Some Fields for the ElGamal Algorithm

Toan Nguyen Duc
Food industrial College

Hong Bui The
Hung Yen University of Technology and Education

Abstract
In this paper, we develop a new encryption scheme based on the ELGAMAL encryption algorithm and the degree of difficulty of the discrete logarithm problem (DLP). In public key cryptography, a secret key is often used for a long period of time, thus expelling the secret key. Moreover, devices used to calculate cryptography can also be physically attacked, leading to the secret key being exposed. This paper proposes a new encryption scheme to reduce the risk of revealing a secret key.

Keywords:
ElGamal, discrete logarithm, secret key

1. INTRODUCTION

In recent years cryptography uses and attaches more mathematics, encryption is more used in network security. This is a very important industry and has many uses in human social life. Along with the development of the Internet, cryptographic research has become increasingly diversified, opening up many areas of research in depth. Encryption applications not only encrypt and decode information but also cover a variety of issues that need to be investigated and resolved such as: authenticating the origin of information content, authenticating the owner of the lock code, The process of exchanging information securely online.

However, the security and coding time is the problem that algorithms tend to optimize in addition to the key exchange problem is also a general impediment to the algorithm. This issue may refer to two recent articles, one about the safety of Poincheval and Stern and the counterfeiting of Bleichenbacher's signature. In order to overcome these obstacles, we propose to develop a new encryption scheme based on the ELGAMAL encryption algorithm and the difficulty of the discrete logistic problem (DLP).

The rest of the article is presented as follows. Part 2: Some basic concepts and schemas proposed. Part 3: Conclusion, Part 4: References.

Manuscript received March 5, 2026
Manuscript revised March 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.3.6

2. SOME BASIC CONCEPTS AND AGE TO PROPOSE

A. ElGamal Encryption [3]

Elgama bile was proposed in 1984 on the basis of a discrete logarithm problem. Then, the US DSS [6] and GOST R34.10-94 [7] of the Russian Federation were developed on the basis of the digital signature algorithm of the cryptosystem, while the cryptographic algorithm The ElGamal public key has been used by the National Security Agency (NSA).

+) *Parametric and key shaping algorithms*

The members of the system want to exchange confidential information with Elgamma cryptographic algorithm, the key formation process is as follows:

1- Select prime numbers large enough p so that the logarithm problem in Z_p is hard to solve.

2- Select $g \in Z^*_p$ as the primitive element.

3- Select the secret key x as a random number such that: $1 < x < p$.

Generic public key y according to the formula:

$y = g^x \bmod p$.

+) *Encryption algorithms*

Suppose the sender is A, the receiver is B. The sender A has the secret key: x_A and the public key is: y_A.

The receiver B has a secret key of :x_B and the public key is: y_B. Then, to send message M to B, with: $0 \leq M < p$, Sender A will perform the following steps:

1- Select the random number k satisfactory: $1 < k < p$. Calculate the R value by the formula:

$$R = g^k \bmod p.$$

2- Use public key of B to calculate:

$$C = M \times (y_B)^k \bmod p$$

3- Send the code (C, R) to the receiver B.

+) *Decoding algorithms*

To retrieve the original message (M) from the ciphertext (C, R) received, the receiver B performs the following steps:

1- Calculate the Z value by the formula:

$$Z = R^{xB} \bmod p = g^{k.xB} \bmod p$$

2- Calculate the inverse of Z:

$$Z^{-1} = (g^{k.xB})^{-1} \bmod p = g^{-k.xB} \bmod p$$

3- Restore initial message *(M):*

$$= C \times Z^{-1} \bmod p$$

+) *Correctness of Elgamal Cryptographic Algorithm*

Suppose the message received after decryption *(C, R)* is $\overline{M}$

$\overline{M} = C \text{ x } Z^{-1} \bmod p =$

$[(M \times (y_B)^k \bmod p) \times (g^{-k.xB} \bmod p)] \bmod p$

$M \times g^{k.xB} \times g^{-k.xB} \bmod p = M$

Thus, the message received after decoding (M) is the original message (M).

