An IBE Implementation of REESSE1+

CHEN.Jiankang [1]
[1]College of Computer Science
Beijing University of Technology
Beijing, China 100124
jiankang718@126.com

SU.Shenghui[1, 2]
[2]College of Information Engineering
Yangzhou University
Yangzhou, China 225009
sheenway@126.com

***Abstract*—IBE (Identity-based Encryption) technology, no digital certificates, is user-friendly and convenient for back-office management. It simplifies the key management process of a public key cryptosystem and diminishes the cost of application. This paper presents the thought of IBE systems, and analyzes the typical encryption algorithm. The main works are as follows. First, through two SHA-256 Hash mappings, the authors convert a user's 72-bit ID into a REESEE1+ public key sequence. Second, from the REESEE1+ key transform, the authors design an algorithm that can use a public key sequence to generate a private key sequence, and analyze its security and time complexity. Finally, the encryption and decryption algorithms of the new IBE scheme are described the same as those of REESEE1+. According to MPP proposed in the REESSE1+ scheme, the security of a private key generated from a public key can be ensured, and according to ASPP in REESSE1+, the security of a ciphertext can be ensured.**

Keywords-Identity-based Encryption; REESSE1+; MPP; SHA-256; ASPP

I. INTRODUCTION

In 1984, Shamir[1] first proposed the concept of IBE (Identity Based Encryption) with the original purpose to simplify the certificate management in E-mail systems. IBE is an encryption which uses arbitrary character strings published by users (such as e-mail address, ID number, telephone number, etc.) as public keys. A user corresponds directly to the identity of the user, and there is no need to bind them with a digital certificate. Thus problems of public key management and effectiveness validation in a public key system are solved.

In this paper, the authors present the thought of IBE systems, and design a new IBE scheme based on the REESSE1+ public key cryptosystem. The main work is as follows: (1) Map the user's ID number into a REESEE1+ public key sequence by shift operations and hash functions. (2)Calculate the new private key sequence through the public key sequence of the user's ID number and the key transformation formula

$$A_i \equiv (C_i^{\delta^{-1}} W^{-l(i)})(\%M) \tag{1}$$

to encrypt the user's information. (3)Analyze the time complexity and security of this new IBE scheme.

Throughout the paper, unless otherwise specified, the sign % means 'modulo', M means 'M-1', $|x|$ denotes the size of a set x, $\|x\|$denotes the order of $x\%M$, and gcd(a,b) represents the greatest common divisor of two integers. Without ambiguity, $\%M$ is usually omitted in expressions.

II. OUTLINE OF IBE

In 1984, Adi Shamir, one of the inventors of RSA, proposed the thought that identities can be used directly as public keys without certification. But until 2001, a truly practical IBE scheme was first proposed by Boneh and Franklin[2]. The scheme employs bilinear mapping, and it is based on the bilinear Diffie-Hellman assumption. It has adaptively chosen ciphertext attack security in the random oracle. In the same year, Cocks[3] proposed an encryption scheme without bilinear pairings, which is based on the quadratic residue assumption.

In IBE, the public keys are the users' unique identities. The elementary operations of PKG are to setup and to extract. There are 4 algorithms in an identity based encryption scheme:

a) Setup: a PKG creates its system parameters and a master secret key.

b) Extract: the user submits the identity information to the PKG, after which the PKG would generate a private key and return to the user.

c) Encrypt: anthor user encrypts a message using single identity information ID.

d) Decrypt: a reciver decrypt the cipher text using the private key which corresponds to the ID and get the message.

III. THE REESSE1+ PUBLIC KEY CRYPTOSYSTEM

A. The Problems

Definition 1: Seeking the original $\{A_i\}$, $\{l(i)\}$,W from

$$C_i \equiv (A_i W^{l(i)})^{\delta} (\%M) \tag{2}$$

with M prime is called the multivariate permutation problem, shortly MPP.

