World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:1, No:6, 2007

Key Exchange Protocol over Insecure Channel

Alaa Fahmy

Open Science Index, Computer and Information Engineering Vol:1, No:6, 2007 publications.waset.org/5377/pdf

***Abstract*—**Key management represents a major and the most sensitive part of cryptographic systems. It includes key generation, key distribution, key storage, and key deletion. It is also considered the hardest part of cryptography. Designing secure cryptographic algorithms is hard, and keeping the keys secret is much harder. Cryptanalysts usually attack both symmetric and public key cryptosystems through their key management. We introduce a protocol to exchange cipher keys over insecure communication channel. This protocol is based on public key cryptosystem, especially elliptic curve cryptosystem. Meanwhile, it tests the cipher keys and selects only the good keys and rejects the weak one.

***Keywords*—**Key management and key distribution.

I. Introduction

KEY management is considered the hardest part of cryptography. Designing secure cryptographic algorithms is hard, and keeping the keys secret is much harder. Cryptanalysts usually attack both symmetric and public key cryptosystems through their key management. When people choose their own keys, they generally choose poor ones. Choosing keys that are relevant to personal information e.g. user's names, initials, and account name. Good keys are random bit strings generated by some automatic process. Some encryption algorithms have weak keys, specific keys that are less secure than other keys. Therefore, it has been argued to test keys before use. For example, DES cryptosystem has 16 weak keys out of 2^{56} [1].

Generating a random key isn't always possible. Sometimes you need to remember your key. Therefore, you have to select your key in a way that is easy to remember, but difficult to guess. In this paper, we introduce a technique based on elliptic curve cryptosystem [2] to exchange the cipher keys. The rest of the paper includes the following: section 2 presents motivation and overview of elliptic curves. Section 3 introduces key exchange protocol, which is based on ElGamal cryptosystem [3]. Section 4 concludes the paper.

II. Motivation and Overview

The study of elliptic curves has led to a solution of the congruence problem [4]. Lenstra [5] proposed a technique for factoring algorithm using group law that relates the points of an elliptic curve. This group law is the basis for Miller's elliptic logarithm [6] adaptation of the Diffie Hellman key exchange protocol [7]. The most common equation to define the elliptic curves are known as Weierstrass equation [8]. For the prime field GF (P) with P>3, the Weierstrass equation is given by "(1)":

$$y^2 = x^3 + ax + b \quad (1)$$

Where a, and b are integers modulo P for which $4a^3 + 27b^2 \neq 0 \pmod P$. The hard problem is "elliptic logarithm" on an elliptic curve modulo P: given points G, y, find "a" such that y = a G. For the binary finite fields GF (2^m), the Weierstrass equation is given by "(2)":

$$y^2 + xy = x^3 + ax^2 + b \quad (2)$$

Where a, and b are elements of GF(2^m) with $b \neq 0$. The elliptic curve E consists of the solutions (x,y) over GF(q) to the defining equation, along with an additional point called the point at infinity (denoted O). The points other than O are called finite field points. The number of points on E (including O) is called the order of the curve E and denoted by # E(GF(q)).There are two basic operations of elliptic curves, namely addition, and multiplication defined as follows:

A. Addition Operation

Define the inverse of the point p =(x,y) by "(3) to be:

$$\begin{aligned} -p &= (x, -y) \text{ if } q = P \text{ prime}, \\ &= (x, x+y) \text{ if } q = 2^m. \end{aligned} \quad (3)$$

Then, the sum p + q of the points p and q is the point R, with p, q, and –R lie on a curve, with the property p + O = p, and p + (-p) = O, for all points p. To illustrate the addition operation on E over Z_p, let p=(x_1,y_1), and q=(x_2,y_2) are points on E. If $x_2=x_1$, $y_2=-y_1$, then p + q =O.
Otherwise p + q = (x_3,y_3), defined by "(4)", where

$$\begin{aligned} &x_3=\lambda^2-x_1-x_2,\ y_3=\lambda(x_1-x_3)-y_1, \\ &\lambda = (y_2-y_1)/(x_2-x_1) \quad \text{if } p \neq q \\ &\quad = (3x_1^2+a)/2y_1 \quad \text{if } p=q \end{aligned} \quad (4)$$

B. Scalar Multiplication

Elliptic curve points can be added but not multiplied. However, it possible to perform scalar multiplication, which is another name for repeated addition of the same point. If n is a positive integer and p a point on E, then the scalar multiplication is "n p" (adding "p" n times), with the property Op = O, and (-n)p = n(-p). Meanwhile Meneze, Vanstone (MQV) [3], assume that the points p, q, and –R could not lie on E.

