International Conference on Computational Science and Information Management (ICoCSIM)
Vol. 1 (2012) 147-151

New Lightweight Identity Based Encryption Algorithm for Mobile Device: Preliminary Study

Norhidayah Muhammad[a], Jasni Mohd Zin[b], Md Yazid Mohd Saman[c]

[ab]*University Malaysia Pahang,26600,Pahang,Malaysia*
[c]*University Malaysia Terengganu, 21300,Terengganu,Malaysia*

Abstract

Recently the importance of mobile security coincides with the development of mobile computing. Mobile security has become the most important part of the mobile telecommunication, but mobile device has a limited processing capabilities, bandwidth is limited , high latency networks, storage capabilities are limited, lack of computing power to support strong encryption are constrained in using traditional encryption scheme such as RSA. Therefore for this study we try to create a new lightweight algorithm for mobile device, we want to implement identity based encryption with new feature, suitable for mobile device specification. Mobile information security should be enhanced to new scheme that more simple and use the small key size, also high security level. The main problem in traditional cryptosystem is a public key in determining validity, but this problem can be solved by identity based cryptography, where the public key can be obtained from users of public information known users. One method called elliptic curve will be implemented in IBE. Elliptic curve method has shorter key size, smaller signature length, fast operations and high security working. Thus, it is suitable for mobile devices, it uses 160 bits key and provides the same security as RSA 1024 bits key.Some benefits are expected from this study to improve the encryption algorithm for mobile security.

Keywords: Mobile security, identity based encryption, lightweight encryption algorithm;

1. Introduction

Mobile security has become crucial issue because consumers prefer mobile computing, 50.4% of U.S consumers used smart phones (Nielsen), it is used for business activities, communicate in social web, and sending confidential data to companies and individuals. Any third party that provides wireless data services (e.g., mobile banking) must have its own solution for end-to-end security [1]. Mobile security is very important to protecting information from unauthorized access, stole, disruption, inspection, modification or whatever manipulation of information, but mobile device also have several constrain like Limited processing capabilities, limited Bandwidth, High latency networks, limited Storage capabilities, Lack of computing power to support strong encryption [2]. Therefore, the security system on the mobile computing should be enhanced so that the process of data transmission and data storage more secure. There are many algorithm have done for mobile device like RSA, but for this study we try to implement the identity base encryption for mobile and improve better the algorithm. We choose identity based encryption because the special specification of identity based encryption.

Identity based encryption algorithm is used for information security. IBE different from traditional algorithms such as public key cryptography and private key cryptography, IBE was introduced in 1984 by Adi Shamir. Shamir [3] introduced identity-based (ID-based) cryptography where user public key can be obtained from public information that uniquely identifies the user. For example, a user's public key can only his / her e-mail address or phone number, and thus implicitly known to all other users. Since then, many IBE schemes have been proposed, e.g., [4-8]. The main advantage of the ID-based cryptosystem is a certificate is not required to bind a public key user name them. First complete ID-based encryption scheme was proposed by Boneh and Franklin in 2001 [9]. They use the bilinear map (pairing Weil) over elliptic curve encryption scheme to build / decryption.

Identity based encryption has long been studied and a lot of schemes have been taken out using this cryptosystem, Identity-Based Encryption system (IBE) consists of four algorithms [9]: Setup, Extract, Encrypt, Decrypt.

- The Setup algorithm generates public system parameters, and a secret master key.
- The Extract algorithm uses the master key to extract a private key corresponding to a given identity.
- The encryption algorithm encrypts messages for a given identity (using the system parameters).
- The decryption algorithm decrypts cipher text using the private key.

Some output from this research is expected and will become up with the new algorithm for identity based encryption algorithm used in mobile device, and that algorithm can fulfill all this criteria for good algorithm. Generally, a good cryptosystem scheme must satisfy a combination of four different goals [2,10], Authentication, Non repudiation, Data integrity,

Confidentiality.Otherwise this study will be focus on to create new lightweight for identity based encryption that can be efficiency, faster and suitable for power of mobile device. For research method, we use Elliptic curve method for identity based encryption algorithm. ECC use a160 bits key[11], but its provides the same security as RSA 1024 bits key, thus lower computer power is required. ECC not only allow major size reduction, but also able to perform ECC operations very quickly. In addition, the processing power can be reduced in the ECC, that why elliptic curve is suitable for identity based encryption for mobile device.

