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 for authentication and private key computation has not been discussed as well. In this paper, based on a signature scheme similar to a short blind signature, 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.

Keywords. Identity-based cryptography, bilinear pairings, GDH groups, key issuing, anonymity, privacy, secure channel, separation of duties

---

* An extended abstract of this paper appeared in the 1st International Workshop on Security in Networks and Distributed Systems (SNDS 2005), in conjunction with 11th International Conference on Parallel and Distributed Systems (ICPADS 2005), July 20-22, 2005, Fukuoka, Japan. Proceedings. IEEE Computer Society.

+ 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).

^ Corresponding author

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 relies 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 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 so 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 delivery of the private key 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 Key Issuing Protocol in ID-Based Systems

There are a few key ID-based key issuing protocols, most of them aimed to tackle the key escrow problem of ID-based systems. 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.

Gentry [6] proposed a certificate-based encryption using some user-chosen secret information. Certificateless public key cryptography [7] successfully removed the necessity of certificate and use user-chosen information. But they both lose the advantages of ID-based cryptography since in both cases; the public key is not solely determined by the publicly available information of the user's identity.

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.

The rest of the paper is organized as follows. Some background on bilinear map and relevant concepts that we use in our scheme are introduced in Section 2. Section 3 describes our building block in the key-issuing protocol. In Section 4, we describe our ID-based key issuing scheme based on short blind signature over the GDH groups proposed in Section 3. The basic protocol supports the separation of duties for au-

thentication and private key computation. We also extend the protocol to address the key-escrow problem. Finally, Section 5 concludes the paper.

2 Preliminaries

We summarize some concepts of GDH assumption and short signature in this section. We use a similar set of notations as in [8] and [9]:

1. G_1 and G_2 are two cyclic groups of prime order p.
2. g_1 is a generator of G_1 and g_2 is a generator of G_2.
3. ψ is an isomorphism from G_2 to G_1, with $\psi(g_2) = g_1$.
4. e is a bilinear map $e: G_1 \times G_2 \rightarrow G_T$, where G_T is a group of order p.

Bilinear pairing is an important primitive for many cryptographic schemes. When $G_1 = G_2$ and $g_1 = g_2$, one could take ψ to be the identity map. Here we describe some of its key properties.

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

When $G_1 ? G_2$ and $g_1 = g_2$, we consider their "co-" variants which are defined in a similar way. We define a *Gap co-Diffie-Hellman group (co-GDH group)* pair to be a pair of groups (G_1, G_2) on which co-DDH is easy to compute but co-CDH is hard. Two groups (G_1, G_2) are said to be a (t, ε) co-GDH pair if they satisfy the following properties:

1. The group action on both G_1 and G_2 and the map ψ from G_2 to G_1 can be computed in constant number of steps.
2. The Decision co-Diffie-Hellman problem on (G_1, G_2) can be solved efficiently.
3. No algorithm can (t, ε)-break the co-CDH problem on (G_1, G_2), that is, no algorithm running in time at most t can solve co-CDH with an advantage at least ε.

When (G_1, G_1) is a (t, ε) co-GDH pair, we say G_1 is a (t, ε)-Gap-Diffie-Hellman group (*GDH group*). The first example of a GDH group is given in [12] and more details on the existence and composition of GDH groups can be found in [2, 8, 13].

Consequently, if two groups (G_1, G_2) are a (t, ε)-bilinear group pair, then they are also a $(t/2, \varepsilon)$ co-GDH group pair [12].

2.2 Short Signature and Blind Signature

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.* [8] 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 [8], Boldyreva [9] developed a blind signature scheme. Our scheme makes use of these ideas developed in [8, 9].

Remark. Recently, both [10] and [11] tried to improve the scheme in [8] by providing a more efficient system generating signatures of the same length. Their security is based on stronger assumptions. Key generation is identical to that in [8], except that they use a simpler hash function, $H: \{0,1\}^* \rightarrow Z_p$, which is a great simplification compared to *MapToPoint* mapping in [8]. However, it is not trivial how these schemes can be used in our construction. We leave this as an open problem.

Using the Weil and Tate pairings, [8] obtains co-GDH groups from a family of non-supersingular curves over a prime finite field to construct short signatures. Signature generation is just a simple multiplication on an elliptic curve and is faster than RSA signature generation. Verification requires two computations of the bilinear map and is slower than RSA signature verification.

Security of the signature scheme follows from the hardness of co-GDH on (G_1, G_2). Note that when $G_1 = G_2$, the security is based on the standard CDH assumption in G_1. Boldyreva [9] proposed a blind signature which works in the special case $G_1 = G_2$. The scheme is proved to be blind and secure *against one-more-forgery* (based on chosen-target CDH assumption, to be defined later). In this paper, the blind signature is revised to construct an ID-based key issuing scheme.

3 Building Block

Due to the nice properties of the above short signature scheme [8], our scheme proposed below is simple and efficient.

3.1 Short Blind Signature (SBS)

We call the scheme *SBS=(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 $p \neq q, p \mid q-1$. 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, 8]. 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 [8]. 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]. This is because that the signature σ could have come from either the point S or $-S$.

