ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Identity Based Encryption Using Semi - Functional Keys

[I]Yamini.E.J, [II]Ram Lal
[I]Assistant Professor in IT Dept., BIT, Tamilnadu and Faculty Research Fellow in IITD
[II]Computer Services Center, IIT Delhi, Hauz Khas, New Delhi

Abstract
Due to improper system usage and handling of data through untrustworthy systems, we are facing several problems. There is need to safeguard confidential data through specific techniques. In this paper, we propose a semi functional encryption along with identity based encryption. Here the extra keys called semi functional keys are generated by the functional key generator (FKG) which overcomes the problem of compromisation of master key generator in the previous paper and provide additional security. To simplify the certificate management in network we are opting for Identity Based Encryption (IBE), where the users get authorized by their own IDs. The original key generation can be done only with the functional keys. Also an extra level security is provided by discarding the generated functional keys after the keys were sent to the master key generator. Here even with the secret keys, no one can generate the accurate keys, which made the system more secured compared to the previous ones.

Keywords
UID-User Identity, IBE-Identity Based Encryption, MKG-Master Key Generator, SKG-Secret Key Generator, FSK-Functional Key Generator.

Introduction

Identity based cryptography is based on the identity of the user like unique identity number, email-id, ip-address, mobile number, digital signatures, passwords, pin numbers etc. These systems authenticate and allow the users based on their identity. It is more convenient and easy to generate keys based on their own identity for millions of users. It simplifies the key generation and certificate management process in the traditional method.

Several authors discussed about the identity based encryption in different ways [6-14], such as how the system actually works, its implementation, enhancing methods, speed optimizing techniques and handled various problems occurred in the IDE. Identity Based encryption is an important concept in cryptography, since it provides a unique technique of securing the data by using user information itself. Also the functional encryption is one of the best ways of securing the information by generating the secret keys for each function happening in the system [22-24, 26]. The main advantage of functional encryption is that there is no need to generate a public key earlier.

The underlying advantageous concepts of functional encryption process are:

- The master public key is provided to all the authenticated users for crypting.
- Separate functional key will be provided during the process.
- Once a user is authenticated using their personal ID(unique ID, name, mobile number, digital signature, password etc) they can crypt with same master key for a particular time limit.
- Generate functional keys for each process which made the system more secured.

The problem in the previous paper is that if the MKG got compromised, all the keys can be taken by the attacker. It will lead to the complete collapse of the system. If the attacker got the master key once, he can get any user data and can pretend to be a sender for any user. So it is mandatory to secure the MKG or we have to provide an extra level of security to the system so that even though the MGK is attacked the hacker, he could not get the complete key details.

To avoid this problem, some authors suggested that changing the master key at regular interval of time is necessary. But that alone is not enough. So here i proposed an additional layer of functional encryption with semi functional keys.

Literature Review

The identity based cryptosystem was introduced in order to avoid the complications in generating the public keys, since it is complex to select random prime numbers for millions of users at the same time without redundancy. The identity based cryptosystem is rely on the user identity. The details of both identity based encryption and functional encryption is discussed here.

The signature based encryption schemes are introduced for the purpose making messages private and signed. Since signed messages are the proof that it is originated from the user[1]. Key distribution is the common problem happening everywhere. But it can be easily solved if we choose the right set of numbers. In the paper Rivest, Shamir and Adelman discussed how to avoid the reblocking in signature based encryption by choosing an threshold key.

Based on this value we have to choose the public key values for both ciphering and signature verification.

Collision is the major problem occurring in all kind of transmission in network. In 2002, a collusion attack free identity based system was proposed with the underlying concept of elgammal by Diffie Hellman. A trusted key generation center and a non-interactive key sharing scheme is introduced in it. Here if A and B are the users, A calculates B's public key using B's unique ID information and common public information to both.

Also A calculates the common key using A's secret information with the help of B [2]. Even though it reduces collusion up to some extent, it is a complex process with take time.

