ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.7, July 2009, pp.1977−1985
doi: 10.3724/SP.J.1001.2009.00559

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

低耗后向无关联性的本地验证撤销群签名方案*

魏凌波[1,2+], 武传坤[1], 朱婷鹃[3]

[1](中国科学院软件研究所 信息安全国家重点实验室,北京 100190)

[2](中国科学院 研究生院,北京 100049)

[3](西安邮电学院 通信工程学院,陕西 西安 710121)

Backward Unlinkability and Verifier-Local Revocation Group Signature Scheme with Lower Cost

WEI Ling-Bo[1,2+], WU Chuan-Kun[1], ZHU Ting-Ge[3]

[1](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

[3](School of Communication Engineering, Xi'an University of Posts and Telecommunication, Xi'an 710121)

+ Corresponding author: E-mail: lingbowei@is.iscas.ac.cn

Wei LB, Wu CK, Zhu TG. Backward unlinkability and verifier-local revocation group signature scheme with lower cost. *Journal of Software*, 2009,20(7):1977−1985. http://www.jos.org.cn/ 1000-9825/559.htm

Abstract: In the current group signature schemes with backward unlinkability and verifier-local revocation (BU-VLR), the size of the public key is linear with the total number of time intervals, and the size of the revocation list (RL) is linear with the total number of time intervals and revoked members. Therefore, the cost is high not only in memory space but also in revocation token computation and revocation check. This paper proposes a BU-VLR group signature scheme under the DTDH assumption and the *q*-SDH assumption, which has short public key and RL to reduce the overheads in previous schemes. Moreover, it also has shorter signature length and smaller computation in signing.

Key words: group signature; backward unlinkability; verifier-local revocation; anonymity; traceability

摘 要: 目前在具有后向无关联性的本地验证撤销群签名方案中,公钥长度和时间间隔的总数线性相关,撤销列表的大小与时间间隔的总数和被撤销用户的总数线性相关.因此,当时间间隔总数和被撤销成员总数比较大时,所需的存储空间和撤销验证时的开支都比较高.在DTDH和*q*-SDH假设下,提出一种具有后向无关联性的本地验证撤销群签名方案,它具有较短公钥长度和撤销列表.

关键词: 群签名;向后无关性;本地验证撤销;匿名性;可追踪性

中图法分类号: TP309 **文献标识码**: A

* Supported by the National Basic Research Program of China under Grant No.2007CB807902 (国家重点基础研究发展计划(973)); the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z423 (国家高技术研究发展计划(863))

Received 2007-10-09; Accepted 2008-03-14

1 Introduction

Group signature, introduced by Chaum and Van Heyst[1] in 1991, is a kind of group-oriented signature with one public key and multiple corresponding private keys held by each group member. It allows any group member to sign anonymously on behalf of the group. In case of dispute, the actual signer can be identified by the group manager (GM).

The salient features of group signatures make them attractive for many applications, such as anonymous authentication, Internet voting and bidding. More generally, they can be used to conceal organizational structures, or be integrated with electronic currency mechanisms (as blind group signatures)[2]. But wide implementation in practice is still confined due to some factors, among which is membership revocation as pointed out in Ref.[3].

Membership revocation in group signatures is a sophisticated problem. Revocation of a member should disable his signature ability in the future, and preserve the anonymity of his past signatures. There are two main nontrivial resolutions: one is based on witness[4−6], another is based on RL[7,8]. The former is more efficient. However, in some applications, RL-based revocations are more suitable especially for mobile environments[9] where mobile hosts anonymously communicate with the servers.

The RL-based revocation was improved in Ref.[7] such that the signature size and computation complexity are constant while complexity of verification is linearly dependent on the size of RL. This improved method is called VLR and formalized by Boneh, *et al*. in Ref.[10], where a short VLR group signature scheme based on the decision linear DH (DLDH) assumption and the *q*-SDH assumption was proposed. The signature length is 1 192 bits. The revocation is to publish the value A_i contained in the signing key of the revoked member *i*. This method has short RL but makes the revoked member once for all. When the member wants to rejoin, he must register to get a new valid singing key. Another disadvantage is backward linkable as pointed out in Ref.[9].