3.2 Analysis

We use similar techniques in [9] to prove the security of the short blind signature. Two main properties, namely blindness and security against *one-more-forgery* [14, 15], which is a special form of unforgeability, are considered. *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 blind signing 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 $Adv_I^{BSEC}(A)$, where $Adv_I^{BSEC}(A)$ 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, [9] defines the chosen-target CDH assumption and proved an equivalence relation between the unforgeability and chosen-target CDH assumption. Here we define *the chosen-target CDH assumption* for our blind signature in the similar way.

Definition 1. Let $G = \langle P \rangle$ be a group of order p. Let s be a random element of Z_p^* and $P_{\text{sgn}} = sP$. Let H be a random instance of a hash function family $[\{0,1\}^* \to G]$. Define the target oracle T_G that returns random points $R_i \in G$ and the helper oracle $cts(\cdot)$. The adversary B is given (p, P, H, P_{sgn}) and has access to T_G and $cts(\cdot)$. Let ($q_{T,} q_H$) be the number of queries B made to T_G and $cts(\cdot)$. The advantage of B attacking the chosen-target CDH problem $Adv_G^{ctCDH}(B)$ is defined as the probability of B to output l pairs $((V_1, j_1),...(V_l, j_l))$, where for $1 \le i \le l$, $\exists 1 \le j_i \le q_T$, such that $V_i = sR_{j_i}$ (all V_i are distinct) and $q_H < q_T$.

The chosen-target CDH assumption states that there is no polynomial-time adversary B with non-negligible $Adv_G^{ctCDH}(B)$.

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

The proof is to construct a polynomial-time adversary B for the chosen-target CDH problem such that $Adv_I^{BSEC}(A) = Adv_G^{ctCDH}(B)$.

Proof:

The adversary A has access to a blind signing oracle $s(\cdot)$. We analyze security of *SBS* in the random oracle model, so A is also given access to the random hash oracle $H(\cdot)$. We now construct the algorithm B to simulate A in order to solve the chosen-target CDH problem. B is given $(p, P, H, P_{\text{sgn}})$, T_G and $cts(\cdot)$. B first provides A with the public key $pk = (p, P, H, P_{\text{sgn}})$. B has to simulate the random oracle hash oracle $H(\cdot)$ and the blind signing oracle $s(\cdot)$.

1. When A makes a new hash oracle query, B forwards it to its target oracle T_G, returns the reply to A and adds this query and the reply to the stored list of such pairs.

2. When A makes a query to the blind signing oracle $s(\cdot)$, B forwards it to its helper oracle $cts(\cdot)$ and returns the reply to A.

At some point, A outputs a list of message-signature pairs $((m_1,\sigma_1),...,(m_l,\sigma_l))$. For each $1 \le i \le l$, B finds m_i in the list of stored hash oracle queries and replies $(\sigma_1, j_1),...,(\sigma_l, j_l)$, where j_i be the index of the found pair. From A's viewpoint, the above simulation is indistinguishable from the real protocol, and B is successful only if A is successful. Thus $Adv_I^{BSEC}(A) = Adv_G^{ctCDH}(B)$.

4 Separable and Anonymous ID-based Key Issuing

In this section, we present our separable and anonymous ID-based key issuing scheme. We denote it as SAKI. In SAKI, the KGC and the user cooperate to generate the private key for the user using the above short blind signature. Let A be a user and KGC be the trusted authority.

4.1 Proposed ID-Based Key Issuing Protocol (SAKI)

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.

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 $H:\{0,1\}^* \to G$ is a one-way hash function and $Q_A = H(id_A)$. We use the *MapToPoint* method in [8] 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 sQ. $KGC \rightarrow A$: $S = sQ$.
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* after obtained the private key. The KGC can also remove the tuple *(ID, password)* from the database after the protocol, so the database is always holding the tuples corresponding to "private key to be issued". It will not grow to the gigantic size of the certificate repository of traditional certificate based system.

4.2 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, in contrast with some of the non ID-based solutions [6, 7]. 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 of SAKI. 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 of SAKI. 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 of SAKI. It is not possible for the user to request for any private key which does not correspond to his/her identity by the validity check of KGC in Step 2 of the protocol.

Blindness of SAKI. From the blindness property of the blind signature, it is easy to see that our ID-based key issuing protocol achieves the anonymity requirement.

4.3 Separable and Anonymous ID-based Key Issuing without Key-Escrow

One major problem of the ID based key scheme is the key escrow, i.e. the trusted authority can impersonate a user. Here we present the extension of our proposed SAKI to support multiple KGC so as to avoid the key-escrow problem.

Let P is generator of G and $H:\{0,1\}^* \rightarrow G$ is a one-way hash function and $Q_A = H(id_A)$. Public information is $I_{SAKI} = (G, p, H, P_{KGC1} = s_1P, P_{KGC2} = s_2P)$ 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*). $P_{KGC} = s_1 s_2 P$ is the system public keys.

