I.J. Engineering and Manufacturing, **2012,4, 29-34**
Published Online August 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijem.2012.04.04

Available online at http://www.mecs-press.net/ijem

A Scheme of IBE Key Issuing Protocol Based on Identity-password Pair

Weimin Shi

College of Computer Science and Technology Beijing University of Technology Beijing, China

Abstract

To avoid the impersonation attack, an efficient and secure key issuing protocol based on identity-password pair is proposed, in which an additional identity-password pair issued by KGC and KPAs is used to authenticate a user's identity. In this protocol we use a simple blinding technique to eliminate the of secure channel and multiple authorities approach to avoid the key escrow problem. Our protocol solves the key-escrow problem successfully and saves at least 4n pairing and 2n Hash operations in comparison to Lee B et al's protocol.

Index Terms: Identity-based cryptograph; key issuing protocol; key-escrow problem

1. Introduction

In traditional certificate-based public key cryptosystems, a certificate issued by a certification authority (CA) is use to bind an entity's identity information with the corresponding public key. The validity and correctness of the digital certificate must be verified before its usage. When a digital certificate is signed by an authority whose public key is not already trusted by the user of the certified public key, the user is led to validate an entire chain of digital certificates before acquiring confidence in the authenticity of a given key and, furthermore, finding such a chain of certificates between the enquired key and a trusted one is not a trivial problem. Other problems with PKI is the fact that key revocation and certificate management are a big issue, which requires a large amount of storage and computing [1].

In order to bypass the above problems encountered in conventional Public Key Infrastructures, in 1984, Shamir introduced the concept of identity-based cryptography [2], where an entity's public key can be a unique binary string identifying its owner non-ambiguously, such as name, e-mail address, or IP address, et at.. The motivation of this kind of scheme was to simplify key management and remove the need of public key certificates as much as possible: since a key is the identity of its owner, there is no need to bind them by a digital certificate, and thus end users do not have to enquire for a certificate for their public key. However, Boneh and

* Corresponding author.
E-mail address: shiweimin@bjut.edu.cn

Franklin proposed the first efficient identity encryption scheme based on the bilinear pairings over elliptic curves until 2001. Since then, a great deal of research has been done about the ID-based cryptosystems.

In identity-based encryption scheme, a user's private key is generated for the user by a trusted third party called the Key Generation Center (KGC), where has an inherent key escrow because of its dependence on a KGC that uses a single master secret key to generate a user's private key. Therefore, the KGC can decrypt all of the ciphertext and forge signature for any message in its domain. Another issue is that it also requires a secure channel between users and the KGC to deliver private keys.

1.1. Related Works

To eliminate the problem of key escrow, many schemes have been proposed using multiple authority approach or some user-chosen secret information or blinding technique [3,4,5,6]. Boneh et al. and Chen et al. both proposed a multiple authority scheme to tackle the problem of key escrow [3,4]. Boneh et al's solution was to distribute a master key to n KGCs using a secret sharing method in which users computed the private key in a threshold manner. An alternative to this approach was suggested by Chen et al. who assumed n different KGCs with its own independent master key. Key escrow problem of a single KGC can be prevented in Boneh et al's. and Chen et al's schemes, but n KGCs have to check user's identification and build a secure channel with user independently, which are quite a burden.

A user-chosen secret information approach to tacking the issue of key escrow is proposed by Gentry et al. and Al-Riyami et al. [5,6]. Gentry et al. proposed a certificate-based encryption and Gentry et al. proposed a certificateless public key cryptography which successfully removed the necessity of certificate. They can eliminate key escrow, but they lose the advantage of identity-based cryptography in which the public key is directly derived from the identity.