Manuscript received May 1, 2005.

Alaa Fahmy is with the Military Technical College, Cairo, Egypt. Work as visiting professor at the university of Calgary, Alberta, Canada (e-mail: af200345@hotmail.com).

Open Science Index, Computer and Information Engineering Vol:1, No:6, 2007 publications.waset.org/5377/pdf

III. Key Exchange Protocol

The protocol uses the ElGamal cryptosystem [9] based on elliptic curve as an application. To illustrate how the ElGamal cryptosystem works, let P be a prime such that the discrete logarithm problem in (Z^*_P) is infeasible, and let $\alpha \in Z^*_P$ be a primitive element. Let $P = Z^*_P$, $\xi = Z^*_P \times Z^*_P$, and define $\kappa=\{(P,\alpha,a,\beta): \beta \equiv \alpha^a \bmod P\}$. The values P, α, and β are public key, and "a" is the private key. For $\kappa=(P,\alpha,a,\beta)$, and $\kappa \in Z_{P-1}$, define the encryption process by "(5)":

$$E_\kappa(x, \kappa)=(y_1, y_2) \quad (5)$$

Where,
$y_1 = \alpha^\kappa \bmod P$,
$y_2 = x\,\beta^\kappa \bmod P$.

For $y_1, y_2 \in Z^*_P$ define the decryption process by "(6)":

$$D_k(y_1, y_2) = y_2 (y_1{}^a)^{-1} \bmod P. \quad (6)$$

But it is not our goal to make encryption & decryption of a message x. We want to exchange a cipher key over insecure channel. Therefore, we consider x is our secret session key to be exchanged in a secure manner. To achieve this goal, let Alice and Bob are two parties want to exchange their session key. Alice and Bob both are agreed upon elliptic curve E, and the prime P. The key exchange protocol was implemented by using MATLAB 6.5, and was proceeded as follows:

