A New Revocation Method for Standard Model Group Signature

Xiaogang Cheng[1, 2]
[1]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China
[2]College of Computer Science and Technology, Huaqiao University, Quanzhou, China
Email: cxg@hqu.edu.cn

Jian Wang[1] and Jixiang Du[2]
[1]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China
[2]College of Computer Science and Technology, Huaqiao University, Quanzhou, China

***Abstract*—Membership revocation is practically necessary for group signature schemes. At present, most revocable group signature schemes are based on ROM model and many standard model group signature schemes do not support revocation. We present a novel and general revocation method for standard model group signature scheme based on length-reducing commitment and Groth-Sahai proof system, and demonstrate its usage by adding revocation capability to the Groth's full secure group signature scheme. The new method supports two different kinds of linkability for members when signing.**

***Index Terms*—membership revocation, group signature, standard model, dynamic accumulator, linkability**

I. Introduction

Group signature was introduced by Chaum and Heyst in 1991 [1]. Since it combined anonymity and traceability, it soon became a central cryptographic primitive, of which many applications had been found such as e-cash, e-voting and trust computing etc.

As pointed out in [2], one of the major issues for group signature's practical application is the ability to revoke a member when he becomes malicious or when he leaves the group deliberately.

Currently most revocable group signature schemes are based on ROM model such as [3,4,5]. Since ROM model can only provide heuristic security, recently there are many works on constructing cryptographic schemes without ROM such as [6,7]. For standard model group signature schemes such as [8,9,10], revocation is not supported. In [11], an ID-based revocable group signature was presented. However the drawback of the scheme in [11] is that the GM (Group Manager) has to be online when signing.

In this paper, we present a novel and general revocation method for standard model group signature, which is based on a length-reducing commitment scheme [12] and Groth-Sahai proof system [13], and demonstrate its usefulness by adding revocation ability to the well-known Groth's full secure standard model group signature scheme [10].

We note that recently in [14], a highly efficient revocable group signature scheme in standard model was introduced, which was based on broadcast encryption and concise vector commitment. But their revocation is based on assumptions like FlexDHE etc., while our scheme is based on the standard DLIN assumption. Moreover, their method is not easily adapted to other standard model group signatures like [8,9,10], since they use broadcast encryption techniques which is a departure from traditional group signature construction. Our revocation method is conceptually simpler and can be used in more scenarios such as [8, 9].

The general idea is simple. GM publishes a short commitment which contains all the public keys of legal members and gives each member a witness. Then when making group signatures, legal member has to prove that his public key is included in the commitment using the witness he got from the GM. We use Groth-Sahai NIWI/NIZK proof system to achieve anonymity. To revoke a member, GM makes another commitment excluding the member's public key. Hence this member lost its signing right. The whole idea is like the DA (Dynamic Accumulator) revocation method in ROM model [3]. We realize it in standard model, although the cost is not as efficient as the ROM DA method.

This paper is organized as follows. In section II we introduce the tools we used for the construction of this new method. The concrete construction is given in section III. In section IV we analyze its securities, and efficiency issues are discussed and compared in section V. Then we make a conclusion in section VI.

II. Preliminaries

In this section we introduce assumptions and cryptographic tools used for the construction of our new revocation method.

Bilinear groups: Let G_1, G_2 and G_T be groups of order p. A bilinear map e: $G_1 \times G_2 \rightarrow G_T$ must satisfy the following:

(1) For arbitrary $a \in G_1$, $b \in G_2$ and $x \in Z_p$, $y \in Z_p$, $e(a^x, b^y) = e(a,b)^{xy}$.

doi:10.4304/jcp.9.5.1053-1057

(2) *e(g, h)* generates G_T whenever *g* generates G_1 and *h* generates G_2.

(3) There is an efficient algorithm to computer *e(a, b)* for any $a \in G_1$ and $b \in G_2$.

If $G_1=G_2$, we call them symmetric bilinear groups, and use the symbol *G* for both G_1 and G_2. If $G_1 \neq G_2$ and there is no efficiently computable non-trivial homomorphism between them, then we call them asymmetric bilinear groups.

Definition 1. DLIN (Decisional Linear) assumption: In symmetric bilinear groups *G*, G_T of order *p*, given a generator *g* of *G*, and tuple $(g^a, g^b, g^{ac}, g^{bd})$ where *a, b, c, d*$\in Z_p^*$ are random, it is hard to distinguish between a random element $T \in G$ and $T=g^{c+d}$.

