A Novel and Efficient Cryptosystem for Long Message Encryption

Debasish Jena
Centre for IT Education Bhubaneswar
Orissa, 751 010, India
debasishjena@ieee.org

Saroj Kumar Panigrahy and Sanjay Kumar Jena
National Institute of Technology Rourkela
Orissa, 769 008, India
skp.nitrkl@gmail.com, skjena@nitrkl.ac.in

***Abstract*—Due to more overhead of asymmetric cryptosystems, traditionally, the symmetric cryptosystem is used to encrypt long messages. In case of symmetric cryptosystems, it creates the problem of key management. So to encrypt long messages, we usually, take the help of both symmetric and asymmetric cryptosystems. In this paper, we proposed an asymmetric cryptosystem for encrypting long messages, which is not only efficient but also secure. In consideration of the aspect of efficiency and computation, our proposed scheme uses elliptic curve cryptosystem.**

***Index Terms*—ElGamal, Elliptic Curve, Public Key, Diffie-Hellman.**

I. Introduction

Since the invention of public-key cryptography in 1976 by Whitfield Diffie and Martin Hellman [1], numerous public-key cryptographic systems have been proposed. All of these systems based their security on the difficulty of solving a mathematical problem. Over the years, many of the proposed public-key cryptographic systems have been broken and many others have been demonstrated to be impractical. Today, only three types of systems are considered both secure and efficient. Examples of such systems and the mathematical problems on which their security is based, are [2]:

- **Integer factorization problem (IFP):** RSA and Rabin-Williams.
- **Discrete logarithm problem (DLP):** the U.S. governments Digital Signature Algorithm (DSA), the Diffie-Hellman key agreement scheme, the ElGamal encryption and signature schemes, the Schnorr signature scheme, and the Nyberg-Rueppel signature scheme.
- **Elliptic curve discrete logarithm problem (ECDLP):** the elliptic curve analog of the DSA (ECDSA), and the elliptic curve analogs of the Diffie-Hellman key agreement scheme, the ElGamal encryption and signature schemes, the Schnorr signature scheme, and the Nyberg-Rueppel signature scheme.

Given the current state of our knowledge about algorithms for the IFP, DLP and ECDLP problems, we can conclude that the ECDLP is significantly more difficult than either the IFP or the DLP. Figure 1 compares the time required to solve an instance of the ECDLP (and hence break Elliptic Curve Cryptography (ECC)) with the time required to solve instances of the IFP or DLP (and hence break RSA or DSA, respectively) for various modulus sizes and using the best general algorithms known. The running times are computed in MIPS years. As a benchmark, it is generally accepted that 1012 MIPS years represents reasonable security at this time. In Figure 1, the times to break RSA and DSA are grouped together because the best algorithms known for IFP and DLP have approximately the same asymptotic running times. From Figure 1, we see that to achieve reasonable security, RSA and DSA should employ 1024-bit moduli, while a 160-bit modulus should be sufficient for ECC. Moreover, the security gap between the systems increases dramatically as the moduli sizes increases. For example, 300-bit ECC is dramatically more secure than 2048-bit RSA or DSA.

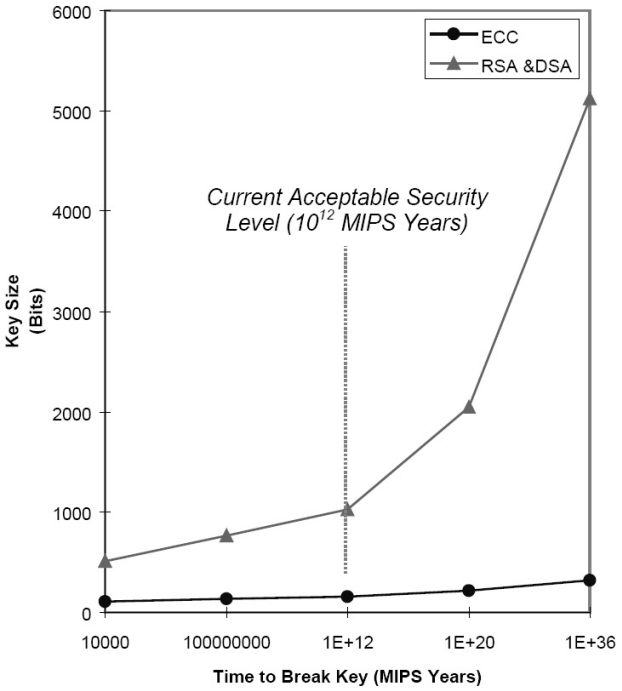

Fig. 1. Comparison of Security Levels

Asymmetric cryptosystems such as RSA [3], Diffie-Hellman [1] and Elliptic Curve [4] have been widely used in many applications. However, because asymmetric encryptions are more expensive than symmetric encryptions such as DES [5],

[6] and AES [7] in terms of computational cost, generally they are not directly used to encrypt long messages. Traditionally, if there is a need to encrypt a long message using an asymmetric cryptosystem, then a symmetric cryptosystem is used in addition. The message itself is encrypted using the symmetric cryptosystem and the symmetric key is encrypted using the asymmetric cryptosystem. To eliminate this requirement for an additional cryptosystem, we propose a novel asymmetric cryptosystem based on ECDLP. Elliptic curve cryptosystem gives more security with less bit size key and computationally faster than the other asymmetric cryptosystems. Because of these reasons, we proposed a novel and efficient cryptosystem for encrypting long message based on ECDLP.