Nakanishi, *et al*. introduced backward unlinkability (BU) in Ref.[9], a property which means signatures generated by a group member are unlikable, even after the member has been revoked. Based on the DBDH assumption and the *q*-SDH assumption, a BU-VLR scheme was also proposed. However, the signature length exceeds two times as that of the scheme in Ref.[10]. Later, Nakanishi, *et al*. proposed a shorter BU-VLR group signature in Ref.[11], which was based on the DLDH assumption and the *q*-SDH assumption, and the signature length is only 1 533 bits. Several BU-VLR schemes were also proposed in Ref.[12]. However, the above BU-VLR schemes have a common disadvantage over Boneh's VLR scheme: long public key and RL when the revoked members become more. The reason lies in the construction of the RL. At time interval *j*, the RL_j contains the revoked member *i*'s revocation token $B_{ij} = h_j^{x_i}$ instead of A_i, where h_j,x_i are included in the public key and signing key respectively. Therefore, the corresponding token needs to be recomputed when the current time interval is changed. In short, to achieve the BU property, it has to sacrifice not only the cost of computation but also the size of the public key and the RL.

Our purpose is to design a BU-VLR group scheme with short public key and RL. The proposed scheme is under the DTDH assumption and the *q*-SDH assumption. The signature length is 1 363 bits and the computation cost is no more than the above VLR schemes (comparison is shown in Table 1). Moreover, it has shorter public key and RL.

This paper is organized as follows. The preliminaries are given in Section 2. In Section 3, the model and security definitions of BU-VLR group signature are described. Our proposed scheme is presented in Section 4, and its security is proved in Section 5. Section 6 is conclusion.

2 Preliminaries

2.1 Bilinear maps

Our scheme is constructed by using the following bilinear map:

1. G_1,G_2 are multiplicative cyclic groups of prime order p;

2. g_1 is a generator of G_1, and g_2 is generators of G_2;

3. φ is an isomorphism from G_2 to G_1 with $\varphi(g_2)=g_1$;

4. $e:G_1\times G_2\to G_3$ is an efficient bilinear map, i.e., (1) bilinear: for any $u\in G_1$, $v\in G_2$ and $a,b\in Z$, $e(u^a,v^b)=e(u,v)^{ab}$, and (2) non-degenerate: $e(g_1,g_2)\neq 1$.

For general case, the MNT elliptic curves proposed in Ref.[13] are adopted, where $G_1\neq G_2$, φ is implemented by the trace map. For the comparability with previous VLR schemes in Table 1, we choose the same parameters: p is a 170-bit prime. Consequently, elements in G_1 are 171 bits, and elements of G_3 are 1020 bits.

2.2 Complexity assumptions

Definition 1 (**q-SDH assumption**). Given the above (e,G_1,G_2), for all PPT A, the probability

$$\Pr\left[A(g_1,g_2,g_2^{\gamma},...,g_2^{(\gamma^q)})=(g_1^{1/(\gamma+x)},x):x\in Z_p^*\right]$$

is negligible, where $\gamma\in Z_p^*$.

Definition 2 (**DTDH assumption**). Given the above (e,G_1,G_2), for all PPT A, the probability

$$|\Pr[A(g_2^a,g_2^b,g_1^c,g_1^{abc})=1]-\Pr[A(g_2^a,g_2^b,g_1^c,g_1^d)=1]|$$

is negligible, where $a,b,c,d\xleftarrow{R}Z_p^*$.

2.3 Signature of knowledge

Signatures obtained from a proof of knowledge via the Fiat-Shamir heuristic are often called signatures of knowledge[4]. Just as in Refs.[9–11], we use a variant of the Fiat-Shamir heuristic from zero-knowledge proofs of knowledge, a non-interactive proof of knowledge that the challenge is generated by hashing the message and other related values. We adopt the denotation $SPK\{(x_1,\ldots,x_t):R(x_1,\ldots,x_t)\}(M)$, which means a signature on message M by a signer who knows secret values $x_1,\ldots,x_t$ satisfying the relation $R(x_1,\ldots,x_t)$.

3 Model and Definitions of BU-VLR Group Signature

Now, we describe the model of our BU-VLR group signature scheme, which is somewhat different from that in Ref.[9] due to the different construction of RL.

Definition 3 (**BU-VLR group signature**). A VLR group signature scheme with backward unlinkability consists of the following algorithms:

- *Setup*(n,T): On input the number of time intervals T and a total number of group members n, this probabilistic algorithm generates a group public key *gpk* and a group manager key *gmk*.
- *Join*(i,*gmk*): When a user wants to join the group, the GM generates a private signing key *gsk*[i] for this member.
- *Sign*(*gpk*,j,*gsk*[i],M): A probabilistic algorithm generates the signature σ on message $M\in\{0,1\}^*$ at the current time interval j by member i using his signing key *gsk*[i] and *gpk*.
- *Verify*(*gpk*,j,RL_j,σ,M): A deterministic algorithm can be performed by anyone to generate one bit b. If b=1, it means σ is a valid signature on M at interval j by one member whose revocation token is excluded in RL_j (the revocation list at interval j). If b=0, then σ is invalid.