Definition 2. DBP (Double Paring) assumption: In asymmetric bilinear groups G_1, G_2, G_T of order *p*, given random elements $G_r \in G_1$, $G_s \in G_1$, it is hard to find non-trivial $R \in G_2$, $S \in G_2$ satisfying $e(G_r, R)e(G_s,S)=1$.

Definition 3. SXDH (Symmetric eXternal Diffie-Hellman) assumption: In asymmetric bilinear groups G_1, G_2, G_T of order *p*, DDH (Decisional Diffie-Hellman) assumption is hard in both G_1 and G_2.

1. Homomorphic, Trapdoor and Length-reducing Commitment

In [12], the authors put forward a homomorphic, trapdoor and length-reducing commitment scheme, which is proved to be both hiding and binding based on the DBP (Double Pairing) assumption.

To set up the scheme, generate groups with bilinear maps $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. The public key for this commitment scheme is $ck=(G_R, G_1=G_R^{x1}, \ldots, G_n=G_R^{xn}) \in \mathbb{G}_1^{n+1}$, the trapdoor is $tk=(x_1, \ldots, x_n)$. To commit to $(M_1, \ldots, M_n) \in \mathbb{G}_2^{n+1}$, return $C = e(G_R, R)\prod_{i=1}^{n} e(G_i, M_i)$. To open this commitment, just give out *R* and $(M_1, \ldots, M_n)$. To open to a different message tuple $(M_1', \ldots, M_n')$, compute $R' = R\prod_{i=1}^{n} (M_i / M_i')^{x_i}$ using *tk*. This trapdoor opening is valid since:

$$e(G_R, R')\prod_{i=1}^{n} e(G_i, M_i') = e(G_R, R)\prod_{i=1}^{n} e(G_i, M_i) = C$$

2. Groth-Sahai Proof System

Groth-Sahai proof [13] is the first efficient NIWI/NIZK proof system for a large class of quadratic equations in bilinear groups, esp. in standard model without ROM. It can be realized in a couple of different assumptions such as DLIN, SXDH and subgroup decision etc. Here we introduce the instantiation based on DLIN assumption.

To set up the proof system, generate prime order groups with bilinear map $e: G \times G \rightarrow G_T$. And set the CRS (Common Reference String) as $\vec{f}_1, \vec{f}_2, \vec{f}_3 \in G^3$, where $\vec{f}_1 = (f_1, 1, g), \vec{f}_2 = (1, f_2, g)$ for $f_1, f_2 \in G$. To commit to a $X \in G$, compute $C = (1,1,X) \odot \vec{f}_1^{\,r} \odot \vec{f}_2^{\,s} \odot \vec{f}_3^{\,t}$ with $r, s, t \leftarrow Z_p^*$, where $\odot$ stands for component wise product. $\vec{f}_3$ can be set in two different yet indistinguishable ways, which give perfect sound setting and WI setting respectively. In the perfect sound setting, set $\vec{f}_3 = \vec{f}_1^{\,\zeta_1} \odot \vec{f}_2^{\,\zeta_2}$ for $\zeta_1, \zeta_2 \in Z_p^*$. So $C = (1,1,X) \odot \vec{f}_1^{\,r} \odot \vec{f}_2^{\,s} \odot \vec{f}_3^{\,t}$ is a DLIN encryption of *X*, and can be decrypted by using $\beta_1 = \log_g f_1, \beta_2 = \log_g f_2$. In the WI setting, $\vec{f}_1, \vec{f}_2, \vec{f}_3$ are linear independent vectors and *C* is a perfectly hiding commitment. Under DLIN assumption, these two different are computationally indistinguishable.

To commit an element *x* in Z_p, compute $C = \psi^x \odot \vec{f}_1^{\,r} \odot \vec{f}_2^{\,s}$ for $r, s \leftarrow Z_p^*$, with a CRS including $\psi, \vec{f}_1, \vec{f}_2$. Similarly as above, ψ can be set up with two different ways to achieve WI and soundness setting respectively. For soundness setting $\psi, \vec{f}_1, \vec{f}_2$ are linear independent. For WI setting, set $\psi = \vec{f}_1^{\,\zeta_1} \odot \vec{f}_2^{\,\zeta_2}$, to give a perfectly hiding commitment since in this scenario *C* is always a DLIN encryption of 1, no matter what the *x* is.

To prove the committed variables satisfy a set of quadratic equations, the prover generates one proof element (which may include a couple of group elements) per equation in a way so that NIWI/NIZK is achieved.