The organization of this paper is as follows. In the Section II, the basic concept of elliptic curve (EC) is explained. In Section III, discussion on Elliptic Curve Cryptosystem based on ElGamal scheme has been illustrated. The proposed scheme and its security analysis are discussed in section IV. Finally, Section V presents the concluding remarks.

II. Elliptic Curve Over Finite Field

The use of ECC was initially suggested by Neal Koblitz [8] and Victor S. Miller [9] and there after many researchers have suggested different application of Elliptic Curve Cryptosystems. Elliptic curve cryptosystems over finite fields have some definite advantages. One advantage is the "much smaller key size" as compared to other cryptosystems like RSA or Diffie-Hellman, since: (a) only exponential-time attack is known so far if the curve is carefully chosen [4], and (b) elliptic curve discrete logarithms might be still intractable even if factoring and multiplicative group discrete logarithms are broken. Further ECC is also more computationally efficient than the first-generation public key systems such as RSA or Diffie-Hellman [10].

A. Elliptic Curve Groups Over F_q

A non-super singular Elliptic curve E over F_q can be written as:

$$E : y^2 \bmod q = (x^3 + ax + b) \bmod q \tag{1}$$

where $(4a^3 + 27b) \bmod q \neq 0$. The points $P = (x, y)$ where $x, y \in F_q$. $P(x, y)$ that satisfy the Eqn. 1 together with a "point of infinity" denoted by O form an abelian group $(E, +, O)$ whose identity element is O.

Adding Distinct Points P and Q: The negative of the point $P = (x_1, y_1)$ is the point $-P = (x_1, -y_1)$. If $P(x_p, y_p)$ and $Q(x_q, y_q)$ are two distinct points such that P is not $-Q$, then

$$P + Q = R \tag{2}$$

where $R = (x_r, y_r)$. Therefore,

$$\begin{aligned} s &= (y_q - y_p)/(x_q - x_p) \bmod q \\ x_r &= (s^2 - x_p - x_q) \bmod q \\ y_r &= (-y_p + s(x_p - x_r)) \bmod q \end{aligned}$$

where s is the slope of the line passing through P and Q.

Doubling the Point P: Provided that y_p is not 0,

$$2P = R \tag{3}$$

where $R = (x_r, y_r)$. Therefore,

$$\begin{aligned} s &= ((3x_p^2 + a)/(2y_p)) \bmod q \\ x_r &= (s^2 - 2x_p) \bmod q \\ y_r &= (-y_p + s(x_p - x_r)) \bmod q \end{aligned}$$

The elliptic curve discrete logarithm problem is defined as follows [11].

Definition: Let E be an elliptic curve over a finite field F_q and let $P \in E(F_q)$ be a point of order n. Given $Q \in E(F_q)$, the elliptic curve discrete logarithm problem is to find the integer $d \in [0, n-1]$, such that $Q = dP$.

III. Elliptic Curve Cryptosystem based on ElGamal

In this section, we discuss ECC based on Elgamal. Suppose Alice wishes to send a message M to Bob. First, she imbeds the value m onto the elliptic curve E, i.e., she represents the plaintext M as a point $P_m \in E$. Now she must encrypt P_m. Let d_B denote Bob's secret key. Alice first chooses a random integer k and sends Bob a pair of points (C_1, C_2) on E where

$$\begin{aligned} C_1 &= kG \\ C_2 &= P_m + kd_BG \end{aligned}$$

To decrypt the cipher text, Bob computes

$$\begin{aligned} C_2 - d_BC_1 &= P_m + kd_BG - d_BkG \\ &= P_m \end{aligned}$$

IV. Proposed Scheme

In this section, we propose an efficient scheme for enciphering a large plaintext using ECDLP. Our proposed scheme is based on both the Diffie-Hellman distribution scheme and ElGamal cryptosystem. The Diffie-Hellman key distribution scheme is used to generate the key pair of public and secret keys for all users u_i for $i = 1, 2, ..., n$. Each user u_i randomly selects secret key d_i and computes the corresponding public key $Q_i = d_iP$.

In our proposed scheme, let Bob and Alice want to deliver a confidential large message M as per the following algorithm:

A. The Algorithm

Initially, Bob breaks the plaintext $M(M_x, M_y)$ into t pieces $M_1, M_2, ..., M_t$ of length being 512 bits and convert them into points in EC.

Key Generation (Alice):

1) Select a random integer d from $[1, n-1]$.
2) Compute $Q = dP$.
3) A's public key is Q and private key is d.