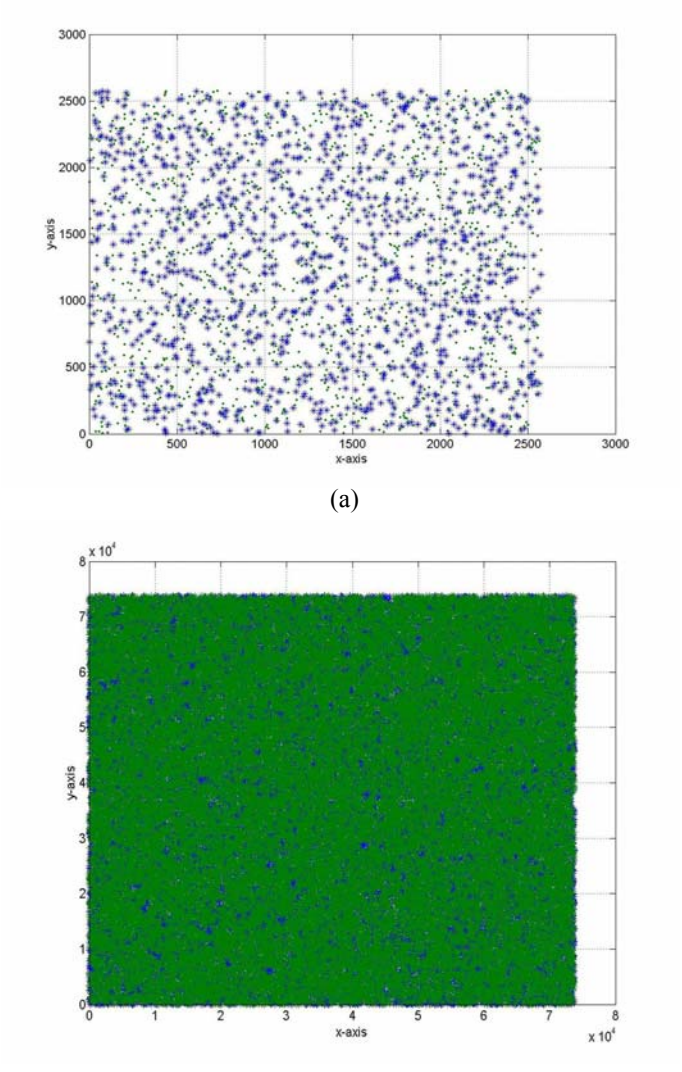
A. At Alice Side

1) Selects the pre-agreement prime number P.
2) Constructs the elliptic curve E: $y^2 = x^3 + ax + b$ over Z_P, where a, b are constants such that:
$$4a^3 + 27b^2 \neq 0 \pmod P.$$
3) Computes the curve order #E = N.
4) Find all field elements (F).
5) Check for **Q**uadratic **R**esidues and **N**on- **Q**uadratic **R**esidues (**QR** & **NQR**).
6) Find the **R**ational points that satisfy the field equation (**R**).
7) Find the **g**enerator element (**g**), that can generates all field elements. This can be achieved by computing (P-1), find the factors of (P-1) "$\mathbf{g}_i$" , and then check for $\mathbf{g}^{(P-1)}/q_i \neq 1$, $\mathbf{g}$=2 to P-1.
8) Find ϕ (n)= (P-2), which are required to compute λ (elliptic curve operations).
9) Selects the session key to be exchanged k <N-1.
10) Set x = k in ElGamal cryptosystem and tests it (good/weak) just by using the decryption process. If you could recover x/ k, then select that key as a good key, otherwise reject it (weak one) [10]. On the other hand the scheme suggests the nearest good key to be used as a session key.
11) Selects a rational point $r \varepsilon \mathbf{R}$ such that $r = (r_x, r_y)$.
12) Computes the doubling of that point r by k., i.e. find another a rational point $r^* = (r^*_x, r^*_y)$ such that $r^*_x = k\, r_x$, and , $r^*_y = k\, r_y$
13) Alice sends r^* to Bob.

B. At Bob side

1) Performs the steps 1:8 as Alice did (off line, and waiting for Alice transmission), just loading **F**, **QR**, **NQR**, **R**, and **g**.
2) Bob receives r*, and look for it in R.
3) Counts and Finds the amount of doubling for $r^* \varepsilon R$, which represents the original session key k.

Fig.1 illustrates an example of the field elements over F2579, and F73727 respectively.



(a)

(b)

Fig.1 Field Elements (a) Over F2579 (b) Over F73727

IV. Conclusion

Designing secure cryptographic algorithms is hard, and keeping the keys secret is much harder. Cryptanalysts usually attack both symmetric and public key cryptosystems through their key management. We introduced a protocol to exchange cipher keys over insecure communication channel. This protocol is based on public key cryptosystem, especially elliptic curve cryptosystem. Meanwhile, it tests the cipher keys, selects only the good keys, and rejects the weak one. On

the other hand it suggests the nearest good key on E to be used as a session key.

REFERENCES

[1] Bruce Schneier "*Applied Cryptography*", 2nd edition, John Wiley & Sons, Inc, 1996.
[2] IEEE Standard Specifications for public key cryptography, IEEE std 1363-2000.
[3] Donglasr Stinson, "*Cryptography Theory and Practice*", 2nd edition, Chapman & Hall/CRC, 2002.
[4] Neal Koblitz, "*Introduction to elliptic curves and modular forms*", vol.97 of graduate texts in mathematics, Springer-Verlag, 1984.
[5] H.W. Lenstra, " *Elliptic curve factorization*" , Memorandum, 1985.
[6] Victor Miller, "*Elliptic curves and cryptography*", proceeding of crypto85, 1985.
[7] Whitfield and Martin E. Hellman, " *New directions in cryptography*", IEEE transactions in Information theory, IT-22(6), pp 644-654, Nov., 1966.
[8] Meneze, A., Okamoto, T., and Vanstone, S. "*Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*", IEEE Transactions on Information Theory 39 (1993), pp. 1639-1646.
[9] T. ElGamal, "*A public key cryptosystem and a signature scheme based on discrete logarithms*", IEEE Trans. On information theory,IT-31, no.4, pp.469-472, 1985.
[10] Alaa Fahmy, "*Weak Keys For ElGamal Cryptosystem*", 4th International Conference on Electrical Engineering ICEENG2004, 23-25 Nov. 2004.

Alaa Fahmy was borned in Cairo 1959, graduated from MTC, Cairo 1982. Had M.Sc. degree from MTC, Jan.1991. Full time Ph.D. student at the university of Kent, Canterbury, England and had Ph.D. degree in electrical engineering in the field of cryptography Aug. 1994. Teacher at the MTC by sept. 1994 in the electrical engineering dept. Supervising so many M.Sc. & Ph.D. thesises and many reseaches in the field of cryptography. Promted to Associate Professor at MTC, electrical engineering dept. by sept.2001. Worked as visiting professor at the univeristy of Calgary, Electrical and Computer Engineering (ECE), dept., Alberta, Canada, Jun.2003. Field of interset, cryptography, and steganography.

Open Science Index, Computer and Information Engineering Vol:1, No:6, 2007 publications.waset.org/5377/pdf