ENHANCED MENEZES-VANESTONE ELLIPTIC CURVES CRYPTOSYSTEM

Ahmed Tariq Sadiq* and Nasreen J. Kadhim**

***Department of. Computer Sciences, University of Technology, Baghdad, Iraq.**
****Department of Computer Science, College of Sciences, Baghdad University, Baghdad, Iraq.**

Abstract

The group of the elliptic curve points forms an Abelian group, which is a suitable choice for constructing a good problem similar to Discrete Logarithm Problem. This paper introduces a brief overview of the Menezes-Vanestone Elliptic Curves Cryptosystem (MVECC), and attempts to improve it by suggesting a new variation on MVECC to make encryption more efficient than the original elliptic curves cryptosystems.

Introduction

With the invention of public-key cryptography in 1976 by Whitfield Diffie and Martin Hellman, numerous public-key cryptographic systems have proposed. All of these systems rely on the difficulty of a mathematical problem for their security.

Elliptic curves are mathematical constructs that have studied by mathematicians since the seventeenth century[6]. Elliptic curves are not ellipse. They so named because they described by cubic equation, similar to these, that, used for calculating the circumference of an ellipse. So the word elliptic actually came from theory of the elliptic integrals.Unlike earlier cryptosystem, an elliptic curve works with a finite Abelian group formed by the points on an elliptic curve defined over a finite field [4,7]. Eilliptic Curve CryptoSystem (ECCS) includes key distribution, encryption/decryption schemes, and digital signature algorithm (DSA). The key distribution algorithm used to share a secret key, the encryption/ decryption algorithm enables confidential communication, and the DSA used to authenticate the signer and validate the integrity of the message.

In 1985, Lenstra succeeded in using the elliptic curves for integer factorization, this result suggests the possibility of applying elliptic curve to public-key cryptosystem [4,5, and 7].

Miller and Koblitz were the first to propose cryptosystem that employs elliptic curves independently [4]. The point addition operation in ECC is the counterpart of modular multiplication in RSA and multiple addition of point (scalar multiplication) is the counterpart of the modular exponentiation [5]. To form cryptographic system using elliptic curves, one needs to find a “hard problem” corresponding to the complexity of factoring the product of two primes or taking the discrete logarithm.

This paper organized as follows:

Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC)

This cryptosystem has no analogue for Discrete Logarithm Problem (DLP). Once one has a curve and a point on it, one is sure to succeed in embedding data into the system. That is not true for the elliptic curve analogue of DLP, it is a variant of the ElGamal analogue.

In this system the finite field F_q, the elliptic curve E, and the “base point” $B \in E$ (preferably, but not necessarily a generator of the curve) are public information. Bob randomly chooses a secret integer d ($1 < d < N$, where N is the number of points of E) and publishes the point dB. If Alice wants to send the message M (as any two number) to Bob, she will choose a secret random integer e ($1<e<N$) and send the pair $[(c_1,c_2),eB]$, where

$(k_1, k_2) = edB$
$(m_1, m_2) = M$ and
$c_1 = m_1 * k_1 \mod q$
$c_2 = m_2 * k_2 \mod q$

Bob will then multiply the second point in the pair by d to find d(eB) ($(k_1,k_2)=deB$) and compute the inverse of each number in this point (i.e. $k_1 * k_1^{-1}=1 \bmod q$, and $k_2 * k_2^{-1}=1 \bmod q$), and find the original message $M=(m_1, m_2)$ as follows

$m_1 = c_1 * k_1^{-1} \quad \bmod q$

$m_2 = c_2 * k_2^{-1} \quad \bmod q$

In the meantime, Charlie has only seen eB and dB, without solving the ECDLP, there is no way for him to find M [10].

The difference between the analogue of ElGamal and MVECC is that Alice will “mask” her plaitext instead of the embedding it. Therefore, the advantage in the MVECC is the message may be any random pair of number.

Example 1:- Let elliptic curve E defined over F_p (where p=4129) with parameters a=160 and b=1, where $4*a^3 + 27b^2=155 \bmod 4129$ is:

$E(F_{4129})$: $y^2= x^3+160 x+1$,

where $4*a^3 +27b^2 \neq 0 \bmod 4129$

Let B= (19, 2683) as a base point

Suppose the private key of Bob is d=621 then the public key of Bob is

Q=dB=621(19, 2683)= (2474, 921), and suppose Alice selects a random number which is e=1724.

For Aliceto send a message M=(1357,2468) to Bob, she does following

Compute eQ=1724(2474, 921)=(4042, 542)

Compute eB=1724(19, 2683)=(392, 664)

Compute C:

$C = (c_1, c_2)$

$(k_1, k_2) = eQ =(4042, 542)$

$(m_1, m_2) = M =(1357,2468)$

$c_1 = m_1 * k_1 \quad \bmod p$

$c_1 = 1357 * 4042 \quad \bmod 4129 = 1682$

$c_2 = m_2 * k_2 \quad \bmod p$

$c_2 = 2468 * 542 \quad \bmod 4129 = 3989$

Then Alice sends

C_m ={C,eB = (1682,3989), (392,664)} to Bob.