- *Revoke*(*gpk*,*i*,*j*): When member *i* is to be revoked at interval *j*, GM computes the corresponding revocation token $grt[i][j]=B_{ij}$ published in RL_j, and updates the data $B_{k,j-1}=h_{j-1}^{x_k}\in RL_{j-1}$ by computing $B_{k,j}=h_j^{x_k}$.

Definition 4 (**correctness**). This requires that, for all $gsk[i], j\in[1,T]$ and $M\in\{0,1\}^*$,

$$Verify(gpk,j,RL_j,Sign(gpk,j,gsk[i],M),M)=1\Leftrightarrow grt[i][j]\notin RL_j.$$

Definition 5 (**BU-anonymity**). BU-anonymity requires that for all PPT adversary *A*, the advantage of *A* on the following BU-anonymity game is negligible.

- Setup: The challenger runs *Setup*(*n*,*T*), and provides *A* with *gpk*.
- Queries: *A* can request the challenger about the following queries at the current interval $j\in[1,T]$.
  - Signing: *A* requests a signature of any group member *i* on arbitrary message *M* at interval *j*. The corresponding signature is responded by the challenger.
  - Corruption: *A* requests the private key of any group member *i*.
  - Revocation: *A* requests the revocation token of any group member *i* at the current interval *j*. The challenger responds with *grt*[*i*][*j*].
- Challenge: *A* outputs some (M,i_0,i_1,j) with restrictions that members i_0 and i_1 have not been corrupted, and their revocation tokens have not been queried before the current interval *j* (including *j*). The challenger randomly selects $\phi\in\{0,1\}$, and responds with signature of member i_ϕ on *M* at interval *j*.
- Restricted queries: *A* is allowed to make queries of signing, corruption and revocation, except the corruption queries of i_0 and i_1 and their revocation queries at interval *j*. Note that *A* can query revocations of i_0 and i_1 after *j* due to the property of BU.
- Output: *A* outputs a bit ϕ' as its guess of ϕ.
- If $\phi'=\phi$, *A* wins the game. The advantage of *A* is defined as $|\mathrm{pr}[\phi'=\phi]-1/2|$.

Definition 6 (**traceability**). Traceability requires that for any PPT adversary *A*, the advantage of *A* on the following game is negligible.

- Setup: The challenger runs *Setup*(*n*,*T*), sets *U* empty, and provides *A* with *gpk*.
- Queries: *A* can request the challenger about the following queries at interval $j\in[1,T]$.
  - Signing: *A* requests a signature of any group member *i* on arbitrary message *M* at interval *j*. The challenger responds the corresponding signature.
  - Corruption: *A* requests the private key of any member *i*. The challenger responds *gsk*[*i*] and adds *i* to *U*.
  - Revocation: *A* requests the revocation token of any group member *i* at any interval $j'\in[1,T]$. The challenger responds with *grt*[*i*][*j*′].

Output: *A* outputs $(M^*,j^*,RL_{j^*}^*,\sigma^*)$. *A* wins if (1) $Verify(gpk,M^*,j^*,RL_{j^*}^*,\sigma^*)=1$, and (2) σ^* is traced to a group member outside of $U\setminus RL_{j^*}^*$ or failure, and (3) *A* has not obtained σ^* in signing queries on message M^* for this group member at interval j^*.

4 Our Proposed Scheme

Setup(*n*,*T*): This algorithm runs as follows:

1) Let (e,G_1,G_2,φ) be defined in Section 2.1, select collision resistant hash functions $H_0:\{0,1\}^*\to G_2$, $H:\{0,1\}^*\to Z_p^*$, which are regarded as random oracles. H_0 is used to construct h_j which is used by GM to generate RL_j and by the group members in signing. h_j is constructed at the beginning of interval *j* as following: if no member

is to be revoked, then $h_j=h_{j-1}$. Otherwise, $h_j=H_0(j)$. That is to say: if the revoked members in RL_j are the same as that in RL_{j-1}, then $h_j=h_{j-1}$; otherwise, $h_j=H_0(j)$.

2) Select $\gamma \in Z_p^*$ and compute $w=g_2^{\gamma} \in G_2$.

Output $gpk=(g_1,g_2,w,\varphi,H_0,H)$, and $gmk=\gamma$ is given to GM.

Remark: Compared with previous BU-VLR schemes, our scheme uses H_0 to construct h_j instead of choosing different h_j. This method has two merits: (1) the public key size is reduced from $O(T)$ to $O(t)$ ($t\le r$), where t is the total number of time intervals when the group members are changed. (2) the RL is short, and the computation for GM to compute the data in RL is also reduced. The reason is given in the revoke algorithm.

