American Journal of Applied Sciences 9 (9): 1443-1447, 2012
ISSN 1546-9239

Development of a New Elliptic Curve Cryptosystem with Factoring Problem

E.S. Ismail and M.S. Hijazi
School of Mathematical Sciences, Faculty of Science and Technology,
Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

Abstract: Problem statement: The security of elliptic curve cryptosystems are based on elliptic curve discrete logarithm problem (ECDLP). However, if an attacker finds a solution to ECDLP, the elliptic curve-based systems will no longer be secure. **Approach:** To improve this, we develop a new elliptic curve cryptosystem using one of the old/novel problem in computational number theory; factoring problem (FAC). Specifically, our encrypting and decrypting equations will heavily depends on two public keys and two secret keys respectively. **Results:** We show that, the newly designed cryptosystem is heuristically secure against various algebraic attacks. The complexity of the scheme shows that the time complexity for each encryption and decryption are given by $299T_{mul}$ and $270T_{mul}$. **Conclusion:** The new system provides greater security than that system based on a single hard problem. The attacker has not enough resources to solve the two hard problems simultaneously in a polynomial time.

Key words: Cryptosystem, elliptic curve, factoring problem, elliptic curve discrete logarithm problem

INTRODUCTION

Diffie and Hellman (1976) were the first to propose the idea of transmitting secret message between two communicating parties; a sender and a receiver in an insecure channel (with the presence of attackers). Their idea (is called cryptosystem) consists of these following properties:

- The sender first encrypts the message using receiver's public key and sends the encrypted message to the receiver
- The receiver who possesses the secret key can decrypt and read the original message
- The security of the system is depends on the underlying hard problems in computational number theory
- Knowing only the public key of receiver, the attacker is not able to read the message since he has no information about the corresponding secret key

Unfortunately, they did not develop any such system. The first realization was developed by Rivest *et al*. (1978) and is called RSA cryptosystem after their first names. The security of RSA is based on the hardness of solving factoring problem (FAC). Informally, if the attacker manages to solve FAC, the underlying system will no longer be secure. With the proper selection of parameters, no one is able to break the novel RSA system. Rabin (1979) designed a new cryptosystem whose security is depends heavily on residuosity problem (RES). His system relies on the difficulty of finding prime divisors of a given large composite integer as in RSA. However, no concrete relationship between the hardness of solving FAC and RES is found. Six years later, Elgamal (1985) proposed his new cryptosystem based on Discrete Logarithm Problem (DLP). Later, Koblitz (1987) and Miller (1986) independently proposed the use of elliptic curve in cryptosystems. Their security lies on the so-called Elliptic Curve Discrete Logarithm Problem (ECDLP). Their systems are more efficient than previous systems since the size of the main parameter is only 160-bits. Many such systems were then been developed (Menezes, 1993; Rabah, 2005). One common feature of these schemes is that the security of the systems is based on a single hard problem. If one day in a near future an attacker solves the hard problem, the underlying system will no longer be secure. Thus to overcome this disadvantage, many designers are proposing cryptosystems based on two hard problems (Baocang and Yupu, 2005; Elkamchouchi *et al*., 2004; Harn, 1994; Ismail and Hijazi, 2011). If the attacker find a solution to one of these hard problem the system stays secure as the another problem is still hard to solve. It is impossible for the attacker to solve the two problem simultaneosly. In this study, we develop a new cryptosystem based on two hard problems; ECDLP and FAC. A desirable system with two hard problems should come with the following criteria: (1) the system uses only one pair of public and private keys; (2) each

Corresponding Author: E.S. Ismail, School of Mathematical Sciences, Faculty of Science and Technology,
Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

user uses common arithmetic modulus; and (3) the system uses the most novel two hard mathematical problems for its security base. Our system enjoys the last two criteria.

MATERIALS AND METHODS

An elliptic curve in a general form is given by:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

where, a, b, c, d and e are real numbers. We define on this curve an elliptic curve addition operation with a point at infinity and we denote this point as ∞. Now, suppose that q is a 160-bits prime with characteristics neither two nor three. We thus obtain an elliptic group over the Galois Field $E(F_q)$ defined by:

$$y^2 = x^3 + ax + b \pmod q \text{ where } 0 \le x \le q$$

The coefficients a, b < q are non-negative integers and satisfy the condition $4a^3 + 27b^2 \neq 0 \pmod q$. This condition guarantees that the defined elliptic curve has no multiple roots of unity.