2. Research Aim

This research aims to establish a new algorithm using identity based cryptosystem for mobile security, which can extract the precise solution for mobile data security. This research embarks on the following objectives:

- To develop the new algorithm for identity based encryption in mobile device.
- To implement elliptic curve method in identity based encryption.
- To evaluate the new lightweight identity based encryption algorithm in mobile device.

3. Related Work and Encryption Techniques

For this section, we describe three types of encryption techniques, each of these methods, it has its own advantages and disadvantages, full details will be explained below.

a. Symmetric Key Encryption

Symmetric key encryption also known as private key cryptography, in symmetric key encryption, the same key is used to both encrypt and decrypt the data [12]. The key manager generates a new key for every message at the sender's request. The key is stored in a database along with the list of receivers. When the receiver authenticates, the key is retrieved from the database and the receiver name is matched against the list of authorized recipients.Symmetric key management systems have two significant drawbacks. For the first significant is high storage costs, but not all, symmetric key systems require that a database containing the key for every message is present in the system. While some proponents of symmetric key systems will insist that this database is not a significant impediment, this key database must be replicated, backed up, and generally managed. And the second significant is high availability needs, sender must request a key for each message from the key manager, the key manager is involved in every encryption operation. This means that the key manager must be highly available and the scale of the key manager will limit the scale of the entire messaging or data encryption system [13]. That why symmetric key not suitable for mobile device because mobile device less battery and CPU resources.

b. Public Key Encryption

In conventional public key encryption like Rivest-Shamir-Adleman algorithm (RSA), In public-key cryptosystem each user has a key pair (KU,KR) [14], where KU is the public key and KR is the private key. To generate the key pair, one first chooses a private key KR and applies some one-way function to KR to obtain a random and uncontrollable KU. The main concern in a public-key setting is the authenticity of the public key. For example here, the encryption key is stored on system provided by third party such as (online banking), and the decryption key is stored safely elsewhere at a trusted location like the CA. When the system is compromised, the adversary will only learn the encryption key and cannot decrypt the data. However, once the secret key is revealed, all encrypted data is vulnerable. This poses a problem when temporary access to the system data is needed.

c. Identity Based Encryption (IBE)

In 1984, Shamir [3] introduced the concept of identity-based (ID-based) cryptography and also presented an ID-based signature (IBS) scheme. In a IBS scheme, a public key can be derived from user's identity, e.g., his email address, and a corresponding secret key can be evaluated by a Private Key Generator (PKG).]. The corresponding private key can be generated separately later. For more detail we can look for example in BSN, how BSN implement IBE and how BSN using a string as a public key.

i. example

This example show how IBE used in Body Sensor Network BSN [12]. the patient may instruct the CA to release the keys to any ER doctor. Each day, the patient's BSN will create a new public key using the string str = *{*date | time | ER*}*. The CA

does not have to create the corresponding private key.When an ER doctor wants to obtain data for January 1st between 9 and 10 a.m., he will first authenticate himself to the CA. The CA will then create the decryption key using that same string str = {date | time |ER}. This key can only decrypt data collected on that date and time. Storing the syntax in the BSN is secure even if the sensors are compromised due to the asymmetric property of IBE. An adversary with access to a BSN sensor and knowledge of the syntax can only create a public key that cannot decrypt any information. Only the CA (or the patient himself) can create the private key to decrypt the data. Key management is also simplified, since the CA can generate a particular secret keybased on the syntax, for instance date and time, on demand.

ID-based cryptosystem transparently provides security enhancement to the mobile applications without requiring the users to memorize extra public keys. For example, sending an ID-based encrypted short message is exactly the same as sending a normal short message [15] if the mobile phone number of the short message recipient is used as the public key. Therefore, the mobile user (the sender) does not need to memorize the public key of the receiver. This feature is especially desirable for mobile applications such as bank or stock transactions. However, in the existing ID-based cryptosystem, the pairing computing has significant overhead [14]. Therefore, efficient algorithm for ID-based cryptosystem is essential in mobile devices with limited computing power.

d. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) [16] is an approach requiring a set of algorithms for key generation, encryption Key(K) and decryption for doing public-key cryptography. ECC is based on the mathematics of elliptic curves developed independently by [17]. ECC as all asymmetric cryptographic algorithms uses a key pair: one key which is public is used for encryption and other one is private key which is used for decryption process. The good point about this key pair is that one of these keys cannot be obtained from the other key which makes it useful for encryption and decryption process.

