On the Computational Cost of Cocks' Identity Based Encryption

Gabriel Moo Ka Lin[1,2*], Arif Mandangan[1,2] and Rozaimi Zakaria[1,2]

[1]*Faculty of Science and Natural Resources, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia.*

[2]*Mathematics – Graphics & Visualization Research Group (M-Gravs), Faculty of Science and Natural Resources, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia*

Identity Based Encryption is a public key cryptosystem where the user's identity becomes the public key. The first Identity Based Encryption scheme was constructed in 2001 based on elliptic curves and with pairings. Another variant of Identity Based Encryption which is without pairings was the Cocks' Identity Based Encryption. The security of Cocks' Identity Based Encryption lies on integer factorization problem and quadratic residuosity modulo composite N problem. Unfortunately, lack of efficiency becomes a major drawback of the Cocks' Identity Based Encryption. The algorithms in Cocks' Identity Based Encryption consists of four stages: Setup, Extract, Encrypt and Decrypt. Therefore, the aim of this paper is to investigate which algorithm in Cocks' Identity Based Encryption consumes high computational cost and subsequently contributes to its inefficiency. The experiments were conducted by comparing the computational time between Encrypt and Decrypt algorithms. Results from the study showed that decryption in Cocks' Identity Based Encryption has higher computational cost as compared to the encryption. A further improvement can be made on accelerating the decryption process without compromising the security.

Keywords: Identity Based Encryption, quadratic residue, non-pairings, computational cost, decryption, time efficiency

I. INTRODUCTION

Cryptography served to be one of the best application that can provides a secure channel for electronic communications across the Web. There are two types of cryptography which are classified as symmetric cryptosystem and asymmetric cryptosystem respectively. Symmetric cryptosystem uses the same key for both encryption and decryption processes. While the asymmetric cryptosystem uses a pair of keys: public key for encryption and private key for decryption. The asymmetric cryptosystem such as Rivest-Shamir-Adleman(RSA), ElGamal Elliptic Curve Cryptography(ECC) are notably important and widely used in many applications. Shamir (1984) proposed the idea of Identity Based Encryption (IBE) system which is another variant of asymmetric cryptosystem. However, Shamir failed to design a fully functional IBE system. The first IBE was then proposed by Boneh and Franklin (2001) where the security lies on bilinear mappings between groups.

*Corresponding author's e-mail: sgmkl@hotmail.com

In the same year, Cocks introduced another type of IBE which is without pairings. The security of Cocks' IBE lies on quadratic residue problem modulo RSA composite N. There are four algorithms in Cocks' IBE namely Setup, KeyGen, Encrypt and Decrypt. Setup and KeyGen can be carried out without affecting the size of original message or data. Hence, the computational time of first two algorithms will not be influenced by the size of data. However, Cocks' IBE performed encryption of data bit by bit. Thus, an increase in the size of data accompanied by a proportional increase to the time of encryption. Decryption then recover the ciphertexts bit by bit back into the original data. Under the same bit of data, it is not able to determine either encryption or decryption will have a higher computational cost. Therefore, the main objective of this paper is to investigate the algorithm that has higher computational cost in Cocks' IBE scheme.

II. LITERATURE REVIEW

Public key cryptosystem was introduced by Diffie and Hellman (1976) to resolve two major problems which were privacy and authentication. The main interest of public key cryptosystem was to deliver message securely over a channel between two parties and provides authentication to the message delivered by the sender. The public key cryptosystem has the property of one-way trapdoor and secured by using hard mathematical problems. Rivest, Shamir and Adleman (1978) had proposed an encryption method which is also known as the RSA, a public key cryptosystem. The encryption key is distributed to the sender while the decryption key kept by the intended recipient. the security part of RSA cryptosystem was developed based on the difficulty in factorizing two large prime numbers.

Later in 1984, Shamir introduced the idea of designing an asymmetric cryptosystem that does not require the exchange of private or public keys. His motivation was to simplify e-mail encryption. This cryptosystem was known as IBE where user's identity becomes the public key. Shamir was unable to design a functional IBE system. This problem remained as an open problem for many years. Instead, Shamir was only able to design Identity Based Signature(IBS) scheme based on RSA algorithm.

Researches were continued until Boneh and Franklin (2001) successfully designed the first functional IBE cryptosystem. Boneh-Franklin IBE was IBE with pairings due to the design on bilinear mappings between groups. It had chosen ciphertext security in random oracle model by the assumption of Bilinear Diffie-Hellman (BDH) problem. In 2004, Boneh and Boyen introduced an IBE scheme and proven its security without random oracle. The security based on decisional bilinear Diffie-Hellman assumption. Boneh and Boyen later designed two different IBE systems without random oracles that are secure against selective identity attacks.

Girish and Phaneendra (2014) had reviewed some basics of IBE and IBS. The paper also discussed on a few important IBE. Comparisons were made between public key encryption and IBE scheme. The advantages and disadvantages of IBE also mentioned in the paper.

Cocks (2001) was the first who introduced IBE scheme without pairings. There are four algorithms in Cocks' IBE scheme namely Setup, Extract, Encrypt and Decrypt respectively. Setup is the place where Cocks' IBE generates all the necessary public and private parameters. The private parameters are primes p,q where p,q≡3 modulo 4. While the public parameter, N is the product of p and q. Extract is the algorithm that determines the root, r by computing r=a^((φ(N)+4)/8) mod N. Next, the Encrypt is algorithm for encryption of original data which is done bit by bit. Each bit of the original data will yield a pair of ciphertext and to be sent to the recipient. Upon received the ciphertext, decryption will be performed. Recipient is the only one who knows which ciphertext to be decrypted in the pair and recover every bit in the message. Due to the encryption in Cocks' IBE system is done bit by bit, it produced a long ciphertext which leads into space inefficiency problem. Space inefficient problem was then solved by Boneh, Gentry and Hamburg (2007). Unfortunately, the encryption and decryption speed of their system were slower than in Cocks' IBE scheme.