Definition 2: Seeking the original $\underline{b}_1 \ldots \underline{b}_n$ from

$$\overline{G} \equiv \prod_{i=1}^{n} C_i^{\underline{b}_i} (\%M) \tag{3}$$

with M prime is called the anomalous subset product problem, shortly ASPP.

B. A Coprime Sequence

If $A_1,\ldots,A_n$ are n pairwise distinct positive integers such that $\forall A_i, A_j$ with $i \neq j$, either gcd(A_i, A_j)=1 or gcd(A_i, A_j)=$H \neq 1$,

Published by Atlantis Press, Paris, France.

$(A_i/H) \nmid A_k$ and $(A_i/H) \nmid A_k \in [1,n]$, the serial integers are called a coprime sequence denoted by$\{A_1,\ldots,A_n\}$, shortly$\{ A_i \}$.

C. The Key Generation Algorithm

Let $P_1,\ldots,P_n$ be n primes in the set N, Λ= {2,3,…,1021},Ω ={5,6,…,2n+4}.Assume that d, D, T, S are four pairwise coprime integers, with $d\in[5,2^{16}]$,$D,T\geq 2^n$.

Here are the procedures of the key generation algorithm:

a) Random generate a coprime sequence $\{A_1,\ldots,A_n\}$ with $A_i\in\Lambda$.

b) Select a prime $M>(\max_{1\leq i\leq n} A_i)^n$ making $dDT|M$, gcd(s, $\overline{M}$)=1.

c) Pick $W,\delta\in(1, \overline{M})$ making gcd(δ, $\overline{M}$)=1, $/\!/\delta/\!/=dDT$,$/\!/W/\!/\geq 2^{n-20}$.

d) Randomly product pairwise sequences $l(1),\ldots,l(n)\in\Omega$.

e) Compute $C_i\leftarrow(A_iW^{l(i)})^{\delta}(\%M)$ for $i=1,\ldots,n$.

At last, $\{C_i\}$ is a public key, and $(\{A_i\},\{l(i)\},W,\delta,D,d)$ is a private key.

IV. Description of the New IBE Algorithm Based REESEE1+ Scheme

A. System-parameter Generation

According to "(2)", in which i=1,…,n, the authors take <W,$\{l(i)\}$> of the key generation formula as the system parameters. In order to make the generation of the private key facile, the system parameters will be public. The PKG privately owns the master key δ and will keep it confidential and equal to every user.

System params= <W, $\{l(i)\}$>; Master key=δ.

The constraint condition: select two integers W, $\delta\in(1, \overline{M})$ and make gcd(δ, $\overline{M}$)=1. l(1),…,l(n) are different integers.

B. User Identification Mapping

In this paper, user's ID of arbitrary lengths will be mapped into a REESEE1+ public key sequence $\{C_i\}$. The new IBE scheme will provide an user identification mapping and maps a user's 72-bit binary string ID number into a REESEE1+ public key sequence $\{C_1C_2\ldots C_{96}\}$.

The process is as follows:

a) Convert the user's identification ID into a 0,1 bit string. The identity transformation rule is: transform the 18-digit ID number into a form of 0,1 bit string. Each of the 18 digits will be turned into hexadecimal forms and converted into 4 bits, thus 18×4=72.

b) Convert the 72-bit ID number of the user into 512-bit messages. Rules of Mapping and filling are as follows:

Firstly, the authors map the original information into 2 parts: the left is the original 72-bit identity information: L= $a_1a_2\ldots a_{72}$; the right is totally negated from the original: R= $b_1b_2\ldots b_{72}$.

Secondly, the authors fill bits of each part of the 72-bit information into a 512-bit string S and thus to ensure the length of the SHA-256 input block. In the constructing of S, fill a 1 in the right of L, and 0s in the remaining bits until the length will satisfy that after taking the modulo of 512, the remainder is 448. Finally the bit string is cascaded with |L|mod264 message which is the 64-bit binary representation.

Thirdly, the authors take both the left and the right 512-bit string S1, S2 as a input of a Hash Function SHA-256, and then output respectively the 256-bit data.