Such NIWI/NIZK proofs are available for PPE (Pairing Production Equations) and multi-exponential equations. Here PPE means:

$$\prod_{i=1}^{n} e(A_i, X_i) \cdot \prod_{i=1}^{n} \cdot \prod_{j=1}^{n} e(X_i, X_j)^{a_{ij}} = t_T$$

For variables $X_1, \ldots, X_n \in G$ and constants $t_T \in G_T$ and $A_1, \ldots, A_n \in G$, $a_{ij} \in Z_p$.

And multi-exponential equations are:

$$\prod_{i=1}^{m} A_i^{y_i} \cdot \prod_{j=1}^{n} X_j^{b_j} \cdot \prod_{i=1}^{m} \cdot \prod_{j=1}^{n} X_i^{y_i \gamma_{ij}} = T$$

For variables $X_1, \ldots, X_n \in G$, $y_1, \ldots, y_m \in Z_p$ and constants $T, A_1, \ldots, A_m \in G$ and $\gamma_{ij}, b_1, \ldots, b_n \in Z_p$.

3. SPS based on DLIN

SPS (Structure Preserving Signature) means that the signature, public key and message are all elements of a bilinear group, and the verification procedure is nothing but checking a couple of PPEs (Pairing Product Equations). The purpose of SPS is to combine with Groth-Sahai proof system [13] to prove that the prover hold a valid signature/message pair in a zero-knowledge way. So SPS can be used in many anonymous and privacy-preserving scenarios.

In [17], a SPS scheme based on Decision Linear assumption was presented. The SPS is based on binary Merkle tree [18] by transforming a one-time signature scheme. On the tree, every node has its own public/private key pair *(vk, sk)*, and parent node's private key is used to sign the public key of child node to authenticate the child node. The leaf node is used to sign messages. The leaf node's public key is authenticated by the nodes on the path from this leaf node up to the root. To verify a message/signature pair, just verify the d (Height of the tree) one-time signatures on path from root to the leaf.

Since it is structure preserving, we can prove that we hold a message/signature pair anonymously by using Groth-Sahai's NIWI/NIZK proof system. It was shown in [17] that signature verification is up to verify a set of PPEs:

$$S_{vk,M}^{TSig} = \{OR(S_{L,i}, S_{R,i})\}_{i\in[d]}$$

where $S_{D,i}$ (for $D\in \{L,R\}$ and $i\in [d]$) is

$$S_{D,i} = \{(\prod_{j=1}^{8} E(U_i, m_{i,j})) \cdot E(G, s_i) \cdot E(H, t_i)$$
$$= E(X_{D,i}, z_{D,i})\}$$

Intuitively this set of PPEs proves that from the root to a leaf, the prover has all the one-time signatures and thus he holds a valid message/signature pair according to the public key of the SPS scheme.

III. CONSTRUCTION

1. Weak Commitment Scheme

The homomorphic, trapdoor and length-reducing commitment scheme mentioned above work in asymmetric bilinear groups, in which G_1, G_2 are different and there are no efficiently computable homomorphism between G_1 and G_2. And its security is based on DBP assumption, which is implied by DDH assumption in G_1 [12].

In our construction we use a variant of this commitment scheme, which works in symmetric bilinear groups, where DDH is easy in the based group G. This variant cannot be proved to be a secure commitment scheme based on any standard assumption. But we do prove that it satisfies a weaker security property which is sufficient for our revocation purpose based on DLIN assumption, as shown in the next section.

To set up this weak commitment scheme, generate prime order bilinear groups G, G_T with $e: G \times G \rightarrow G_T$. The public key is $ck=(G_R, G_R^{x1}, ..., G_R^{xn}) \in G^{n+1}$, where $G_R \leftarrow G$ and $x_1, ..., x_n \leftarrow Z_p^*$. The trapdoor is $tk=(x_{1,...,} x_n)$. To commit to messages $(M_1,...,M_n) \in G^n$, one computes $C = e(G_R, R)\prod_{i=1}^{n} e(G_i, M_i)$. To open this commitment, the committer just gives out R and $(M_1,...,M_n)$. To open to a different message tuple $(M_1',...,M_n')$, compute $R' = R\prod_{i=1}^{n}(M_i / M_i')^{x_i}$ using tk. This trapdoor opening is valid since:

$$e(G_R, R')\prod_{i=1}^{n} e(G_i, M_i') = e(G_R, R)\prod_{i=1}^{n} e(G_i, M_i) = C$$