In [3] the key agreement scheme is discussed by the author, which is forward secured. A trusted key generating center provides secret key to the users at same time. With the methodology, the process is secured from active and passive attacks. But if the TC is compromised anyone can easily get the keys. So it is not fully secured.

The key distribution center plays a vital role in all the cryptographic systems. The major function of KDC is

- Maintain database of user details such as IDs, username, passwords etc.
- Distribute and maintain secret key details.

- Update database with the newly generated keys.

In some papers the authentication for identity based digital signature is done by analyzing the matching two generated values with the help of bilinear properties,[5] where the public key is generated from user's ID and private key is generated by trusted authority.

In 2003, the mediated RSA scheme for identity based cryptography is introduced. Here all users do not have their own private keys [6]. Instead the keys are used in efficient manner redundantly. It is an enhancement of RSA algorithm with extra features like collision and division resistance.

In 2004, a faster ID based encryption is introduced to speed up pairing calculation [7]. Here the super singular curve concept of Boneh and Franklin is optimized and improved the process speed by nearly 50%. This is done by eliminating the denominator. Initially R=Rs+Rt, later Rs= tr(R)/2 and Rt = R- Rs. Then by Tate pairing, the denominator elimination is done. But there is no assurance given that it will work in all random curve points.

E-mails can also be secured by using the IBE. Authentication is done by a KGC which creates a constant domain parameter [8] for all the users based on their identity name, mail id, system date and time etc. So once a user get authentication, he can send emails to peoples in the same domain for one day. No need of authentication every time. It is time saving and reduced the load of key generator, But one day time period should be reduced for domain authentication since sometimes the same system is used by multiple users in common places like offices, institutions etc.

An identity based cryptosystem for end to end mobile security was well noticed in the year 2006, in which the issue of public key setting is the authenticity of public key. It is resolved by the identity based cryptography where the public key of the user is derived from the unique public information of the user [9].

Trapdoor permutations in IBE are always been difficult. Black box construction method with IBE creates multiple public key identities then compress it all, which cannot represent many keys with short string[10]. So the authors suggested functional encryption. If x is the original message and a user applies SKf (secret functional key) to a ciphertext. He will learn the value of f(x) and nothing more [10].So the problem will be partially solved.

In 2008, the concept of ID based encryption with efficient revocation is proposed. It is necessary to maintain time limits for the generated keys not only for the receiver also to the sender. The private key should be regularly get updated through some trusted third party. But as the number of users increases, it is complex to update the keys [13]. So a revocation algorithm is established to make sure that the keys are used effectively.

The concept of distributed hierarchical key management is followed for updating the key using a best, energetic and secured parent or sibling node. In multi receiver ID based encryption, individual ciphertext generation is done for the receiver i.e.) all members of a group will receive the message but only the receiver can decrypt it. Later an improved efficiency encryption scheme is introduced for managing the session key using a key management scheme to avoid attacks.

Even though Identity based encryption has been made secured through various techniques and methodologies, many issues are still arising which make the system unsecure. When functional encryption

Methodology

In this system, we have a master key generator which constitutes of a secret key generator and a functional key generator. Also this system has a trusted third party, which shares all the keys between users i.e.) both sender and receiver.Here initially the user gives their identity details to the secret key generator to get authentication.

The SKG verifies the details provided by the user and authenticate it by generating a key based on the given UID. The same user can use the same keys when he wants to send data again. Once the user gets authenticated, he has to describe what kind of function he is going to perform to the FKG. FSK receive the details and generates the semi functional keys fk1 and fk2 at a regular interval of time for security reasons. Here to avoid middle attacks, the functional keys are sent one after the other.

Now the MKG having both UID and functional keys generate a secret key which is send to the user. After sending the secret key to the sender and arbitrary user, the FKG automatically discard the keys from the database. So even the MSK get compromised, no one can generate the appropriate keys without having the functional keys. It is the major advantage of this system.