B. Proposed new schema based on ElGamal

+) *Parametric and key formation [2]*

- Choose a pair of prime numbers p and q with *(p-1 / 2q)* as prime numbers.
- Select random primes p_1 with length $|p| - |q| - 1$. -
- Select g as the primitive element: $g \in Z_p$ Assuming the sender is A, the receiver is B. The key exchange on the *DLP* problem with general parameters is (p, q, g). In which A has the secret key: $x_A \in [1,q-1]$.

The public key is: y_A. $y_A = g^{xA} \bmod p$

B has a secret key: x_B, the public key is: y_B.

$y_B = g^{xB} \bmod p$

-Choose hash function safe (Hash): $H\{0,1\}^* \rightarrow Z_q$

This algorithm can be attacked when reusing x. So we use the value $H(x \| M)$ instead of x.

Then the public key will be calculated according to the formula : $y_A = g_A^{H(x \| M)} \bmod p$

$$y_B = g_B^{H(x \| M)} \bmod p$$

+) *Encryption and decryption algorithms*

Suppose the sender is A, the receiver is B. The sender A has the secret key: x_A and the public key is: y_A.

The receiver B has a secret key of : x_B and the public key is: y_B. Then, to send message M to B, with: $0 \le M < p$, Sender A will perform the following steps:

1- Select the random number k satisfactory: $1 < k < p$. Calculate the R value by the formula:

$$R = g^k \bmod p.$$

2- Use public key of B to calculate:

$$C = M \times (y_B)^k \bmod p$$

3- Send the code *(C, R)* to the receiver B.

+) *Decoding algorithms*

To retrieve the original message *(M)* from the ciphertext *(C, R)* received, the receiver B performs the following steps:

1- Calculate the Z value by the formula:

$$Z = R_B^{H(x \| M} \bmod p$$

2- Calculate the inverse of Z:

$$Z^{-1} = (g_B^{H(x \| M)})^{-1} \bmod p = g^{-H(x \| M)} \bmod p$$

3- Restore initial message *(M):*

$$M = C \times Z^{-1} \bmod p$$

+) *Correctness of Elgamal Cryptographic Algorithm*

Suppose the message received after decryption *(C, R)* is $\overline{M}$

$\overline{M} = C \text{ x } Z^{-1} \bmod p =$

$[(M \times (y_B)^k \bmod p) \times (g_B^{-k.H(x \| M)} \bmod p)] \bmod p$

$M \times g_B^{k.H(x \| M)} \times g_B^{-k.H(x \| M)} \bmod p = M$

Thus, the message received after decoding (M) is the original message (M).

C. Proposed new 2 schema based on ElGamal

- Choose a pair of prime numbers p and q with *(p-1 / 2q)* as prime numbers.
- Select random primes p_1 with length $|p| - |q| - 1$. -
- Select g as the primitive element: $g \in Z_p$ Assuming the sender is A, the receiver is B. The key exchange on the *DLP* problem with general parameters is (p, q, g). In which A has the secret key: $x_A \in [1,q-1]$.

The public key is: y_A. $y_A = g^{xA} \bmod p$

B has a secret key: x_B, the public key is: y_B.

$y_B = g^{xB} \bmod p$

-Choose hash function safe (Hash): $H\{0,1\}^* \rightarrow Z_q$

This algorithm can be attacked when reusing x. So we use the value $H(x | M)$ instead of x.

Then the public key will be calculated according to the formula : $y_A = g_A^{H(x \| M)} \bmod p$

$$y_B = g_B^{H(x \| M)} \bmod p$$

+) *Encryption and decryption algorithms*

Suppose the sender is A, the receiver is B. The sender A has the secret key: x_A and the public key is: y_A.

