A New Type of Group Signature Scheme

ZHONG Jun, HE Da-Ke

（School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China）

Abstract: On the basis of BB short signature scheme, this paper derives a new signature scheme, from which we construct a new kind of group signature scheme. The security of the new group signature scheme is based on the q-Strong Diffie-Hellman assumption and the Decisional Diffie-Hellman assumption in the random oracle model. The length of the new group signature is a little longer than that of BBS short group signature. However, in the new group signature scheme, giving certificates and private keys to group members do not need any third trusted party, while in BBS short group signature scheme it does need.

Key Words: Signature Group Signature Information Security

CLC: TP309

1 Introduction

In 1991 Chaum and van Heyst put forth the concept of a group signature scheme[8]. Participants are group members, group manager. And as for group manager, it consists of a membership manager, and a revocation manager. A group signature scheme allows a group member to sign messages anonymously on behalf of the group. More precisely, signatures can be verified with respect to a single public key of the group and do not reveal the identity of the signer. The membership manager is responsible for the system setup and for adding group members while the revocation manager has the ability to revoke the anonymity of signatures.

A group signature scheme could for instance be used by an employee of a large company to sign documents on behalf of the company. In this scenario, it is sufficient for a verifier to know that some representative of the company has signed. Moreover, in contrast to when an ordinary signature scheme would be used, the verifier does not need to check whether a particular employee is allowed to sign contracts on behalf of the company, i.e., he needs only to know a single company’s public key. A further application of group signature schemes is electronic cash. In this scenario, several banks issue coins, but it is impossible for shops to find out which bank issued a coin that is obtained from a customer. Hence, the central bank plays the role of the membership and the revocation manager and all other banks issuing coins are group members.

Various group signature schemes have been proposed so far. However, in the schemes presented in [8,9,10] the length of signatures and/or the size of the group’s public key depend on the size of the group and thus these schemes are not suitable for large groups. Camenisch first propose a group signature scheme suitable for large groups[11]. In that scheme, the length of signatures and the size of the group’s public key are independent of the number of group members. After that, researchers concentrate their attentions on how to add security property to group signature scheme[5] and standardize the security of group signature scheme[6]. In paper[5], the group signature scheme proposed by Ateniese et al. not only has high efficiency but also adds another security property, coalition-resistance. In paper[6], Bellare et al. standardize the different properties of group signature scheme into two characters: Full-Anonymity and Full-Traceablity, which provides the standard mode for proving the security of group signature scheme. The scheme proposed by CL[12] and the one proposed by BBS[7] have all been proven in this mode.

This paper derives a new signature scheme from the short signature proposed by BB[3], and from which constructs a new type of group signature scheme. The new proposed group signature scheme has been proven in the standard mode of paper[6].

2 Preliminaries

In this section, we give some cryptographic building blocks, assumptions and definitions for the signature we will build.

2.1 Bilinear Groups

G_1 and G_2 are two(multiplicative) cyclic groups of prime order p , g_1 is a generator of G_1 and g_2 is a generator of G_2. ψ is an isomorphism from G_2 to G_1, and $\psi(g_2) = g_1$.Let G_T be an additional group such that $|G_1| = |G_2| = |G_T| = p$.

Definition1. A bilinear map is a map $e: G_1 \times G_2 \to G_T$ with the following properties:

1. Bilinear: $\forall u \in G_1, \forall v \in G_2$, $a, b \in Z$, $e(u^a, v^b) = e(u,v)^{ab}$;

2. Non-degenerate: $e(g_1, g_2) \neq 1$;

Definition2. We say that (G_1, G_2) are bilinear groups if they satisfy the following properties:

1. There exists a bilinear map $e: G_1 \times G_2 \to G_T$;

2. an isomorphism ψ from G_2 to G_1;

3. $\forall u \in G_1, \forall v \in G_2$, there exists an efficient algorithm computing $e(u,v)$.

We know that Gap Diffie-Hellman(GDH) groups can be constructed from bilinear groups[1]. In GDH groups, the DDH problem can be solved, however, CDH problem is still difficult. It is worth noting that DDH problem is still hard in group G_T .

2.2 Signature of Knowledge

So-called zero-knowledge proofs of knowledge allow a prover to demonstrate the knowledge of a secret to a verifier without revealing anything else. The protocol we use in the following is a 3-move protocol and can be proven zero-knowledge in an honest-verifier model. Such protocol can be performed non-interactively with the help of an ideal hash function H . Following paper[2], we refer to the resulting constructs as signature of knowledge.

