Separable and Anonymous Identity-Based Key Issuing*

Ai-fen Sui, Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu,
K.P. Chow, W.W. Tsang, C.F. Chong, K.H. Pun, H.W. Chan
Department of Computer Science, The University of Hong Kong, Pokfulam, Hong Kong
{afsui, smchow, hui, smyiu, chow, tsang, chong, pun, hwchan}@cs.hku.hk

Abstract

In identity-based (ID-based) cryptosystems, a local registration authority (LRA) is responsible for authentication of users while the key generation center (KGC) is responsible for computing and sending the private keys to users and therefore, a secure channel is required. For privacy-oriented applications, it is important to keep in secret whether the private key corresponding to a certain identity has been requested. All of the existing ID-based key issuing schemes have not addressed this anonymity issue. Besides, the separation of duties of LRA and KGC has not been discussed as well. We propose a novel separable and anonymous ID-based key issuing scheme without secure channel. Our protocol supports the separation of duties between LRA and KGC. The private key computed by the KGC can be sent to the user in an encrypted form such that only the legitimate key requester authenticated by LRA can decrypt it, and any eavesdropper cannot know the identity corresponding to the secret key.

1. Introduction

Traditional certificate-based public key infrastructure (PKI) has succeeded in many applications, but it is ill-suited for cross-enterprise usage due to the administrative burden of certificates, revocation lists, and cross-certification problems. Besides, the requirement of PKI for pre-enrollment of all users limits its widespread adoption. On the other hand, ID-based cryptosystem eliminates the need for certificates and overcomes those hurdles of PKI by allowing a public key to be derived from publicly known identifiers of the receiver, such as email addresses. A sender can send a secure message to a receiver even before the receiver obtains his/her private key from the key generation center (KGC). To read the encrypted messages, the receiver then obtains his private key from the KGC by authenticating himself in a similar way as in PKI systems. These ID-based systems are scalable, simple to administer, and users can carry out anytime/anywhere encryption.

ID-based cryptosystem was introduced in 1984 by Shamir [1]; however, the first practical encryption scheme (IBE) was not available until 2001 which was developed by Boneh and Franklin [2]. Boneh and Franklin's scheme (BF's scheme) is based on bilinear mappings. Its security is based on a natural analogue of the computational Diffie-Hellman (CDH) assumption, Bilinear Diffie-Hellman (BDH) assumption.

1.1. Motivations

One of the advantages of ID-based cryptosystems over certificate based PKI systems appear in the signature schemes with anonymity concern. Let us investigate the case for ring signature. In ring signature, any user can anonymously sign a message on behalf of a group of *spontaneously* conscripted users. By *spontaneity* we mean no previous setup is involved in the generation of this group of "signers" and we do not rely on any form of action performed before the generation of signature by non-participating signers. For non ID-based schemes, *real* spontaneity is not always possible [3]: the public key of each member of the group is required to be published by the underlying PKI before it can be used to generate the signature, i.e. the rest of the group other than the actual signer have actively enrolled the PKI (which is an "action performed before the generation of signature"). With the help of

* Full version available at Cryptology ePrint Archive, 2004/322. This research is supported in part by the Areas of Excellence Scheme established under the University Grants Committee of the Hong Kong Special Administrative Region (HKSAR), China (Project No. AoE/E-01/99), two grants from the Research Grants Council of the HKSAR, China (Project No. HKU/7144/03E and HKU/7136/04E), and two grants from the Innovation and Technology Commission of the HKSAR, China (Project No. ITS/170/01 and UIM/145).

ID-based ring signature, this assumption is no longer necessary [3]. Every people, even those who do not know what PKI is, "have" their public key implicitly.

But we need to solve another problem before getting the full solution: if an adversary can gain knowledge on which "identities" have requested the corresponding private keys, then the anonymity of these privacy-oriented signature schemes is greatly affected. Hence, it is important to have an anonymous ID-based key issuing protocol.

Though ID-based cryptosystems have many advantages over certificate based PKI systems in key distribution, they have an inherent drawback of requiring a secure channel between users and the KGC for the private key delivery from the KGC to users.

