Anonymous Identity-Based Key Scheme in Application of Privacy Protection

Changjiang Shen[1,a], Lan Yang[1,b] Chuansheng Zhou[1,c]*

College of Computer Application Technology, Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
[a] 474456226@qq.com, [b] 1017467789@qq.com, [c] 252752602@qq.com
*corresponding author

Keywords: privacy protection, Identity-Based Encryption, anonymity

Abstract: With the advancement of cloud computing application and research, there is a lot of data interaction between the users and the cloud computing platforms where exists a threat to the transmission and storage of users' data. Providing an efficient revocation mechanism for identity-based encryption (IBE) is very important since a user's credential (or private key) can be expired or revealed. For the current identity-based encryption program is not anonymous. We construct a new identity-based anonymous encryption scheme (AIBKE) based on the character of bilinear group and the bilinear DH. The new scheme not only solves the problem that the existing scheme can not protect the privacy of the receiver, but also ensures anonymous that both sender and receiver of the signcryption program. The scheme can satisfy both semantic security, unforgeability, and anonymity.

1. Introduction

Identity-based cryptography is a special public key cryptography, it was originally designed by the RSA cryptographic algorithm co-inventor Adi Shmai who proposed this identity-based encryption algorithm named IBE (Identity-based Encryption) in 1980's. Shamir initially proposed the mechanism is to simplify the traditional public key infrastructure in the CA public key certificate management[1]. The basic of idea is to bind the user's identity to public key which the user's identity information is the user's public key in the most natural way.

In the identity-based cryptosystem, there is a credible party called the private key generation center (PKG, private key generator), a file can be responsible for the user in the system that generate identity information corresponding to the secret key. After confirming that the identity information does belong to the corresponding user, which was generated corresponding key and secretly transmitted to the user. When you need to use the public key of a user in the system, you only need to know the user's identity information without obtaining and verifying the user's public key certificate. We can use Bob's email (bob@sina.com) as his identity when Alice sends an encrypted message to Bob, it is only necessary to use the identity information of bob@sina.com as a public key for encryption. This shows that identity-based encryption simplifies the public key management process, thereby avoid the various drawbacks due to management of public key certificate in traditional public key cryptosystem. The brief process is shown in Figure 1.

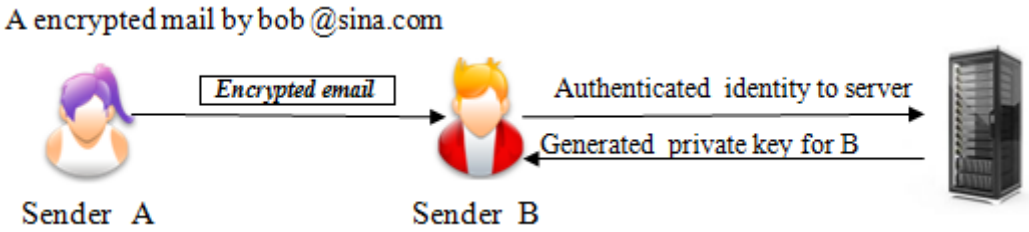

Figure 1. The process of E-mail encryption

While under the concept of identity based cryptosystem identity-based signature, an identity-based signature scheme (IBS) is proposed. Compared with the traditional public key signing scheme (Public Kay Signature, PKS), these IBS schemes have no obvious advantages, even when the PKS program's signature and certificate use short signatures, the efficiency will be better than most IBS programs. In 2001, Boneh, Franklin[2] and Ohgishi, Kasahara[3] and Crocks[4] respectively proposed three identity-based encryption schemes, thus opening a new chapter based on identity cryptography research. Among them, Crock's program is based on quadratic residual problems, but there is a quadratic residue problem that does not cause much reaction.The Boneh and Franklin's scheme and Ohgishi and Kasahara's program both use pairs of operations that satisfy the bilinear mapping, besides Boneh and Franklin proved that their program in the random oracle mode can meet the anti-adaptive choice of identity and selected the ciphertext attack indistinguishable security (IND-ID-CCA). In the random oracle model, it is proved that their scheme can meet the anti-adaptive selection status and choose the ciphertext attack indistinguishable security.