2. Revocation to the Groth's Full Secure Group Signature

We introduce our new revocation method by adding revocation ability to the well-known Groth's full secure group signature scheme [10]. The main revocation related operations are the following:

Setup: Generate groups with bilinear map $e: G \times G \rightarrow G_T$, and $(g^r, g^{x1}, g^{x2}, g^{x3}, ..., g^{xn}) = (G_R, G_1, G_2, G_3, ..., G_n) \in G^{n+1}$. To commit to $(V_1, V_2, ..., V_n) \in G^n$, let $C = e(G_R, R)\prod_{i=1}^{n} e(G_i, V_i)$. Here the $(V_1, V_2, ..., V_n)$ are public keys of legitimate members and C is the public commitment value. But at the beginning nothing is committed so $C=e(G_R, R)$ where R is a random element in G. The secret key for revocation is $(R, r, x_1, x_2, x_3, ...x_n)$. GM also maintains two lists which are empty at the beginning: A-List and D-List for recording new added user and deleting user's information. Non-revoked members can update their witness according to these two lists.

Generate a SPS scheme public/private key pair, which is introduced above, to sign $G_1, G_2, G_3, G_4, ..., G_n$. The purpose of these signatures is for set membership proof as in [19]. I.e. a user can commit to a $G_i \in \{G_1, G_2, G_3, G_4, ..., G_n\}$, to prove that the committed value is indeed one of the $G_1, G_2, G_3, G_4, ..., G_n$, he can show that he holds a SPS signature of the committed value by Groth-Sahai's NIWI/NIZK proof system. Since the SPS we used is based on Merkle tree, the length and cost of the signature are $O(logN)$, where N is the total number of users.

Join: After the joining process of the Groth's group signature scheme, GM adds the user's public key V_k to the public commitment C by computing $C=C \bullet e(G_k, V_k)$. Thus the new user's public key is accumulated into the public commitment C. Then the GM has to give the user the witness that his public key is indeed in C. GM computes

$$e(G_R, R)\prod_{i=1,i\neq k}^{n} e(G_i, V_i) = e(g, R^r)\prod_{i=1,i\neq k}^{n} e(g, V_i^{x_i})$$
$$= e(g, R^r \prod_{i=1,i\neq k}^{n} V_i^{x_i})$$

and lets $W_k = R^r \prod_{i=1,i\neq k}^{n} V_i^{x_i}$ and gives W_k to User_k as the witness. User_k can verify the witness by checking if $e(g, W_k) \bullet e(G_k, V_k) = C$. Later this user has to prove he is not revoked by showing that he holds such a witness in a zero knowledge way. GM also add V_k^{xk} to the A-List, then non-revoked user can update his witness by $W_j = W_j V_k^{xk}$.

Sign: Before signing, member should update his witness according to A-List and D-list. Then besides the normal signature of the Groth's scheme, User_k has to prove he is not revoked by showing that his public key V_k is in C. This can be done by proving that he has a W_k so that:

$$e(g, W_k) \bullet e(G_k, V_k) = C$$

Here V_k is user's public key such that $V_k = g^{yk}$.

User_k can prove his membership in two different ways with different levels of privacy, i.e. linkable and unlinkable. One is proving he is the K^{th} user by $PK\{(W_k, V_k): e(g, W_k) \bullet e(G_k, V_k) = C\}$, so verifier can know that the signer is the K^{th} user. This way is very efficient, signing cost is constant $O(1)$, and the verification cost is also $O(1)$.

To attain stronger anonymity, the other way is to show $PK\{(W_k, V_k, G_k): e(g, W_k) \bullet e(G_k, V_k) = C$ *and* G_k *is one of the* $G_1, ..., G_n\}$. Note that this time the user doesn't make the G_K public. Instead he makes a commitment to the G_K, then he prove that it is one of $G_1, G_2, G_3, G_4, ..., G_n$ by showing he hold a SPS signature on the committed value. This is the set membership proof trick we mentioned above. But this time the signing and verification cost is $O(logN)$, since the SPS is based on Merkle tree and the height of this tree is $logN$. Note that this stronger

anonymity can also be done by using standard model ring signature techniques such as [15,16], instead of this set membership proof trick. But the performance could be worse to $O(N)$ or $O(N^{1/2})$.

Note that in these proofs, the V_k should be the same with the one used in normal Groth's group signature. This can be done easily by using the same commitment to V_k.

Verify: Verifier should get the latest public commitment C. Then just verify if the ZK proof above is valid or not, after the normal verification procedure of the Groth's scheme.