Key Generation Algorithm IBE-FE

A. Secret Key Generation

1. Generate 2 random primes numbers: p, q within limit k.

   Let k be the security parameter.

2. Calculate $p^1=2p+1$, $q^1=2q+1$.

2a. Check whether p^1 ,q^1 prime.
2b. If p^1 and q^1 are non- prime numbers, return (Error).
2c. Reselect p,q randomly .

B. Functional Key Generation:

For individual user functions

3. f(x) ← function of particular user.
4. Generate semi functional keys through FKG.
   - 4a. Generate f1 key randomly.
   - 4b. After t(x) time , generate f2 randomly.
5. Compute f1,f2 ← FKG(f(x)).
6. Calculate f ← f1⊕ f2 , f ← semi prime number. (using $X_{n+1} \leftarrow X^2_n \bmod M$)
7. Calculate $f^1 \leftarrow 2f+1$.

C. Master Key Generation

8. Calculate M ← pq,

9. Calculate $n \leftarrow p^1 . q^1 . f^1 \in k$.

10. Calculate $\phi(n) \leftarrow ((p^1-1). (q^1-1). (f^1-1))$

11. Choose e randomly within limit $\phi(n)$, e $\in Z\ \phi(n)$.

12. Calculate d , ed mod $\phi(n) \leftarrow 1$.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Encryption Algorithm IBE-FE

1. Retrieve n,e and om original message.
2. crypt(e,d,n,m) , cm ← ciphertext, om ← plaintext
3. Encrypt input message m with master key.
4. cm ← om^e mod n.

Decryption Algorithm IBE-FE

1. User: A send cm to receiver.
2. TTP : Send master key to B.
3. Decrypt cipher message cm with master key.
4. cm^d mod n ← om.
6. User : If succeed, return (m)

User encrypts the message using those keys with the help of F-RSA algorithm. Same time a part of the secret key is send to the arbitrary user and it send the keys to receiver of the message.
Now as usual the encrypted message is sent to another user through a secured mode, which is decrypted using the keys later. If the same user wishes to do another function, the system will use the same UID keys but generate a new set of functional keys based on the current function that the user is going to perform.

