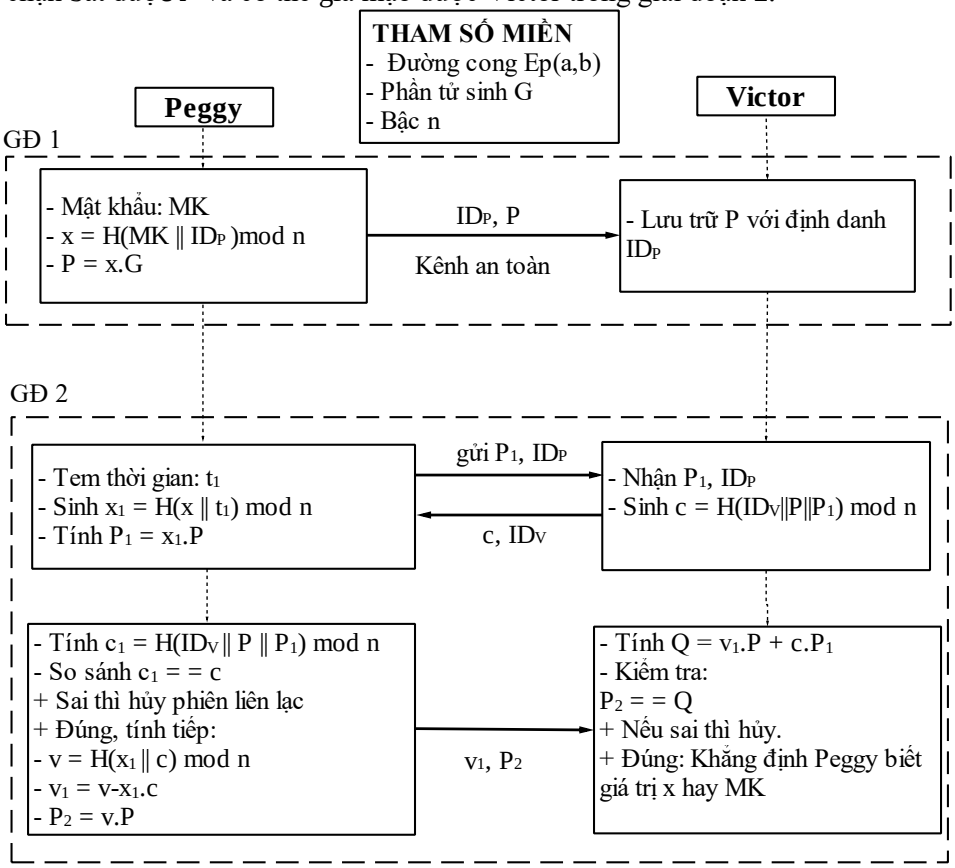
Ý nghĩa của lược đồ ZKP trong hình 2 là Peggy muốn chứng minh cho Victor rằng mình biết về giá trị bí mật x. Hoạt động của lược đồ đề xuất được mô tả như sau:

- Các tham số miền thực hiện trong lược đồ: Đường cong Elliptic dạng Weierstrass có phương trình dạng $y^2 = x^3 + ax + b$ trên trường F_p với p là số nguyên tố ($p > 3$) và hai số nguyên a, b thỏa mãn $4a^3 + 27b^2 \neq 0$, được ký hiệu là $E_p(a, b)$. G là phần tử sinh của đường cong $E_p(a, b)$ với bậc n và H là một hàm băm mật mã an toàn.

- Giai đoạn 1 – Đăng ký:

+ Peggy có một mật khẩu là MK, định danh ID_P, tiến hành tính giá trị x theo hàm băm H là $x = H(MK||ID_P) \, mod \, n$ và điểm $P = x.G$. Rồi gửi tọa độ điểm P tới Victor cùng với định danh ID_P của mình.

+ Victor sẽ lưu trữ điểm P với định danh của Peggy vào cơ sở dữ liệu để phục vụ cho việc xác minh trong giai đoạn 2. Chú ý giai đoạn 1 cần thực hiện trên kênh an toàn tránh việc bên thứ ba tấn công chặn bắt được P và có thể giả mạo được Victor trong giai đoạn 2.