Join(i,gmk): When a user wants to join the group as member i, GM selects $x_i \in Z_p^*$ and computes $A_i=g_1^{1/(\gamma+x_i)} \in G_1$. (A_i,x_i) is sent to the member as his private signing key.

$\mathrm{Sign}(gpk,j,gsk[i],M)$:

1) Select $\alpha,\beta \in Z_p^*$, set $\eta=x_i\beta$.

2) Compute $T_1=A_i^{\alpha}, f=H_0(gpk,M,T_1) \in G_2, T_2=\varphi(f^{\beta})=\hat{f}^{\beta}, T_3=\varphi(h_j^{\eta})=\hat{h}_j^{x_i\beta}$.

3) The signature of knowledge is expressed by the following equation:

$$V=SPK\{(\alpha,\beta,\eta,x_i,A_i): T_1=A_i^{\alpha}, T_2=\hat{f}^{\beta}, T_3=\hat{h}_j^{\eta}, e(A_i,wg_2^{x_i})=e(g_1,g_2)\}(M)$$

$$=SPK\{(\alpha,\beta,\eta,x_i,A_i): T_2=\hat{f}^{\beta}, T_3=\hat{h}_j^{\eta}, e(T_1,w)=e(g_1,g_2)^{\alpha}/e(T_1,g_2)^{x_i}\}(M),$$

Which is computed as follows:

(a) Pick blinding factors $r_{\alpha},r_{\beta},r_{\eta},r_{x_i} \in Z_p^*$.

(b) Compute $R_1=\hat{f}^{r_{\beta}}, R_2=T_2^{r_{x_i}}(1/\hat{f})^{r_{\eta}}, R_3=\hat{h}_j^{r_{\eta}}, R_4=e(g_1,g_2)^{r_{\alpha}}/e(T_1,g_2)^{r_{x_i}}$.

(c) Compute a challenge $c \in Z_p^*$, $c=H(gpk,j,M,T_1,T_2,T_3,R_1,R_2,R_3,R_4)$.

(d) Compute the following values

$$s_{\alpha}=r_{\alpha}+c\alpha, s_{\beta}=r_{\beta}+c\beta, s_{\eta}=r_{\eta}+c\eta, s_{x_i}=r_{x_i}+cx_i.$$

The last signature output is $\sigma=(T_1,T_2,T_3,c,s_{\alpha},s_{\beta},s_{\eta},s_{x_i})$.

Verify(gpk,j,RL_j,σ,M):

1) Signature check. Verify the validity of σ by checking V as follows.

(a) Compute $\hat{f}=\varphi(H_0(gpk,M,T_1)), \hat{h}_j=\varphi(h_j)$, then retrieve

$$\overline{R}_1=\hat{f}^{s_{\beta}}(1/T_2)^c \quad (1)$$

$$\overline{R}_2=T_2^{s_{x_i}}(1/\hat{f})^{s_{\eta}} \quad (2)$$

$$\overline{R}_3=\hat{h}_j^{s_{\eta}}(1/T_3)^c \quad (3)$$

$$\overline{R}_4=e(g_1,g_2)^{s_{\alpha}}(1/e(T_1,g_2))^{s_{x_i}}(1/e(T_1,w))^c \quad (4)$$

(b) Verify that the challenge c is correct if the equation below holds:

$$c=H(gpk,j,M,T_1,T_2,T_3,\overline{R}_1,\overline{R}_2,\overline{R}_3,\overline{R}_4).$$

2) Revocation check. For all $B_{ij} \in RL_j$ at interval j, if $e(T_2,B_{ij}) \ne e(T_3,f)$ return 1. Otherwise return 0.

Revoke(gpk,i,j):

When member i is to be revoked at interval j, GM computes the corresponding revocation token $grt[i][j]=B_{ij}=h_j^{x_i}=(H_0(j))^{x_i}$ which will be published in RL_j, and updates the revoked member k's revocation token $B_{k,j-1}=h_{j-1}^{x_k} \in RL_{j-1}$ in RL_{j-1} by computing $B_{k,j}=h_j^{x_k}$.

From the construction of h_j, we can see that: GM does not need to compute and update all the revocation tokens B_{ij} in RL_j with interval incrementing as previous BU-VLR schemes. He only updates B_{ij} at the intervals when

the group is changed; otherwise, $B_{il}=B_{ij}$ ($j \le l \le T$).

