International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34974-34977

Threshold Cryptosystem with Factoring and Elliptic Curve Discrete Logarithm Problems

Mohd Saiful Adli Mohamad
Lecturer,
School of Quantitative Sciences,
Universiti Utara Malaysia,
06010 UUM Sintok, Kedah, Malaysia
msadli@uum.edu.my

Eddie Shahril Ismail
Associate Professor,
School of Mathematical Sciences,
Universiti Kebangsaan Malaysia,
43600 UKM Bangi, Selangor, Malaysia
esbi@ukm.my

Abstract- Recently, the development of cryptosystems based on multiple hard problems attracts attention from mathematicians and computer scientists as it is believed that such systems provide long-term security. In another side, the concept of threshold cryptography gives benefit in group-oriented community. For these reasons, in this paper we propose a new threshold cryptosystem based on factoring and elliptic curve discrete logarithm problems. We show that our scheme is heuristically secure against some cryptographic attack. From the efficiency analysis, it can be seen that our scheme requires reasonable time complexity in encryption and decryption phases.
Keywords: Threshold cryptosystem; factoring problem; elliptic curve discrete logarithm problem.

Introduction

Cryptosystem is a cryptographic scheme that allows sender to encrypt and send a secret and confidential message or document using public keys. In another hand, the receiver, who has access to the secret key, can decrypt and recover the encrypted message into its original form. The idea of the public key cryptosystem was presented by Diffie and Hellman [1]. Rivest et. al. [2] introduced the first public key cryptosystem based on factoring prime numbers problem. After that, many cryptosystems were designed based on various problems such as quadratic residue problem [3], discrete logarithm problem [4], and elliptic curve problem [5-6].

Later on, Desmedt [7] presented the concept of group-oriented cryptography, which is known as threshold cryptography. In his paper, Desmedt applied the concept of Shamir's secret sharing [8] in constructing of the threshold cryptographic scheme. However, the first threshold cryptosystem was only proposed by Desmedt and Frankel [9]. In such cryptosystem, they adapted the ElGamal cryptosystem to become a threshold cryptosystem based on discrete logarithm problem. After that, many threshold cryptosystem based on various problems were proposed [10-13]. In a threshold cryptosystem, the secret key is shared among the receivers. In order to decrypt and recover the encrypted message or document, the number of receivers must exceed the threshold value.

Currently, most cryptosystems are developed based on single hard problem such as factoring, quadratic residue, discrete logarithm, and elliptic curve discrete logarithm problems. It is understood that in the future, if the problems can be solved, then the system no longer be secure. For that reason, the development of cryptosystems based on multiple hard problems can be an alternative to overcome this problem. Besides that, such systems also can be applied in applications needing long-term security [14].

In this paper, we proposed a threshold cryptosystem based on factoring and elliptic curve discrete logarithm problems. Note that our scheme is modified version from ordinary cryptosystem developed by Ismail and Hijazi [15]. In their scheme, single receiver can decrypt and recover the encrypted message. We apply the concept of threshold cryptography in our scheme, where t out n of receivers is required to recover the encrypted message. The security of our scheme is based on the difficulty of solving factoring and elliptic curve discrete logarithm problems simultaneously.

Proposed Threshold Cryptosystem

In this section, we will introduce our new threshold cryptosystem based on factoring and elliptic curve discrete logarithm problems. Basically, a cryptosystem consists of three phases; initialization, encryption, and decryption.

A. Initialization

In this phase, a system authority is required to set the parameters and generate the public and secret keys. System authority also plays the role to construct the threshold polynomial function, as the secret key need to be shared in secret shadows among the receivers. The following parameters will be used throughout this scheme:

- The field order q, where q is the number of elements in F_q.
- Two coefficients $a_1, b_1 \in F_q$ that define the equation $y^2 \equiv x^3 + a_1 x + b_1 (\mathrm{mod}\, q)$ of elliptic curve E over F_q.
- The number of points in $E(F_q)$ denoted as $\#E(F_q)$.
- Two field elements x_1 and y_1 in F_q that define a finite point $G = (x_1, y_1)$.
- G has a large order N and is called as the base point. In order to choose G with order N, we fixed N and then

compute $NG_1, NG_2, \ldots$. We choose G that satisfied $NG = O$, where O is the point at infinity.

- $N = ab$, where a and b are two distinct safe primes.
- The Euler's phi function of N, denoted as $\phi(N)$.