In certificate based PKI system, the duties of authentication and certificate generation are usually separated: certificate authority (CA) is responsible for the generation of certificate while local registration authorities (LRAs) are responsible for the subject authentication. The word *local* shows that these registration authorities are usually geographically distributed for the convenience of the subscribers. On the other hand, CA may be geographically far from the subscribers. In ID-based cryptosystems, similar to certificate based PKI system, we need to authenticate the user before the generation of the private key corresponding to the purported identity.

1.2. Existing ID-based Key-issuing Protocol

There are a few key ID-based key issuing protocols, most of them aimed to tackle the key escrow problem. Some of them have tackled the secure channel issue but *none* of them addressed the anonymity issue and the separation of authentication and key-issuing.

In [2], the master key of the KGC is distributed into multiple authorities, and the private key of a user is computed in a threshold manner, thus the key escrow problem of a single authority is prevented. Another proposal generates the private key of a user by adding multiple independent subkeys from multiple authorities [4]. The authorities work in a parallel mode. However, in the above two schemes, different authorities have to check and authenticate the user's identity independently, which is quite a burden to the system. Lee *et al*. proposed a new scheme [5] in which a user's private key is issued by a KGC, and its privacy is protected by multiple key privacy authorities (KPAs). The authorities work in a sequential mode. Only one authority (the KGC) has to authenticate the user and thus it greatly reduces the cost of user identification. The scheme also makes use of user-chosen secret information for constructing a secure channel for a user to retrieve his private key securely. However, it requires quite an amount of computation.

In this paper, we propose an anonymous and secure key issuing protocol without secure channel. Our construction is inspired from a variation of blind signature scheme. In the following, we first review some of the existing short signature schemes before presenting our contributions.

1.3. Short Signatures based on GDH

While researchers are trying to improve the IBE system, some new signature schemes based on the idea of IBE are proposed. In particular, Boneh *et al.* [6] introduced a short signature scheme based on the co-Gap Diffie-Hellman (co-GDH) assumption on certain elliptic and hyper-elliptic curves. The signature length is approximately 170 bits, which provides a level of security similar to that of 320-bit DSA signatures. Thus it helps to reduce the communication cost by half for transmitting the signature. This is essentially important for constrained channels. The scheme is secure against existential forgery under a chosen-message attack in the random oracle model. Generating a signature is a simple multiplication on the curve, which is very similar with the private key extraction in IBE scheme [2]. Verifying the signature is done using a bilinear pairing on the curve. Based on the short signature scheme in [6], Boldyreva [7] developed a blind signature scheme. Our scheme makes use of these ideas as well [6, 7].

2. Building Block

2.1. Bilinear Pairings and Related Problems

Bilinear pairing is an important primitive for many cryptographic schemes. Here we describe some of its key properties.

Let $(G_1, +)$ and $(G_2, \times)$ be two cyclic groups of prime order p. The bilinear pairing is given as e: $G_1 \times G_1 \rightarrow G_2$, which satisfies the followings properties:

1. Bilinearity: For all $P, Q, R \in G_1$, $e(P + Q, R) = e(P, R)e(Q, R)$, and $e(P, Q + R) = e(P, Q)e(P, R)$.
2. Non-degeneracy: $\exists\, P, Q \in G_1$ s.t. $e(P, Q) \neq 1$.

Definition 1. Given a generator P of a group G and a 3-tuple (aP, bP, cP), the Decisional Diffie-Hellman problem (DDH problem) is to decide if $c = ab$.

Definition 2. Given a generator P of a group G and a 2-tuple (aP, bP), the Computational Diffie-Hellman problem (CDH problem) is to compute abP.

Definiton 3. We define G as a Gap Diffie-Hellman (GDH) group if G is a group such that DDHP can be solved in polynomial time but no algorithm can solve CDHP with non-negligible advantage within polynomial time.

2.2. Short Blind Signature with Linkability

We call the scheme *SBSL=(BK,BS,BV),* and *BK*, *BS*, *BV* are the KeyGeneration, Signing, and Verifying algorithms respectively. The setup procedure is as follows. Let $E(F_q)$ be an elliptic curve and let $P \in E(F_q)$ be a point of prime order p, where $p \neq q,\ p \nmid q-1$. Let $G = \langle P \rangle = \langle P, 2P, ..., pP \rangle$. Then G is an abelian additive group generated by P. Define $H : \{0,1\}^* \rightarrow G$ in the way as described in [2, 6]. Let P_{sgn} be the public key of the signer. The global information is $I_{BSEC} = (G, p, P, H, P_{\text{sgn}})$. The signature scheme works as follows.