Elliptic curve systems have been fine tuned to have analogues of other systems, such as El-Gamal, Diffie-Hellman, and RSA[18]. There is not much gain in the difficulty of the integerfactorization problem in RSA over the field of elliptic curves, as contrasted with the discretelogarithm problem in elliptic curves which is much harder than in El-Gamal, and Diffie-Hellman systems. Hence elliptic curves in cryptography usage are based on the hardness ofthe discrete logarithm problem.

4. Discussion

Identity based encryption has been used in a variety of security purposes, a different method to produce a better algorithm and quality, several methods have been used in identity based encryption in previous studies, especially in the more simple algorithm, and the higher safety. That why we want to apply this algorithm for mobile device with new enhancement for the new algorithm, table below shows the study in identity based encryption that uses a different method.

Table 1. Table show the different method used in identity based encryption.

Title	Descriptions	Method
A New Identity Based Encryption (Ibe) Scheme Using Extended Chebyshev Polynomial Over Finite Fields	this paper present a method to extract key pairs needed for the identity based encryption (ibe) its proposed scheme relies on the hard problem and the bilinear property of the extended chebyshev polynomial over z p.	Chebyshev Polynomial Over Z P
Ibe-Lite: A Lightweight Identity-Based Cryptography For Body Sensor Networks	(bsn) for health care monitoring. the protocols based on ibe-lite that balance security and privacy with accessibility and perform evaluation using experiments conducted on commercially available sensors.	Elliptic Curve
Lightweight Identity-Based Broadcast Encryption Over Wireless Ad Hoc Networks	due to wireless ad hoc networks' properties of low bandwidth, high delay, high loss rate, and mobility. This paper describes a ibe broadcast encryption scheme including traitor tracing function, which achieves constant size cipher texts, constant size private keys, and constant size public key.	Bilinear Map
New Construction Of Fuzzy Identity-Based Encryption	in this paper the concept of fuzzy identity-based encryption schemes with dynamic threshold (dt-fibe) , collusion attacks in the fuzzy selective-id attack model. Under a new complexity assumption: k-bdh assumption, a comprehensive secure proof is given.	Fuzzy
Pseudo-identity based encryption and its application in mobile ad hoc networks	provide an elegant solution to these two problems using our proposed algorithm called pseudo-identity based encryption to dedicated routers, routing function is accomplished through multiple peer-peer connections.	RSA

Table 1 shows the different methods implemented in the identity-based encryption, researchers are trying to create an algorithm which is better than the previous algorithm, and recently have many reforms achieved in identity based encryption algorithm, many shortcomings in tackling such problems public key and private key, also in determining the validity of identity.

Table 2. Table show the new algorithm for identity based encryption

Title	Description	Algorithm
Pseudo-identity based encryption and its application in mobile ad hoc networks	provide an elegant solution to these two problems using our proposed algorithm called pseudo-identity based encryption to dedicated routers, routing function is accomplished through multiple peer-peer connections.	Pseudo
Ibe-Lite: A Lightweight Identity-Based Cryptography For Body Sensor Networks	(bsn) for health care monitoring. the protocols based on ibe-lite that balance security and privacy with accessibility and perform evaluation using experiments conducted on commercially available sensors.	Ibe-Lite
Lightweight Identity-Based Broadcast Encryption over Wireless Ad Hoc Networks	This paper describes a lightweight identity-based broadcast encryption scheme including traitor tracing function, which achieves constant size cipher texts, constant size key. When adding new users, system doesn't have to change previous setups.	IBBE

Table 2 show several new algorithm for identity based encryption, researcher used different method to achieve their specific goal, but for this study we try to create an algorithm that implements identity based encryption for mobile devices in android operating system. Algorithm conducted by others mainly focus on fixed nodes (such as a PC), that algorithm is not suitable to be used on mobile devices Because Of less battery and CPU resources.