To decrypt the ciphertext, Bob does following:

Compute d(eB)=621(392,64)=(4042,542)=(k_1,k_2).

Compute $(k_1^{-1} \quad \bmod p, k_2^{-1} \bmod p)$:

$k_1^{-1} =4042^{-1} \bmod 4129=1756$

$k_2^{-1} =542^{-1} \bmod 4129=1516$

Compute M: $m_1= c_1 * k_1^{-1} \quad \bmod p$

$m_1= 1682* 1756 \quad \bmod 4129 = 1357$

$m_2= c_2 * k_2^{-1} \quad \bmod p$

$m_2= 3989 * 1516 \quad \bmod 4129 = 2468$

The Proposed Enhanced Method of MVECC

In the elliptic curve encryption/decryption schemes, the plaintext becomes twice as long as the cipher text. This characteristic may exploited to make the system more efficient in security or more efficient in performance.

We propose several variants of MVECC these represent the plaintext message as any two random numbers as follows.

Suppose Alice wants to send a message $M=(m_1, m_2)$ to Bob. Let d denote Bob’s secret key and Q = dB denote Bob’s public key. Alice chooses a random integer e and sends C_m,

$C_m = \{C, eB\}$

where

$C = (c_1, c_2)$

$(k_1, k_2) = eQ$

$c_1= m_1 k_2 - m_2 \quad \bmod p$

$c_2= m_1 k_1 + m_2 \quad \bmod p$

To decrypt the ciphertext Bob computes

$(k_1, k_2) = d(eB)$

$m_1= (c_1 + c_2) * (k_1 + k_2)^{-1} \quad \bmod p$

$m_2= (c_2 k_2 -c_1 k_1) * (k_1 + k_2)^{-1} \quad \bmod p$

To prove this:

We have

$m_1= (c_1 + c_2) (k_1 + k_2)^{-1} \bmod p$

$= [(m_1 k_2- m_2)+(m_1k_1+ m_2)](k_1+k_2)^{-1} \quad \bmod p$

$= (m_1 k_2-m_2+ m_1 k_1+ m_2) (k_1+k_2)^{-1} \quad \bmod p$

$= m_1(k_1 + k_2) (k_1+k_2)^{-1} \quad \bmod p$

$= m_1 \quad \bmod p$

We have

$m_2= (c_2 k_2 - c_1 k_1) (k_1+ k_2)^{-1} \quad \bmod p$

$=[(m_1k_1+m_2)k_2-(m_1 k_2-m_2)k_1](k_1+k_2)^{-1} \bmod p$

$=(m_1k_1k_2+m_2k-m_1k_1k_2+m_2 k_1)(k_1+k_2)^{-1} \bmod p$

$= (2 m_2 k_2) (2k_2)^{-1} \quad \bmod p$

$= m_2 (2k_2) (2k_2)^{-1} \quad \bmod p$

$= m_2 \quad \bmod p$

Example 2:- Let elliptic curve E be defined over F_p (where p=4129) with parameters a=160 and b=1, where $4*a^3 +27b^2=155 \bmod 4129$ is:

$E(F_{4129})$: $y^2 = x^3 + 160 x + 1$,

where $4*a^3 + 27b^2 \neq 0 \bmod 4129$.

Let B= (19, 2683) as a base point

Suppose the private key of Bob is d=621 then the public key of Bob are

Q=dB=621(19, 2683) = (2474, 921), and suppose Alice selects a random number which is e =1724.

To send Alice a message M=(1357,2468) to Bob, she does following :

Compute eQ=1724(2474, 921) = (4042, 542)

Compute eB=1724(19, 2683) = (392, 664)

Compute C:

$C = (c_1, c_2)$

$(k_1, k_2) = eQ=(4042, 542)$

$(m_1, m_2) = M =(1357,2468)$

$c_1= m_1 *k_2 - m_2 \bmod p$

$c_1=1357*542 -2468 \bmod 4129 = 2193$

$c_2= m_1 *k_1 + m_2 \bmod p$

$c_2 = 1357*4042 +2468 \bmod 4129 = 21$

Then Alice sends

$C_m =\{C,eB\}=\{(2193, 21), (392, 664)\}$ to Bob.

To decrypt the ciphertext, Bob does following:

Compute

d(eB)=621(392, 664)=(4042, 542) = (k_1, k_2).

Compute $(k_1 + k_2)^{-1}$:

$k_1 + k_2 =4042 +542 \bmod 4129=455.$

$(k_1 + k_2)^{-1} = 455^{-1} \bmod 4129=2550.$

Compute M :

$m_1= (c_1 + c_2) * (k_1 + k_2)^{-1} \bmod p.$

$m_1= (2193+ 21)* 2550 \bmod 4129$

$= 2214 * 2550 \bmod 4129 =1357$

$m_2= (c_2 k_2-c_1 k_1)*(k_1+ k_2)^{-1} \bmod p$

$m_2=(21*542–219*4042)*2550 \bmod 4129 =2468$

Computational Complexity

In this section, the computational complexity of the encryption and decryption functions for the MVECC and the proposed method is calculated.