Smart[5] first introduced the concept of multi-receive key encapsulation (KEY) in 2004. The program uses a number of public keys for the KEM scheme as input, combined with the data encapsulation mechanism (DEM), so that the entity can send a single plaintext message to a receiver set. Subsequently, Bentahar et al. Extended the concept of key encapsulation to identity-based cryptography primitives, who proposed a general construction method based on identity key encapsulation (ID-KEM). In 2005, Barbosa and Farshim[6] proposed in conjunction with the identity key encapsulation and multi-recipient key encapsulation in order to deduce the identity-based multi-recipient key encapsulation (ID-KEM). Meanwhile, Several elegant revocation constructions [7,8,9,10] have been proposed.

Combining with the character of bilinear group under DH hypothesis, we propose a recipient anonymous key encapsulation scheme that can protect the recipient's privacy. The random oracle is derived from Gap-BDH difficulty hypothesis，and we formally prove that the proposed scheme satisfies confidentiality and anonymity. Compared with the program based on identity of the anonymous broadcast that Hur et al[11] proposed we show the high efficiency and better security of the scheme in this paper.

1.1 Preliminaries

K_1 and K_2 are the cyclic group that both have two order of prime p. Bilinear mapping needs to satisfy the following three properties $e: K_1 \times K_2 \to K_2$.

1) Bilinear property. For

$a, b \in z_p^*$ and $x, y \in K_1$，$e(x^a, y^b) = e(x, y)^{ab}$ (1)

2) Non-degeneracy. All elements of $K_1 \times K_2$ are not mapped to the K_2 unit in the element. When k is the generator of K ,it is also $e(k, k)$.

3) Computability. For any $x, y \in K_1$,there is a effective algorithm calculation $e(x, y)$,and then

calculate $e(x,y)\neq 1$.

Supposing K_{p_1}、K_{p_2} are the subgroup of order p_1、p_2 in K, $K_{1.p_1}$、$K_{1.p_2}$ are presented as the subgroup of order p_1、p_2 in K_1, according to the properties of cyclic group[8]:If the order of K is the finite order in m, x^q is the finite order of K.Because of $(q,m)=1$,so x^q is the generator. We say that k^{p_2}、k^{p_1} are the generator of K_{k_1}、K_{k_2} respectively.

For any $h_{k_1}\in K_{k_1}$、$h_{k_2}\in K_{k_2}$, there will be $a,b\in Z_n$ and satisfy

$$e(h_{p_1},h_{p2})=e(h_{p1}^a,h_{p2}^b)=e(k,k)^{k1k2ab}=1 \qquad (2)$$

1.2 Several Difficult Assumptions of Diffie-Hellman

To determine the help of Diffie-Hellman oracle: Given the value (k,k^a,k^b,R), if the value $e(k,k)^{abc}=R$ that can be outputted 1 or 0.

1)To determine the question of Bilinear Diffie-Hellman Problem (BDH):Let k be a generator of $K_1,k^a,k^b,k^c\in K_1$, $R\in K_2$, which a,b,c are there random number in group Z_p^*, now it is difficult to judge $e(\mathrm{k},\mathrm{k})^{abc}=R$.

2)To determine the question of Twin Diffie-Hellman: For any $a,b,c\in Z_q^*$, giving the value P、aP、bP、cP, then calculating acP and bcP.

3) To determine the question of Strong Twin Diffie-Hellman : For any $a,b,c\in Z_q^*$,the value of P、aP、bP、cP was given and we calculate acP and bcP in the help with Twin Diffie-Hellman oracle. After we determine Twin Diffie-Hellman oracle: Given the value $(P,aP,bP,cP,\mathrm{Z},\mathrm{X})$, if the result is $abP=Z$ 、 $acP=X$ and then output 1 else output 0.

4) To determine the question of Bilinear Diffie-Hellman Index Problem: selecting (q-DHBHE) and β in a random order, furthermore , $Z\in K_1$, k 、$k^{'}$ both are the generator of K_1, $(\mathrm{k}^{'},\mathrm{k},\mathrm{k}^{\beta},\mathrm{k}^{\beta+1},\mathrm{k}^{\beta+2},\cdots,\mathrm{k}^{\beta^{2q}},\mathrm{Z})\in K_1^{2q+1}\times K_2$.

