Secure and Anonymous Identity-Based Key Issuing without Secure Channel

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 Road, Hong Kong
{afsui, smchow, hui, smyiu, chow,
tsang, chong, pun, hwchan}@cs.hku.hk

Abstract. In identity-based (ID-based) cryptosystems, the key generation center (KGC) needs to send the private keys to users and therefore, a secure channel is required. On the other hand, for some applications, it is important to keep in secret whether the private key corresponding to a certain identity has been requested. Existing ID-based key issuing schemes have neither addressed the issue of removing the secure channel requirement nor the anonymity requirement. In this paper, based on a signature scheme similar to a blind short signature, we propose a novel ID-based key issuing scheme from Weil Pairing on elliptic curves that the private key can be sent to user in an encrypted form such that only the key requester can decrypt it, while eavesdropper cannot know the identity corresponding to the secret key.

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

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 D. Boneh and F. 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.

One of the advantages of ID-based cryptosystems over certificate based PKI systems appear in privacy-oriented signature scheme like ring signature. For non ID-based schemes, real spontaneity is not always possible: 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 [3]. But it give rise to another problem: 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.

1.1 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. Existing solutions mainly use two approaches: (1) Using multiple authorities [2, 4-5] so that no single authority can deduce the private key of user; (2) Using user-chosen secret information [5-7] when generating the private key so that the private key is not known to the KGC.

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 key escrow problem of a single authority is prevented. On the other hand, the private key of a user is generated by adding multiple independent subkeys from multiple authorities in [4]. The authorities work in a parallel mode. However, in the above two schemes, different authorities have to check and authenticate 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 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. [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 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 signatures. In the following, we first review some of the existing short signature schemes before presenting our contributions.

1.2 Short Signatures Based on GDH Groups

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, which uses GDH groups instead of co-GDH groups. It turns out that their constructions are much simpler, more efficient and have more useful characteristics. In fact, our scheme makes use of the ideas of the signature scheme developed in [8, 9].

Remark. Recently, both [10] and [11] try 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.

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. In Section 3, we describe our ID-based key issuing scheme based on short blind signature over the GDH groups. Section 4 analyzes the security and efficiency of the proposed scheme. 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. y is an isomorphism from G_2 to G_1, with $y(g_2) = g_1$.
4. e is a bilinear map $e: G_1 \times G_2 \rightarrow G_T$, where G_T is a group of order p.

2.1 Gap Diffie-Hellman (GDH) Groups and Bilinear Maps

GDH Group. We first give some definitions as in [8].

Computational co-Diffie-Hellman (co-CDH) on (G_1, G_2): Given $g_2, g_2^a \in G_2$ and $h \in G_1$, compute $h^a \in G_1$.

Decision co-Diffie-Hellman (co-DDH) problem on (G_1, G_2): Given $g_2, g_2^a \in G_2$ and $h, h^b \in G_1$, output "yes" if $a = b$ and "no" otherwise. When the answer is "yes", we say that (g_2, g_2^a, h, h^a) is a co-Diffie-Hellman tuple.

When $G_1 = G_2$ and $g_1 = g_2$, one could take y to be the identity map. The above problems reduce to standard CDH and DDH [2].

Next 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, e) co-GDH pair if they satisfy the following properties:

1. The group action on both G_1 and G_2 and the map y 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, e)-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 e.

When (G_1, G_1) is a (t, e) co-GDH pair, we say G_1 is a (t, e)-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].

Bilinear Map. Currently, the only examples of GDH groups arise from bilinear maps. Let G_1 and G_2 be two groups as above, with a multiplicative group G_T such that $|G_1| = |G_2| = |G_T|$. A bilinear map is a map $e: G_1 \times G_2 \rightarrow G_T$ with the following properties:

1. Bilinear: for all $u \in G_1, v \in G_2$, and $a, b \in Z$, $e(u^a, v^b) = e(u, v)^{ab}$.
2. Non-degenerate: $e(g_1, g_2) \neq 1$.

An efficiently computable bilinear map e provides an algorithm for solving the co-DDH problems by using the following property: $a = b \bmod p \Leftrightarrow e(h, g_2^a) = e(h^b, g_2)$. Consequently, if two groups (G_1, G_2) are a (t, e)-bilinear group pair, then they are also a $(t/2, e)$ co-GDH group pair [12].

2.2 Short Signature and Blind Short Signature

We denote the basic signature scheme of [8] as *GS=(K,V,S)*, which comprises three algorithms, KeyGeneration (*K*), Signing (*S*), and Verifying (*V*). It works on co-GDH groups (G_1, G_2). A full-domain hash function $H:\{0,1\}^* \rightarrow G_1$ is used. The global information I_{GS} contains { G_1, G_2, g_1, g_2, p, H }. Details of the algorithms *K, S, V* are as follows:

$K(I_{GS})$: Pick random $x \in Z_p^*$, and compute $y = g_2^x$. Return $(pk = (p, g_2, H, y)$, $sk = x)$

$S(I_{GS}, sk, m)$: Given a message $m \in \{0,1\}^*$, compute $h = H(m) \in G_1$, and the signature $s = h^x \in G_1$. Output (m, s)

$V(pk, m, s)$: Compute $h = H(m) \in G_1$ and verify that (g_2, y, h, s) is a valid co-Diffie-Hellman tuple (i.e. verify co-DDH(g_2, y, h, s) using bilinear map). If so, output valid.