The key generation procedure is a probabilistic polynomial algorithm that takes as input *params*, the KGC private key and an arbitrary $ID \in \{0,1\}^*$; 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*) is stored in KGC1 and KGC2's databases of "pending private key" (possibly with pre-computation as the basic version). 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_1 and s_1T_1. $KGC1 \rightarrow A$: $S_1 = s_1Q_1$, $\sigma'_1 = s_1T_1$,
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 on the password $\sigma_1 = s_1H(password)$.
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* → *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 $S = s_2 s_1 H(ID)$.

Notice that the KGCs blindly sign on the "message" *password* chosen by the user in the above protocol (the resulting signature is in the form of the short signature we reviewed), so preferably some restrictions (e.g. padding the password with the keyword "PASSWORD: ") is necessary for the password.

5 Conclusions

An ID-based key issuing scheme, combining the properties of anonymity and confidentiality, is proposed in the paper. Moreover, our scheme is separable: the authentication and the private key generation can be computed by two different entities. The scheme is based on a short blind signature. User chosen information contributes for blinding purpose to eliminate the need for secure channels. The security relies on the Gap Diffie-Hellman assumptions over elliptic curves. 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. Shamir, A.: Identity-based Cryptosystems and Signature Schemes. Proceedings of Crypto'84, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, (1984) pp. 47-53
2. Boneh, D., Franklin, F.: Identity-based Encryption from the Weil Pairing. Advances in Cryptology - Crypto'2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, Berlin, 2001, pp.213-229. Also appeared in Society for Industrial and Applied Mathematics (SIAM) J. Comput. 2003, vol. 32, no. 3, pp. 586-615
3. Chow, Sherman S.M., Hui, Lucas C.K., Yiu, S.M.: Identity-based Threshold Ring Signature. In 7th International Conference on Information Security and Cryptology (ICISC 2004), Lecture Notes in Computer Science, Seoul, Korea, December 2004. Springer-Verlag. Also available at Cryptology ePrint Archive, Report 2004/179.
4. Chen, L., Harrison, K., Smart, N.P., Soldera, D.: Applications of Multiple Trust Authorities in Pairing Based Cryptosystems. InfraSec 2002, Lecture Notes in Computer Science, Vol. 2437, Springer-Verlag, Berlin, 2002, pp. 260-275.

5. Lee, B., Boyd, C., Dawson, E., Kim, K., Yang, J., Yoo, S.: Secure Key Issuing in ID-Based Cryptography. ACM Second Australasian Information Security Workshop (AISW 2004), New Zealand, Jan. 2004, pp. 69-74
6. Gentry, C.: Certificate-based Encryption and the Certificate Revocation Problem. Advances in Cryptology - Eurocrypt 2003, Lecture Notes in Computer Science, Vol. 2656, Springer-Verlag, Berlin, 2003, pp. 272-293.
7. Al-Riyami, S., Paterson, K.: Certificateless Public Key Cryptography. Advances in Cryptology - Asiacrypt'2003, Lecture Notes in Computer Science, Vol. 2894, Springer-Verlag, Berlin, 2003, pp. 452-473
8. Boneh, D., Lynn, B., Shacham, H.: Short Signatures from the Weil Pairing. Advances in Cryptology - Asiacrypt'2001, Lecture Notes in Computer Science, Vol. 2248, Springer-Verlag, Berlin, 2001, pp. 514-532.
9. Boldyreva, A.: Efficient Threshold Signature, Multisignature, and Blind Signature Schemes, Based on the Gap Diffie-Hellman Group Signature Scheme. Proceedings of Public Key cryptography - PKC2003, Lecture Notes in Computer Science, Vol. 2567, Spring-Verlag, Berlin, 2003, pp. 31-46
10. Boneh, D., Boyen., X.: Short Signatures without Random Oracles. Advances in Cryptology - Eurocrypt 2004, Lecture Notes in Computer Science, Vol. 3027, Springer-Verlag, Berlin, 2004, pp.56-73
11. Zhang, F., Safavi-Naini, R., Susilo, W.: An Efficient Signature Scheme from Bilinear Pairings and Its Applications. In Proceedings of PKC 2004, Lecture Notes in Computer Science, Vol. 2947, Springer-Verlag, Berlin, 2004, pp. 277-290
12. Joux, A.: A One-round Protocol for Tripartite Diffie-Hellman. Algorithmic Number Theory Symposium-ANTS-IV, Lecture Notes in Computer Science, Vol. 1838, Springer-Verlag, 2000. pp. 385-394
13. Joux, A., Nguyen, K.: Separating Decision Diffie-Hellman from Diffie-Hellman in Cryptographic Groups. IACR Eprint Archive. Available from http://eprint.iacr.org/2001/003, 2001.
14. Bellare, M., Namprempre, C., Pointcheval, D., Semanko, M.: The One-More-RSA Inversion Problems and the Security of Chaum's Blind Signature Scheme, Journal of Cryptology, Vol. 16, No. 3, 2003, pp. 185-215. Extended abstract of the preliminary version appeared in Financial Cryptography 01, Lecture Notes in Computer Science, Vol.. 2339, Springer-Verlag, 2001
15. Pointcheval, D., Stern, J.: Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology, 13(3): 361-396, 2000