Hình 2. *Lược đồ ZKP kiểu Schnorr trên đường cong Elliptic*

- Giai đoạn 2 – Xác minh:

+ Peggy tính giá trị $x_1 = H(x||t_1) \, mod \, n$ với $t_1$là tem thời gian thời điểm cần xác minh và điểm $P_1 = x_1.G$. Rồi gửi yêu cầu xác minh tới Victor chứa tọa độ điểm P_1 cùng với định danh ID_P của mình.

+ Victor nhận điểm P_1và định danh ID_P của Peggy sẽ tìm được điểm P tương ứng trong cơ sở dữ liệu đã lưu. Thực hiện tính giá trị $c = H(ID_V || P ||P_1) mod\ n$ và gửi tới Peggy cùng với định danh của mình.

+ Tiếp theo, Peggy tính toán giá trị trị $c_1 = H(ID_V || P ||P_1) mod\ n$ và so sánh với giá trị c đã nhận được từ Victor. Nếu giống nhau thì xác thực đúng Victor đang liên lạc và gửi thông tin đến, ngược lại thì hủy phiên liên lạc. Trường hợp giống nhau, thực hiện tính các giá trị $v = H(x_1 || c) mod\ n$, $v_1 = (v - cx)\ mod\ n$ và điểm $P_2 = v.P$ và gửi hai giá trị là v_1 và điểm P_2 ngược lại cho Victor.

+ Cuối cùng, Victor sẽ thực hiện so sánh hai điểm P_2 với Q với giá trị điểm $Q = v_1P + cP_3$. Nếu hai giá trị này giống nhau thì Victor sẽ khẳng định được rằng Peggy biết x, ngược lại thì không xác minh được Peggy có biết x hay không.

2.3.1. Xem xét kiểm tra các tính chất của lược đồ ZKP đề xuất

Completeness: Nếu Victor và Peggy là hai bên không bị giả mạo thì lược đồ hoàn thành khi hai giá trị 2 điểm P_2 và Q là giống nhau. Phân tích công thức tính: $\mathrm{Q} = v_1\mathrm{P} + \mathrm{c}P_1 = (\mathrm{v} - \mathrm{c}x_1)\mathrm{P} + \mathrm{c}(x_1\mathrm{P}) = \mathrm{vP} - \mathrm{c}x_1\mathrm{P} + \mathrm{c}x_1\mathrm{P} = \mathrm{vP} = P_2$. Như vậy, P_2 và Q là giống nhau hay lược đồ ZKP này hoàn thành.

Soundness: Thấy rằng, Peggy không thể bị giả mạo vì phương trình giá trị 2 điểm P_2 và Q là giống nhau khi và chỉ khi Peggy biết giá trị x.

Zero-Knowledge: Trong giai đoạn 2 thì thấy rằng Peggy không cung cấp giá trị x hoặc điểm P cho bên Victor để xác minh rằng Peggy biết x. Với kẻ tấn công thì chỉ biết giá trị P_1, c, v_1, P_2 chặn bắt được trên kênh truyền, suy ra để tìm giá trị x này thì cần phải giải bài toán logarit rời rạc trên trường Elliptic để tìm được x_1, v và đây là một bài toán khó không thể giải trong thời gian đa thức khi độ dài của p lớn.

2.3.2. Những ưu điểm của lược đồ đề xuất

Lược đồ ZKP chúng tôi đề xuất có những ưu điểm sau so với lược đồ hình 1 và các lược đồ trong [10]: độ dài khóa nhỏ và chi phí tính toán thấp, tính xác thực hai chiều, khả năng chống lỗi cài đặt.

Việc sử dụng Elliptic giúp sự an toàn của lược đồ ZKP đề xuất được đảm bảo bởi bài toán logarithm rời rạc trên đường cong Elliptic giúp giảm độ dài các tham số miền so với trên trường hữu hạn và vẫn đảm bảo được độ an toàn tương đương. Việc giảm độ dài các tham số miền giúp chi phí tính toán thấp hơn nhiều so với lược đồ ban đầu.

