Hasil Penelitian Hibah Pascasarjana ”Algoritma Efisien untuk Menentukan Kurva Eliptik yang sesuai untuk Kriptografi”

Efficient Algorithm for Determining Elliptic Curves Suitable for Cryptography

Dr. Ahmad Muchlis,

Dr. Intan Muchtadi,

Prof. Kuspriyanto

EXTENDED ABSTRACT

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.

Koblitz [Kob87] and Miller [Mil86] have pointed out that the group of points on an ellipticcurve over F_q can be used to develop a secure key-exchange system. In [Baier2002] Baier proposed an efficient algorithm for determining elliptic curves over finite field of characteristic more than three. The aim of this research is to generate an efficient algorithm for determining elliptic curves over finite field of characteristic 2 or 3 suitable for cryptography. These types of curves are more implementable than elliptic curves over finite field of characteristic more than 3.

For this purpose, in this research we studied about finite field basis conversion and generated some algorithms and implementation for this basis conversion, as the elliptic curves operations basically generated by finite field operations. Two of the most common basis used are polynomial basis and normal basis. The ONB especially are known to be more efficient for hardware implementation than polynomial basis. A combination of both normal basis and polynomial basis can take advantage of the strength of each for maximum efficiency.

Conversion of finite field elements from one basis representation to another representation in a storage-efficient manner is crucial if these techniques are to be carried out in hardware for cryptographic applications. Kaliski and Yin [KaliskiYin99] describe algorithms for basis conversion

between normal and polynomial basis that involve primarily finite-field operations, rather than, for instance, matrix multiplications.

In [MPK2009] we proposed some modifications from the general algorithms for some specific cases, i.e. basis conversion between polynomial basis and type I and type II optimal normal basis to gain more computational efficiency, using the properties of type I and type II optimal normal basis and field operations. We showed that in the change-of-basis matrix there exists one row in which there exists only non-zero element. For the case of binary fields where the two bases have the same generator, we constructed the algorithms based on these non-zero elements. With the algorithms, it is possible to extend an implementation in one basis so that it supports other choices of basis.

In [PRMK2009] we have shown an implementation of the algorithms in [MPK2009] to perform conversion from PB to ONB-I and vice versa. The implementation was done in C language. The implementation was aimed to use memory efficiently and left further research for execution time-optimized implementation.

In [MPK2009b] we proposed some modifications from the general algorithms for some specific cases to gain more computational efficiency, using the properties of type I and type II optimal normal basis and field operations. We gave a general case of the results in [MPK2009] and [PRMK2009] for the conversion polynomial basis – optimal normal basis type I. For the conversion polynomial basis –optimal normal basis type II we modify the result in [MPK2009] in order to get a more efficient implementation.

An improvement of the above results has been carried out in [MKY2009]. We described several newalgorithms for storage-efficient conversion betweenoptimal normal basis and polynomial basis. The use ofsome permutation of optimal normal basis andpolynomial basis with the same generator enable us toreplace multiplications on optimal normal basis withsimpler operations and some multiplications onpolynomial basis. The storage requirements of the newalgorithms are the same as previous algorithms, whichis O(m) bits.An implementation of these new algorithms has been done and we are preparing an article on this implementation.

CONCLUSION:

In this research we have obtained several algorithms and implementations on finite field basis conversion. The next step will be to apply these algorithms on elliptic curve operations in order to obtain an efficient algorithm for determining elliptic curves suitable for cryptography. Moreover, these algorithms can also be used for elliptic curve cryptography since this cryptography is performed via elliptic curve operations, finite field operations and finite field basis conversion. This will be subject of further research.

REFERENCE:

[Baier2002] H.Baier: *Effcient Algorithms for Generating Elliptic Curves over Finite Fields Suitable for Use in Cryptography,* PhD Dissertation, 2002.

[KaliskiYin99] B. S. Kaliski Jr. and Y. L. Yin: *Storage-efficientfinite field basis conversion*, in S. Tavares and H.Meijer (Eds.), SAC '98, **LNCS**156, 81-93, 1999.

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

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

[MKY2009] A. Muchlis, M.H. Khusyairi, F. Yuliawan: *Storage-Efficient Finite Field Basis Conversionvia Efficient Multiplication,* submitted to Proceeding International Symposium on Computational Sciences, Bali October 2009.

[MPK2009] I. Muchtadi-Alamsyah, M.W. Paryasto, M.H. Khusyairi: *Finite Field Basis Conversion,* Proceeding International Conference on Mathematics, Statistics and Its Applications, Bukittinggi June 2009, pp. 15-18.

[MPK2009b] I. Muchtadi-Alamsyah, M.W. Paryasto, M.H. Khusyairi: *Finite Field Basis Conversion and Its Implementation,* submitted to Proceeding International Symposium on Computational Sciences, Bali October 2009.

[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.

[PRMK2009] M.W. Paryasto, B. Rahardjo, I. Muchtadi-Alamsyah, M.H. Khusyairi: *Implementation of Polynomial Basis-Optimal Normal Basis I Basis Conversion,* submitted to Jurnal Ilmiah Teknik Komputer.

LIST OF RESEARCH OUTPUT

- A. Muchlis, M.H. Khusyairi, F. Yuliawan, *Storage-Efficient Finite Field Basis Conversionvia Efficient Multiplication,* submitted to Proceeding International Symposium on Computational Sciences, Bali October 2009.

- I. Muchtadi-Alamsyah, M. W. Paryasto, M. H. Khusyairi, *Finite Field Basis Conversion*, Proceeding International Conference on Mathematics, Statistics and Its Applications, Bukittinggi, June 2009, pp 15-18.

- I. Muchtadi-Alamsyah, M. W. Paryasto, M. H. Khusyairi, *Finite Field Basis Conversion and Its Implementation*, submitted to Proceeding International Symposium on Computational Sciences, Bali, October 2009.

- 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.

- M.W. Paryasto, B. Rahardjo, I. Muchtadi-Alamsyah, M.H. Khusyairi, *Implementation of Polynomial Basis-Optimal Normal Basis I Basis Conversion,* submitted to Jurnal Ilmiah Teknik Komputer.