In 2004, Lee B et al. proposed a novel secure key issuing protocol to solve ID-based key-escrow problem[7]. The protocol model includes a single key generation center (KGC) and multiple key privacy authorities (KPAs). A single KGC checks user's identification and issues a blinded partial private key to the user. Multiple KPAs sequentially provide key privacy service to user's private key by issuing their signature in a blinded manner. To provide a secure channel between users and authorities, a simple blinding technique is used in pairing-based cryptography. Recently, Sui el al. proposed a novel separable and anonymous ID-based key issuing scheme without secure channel based on a signature scheme similar to a short blind signature [8]. Their system supports the separation of duties between local registration authority (LAR) and key generation center (KGC). A user chooses a one-time password after offline authentication by LRA which is stored in KGC's databases together with the user's ID. The KGC verifies the user identity by the one-time password information and issues a blinded partial key for the user. Lee B et al.'s and Sui el al.'s solutions needn't build a secure channel between KGC and user which greatly reduced the cost of the system, but they are vulnerable to the impersonation attack, so they do not really solve the key escrow problem.

1.2. Our Contribution

In this paper, we present an efficient and secure ID-based Key Issuing Protocol, for the security, in which we use a single key generation center (KGC) and multiple key privacy authorities (KPAs) , and we suppose that for each user, there is an identity-password pair published to validate the user identity. The improved scheme solves the key-escrow problem and improves efficiency.

The rest of the paper is organized as follows: In section 2, we describe some concepts of bilinear pairings and related Mathematic problems. In section 3, we propose an efficient and secure protocol. In section 4, we analyze its security and performance. Finally, we conclude in section 5.

2. Preliminaries

In this section, we briefly review some concepts about bilinear maps and some related mathematic problems.

2.1. Bilinear-pairing:

Let G_1 be an additive group of prime order q and G_2 be a multiplicative group of the same order. Let P denote a generator of G_1. The discrete logarithm problem (DLP) in these groups is believed to be hard. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinear: $e(aQ_1, bQ_2) = e(Q_1, Q_2)^{ab}$, where $Q_1, Q_2 \in G_1$ and $a, b \in Z_q^*$.
2. Non-degenerate: $e(P, P) \neq 1$ and therefore it is a generator of G_2.
3. Computable: There is an efficient algorithm to compute $e(Q_1, Q_2)$ for all $Q_1, Q_2 \in G_1$.

Typically, the way of obtaining such pairings is by deriving them from the Weil pairing or the Tate pairing on an elliptic curve over a finite field. We refer to [3,9,10,11] for a more comprehensive description of how these groups, pairings and other parameters should be selected for efficiency and security.

2.2. Mathematic problems:

1. Discrete Logarithm Problem (DLP): Given two group elements P and Q in G1, find an integer *n*, such that Q = *n*P whenever such an integer exists.
2. Computational Diffie-Hellman Problem (CDHP): For any $a, b \in Z_q^*$, given <P,aP,bP>, compute abP .
3. Decisional Diffie-Hellman Problem (DDHP): For any $a, b, c \in Z_q^*$, given <P,aP,bP,cP>, decide whether $c \equiv ab \bmod q$.
4. Billnear Diffie-Hellman Problem (BDHP): For any $a, b, c \in Z_q^*$, given <P,aP,bP,cP>, compute $e(P, P)^{abc} \in G_2$
5. Gap Diffie-Hellman Problem (GDHP): A class of problems where DDHP is easy while CDHP is hard.

3. Proposed Key Issuing Protocol

Our protocol still use includes a single key generation center (KGC) issuing a user's blinded partial private key and multiple key privacy authorities (KPAs) providing the user's key privacy service as Lee B et al's protocol , but a master key s is distributed to KPAs in a *t*-out-of-*n* fashion. Moreover, In our protocol, we suppose that for each user, there is an identity-password pair (ID, Q_x) ,where $Q_x = x \cdot Q_{ID}$, $Q_{ID} = H(ID)$, (ID, Q_x) is public, but $x \in Z_q^*$ is randomly selected and keep securely by the user. KGC or KPA_i verifies a user identity by its identity-password pair.

The protocol includes the following 6 stages: system setup, system public key setup, user identity-password pair setup, key issuing, key securing, key retrieving.