Lược đồ ZKP đề xuất có tính chất xác thực hai chiều (xác thực cả hai bên Peggy và Victor) trong khi lược đồ ZKP ban đầu chỉ xác thực bên Peggy.

Lược đồ ZKP đề xuất có khả năng chống lỗi cài đặt liên quan bộ sinh số giả ngẫu nhiên.

Chi tiết luận giải cho các ưu điểm này, chúng tôi trình bày trong phần 3 của bài báo.

3. Kết quả và bàn luận

Lược đồ ZKP đề xuất có ưu điểm về vấn đề an toàn và hiệu năng sẽ được chứng minh và thảo luận trong phần này của bài báo thông qua cơ sở lý thuyết toán học và kết quả thực nghiệm của chúng tôi.

3.1. Vấn đề an toàn của lược đồ ZKP đề xuất

Sự an toàn của lược đồ ZKP đề xuất cần xem xét các vấn đề:

- Vấn đề xác thực hai chiều trong ZKP: điều này dẫn tới khả năng kháng tấn công giả mạo hoặc xen giữa của lược đồ ZKP đề xuất.
- Vấn đề tấn công phá vỡ theo lý thuyết toán học của lược đồ. Cụ thể kẻ tấn công tiến hành chặn bắt được các giá trị $P_1, P_2, \mathrm{c}, v_1$ và tiến hành dự đoán các giá trị x_A và điểm P.
- Vấn đề lỗ hổng bảo mật trong bộ sinh số giả ngẫu nhiên
- Vấn đề tấn công tiêm lỗi vào hàm băm sinh tham số x, c, v
- Vấn đề kháng tấn công lượng tử

- Vấn đề thiết lập kênh an toàn trong giai đoạn đăng ký của lược đồ đề xuất

3.1.1. Vấn đề xác thực hai chiều

Trong giai đoạn 1 – Đăng ký của lược đồ được thực hiện trên kênh an toàn vì vậy giai đoạn này không xét đến vấn đề xác thực.

Trong giai đoạn 2 – Xác minh: Peggy tiến hành xác thực được Victor thông qua việc so sánh hai giá trị c và c_1. Dựa theo tính chất an toàn hàm băm mật mã H được sử dụng thì c và c_1bằng nhau khi và chỉ khi bên tính giá trị c biết chính xác giá trị điểm P hay chính là Victor. Còn Victor sẽ tiến hành xác thực được Peggy thông qua việc so sánh hai điểm P_2 và Q. Theo tính chất Completeness của ZKP đề xuất đã nêu thì P_2 và Q giống nhau khi Peggy biết chính xác giá trị điểm P đã đăng ký ban đầu với Victor.

3.1.2. Vấn đề tấn công lược đồ theo lý thuyết toán học

Trong giai đoạn 2, kẻ tấn công tiến hành chặn bắt được các giá trị P_1, P_2, c, v_1 và tiến hành dự đoán các giá trị x_A và điểm P. Cụ thể các bài toán cần giải đối với kẻ tấn công sẽ là:

- Biết được điểm P_1 tiến hành tìm các giá trị x_A và điểm P theo bài toán logarit rời rạc trên đường cong Elliptic với hai biến chưa biết là x_A và P. Bài toán chỉ có thể giải được bằng phương pháp tấn công vét cạn hết các giá trị x_A và P, điều này hoàn toàn không thể nào được thực hiện trong thời gian đa thức khi tham số miền đường cong sử dụng trong lược đồ ZKP đủ lớn hay số modulo p đủ lớn.

- Biết được giá trị c và v_1 tiến hành tìm giá trị x_A thông qua phương trình $v_1 = (v - cx_A)\ mod\ n$. Bài toán này cũng chỉ được giải khi thực thi vét cạn hết các giá trị có thể có của v, điều này cũng không thể nào được thực hiện trong thời gian đa thức khi lựa chọn tham số miền là điểm sinh G có bậc n đủ lớn.