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] proposes a blind signature *BGS=(BK,BS,BV)* which works in the special case $G_1 = G_2$. The algorithms *BK* and *BV* are the same as those of short signature on G. The blind signing algorithm *BS* is defined as follows. User holds a public key $pk = (p, g, H, y)$. In order to blindly sign a message $m \in \{0,1\}^*$, user picks a random number $r \in Z_p^*$, computes $\bar{m} = H(m) \cdot g^r$ and sends it to the signer. The signer knows $I_{BGS} = (p, g, H)$ and $sk = x$. The signer computes $\bar{s} = (\bar{m})^x$ and sends it to user. User then computes $s = \bar{s} \cdot y^{-r}$ and outputs (m, s). The scheme is proved to be blind and secure *against one-more-forgery*. In this paper, the blind signature is revised to work on elliptic curves to construct an ID-based key issuing scheme.

3 Proposed ID-Based Key Issuing Protocol

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

3.1 Blind Short Signature over Elliptic Curves (BSEC)

We call the scheme *BSEC=(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, 8]. Let P_{sgn} be the public key of the signer. The global information is $I_{BSEC} = (G, p, P, H, P_{\mathrm{sgn}})$. The signature scheme works as follows.

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

$BS(I_{BSEC}, sk, m)$: A 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 $\bar{s} = X(s \cdot \bar{M})$ and sends it to user, where $X(\cdot)$ denotes the *x*-coordinate of the element. Note that $\bar{s} \in F_q$. User then computes the signature $s = r^{-1} \cdot \bar{s}$.

$BV(pk, m, s)$: The verifying process is similar to that in [8]. Find a $y \in F_q$ such that $S = (s, y)$ is a point of order p in $E(F_q)$. Test if either $e(S,P) = e(H(m), P_{\mathrm{sgn}})$ or $e(S,P)^{-1} = e(H(m), P_{\mathrm{sgn}})$, where e is a Weil Pairing, a bilinear map constructed over elliptic curves [2]. This is because that the signature s could have come from either the point S or $-S$.

Security of Blind Signature. We use similar techniques in [9] to prove the security of the blind short 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 user obtains signatures on. *Unforgeability* means that user that 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, s).

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 BSEC 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 BSEC 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_{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 $((m_1, s_1),...,(m_l, s_l))$. For each $1 \le i \le l$, *B* finds m_i in the list of stored hash oracle queries and replies $(s_1, j_1),...,(s_l, j_l)$, 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 $Adv_I^{BSEC}(A) = Adv_G^{ctCDH}(B)$.

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.

3.2 Secure and Anonymous ID-based Key Issuing (SAKI)

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

The setup procedure is a probabilistic polynomial algorithm, run by TAs, 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 $I_{SAKI} = (G, p, H, P_{TA})$. 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 the hash function. $P_{TA} = sP$ 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 ID is a user' s identity and works as the user's public key.

1. A: selects a random number r, A→TA: rQ_A, rP_{TA}.
2. TA: checks the validity of the request by checking whether $e(rQ_A, P_{TA}) = e(H(id_A), rP_{TA})$.
3. TA: computes srQ_A. TA→User A: srQ_A.
4. A: verifies the blinded private key by checking $e(srQ_A, P) = e(rQ_A, P_{TA})$. If it holds, A unblinds the private key and obtains sQ_A.

Careful reader may find that TA knows the identity of the private key requester before the execution of the protocol. However, it is unavoidable for TA to authenticate the identity of user in an offline manner. A one-time password can be issued by the TA to user after the offline authentication. With the help of this password, TA can know the identity associated to the private key to be requested when user present this one-time password to the TA. Note that the one-time password should be stored securely by 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.

4 Analysis

Since our scheme is really ID-based, 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.

Efficiency of SAKI. On user's side, 3 scalar multiplications, 1 modular inversion and 2 pairing computations are needed. On TA side, 1 scalar multiplication and 2 pairing computations are needed. Our scheme can operate on co-GDH groups, but that will cost more computation.

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 $H:\{0,1\}^* \to G$, 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 user to request for any private key which does not correspond to his/her identity by the validity check of TA 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 achieve anonymity. 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 user). The signature issuer (i.e. the KGC) should have the knowledge of the identity of the signature (i.e. private key) requester. Linkability of the scheme does not give any advantage to the KGC or incur any disadvantage to user.

5 Conclusions

An ID-base Key issuing scheme, combining the properties of anonymity and confidentiality, is proposed in the paper. The scheme is based on a blind short 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 user' s public key is solely dependent on the publicly available information, the scheme is a true ID-based system and can work with any existing ID-based cryptosystems, preserving the advantages of ID-based systems.

References

1. Shamir, A.: Identity-base Cryptosystems and Signature Schemes. Proc. of Crypto'84, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, (1984) 47-53
2. Boneh, D., Franklin, F.: Identity-based Encryption from the Weil Pairing. Advances in Cryptology - Crypto'2001, LNCS 2139, Springer-Verlag, Berlin, 2001, pp.213-229. Also appeared in SIAM (Society for Industrial and Applied Mathematics) 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, LNCS 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, LNCS 2656, Springer-Verlag, Berlin, 2003, pp. 272-293.
7. Al-Riyami, S., Paterson, K.: Certificateless Public Key Cryptography. Advances in Cryptology - Asiacrypt'2003, LNCS 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, LNCS 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, LNCS 2567, Spring-Verlag, Berlin, 2003, pp. 31-46
10. Boneh, D., Boyen., X.: Short Signatures without Random Oracles. Advances in Cryptology - Eurocrypt 2004, LNCS 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, LNCS 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, LNCS 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, LNCS. 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