3.1. System setup (by KGC)

1) Generates two groups of prime order q : $(G_1, +)$, $(G_2, \bullet)$ and a bilinear map e: $G_1 \times G_1 \to G_2$;

2) Selects a master key $s_0 \in Z_q^*$ at random and computes public key $P_0 = s_0 P$;

3) Selects a hash function $H : \{0,1\}^* \to G_1$;

4) Keeps s_0 secure and publishes the system parameters (G_1, G_2, e, P, H, P_0).

3.2. System public key setup (by KPAs and KGC)

1) A master key $s \in Z_q^*$ is distributed in a *t*-out-of-*n* fashion by giving each of the *n* KPAs one share s_i as Boneh&Franklin using distributed PKG [3]. Each of the *t* chosen KPAs computes its share $P_i = s_i P_0$ and sends it to the KGC.

2) The KGC computes the system public key as $Y = \sum \lambda_i P_i$, where λ_i's are the appropriate Lagrange coefficients.

3.3. User identity-password pair setup (by user)

1) Selects a secret key $x \in Z_q^*$ at random and computes $Q_x = x \cdot Q_{ID}$ with identity ID, where $Q_{ID} = H(ID)$;

2) Keeps x secure and publishes the identity-password pair (Q_{ID}, Q_x).

3.4. Key issuing (by KGC and KPAs and user)

1) A user computes $T_x = xP_0$, then sends $\{T_x\}$ to KGC for partial private key issuing;

2) KGC verifies the user identity by checking $e(T_x, Q_{ID}) \stackrel{?}{=} e(P_0, Q_x)$, then computes a blinded partial private key as $Q_0 = s_0 Q_x$, and sends $\{Q_0\}$ to the user over public channel;

3.5. Key securing (by user and KPAs)

1) The user computes signature on P as $D_x = x^{-1} P$, and sends $\{D_x, Q_0\}$ to each of the t chosen KPAs for key privacy service;

2) KPA_i （ $i = 1,2,\cdots,t$ ） verifies the user and the KGC identity by checking $e(D_x, Q_x) \stackrel{?}{=} e(P, Q_{ID})$ and $e(Q_0, P) \stackrel{?}{=} e(Q_x, P_0)$, then computers $Q_i = s_i Q_0$, and sends $\{Q_i\}$ to the user over public channel;

3.6. Key retrieving (by user)

The user computes $S_{ID}' = \sum \lambda_i Q_i$ where λ_i's are the appropriate Lagrange coefficients, then computes its private key $S_{ID} = x^{-1} S_{ID}' = x^{-1} \sum \lambda_i s_i s_0 x Q_{ID} = \sum \lambda_i s_i s_0 Q_{ID}$.

The user can verify his private key by checking $e(S_{ID}', P) \stackrel{?}{=} e(Q_x, Y)$.

4. Analysis

4.1. Security

Scenario 1

Eavesdropping on communication between the KGC and KPAs.

In the system public key setup phase the *t* KPAs send their shares $P_i = s_i P_0$ to the KGC. Extracting s_i from the publicly transmitted parameters is equivalent to the DLP, which is assumed to be computationally hard.

Scenario 2

Eavesdropping on communication between the User and KGC.

In key issuing phase, for avoiding a malicious attacker impersonating the user to obtain Q_0, the KGC confirms the user identity by checking the equality $e(T_x, Q_{ID}) \stackrel{?}{=} e(P_0, Q_x)$. Note that T_x is just a short signature [9] on P_0 which signed by a user's identity password key x. Since the short signature is secure under DLP, T_x can not be forged even by the KGC because it can not obtain the user's password key x.

Scenario 3

Eavesdropping on communication between the User and KPAs.