At last, we combine the two 256-bit strings to generate a 512-bit binary character string. Through the Hash function SHA-256, the mapping not only guarantees the length of the binary string, but also ensures the uniqueness of the conversion of user information

c) Through P-box, map the 512-bit binary string into a REESEE1+ public key sequence $\{C_1C_2\ldots C_{96}\}$. The corresponding P box rules are:

- Divide a 512-bit binary string into 96 groups. Each group contains 5 bits and the last one contains all the remaining bit strings. These 96 groups will be presented separately as: $\{B_1,\ldots,B_{96}\}$. Data of these bits and their corresponding public key sequence $\{C_1C_2\ldots C_{96}\}$ is like this: $C_i\equiv(B_1\ldots\ \overline{B_i}\ldots B_{96})\%M$.
- Negate all the bit blocks B_i that corresponds to C_i and combine the original B_i to construct a new bit string M, with i=1…n-1. Then user's 72-bit binary string ID is mapped to the public key sequence $\{C_1C_2\ldots C_{96}\}$.

The user identity mapping process is as shown in Figure1.

C. User Private Key Generation

A 72-bit binary user identification string is mapped to a REESEE1+ public key sequence: $\{C_1C_2\ldots C_{96}\}$. The private key is generated by the PKG. In the IBE-based REESEE1+ algorithm, System params =<W, $\{l(i)\}$>, master key= δ.

The authors transform the formula of REESEE1+ key generation into "(1)".Then PKG use the new formula to compute a private key sequence $\{A_1,\ldots,A_n\}$, ensuring that A_i and $A_{i+1}$are coprime, with i=1…n-1.

The description of the algorithm is as follows:

S1: Set $i\leftarrow 1$,$\Omega\leftarrow\{5,6,\ldots,2n\text{-}4\}$,$\Lambda\leftarrow\{\varnothing\}$.

S2: Randomly select a $l(i)$ in the set ofΩ, and choose a generator W, the master key δ. Compute a private key A_i by the formula "(1)" with $\Omega\leftarrow\Omega-\{l(i)\}$.

S3: According to the definition of coprime sequence, decide whether A_i and elements of Λ are coprime or not:

a) when A_i and any element of Λ are coprime,$\Lambda\leftarrow\Lambda+A_i$; $i\leftarrow i+1$:

If $i<n$: {goto S2,loop continues ;}

Otherwise $i\geq n$: {goto S4,loop end ;}

b) when A_i and any element of Λ are not coprime, goto S2 to recalculated A_i;

S4: Get the private key sequence through circularly outputting all the elements of Λ.

The time complexity of the algorithm lies mainly in the cycle of determining whether A_i and A_{i+1} are coprime in Step 3, in which $l(i)$ is a randomly selected number. It is a probabilistic algorithm. In order to increase the success ratio of computing, we will adopt the method of randomly selection to make the range of $l(i)$ average and easily computer n pairs of coprime A_i.

Here are the private key generation algorithm analysis from the best and the worst aspect:

Best case: For each calculated A_{i+1}, it is coprime with A_i. So that each A_i which is computed out by using those randomly selected $l(i)$ is coprime with others and just constitutes the private key prime sequence. The time complexity is linear O(n).

Worst case: each A_i calculated out by using the randomly selected $l(i)$ needs to be recalculated. So we need to carry out $2n+1$ coprime inspections to compute the final coprime sequence. The time complexity is O(n!).

D. Encryption and Decryption

The new IBE scheme adopts the same encryption and decryption algorithms of REESSE1+ public key cryptosystem. A sender utilizes the public key sequence $\{C_1C_2\ldots C_{96}\}$ which is mapped from the user identification to encrypt message; the recipient inquires from PKG a private key sequence $\{A_1,\ldots,A_n\}$ that is generated from the public key sequence and use it to decrypt ciphertext.