Revoke: GM can revoke the signing right of User_k by updating the public commitment C with $C=C/e(G_k,V_K)$. Of course the non-revoked user has to update their witness too.

For this purpose, GM adds the value V_k^{xk} to the D-List, now non-revoked user j can update his witness by $W_j=W_j/V_k^{xk}$.

IV. Security

As mentioned above, the trapdoor homomorphic commitment scheme is proved to be secure based on DBP (Double Pairing) assumption.

It is clear that DBP works in asymmetric bilinear groups. We used a variant of the commitment schemes, which worked in symmetric bilinear groups. But we cannot prove its security based on any standard assumption. But we do prove that the commitment scheme satisfy a weaker security based on ODBP (One side DBP) assumption, which is implied by the well-known standard DLIN assumption.

Definition 4. ODBP (One Side DBP assumption) assumption: In symmetric bilinear groups G, G_T. Given G_R, $G_1 \in G$. For a specific random value $V \in G$, it is hard to find $R \in G$ satisfying $e(G_R, R)e(G_1, V)=1$.

Lemma 1. Based on DLIN, the ODBP assumption is hard.

Proof: For a specific value V, it is hard to come up with R to satisfy $e(G_R, R)e(G_1, V)=1$. Suppose an adversary A can break it, we show how to use this to solve DLIN.

We get a DLIN instance $(g, g^a, g^b, g^{ac}, g^{bd}, T)$ to judge whether $T=g^{c+d}$ or T is random. First set $G_R=g^a$, $G_1=g^{ac}$, using A we can get a R_1 s.t. $e(g^a, R_1)e(g^{ac},V)=1$, This means $R_1{}^a V^{ac}=1$, i.e. $R_1 V^c=1$, $R_1=V^{-c}$. Similarly with g^b and g^{bd}, we can get a $R_2=V^{-d}$. So $R_1R_2=V^{-c-d}=(V^{-1})^{c+d}$. With this value plus a single paring computation we can distinguish whether T is g^{c+d} or not (Since this is a Decisional Diffie-Hellman problem which is easy in a group with symmetric bilinear map.) □

Lemma 2. Based on ODBP, the weak-commitment cannot be opened to a chosen message.

Proof: Suppose it is not the case, i.e. an adversary A can find R' for a chosen T satisfy $e(G_R,R)e(G_1,V_1)=e(G_R,R')e(G_1,T)$. We show how to use the adversary A to solve the ODBP problem.

Given an ODBP instance to find R_x for a specific X satisfying $e(G_R,R_x)e(G_1,X)=1$. Set $C= e(G_R,R)e(G_1,V_1)$ for random R and V_1, use A to open C to $Z=V_1/X$, i.e. $C=e(G_R,R)e(G_1,V_1)=e(G_R,R_z)e(G_1,Z)$. Manipulate this equation a little we get $e(G_R, R/R_z)e(G_1,V_1/Z)=1= e(G_R, R/R_z)e(G_1,X)$. So it is obvious that $R_x= R/R_z$ is what we get for the ODBP solution. □

Theorem 1. Based on ODBP, revoked user in the above scheme can no longer generate valid group signatures.

Proof: From Lemma 2, we see that the commitment cannot be opened to a chosen different message. But for a revoked user, his public key V_i is deleted from the accumulator commitment C. For legitimate signature, he needs an opening of C to his public key V_i, which is generated by him and the GM in the joining protocol. But as discussed above, this is impossible as long as the ODBP assumption holds. □

V. Efficiency

See Table I for a comparison of efficiency between different revocable group signatures. Note that in our scheme, verification of linkable signature takes $O(1)$ time, while unlinkable signature takes $O(logN)$ time. It can be seen that our scheme is not very efficient compared with other revocable signatures. But it is the first general way of revocation for standard model group signature and based on standard assumption DLIN, and it can support two different kinds of linkability when signing, which could be an advantage in some scenarios such as trust computing [20].

TABLE I.

Cost of Revocable Group Signatures

RGS	Sign	Verify	History	Public Key	Model
VLA [4]	O(1)	O(R)	No	O(1)	ROM
DA [3]	O(1)	O(1)	Yes	O(1)	ROM
NFHF09 [5]	O(1)	O(1)	No	O(N)	ROM
LPY12 [14]	O(1)	O(1)	No	O(logN)	Std
Ours	O(1)/ O(logN)	O(1)/ O(logN)	Yes	O(N)	Std

VI. Conclusion and Further Research

In this paper, we present a novel and general method for the revocation of membership in standard model group signature. The idea is to mimic DA method which woks in ROM model, though ours works in standard model. But our scheme is not as efficient as the DA method, esp. the public key size is $O(N)$, while it is $O(1)$ in DA. Further research is needed to reduce the public key size to constant first. Second, our scheme is history-dependent, which could be inefficient when lots of joining and revocation happen. A focus of further research could be carried out to remove the dependent on history, while still maintain the generality of our scheme.