The receiver B has a secret key of : x_B and the public key is: y_B. Then, to send message M to B, with: $0 \le M < p$, Sender A will perform the following steps:

1- Select the random number k satisfactory: $1 < k < p$.
2- Select $K_A \in Z_q$

3- - Calculating $R_A = g_A^{H(x\|M)} mod\ p$
4- - Calculate $K_A = (R_B \text{ x } y_B)^{H(x\|M)} mod\ p$
5- - Key function: $K = H(y_B^{KA}, R_A, d)$, where d is the time of label
6- - Calculate $C = M \text{ x} (y_B)^{H(x\|M)} mod\ p$
7- - Send RA, d, C to B

Step 2: Person B
8- Select $K_B \epsilon Z_q$.
9- Calculate $K_B = (R_A \text{ x } y_A)^{H(x|M|)} mod\ p$
10- Calculate $R_B = g_B^{H(x\lceil M\rceil)} mod\ p$
11- Calculate $K = H(R_A^{H(x\|M)}, R_A, d)$
12- Calculate $\bar{M} = C \text{ x } (\bar{R}_A)^{H(x\|M}$ mod p
13- Testing: $E_A = E'_A$
14- If the wrong stop, the transaction fails
15- If true then the post-decrypt message is safe and is the original message

D. *Prove the correctness of the algorithm:*

If $K_A = K_B$

$K_A = (y_B \text{ x } R_B)^{H(x\|M} = (g_B)^{H(x\|M} (R_B^{H(x\|M} = g_A^{H(x\|M} R_A^{H(x\|M} = (R_A \text{ x } y_A)^{H(x\|M} = K_B$

Similarly we will prove: $\bar{M} = M$ when $g_A = g_B$

We have:

$\bar{M} = C \text{ x } (\bar{R}_A)^{H(x\|M} = M \text{ x } (y_B)^{H(x\|M} \text{ x } (\bar{R}_A)^{H(x\|M}$

Which: $y_B = g_B^{H(x\|M}$

That $R_A = g_A^{H(x\|M}$ should

$(\bar{R}_A) = g_A^{-H(x\|M}$

replace the formula we have:

$$\bar{M} = M \text{ x } g_B^{H(x\|M} \text{ x } g_A^{-H(x\|M}$$

$\bar{M} = M$ (Article must prove)

3. CONCLUSION

The article proposes a new encoding scheme based on the *ELGAMAL* encryption algorithm and the difficulty of the discrete logarithm problem *(DLP).* However, with prime q of size 160bit to solve the discrete Logarithm problem $y_A = g^x A\ mod\ p$, where g is an element of q in Z_p, it should use $O(2^{80})$ operations, with the current methods post This math is very difficult to solve. The proposed encryption scheme addresses the disadvantages of revealing a secret key for a period of time, and the applicability of the advanced algorithm is fully applicable in practice.

References

[1] Nguyen Binh, Nguyen Minh Trung, *"Some Modified Forms of the ELGAMAL Cryptosystem on Discrete Logical Problem"*, Institute of Technology, Post and Telecommunications, 2016.

[2] Nguyen Quoc Toan, Do Dai Chi, Trieu Quang Phong *"On a parameter standard for discrete logarithm problem"* Journal of Information Security, Government Cipher Board, (2016)

[3] Luu Hong Dung, *"Development of public key cryptography algorithm based on ElGamal Cryptosystem",* Specialized Research, Development and Application of Information and Communication Technology, Journal of Science and Technique Institute of Psychology), No. 149 (08-2012).

[4] D. Pointcheval, J. Stern. *"Security proofs for signature schemes"*, EUROCRYPT'96, vol. 1070, pp. 387-398, 1996.

[5] D. Bleichenbacher, *"Generating ElGamal Signatures Without Knowing the Secret Key"*, EUROCRYPT'96, vol. 1070, pp. 10-18, 1996.

[6] National Institute of Standards and Technology, NIST FIPS PUB 186-3. Digital Signature Standard, U.S. Department of Commerce,1994.

[7] GOST R 34.10-94. Russian Federation Standard. Information Technology,"*Cryptographic data Security. Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm"*, Government Committee of the Russia for Standards, 1994 (in Russian).

Toan Nguyen Duc, Graduated Master Degree in 2015. Current College of Food Industries. Studying for PhD in Thai Nguyen University. Research area: Security and confidential information.
ductoanndt9@gmail.com

Hong Bui The, Graduated from Hanoi University. Associate Professor Ph.D. Show art at Hung Yen University of Technical Education. Areas of Study: Password Security and Security, Cryptography, Machine Learning.