5. Conclusion

The outcome from this study is to perform a study on the lightweight of algorithm for mobile device and for the output from this research study, we want to create a new lightweight algorithm for mobile device. To implement this framework, a middleware will be developed to encrypt the plaintext to chipper text, and to decrypt the chipper text to plaintext using identity based encryption approach that uses a string as a public key. We believe that this study will give a good impact in adaptation of Identity Based Encryption algorithm in the other way.

References

1. Y.-B. Lin, M.-F. Chen, and H. C.-H. Rao, “Potential Fraudulent Usage inMobile Telecommunications Networks,” *IEEE Trans. Mobile Computing*,vol. 1, no. 2, 2002, pp. 123-131.
2. Malhotra, K., S. Gardner, and R. Patz. *Implementation of Elliptic-Curve Cryptography on Mobile Healthcare Devices*. in *Networking, Sensing and Control, 2007 IEEE International Conference on*. 2007.
3. A. Shamir, “Identity-based cryptosystems and signature schemes,” *Advancesin Cryptology-CRYPTO’84*, pp. 47-53.
4. P. Barreto, B. Libert, N. McCullagh, and J.Quisquater, \Effiencient and provably-secure identity-based signatures and signcryption from bilinear maps," *Asiacrypt 2005*, LNCS 3788, Springer-Verlag,pp.515{532, 2005.
5. F. Hess, \efficient identity based signature schemes based on pairings," *Selected Areas in Cryptography (SAC 2002)*, LNCS 2595, Springer-Verlag, pp.310 {324, 2003.
6. X. Huang, W. Susilo, Y. Mu, and F. Zhang, \Short designated verifier signature scheme and its identity-based variant," *International Journal of Network Security*, vol. 6, no. 1, pp.82{93, 2008.
7. K. Paterson, and J. Schuldt, “Efficient Identity-based Signatures Secure in the Standard Model," *The 11th Australasian Conference on Information Security and Privacy (ACISP 2006)*, LNCS 4058,Springer-Verlag, pp. 207{222, 2006.
8. H. Xiong, Z. Qin, and F. Li, \Identity-based Thresh-old Signature Secure in the Standard Model," *Inter-national Journal of Network Security*, vol. 10, no. 1,pp.75{80, 2010.
9. D. Boneh and M. Franklin, “Identity-based encryption from the Weilpairing,” *Advances in Cryptology-CRYPTO’01*, pp. 213-239.
   A. Furht, M. Ilyas, "*Wireless Internet Handbook Technologies, Standards, and Applications*", CRC Press, 2003.
10. N. Koblitz, “Elliptic curve cryptosystems,” *Math. Comput.*, vol. 48,pp. 203–209, 1987.
11. Tan, C. C., W. Haodong, et al. (2009). "*IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks*." Information Technology in Biomedicine, IEEE Transactions on
12. Arastradero Drive, Palo Alto, CA 94304 USA,The Identity-Based Encryption Advantage,Voltage Security, Inc,w w w. v o l t a g e . c o m.

13. Hwu, J. S., R. J. Chen, et al. (2006). "*An efficient identity-based cryptosystem for end-to-end mobile security*." Wireless Communications, IEEE Transactions on**5**(9): 2586-2593.
14. H.-N. Hung *et al.*, "A Statistic Approach for Deriving the Short MessageTransmission Delay Distributions," *IEEE Trans. Wireless Commun.*, vol.3, no. 6, 2004.
15. Enge Andreas, "Elliptic Curves and Their Applications to Cryptography: An Introduction", Kluwer Academic Publishers, 1999.
16. V.Miller, Uses of ellipticcurves in cryptography Advancesin-Cryptology CRYPTO '85, Lecture Notes in Computer Science,springer-verlag.218.(1986)pp.417-426
17. Raja Ghosal, Peter H. Cole. Elliptic Curve Cryptography. The University of Adelaide.
18. Benasser Algehawi, M. and A. Samsudin (2010). "*A new Identity Based Encryption (IBE) scheme using extended Chebyshev polynomial over finite fields*." Physics Letters A**374**(46): 4670-4674.
19. Chun, Y., G. Hongyang, and Z. Wenshuo. *Lightweight Identity-Based Broadcast Encryption over Wireless Ad Hoc Networks*. in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*. 2011.
20. Veeraraghavan, P. (2011). *Pseudo-identity based encryption and its application in mobile ad hoc networks. Communications (MICC),* 2011 IEEE 10th Malaysia International Conference on.