- Biết được điểm P_2 thực hiện tìm các giá trị v và điểm P. Việc này tương tự như việc kẻ tấn công biết được điểm P_1 tiến hành tìm các giá trị x_A và điểm P. Tức là bài toán cũng không thể thực hiện được trong thời gian đa thức khi tham số miền đường cong sử dụng trong lược đồ ZKP đủ lớn hay số modulo p đủ lớn.

Như vậy, lược đồ ZKP đề xuất an toàn khi chúng ta lựa chọn tham số miền là các đường cong Elliptic an toàn. Chúng tôi tham khảo khuyến nghị theo hình 3 dưới đây 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 [12] được đưa ra năm 2020 (an toàn trước các cuộc tấn công phổ biến giải bài toán logarit rời rạc trên đường cong Elliptic [13]).

Từ số liệu khuyến nghị NIST thì việc thực thi lược đồ ZKP đề xuất có thể lựa chọn đường cong có độ dài số modulo p từ 256 bit trở lên để có mức bảo mật sử dụng tốt cho tới năm 2030 và lâu hơn nữa. Mức khuyến nghị này đưa ra có xem xét tới sự phát triển của tính toán lượng tử, cụ thể ở với đường cong Elliptic có số modulo dài 256 bit thì cần bộ nhớ 2330 qubit với máy tính lượng tử [11].

Date	Security Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
Legacy (1)	80	2TDEA	1024	160	1024	160	SHA-1 (2)	
2019 - 2030	112	(3TDEA) (3) AES-128	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2019 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128
2019 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
2019 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256

Hình 3. *Khuyến nghị NIST về độ an toàn và thời gian sử dụng các thuật toán mật mã cơ bản*

Từ bảng khuyến nghị thì chúng ta cũng thấy rằng lược đồ ZKP đề xuất có thêm một số ưu điểm so với lược đồ ZKP kiểu Schnorr trên trường hữu hạn. Đó là lược đồ ZKP đề xuất dựa trên đường cong Elliptic với độ an toàn bằng nhau nhưng độ dài số nguyên tố modulo nhỏ hơn rất nhiều so với trường hữu hạn. Điều này giúp việc sinh khóa, dung lượng trao đổi của lược đồ ZKP đề xuất được tiết kiệm chi phí đáng kể so với lược đồ ZKP trên trường hữu hạn. Vấn đề sẽ rất có lợi khi lược đồ ZKP đề xuất được áp dụng vào hệ thống xác thực với cả hàng triệu người dùng.

3.1.3. Vấn đề lỗ hổng bảo mật trong bộ sinh số giả ngẫu nhiên

Trong lược đồ ZKP kiểu Schnorr trên trường hữu hạn (hình 1) và các phiên bản khác của lược đồ này trên đường cong Elliptic, cụ thể trong [10], thì các giá trị x, c, v đều được sinh giả ngẫu nhiên theo bộ tạo số bằng phần cứng hoặc phần mềm.

Như trong mục 2.2.2. đã trình bày trong [14] và [15] 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. Điều này gây ra phá vỡ hoạt động lược đồ bởi từ việc biết các giá trị x, c, v thì kẻ tấn công luôn tìm được điểm P.

Chúng tôi sử dụng hàm băm mật mã thay cho các bộ tạo số giả ngẫu nhiên trong lược đồ đề xuất, điều này được khẳng định là khắc phục được việc cài đặt bộ tạo số giả ngẫu nhiên có lỗ hổng bảo mật như công bố trong [16] trong lược đồ ký số EdDSA của tác giả Bernstein.

3.1.4. Vấn đề tấn công tiêm lỗi vào hàm băm sinh tham số x, c, v

Khi sử dụng hàm băm thay cho bộ sinh số giả ngẫu nhiên thì tồn tại các tấn công tiêm lỗi vào quá trình hoạt động hàm băm từ đó dự đoán được đầu ra hay các giá trị x, c, v. Vấn đề đã được công bố trong các công trình [17] lên lược đồ ký số EdDSA và lược đồ đề xuất cũng sẽ bị ảnh hưởng.