After all parameters were set, system authority performs the following actions in generating the public and secret keys of the scheme:

i. Picks $e \in \mathbf{Z}_N^*$ such that $\gcd(e, \phi(N)) = 1$. Then, calculates d such that $ed \equiv 1 (\mathrm{mod}\ \phi(N))$.
ii. Calculates $V = a_0 G = (f_1, f_2)$.
iii. Constructs two secret threshold polynomial functions

$$P_1(x) = d + d_1 x + d_2 x^2 + \ldots + d_{t-1} x^{t-1} (\mathrm{mod}\ N)$$

$$P_2(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} (\mathrm{mod}\ N)$$

iv. Sets $(x_i, P_1(x_i), P_2(x_i))$ for each receiver, where x_i is the public identity, while $P_1(x_i)$ and $P_2(x_i)$ are the secret shadows for each receiver.
v. Makes e and V public.

B. Encryption

Suppose that a sender wants to encrypt and send a message M to the group of receivers. By using the public keys e and V, he performs the following actions:

i. Chooses one-time secret integer r, where $1 \le r \le N - 1$.
ii. Computes $K = rG$ and $T = rV = (r_1, r_2)$.
iii. Calculates $s = M - f_1 r_1 (\mathrm{mod}\ N)$ and $\alpha \equiv s^e (\mathrm{mod}\ N)$.
iv. Sends (α, K) to the receivers.

C. Decryption

In this phase, t out of n receivers are required to decrypt the encrypted message, while $t-1$ receivers will not gain any information about the message. After they receive (α, K) from the sender, each of them takes the following actions:

i. By using the secret shadows $P_1(x_i)$ and $P_2(x_i)$, calculates $\alpha_i \equiv \alpha^{P_1(x_i)} (\mathrm{mod}\ N)$ and $K_i = P_2(x_i) K$.
ii. Sends α_i and K_i to other receivers via a secure channel.
iii. Upon receiving α_i and K_i from other receivers, calculates $s \equiv \prod_{i=1}^{t} \alpha_i^{L_i} (\mathrm{mod}\ N)$ and $r_1 = \sum_{i=1}^{t} K_i L_i$, where $L_i = \prod_{j=1, j \ne i}^{t} \frac{-x_j}{x_i - x_j} (\mathrm{mod}\ N)$.
iv. Recovers the message by calculating $M = s + f_1 r_1 (\mathrm{mod}\ N)$.

The equations in decryption phase are correct for all α and K since:

$$\prod_{i=1}^{t} \alpha_i^{L_i} \equiv \prod_{i=1}^{t} \alpha^{P_1(x_i) L_i} \equiv \alpha^{\sum_{i=1}^{t} P_1(x_i) L_i} \equiv \alpha^d \equiv s^{ed} \equiv s (\mathrm{mod}\ N)$$

and

$$\sum_{i=1}^{t} K_i L_i = \sum_{i=1}^{t} P_2(x_i) K . L_i = K \sum_{i=1}^{t} P_2(x_i) L_i = a_0 K$$

$$= a_0 rG = rV = (r_1, r_2)$$

Analysis of Security

We will show that our scheme is heuristically secure against some cryptographic attack. In this analysis, we consider the following attacks:

A. Key-only attack

Adversary wishes to obtain all secret keys from the public keys and parameters of the scheme. In this attempt, he needs to solve $ed \equiv 1 (\mathrm{mod}\ \phi(N))$ and $V = a_0 G$. However, his attempts will not succeed since it is clearly infeasible to solve both equations due to the difficulty of solving factoring and elliptic curve discrete logarithm problems.

B. Factoring attack

Assume that the factoring problem is solvable. In this case, adversary could find the value of d from the equation $ed \equiv 1 (\mathrm{mod}\ \phi(N))$. Then, he can solve for s from $\alpha \equiv s^e (\mathrm{mod}\ N)$. However, he still cannot recover the message from the equation $M = s + f_1 r_1 (\mathrm{mod}\ N)$ since he does not know the value of r_1, which is only be discovered if the elliptic curve discrete logarithm problem can be solved.

C. Elliptic curve discrete logarithm attack

Suppose that adversary is able to solve the elliptic curve discrete logarithm problem. He could find a_0 from the equation $V = a_0 G$ and then solve for r_1 from the equation $a_0 K = (r_1, r_2)$. However, without knowing s that only can be obtained if the factoring problem is solvable, he still cannot recover the message.