In key securing phase, KPA_i confirms a 2-tuple $\{D_x, Q_0\}$ deriving from the user by checking the equality $e(D_x, Q_x) = e(P, Q_{ID})$, then checks $e(Q_0, P) \stackrel{?}{=} e(Q_x, P_0)$ to confirm the user's partial private key Q_0 issued by KGC. For any attacker, extracting the user's identity password key x or the KGC's master key s_0 from the publicly available information is computationally hard as it is equivalent to the DLP. Similarly, in key retrieving phase, the user unblinds S_{ID}' using its password key x, so any attacker can not extract the user's private key S_{ID}.

4.2. Performance

In order to analyze the performance of our protocol, we compare the computational complexity of our protocol with Lee B et al's protocol. The notations used in the as Table-1 are as follows.

- P_e - Pairing Operation
- P_m - Multiplication Operation
- I - Inverse Operation
- h - Hash Operation
- n - Number of KPAs
- t - Number of chosen KPAs in a *t*-out-of-*n* fashion, where $t \leq n$

Table 1. Computational efforts required for Schemes

Lee et al.	Our Protocol
$(7n+6)\ P_m$	$(4t+5)\ P_m$
nI	$2I$
$(2n+3)h$	$1h$
$(6n+5)\ P_e$	$2(t+1)\ P_e$

5. Conclusion

In this paper, we propose an efficient and secure key issuing protocol using multiple authorities approach in ID-based cryptosystems, in which we suppose that for each user, there is an identity-password pair for confirming the user identity. Our protocol avoids the key escrow problem successfully. Moreover, as depicted in Table-1, our protocol saves at least 4n pairing and 2n Hash operations in comparison to LeeB et al.'s scheme.

Acknowledgment

This paper is supported by Youth Scientific Research Foundation of Beijing University of Technology under Grant No X1007016200802 and by National 973 Foundation under Grant No 2007CB311100

References

[1] Jerry Krasner, Using Elliptic Curve Cryptography (ECC) for Enhanced Embedded Security, 2004.
[2] Shamir A. Identity-based Cryptosystem and Signature Schemes[A]. Blakley G R, chaum D CRYPTO84[C]. Berlin:Springer-Verlag, 1984, 47-53.
[3] Boneh D, Franklin M. Identity based Encryption from Weil Pairing [A] Kilian J CRYPTO 2001[C]. Berlin: Springer-Verlag, 2001, 213-229.
[4] Chen L, Harrison, K Smart, N.P & Soldera D. Applications of multiple trust authorities in pairing based cryptosystems, InfraSec 2002, LNCS 2437, Springer-Verlag, pp. 260-275.
[5] Al-Riyami S, Paterson K. Certificateless public key cryptography. Advances in Cryptology-Asiacrypt'2003, Springer-Verlag, pp.452-472.
[6] Gentry C., Certificate-based encryption and the certificate revocation problem, Advances in Cryptology-EUROCRYPT 2003, Springer-Verlag, pp.272-293.
[7] Lee B., Boyd E., Daeson E., Kim K. Yang J. and Yoo S., Secure key issuing in ID-based cryptography. In proceedings of the Second Australian Information Security Workshop-AISW 2004, pp.69-74.
[8] A. Sui, S. S. M. Chow, L.C.K. Hui, S. M. Yiu, K. P. Chow, W. W. Tsang, C. F. Chong, K. H. Pun and H. W. Chan, Seperable and Anonymous Identity-Based Key Issuing without Secure Channel, in proc. Of the 11th international Comference on Parallel and Distributed Systems (ICPADS 2005),Vol. 2, pp.275-279, 2005.
[9] D.Boneh, H.Shacham, and B.Lynn, Short signatures from the Weil pairing, Advance in Cryptology – ASIACRYPT 2001, LNCS 2248, 514-532(2001).
[10] P.S.L.M. Barreto et al. Efficient algorithms for pairing-based cryptosystems. In Proc. CRYPTO 2002, LNCS vol. 2442, pp. 354-368. Springer, 2002.
[11] S.D. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate pairing. In Algorithmic Number Theory 5th International Symposium, ANTS-V, LNCS vol. 2369, pp. 324-337. Springer, 2002.