Above all，we need to judge whether Z is equal to $e(\mathrm{k}^{'},\mathrm{k})^{\beta^{q+1}}$.

2. Identity-Based Encryption

2.1 The Definition of Identity-Based Encryption

The identity-based encryption mechanism consists of our polynomial time probability algorithms that are Setup, Extract, Encrypt and Decrypt.

Setup The setup algorithm additionally chooses the security parameters k, then return the system Public Params and the master-key of system. System public parameters including: Limited description of the message space M and description of the ciphertext space C. Only PKG knows the secret key that stored in the master key secretly named master-key，and open parameters of the system params is announced.

Extract The Extract algorithm generates the corresponding private key for the public key ,and inputs params、master-key and $c=Encrypt(param,ID,m)$ randomly, then returns to the

corresponding private key. d is corresponding private decryption private key where ID is an arbitrary long string as a public key.

Encrypt Input params, ID and plain text messages $m \in M$, and output ciphertext c , $c \in C$.

Decrypt Input params, private key d and ciphertext $c \in C$,then returns to the plaintext message.

As mentioned，I hope that the algorithm must meet the consistency condition, that is, when the private algorithm is generated by the public key corresponding to the private key, the following calculation established:

For any $m \in M$, $Decrypt(params, c, d) = m$, $c = Encrypt(param, ID, m)$.

2.2 Security Definition

The security definition is based on the choice of identity under the choice of indivisible ciphertext attack (IND-sMID-CCA) and the identity of the selected ciphertext attack under the anonymous security (ANON-IND-sMID-CCA).

1) Confidentiality of ciphertext

The IBE's IND-sMID-CCA2 security is defined by the game between the following A and Challenge C.

Phase1: Adversary A chooses a set of challenge recipients $S^* = \{ID_1, ID_2, \cdots ID_n\}$, among this n is positive number.

Setup: Challenger B sets the algorithm to get the params and master key msk , then sends params to attacker A.

Phase 2: Attacker A can make a series of inquiries at this stage, including key extraction inquiries, decryption inquiries.

Cipherkey extraction inquire: B returns value to the attacker A by using Operation key extraction algorithm if it receives the inquire of $ID_j \notin S^*$.

Decryption inquire: Because of $i \in \{1, 2, \cdots, n\}$ 、 $Hdr = (U, V, c_1, c_2, \cdots, c_n)$, B may make use of sk_{ID_i} by using key extraction algorithm when receipting the inquire of (Hdr, ID_i). At last, We run the encapsulation algorithm $\varepsilon = r\left|\Pr[b = b'] - \frac{1}{2}\right|$ and return the result to the attacker A.

3. Description of AIBKE Program

In this section we propose a new multi-receive anonymous identity encapsulation scheme through using anonymous identity negotiation technique. The new program not only satisfies anonymity, but also has more security, higher algorithm efficiency and shorter ciphertext.

3.1 The AIBKE was made up of following four algorithms:

1) Initialization (k) : Inputting the security parameter k to obtain a bilinear mapping group system $\lambda = \{p, G_1, G_2, e(\cdots)\}$, $|p| = k$. g_1 and g_2 are the two generators of the group. Choose three cryptographic hash functions: $H : G_1^2 \times G_2 \to Z_p^*$, $H_1 : \{0,1\}^* \to G_1$, $H_2 : G_1 \to Z_p^*$ .Let system public parameters be $params = \{g_1, g_2, \lambda, H_1, H_2\}$,the System master key be

$MSK = x$, the public key system be $PK = g_1^*$.

2) Private key extraction (MSK, ID_i) :Computing private key $sk_{ID_i} = H_1(ID_i)^x$ before Inputting MSK 、 $params$ and identity information ID_i .