ACKNOWLEDGMENT

This work is supported by the grant of the National Science Foundation of China (No.61175121), the grant of the National Science Foundation of Fujian Province (No.2013J06014), Promotion Program for Young and Middle-aged Teacher in Science and Technology Research of Huaqiao University (No.ZQN-YX108). We also thank the anonymous reviewers for helpful advice.

REFERENCES

[1] D. Chaum and E. Van Heyst. “Group Signatures.” Advances in Cryptology - Eurocrypt 91, vol. 547, pp. 257-265, 1991.

[2] G. Ateniese and G. Tsudik. “Some open issues and new directions in group signatures.” In Financial Cryptography, volume 1648 of LNCS, pages 196–211, 1999.

[3] J. Camenisch and A. Lysyanskaya. “Dynamic accumulators and application to efficient revocation of anonymous credentials.” Advances in Cryptology-CRYPTO 2002, vol. 2442 of LNCS, Springer-Verlag, pp. 61-76, 2002.

[4] D. Boneh and H. Shacham. “Group signatures with verifier-local revocation.” In: Proc.11th ACM Conference on Computer and Communications Security (ACM-CCS2004), pp. 168–177 (2004)

[5] T. Nakanishi, et al. “Revocable Group Signature Schemes with Constant Costs for Signing and Verifying,” in 12th International Conference on Practice and Theory in Public Key Cryptograhy, Irvine, CA, 2009, pp. 463-480.

[6] Y. Ming, X. Shen, Y. Peng. "Provably Security Identity-based Sanitizable Signature Scheme Without Random Oracles." Journal of Software, 6(10), Academy Publisher, 2011, 1890-1897.

[7] L. Zhang, Q. Wu, Y. Hu. "New Constructions of Short Signatures in the Standard Model." Journal of Software, 6(10), Academy Publisher, 2011, 1921-1928.

[8] G. Ateniese, J. Camenisch, S. Hohenberger, and B. Medeiros. “Practical group signatures without random oracles.” Cryptology ePrint Archive, Report 2005/385, 2005. http://eprint.iacr.org/

[9] X. Boyen and B. Waters. “Full-domain subgroup hiding and constant-size group signatures.” In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 1–15. Springer, Heidelberg (2007)

[10] J. Groth. “Fully anonymous group signatures without random oracles.” In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164–180. Springer, Heidelberg (2007)

[11] X. Cheng, S. Zhou, L. Guo, J. Yu, H. Ma. An ID-Based Short Group Signature Scheme. Journal of Software, 8(3), Academy Publisher, 2013, 554-559.

[12] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev and M. Ohkubo. “Structure-preserving signatures and commitments to group elements.” In: T. Rabin(Ed.) CRYPTO 2010, LNCS 6223, pp. 209-236, 2010

[13] J. Groth and A. Sahai. “Efficient non-interactive proof systems for bilinear groups.” In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (2008)

[14] B. Libert, T. Peters, M. Yung. “Group signatures with almost-for-free revocation.” Crypto 2012, LNCS 7417, pp. 571-589, 2012.

[15] H. Shacham, B. Waters. “Efficient ring signatures without random oracles.” Available at http://eprint.iacr.org/2006/289.pdf, 2006.

[16] N. Chandran, J. Groth, A. Sahai. “Ring signatures of sub-linear size without random oracles.” In ICALP, LNCS 4596, pp. 423-434, 2007

[17] D. Hofheinz and T. Jager. “Tightly secure signatures and public-key encrtyption.” In: R.Safavi-Naini and R.Canetti(Eds.): CRYPTO2012, LNCS 7417, pp. 590-607, 2012

[18] R. C. Merkle. “A Certified Digital Signature.” In: Brassard, G. (ed.)CRYPTO 1989. LNCS, vol.435, pp.218-238, 1990

[19] J. Camenisch, R. Chaabouni, A. Shelat. “Efficient Protocols for Set Membership and Range Proofs.” In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 234-252, 2008

[20] E. Brickell, J. Camenisch, and L. Chen. “Direct Anonymous Attestation,” Proc. 11th ACM Conf. Computer and Comm. Security, pp. 132-145, 2004.