$BK(I_{BSEC})$: Pick $s \in Z_p^*$ randomly, compute $P_{\text{sgn}} = sP$, and return ($pk = (G, p, P, H, P_{\text{sgn}})$, $sk = s$).

$BS(I_{BSEC}, sk, m)$: The user picks a random number $r \in Z_p^*$, computes $\bar{M} = rH(m) \in G$, where $m \in \{0,1\}^*$, and sends $\bar{M}$ to the signer. The signer computes $\bar{\sigma} = X(s \cdot \bar{M})$ and sends it to the user, where $X(\cdot)$ denotes the *x*-coordinate of the element. Note that $\bar{\sigma} \in F_q$. User then computes the signature $\sigma = r^{-1} \cdot \bar{\sigma}$.

$BV(pk, m, \sigma)$: The verifying process is similar to that in [6]. Find a $y \in F_q$ such that $S = (\sigma, y)$ is a point of order p in $E(F_q)$. Test if either $e(S,P) = e(H(m), P_{\text{sgn}})$ or $e(S,P)^{-1} = e(H(m), P_{\text{sgn}})$, where e is a Weil Pairing, a bilinear map constructed over elliptic curves [2].

2.3. Analysis

We use similar techniques in [7] to prove the security of the short blind signature. Two main properties, namely blindness and security against *one-more-forgery* [8]. *Blindness* means that the signer and also any other third party should not learn any information about the messages the user obtains signatures on. *Unforgeability* means that the user who has been engaged in l runs of the protocol should not be able to obtain more than l signatures.

Blindness. Since r is chosen randomly from Z_p^*, $\bar{M} = rH(m)$ is also a random element in the group G. The signer receives only random information that is independent of the output of the user (m, σ).

Unforgeability. This property provides the security of our ID-based key issuing protocol in Section 3.2. It means that there exists no polynomial-time adversary A with non-negligible advantage $Adv_l^{BSEC}(A)$, where $Adv_l^{BSEC}(A)$ is the probability of A to output l valid message-signature pairs while the number of invoked blind signing protocols is strictly less than l.

To prove the *unforgeability* of the blind signature, [7] defines the chosen-target CDH assumption and proved an equivalence relation between the unforgeability and chosen-target CDH assumption. The security of our scheme can be proven in a similar way.

Theorem 1. *If the chosen-target CDH assumption is valid in G, then SBSL is secure against one-more forgery chosen message attack.*

Linkability. We remark that the scheme proposed is indeed linkable, i.e. the signature issuer can link the unblended signature presented by the signature requester later with the previous invocation of the blind signature issuing protocol. However, we will discuss the linkability is not a concern if the scheme is applied in anonymous ID-based key issuing protocol.

3. Separable and Anonymous Key Issuing

It is unavoidable for a trusted party to authenticate the identity of the user in an offline manner. However, this authentication authority may not be necessary the same party as the KGC for generation of private key. This is where the concept of local registration authority (LRA) comes to play. A one-time password can be established between the LRA and the user after the offline authentication. Then this password (may be in the form of a hash value instead of the password itself) together with the identity of the user is redirected to the KGC. With the help of this information, KGC can know the identity associated to the private key to be requested when the user present this one-time password to the KGC. This information also helps the KGC to check the correctness of the "blinded" identity.

Note that the one-time password should be stored securely by the user but it is not necessary to be sent in encrypted form if the key issuing protocol can be implemented as an all-or-none transaction.

We name our protocol as SAKI and let A be the user.

The setup procedure is a probabilistic polynomial algorithm, run by KGC, that takes a security parameter k , and returns *params* (system parameters) and the master-key. Let G be a GDH group of prime order p. Public information is $I_{SAKI} = (G, p, H, P_{KGC})$. P is generator of G and $H:\{0,1\}^* \rightarrow G$ is a one-way hash function and $Q_A = H(id_A)$. We use the *MapToPoint* method in [6] to construct this hash function. $P_{KGC} = sP$ is the system public keys.