The stage of the private key generation algorithm is constructed according to MPP, the difficulty of which is at least equal to DLP. And there are some evidences showing that its degree of difficulty is even higher than DLP, which ensures the security of the private key. What's more, the encryption and decryption stage of the REESSR1+ is based on ASPP, which makes the ciphertext encrypted through the new IBE scheme more reliable and safer than the traditional IBE based on bilinear methods. The new scheme is easier to achieve and calculate, and more convenient, efficient and securer.

V. ALGORITHM ANALYSIS

In the typical Boneh-Franklin(BF) IBE scheme, the private key is generated by the multiplication of a hash function and a master key, which is much too simple. In this paper, we generate the private key through a REESEE1+ key generation algorithm whose difficulty is based on MPP. Its difficultness is equal to DLP but with the advantages of easy achieving and higher security.

A. User Parameters Analysis

In the new IBE scheme, System params is $<W, \{l(i)\}>$, the master key is δ, where $W,\delta \in (1, \bar{M})$ making $\gcd(\delta, \bar{M})=1$, $\|\delta\|=dDT$, $\|W\|\geq 2^{n-20}$.These parameters with strict constraints can improve the security of the algorithm. In the case that master keys are of the same length, the proposed algorithm based on the multiple problems is much safer than the traditional IBE algorithm. It requires square root operations when a attacker want to compute δ, which is equivalent to the index level of difficulty, i.e. DLP. So, δ can be used as the master key to ensure the security of the generation algorithm. System parameters $<W,\{l(i)\}>$ are randomly selected by a PKG, so that the new scheme has characteristics of the probability algorithm. It is much more difficult to crack private key.

The authors map user's 72-bit ID number into 256-bit identity information by hash function SHA-256 to ensure the uniqueness of the transformation. Thus the converted public key sequence is also unique. To generate private keys by combining a IBE system with the REESEE1+, which is based on MPP, the new IBE scheme definitely increases the difficulty of the private key generation process, and its time complexity.

B. Identify Collusion attack Problems Analysis

In view that different users have their own IDs, each of the generated sequences $\{C_i\}$ is different from others. Users' private keys $\{A_1,\ldots,A_n\}$ maintain a nonlinear relationships each other. Such a nonlinear relationship also exists between the identity sequences and the private key sequences. There are $2n+2$ variables in the transform formula "(1)" and each formula contains 4 mutually independent variables. The multivariable key transformation formula is based on multivariable problems, which leads to fully security. It is difficult to solve $\{l(i)\},\{A_i\},W,\delta$ on the premise that $\{C_i\}$ is known. This is so-called MPP. Its difficulty of time complexity is at least equal to that of the discrete logarithm problem. Therefore, there is no such matter as to perform collusion attack by using nonlinear equations, and the new scheme can resist linear collusion attack[7].

C. Algorithm time Complexity Analysis

The new IBE scheme is constructed on the basis of MPP. In computation, within the same prime field, MPP is at least equivalent to DLP[8].

Assume that every $g_i \equiv (A_i W^{l(i)})(\%M)$ is a constant, and let $g \equiv g_i^{x_i}(\%M)$, $Z_i \equiv \delta x_i (\%M)$ for $i=1,\ldots,n$ where $g \equiv Z_M^*$ be a generator. Then we have $C_i \equiv g_i^{\delta} \equiv g^{\delta x_i} \equiv g^{z_i}(\%M)$.

Seen from the above transformation, it is obvious that, if an attacker wants to attack the MPP, he must first reduce it to DLP. So the time complexity of MPP is equivalent to that of DLP. In other words, finding out the time complexity of z_i from $C_i \equiv g^{z_i}(\%M)$ is at any rate equivalent to DLP.

When every g_i is assumed to be a constant, seeking δ from $C_i \equiv g_i^{\delta}(\%M)$ with $i=1,\ldots,n$ is equivalent to solving DLP problems. However, In fact, g_i is not a constant. Though $C_i \equiv g_i^{\delta}(\%M)$ could be reduced to DLP, it still remains unknown that whether DLP can be reduced to MPP. Therefore, since g_i is not constants, the authors incline to believe that MPP is more intricate and difficult than DLP. There is higher level of security and more reliability when we adopt algorithms constructed on MPP rather than that constructed on DLP.