3)Key encapsulation (S, PK) :After inputting $params$, $S = \{ID_1, ID_2, \cdots, ID_n\}$ PK , the algorithm follows the following steps:

(1) Computing the equation $U = g_1^r$ from r randomly in Z_p^* . (2) For any of ID_i in sets S , computing the equation $Q_i = H_1(ID_i)$ and $s_i = H_2(e(Q_i^r, g_1^x)$. (3) Computing $V = g_1^t$ and $\alpha = H(U, V, e(g_1^{s_i}, g_2)^t)$ before selecting t from Z_p^* randomly. (4) Selecting numerical value that satisfies $K \in Z_p^*$ and computing the equation $c_i = K \cdot e(g_1^{s_i}, g_2)^{t+\alpha}$. (5) Outputting the encapsulated ciphertext $Hdr = \langle U, V, (c_1, c_2, \cdots, c_n) \rangle$. (6) De-encapsulation $\left(ID_i, sk_{ID_i}, Hdr\right)$:This ,in turn, we input ciphertext including Hdr 、 $params$ and the recipient identity of ID_i and sk_{ID_i} .

Specific steps are as follows:

a)computing $s_i = H_2\left(e\left(sk_{ID_i,}, U\right)\right)$.

b) computing $\alpha = H\left(U, V, e\left(V, g_2\right)^{s_i}\right)$

c)Inputting $K = \dfrac{c_i}{e\left(V, g_2\right)^{s_i} \cdot e\left(g_1^{\alpha}, g_2\right)^{s_i}}$

The correctness of the algorithm can be verified by the following equation:

$$K = \frac{c_i}{e\left(V, g_2\right)^{s_i} \cdot e(g_1^{\alpha}, g_2)^{s_i}} = \frac{c_i}{e\left(g_1^t, g_2\right)^{s_i} \cdot e(g_1^{\alpha}, g_2)^{s_i}} = \frac{c_i}{e\left(g_1^t, g_2\right)^{t+\alpha}} = \frac{K \cdot e\left(g_1^{s_i}, g_2\right)^{t+\alpha}}{e\left(g_1^{s_i}, g_2\right)^{t+\alpha}} = K \quad (3)$$

3.2 Security Analysis

The study will be extended to the chosen ciphertext attack [13,14] under security model by selecting plaintext attack status that Hur et al[12] proposed. We analysis the security of the proposed scheme based the hypothesis of Gap-BDH.

We assume k is a safety parameter, exist a probable polynomial time of the IND-sMID-CCB attacker A, runtime τ . Through inquiring about random questioner H_i in q_i times, extracting q_k times key of inquiry and q_d times of sub-decryption inquiry, this give us possibility to attack the program of this article with advantage by $\varepsilon(k)$. So, there exists a probable polynomial time within the algorithm named B that run time in τ' with a non-ignorable advantage. To solve difficult

problems of Gap-BDH by $\varepsilon' \geq \varepsilon - \frac{q_d}{q}$,where the runtime is $\tau' \approx \tau + (q_1 + q_k)O(\tau_1) + (nq_2 + q_d q_2)O(1)$ .Among them, τ_1 is the time to complete a scalar multiplication in group G_1, n is the total number of recipients, q_b is the number of times to ask the DBDH oracle machine.

Phase 1: Attacker A selects a challenge receiver, $S = \{ID_1, ID_2, \cdots, ID_n\}$, besides n is positive integer.

Initialization: Challenger B sends

$Params = \{g_1, g_2, G_1, G_2, e(\cdot,\cdot), PK, H, H_1, H_1\}$ to attacker A,

$PK = g_1^b, Q = g_1^a$, H_1、H_2 and H are controlled by the random oracle machine of B.

H_1 Inquiry: B maintains a list of initial forwarding states that are empty called $L_1 = (ID_i, \omega_i, Q_i)$. If there exists (ID_j, ω_j, Q_j), B firstly searches the list L_1, once H_1 receipts the inquiry of identity ID_i,then returns Q_j to A;

Otherwise the proceed as follows:

1) If the condition meets $ID_j \in S$, B selects $\omega_j \in Z_p^*$ randomly. Computing and returning the equation $Q_j = Q^{\omega_j}$, adding the value $(D_j, \omega_j Q)$ to list L_1.