Cũng trong [17] đưa ra giải pháp phòng chống cho tấn công tiêm lỗi là sử dụng thêm một đầu vào ngẫu nhiên cho hàm băm. Trong đề xuất của chúng tôi đã sử dụng tem thời gian như một đầu vào ngẫu nhiên thêm vào này (các giá trị v, c sinh đều phụ thuộc vào thời gian t), vì vậy lược đồ đề xuất của chúng tôi có khả năng phòng chống được các cuộc tấn công tiêm lỗi vào hàm băm.

Chú ý việc cài đặt lược đồ mà không có triển khai hệ thống tem thời gian thì có thể lấy thời gian thực trên thiết bị để thực hiện lược đồ.

3.1.5. Vấn đề kháng tấn công lượng tử

Các thuật toán mật mã dựa trên bài toán phân tích số nguyên như RSA hay bài toán logarit rời rạc trên đường cong Elliptic (ECDLP – Elliptic Curve Discrete Logarithm Problem) đều bị ảnh hưởng bởi tấn công lượng tử, cụ thể là thuật toán Shor. Trong [11] đưa ra số lượng qubit tối thiểu giải bài toán phân tích số nguyên và logarit rời rạc theo độ an toàn tương đương độ dài tham số khóa hay số modulo như trong bảng 1.

Bảng 1. *Số qubit tối thiểu giải bài toán phân tích số nguyên và ECDLP*

Độ an toàn	Số qubit cần thiết giải bài toán phân tích số nguyên trong thuật toán RSA hoặc DSA	Số qubit cần thiết giải bài toán ECDLP
112	4098	2042
128	6146	2330
192	15362	3484

Lược đồ ZKP đề xuất dựa trên bài toán ECDLP vì vậy bị ảnh hưởng bởi tấn công Shor trên máy tính lượng tử, tuy nhiên theo bảng 1 thì khi lựa chọn tham số cho lược đồ đề xuất có độ an toàn từ 112 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 NIST trong hình 3 thì khi lựa chọn tham số cho lược đồ ZKP đề xuất có độ an toàn từ 128 bit thì lược đồ có thể sử dụng đến 2030 hoặc lâu hơn nữa.

3.1.5. Vấn đề thiết lập kênh an toàn trong giai đoạn đăng ký của lược đồ đề xuất

Một nhược điểm của lược đồ đề xuất trong bài báo này là giai đoạn đăng ký cần thiết lập một kênh truyền an toàn để truyền giá trị điểm P tới bên chứng minh. Với kênh an toàn này thì lược đồ đề xuất sẽ cần thêm giải pháp để thiết lập kênh này và dẫn tới tốn kém chi phí hơn so với lược đồ hình 1 và lược đồ công bố trong [10].

Lý giải cho việc thiết lập kênh truyền an toàn trong lược đồ đề xuất: với lược đồ hình 1 không yêu cầu kênh truyền an toàn trong giai đoạn đăng ký vì xuất phát từ mục tiêu lược đồ là Peggy biết x và chỉ đưa ra giá trị y để bên Victor hoặc bất kỳ bên nào khác có thể xác minh được Peggy biết x dựa trên giá trị y này và các giá trị liên quan khác như t, c, r. Nhưng xét trên khía cạnh ứng dụng lược đồ này trong mạng máy tính, cụ thể mô hình mạng Client-Server đang áp dụng phổ biến hiện nay thì Peggy chính là người dùng phía Client và Victor là phía Server. Vậy thì các giá trị x, y tương ứng với thông tin xác thực của người dùng Peggy cần được đăng ký bởi một Server cụ thể (ở đây là Victor) để phục vụ cho việc đăng nhập hoặc sử dụng dịch mạng trong hệ thống. Trường hợp y mà được công khai tức truyền qua kênh công khai trong giai đoạn đăng ký thì bên Server phải công bố công khai giá trị này là của người dùng Peggy tức là phải có thêm giải pháp kiểm tra công bố này. Thực tế hiện nay việc công bố giá trị y có thể thực hiện giống với việc công bố khóa công khai người dùng thông qua chứng thư số, tuy nhiên giải pháp này cần thiết lập hệ thống PKI với trung tâm CA tin cậy điều này thực sự tốn kém và sẽ yêu cầu thêm chi phí duy trì từ phía người dùng (giống việc người dùng mua chứng thư số). Vì vậy, chúng tôi đề xuất giữ bí mật giá trị y này (hay chính là P trong lược đồ hình 2) khi này phía Server không cần có giải pháp công bố và xác minh giá trị y. Vấn đề xác minh Peggy biết x đối với phía Server Victor là diễn ra bình thường, còn với các bên khác muốn xác minh thì chỉ cần gửi các giá trị tham số liên quan khác (như t, c, r trong lược đồ hình 1 hay P_1, v_1 trong lược đồ hình 2) tới phía Server Vitor để xác minh là được. Điều này hợp lý vì hoàn toàn giống với giải pháp Single Sign-On của tập đoàn Google khi các máy chủ dịch vụ của các công ty khác chấp nhận cho đăng nhập với tài khoản Gmail thì sẽ yêu cầu người dùng cung cấp tài khoản/mật khẩu Gmail trên trang đăng nhập tại máy chủ dịch vụ và chuyển tiếp về cho bên máy chủ Google để xác minh và chấp thuận kết quả xác minh này.