Lemma 1. The above V is a signature of knowledge of $(\alpha,\beta,\eta,x_i,A_i)$ that satisfies

$$T_1 = A_i^{\alpha}, T_2 = \hat{f}^{\beta}, T_3 = \hat{h}_j^{x_i\beta}, e(A_i, wg_2^{x_i}) = e(g_1, g_2) .$$

Proof: Suppose that an extractor can rewind a prover in the protocol of the above SPK, then for the same (T_1,T_2,T_3), we can get two different pairs of challenges and responses $(c,s_\alpha,s_\beta,s_\eta,s_{x_i})$ and $(c',s'_\alpha,s'_\beta,s'_\eta,s'_{x_i})$. Let $\alpha=(s_\alpha-s'_\alpha)/(c-c'), \beta=(s_\beta-s'_\beta)/(c-c'), \eta=(s_\eta-s'_\eta)/(c-c')$ and $x_i=(s_{x_i}-s'_{x_i})/(c-c')$, then from the Eqs.(1)~(4) we have $\eta=x_i\beta$ and $T_1 = A_i^{\alpha}, T_2 = \hat{f}^{\beta}, T_3 = \hat{h}_j^{\eta}, e(A_i, wg_2^{x_i}) = e(g_1, g_2)$.

Performance Comparison. Table 1 shows a performance comparison between schemes[9−12] and our proposal in signature size (length of σ in bits) and computation cost. We denote multi-exponentiation, isomorphism computation and bilinear map as ME, IC and BM respectively. The computation of IC takes roughly the same time as ME in G_1 (using fast computations of the trace map)[10]. The computation of $\hat{h}_j$ in Ref.[11] and our schemes is not counted in Table 1, since it can be recomputed. Note that each ME may take different time. We ignore the differences just as that in the previous schemes for convenience to statistical comparison.

Table 1 Performance comparison

	$\lvert\sigma\rvert$ (bits)	SIGN	VER	BU	Assumption
BS04[10]	1 192	8ME+2BM	6ME+(3+$\lvert RL\rvert$)BM	No	DLDH, q-SDH
NF05[9]	2 893	10ME+1BM	6ME+(2+$\lvert RL_j\rvert$)BM	Yes	DBDH, q-SDH
ZL06[12]-5	1 704	9ME+1BM	7ME+(4+$\lvert RL_j\rvert$)BM	Yes	Weak DTDH, DL
ZL06[12]-7	1 364	8ME+1BM	6ME+(4+$\lvert RL_j\rvert$)BM	Yes	DDH, DL
NF06[11]	1 533	7ME+1BM	5ME+(3+$\lvert RL_j\rvert$)BM	Yes	DLDH, q-SDH
Ours	1 363	7ME+1BM	5ME+(3+$\lvert RL_j\rvert$)BM	Yes	Weak DTDH, q-SDH

From Table 1 we can see the following main results: (1) Compared with the current most efficient VLR scheme[9], our proposed scheme is 271 bits longer in signature length, but 2ME+1BM computation cost is reduced and BU property is obtained; (2) Compared with the scheme in Ref.[11], 170 bits is reduced in our scheme (i.e. its length is 89% of the former); (3) Compared with the most known efficient BU-VLR scheme-7 in Ref.[12], 2ME+1BM computation is reduced.

Suppose that members $n_1,\ldots,n_t$ (the total revoked number is $r=\sum_{i=1}^{t} n_i$) are revoked at the intervals $j_1,\ldots,j_t$ Respectively. Then the following results can be obtained.

Table 2 Comparison about public key and RL

	Size of public key	$\lvert RL\rvert=\sum_{i=1}^{T}\lvert RL_j\rvert$ (total number of elements in G_2)	Computation cost for RL
Schemes in Ref.[9,11,12]	$O(n)$	$\sum_{i=1}^{t} n_i(T-i+1)$	$\sum_{i=1}^{t} n_i(T-i+1)$ ME
Ours	$O(t)$	$\sum_{i=1}^{t} n_i(t-i+1)$	$\sum_{i=1}^{t} n_i(t-i+1)$ ME

5 Security Analysis

Correctness is easy to verify. BU-anonymity and traceability are satisfied by the following theorems.

Theorem 1. Suppose an adversary A breaks the BU-anonymity of the proposed scheme with advantage ε, after q_H hash queries, q_S signing queries and q_R revocation queries, then there exists an algorithm B breaking the weak DTDH assumption with advantage $(1/nT-q_Hq_S/p)\varepsilon$.

Proof: The input of B is $(g_1,g_2,P_1=g_2^a,P_2=g_2^b,P_3=g_1^c,Z)$, where $a,b,c\in Z_p^*$ and either $Z=g_1^{abc}$ or

$Z = g_1^d$ for $d \in Z_p^*$. B decides which Z it is given by communicating with A as follows.

Setup 1. B picks $i^* \in [1,n]$ and $j^* \in [1,T]$.

2. B selects $r_j \in Z_p^*$ and $\gamma \in Z_p^*$ to compute $w = g_2^{\gamma}$. For j^*, B sets $h_{j^*} = H_0(j^*) = g_2^a$.