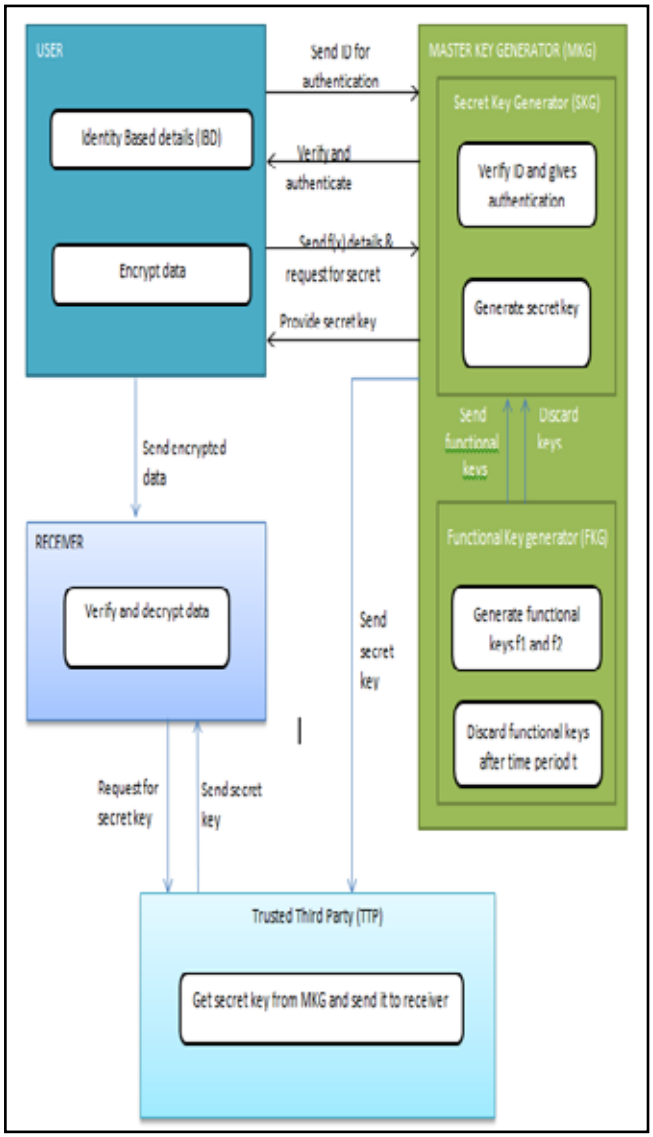

Fig. 1: Process flow of semi functional key encryption

Result And Discussion

The proposed scheme is completely secured one compared to the simple identity based system that was previously proposed. Here it is not possible to make compromisation on both the FKG and SKG at the same time. So the attacker cannot get the original key at any cost. So this scheme is the better secured one.
Our results confirmed that the proposed system is much efficient than the previous one, because of the two main features called semi functional key generation with automatic key discard and also the way we generate our secret keys.

- **Provides extra level security:**
  The generation of semi functional keys is an added advantage to the system. It made the crypt process difficult to crack. Thus it provides additional protection to the system.
- **Resistance to attacks:**
  The functional keys are sent to the SKG one by one to avoid the man-in middle attack. Also the keys will be discarded after the generating of master key. It won't get stored in any database.
- **Secured, even one key generator is compromised:**
  In the previous system, there is only one key generator. If it is compromised the entire system will be leaked. But here, even if one KG got compromised, the original keys cannot be retrieved.
- **User convenience:**
  Once the user enrolled and get authenticated from the MSK using their own identity, they will be allowed to use the system for particular amount of time. So no need to get authentication repeatedly to send messages continuously.

The semi functional key generation concept added an extra layer of security. The automatic generation of key in a random manner with a sequence will improve the performance of the system to a greater extent. Alsothe changes we made in random key generation improve the security level of the system to the next level.

Conclusion

The semi functional encryption scheme improved the security level of the identity based system. Since we arediscardingthe functional keys after the generation of master key, the attackers cannot get the whole key by compromising the SKG. Also the functional encryption acts as the extra layer of security. It makes the crypt process complex. So it is not easy to decrypt without original keys.
Thus the proposed concept is more secured methodology based on identity based encryption schemes. In future, some changes can be made in the crypting technique in order to make the system more secured and faster.

References

[1] *R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"*
[2] *Hatsukazu TANAKA, "Collusion Attack Free Identity-Based Cryptosystems", ISIT 2002, Lausanne, Switzerland, June 30 -July 5,2002.*
[3] *Xun Yi, Chik How Tan, Chee Kheong Siew and Mahbubur Rahman Syed, "ID-Based Key Agreement For Multimedia Encryption", IEEE Transactions on Consumer Electronics, Vol. 48, No. 2, MAY 2002.*
[4] *Ian Downnard, "Public-key cryptography extensions into Kerberos" IEEE, 2002.*