In the following, we consider the building block for the signature of knowledge of a discrete logarithm.

Definition3. Let $y, g \in G$, a pair $(c, s) \in \{0,1\}^k \times Z_n^*$ satisfying $c = H(m \| y \| g \| g^s y^c)$ is a signature of knowledge of the discrete logarithm of $x = \log_g y$ on a message $m \in \{0,1\}^*$.

The party in possession of the secret $x = \log_g y$ is able to compute the signature by choosing a random $r \in Z_n^*$, and then computing c and s as: $c = H(m \| y \| g \| g^r)$, $s = r - cx(\bmod n)$. When the verifier receives the signature (c,s) on message m, he can compute $c' = H(m \| y \| g \| g^s y^c)$, if $c' = c$, then (c,s) is a valid signature on message m.

Following paper[2], we use $SPK\{(\alpha): y = g^\alpha\}(m)$ as the notation for the signature of knowledge and $PK\{(\alpha): y = g^\alpha\}$ for the corresponding interactive protocol. As for signature of knowledge, the Greek letter α denotes the signer's private key, while for the protocol, the Greek letter α is the knowledge of which is being proved.

2.3 CS98 Encryption Scheme[4]

We give a brief description of CS98 encryption scheme. Assume that we have a group G of prime order q. We also assume that cleartext messages are elements of G. We also use a collision-resistant hash function $H:\{0,1\}^* \to Z_q^*$. The scheme is as follows:

Key Generation. Randomly chooses $g_1, g_2 \in_R G, x_1, x_2, y_1, y_2, z \in_R Z_q^*$, and computes $c \leftarrow g_1^{x_1} g_2^{x_2}, d \leftarrow g_1^{y_1} g_2^{y_2}, h \leftarrow g_1^z$. The public key is $pk \leftarrow (g_1, g_2, c, d, h, H)$,and the private key is $sk \leftarrow (x_1, x_2, y_1, y_2, z)$.

Encryption. Given a message $m \in G$, randomly chooses $r \in_R Z_q^*$, and computes $u_1 \leftarrow g_1^r, u_2 \leftarrow g_2^r, e \leftarrow h^r m, \alpha \leftarrow H(u_1 \| u_2 \| e), v \leftarrow c^r d^{r\alpha}$. Then the ciphertext is (u_1, u_2, e, v).

Decryption. Given a ciphertext (u_1, u_2, e, v), it first computes $\alpha \leftarrow H(u_1 \| u_2 \| e)$, and then verifies whethter the equation $u_1^{x_1 + y_1\alpha} u_2^{x_2 + y_2\alpha} = v$ is equal. If it is equal, then it outputs cleartext $m \leftarrow e / u_1^z$.

2.4 $q-$Strong Diffie-Hellman Assumptiong

$q-$Strong Diffie-Hellman($q-SDH$) assumption is proposed by paper[3]. The definition is described as follows. Parameters G_1, G_2, g_1, g_2 are just defined as section2.1.

$q-$*Strong Diffie-Hellman Problem.* The $q-SDH$ problem in bilinear groups (G_1,G_2) is defined as follows: given a $(q+2)$ tuple $(g_1,g_2,g_2^x,g_2^{x^2},\cdots,g_2^{x^q})$ as input where $\psi(g_2)=g_1$, outputs a pair $(c,g_1^{1/(x+c)})$ where $c\in Z_p^*$. An algorithm A has advantage ε in solving $q-SDH$ problem in bilinear groups (G_1,G_2) if $\Pr[A(g_1,g_2,g_2^x,g_2^{x^2},\cdots,g_2^{x^q})=(c,g_1^{1/(x+c)})]\geq\varepsilon$.

Definition4. We say that the $(q,t,\varepsilon)-SDH$ assumption holds in bilinear groups (G_1,G_2) if no t-time algorithm has advantage at least ε in solving $q-SDH$ problem in (G_1,G_2).

Occasionally we drop the t,ε and refer to the $q-SDH$ assumption rather than the $(q,t,\varepsilon)-SDH$ assumption.