3. B selects $x_i \in Z_p^*$ to compute $A_i = g_1^{1/(\gamma + x_i)}$ for all $i \in [1,n]$ except i^*. For i^*, set $x_{i^*} = c$ then $A_{i^*} = g_1^{1/(\gamma + c)}$ which is unknown to B.

4. B computes $B_{ij} = h_j^{x_i}$ for i and j except all i^* and j. For all i^* and j except j^*, set $B_{i^* j} = g_2^{ar_j} = h_j^a$. For i^* and j^*, set $B_{i^* j^*} = g_2^{ac} = h_j^c$ which is also unknown to B.

Hash queries. At any time, A can query the hash value on H_0, H. B feeds back random values with consistency.

Phase 1. At any interval j, A can request signing queries, corruption queries, and revocation queries. If $i \neq i^*$, B responds to queries as usual by using the secret key of member i. If $i=i^*$, B responds as follows.

Signing queries. If $j \neq j^*$, B computes a simulated group signature of member i^* as follows.

1. Randomly select $\beta \in Z_p^*, T_1 \in G_1$, let $f=H_0(gpk,M,T_1)$.

2. Compute $T_2 = \hat{f}^{\beta}, T_3 = P_3^{r_j \beta} = \hat{h}_j^{x_{i^*} \beta}$.

3. Compute the simulated V by using the simulator of the perfect zero-knowledgeness as follows: randomly choose $c, s_\alpha, s_\beta, s_\eta, s_{x_i} \in Z_p^*$ to compute R_1,R_2,R_3,R_4 by Eqs.(1)~(4), and define $H_0(gpk,M,T_1)=f$, $H(gpk,j,M,T_1,T_2,T_3,R_1,R_2,R_3,R_4)=c$. If A has requested $H_0(gpk,M,T_1)$ or $H(gpk,j,M,T_1,T_2,T_3,R_1,R_2,R_3,R_4)$ before, i.e. the backpatch is failure, then B outputs a random guess $\omega' \in \{0,1\}$ and aborts.

Finally, B responds the signature $\sigma = (T_1,T_2,T_3,c,s_\alpha,s_\beta,s_\eta,s_{x_i})$ and the message M to A. Each value in σ has the same distribution as the real, for random $\alpha, \beta \in Z_p^*$ and $T_1 \in G_1$ in the simulation, due to the perfect zero-knowledgeness of V.

If $j=j^*$, B selects $s,t \in Z_p^*, T_1 \in G_1$, and computes $f = P_3^t = g_2^{ct}, T_2 = g_1^{st}, T_3 = \varphi(P_1^s) = g_1^{sa}$ which imply $T_2 = \hat{f}^{\beta}, T_3 = B_{i^* j^*}^{\beta}, \beta = s/c$. Next, B computes the simulated V and defines $H_0(gpk,M,T_1)=f$ and $H(gpk,j,M,T_1,T_2,T_3,\overline{R}_1,\overline{R}_2,\overline{R}_3,\overline{R}_4)=c$. If the backpatch is failure, B outputs a random guess $\omega' \in \{0,1\}$ and aborts. Otherwise, B outputs the simulated signature $\sigma=(T_1,T_2,T_3,V)$.

Revocation queries. If $j \neq j^*$, B responds $B_{i^* j}$. Otherwise (i.e., $j=j^*$), B outputs a random guess $\omega' \in \{0,1\}$ and aborts.

Corruption queries. B outputs a random guess $\omega' \in \{0,1\}$ and aborts.

Challenge. A outputs (M,j,i_0,i_1) to be challenged. If $j \neq j^*$, B outputs a random guess $\omega' \in \{0,1\}$ and aborts; otherwise, B picks $\phi \in \{0,1\}$. If $i_\phi \neq i^*$, B outputs a random guess $\omega' \in \{0,1\}$ and aborts. Otherwise, B responds the following simulated group signature.

1. Select $r, T_1 \in G_1$, set $\beta = b, f = H_0(gpk,M,T_1) = g_2^r, T_3 = Z$, and compute $T_2 = \hat{f}^b = g_1^{rb} = \varphi(P_2^r)$. Note that if $Z = g_1^{abc}$, then $T_3 = \varphi(P_1^{cb}) = \hat{h}_{j^*}^{x_{i^*} \beta}$.

2. Compute the simulated V as in signing queries. If the backpatch is failure, B outputs a random guess $\omega' \in \{0,1\}$ and aborts. Otherwise, B outputs the simulated signature $\sigma=(T_1,T_2,T_3,V)$.