The laws for elliptic curve addition over the elliptic group $E(F_q)$ are given as follows:

- If three elliptic curve points are on a straight line and intersects an elliptic curve, then their sum equals the point at infinity ∞
- Suppose that Q = (r, s) and N = (t, u) are two elliptic curve points in $E(F_q)$. Then:

i. $Q + \infty = Q = \infty + Q$.
ii. If N = -Q = (r, -s), then $Q + N = \infty$.
iii. If $Q \neq N$, then $Q + N = (e, f)$ where $e = \mu^2 - r - t \pmod q$ and $f = \mu(r-e) - s \pmod q$ and the number μ is calculated by $\mu = (u-s)/(t-r)$ if $r \neq t$ and $\mu = (3r^2+a)/2s$ if $r=t, s \neq 0$.
iv. If n is a positive integer greater than 1, we can calculate nQ = Q + Q + Q + … (n times) in $E(F_q)$.

If Q is a point on the elliptic curve and m is the smallest positive integer satisfying $mQ = \infty$, then we say that Q has an order m and Q is called the base point of $E(F_q)$.

Washington (2003) for a solid material on elliptic curve and its application in cryptography. We now define the two hard problems that we apply in our new system.

Definition 1: (ECDLP problem) Let Q and N be two elliptic curve points in $E(F_q)$ where q is a 160-bits prime. Then find a positive integer k satisfying kQ = N.

Definition 2: (FAC problem) Let n be a large composite integer with n = rs where r and s are two large strong primes of 512-bits. Then find the primes r or s.

RESULTS

We propose a new cryptosystem based on FAC and ECDLP problems. The scheme consists of three phases:

- Initialization
- Encryption
- Decryption

with two communicating parties; a sender and a receiver. In Initialization phase, the reciever first selects and computes all required parameters and modulus for the system. Then two pairs of public and private keys for the sender are calculated. The computed public keys will then be published in an open public key directory but the private keys are kept secret to the receiver. In Encryption phase, an encrypted original message is computed by the sender using the receiver's public key and sender's one-time secret number. The resulted encrypted message is then delivered to the receiver. In Decryption phase, the reciever decrypts the encrypted message to recover the original message using his own private keys. No one can learn the actual message without these private keys. Now we give the description for each phase.

Initialization: The receiver obtains his or her public and private keys as below:

- Select a 160-bits prime q and this prime determines the order of field F_q
- Choose two numbers a and b in F_q. These coefficients define the elliptic curve $y^2 = x^3 + ax + b \pmod q$ over F_q. Let $E(F_q)$ represents a group of all points on this curve and $\#E(F_q)$ represents the group order
- Pick a base elliptic curve point G with a large prime order m and this gives us $mG = \infty$
- Choose two strong and safe primes r and s (Gordon, 1984) and compute the modulus, n = rs. This modulus determines the multiplicative group $Z_n^* = \{z | \gcd(z,n) = 1\}$
- Calculate the phi-Euler function $\phi(n) = (r-1)(s-1)$.
- Select two integers e < n with $\gcd(e, \phi(n)) = 1$ and f < m
- Compute $d = e^{-1} \bmod \phi(n)$ and $Z = fG = (f_1, f_1)$

The public keys of the system are formed by (Z,n,e) and can be publicly accessed in the open

directory while the private keys of the system are given by (r,s,d,f) and kept secret by the receiver. One has to confirm that the group order, $\#E(F_q)$ must be divisible by a sufficiently large prime number to avoid the Pohlig-Hellman attack and Pollard's rho attack (Pohlig and Hellman, 1978). For maximum resistance to these attacks is by confirming that $\#E(F_q)$ is prime or almost prime.

Encryption: To encrypt any message, m, the sender does the following:

- Choose randomly the secret integer $p < m$
- Calculate $T = pZ = (r_1,r_2)$ and $K = pG$
- Compute $s_1 = m\text{-}f_1r_1 \pmod n$
- Calculate $c = (s_1)^e \bmod n$
- Send (c, K) to the receiver

Decryption: To decrypt the received ciphertext (c,K), the receiver needs to do the following:

- Compute $R = fK$
- Calculate $L = (c)^d \bmod n$
- Recover $m = s_1 + f_1r_1 \pmod n$

The abovementioned three phases or algorithms complete the newly developed cryptosystem based on two hard problems. We now discuss our system according to the following criteria:

- Exactness of the new cryptosystem
- Security analysis
- Efficiency performance

To validate the newly designed cryptosystem, we prove that the decrypting equation in Decryption is always true for any ciphertext (c,K) developed in Encryption.