The O-notation has been extremely useful in helping analyst to classify algorithms by performance and in guiding algorithm designers to search for the “best” algorithms for important problem.

So addition two s-bit number requires s bit operations. That is [6]:

T(s-bit + s-bit) = O(s)

For the input numbers of size n decimal digits

T(n + n) = O(log n) ,

where the number of bits of n equal $\log_2$ n.

The multiplication of two s-bits binary integers requires s^2 (s * s) bit operation, because it needs s addition operations. That is:

T(s-bit * s-bit) = $O(s^2)$

For the input numbers of size n decimal digits

$T(n * n) = O(\log n)^2$,

where the number of bits of n equals $\log_2$ n.

The Computational Complexity for the MVECC compared to the proposed methods is as follows:

Let the size of the input message unit is n in MVECC Method the encryption function is :

$c_1= m_1 * k_1$

$c_2= m_2 * k_2$

then:

$T(c_1)=O(\log n)^2$ bit operation.

$T(c_2)=O(\log n)^2$ bit operation.

The decryption function is:

$m_1= c_1 * k_1^{-1}$

$m_2= c_2 * k_2^{-1}$

then:

$T(m_1)=O(\log n)^2 + T(k_1^{-1})$

$T(k_1^{-1}) = O(\log n)^3$, by extend Euclid’s method

$T(m_1) = O(\log n)^2 + O(\log n)^3$ bit operation.

$T(m_2) = O(\log n)^2 + O(\log n)^3$ bit operation.

In Enhanced Method of MVECC

The encryption function is as follows:

$c_1= m_1 k_2 - m_2 \quad \bmod p$

$c_2= m_1 k_1 + m_2 \quad \bmod p$

Then:

$T(c_1)= O((\log n)^2) + O(\log n)$ bit operation.

$T(c_2)= O((\log n)^2) + O(\log n)$ bit operation.

The decryption function is:

$m_1= (c_1 + c_2) * (k_1 + k_2)^{-1} \quad \bmod p$

$m_2= (c_2 k_2 - c_1 k_1) * (k_1 + k_2)^{-1} \bmod p$

then,

$T(m_1)=O(\log n)^2 + O(\log n) + T((k_1 + k_2)^{-1})$

$T((k_1 + k_2)^{-1}) = O(\log n) + O(\log n)^3$

$T(m_1)=O(\log n)^2+O(2 \log n)+O(\log n)^3$ bit operation.

$T(m_2)=O(3 \log n)^2+O(2\log n)+O(\log n)^3$ bit operation.

Conclusion

After this, it is clear that the Menezes-Vanstone scheme has advantage that it does not need encoding the plaintext message in the elliptic curve. This makes it more efficient than the original ElGamal scheme. However, it needs computing the inverse of the two numbers in the key point. The plaintext as long as the cipher text and the key are pairs of two numbers. This characteristic exploited to make the system more efficient.

We proposed new variations of the MVECC. This variation gives the system more security because it mixes between the two numbers of the two-plaintext unit, it may be more confusion than the MVECC, and it needs calculating the inverses operation once only.

References

[1] J. H. Silverman," The Arithmetic of Elliptic Curves”, Graduate Text in Mathematics 106, Springer Verlag, 1986.

[2] K. Araki, T. Satoh and S. Miura, “Overview of Elliptic Curve Cryptography”, Proc.1998, International Workshop on Practice and Theory in Public-Key Cryptography (PKC 98) LNCS. Vol. 1431, pp.29-49, Springer-Verlag 1998.

[3] J.C.A.V.D. Lubbe, “Basic Methods for Cryptography”, Cambridge ISPN 1998.

[4] IEEE P1363: Standard Specification for Public-key Cryptography, Working Draft, Oct. 1998.

[5] W. Stallings, “Cryptography and Network Security Principle and Practice”, Addison Wesley, 1999.

[6] S. Y. Yan, “Number Theory for Computing”, Springer, 2000.

[7] E. Oswald, “Introduction to Elliptic Curve Cryptography”, Institute for Applied information Processing and Communication A-8010 Inffeldgasse 16a, Graz, Austria, Jul.2002.

الخلاصة:

أن مجموعة نقاط المنحنى البيضوي تشـــكل مجموعـــة أبيلية، والتي تكون أختيار مناسب لبناء حيز مشابه لمشـــكلة اللوغاريتم المتقطع .في هذا البحث سنقدم نظرة مبسطة الـــى نظام التشفير بطريقة مينزس-فانستون للمنحنيات البيضـــوية ونقدم مقترح متنوع لتحسين هذه الطريقة مما يجعلهـــا اكثـــر كفاءة من الطريقة الاصلية.