Sains Malaysiana 41(7)(2012): 907–910

Key Exchange in Elliptic Curve Cryptography Based on the Decomposition Problem

(Pertukaran Kekunci dalam Lengkungan Kriptografi Eliptik berdasarkan Masalah Perlupusan)

HILYATI HANINA ZAZALI & WAN AINUN MIOR OTHMAN*

ABSTRACT

In this paper, we presented a new key exchange method based on decomposition problem for elliptic curve cryptography. We showed that our key exchange method was not only an alternative method for designing keys in cryptography, but it also has improved security condition from the previous key exchange based on decomposition problem over non-commutative groups. We proposed elliptic an curve cryptography to be the new platform for our key exchange protocol and showed how it was implemented. The security of our protocol was based on discrete logarithm problem, which was not infeasible and strictly difficult to retrieve in elliptic curve cryptography without any prior knowledge.

Keywords: Discrete logarithm problem; elliptic curve cryptography; key exchange using decomposition problem; non-commutative groups

ABSTRAK

Kertas ini membentangkan satu kaedah pertukaran kekunci baru berdasarkan masalah pelupusan untuk lengkungan eliptik kriptografi. Kaedah pertukaran ini bukan sahaja suatu kaedah alternatif bagi mereka cipta kekunci dalam kriptografi, tetapi ia juga menambah baik lagi sistem keselamatan berbanding kaedah pertukaran kekunci berdasarkan masalah pelupusan tak kalis tukar tertib yang terdahulu. Lengkungan kriptografi eliptik akan digunakan sebagai platform utama dalam kaedah pertukaran kekunci berdasarkan masalah pelupusan tak kalis tukar tertib dan bagaimana kaedah aplikasinya akan ditunjukkan. Keselamatan bagi protokol baru ini adalah berdasarkan penyelesaian masalah diskrit logarithma dalam lengkungan eliptik kriptografi, dan kaedah ini adalah tak tersaur dan sukar untuk diselesaikan tanpa syarat-syarat tertentu.

Kata kunci: Kumpulan tak kalis tukar tertib; lengkungan elliptik kriptografi; masalah diskrit logaritma; pertukaran kekunci bagi masalah perlupusan

INTRODUCTION

Our aim in this paper was to study the mathematics of key exchange using decomposition problem in elliptic curve. Decomposition problem is a method introduced by Shpilrain and Ushakov (2005). It is a method of arranging certain parameters in a subgroup, depending on the particular group of , which needs to be a non-commutative group and denoted by centralizer . We extend the idea of key exchange using decomposition problem to elliptic curve cryptography that improved the security of key establishment protocol. We showed that the protocol is more secured and easier to compute than the previous protocol of key exchange over non- commutative group. The main idea was based on cyclic group and the discrete logarithm problem that relies in elliptic curve.

In the first section of this paper, we introduced the algebraic structure regarding the computations that are related to the protocols. Next we discuss on the mathematical background, which is needed in the construction of protocol. After a brief explanation on decomposition problem in non-commutative groups by Shpilrain and Ushakov (2005), we proposed an alternative method of key exchange based on decomposition problem using elliptic curve cryptography. Then we presented an analysis of computing the discrete logarithm problem. We also showed ways of choosing parameter in elliptic curve, which need to be considered to ensure the smoothness form for cryptography. At the end of this paper, we discuss some implementation issues and the advantages of using elliptic curve as the main platform.

ALGEBRAIC STRUCTURE IN ELLIPTIC CURVE CRYPTOGRAPHY

To determine the numbers of points we need to satisfy certain combination of operations called algebraic structure which is known as *groups* (Forouzan 2008). For elliptic curve, the group () is set of elements with binary operation +, that satisfies four properties (axioms). A *commutative group*, also known as an *abelian group*, satisfies four properties in groups plus property in commutativity. The properties are defined as follows:

Consider an elliptic curve with points $P = (x_p, y_p)$, $Q = (x_Q, y_Q)$ and $R= (x_R, y_R)$.

1. Closure:
   If P and Q are elements of G, then $R = P + Q$ is also an element of G.
2. Associativity:
   If P, Q and R are elements of G, then $(P + Q) + R = P + (Q + R)$.
3. Commutativity:
   For all P and Q in G, then $P + Q = Q + P$.
4. Existence of inverse:
   For each P in G, there exist an element P^*, called the inverse of P, such that $P + P^* = P^* + P = e$.
5. Existence of identity:
   For all P in G, there exist an element e, called the identity element, such that $e + P = P + e = P$.