Exactness: We validate our new scheme by proving the following theorem.

Theorem: If the first two algorithms; Initialization and Encryption run smoothly, then the decryption process of the encrypted message in Decryption is correct.

Proof: The decrypting equation is true for all encrypted message (c,K) using the following steps:

- Calculate $R = fK = f(pG) = p(fG) = pZ = (r_1,r_2)$
- Compute $L = (c)^d = (s_1)^{ed} = s_1 \bmod n$

Knowing r_1 and s_1 with the public key Z, the original message can be recovered as below:

$s_1 + f_1r_1 = m \bmod n$.

Security analysis: We analyse our system by applying a technique from heuristic security. We do this by considering possible cryptographic attacks by an attacker for the system.

First, we define each attack and give the corresponding analysis of why this attack would fail.

Attack 1: The attacker tries to obtain the private keys of the system and to manipulate the system parameters.

In this attack, the attacker needs to solve:

$$ed = 1 \bmod \phi(n) \text{ and}$$
$$Z = fG$$

For d and f respectively. However these are hard to solve due to the difficulty of solving factoring and elliptic curve discrete logarithm problems. Lenstra *et al*. (1993) developed the method to factorize the modulus n = pq but it is siza-dependent. Díaz and Masque (2005) said in their paper, to increase the security of the scheme and to avoid attacks using special-purpose factorization algorithms, one must select strong primes in the Initialization phase.

Attack 2: Suppose that the attacker manages to solve factoring problem. Thus he knows the secret d and (c,K). He then computes $s_1 = c^e \bmod n$ and learns the original message, m, if he knows r_1 via $m = s_1 + f_1r_1 \pmod n$.

Unfortunately the integer r_1 is calculated via $R = fK$ where f is a secret number from $Z = fG$. Finding f is hard due to nonexistence of polynomial algorithm to solve elliptic curve discrete logarithm problem for public Z and G.

Attack 3: Suppose that the attacker can solve elliptic curve discrete logarithm problem. He thus manages to get the secret value, f. He also knows (c,K) and obtains r_1 via $R = fK = (r_1,r_2)$. He can obtain the original message, m, if he knows s_1 via:

$$m = s_1 + f_1r_1 \pmod n$$

Unfortunately the integer s_1 is computed via $L = c^d = s_1 \bmod n$. Finding s_1 is hard due to nonexistence of polynomial algorithm to solve $ed = 1 \bmod \phi(n)$ for d due to the hardness of solving factoring problem.

Attack 4: Assume that the attacker collects two ciphertext (c_1,K_1) and (c_2,K_2). These ciphertext corresponds to the following equations:

$$s_{11} + f_{11}r_{11} = m_{11} \bmod n, \text{ and}$$
$$s_{12} + f_{11}r_{12} = m_{12} \bmod n$$

where, f_{11} is a public key. These two equations have six unknowns and the attacker fails to obtains m_{11} and m_{12}. However let us assume that Attack 2 is solvable then the attacker knows s_{11} and s_{12}. This make the above system of equations now has four unkowns. Still, it will give us infinitely many solutions for m_{11} and m_{12}. The case where we assume Attack 3 is solvable goes similarly.

Efficiency performance: We measure and describe the efficiency performance of our system in terms of number of keys used, computational complexity overhead and the communication costs for each algorithm; encryption and decryption. We use the following notations to analyse the performance of the system:

- SK and PK denote the number of private and public keys respectively
- T_{exp} is the time complexity taken for a modular exponentiation
- T_{mul} is the time complexity taken for a modular multiplication
- $T_{ec\text{-}mul}$ is the time complexity for executing the multiplication on elliptic curve points
- $T_{ec\text{-}add}$ is the time complexity for executing the addition of two elliptic curve points
- T_{hash} is the time complexity taken for performing a hash function
- |x| denotes the bit length of x

We assume that the time complexity for modular addition or subtraction is negligible. We also assume that the probability of the bit being chosen as 0 or 1 is 0.5. Note that, the time complexity for Encryption is given by $2T_{ec\text{-}mul} + T_{mul} + T_{exp}$ and the time complexity for Decryption is $T_{ec\text{-}mul} + T_{exp} + T_{mul}$. The communication costs of the system is only 4|n|. We use the conversions $T_{exp} = 240T_{mul}$, $T_{ec\text{-}mul} = 29T_{mul}$ and $T_{ec\text{-}add} = 0.12T_{mul}$ given by Koblitz *et al.* (2000) to measure the performace in terms of T_{mul} time complexity. The summary of efficiency performance is given in Table 1.

