2024 ICCE-Taiwan 1571008532

2024 International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan) | 979-8-3503-8684-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCE-Taiwan62264.2024.10674337

Key Expansion Based on Elliptic Curve Cryptography for Anonymous Voting

Abel C. H. Chen
Information & Communications Security Laboratory
Chunghwa Telecom Laboratories,Taoyuan, Taiwan
chchen.scholar@gmail.com
0000-0003-3628-3033

Chia-Yu Lin*
Department of Computer Science & Information Engineering
National Central University,Taoyuan, Taiwan
sallylin0121@ncu.edu.tw (Corresponding Author)
0000-0002-5106-7286

***Abstract*—This study designs a security credential management system, including a certificate authority (CA), a registration authority (RA), and other individuals outside the CA and the RA. An anonymous voting method using elliptic curve cryptography (ECC)-based key expansion has been proposed to achieve anonymity to CA, RA, and individuals. In experiments, the performance of the proposed method based on different security strengths has been evaluated.**

***Index Terms*—Key expansion, elliptic curve cryptography, anonymous voting**

I. Introduction

Voting is a means of expressing public opinion. However, to allow individuals to express their thoughts freely, it is common to adopt an anonymous approach to protect everyone from potential attacks when expressing their opinions. With the development of information security and cryptography, digital voting has become a viable solution. Nevertheless, ensuring anonymity in digital voting will be a key consideration influencing the public's willingness to use it.

The current commonly used cryptography method, elliptic curve cryptography (ECC) [1], allows the generation and verification of signatures through the use of elliptic curve digital signature algorithm (ECDSA) [2]. However, it is possible to trace the public key in the certificate back to its owner. Therefore, some studies have proposed solutions such as implicit certificates [3] and anonymous authentication [4] to achieve anonymity based on key expansion. However, these methods only offer anonymity to individuals outside the certificate authority (CA), as the CA can still trace the ownership of the public key before key expansion. In response to this issue, this study aims to propose the design of an anonymous voting method using ECC-based key expansion, achieving anonymity not only towards the Certificate Authority but also towards all participants and devices involved.

II. Elliptic Curve Cryptography

This section presents the key generation and key expansion based on ECC. An elliptic curve (EC) point (x, y) with constants α and β can be defined by Eq. (1) [5]. The stanard of National Institute of Standards and Technology (NIST) [1] for secure ECC parameters, including the values of α, β, a prime modulus p, and the base point G can be adopted. The key generation and key expansion based on ECC are illustrated in Subsection II.A and II.B.

$$y^2 = x^3 + \alpha x + \beta \tag{1}$$

A. Key Generation

For key generation, an integer number a can be randomly generated. Subsequently, the random integer number a is subjected to modulo the prime modulus p to obtain the integer a' as a private key. The public key A is generated using the integer a' and the base point G according to Eq. (2) [5].

$$A = a'G \quad \text{where} \quad a' \equiv a \pmod{p} \tag{2}$$

B. Key Expansion

For key expansion, another integer number r_1 is randomly generated. Subsequently, the random integer r_1 is subjected to modulo the prime modulus p to obtain the integer r_1' as a private reconstruction value. The public reconstruction value R_1 is generated using the integer r_1' and the base point G according to Eq. (3). Furthermore, the expanded public key B can be generated based on the original public key A and the public reconstruction value R_1, and the expanded private key B can be generated based on the original private key a' and the private reconstruction value r_1' (as shown in Eq. (4)) [5].

$$R_1 = r_1'G \quad \text{where} \quad r_1' \equiv r_1 \pmod{p} \tag{3}$$

$$\begin{aligned} B &= A + R_1 = a'G + r_1'G = (a' + r_1')G \\ &= b'G \quad \text{where} \quad b \equiv a' + r_1' \pmod{p} \end{aligned} \tag{4}$$

III. Anonymous Voting Method Using ECC-Based Key Expansion

Subsection III.A defines the objectives of anonymous voting based on digital signature algorithm (DSA), and the detailed steps of the proposed method is presented in Subsection III.B.

Authorized licensed use limited to: National Central University. Downloaded on November 06,2024 at 02:35:32 UTC from IEEE Xplore. Restrictions apply.

979-8-3503-8684-4/24/$31.00 ©2024 IEEE

A. Objectives

This study designs a security credential management system including a CA, a registration authority (RA), and other individuals outside the CA and the RA. Therefore, the proposed method should satisfy the following requirements.