III. MATERIALS AND METHODS

The machine used to run the experiments in this study was ASUS laptop of Intel® Core™ i5-3210M CPU @2.50GHz processor with 64-bit operating system in Windows 8. In addition, Maple 18 software was used to test execution time of encryption and decryption in this study. A simulation of the encryption and decryption time was made to test the execution time of both processes by using the same machine and software. First, the experiments started with Setup and Extract where all the required public and private parameters were set to go. Taking into consideration where different public and private parameters might give different results, the study also used the same message space starting with 2 bits, M=(1,0). Upon obtaining the results of encryption time and decryption time. The experiment continued by using same public and private parameters but with larger bits of 4,6,8 and 10 bits respectively. The results were then tabulated as in Table 1 and represented in Figure 1.

IV. RESULT AND DISCUSSION

The simulation in the experiments showed that there were increment in both encryption and decryption time as the size of data increases. The original 2 bits message space, S=(1,0) was used for obtaining the results of encryption time and decryption time. The message of higher bits obtained by duplicating the 2 bits into 4 bits, 6 bits and so on. Figure 1 showed that encryption time and decryption time in Cocks' IBE increasing proportional to the size of data. The lowest encryption time is 0.07s while the highest one is 0.1s. The lowest decryption time is 0.09s while the highest is 0.12s. Another significant trend that can be observed from the graph is that the decryption time in Cocks' IBE always higher than encryption time even for different sizes of data.

Table 1. Computational time for encryption and decryption in Cocks' IBE

Size of Data (bits)	Time (s)	
	Encryption	Decryption
2	0.07	0.09
4	0.09	0.10
6	0.09	0.10
8	0.09	0.10
10	0.10	0.12

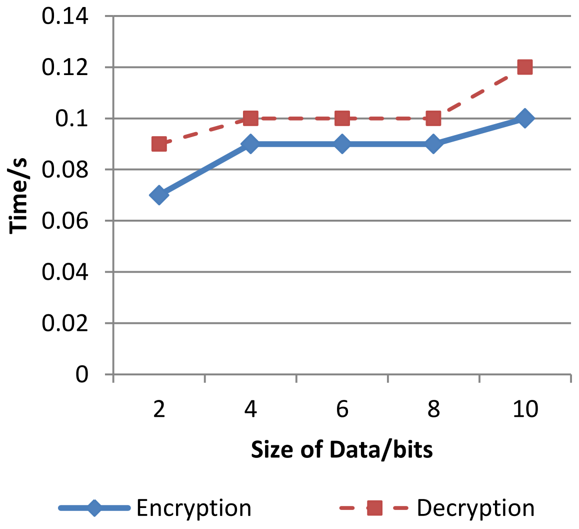

Figure 1. Graph of encryption time and decryption time in Cocks' IBE

V. CONCLUSION

In conclusion, this study showed that the time for encryption and decryption increases as the size of data increases. This is due to the property of encryption and decryption in Cocks' IBE are done bit by bit. Longer message will produce larger size of data resulting into longer time for encryption and decryption. Based on the results from experiments done in this study, the algorithm of Decrypt in Cocks' IBE has higher computational cost as compared to Encrypt under same bit of data. This is because encryption of every bit in the message will produce a pair of ciphertexts for decryption. A high computational cost in decryption would cause time inefficient problem in Cocks' IBE. A future study of this paper can be conducted by improving the time efficiency of Cocks' IBE without compromising the security part. The implementation of some variants in RSA cryptosystems such as Chinese Remainder Theorem or by data compression technique could be useful in accelerating the decryption in Cocks; IBE.

VI. ACKNOWLEDGEMENTS

The authors would like to express heartfelt thanks to Universiti Malaysia Sabah for providing financial support under UMSGreat Grant (GUG0132-1/2017).

[1] Boneh, D. & Boyen, X. (2004). Efficient selective-ID secure identity based encryption without random oracles. Advances in Cryptology-EUROCRYPT 2004, LNCS 3027, pp. 223-228.

[2] Boneh, D. & Boyen, X. (2004). Secure identity based encryption without random oracles. Advances in Cryptology-CRYPTO, LNCS 3152, Springer Berlin Heidelberg, Springer-Verlag, pp. 443-459.

[3] Boneh, D. & Franklin, M. (2001). Identity based encryption from Weil Pairing. Advances in Cryptology-Crypto, LNCS 2139, Springer-Verlag, pp.1-27.

[4] Boneh, D., Gentry, C. & Hamburg, M. (2007). Space-efficient Identity Based Encryption without pairings. Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science, pp. 647-657

[5] Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. Proceedings of the 8th IMA International Conference on Cryptography and Coding, pp. 360-363.

[5] Cohen, H. (1993). A course in computational algebraic number theory. Springer-Verlag, pp. 1-27.

[6] Diffie, W., Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654.

[7] Girish, Phaneendra, H.D. (2014). Identity based cryptography and comparison with traditional public key encryption: a survey. International Journal of Computer Science and Information Techinologies vol. 5, no. 4, pp. 5521-5525.

[8] Menezes, A.J., Oorschot, P.C.V., Vanstone, S.A. (1997). Handbook of applied cryptography. CRC Press, pp. 1-35, 63-74, 80-84, 87-113.

[9] Rivest, R.L., Shamir, A., Adleman, L. (1978). A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, vol. 21, no. 2, pp. 120-126.

[10] Shamir, A. (1984). Identity-based cryptosystems and signature schemes. Advances in Cryptology-CRYPTO, LNCS 196, Springer-Verlag, pp. 47-53.