Như vậy theo lập luận ở trên thấy rằng vấn đề thiết lập kênh an toàn trong giai đoạn đăng ký giúp cho lược đồ ZKP đề xuất sẽ hoạt động tốt cho mô hình mạng Client/Server. Và giải pháp để thiết lập kênh truyền này hoàn toàn giống với việc thiết lập kênh truyền an toàn cho việc đăng ký tài khoản/mật khẩu người dùng trên Server đang diễn ra trong hệ thống mạng máy tính hiện nay. Tức là điều này hoàn toàn khả thi và không hề tốn kém bằng việc thiết lập hệ thống PKI. Trên thực tế các giải pháp cho vấn đề này có thể thực hiện như sau:

- Đối với mạng riêng của một tổ chức, doanh nghiệp giai đoạn đăng ký được thực hiện trực tiếp bởi người quản trị cung cấp cho mỗi nhân viên, cán bộ một mật khẩu và thiết lập thêm yêu cầu thay đổi mật khẩu ở lần đăng nhập đầu tiên.
- Đối với mạng Internet có thể thiết lập kênh truyền bảo mật qua giao thức TLS hoặc thông qua hệ thống Email có bảo mật.

3.2. Về hiệu năng lược đồ ZKP đề xuất

Để đánh giá hiệu năng giải pháp đề xuất, chúng tôi thực hiện cài đặt thực nghiệm so sánh lược đồ đề xuất và lược đồ ZKP kiểu Schnorr trên trường hữu hạn. Tham số miền của lược đồ ZKP trên trường hữu hạn sử dụng tham số của giao thức Diffie-Hellman nhóm 15 trong [18] với p có độ dài 3072 bit và $g = 2$, còn tham số miền ZKP đề xuất sử dụng là đường cong chuẩn SECP là secp256k1 với p có độ dài 256 bit. Các tham số lược đồ ZKP hình 1 và đề xuất được chọn như vậy vì nó đảm bảo hai lược đồ có cùng độ an toàn mức 128 bit.

Việc cài đặt này sử dụng ngôn ngữ lập trình Python với giao diện Console trên cùng nền tảng phần cứng là Laptop HP ZBOOK 15 với RAM 16GB, HĐH Windows 11, 64 bit, Intel(R) Core(TM) i7-4800 MQ CPU @ 3.00GHz. Các kết quả đo thực tế được đưa ra theo bảng 2.