[5] K.G. Paterson, "ID-based signatures from pairings on elliptic curves", Electronics letter, 29th August 2002 Vol.38 No. 18 1025.
[6] Xuhua Ding and Gene Tsudik, "Simple Identity-Based Cryptography with Mediated RSA", Springer-Verlag Berlin Heidelberg 2003.
[7] M. Scott, "Faster identity based encryption", Electronics Letters, Vol. 40 No. 14, 8th July 2004.
[8] Noel McCullagh, "Securing E-Mail with Identity-Based Encryption" IEEE Computer Society, May-June 2005.
[9] Jing-Shyang Hwu, Rong-Jaye Chen, and Yi-Bing Lin, "An Efficient Identity-based Cryptosystem for End-to-end Mobile Security", IEEE transactions on wireless communications, vol. 5, no. 9, September 2006.
[10] Dan Boneh, Periklis A. Papakonstantinou, Charles Rackoff, Yevgeniy Vahlis, Brent Waters, "On The Impossibility of Basing Identity Based Encryption on Trapdoor Permutations", IEEE 2006.
[11] Geng Yang, Jiangtao Wang, Hongbing Cheng ,Chunming Rong, "An Identity-Based Encryption Scheme for Broadcasting", IFIP International Conference on Network and Parallel Computing, 2007.
[12] Shanqing Guo, Chunhua Zhang, "Identity-based Broadcast Encryption Scheme with Untrusted PKG", IEEE Computer Society, 2008.
[13] Alexandra Boldyreva,Vipul Goyal, Virendra Kumar, "Identity-based Encryption with Efficient Revocation", 14th ACM Conference on Computer and Communications Security, CCS 2008, ACM Press, 2008.
[14] Minghui Zheng, Huihua Zhou, Guohua Cui1, "An Improved Identity-Based Encryption Scheme without Bilinear Map", International Conference on Multimedia Information Networking and Security,2009.
[15] F. Richard Yu, Helen Tang, Peter C. Mason, and Fei Wang, "A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks", IEEE Transactions on Network and Service Management, Vol. 7, No. 4, December 2010.
[16] Christian Schridde, Tim Dornemann, Ernst Juhnke, Bernd Freisleben, Matthew Smith, "An Identity-Based Security Infrastructure for Cloud Environments", IEEE, 2010.
[17] Chun-I Fan, Ling-Ying Huang, and Pei-Hsiu Ho, "Anonymous Multi Receiver Identity-Based Encryption" , IEEE Transactions on Computers, Vol. 59, No. 9, September 2010.
[18] Rohit Ranchal, Bharat Bhargava, Lotfi Ben Othmane, Leszek Lilien, "Protection of Identity Information in Cloud Computing without Trusted Third Party", 29th IEEE International Symposium on Reliable Distributed Systems, 2010.
[19] Xu Chi , Zhang Wenfang, "Improved Efficient Identity-based Encryption Scheme", International Conference on Computer Science and Service System, 2012.
[20] Darpan Anand, Vineeta Khemchandani, Rajendra K. Sharma "Identity-Based Cryptography Techniques and Applications (A Review)",5th International Conference on Computational Intelligence and Communication Networks,2013.
[21] Huiyan Chen, Dongmei Chen, Yan Shuo Zhang, "Efficient Identity-based Encryption from Lattice" International Conference on Information Science and Cloud Computing Companion,2013.
[22] Yusuke Niwa, Akira Kanaoka, and Eiji Okamoto, "Construction of a Multi-Domain Functional Encryption System on Functional Information Infrastructure", 6th International Conference on Network-Based Information Systems,2013.
[23] Katsuyuki Takashima, "Recent Topics on Practical Functional Encryption", Second International Symposium on Computing and Networking, 2014.
[24] Chen Yang, Lin You, "Multi-Input Functional Encryption based Electronic Voting Scheme", Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing,2014.
[25] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing" IEEE Transactions on Computers, Vol. 64, No. 2, February 2015.
[26] Wang Jing, Huang Chuanhe, Yang Kan, Wang Jinhai, Wang Xiaomao, Chen Xi, "MAVP-FE: Multi-Authority Vector Policy Functional Encryption with Efficient Encryption and Decryption" China Communication, 2015.

Author's Profile

Ms. E.J.Yamini, Assistant Professor, Department of Information Technology, Bannari Amman Institute of Technology. Her research interests include Cryptography, Routing Network Security and Management.

Dr. Ram Lal is an academic staff in Computer Services Centre at I.I.T Delhi since 1988. He has more than 25 years experience in System Operations,User consultancy, Programming languages, Sun-System Administration.His areas of research interests are e-governance applications using Digital Image Processing, Fuzzy Logic and Cryptography.