Hasil Penelitian Riset KK ITB ”Identifikasi Weak Class dari Kurva Eliptik untuk menguji Tingkat Keamanan Kriptografi”

Elliptic Curve Weak Class Identification for the Security of Cryptosystem

Dr. Intan Muchtadi,Dr. Ahmad Muchlis, Prof. Kuspriyanto

EXTENDED ABSTRACT :

Cryptography is a science of securely transmitting messages from a sender to a receiver. The objective is to encrypt the message in a way such that an eavesdropper would not be able to read it. A cryptosystem is a system of algorithms for encrypting and decrypting messages for this purpose. Interoperability and security are the most important things for this networking environment. Elliptic Curve Cryptosystem (ECC) is a relatively new public key cryptosystem suitable for environment with limited resources such as mobile computers and smart cards, as ECC efficiently gives high level security with key length shorter than other known public key cryptosystem such as RSA. In [PKSS2009] we discussed issues in implementing Elliptic Curve Cryptography (ECC) and we provided a brief explanation about ECC basic theory and implementation.

In [DiHe76], Diffie and Hellman described a scheme by which two individuals A and B could exchange a secret cryptographic key. The system had the advantage that all transmission could be made over a public channel, and yet at the termination of this process only A and B would be in possession of the secret key. The security of the system is based on the computation of discrete logarithms in some group (the Discrete Logarithms Problem –DLP).

For the class group of an imaginary quadratic order –the group proposed by Buchmann and Williams [BuWi88]- the DLP seems to be hard. Also, Koblitz [Kob87] and Miller [Mil86] have also pointed out that the group of points on an elliptic curve over a finite field can also be used to develop a secure key-exchange system, meaning that the DLP for this group is also hard to solve.

Imaginary quadratic orders are closely related to non-supersingular elliptic curves over finite fields. They happen to be isomorphic to their endomorphism rings. Thus a sound understanding of imaginary quadratic orders may lead to a better understanding of the security of elliptic curve cryptosystems.

In [PaTa98], there was proposed a cryptosystem based on non-maximal imaginary quadratic orders, a public key cryptosystem with quadratic decryption time, which makes the decryption as efficient as RSA-encryption. In [HT99] it is shown that for the special case of *totally non-maximal* imaginary quadratic orders, there is an algorithm to compute discrete logarithms. It is shown that the discrete logarithm problem in the class group of a *totally* non-maximal imaginary quadratic order can be reduced to the discrete logarithm problem in finite fields. In other word, there is a *week class for class groups* of imaginary quadratic orders. Hence one open question is whether this result might yield another week class of elliptic curves, i.e. where the corresponding endomorphism ring is a *totally non-maximal* imaginary quadratic order.

The aim of this research is to identify a weak class of elliptic curves, a specific class which gives low level security of cryptosystems. The method for this identification is the study of the close relation between imaginary quadratic orders and elliptic curves, also of the weak class of non-maximal imaginary quadratic orders in order to get the weak class of elliptic curves. From this

identification, we can avoid the use of this class to get elliptic curve cryptosystems with high level security.

In [MM] we explained the close relation between elliptic curves and imaginary quadratic orders, especially totally non-maximal imaginary quadratic orders, with respect to its application in cryptography. We have shown that for a fundamental discriminant D, a prime q satisfies $4q = 1 - D$ such that $p = q + 2$ is a prime, and E an elliptic curve over Fq whose number of points is p and End(E) is some imaginary quadratic order, the discrete logarithm problem in E(Fq) can be reduced to the discrete logarithm problem in finite field of order p^2 as an additive group. Hence we get a necessary condition to classify a class of cryptographically weak curves.

In [P2009] we explained how to solve the discrete logarithm problem of anomalous elliptic curves and because of that, the anomalous curves are considered as weak. In [Y] we explained how to construct elliptic curves if we know the imaginary quadratic order. Moreover in [LMVV2005] it is explained how to construct the anomalous elliptic curves. Based on these results, in [MMY2009] we explained how to construct the curves with properties explained in [MM], based on the construction of anomalous curves ([LMVV2005]). We gave an algorithm to construct such class. Moreover this algorithm can be used for more general situation not only for constructing the weak class explained in [MM].