2) Otherwise, computing and returning the equation $Q = g_1^{\omega_j}$ when B selecting $\omega_j \in Z_p^*$ randomly, meanwhile, adding the value (ID_j, ω_j, Q_j) to list L_1. H_2 Inquiry: B maintains a list of initial forwarding states that are empty called $L_2 = (V_i, v_i)$. B firstly searches the list, once H_2 receipts the inquiry of V_j, in this way we ensure that the security model is safe for both parties.

4. Conclusion

This study is based on stochastic models and Gap-BDH assumptions, and an identity-based anonymous encryption scheme is constructed under the union of bilinear groups The study satisfies the confidentiality and anonymity of the choice of ciphertext attack under the choice of identity model. In the future era of rapid development of communications technology, it will put forward higher requirements in identity based on encryption design.

Acknowledgement

This paper is sponsored by:

(1) Educational Department of Liaoning Province (Project Number: LiaoJiaoHan L201611)

(2) National Center for Educational Technology (Project Number: JCZY2015-GJ-KJZTJXWZ-04)

References

[1] Draves R., Padhye J., Zill B. (2004) Routing in multi-radio, multi-hop wirelessmesh networks[C] // Proceedings of the 10th annual international con-ference on mobile computing and networking. ACM, 114-128.

[2] Gentry C., Silverberg A., (2002) Hierarchical Identity-Based Encryption. EUROCRYPT, 466-481.

[3] Lewko A., Waters B. (2009) Fully Secure HIBE with Short Ciphertexts. Cryptology ePrint Archieve, Report 482.

[4] Kenneth G. P., Jacob C. N. (2006) Schuldt: Efficent Identity-Based Signitures Secure in the Standard Model. ACISP,207-222.

[5] Smart N.P. (2005) Efficient Key Encapsulation to Multiple Parties. Carlo Blundo and Stelvio Cimato. Security in Communication Networks 2004: LNCS 3352. Berlin:Springer-Verlag, 208-219.

[6] Barbosa M., Farshim P. (2005) Efficient Identity-Based Key Encapsulation to Multiple Parties. Smart Nigel P. IMA International Conference , LNCS 3796. Berlin: Springer-Verlag, 428-441.

[7] Attrapadung N., Imai H., (2009) Attribute-based encryption supporting direct/indirect revocation modes. In Parker, M.G., ed.: IMA Int. Conf. Volume 5921 of Lecture Notes in Computer Science., 278-300

[8] Attrapadung N., Imai, H. (2009) Conjunctive broadcast and attribute-based encryp-tion. In Shacham, H., Waters, B., eds.: Pairing. Volume 5671 of Lecture Notes in Computer Science., Springer 248-265

[9] Nieto, J.M.G., Manulis, M., Sun, D. (2012) Fully private revocable predicate encryption.In Susilo, W., Mu, Y., Seberry, J., eds.: ACISP. Volume 7372 of Lecture Notes in Computer Science., Springer350–363

[10] Sahai, A., Seyalioglu, H., Waters, B. (2012) Dynamic credentials and ciphertext del-egation for attribute-based encryption. In Safavi-Naini, R., Canetti, R., eds.:CRYPTO. Volume 7417 of Lecture Notes in Computer Science., 199-217

[11] Hur J., Park C., Hwang S.O. (2012) Privacy-preserving identity-based broadcast encryption. Information Fusion , 13(4), 296-303.

[12] Soldati P., Johansson B., Johansson M. (2006) Proportionally fair allocation ofend-to-end bandwidth in STDMA wireless networks. Proceedings of the 7th ACM international symposium on mobile ad hoc networkingand computin. ACM, 286-297.

[13] Barth A., Boneh D., Waters B. (2006) Privacy in encrypted content distribution using private broadcast encryption. Giovanni Di Crescenzo,Avi Rubin. Financial Cryptography LNCS 4107. Berlin: Springer-Verlag, 2006: 52-64.

[14] Boneh D., Gentry C. (2005) Collusion resistant broadcast encryption with short ciphertexts and private keys . Victor Shoup. Advances in Cryptology-CRYPTO: LNCS 3621. Berlin: Springer-Verlag,258-275.