Bảng 2. *Bảng so sánh kết quả thực nghiệm của giải pháp đề xuất và lược đồ ZKP trên trường hữu hạn*

Phiên bản	Thời gian thực thi trung bình (giây)	Số thông điệp trao đổi	Dung lượng trao đổi (max byte)
Lược đồ ZKP Schnorr trên trường hữu hạn	3,62	4	1056
Lược đồ ZKP đề xuất	0,032	4	320

Dữ liệu trên bảng 2 cho thấy thời gian thực thi lược đồ ZKP đề xuất nhanh hơn rất nhiều lần so với trên trường hữu hạn. Điều này được lý giải do việc tính toán trên đường cong Elliptic với các tham số miền có độ dài bit nhỏ hơn trên trường hữu hạn. Và điều này dẫn tới lược đồ có thể được triển khai tốt cho các thiết bị tài nguyên hạn chế (như được chỉ ra trong [10]). Số thông điệp trao đổi lược đồ đề xuất bằng so với phiên bản ZKP trên trường hữu hạn, tuy nhiên kích cỡ thông điệp nhỏ hơn nhiều cho nên lược đồ đề xuất tận dụng băng thông mạng tốt hơn.

4. Kết luận

Bài báo đã đưa ra đề xuất về một lược đồ ZKP có tương tác kiểu Schnorr trên đường cong Elliptic. Với những thông số về độ an toàn và hiệu năng đã được chứng minh trong bài báo thì lược đồ đề xuất có tiềm năng và khả thi để áp dụng trong thực tế các hệ thống xác thực hoặc trong công nghệ Blockchain.

TÀI LIỆU THAM KHẢO/ REFERENCES

[1] Goldwasser, "The Knowledge Complexity of interactive Proof Systems," in *Proceedings of the 17th ACM Symposiumon Theory of Computing*, 1985, pp. 186-208.

[2] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. CRYPTO*, 1986, pp. 186-194.

[3] J. Camenisch and M. Stadler, "Proof Systems for General Statements about Discrete Logarithms," *Technical Report*, Dept. of Computer Science, Zurich, 1997.

[4] D. Chaum, J.-H. Evertse, and J. van de Graaf, "An improved protocol for demonstrating possession of discrete logarithms and some generalizations," in *EUROCRYPT*, 1987, pp. 127–141.

[5] J. Partala1, T. H. Nguyen, and S. Pirttikangas, "Non-interactive Zero-knowledge for Blockchain: A Survey," *IEEE Access*, vol. 8, pp. 945 – 961, 2020.

[6] F. Hao and P. Y. A. Ryan, "Password authenticated key exchange by juggling," in *International Workshop on Security Protocols*, Springer, 2008, pp. 159–171.

[7] M. Chase, D. Derler *et al.*, "Picnic signature scheme," *github.com*, 2017. [Online]. Available: https://github.com/microsoft/Picnic/tree/master/spec [Accessed May 03, 2023].

[8] N. Bitansky, "From extractable collision resistance to succinct non-interactive arguments of knowledge, and backagain," in *Proceedings of 3rd innovations in Theoritical Computer Science Conference*, 2012, pp. 326–349.

[9] X. F. Li, "Shell proof: More Efficient Zero-Knowledge Proofs for Confidential Transactions in Blockchain," *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020, pp. 46-59.

[10] F. Hao, "Schnorr Non-interactive Zero-Knowledge Proof," *Internet Engineering Task Force Documents*, RFC 8235, 2017.

[11] 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.

[12] D. Giry, "Recommendation for Key Management," *Special Publication* 800-57 Part 1 Rev. 5, NIST, 05/2020. [Online]. Available: https://www.keylength.com/en/4/. [Accessed May 04, 2023].

[13] T. M. Aung and N. N. Hla, "A Study of General Attacks on Elliptic Curve Discrete Logarithm Problem over Prime Field and Binary Field," *World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering*, vol. 11, no. 11, pp. 1121 – 1128, 2017.

[14] F. Valsorda, "Exploiting ECDSA failures in the bitcoin blockchain," in *Proceedings of Hack in The Box (HITB) - Cloudflare*, 2014, pp. 57 – 66.

[15] 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'2022),* Ha Noi – Viet Nam, 2022, pp. 90-94.

[16] 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.

[17] Y. Romailler and S. Pelissier, "Practical fault attack against the Ed25519 and EdDSA signature schemes," *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, vol. 1, pp. 17-24, 2017.

[18] M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)," *Internet Engineering Task Force Documents* - RFC 3526, 2003.