2.5 The Model for Group Signature Scheme

Definition5. Group signature scheme is a signature consisting of the following five procedures:

Setup: this probabilistic algorithm outputs the initial group public key (including all system parameters) and the secret key for the group manager.

JOIN: A protocol between the group manager and a user that results in the user becoming a new group member. The user's output is a membership certificate and a membership secret.

Sign**:** A probabilistic algorithm that on input a group public key, a membership certificate, a membership secret, and a message m outputs group signature of m.

Verify**:** An algorithm for establishing the validity of an alleged group signature of a message with respect to a group public key.

Open**:** An algorithm that, given a message, a valid group signature on it, a group public key and a group manager's secret key, determines the identity of the signer.

3 New Signature Based on BB Short Signature

In this section, we propose a new type of signature scheme derived from BB short signature[3], which is secure as BB short signature. By means of this new signature scheme, we will use it as a tool to issue certificates in our group signature scheme.

Our new signature scheme is described as follows:

All parameters are just the same as those of section2.1. We assume that messages m to be signed are elements in Z_p^*.

Key Generation. Randomly select $x,y\in_R Z_p^*$ and compute $u=g_2^x, v=g_2^y$.The public key is u,v; The secret key is x,y.

Sign. Given the secret key x,y, and a message $m\in Z_p^*$, compute the signature $\sigma\leftarrow(g_1^m)^{\frac{1}{x+g_1^m+yr}}$.

The signature of message is (r,σ).

Verify. When the verifier receives the signature (r,σ), he verifies whether the equation $e(\sigma, ug_2^{[g_1^m]}v^r) = e(g_1^m, g_2)$ is equal. If the equation is equal, then the (r,σ) is a valid signature of message m.

We now give the security analysis for the above scheme.

With some simple computation, we know that our scheme is correct. Since the equation $e(\sigma, ug_2^{[g_1^m]}v^r) = e(g_1^m, g_2)$ is equal. Next we prove our scheme is secure against existential forgery under an adaptive chosen message attack.

Theorem1. *The proposed signature scheme is secure against existential forgery under an adaptive chosen message attack if the* $(q,t',\varepsilon') - SDH$ *assumption holds in* (G_1, G_2).

$\mathrm{P}roof$. This theorem is proven by the following lemma1 and 2.

Lemma1. *If there exists a* $(t,q_s,\varepsilon) - F$ *using adaptive chosen message attack against the proposed signature scheme, then there exists a* $(t,q_s,\varepsilon) - F$ *against BB short signature scheme.*

$\mathrm{P}roof$. We first give a brief description of BB short signature scheme as follows:

Key Generation. Randomly select $x, y \in_R Z_p^*$ and compute $u = g_2^x, v = g_2^y$.The public key is u, v; The secret key is x, y.

Sign. Given the secret key x, y, and a message $m \in Z_p^*$,compute the signature $\sigma \leftarrow (g_1)^{\frac{1}{x+m+yr}}$.

The signature of message is (r,σ).

Verify. When the verifier receives the signature (r,σ), he verifies whether the equation $e(\sigma, ug_2^m v^r) = e(g_1, g_2)$ is equal. If the equation is equal, then the (r,σ) is a valid signature of message m.

Assume that there exists a $(t,q_s,\varepsilon) - F$ using adaptive chosen message attack against the proposed signature scheme, that is, after at most q_s signatures queries and at most t time, F outputs a valid signature forgery (r,σ) on message m with probability at least ε, here $e(\sigma, ug_2^{[g_1^m]}v^r) = e(g_1^m, g_2)$.

Let $m' = [g_1^m], \sigma' = \sigma^{m^{-1}}$, then we have a forgery on BB short signature. This is because of $e(\sigma', ug_2^{m'} v^r) = e(\sigma^{m^{-1}}, ug_2^{[g_1^m]} v^r) = e(g_1, g_2)$.

Lemma2([3]). *Assume the* $(q, t', \varepsilon') - SDH$ *assumption holds in* (G_1, G_2) *, Then BB short signature scheme is* (t, q_s, ε) *-secure against existential forgery under an adaptive chosen message attack provided that* $q_s < q, \varepsilon \geq 2(\varepsilon' + \frac{q_s}{p}) \approx 2\varepsilon', t \leq t' - \Theta(q^2 T)$.

From the above lemma1 and 2, we know that our theorem1 is correct.

4 Group Signature Scheme

This section will use the above mentioned signature scheme and CS98 encryption scheme to establish our group signature scheme.