The key generation procedure is a probabilistic polynomial algorithm that takes as input *params* , the master-key and an arbitrary $ID \in \{0,1\}^*$; and returns a private key s_{ID} . Here *password* is the user' s chosen password during off-line authentication and the tuple (*ID, password*) is stored in KGC' s database of "pending private key". KGC may choose to pre-compute the value of $\underline{e}(H(ID), H(password))$.

1. A: selects a random number r, $A \rightarrow KGC$: $Q = rH(ID)$, $T = r^{-1}H(password)$.
2. KGC: checks the validity of the request by checking whether $e(Q,T) = e(H(ID), H(password))$ holds for a certain tuple in KGC' s database.
3. KGC: computes $s_1 Q$. $KGC \rightarrow A$: $S = sQ$.
4. A: verifies the blinded private key by checking $e(S, P) = e(Q, P_{KGC})$. If it holds, A unblinds the encrypted private key and obtains $sH(ID)$.

Then the user can delete *password*. The KGC can also remove the tuple *(ID, password)* from the database, so the database only holds the data for "private key to be issued". It will not grow to the gigantic size of the certificate repository of traditional PKI.

3.1. Analysis

Since our scheme preserves the property that the public key can be determined by the identity of the user, it can be used with existing ID-based cryptosystems. Now we discuss the efficiency, confidentiality, soundness and the blindness of SAKI. We also provide extensions to remove the inherent key-escrow problem of ID-based cryptosystem.

Efficiency. On users' side, 2 scalar multiplications, 2 modular inversions and 2 pairing computations are needed (notice that these 2 pairing computations are also necessary for checking the validity of the private key obtained in other key issuing protocols). On KGC side, 1 pairing computation is needed (if pre-computations are performed), and 1 scalar multiplication is needed for the private key generation (again, which is also needed in other key issuing protocols). Note that the user does not need to perform pairing computations to decrypt the encrypted private key, while it is necessary in the previous scheme [5]. On the other hand, KGC does not need to have pairing computation for encryption of the private key, but it is needed in [5]. In our scheme, the pairing computation is needed for the sake of anonymity requirement only.

Confidentiality. The SAKI scheme is directly inspired from the above blind signature scheme. It is obvious that the blinding process cannot serve as a semantically secure encryption scheme against adaptive chosen ciphertext attack. However, in our scenario, the things to be encrypted are the private keys on users' demands. It is reasonable to assume that there exists no oracle helping the adversary to launch the adaptive chosen ciphertext attack. Moreover, the "encryption key" r is used once only. So even in the case some partial information has leaked, it cannot help in another invocation of the protocol.

With a careful design of $H:\{0,1\}^* \rightarrow G$, a user' s identity information is mapped to a point $Q_{ID} = H(id_{ID})$ on G . The order of Q_{ID} is the same as that of G , say p, a prime number large enough that the elliptic curve is secure. Due to ECDLP (the Elliptic Curve Diffie-Hellman Problem), an attacker cannot derive w from wQ . So only the legitimate user who knows the blinding parameter can unblind the messages and retrieve the private key.

The messages over the channel are not part of the private key, in contrast with BF' s basic scheme [2], and its follow-on schemes, such as BF' s threshold scheme [2] and Chen' s parallel subkeys addition scheme [4]. The messages can be transmitted in plaintext and secure channels are not needed.

Soundness. It is not possible for the user to request for any private key which does not correspond to his/her identity by the checking in Step 2 of the protocol.

Blindness. From the blindness property of the blind signature, it is easy to see that our ID-based key issuing protocol achieves the anonymity requirement. Now we discuss why a linkable blind signature is sufficient for our construction. In anonymous ID-based key issuing protocol, we only want to keep the blindness of the message (i.e. the identity) against any third party (other than the KGC and the user). The signature issuer (the KGC) should have the knowledge of the identity of the signature (private key) requester. Linkability of the scheme does not give any advantage to the KGC or incur any disadvantage to the user.

3.2. Removing Key Escrow

Now we present the extension of our proposed SAKI to support multiple KGC so as to avoid the key-escrow problem.

Public information becomes $I_{SAKI} = (G, p, H, P_{KGC1} = s_1P_, P_{KGC2} = s_2P)$ where (s_1, P_{KGC1}) is the private-public key of the first KGC (*KGC1*) and (s_2, P_{KGC2}) is the private-public key of the second KGC (*KGC2*). $P_{KGC} = s_1 s_2P$ is the system public keys.