Cyclic group in elliptic curve is a group that has their own cyclic subgroup. Let say, we have a group which is a cyclic group, and the elements that generates in cyclic subgroup can also generate the group itself. We refer it as a generator. If g is a generator, the elements in a finite cyclic group can be written as:

$$\{e, g, g^2, \ldots, g^{n-1}\} \text{ where } g^n = e.$$

Note that a cyclic group can have many generators. And the finite field is a field with finite number of elements, also known as Galois fields and denoted by GF(q).

MATHEMATICAL BACKGROUND IN ELLIPTIC CURVE CRYPTOGRAPHY

The mathematical computation on elliptic curve cryptography requires an abelian group constructed from elliptic curve over finite fields. From the paper by Závadský and Horňanová (2008), they defined the finite field $\mathbb{F}$ in elliptic curve as a set of $\mathbb{F}$ and two operations (+) and (.) which is:

1. $\mathbb{F}$ is an additive group concerning to operation (+)
2. $\mathbb{F}\backslash\{0\}$ is a multiplicative group concerning to operation $(\cdot)$
3. For all $a, b, c \in \mathbb{F}$ holds

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and}$$
$$(a + b) \cdot \mathrm{c} = (a \cdot c) + (b \cdot c).$$

There are two type of finite fields involve in elliptic curve cryptography which are:

1. Elliptic curve over a field $\mathbb{F}_\mathrm{q} = \{0, 1, \ldots, \mathrm{q} - 1\}$
2. Elliptic curve over a field $\mathbb{F}_2\mathrm{m} = \{0, 1, \ldots, 2^\mathrm{m} - 1\}$ of characterization 2

The points on elliptic curve, E of the form $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{F}$ will be defined as over galois field GF(q) with characteristic q larger than 3 and $4a^3 + 27b \neq 0$. For all points (x, y) on E, there will be a point $x \in \mathbb{F}_q$, $y \in \mathbb{F}_q$ and point at infinity. It can be summarized as below:

Elliptic curve, $E : y^2 \equiv x^3 + ax + b \pmod q$, and defined $\mathbb{F}$ as the finite field with $q > 3$

$$E(\mathbb{F}_q) = \{(x,y) \in \mathbb{F}_{q^2} \,; y^2 = x^3 + ax + b\} \cup \{\infty\},$$

where a, $b \in \mathbb{F}_q$ and $\Delta = 4a^3 + 27b = 0$. Δ is called *discrimant* of elliptic curve, and the condition that $\Delta \neq 0$ ensure that the curve is *smooth* or, there are no points at which the curve has more than one distinct tangent lines. The *point at infinity* denoted by ∞, also said to be one of the set of all points on E serving as identity element in the operations.

DECOMPOSITION PROBLEM

Decomposition problem is a method of computing public key exchange, introduced by Shpilrain and Ushakov (2005). It is an arrangement of different keys in certain subgroup. Specific ways to construct the sequences depend on the particular group of G, which is G has to be non-commutative, and the group of G denote by the centralizer of $g \in G$. Centralizer is used to compute the sufficient element in group G. They introduced this protocol to improve the security of key establishment on decomposition problem. To prevent any possible attacks on the protocol, they also include some requirements in the choosing of group G.

As an alternative method, we proposed elliptic curve cryptography to be the new platform for this key agreement. We used a class of group constructed using points on an elliptic curve. This set of points form a commutative group under a group operation as required in elliptic curve cryptography. This differs from the method in Shpilrain and Ushakov (2005) in which the security of the protocol depends on a particular platform group G, in which, G at the very least has to be non-commutative to avoid the so-called length attacks which present a serious threat.

The elements of the previous protocol will be replaced as points on the curve, and each of the points must satisfy the algebraic structure in elliptic curve. From the previous protocol, the adversary needs to compute the centralizer which is usually hard, before arranging the length attack to the protocol. Compare to the protocol for elliptic curve, the adversary needs to solve the discrete logarithm problem, which is needed to obtain the number of points on the curve, r or s. It is computationally not feasible to obtain, if r or s is large enough.

