Proceedings of the 3rd International Seminar of Basic Sciences
©2017 FMIPA Pattimura University, Ambon, Indonesia
ISBN: 978-602-61644-0-7
pp. 1 – 4

Invited Talk

MARITIME CRYPTOLOGY

Intan Muchtadi Alamsyah

Algebra Research Group, Faculty of Mathematics and Natural Sciences
Institut Teknologi Bandung
Jl. Ganesha No. 10 Bandung 40132, Indonesia

Corresponding Author: ntan@math.itb.ac.id

EXTENDED ABSTRACT

Maritime has special needs for information security, including the protection of classified information. As written in "Cryptography's Role in Securing the Information Society": 'Cryptography provides important capabilities that can help deal with the vulnerabilities of electronic information. Cryptography can help to assure the integrity of data, to authenticate the identity of specific parties, to prevent individuals from plausibly denying that they have signed something, and to preserve the confidentiality of information that may have improperly come into the possession of unauthorized parties [Dam and Lin, 1996].

Elliptic Curve Cryptography (ECC) was first introduced by Neal Koblitz and Victor Miller ([Koblitz1987],[Miller1985]). They independently introduced the elliptic curve to design a public-key cryptography. Compared to other cryptography method, it has several advantages: its arithmetic operations are spesific and can not be predicted, it offers smaller key length for the same security level compared to other method and its operations have many layers and combinations. ECC relies on the security level of the discrete logarithm problem called Elliptic Curve Discrete Logarithm Problem (ECDLP) [Hankerson et al, 2004].

Previously we have conducted research related to problems of implementing elliptic curve cryptography based on composite fields [Paryasto et al, 2012] and the implementation of Elliptic Curve Integrated Encryption Scheme [Susantio and Muchtadi, 2016]. In addition, we also studied implementation of modified algorithm Pollard Rho which is basically attack on Elliptic Curve Cryptography [Muchtadi et al, 2013], [Muchtadi et al, 2014], [Muchtadi and Utomo, 2016]).

For seaport security there is a need of complex system integration on linking local security seaport subsystem into a uniform global system of security based on the wire and wireless telecommunication infrastructure at the seaport territory and water area, and also onboard ships attributed to the port. However, the majority of applications do not protect confidentiality or the integrity of the message in the communication.

In Elliptic Curve Cryptography, the curve 25519 is the elliptic curve that offers 128-bit security and is designed to be used in key agreement scheme elliptic curve Diffie-Hellman (ECDH). This curve is one of the fastest ECC curves and more resistant to weak random number generator. This curve has been implemented in the public domain software [Bernstein, 2006].

The curve is constructed so as to avoid a potential attack on implementation and avoid side-channel attacks and random number generator problem. In messaging application, Curve 25519 is used for key exchange and authentication [Frosch et al, 2014].

In this research we will be develop an efficient algorithm for elliptic curve cryptography using Curve 25519 which is implemented in the security of messaging. Especially new algorithms to streamline area and time of the curve (the operations of addition and point doubling). We will learn the working mechanism of messaging applications, and simulation of unknown-keyshare attack.

On the other hand, some cryptographic scheme would be insecure once quantum computing arrives [Shor1997]. Code-based cryptography, like the McEliece cryptosystem, is a candidate, as it can resist the attacks using Shor Algorithms. This cryptosystem needs a lot of background on Algebraic Coding Theory, and we have conducted many research in this area [Irwansyah et al 2016][Irwansyah et al 2016b][Irwansyah et al 2017a][Irwansyah et al 2017b]. In this research we will develop codes that possess efficient decoding algorithm to be used in code-based cryptography. We can also first get optimal codes then develop efficient decoding algorithms.

REFERENCES

[Bernstein, 2006] D.J.Bernstein, *Curve25519: New Diffie-Hellman Speed Records,* Public Key Cryptography- PKC 2006, Volume 3958 of the series Lecture Notes in Computer Science, 207-228.

[Dam and Lin, 1996] : K.W. Dam and H.S. Lin, *Cryptography's Role in Securing the Information Society*, National Academy Press 1996.

[Frosch et al, 2014] T.Frosch, C.Mainka, F.Bergsma, J.Schwenk, T. Holz, *How Secure is TextSecure?* Cryptology ePrint Archive Report 2014/904, 2014. Available https://eprint.iacr.org/2014/904

[Hankerson et al, 2004] D. Hankerson, A.J. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer 2004.

[Irwansyah et al 2016] Irwansyah, A. Barra, S.T. Dougherty, A. Muchlis, I.Muchtadi-Alamsyah, P. Sole, D. Suprijanto, O. Yemen, *Theta$_S$-cyclic codes over A_k*, International Journal of Computer Mathematics: Computer System Theory, Vol 1 Issue 1 (2016), 14-31 http://dx.doi.org/10.1080/23799927.2016.1146800

[Irwansyah et al 2016b] Irwansyah, I. Muchtadi-Alamsyah, A. Muchlis, A. Barra, D. Suprijanto, *Codes over Infinite Family of Rings, Equivalence and Invariant Ring,* AIP Conf Proceeding (2016) **1707**, 020009.

[Irwansyah et al 2017a] Irwansyah, I. Muchtadi-Alamsyah, A. Muchlis, A. Barra, D. Suprijanto, *Codes over Infinite Family of Algebras,* Journal of Algebra Combinatorics Discrete Structures and Applications, **vol 4** No. 2 (2017) 131-140

[Irwansyah et al 2017b] Irwansyah, Irwansyah, A. Barra, I. Muchtadi-Alamsyah, A. Muchlis, D. Suprijanto, *Skew-cyclic codes over B_k*, Journal of Applied Mathematics and Computing (2017) doi:10.1007/s12190-017-1095-2

[Koblitz1987] N. Koblitz, *Elliptic Curve Cryptosystem,* Mathematics of Computation **48** (1987) 203-209

[Miller1985] V.S.Miller, *Use of Elliptic Curves in Cryptography*, Advances in Cryptology CRYPTO 85, *LNCS* **218** (1985) 417-426.

[Muchtadi et al, 2013] I. Muchtadi-Alamsyah, T. Ardiansyah, S.S. Carita, *Pollard Rho Algorithm for Elliptic Curves over GF(2^n) with Negation Map, Frobenius Map and Normal Basis*, Far East Journal of Mathematical Sciences, Special Volume, Issue IV, (2013) 385-402.

[Muchtadi et al, 2014] I. Muchtadi-Alamsyah, T. Ardiansyah, S.S. Carita, *Pollard Rho Algorithm for Elliptic Curves over GF(2^n) with Negation and Frobenius Map,* Advanced Science Letters **20**(2014), 340-343.

[Muchtadi dan Utomo, 2016] I. Muchtadi-Alamsyah and T.A.Utomo, *Implementation of Pollard Rho over Binary Fields using Brent Cycle Detection Algorithm* accepted in Proceeding AMC 2016.

[Shor1997] P.Shor, *Polynomial time algorithm for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput **26**(5) (1997), 1484-1509.

[Susantio dan Muchtadi, 2016] D.R.Susantio and I.Muchtadi-Alamsyah, *Implementation of Elliptic Curve Cryptography in Binary Field*, Journal of Physics Conference Series **710**(2016) 012022.

[Paryasto et al, 2012] M.W.Paryasto, B. Rahardjo, I. Muchtadi-Alamsyah, F. Yuliawan, Kuspriyanto *Composite Field Multiplier Based on Look-up Table for Elliptic Curve Cryptography Implementation* ITB Journal of Information and Communication Technology Vol **6** no 1 (2012) 63-81.