The system parameters are $(G_1, G_2, G_T, e, p, g_1, g_2, g_T, h, H)$. (G_1, G_2) is bilinear group and a bilinear map is $e: G_1 \times G_2 \to G_T$. g_1, g_2, g_T are generators of G_1, G_2, G_T correspondingly. h is chosen randomly from G_T . There is a collision-resistant hash function $H: \{0,1\}^* \to Z_p^*$.

Key Generation. Randomly choose $x, y \in_R Z_p^*$ and compute $u = g_2^x, v = g_2^y$. Let $sk_M \leftarrow (x, y); pk_M \leftarrow (u, v)$. Randomly choose $x_1, x_2, x_3, x_4, x_5 \in_R Z_p^*$ and compute $y_1 \leftarrow g_T^{x_1} h^{x_2}; y_2 \leftarrow g_T^{x_3} h^{x_4}; y_3 \leftarrow g_T^{x_5}$ .Let $sk_R \leftarrow (x_1, x_2, x_3, x_4, x_5)$ and $pk_R \leftarrow (h, y_1, y_2, y_3)$ .The group public key is $Gpk \leftarrow (pk_M, pk_R, g_1, g_2, g_T)$ and private key for group revocation manager is $Gmsk \leftarrow (sk_R)$.

Join. User randomly chooses his secret key $gsk \leftarrow k, k \in_R Z_p^*$ and computes $P \leftarrow g_1^k$. Then he passes P to group membership manager, meanwhile, he also uses signature of knowledge $SPK\{(\alpha): P = g_1^\alpha\}()$ to give a proof to group membership manager that he has secret key k . After group membership manager completes her verification, she uses her sk_M to generate the signature (σ, r) of secret key k , with the help of signature scheme in section3. She also sends (σ, r) to user as his certificate. At the same time, group membership manager computes $S \leftarrow e(P, g_2)$ and stores S as user's identity in her membership list.

Sign. Group member first blinds his certificate: randomly chooses $r_1, r_2 \in_R Z_p^*$ and computes $\tilde{\sigma} \leftarrow \sigma^{r_1}, \tilde{c} \leftarrow (ug_2^P v^r)^{r_2}$; Secondly, he computes $S \leftarrow e(P, g_2)$ and uses group revocation manager's pk_R to encrypt S : $d_1 \leftarrow g_T^u, d_2 \leftarrow h^u, d_3 \leftarrow y_3^u S$, $d_4 \leftarrow y_1^u y_2^{uQ}$. $Q \leftarrow H(d_1 \| d_2 \| d_3)$; At last, he makes signature of knowledge on message m : $\Delta \leftarrow SPK\{(\mu,\theta,\gamma,\lambda): w_1 = w_2^{\lambda} \wedge \tilde{\sigma} = \sigma^{\mu} \wedge \tilde{c} = (ug_2^P v^r)^{\theta} \wedge d_1 = g_T^{\gamma} \wedge d_2 = h^{\gamma} \wedge d_3 = y_3^{\gamma} w_3^{\lambda} \wedge d_4 = (y_1 y_2^Q)^{\gamma}\}(m)$

Among Δ : $w_1 \leftarrow e(\tilde{\sigma}, \tilde{c}), w_2 \leftarrow e(g_1^{r_1}, g_2^{r_2}), w_3 \leftarrow e(g_1, g_2)$ and the Greek letters $\mu, \theta, \gamma, \lambda$ correspondingly represent secrets r_1, r_2, u, k .

The group signature is $\Sigma \leftarrow ((\tilde{\sigma}, r), (d_1, d_2, d_3, d_4), \Delta)$.

Verify. By means of verifying the correctness of Δ, we know that group signature is correct.

Open. Using her private key $Gmsk = sk_R$, group revocation manager can decrypt (d_1, d_2, d_3, d_4) to get member's identity (d_1, d_2, d_3, d_4) .

She first computes $Q \leftarrow H(d_1 \| d_2 \| d_3)$. Secondly she verifies whether the equation $d_1^{x_1 + x_3 Q} d_2^{x_2 + x_4 Q} = d_4$ is valid, if it is equal, she computes $d_3 / d_1^{x_5} = g_T^{x_5 u} S / g_T^{x_5 u} = S$.