Key Agreement Based On Decomposition Problem For Elliptic Curve

Consider the domain parameters in this protocol defined by elliptic curve, E over the finite field, $\mathbb{F}_q$ with order n. Assume that there are two users involved in this key agreement; Alice and Bob, have no prior contact and the only communication channel between them is public. They both agreed on a same public point $Q \in [1, n-1]$ on the curve E, and the different cofactor for each users: r and s where r or $s = \#\mathrm{E}(\mathbb{F}_q)/\mathrm{n}$. $\#\mathrm{E}(\mathbb{F}_q)$ is the number of points on an elliptic curve. This is the following sequence of steps:

Protocol:-

1. Alice chooses a private point $a_1 \in E(\mathbb{F}_q)$ takes $\#E(\mathbb{F}_q) = r$, and a generator of $E(\mathbb{F}_q)$ is $a_1 = (x_{a1}, y_{a1})$. Alice gathers the points to be $A = \{\alpha_1, \alpha_2, \ldots, \alpha_{r-1}\}$ and publishes it.
2. Bob chooses a private point $b_2 \in E(\mathbb{F}_q)$, takes $\#E(\mathbb{F}_q) = s$, and a generator of $E(\mathbb{F}_q)$ is $b_2 = (x_{b2}, y_{b2})$. Bob gathers the points to be $B = \{\beta_1, \beta_2, \ldots, \beta_{s-1}\}$ and publishes it.
3. Alice gets $< \beta_1, \beta_2, \ldots, \beta_{s-1} >$ from the public channel, and she picks another point as her private and defines it as a_2. Then she multiplies it with private key a_1 and public point Q to obtain $P_A = a_1 Q a_2$, then sends it to Bob.
4. Similarly, Bob gets $< \alpha_1, \alpha_2, \ldots, \alpha_{r-1} >$ from the public channel, picks a point to be his other private and defines it as b_1. Then he multiplies it with his private key b_2 and public point Q to obtain $P_B = b_1 Q b_2$, then sends it to Alice.
5. Alice multiplies the P_B from Bob with her private key a_1, a_2 and defines it as $K_A = a_1 P_B a_2$.
6. Bob multiplies the P_A from Alice with his private key b_1, b_2 and defines it as $K_B = b_1 P_A b_2$.

Since the curve $E(\mathbb{F}_q)$ is cyclic, so that we will have $a_1a_2 = a_2a_1$ and $b_1b_2 = b_2b_1$ and from here it shows that $K_A = K_B = K$. They will have the same shared key using this decomposition problem in E.

Security Analysis

The security of the proposed protocol is based on the difficulty of computing elliptic curve discrete logarithm problem and the decomposition problem scheme.

We present the confidentiality of the private key in this protocol. Let say an eavesdropper want to obtain $a_1, a_2 \in P_A$ and $b_1, b_2 \in P_B$ from all the public information that he can retrieve from the public channel. But the difficulty is equivalent to solving the elliptic curve discrete logarithm problem (ECDLP).

ECDLP: From elliptic curve E defined over a finite field $\mathbb{F}_q$, a point $a_1 \in E(\mathbb{F}_q)$ of order n and a point $a_1 \in < A >$, find the integer $r \in [1, n-1]$ such that $\alpha_1 \in ra_1$. The integer r is called discrete logarithm problem of α_1 to base α_1 denoted by $r = \log_{a1}\alpha_1$.

The computation of the discrete logarithm problem in this protocol should be infeasible or strictly hard to retrieve in $E(\mathbb{F}_q)$.

Our protocol also depends on which elliptic curve platform we need to take since there will be several ways to choose the parameter A and B for elliptic curve defined by $E : y^2 = x^3 + Ax + B$ and must satisfy $4A^3 + 27B^2 \neq 0$. This condition helps to make sure the curve is smooth (i.e.: with no cusps). And it is known as discriminant, it could not be zero for elliptic $E(\mathbb{F}_q)$ to possess three distinct roots. If the discriminant is zero, that would imply for two or more roots to coalesce, giving the curve a cusp or some other form of non-smoothness. Non-smooth curves are singular, and it is not safe to use singular curve for cryptography.

The number of points on E denoted by $\# E(\mathbb{F}_q)$. Since of integers mod are quadratic residues, the number of points will be roughly $q+1$, counting the point to infinity. Hasse's theorem states that the number of points on an elliptic curve (including the point at infinity) is:

$$\#\mathrm{E}(\mathbb{F}_q) = q + 1 - t \quad \text{with } q \text{ is prime where } |t| < 2\sqrt{q}.$$

If the value for $t^2 = 0, q, 2q, 3q$ or $4q$, then the curve E is said to be non-supersingular. Thus, the advantages of choosing curve as non-supersingular helps to prevent from the Menezes, Okamoto, and Vanstone (MOV) attack (Koblitz et al. 2000).