Analysis of Efficiency

We analyse the efficiency of our scheme in terms of number of public and secret keys, computational complexity in encryption and decryption phases, and communication cost. The analysis of our scheme is given in Table 1. The following notations are used in analysing our scheme:

- PK and SK denote the number of public and secret keys respectively.
- T_{mul} is the computational complexity for executing the modular multiplication.
- T_{exp} is the computational complexity for executing the modular exponentiation.
- T_{inv} is the computational complexity for executing the modular inverse.
- $T_{ec\text{-}add}$ is the computational complexity for executing the addition of two elliptic curve points.
- $T_{ec\text{-}mul}$ is the computational complexity for executing the multiplication on elliptic curve.
- $|x|$ denotes the bit length of x.
- t is the number of receivers involved in decryption phase.

TABLE 1. Efficiency Analysis of the Proposed Scheme

Criteria		Analysis of Efficiency
Number of keys	SK	$2t$
	PK	2
Computational complexity	Encryption	$2\,T_{ec\text{-}mul} + T_{mul} + T_{exp}$
	Decryption	$(2t)T_{ec\text{-}mul} + (t-1)T_{ec\text{-}add} + (2t^3 - 2t - 1)T_{mul} + (2t)T_{exp} + (t^2 - t)T_{inv}$
Communication cost	Encryption	$2\|N\|$
	Decryption	$(4t)\|N\|$

Conclusion

In this paper, we proposed a new threshold cryptosystem based on factoring and elliptic curve discrete logarithm problems. We analysed our scheme by showing the security and efficiency of the scheme. In security analysis, it is shown that this scheme is heuristically secure against some cryptographic attack. It is also proved that our scheme will remain secure even one of the problems can be solved. In efficiency analysis, it is shown that our system uses minimum number of secret and public keys, requires reasonable time complexity in encryption and decryption phases, and also requires minimum communication cost.

Acknowledgement

The second author acknowledges the financial support received from the Universiti Kebangsaan Malaysia under research grant FRGS/2/2013/SG04/UKM/02/1.

References

[1] Diffie, W., and Hellman, M., E., "New directions in cryptography," IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp. 644-654, 1976.

[2] Rivest, R., Shamir, A., and Adleman, L., "A method for obtaining digital signature and public-key cryptosystem," Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.

[3] Rabin, M., O., "Digitalized signatures and public key cryptosystems as intractable as factorization," Technical Report MIT/LCS/TR-212, Massachusetts Institute of Technology, Cambridge, MA, 1979.

[4] ElGamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE* Transactions on Information Theory, Vol. IT-31, No. 4, pp. 469-472, 1985.

[5] Koblitz, N., "Elliptic curve cryptosystems," Mathematics of Computation, Vol. 48, No. 177, pp. 203-209, 1987.

[6] Miller, V., "Use of elliptic curves in cryptography," Advances in Cryptology – CRYPTO '85, Vol. 218, pp. 417-426, 1986.

[7] Desmedt, Y., "Society and group oriented cryptography: a new concept," Advances in Cryptology – CRYPTO '87, Vol. 293, pp. 120-127, 1988.

[8] Shamir, A., "How to share a secret" Communications of the ACM, Vol. 22, No. 11, pp. 612-613, 1979.

[9] Desmedt, Y., and Frankel, Y., "Threshold cryptosystems," Advances in Cryptology – CRYPTO '89, Vol. 435, pp. 307-315, 1989.

[10] Pedersen, T., P., "A threshold cryptosystem without a trusted party," Advances in Cryptology – EUROCRYPT '91, Vol. 547, pp. 522-526, 1991.

[11] Laih, C., S., and Harn, L., "Generalized threshold cryptosystem," Advances in Cryptology – ASIACRYPT '91, Vol. 739, pp. 159-166, 1993.

[12] Katz, J., and Yung, M., 2002, "Threshold cryptosystems based on factoring," Advances in Cryptology – ASIACRYPT 2002, Vol. 2501, pp. 192-205, 2002.

[13] Desmedt, Y., and Kurosawa, K., "A generalization and a variant of two threshold cryptosystems based on factoring," Information Security, Vol. 4779, pp. 351-361, 2007.

[14] Poulakis, D., "On the cryptographic long term security," Journal of Applied Mathematics & Bioinformatics, Vol. 3, No. 1, pp. 1-15, 2013.

[15] Ismail, E., S., and Hijazi, M., S., "Development of a new elliptic curve cryptosystem with factoring problem," American Journal of Applied Sciences, Vol. 9, No. 9, pp. 1443-1447, 2012.