In [MYM2009] we answered the question of existence of the weak class obtained in [MM] and [MMY2009], called the twisted anomalous curves. We gave several examples of this class. We used the following method: from some twin primes, we chose the ones which satisfied the conditions in [MM]. Then we used PARI, first to compute the coefficient *a* and *b* in the equation $y^2 = x^3 + ax + b$, second to generate the elliptic curve, and finally to compute the order of the group of rational points of the elliptic curve. From the order of this group we can decide whether the elliptic curve is anomalous or twisted anomalous. Finally we can get anomalous and twisted anomalous curves from one another.

REFERENCES:

[BuWi88] J.Buchmann dan H.C.Williams: *A key exchange system based on imaginary quadratic field*. Journal of Cryptology, **1,** 1988, pp.107-118.

[DiHe76] W.Diffie dan M.Hellman: *New directions in cryptography*, IEEE Transactions on Information Theory **22**, 1976,pp.472-492. [HT99] D.Huhnleim, T.Takagi : *Reducing logarithms in totally non-maxima imaginary quadratic orders to logarithms in finite field,* ASIACRYPT, 219-231.

[Kob87] N.Koblitz: *Elliptic curve cryptosystem*. Mathematics of Computation **48**, 1987, pp.203-209.

[LMVV2005] F. Leprevost, J.Monnerat, S. Varrette, S.Vaudenay: *Generatinganomalous elliptic curves*, Information Processing Letters, **93**, 225-230.

[Mil86]V.S. Miller: *Use of elliptic curve in cryptography*, Advances in Cryptology – CRYPTO '85, Springer-Verlag, **LNCS 218**, 1986, pp.417-426.

[MM] I. Muchtadi-Alamsyah, A. Muchlis: *Elliptic Curve Cryptography via Imaginary Quadratic Orders,* submitted to Proceeding International Conference on Mathematics and Natural Sciences, 2008.

[MMY2009] I. Muchtadi-Alamsyah, A. Muchlis, F. Yuliawan: *Elliptic Curve Weak Class Identification for the Security of Cryptosystem,* submitted to Proceeding Non Commutative Rings and Their Applications, Lens, July 2009.

[MYM2009] I. Muchtadi-Alamsyah, F. Yuliawan, A. Muchlis: *Reducing Logarithms in Twisted Anomalous Elliptic Curves to Logarithms in Finite Fields,* submitted to International Journal of Mathematics and Mathematical Sciences, Hindawi publisher.

[PKSS2009] M.W.Paryasto,Kuspriyanto, S. Sutikno, A. Sasongko: *Issues in Elliptic Curve Cryptography Implementation,* Internetworking Indonesia Journal **Vol. I No.1**, 2009, pp.29-33.

[PaTa98] S.Paulus and T.Takagi : *A new public key cryptosystem with quadratic decryption time*, Journal of Cryptology, 1998.

[P2009]M.R. Pratama: Penyelesaian Masalah Logaritma Diskrit pada Kurva Eliptik dengan Trace satu, Tesis P rogram Magister Matematika ITB, 2009.
[Y] F. Yuliawan : Generating Elliptic Curves, Tesis Program Magister Matematika ITB, in preparation.

LIST OF RESEARCH OUTPUT

1. I. Muchtadi-Alamsyah, A. Muchlis: *Elliptic Curve Cryptography via Imaginary Quadratic Orders,* submitted to Proceeding International Conference on Mathematics and Natural Sciences, 2008.
2. I. Muchtadi-Alamsyah, A. Muchlis, F. Yuliawan: *Elliptic Curve Weak Class Identification for the Security of Cryptosystem,* submitted to Proceeding Non Commutative Rings and Their Applications, Lens, July 2009.
3. I. Muchtadi-Alamsyah, F. Yuliawan, A. Muchlis: *Reducing Logarithms in Twisted AnomalousElliptic Curves to Logarithms in Finite Fields,* submitted to International Journal of Mathematics and Mathematical Sciences, Hindawi publisher.
4. M.W.Paryasto,Kuspriyanto, S. Sutikno, A. Sasongko: *Issues in Elliptic Curve Cryptography Implementation,* Internetworking Indonesia Journal **Vol. I No.1**, 2009, pp.29-33.