VI. CONCLUSION

Through the mapping of user identifications, in this paper, the authors match the ID number with the REESEE1+ public key sequence $\{C_i\}$, and then workout the corresponding private key sequence $\{A_i\}$. By combining the REESSE1+ with the identity based encryption systems, the authors have designed a new, more practical and safer encryption scheme. It has gained the national independent intellectual property rights. The new scheme contributes not only to the promotion of the new multivariable public key encryption system REESEE1+, but also to the further implementation and development of the identity based encryption system IBE. In the future, our study orientation will be: how can we cut down the number of bits of the modulus in the algorithms and how to improve the speed of the algorithm.

REFERENCES

[1] A. Shamir, Identity based cryptosystems and signature schemes[C], In Advances in Cryptology Crypto 84, Lecture Notes in Computer Science 0196, Springer-Verlag, pp. 47-53, 1984

[2] D. Boneh and M. Franklin. Identity Based Encryption from the Weil pairing [J]. In Advances in Cryptology-Crypto 2001, volume 2139 of LNCS, Pages 213-229.Spring-Verlag, 2001

[3] C. Cocks, An Identity Based Encryption Scheme Based on Quadratic Residues[J], in Advances in Cryptology-Crypto 2001, volume 2139, Spring-Verlag, pp.213-229,2001

[4] Senghui Su and Shuwang Lü, A Public Key Cryptosystem Based on Three New Provable Problems, Theoretical Computer Science, v 426 -427,Apr.2012,pp.91-117

[5] Senghui Su and Shuwang Lü, Based on the variable combinations of REESSE1-E signature scheme[J], Chinese Journal of Electronics, 2010(1)

[6] Liang Hu, Kou Zhao, Wei Yuan, Identity based cryptography [M].Bei Jing: HIGHER EDUCATION PRESS,2011

[7] Huanping Chen, Zhi Guan, Some problems about CPK description[J], Information Security and Communications Privacy,pp.47-49.2007(9).

[8] Xuejun Li, Based on the elliptic curve discrete logarithm problem of public key cryptography, Computer Engineering and Applications, pp.20 -22, 2002(6)

[9] Meilin Zhao, Shaowu Zhang, Security analysis of combined public key technique based on ECC [J], Computer engineering, pp.156-157,2008,34(1).

[10] Song Luo; Qingni Shen; Yongming Jin; Yu Chen; Zhong Chen; Sihan Qing, A Variant of Boyen-waters Anonymous IBE Scheme, Information and Communications Security. Proceedings 13th International Conference, ICICS 2011, p 42-56, 2011

[11] Liang Hu, IBE system key management mechanism. Chinese Journal of Computers [J],pp.543-551, 2009(3).

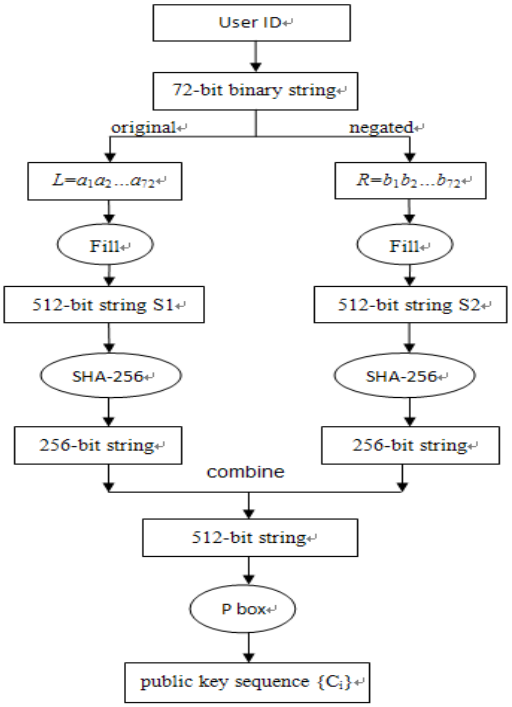

Figure 1. User identity mapping model