5 Security Analysis of Group Signature Scheme

In paper[6], Bellare et al. put forward three properties which group signature scheme must satisfy:

- Correctness: This property ensures that honestly-generated signatures verify and open correctly;
- Full-anonymity: This property ensures that signatures do not reveal their signer's identity;
- Full-traceability: This property ensures that all signatures, even those created by the collusion of multiple users and the group manager, trace to a member of the forging coalition.

In the following, we prove the security of the proposed group signature scheme just according to the above mentioned properties.

Theorem2. *The proposed group signature scheme is correct.*

P*roof*. Given the group public key $(pk_M, pk_R, g_1, g_2, g_T)$, the verification of a group signature Σ is equal to the verification of signature of knowledge Δ . According to the computation in Definition3 of Section2.2, we easily know that the honestly-generated group signatures are valid. Besides, we could easily recover the signer's identity from (d_1, d_2, d_3, d_4) in the valid group signature Σ . The process of computation can be found in Section4.

Theorem3. *If CS98 encryption scheme is semantically secure(IND-CPA) on* G_T *, then the proposed group signature scheme is CPA-fully-anonymous.*

$Proof$. From paper[4], we know that CS98 encryption scheme is IND-CCA2 secure, so it is IND-CPA secure. In the following, we suppose there is an adversary A capable of attacking CPA-full-anonymous of the proposed group signature scheme. And we also assume the number of members in group is n . We show how to construct another adversary B to attack the security of CS98 encryption scheme under the case of IND-CPA.

Adversary B has public key $pk_R = (h, y_1, y_2, y_3)$ of CS98 encryption scheme and all group member's secret key $gsk[i] = k_i, 1 \le i \le n$. He can use the key generation algorithm to generate all other parts of group public key and then send group public key $(pk_M, pk_R, g_1, g_2, g_T)$ and member's secret key $gsk[i] = k_i$ to adversary A .

Adversary A can query collision-resistant hash function H at will. Adversary B randomly chooses element from Z_p^* as its answer to hash query from adversary A . If the queries are the same, the answers also must be the same.

Adversary A supplies two member's identity i_0, i_1 and message m , which is as his challenge for CPA-full-anonymous of group signature scheme. Adversary B supplies the corresponding member's secret key k_{i_0}, k_{i_1} , meanwhile, the challenger of adversary B computes $S_{i_0} \leftarrow e(g_1^{k_{i_0}}, g_2), S_{i_1} \leftarrow e(g_1^{k_{i_1}}, g_2)$ and sends the ciphertext (d_1, d_2, d_3, d_4) about S_{i_b} to adversary B . As for adversary B , his task is to distinguish whether the ciphertext is about S_{i_0} or S_{i_1} .

Adversary B randomly chooses $\sigma' \in_R G_1, r' \in Z_p^*$. We know that the distribution of σ', r' and σ', r' is indistinguishable. Because signature of knowledge Δ in group signature Σ comes from honest-verifier zero-knowledge proof of knowledge, so adversary B can take advantage of simulator of zero-knowledge proof of knowledge to output the description about Δ . Thus, adversary B acquires a valid group signature $\Sigma = ((\tilde{\sigma}, r), (d_1, d_2, d_3, d_4), \Delta)$ and sends it to adversary A .

At last, adversary A outputs a bit b' , adversary B treats b' as the answer to his own challenge. Since the encryption of S_{i_b} is turned by B into a group signature by user i_b , B answers its challenge correctly whenever A does.

Theorem4. *If the signature scheme in section3 is unforgeable under adaptively chosen message attack, then the proposed group signature scheme is fully-traceable.*

$\mathrm{P}roof$. We need to describe a framework for interacting with an adversary A that wins a full-traceability game.

Setup. We run adversary A, giving it group public key $Gpk \leftarrow (pk_M, pk_R, g_1, g_2, g_T)$, the group revocation manager private key $Gmsk = sk_R$ and the group member's secret key $gsk[i] = k_i, 1 \le i \le n$. We answer its oracle queries as follows.

Hash Queries. When adversary A asks hash function in signature of knowledge, we randomly chooses element from Z_p^* as its answer, storing the answer in case the same query is asked again.

Signature Queries. Adversary A asks for a signature on message M by a key of member i. By means of secret key $gsk[i] = k_i$, he gets the group signature Σ as its answer to signature query.