Encryption (Bob):

1) Select two random numbers $(r_1, r_2) \in [1, n-1]$.
2) Compute B_1 and B_2 as follows:

$$B_1 = r_1 P \tag{4a}$$

$$B_2 = r_2 P \tag{4b}$$

such that
$S_{AB1} = r_1 Q = r_1 dP = (x_{s1}, y_{s1})$
$S_{AB2} = r_2 Q = r_2 dP = (x_{s2}, y_{s2})$

3) if $x_{s1} = 0 \bmod P$ and $x_{s2} = 0 \bmod P$ then go to step 2.
4) Compute C_{xj} and $C_{yj}, j = 1, 2, ..., t$ as follows:

$$C_{xj} = M_{xj} * (x_{s1} \oplus x_{s2}^2) \bmod n \tag{5a}$$

$$C_{yj} = M_{yj} * (y_{s1} \oplus y_{s2}^2) \bmod n \tag{5b}$$

5) Send $(B_1, B_2, C_{xj}, C_{yj}), j = 1, 2, ..., t$ to Alice.

Decryption (Alice):

1) Alice receives $(B_1, B_2, C_{xj}, C_{yj}), j = 1, 2, ..., t$ and does the following to get $M = (M_x, M_y)$
2) Compute S_{AB1} and S_{AB1} as follows:
$S_{AB1} = dB_1 = dr_1 P = (x_{s1}, y_{s1})$
$S_{AB2} = dB_2 = dr_2 P = (x_{s2}, y_{s2})$
3) Compute M_{xj} and M_{yj} as follows:
$M_{xj} = C_{xj} * (x_{s1} \oplus x_{s2}^2)^{-1}$
$M_{yj} = C_{yj} * (y_{s1} \oplus y_{s2}^2)^{-1}$
4) Find Message $M_j = (M_{xj}, M_{yj})$.

In our proposed algorithm sender required to only select two random numbers r_1 and r_2. The Table I describes the comparison between the proposed scheme and ElGamal like EC cryptosystems.

TABLE I
COMPARISON BETWEEN THE PROPOSED SCHEME AND ELGAMAL LIKE EC CRYPTOSYSTEMS

Proposed Scheme	ElGamal like EC Cryptosystems
•2 times scalar point multiplication	•$2n$ times scalar point multiplication
•$2n$ times exclusive-OR operation	
•$2n$ times multiplication operation	•$2n$ times multiplication operation

Since the computational complexity depends on elliptic scalar point multiplication, the scheme proposed by us is computationally faster as compared to ElGamal based EC cryptosystem when used to encrypt large messages.

B. Security Analysis

Our proposed scheme is based on both the Diffie-Hellman distribution scheme and ElGamal cryptosystem. Hence, it is computationally hard to find the secrete key d from Q and P. It is also very difficult to compute r_1 and r_2 from the equations (4a) and (4b) as both are based on ECDLP.

If an intruder tries to do the crypto analysis using chosen-plaintext attack, for him/her it is difficult to find x_{s1} and x_{s2} from the equations (5a) and (5b). The proposed scheme is based on the difficulty to find the composite exclusive-OR operation. Thus our proposed scheme is secure against the chosen-plain text attack.

V. CONCLUSION

In this paper, we have shown that our scheme is computationally faster than the conventional ElGamal scheme. Thus the scheme can be used to encrypt the long message as compared to conventional encryption systems. We have also used the Elliptic Curve Cryptosystem which requires less computational power, memory and communication bandwidth giving it clear edge over the traditional crypto-algorithm. We have also shown that our scheme is secure against the chosen-plain text attack.

ACKNOWLEDGMENT

This research is supported by Department of Communication and Information Technology, Government of India, under Information Security Education and Awareness Project and being carried out at department of Computer Science and Engineering, National Institute of Technology Rourkela, Orissa, India.

REFERENCES

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, Nov 1976.
[2] C. T. E. C. Cryptosystem, "Remarks on the security of the elliptic curve cryptosystem," A Certicom White Paper, Sep 1997, updated: July 2000.
[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb 1978.
[4] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.
[5] FIPS, "Data encryption standard," Federal Information Processing Standards, 1977, national Bureau of Standard.
[6] M. Smid and D. Branstad, "The data encryption standard: Past and future," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 550–559, May 1988.
[7] FIPS, "Advanced encryption standard," Federal Information Processing Standards, Nov 2001, publication 197.
[8] N. Koblitz, *CM-Curves with Good Cryptographic Properties*, ser. Lectures notes on Computer Sciences. London, UK: Springer-Verlag, 1991, vol. 576, ch. Advances in Cryptology-Proceedings of Crypto91, pp. 279–287.
[9] V. S. Miller, *Uses of Elliptic Curve in Cryptography*, ser. Lectures notes on Computer Sciences. New York, USA: Springer-Verlag, 1986, vol. 218, ch. Advances in Cryptography- Proceedings of Crypto85, pp. 417–426.
[10] P. C. v. O. Alfred J. Menezes and S. A. Vanstone, *Handbook of Applied Cryptography*, 1st ed. CRC Press, 1996.
[11] D. R. Stinson, *Cryptography: Theory and Practice*, 2nd ed. CRC Press, 2002.