Phase 2. This is the same as Phase 1, with the restrictions of requiring the corruption queries of i_0 and i_1 and their revocation queries at interval j^*. Note that: if the time interval j' in revocation query is a future one, then $B_{i^* j} = (H_0(j))^{x_i}$ which can be done by revoking a dummy member or rejoining this member.

Output. A outputs its guess $\phi' \in \{0,1\}$. If $\phi'=\phi$, B outputs $\omega'=1$ (implying A guesses $Z = g_1^{abc}$), and otherwise outputs $\omega'=0$ (implying A guesses $Z = g_1^d$).

Let the variable $\omega \in \{0,1\}$ represents the state of Z. If $Z = g_1^{abc}$ then $\omega=1$, otherwise $\omega=0$. The advantage of B is

$$|\Pr[B(g_1^a, g_1^b, g_2^c, g_1^{abc}) = 1] - \Pr[B(g_1^a, g_1^b, g_2^c, g_1^d) = 1]| = |\Pr[\omega' = 1 \mid \omega = 1] - \Pr[\omega' = 1 \mid \omega = 0]| = \Pr[\overline{abort}]\varepsilon .$$

If B correctly guesses i^* and j^* (this probability is at least $1/nT$), then B aborts only when A requested the same hash value in the singing query, the probability of which is $q_S q_H/p$. Therefore, the advantage of B is

$$\Pr[\overline{abort}]\varepsilon \geq (1/nT - q_S q_H / p)\varepsilon .$$

Remark: the above theorem implies that the proposed scheme satisfies BU-anonymity in the random oracle model under the DTDH assumption.

Theorem 2. Suppose an adversary A breaks the traceability of the proposed scheme with advantage ε, after q_H hash queries, q_S signature queries, then there exists an algorithm B breaking (n+1)-SDH assumption on G_2 with advantage $(\varepsilon/n-1/p)/16q_H$.

Proof: The following is an interaction framework between A and B.

Setup. B is given $(g_1, g_2, w = g_2^\gamma)$ and n pairs (A_i,x_i) as above. For each $i \in [1,n]$, either $s_i=1$ indicating that an SDH pair (A_i,x_i) is known, or $s_i=0$ indicating that A_i is known but x_i is unknown. Run A on the *gpk* drawn from the given parameters.

Hash queries. At any time, A can query the hash function used in SPK. Random values are responded with consistency.

Signing queries. A requests a signature on message M at interval j of member i. If $s_i=1$, respond a signature using the secret key (A_i,x_i). If $s_i=0$, select $\beta \in Z_p^*, T_1 \in G_1$, let $f=H_0(gpk,M,T_1)$, compute $T_2 = \hat{f}^\beta, T_3 = \hat{h}_j^{x_i\beta}$, and obtain a simulated V. If the backpatch is failure, declare failure and abort. Otherwise, respond (T_1,T_2,T_3,V).

Corruption queries. A requests the secret key of member i. If $s_i=1$, respond (A_i,x_i). Otherwise, declare failure and abort.

Output. A outputs a forged signature $\sigma' = (T_1', T_2', T_3', V')$, from which B can extract the secret key $(A_{i'}, x_{i'})$ by lemma 1. If we fail to identify the member by revocation check, output σ'. Otherwise, some i is identified. If $s_i=0$ then output σ. If $s_i=1$, declare failure and abort.

There are two types of forger on the above framework. Type 1 forges a signature of a member different from all i. Type 2 forges a signature of the member i whose corruption is not requested.

Given q-SDH instance $(g_1', g_2', (g_2')^\gamma, ..., (g_2')^{\gamma^q})$, B can obtain $(g_1, g_2, w = g_2^\gamma)$ and $q-1$ SDH pairs (A_i,x_i) s.t. $e(A_i, wg_2^{x_i}) = e(g_1, g_2)$, following the technique of Ref.[10]. On the other hand, any SDH pair besides these $q-1$ pairs can be transformed a solution of the q-SDH instance, which means that the q-SDH assumption is broken.

Type 1. From (n+1)-SDH instance, B obtains $(g_1, g_2, w = g_2^\gamma)$ and n-SDH pairs (A_i,x_i). Then, apply the framework to A. A outputs a signature with secret key $(A_{i'}, x_{i'})$ such that $A_{i'} \neq A_i$ for $i \in [1,n]$. The simulation is perfect, and A succeeds with advantage ε.

Type 2. From n-SDH instance, B obtains $(g_1, g_2, w = g_2^\gamma)$ and $n-1$ SDH pairs (A_i,x_i), which is distributed amongst n pairs, and set $s_{i'} = 0$. For the unfilled entry at random index i', select $x_{i'} \in Z_P^*$ ($A_{i'}$ is unknown). Apply the framework to A. It succeeds unless A never requests the corruption of i' while the forged signature including $A_{i'}$. The value of i' is independent A's view, thus the probability that A outputs the signature of i' is at least ε/n.