However, the security of Shilprain and Ushakov (2005) is only based on the assumption that given public elements w, P_a, P_b it is hard to distinguish the shared key K from a random element of the form awb. In order to make the protocol secure, they need to choose a large number for the centralizer $C_G(g)$ which G is a group and $g \in G$. Furthermore, they need to choose the platform for group G that satisfy certain properties such as G has to be a non-commutative group. Since public key cryptography is also called asymmetric cryptography, meaning encryption with a public key is easy and decryption without the correct private key is hard. The same concept applies to our key exchange protocol in elliptic curve cryptography; where given the public points P_A, P_B and Q, it is hard to determine the shared key K from the combination of private keys and public key. This shows that the security of the protocol by Shilprain and Ushakov (2005) also applies to our protocol.

The difference between our protocol and Shilprain and Ushakov (2005) is that ours is applied on a new different platform which is on elliptic curve cryptography. Thus, our protocol is more secured since it is based not only on the difficulty of the decomposition problem scheme, but also on the computational infeasibility maintained by the elliptic curve discrete logarithm problem and the security provided by elliptic curve cryptography.

Implementation Issues For Decomposition Problem In Elliptic Curve

The implementation of the group operation in decomposition problem should be easy to apply, but still keeps the inverse of the calculation hard to compute. This is the reason why we are using elliptic curve as the main platform in this protocol. Our new key exchange in elliptic curve cryptography based on decomposition problem observes as an alternative to the previous key exchange in Elliptic Curve Diffie-Hellman (ECDH).

Based on the idea by Koblitz et al. (2000), the efficiency of this protocol can be compared by the times to compute:

1. Point $P_A = a_1 Q a_2$ where $a_1, a_2 \in E(\mathbb{F}_q)$ and $q = q^m$, where q is a prime and m $\approx$ 160, Q is a random public point with 160-bit integer. The computation of P_A repeated doubling and adding to the average and requires 320 elliptic curve doubling and 160 elliptic curve additions.

It should be known that E must be non-supersingular, so that it is suitable to use elliptic curve in cryptography. The advantages of using elliptic curve are with the implementation of a smaller group in elliptic curve systems, helps to low-cost and low-power implementation in computing environments such as smart cards (Agnew et al. 1993), and the underlying of field $E(\mathbb{F}_q)$ and a representation for its elements can be selected so that the field arithmetic (addition, multiplication, inversion) can be optimized.

Conclusion

Key exchange in elliptic curve cryptography using decomposition problem can be considered as an alternative method from the previous protocols such as Elliptic Curve Diffie-Hellman (ECDH) (Forouzan 2008) and key exchange based on decomposition problem over non-commutative groups (Shpilrain & Ushakov 2005). The security of our scheme relies on computing the discrete logarithm problem. This key agreement also considers the parameters that are commonly used in elliptic curve. Compare to the previous protocols, our protocol seems to work better and is more secured because points will be the elements for the computation. For future works, we would like to do an implementation of our key exchange based on decomposition problem with the encryption method in elliptic curve cryptography. We will focus on effort to establish a stronger confidence in the system that determines concrete computer design for practical purposes. We hope to give results on practical values in the future.

Acknowledgements

Our research have been supported by IPPP/UPDiT/Geran(PPF)/FP083/2007C and IPPP/UPDiT/Geran(PPP)/PS300/2008C, University Malaya grants for 2009.

References

Agnew, G.B., Mullin R.C. & Vanstone S.A. 1993. An implementation of Elliptic Curve Cryptosystems over, *IEEE Journal On Selected Area Communication* 11(5): 804-813.

Forouzan, B.A. 2008. *Cryptography and Network Security*. 1st ed. pp. 98 -103. New York: McGraw-Hill.

Koblitz, N., Menezes, A. & Vanstone, S. 2000. The State of Elliptic Curve Cryptography, *Designs, Codes and Cryptography* 19(5): 173-193.

Shpilrain, V. & Ushakov, A. 2005. A New Key Exchange Protocol Based on the Decomposition Problem. *International Association for Cryptologic Research*, available at: eprint.iacr.org/2005/447.pdf

Závadský, P. & Horňanová J. 2008. Group Signatures and Elliptic Curve Cryptography. *Bezadis Cryptography Symposium*, available at: bezadis.ics.upjs.sk/old/cryptosymposium/files/paper15.pdf

Institute of Mathematical Sciences
Faculty of Science
Universiti Malaya
50603 Kuala Lumpur
Malaysia

*Corresponding author; email: wanainun@um.edu.my

Received: 30 December 2010
Accepted: 21 February 2012