Research on the IBE Encryption Scheme and It's Existing Problems

Bai Qinghai[1, 2], Zheng Ying[3], Zhao Linna[1], Chun hua[1], Chen jing[1]

[1]College of Computer Science and Technology, Inner Mongolia University for Nationalities, Tongliao, 028043, China

[2]Institute of Computer Application Technologies, Inner Mongolia University for Nationalities, Tongliao, 028043, China

[3]Journal Editorial Department, Inner Mongolia University for Nationalities, Tongliao, 028043, China

Email:baiqh68@163.com

Keywords: IBE, Problems; Efficiency of algorithm; Optimization

Abstract. This paper introduces the concept of identity-based encryption IBE and the algorithm, briefly explains the mathematical principles of algorithm, discusses the constraints set of algorithm parameters, choice of algorithm, etc. In terms of efficiency and security issue, key escrow, and key update, this paper analyzes the problems of IBE scheme, and proposes some solutions, in the hope of offering useful references for IBE system properly applying to actual environment.

1. Introduction

In the 80s of last century, the Israeli cryptographer SHAMIR [1] proposed the concept of identifier- based encryption. In 2001, two American cryptographers designed the first practical identifier-based cryptography system and its security was proven [2, 3]. This system used the bilinear pairing of elliptic curve to realize the encryption and decryption algorithm [4]. Currently, this algorithm has already been adopted by all IT companies interested in IBE. For instance, HP uses this algorithm for the encryption chip of its IBE system.

There is a key generation center in the identifier-based key system. The key center firstly generates the public system parameter or a master key (only known by the key center). This process is known as the system initialization. An entity sends identity authentication signal to the key center. After the successful identity authentication, the key center generates a private key corresponding to the entity identity (this private key is only known by this entity). This process is called the key extract process. The sender can use the receiver ID and system parameter for encryption. The receiver uses the system parameter and personal private key for decryption.

The identity-based cryptography needs no PKI [5]. It directly takes user's identity as a user's public key, getting rid of the dependence on PKI, which is the latest development in the field of international cryptography [6, 7].

2. The problems in IBE system

Because of the use of IBE system, unlike the CA center of PKI system, the private key generator PKG does not save numerous users' public keys and certificates. When the user encrypts the message by public key, it does not need to go through the complex certificate authentication. IBE system gets rid of the defects of PKI. However, there are still some problems in the application.

2.1 Efficiency and security issue

In IBE system, PKG is responsible for generating all users' private keys. The centralized design brings the bottleneck effect of both efficiency and security.

Firstly, when the system holds too large number of users, the PKG burden is way too heavy. In order to alleviate the burden of the root PKG, Gentry and Silverberg proposed the hierarchical identity-based encryption (HIBE). Its security was based on the bilinear Diffie-Hellman assumption of the random oracle model. Afterwards, Boneh and Boyen put forward an efficient HIBE that proved security without the random oracle model. In the two models, the length of a cipher-text, the length of a private key, and the encryption and decryption time increases linearly with the depth of encryption. HIBE is a natural development of IBE system, similar to the layered structure of the CA system, distributing the PKG generation of private keys to different nodes. This paper tries to solve the overloading issue of PKG by distributing the PKG work.

Secondly, because the PKG administrator can get access to any user's private key, a dishonest PKG may fake user's cipher-text and signature, posing a significant threat for security. The excessive concentration of power has always been a tough problem of PKG. Although the layered control has partially solved the problem, a satisfying solution does not show yet. It has already become one of the main obstacles to applying identity-based cryptography to applications.

2.1.1 HIBE scheme

In HIBE [8], the multiple PKG organized hierarchically will greatly reduce the workload of the root PKG, and make the multi-layer key escrow feasible. For example, if the user is an employee of a company, naturally the company is responsible for generating the private key of an employee. So, the user does not have to apply for private key generation service from the top PKG. More precisely, in a two-layer HIBE, there are three kinds of entities. The root PKG has a master key. The next layer is a domain PKG, which gets the domain key from the root PKG. The last is the user who applies for the private key from the domain PKG. Each user and domain PKG has a primitive identity (PID), may be one any string. A user's public key is the combination of the user's ID and the domain PKG's ID. In this system, the sender can get the user's public key offline. By introducing more layers, we can achieve the multiple-layer identity-based encryption system.

Similar to the IBE system, HIBE contains four algorithms: Setup, KeyGen, Encrypt, and Decrypt. In HIBE, the identity is a vector. A k-dimensional vector represents an identity in k-depth. Setup algorithm generates a series of system parameters, denoted as params, and a master-key. The master key is also taken as a private key in 0-depth. IBE system is a HIBE system with identities in 1-depth. For the algorithm KeyGen, input the k-depth identity ID=(I1, …, Ik) and the private key dID|k-1 of (k-1)-depth father identity ID|k-1 = (I1, . . . , Ik-1), and output the private key dID of ID. The encrypt algorithm uses params to encrypt the plaintext for an ID. The decrypt algorithm uses the private key to decrypt the cipher-text. The security of cipher-text in the HIBE system is based on the ID attack, in which attackers can choose to attack the public key.

2.1.2 The solution

The existing HIBE system needs to further improve the availability. The key is to design a HIBE algorithm, by which the expenses for decryption disconnect with the depth of layers, reduce the space complexity of cipher-text, and make it have nothing to do with the depth of layer. To reduce the space complexity of private key without increasing the encryption space complexity is also one of the main research subjects. The current HIBE schemes are based on the bilinear mapping. The Weil Pairing on elliptic curve is the most favorite one. D. Boneh and M. Franklin firstly proposed the identity-based encryption for Weil Pairing, improving the preview scheme. Use the threshold technology and save the master key in a distributed way. Its security is provable in the random oracle model. The biggest advantage of this program is the security and practicality. It is the first practical identity-based cryptography. Currently, the bilinear cryptosystem design has caused widespread concerns in the domestic and foreign scholars. This paper studies the new linear mapping and tries to seek for the new mapping that satisfies the practical needs for efficiency and be more secure and capable of resist allied attacks. Based on the new mapping, constitute the new IBE and HIBE mapping programs, and use the random oracle model to analyze its security issue.