- Anonymity to CA
- Anonymity to RA
- Anonymity to individuals outside the CA and the RA

B. The Proposed Method

In this process, each township or city office (i.e. an election operation center (EOC)) can take on the role of RA. After confirming the accuracy of citizen's identities, the RA can perform the first key expansion on the citizen's original public key (e.g. A Eq. (2)) to generate the the first expanded public keys (e.g. B Eq. (4)). The central election commission (CEC) can act as the CA, upon receiving the first expanded public key B from various township or city offices (i.e., the EOC), perform the second key expansion C based on Eqs. (5) and (6). The CA (i.e. CEC) can generate the anonymous certificate $Cert$ including the the second key expansion C for voting. The detailed steps are illustrated in Fig. 1.

$$R_2 = r_2' G \quad \text{where} \quad r_2' \equiv r_2 \pmod{p} \tag{5}$$

$$\begin{aligned} C = B + R_2 &= b'G + r_2'G = (b' + r_2')G \\ &= cG \quad \text{where} \quad c \equiv b' + r_2' \pmod{p} \end{aligned} \tag{6}$$

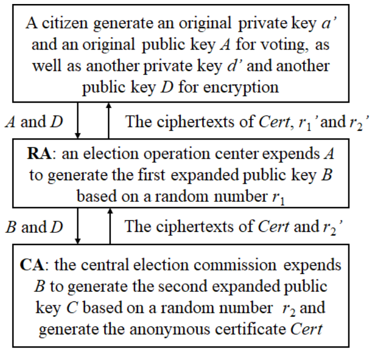
A citizen generate an original private key a' and an original public key A for voting, as well as another private key d' and another public key D for encryption
A and D
The ciphertexts of $Cert$, r_1' and r_2'
RA: an election operation center expends A to generate the first expanded public key B based on a random number r_1
B and D
The ciphertexts of $Cert$ and r_2'
CA: the central election commission expends B to generate the second expanded public key C based on a random number r_2 and generate the anonymous certificate $Cert$

Fig. 1. The proposed method.

Furthermore, the citizen generates another private key d' and another public key D for encryption. The public key D can be sent to both the RA and the CA. The CA utilizes D to encrypt the anonymous certificate $Cert$ and the second private reconstruction value r_2' based on elliptic curve integrated encryption scheme (ECIES) [6]. The ciphertexts of $Cert$ and r_2' are then sent from the CA to the RA. Subsequently, the RA employs D to encrypt the first private reconstruction value r_1' based on ECIES, and the ciphertexts of $Cert$, r_2', and r_1' can be sent from the RA to the citizen. Finally, the citizen uses the private key d' to decrypt the ciphertexts and generate the first expanded private key b based on Eq. (4) and the second expanded private key c based on Eq. (6).

Through the first key expansion, anonymity to individuals outside the RA can be achieved. Therefore, when the CA receives the first expanded public key B, it is no longer possible to trace the original public keys A from the first expanded public key B. Subsequently, after the CA performs the second key expansion, anonymity toward the RA can also be achieved, ensuring that the proposed method meets the requirements for anonymity.

IV. Experimental Results and Discussions

This study adopts the security strengths defined by NIST [7] for performance evaluation. Table I displays the computation time, and the proposed method can be completed at millisecond speed, regardless of the security strength.

TABLE I
The evaluation of computation time (Unit: milliseconds)

Security Strength	Key Generation	Public Key Exp.	Private Key Exp.
80	6.149	5.941	0.001
112	6.205	5.862	0.001
128	6.218	5.970	0.001
192	9.011	8.502	0.002
256	11.338	11.232	0.002

V. Conclusions and Future Work

An anonymous voting method using ECC-based key expansion has been proposed to achieve anonymity for CA, RA, and individuals. In the future, verification can be directed toward citizens' willingness and behavior, for example, through the adoption of technology acceptance models.

Acknowledgements

This work is sponsored by the National Science and Technology Council (NSTC) under the project NSTC 110-2222-E-008-008-MY3.

References

[1] L. Chen, D. Moody, K. Randall, A. Regenscheid and A. Robinson, "Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters," NIST SP 800-186, 2023.

[2] H. Zhang et al., "Asynchronous Threshold ECDSA With Batch Processing," in IEEE Transactions on Computational Social Systems, vol. 11, no. 1, pp. 566-575, 2024.

[3] H. Sun, W. Luo, J. Weng, Z. Liu and M. Li, "ECQV-GDH-Based Group Key Exchange Protocol for CAN Bus," in IEEE Transactions on Vehicular Technology, vol. 72, no. 10, pp. 12857-12872, 20235.

[4] H. Ma, C. Wang, G. Xu, Q. Cao, G. Xu and L. Duan, "Anonymous Authentication Protocol Based on Physical Unclonable Function and Elliptic Curve Cryptography for Smart Grid," in IEEE Systems Journal, vol. 17, no. 4, pp. 6425-6436, 2023.

[5] A. C. H. Chen, "Evaluation and Analysis of Standard Security Techniques in V2X Communication: Exploring the Cracking of ECQV Implicit Certificates," IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT), 2023.

[6] P. Realpe-Muñoz, J. Velasco-Medina, and G. Adolfo-David, "Design of an S-ECIES Cryptoprocessor Using Gaussian Normal Bases Over GF(2m)," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 4, pp. 657-666, 2021.

[7] E. Barker, "Recommendation for Key Management: Part 1 – General", NIST SP 800-57 Part 1 Revision 5, 2023.

Authorized licensed use limited to: National Central University. Downloaded on November 06,2024 at 02:35:32 UTC from IEEE Xplore. Restrictions apply.