The key generation procedure takes *params* , the KGC private key and an arbitrary $ID \in \{0,1\}^*$ as input; and returns a user private key s_{ID} . Here *password* is the user' s chosen password during off-line authentication and the tuple (*ID*, *password*) (possibly with pre-computed result $e(H(ID), H(password))$).is stored in KGC1 and KGC2' s databases. The order of interactions between user *A* and the KGCs does not really matter.

1. *A*: selects a random number r_1, $A \rightarrow KGC1$: $Q_1 = r_1H(ID)$, $T_1 = r_1^{-1}H(password)$.
2. *KGC1*: checks the validity of the request by checking whether $e(Q_1, T_1) = e(H(ID), H(password))$ holds for a certain tuple in *KGC1*'s database.
3. *KGC1*: computes s_1Q and s_1T. $KGC1 \rightarrow A$: $S_1 = s_1Q$, $\sigma'_1 = s_1T_1$,
4. *A*: verifies the blinded partial private key by checking $e(S_1,,P) = e(Q_1, P_{KGC1})$. And verifies the KGC1' s signature on the password by $e(\sigma'_1,,P) = e(T_1, P_{KGC1})$ .If both of them hold, *A* unblinds the encrypted partial private key and the *KGC1*'s blinded signature on the password to obtain the partial private key $s_1H(ID)$ and *KGC1*'s signature $\sigma_1 = s_1H(password)$.
5. *A*: selects a random number r_2, $A \rightarrow KGC2$: σ_1, $Q_2 = r_2s_1H(ID)$, $T_2 = r_2^{-1}H(password)$.
6. *KGC2*: checks the validity of the request by checking whether $e(Q_2, T_2) = e(H(ID), \sigma_1)$ holds and checks the validity of *KGC1*' s signature by verifying $e(\sigma_1, P) = e(H(password), P_{KGC1})$ where *password* is obtained from *KGC2*'s database (possibly from pre-computed results).
7. *KGC2*: computes s_2Q_2. $KGC2 \rightarrow A$: $S_2 = s_2Q_2$.
8. *A*: verifies the blinded private key by checking $e(S_2 P) = e(Q_2 P_{KGC2})$. If it holds, *A* unblinds the encrypted private key and obtains the final private key $S = s_2 s_1H(ID)$.

Notice that the KGCs blindly sign on the "message" *password* chosen by the user in the above protocol (in the form of the short signature[6]), so some restrictions (e.g. padding with "PW:") is preferred for the password.

4. Conclusion

We proposed an anonymous ID-based key issuing scheme. Our scheme is separable: the authentication and the private key generation can be computed by two different entities. User chosen information contributes for the secure channels. Since the user' s public key is solely dependent on the publicly available information, the scheme can work with other existing ID-based cryptosystems and preserving their advantages.

References

[1] A. Shamir, "Identity-based Cryptosystems and Signature Schemes", *Crypto'84*, LNCS 196 pp. 47-53.

[2] D. Boneh, F. Franklin, "Identity-based Encryption from the Weil Pairing", *Crypto '01*, LNCS 2139, pp. 213-229.

[3] Sherman S.M. Chow, S.M. Yiu, Lucas .C.K. Hui, "Efficient Identity-based Ring Signature", *ACNS 05.* LNCS 3531, to appear.

[4] L. Chen, K. Harrison, N.P. Smart, D. Soldera, "Applications of Multiple TAs in Pairing Based Cryptosystems", *InfraSec 02*, LNCS 2437, pp. 260-275.

[5] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, S. Yoo, "Secure Key Issuing in ID-Based Cryptography", *2nd Australasian Information Security Workshop*, pp. 69-74

[6] D. Boneh, B. Lynn, H. Shacham, "Short Signatures from the Weil Pairing", *Asiacrypt 01*, LNCS 2248, pp.514-532.

[7] A. Boldyreva, "Threshold Signature, Multisignature, and Blind Signature Schemes based on the Gap Diffie-Hellman-Group Signature Scheme", *PKC 03*, LNCS 2567, pp. 31-46

[8] D. Pointcheval, J. Stern, "Security Arguments for Digital Signatures and Blind Signatures", *Journal of Cryptology*, 13(3): 361-396, 2000.