The identity-based signature scheme is also a hot topic. Because the PKG knows the private key of each member, thus a dishonest PKG can forge the signature of any member. This paper discusses the solutions for the problems caused by reducing the key escrow. Besides, the identity-based group signature also faces many problems. For the group signature scheme, the public key should reflect the real identity. Otherwise, the group signature cannot be anonymous. This is a contradiction between the identity-based system and the group signature. How to achieve the confidentiality of private key of HIBE is the key for the solution.

2.2 The private key escrow and private key update

The private escrow and private key update are the two urgent issues for IBE system.

Private escrow means to the concentrated generation and management of users' private keys and symmetric keys. As already mentioned above, PKG can provide services for multiple users, like CA. For different users, the PKG assigned private key is relevant to the user's ID, namely sQ_{ID} . In other words, PKG knows the private keys of all users. Therefore, PKG must protect the master key s, just as CA protecting its private key, though it is usually very risky.

Also, if the user's private key is accidentally leaked, it needs to update the original public-private key pair and abolish the last private key. The PKI system informs the user about the updates by releasing the certificates revocation list CRL or using the online certificates status protocol OCSP. Then, rebind the new public-private key and the user's certificate [9]. The IBE system does not use the certificate as the carrier of public key and user's identity, so that the above-described method cannot be directly used for IBE.

The current IBE research and development does not result in any practical system. Most systems and programs are still at the experimental research stage, without any quantitative standards for various quality indicators. The possible deployed applications for the IBE system do not provide a relatively universal and scalable interface. The scalable interface designed in this paper is capable of connecting with the existing system. Without changing the original system structure and hardware facilities, the scalable interface ensures the system's abilities of confidentiality, authentication, and authorization. These abilities include:

(1) Optimize the design of IBE system

The server application PKG of IBE system is mostly the multiprocessor system structure. Considering the characteristics of such system structure, we should study the parallel processing of IBE system server programs, in order to optimize the system and improve the system efficiency.

The efficient implementation of encryption algorithm is the key for the efficiency of cryptosystem. The algorithm design and the implementation process need to completely consider the optimal use of Cache, the development and exploitation of instruction-level parallelism, and other closely related with the CPU system structure features. The client program also needs to be optimized considering the possible system structure of the client.

(2) Generate the distributed private key

For the bottleneck effects caused by the centralized organization of identity-based encryption, this paper explores to introduce the distributed algorithm and scheme for private key generation in the layered identity-based encryption system. The generation of private key is distributed to at least two entities locating on the path from the hierarchical tree root to this node. The private key generation algorithm ensures that any individual entity cannot generate all private keys, but only generate partial private key based on some parameters. The private key is synthesized from the partial private key of each entity. Then, in such a system, PKG cannot have users' private keys, lowering the possibility of PKG leaking private keys or abuses to a great degree. This paper studies the generation algorithm of new private key and the reorganization algorithm of partial private key. These algorithms are new and mean to design the internal distribution, instead of just introducing the distributed character to existing algorithm.

(3) Generate and save the global system parameters and master key

The global system parameters and the master key are the base for private key generation. Their security is the base for the identity-based encryption system. Reasonable storage and access control mechanism for system parameters and master key is the core of the problem. The Lightweight Directory Access Protocol (LDAP) solves the problem of saving and accessing system parameters, private key and other data in the layered identity-based encryption system.

Acknowledgements

This work was supported by Scientific Research Projects in Inner Mongolia University for Nationalities (No.NMD1341) and Ph.D. Scientific Research Foundation in Inner Mongolia

University for Nationalities (No.BS323).

References

[1]Shamir A.Identity-based cryptosystems and signature schemes.Advances in Cryptology Proceedings of CRYPTO84.LNCS 196.Berlin: Springer-Verlag, 1985, 47-53

[2] Dan Boneh,Matt Franklin, Identity-Based Encryption from the Weil Pairing,Computer Science Department,Stanford University, Stanford CA 94305-9045.

[3]Boneh D,Franklin M. Identity-based encryption from the weil pairing.In: Advances in Cryptology-Crypto 2001. LNCS 2139.Berlin: Springer-Verlag, 2001, 213-229

[4] Menezes A,Okamoto T,Vanstone S.Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field[J].IEEE Trans on InformationTheory,1993,39(5);1639-1646

[5] W.E.Burr, Public Key Infrastructure (PKI) Technical Specification:Part A — Technical Concept of Operations[DB/OL],Working Draft, September 1998.

[6]Menezes A J,van O P C,Vanstone S A.Handbook of applied cryptography.New York:CRC Press,1997,300-412

[7] Teng Yue,Wang Shoudao,Lin Yu and Li Hongtu. Comparison of PKI IBE CPK[J]. Science & Technology Information, 2008,18,402-403

[8] Boneh D，Boyen X，Goh E．Hierarchical identity based encryption with constant size ciphertext[C]//Proceedings of Eurocrypt 2005：LNCS 3494． Berlin：Springer-Verlag，2005：440—456

[9] ZHENG Xiaolin,JING Jiwu. Research on Key Management Schemes for IBE[J]. Computer Engineering(in chinese), 2006,21,145-147+151