Output. Finally, adversary A successfully output a forged group signature Σ on message M. We use the group revocation manager private key $Gmsk = sk_R$ to recover its identity S. If $S \ne S_i, 1 \le i \le n$, we output Σ.

We know that adversary A can use the simulator in the zero-knowledge proof of knowledge to get the secrets r_1, r_2, k. Since $w_1 = w_2^k$, we can acquire

$$e(\tilde{\sigma},\tilde{c}) = e(g_1^{r_1}, g_2^{r_2})^k \Rightarrow e(\sigma^{r_1}, (ug_2^P v^r)^{r_2}) = e(g_1^{r_1}, g_2^{r_2})^k \Rightarrow e(\sigma, ug_2^P v^r)^{r_1 r_2} = e(g_1^k, g_2)^{r_1 r_2}.$$

As a result, we get $e(\sigma, ug_2^P v^r) = e(g_1^k, g_2)$. Thus, we have obtained signature (σ, r) on k, which is contradictory to theorem1.

6 Comparison with BBS Short Group Signature

Compared with BBS short group signature scheme in paper[7], the security of BBS short group signature scheme is based on $q-SDH$ and decision linear Diffie-Hellman assumption under random oracle model, while, the security of the proposed one is on the basis of $q-SDH$ and DDH assumption; The group signature Σ of the proposed scheme has 5 elements in G_T and 6 elements in Z_p^*, which has only one more element than that of BBS; Besides, the proposed scheme does not need the third trusted party to issue members secret keys and certificates, while the BBS does need.

7 Conclusion

This paper derives a new signature scheme from BB short signature. Based on the new signature, we construct a new type of group signature scheme. The security of the new group signature scheme is based on the q-Strong Diffie-Hellman assumption and the DDH assumption in the random oracle model. The length of the new group signature is a little longer than that of BBS short group signature. However, in the new group signature scheme, giving certificates and private keys to group members do not need any third trusted party, while in BBS short group signature scheme it does need.

References:

[1] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In Proceedings of Asiacrypt 2001, volume 2248 of LNCS, pages 514–32. Springer-Verlag, Dec. 2001. Full paper: http://crypto.stanford.edu/~dabo/pubs.html.

[2] J. Camenisch. Group signature schemes and payment systems based on the discrete logarithm problem. PhD thesis, vol. 2 of ETH Series in Information Security an Cryptography, Hartung-Gorre Verlag,Konstanz, 1998. ISBN 3-89649-286-1.

[3]D. Boneh and X. Boyen. Short signatures without random oracles. In C. Cachin and J. Camenisch, editors, Proceedings of Eurocrypt 2004, LNCS, pages 56–73. Springer-Verlag, May 2004.

[4]R.Cramer and V.Shoup. A practical public key cryptosystem provably secure against adaptive chosen cipher text attack. In CRYPTO' 98, vol. 1642 of LNCS,pp.13–25，Berlin,1998. Springer Verlag.

[5]G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In M. Bellare, editor, Proceedings of Crypto 2000, volume 1880 of LNCS, pages 255–70. Springer-Verlag, Aug. 2000.

[6]M. Bellare, D. Micciancio, and B. Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In E. Biham, editor, Proceedings of Eurocrypt 2003, volume 2656 of LNCS, pages 614–29. Springer-Verlag, May 2003.

[7]D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In CRYPTO 2004. Springer Verlag, 2004.

[8]D. Chaum and E. van Heyst. Group signatures. In D. W. Davies, editor, Proceedings of Eurocrypt 1991, volume 547 of LNCS, pages 257–65. Springer-Verlag, 1991.

[9]L. Chen and T.P. Pedersen. New group signature schemes. In Advances in Cryptology — EUROCRYPT' 94, vol. 950 of LNCS, pp. 171–181, 1995.

[10]J. Camenisch. Efficient and generalized group signatures. In Advances in Cryptology – EUROCRYPT '97, volume 1233 of Lecture Notes in Computer Science, pages 465-479. Springer Verlag, 1997.

[11]J. Camenisch and M. Stadler. Efficient group signature schemes for large groups. In Advances in Cryptology — CRYPTO' 97, vol. 1296 of LNCS, pp.410–424, Springer-Verlag, 1997.

[12]J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In M. Franklin, editor, Proceedings of Crypto 2004, LNCS. Springer-Verlag, Aug. 2004.