B can obtain another SDH pair beyond the given $q-1$ SDH pairs using the framework with Type 1 or Type 2. B rewinds the framework to obtain two forged signatures on the same message M and the same interval j, where the

commitments in V are the same but the challenges and responses are different. As shown in Ref.[9, 11], the successful probability is at least $(\varepsilon'-1/p)^2/16q_H$, where ε' is the probability that the framework on two forger succeeds. Therefore, B can obtain a pair $(A_{i'},x_{i'})$ s.t. $A_{i'}\neq A_i, x_{i'}\neq x_i$ for all i with the probability $(\varepsilon'-1/p)/16q_H$.

From above, B can solve the $(n+1)$-SDH instance with $(\varepsilon-1/p)^2/16q_H$ using type 1. And B can solve the n-SDH instance with $(\varepsilon/n-1/p)^2/16q_H$ using type 2. B can guess the type of forger with the probability 1/2. Therefore, the pessimistic Type 2 proves the theorem.

Remark: the above theorem implies that the proposed scheme satisfies traceability in the random oracle model under the q-SDH assumption.

6 Conclusion

In this paper, we proposed a BU-VLR group signature scheme based on the DTDH assumption and the q-SDH assumption. Compared with the previous BU-VLR schemes, it is short in the public key and RL and signature length, and has lower overhead computation.

References:

[1] Chaum D, Van Heyst E. Group signatures. In: Davies DW, ed. Advances in Cryptology-EUROCRYPT'91. Berlin: Springer-Verlag, 1991. 257−265.

[2] Lysyanskaya A, Ramzan Z. Group blind digital signatures: A scalable solution to electronic cash. In: Goos G, ed. Proc. of the Final Cryptology'98. Berlin: Springer-Verlag, 1998. 184−197.

[3] Ateniese G, Tsudik G. Some open issues and new directions in group signature schemes. In: Franklin M, ed. Proc. of the Final Cryptology'99. Berlin: Springer-Verlag, 1999. 196−211.

[4] Boneh D, Boyen X, Shacham H. Short group signatures. In: Franklin M, ed. Advances in Cryptology-CRYPTO 2004. Berlin: Springer-Verlag, 2004. 45−55.

[5] Camenisch J, Lysyanskaya A. Dynamic accumulators and application to efficient revocation of anonymous credentials. In: Yung M, ed. 45-55. Advances in Cryptology-CRYPTO 2002. Berlin: Springer-Verlag, 2002. 61−76.

[6] Nguyen L. Accumulators from bilinear pairings and applications. In: Menezes AJ, ed. Proc. of the CT-RSA 2005. Berlin: Springer-Verlag, 2005. 275−292.

[7] Bresson E, Stern J. Efficient revocation in group signatures. In: Kim K, ed. Proc. of the Public Key Crytology 2001. Berlin: Springer-Verlag, 2001. 190−206.

[8] Ateniese G, Song D, Tsudik G. Quasi-Efficient revocation in group signatures. In: Blaze M, ed. Proc. of the Final Cryptology 2002. Berlin: Springer-Verlag, 2003. 183−197.

[9] Nakanishi T, Funabiki N. Verifier-Local revocation group signature schemes with backward unlinkability from bilinear maps. In: Roy B, ed. Advances in Cryptology-ASIACRYPT 2005. Berlin: Springer-Verlag, 2005. 533−548.

[10] Boneh D, Shacham H. Group signatures with verifier-local revocation. In: Proc. of the Computer and Communications Security 2004. Washington: ACM Press, 2004. 168−177.

[11] Nakanishi T, Funabiki N. A short verifier-local revocation group signature schemes with backward unlinkability. IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, 2007,E90-A(9):1793−1802.

[12] Sujing Z, Dongdai L. A shorter group signature with verifier-local revocation and backward unlinkability. In: Pointcheval D, ed. Proc. of the Cryptology and Network Security 2006. Berlin: Springer-Verlag, 2006. 126−143.

[13] Miyaji A, Nakabayashi M, Takano S. New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fundamentals, 2001,E84-A(5):1234−1243.

WEI Ling-Bo was born in 1979. She is a Ph.D. candidate at Institute of Software, the Chinese Academy of Sciences. Her current research area is group signatures.

ZHU Ting-Ge was born in 1976. She is a teacher at the Xi'an University of Posts and Telecommunications. Her current research areas are space-time coding and cryptology.

WU Chuan-Kun was born in 1964. He is a professor of the Institute of Software, the Chinese Academy of Sciences and a CCF senior member. His current research area is group-oriented cryptology.