Table 1: The performance of our new public key encryption scheme

Our new public key encryption scheme		
The number of keys	SK	2
PK	2	
Computational complexity	Encryption	$299T_{mul} + T_{hash}$
Decryption	$270T_{mul}$	
Communication cost	Encryption	2|n|
Decryption	2|n|	

DISCUSSION

So far, the security of most of the developed cryptosystems was based on a single hard problem like discrete logarithm, residuosity, factoring, and elliptic curve discrete logarithm and knapsack problems. These existing systems are no longer secure if one finds a solution to these hard problems and thus, designing a cryptosystem based on two hard problems is a good alternative. The only way the attacker can break the system is by solving the two problems simultaneously and this is very unlikely to happen and with negligible probability. If the attacker manages to find a solution to one of the hard problem, the system remains secure as the other problem is still hard to solve. The new system is shown secure against the common cryptographic attacks.

CONCLUSION

We designed a new cryptosystem based on multiple hard problems; elliptic curve discrete logarithm and factoring. The developed system requires only $299T_{mul}$ and $270T_{mul}$ for each Encryption and Decryption. Some possible algebraic attacks have also been analysed and scheme is heuristically secure from those attacks.

ACKNOWLEDGEMENT

We acknowledge the financial support received from University Kebangsaan Malaysia under the Research University Grant UKM-DLP-2011-028.

REFERENCES

Baocang, W. and H. Yupu, 2005. Public key cryptosystem based on two cryptographic assumptions. IEE Proc. Commun., 152: 861-865. DOI: 10.1049/ip-com:20045278

Díaz, R.D. and J.M. Masque, 2005. Optimal strong primes. Inform. Proc. Lett., 93: 47-52. DOI: 10.1016/j.ipl.2004.09.015

Diffie, W. and M.E. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654.

Elgamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory, 31: 469-472. DOI: 10.1109/TIT.1985.1057074

Elkamchouchi, H.M., M.E. Nasr and R. Esmail, 2004. New public key techniques based on double discrete logarithm problem. Proceeding of the 21st National Radio Science Conference, Mar. 16-18, IEEE Xplore Press, pp: 1-9. DOI: 10.1109/NRSC.2004.1321832

Gordon, J., 1984. Strong RSA keys. Electron. Lett., 20: 514-516. DOI: 10.1049/el:19840357

Harn, L., 1994. Public-key cryptosystem design based on factoring and discrete logarithms. IEE Proc. Comput. Digit. Tech., 141: 193-195. DOI: 10.1049/ip-cdt:19941040

Ismail, E.S. and M.S. Hijazi, 2011. New cryptosystem using multiple cryptographic assumptions. J. Comput. Sci., 7: 1765-1769. DOI: 10.3844/jcssp.2011.1765.1769

Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209.

Koblitz, N., A. Menezes and S. Vanstone, 2000. The state of elliptic curve cryptography. Design, Codes Cryptography, 19: 173-193. DOI: 10.1023/A:1008354106356

Lenstra, A.K., H.W. Lenstra, M.S. Manesse and J.M. Pollard, 1993. The number field sieve. Dev. Number Field Sieve, 1554: 11-42. DOI: 10.1007/BFb0091537

Menezes, A.J., 1993. Elliptic Curve Public Key Cryptosystems. 1st Edn., Springer, Boston, ISBN: 0792393686, pp: 144.

Miller, V.S., 1986. Use of elliptic curves in cryptography. Adv. Cryptol., 218: 417-426. DOI: 10.1007/3-540-39799-X_31

Pohlig, S. and M. Hellman, 1978. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (Corresp.). IEEE Trans. Inform. Theory, 24: 106-110. DOI: 10.1109/TIT.1978.1055817

Rabah, K., 2005. Elliptic curve elgamal encryption and signature schemes. Inform. Technol. J., 13: 299-306.

Rabin, M.O., 1979. Digitalized signatures and public-key functions as intractable as factorization. Technical Report, Massachusetts Institute of Technology Cambridge, MA.

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Mag. Commun. ACM, 21: 120-126. DOI: 10.1145/359340.359342

Washington, L.C., 2003. Elliptic Curves: Number Theory and Cryptography. 1st Edn., Chapman and Hall/CRC, Boca Raton, ISBN-10: 1584883650, pp: 440.