

## Improved VLR Group Signature Based on DTDH Assumption

Ma Li Zhen

College of Information Science and Engineering, Ocean University of China, Qingdao 266100,  
China

zjlmz@ouc.edu.cn

**Keywords:** Group Signature, Verifier-Local Revocation, DTDH Assumption.

**Abstract.** In VLR (verifier-local revocation) group signatures, revocation messages are only sent to signature verifiers (as opposed to both signers and verifiers). Consequently there is no need to contact individual signers when some user is revoked. Since signers have no load, the VLR group signature schemes are suitable for mobile environments. To meet the requirement of speediness in mobile communication, reducing computation costs and shortening signature length are two requirements at the current research of VLR group signatures. Based on this idea, an improved version of Zhou's VLR group signature is given. Compared with the original scheme, the improved scheme not only can achieve the same security level, but also has shorter signature size and lower computation costs.

### Introduction

Group signatures, introduced by Chaum and van Heyst<sup>[1]</sup>, provide anonymity for signers. A group member can sign on behalf of the group; no one can identify the signing member except the group manager (GM).

A group signature scheme generally includes the following steps: *Setup*, *Join*, *Sign*, *Verify*, and *Open*. Later, a new step, *Revocation*, is added into it<sup>[2]</sup>. GM can revoke a dishonest group member with revocation algorithm. The revoked member can't sign again on behalf of the group, but its former signatures are still valid.

There are two main revocation methods in group signature: one is based on witness, the other is based on revocation list (RL). In a membership revocation resolution based on witness<sup>[3]</sup>, GM publishes a single accumulated value  $a$ , every group member proves in a zero-knowledge way that he/she knows corresponding witness  $w$  to  $a$ . It should be hard for users outside the group to forge such witnesses. Revocations in this category are more efficient than RL based resolutions, but they have a common drawback that previously signed signatures might not being able to pass verifying algorithm under the current verification keys. In the category of membership revocation schemes based on RL<sup>[4]</sup>, GM issues a revocation list of identities (public membership keys). Any group member proves in a zero-knowledge way that his/her identity embedded in the signature is not equal to any one in the RL. The corresponding revocation messages are only sent to verifiers, while the signers are not involved. Since the signer's costs are lower, this approach is suitable for mobile environments where mobile hosts anonymously communicate with the servers. This type of group signature is called Verifier-Local Revocation (VLR) group signature.

VLR group signature was formalized in [5], which presented a short group signature with VLR based on [6]. Nakanishi et al.<sup>[7]</sup> pointed out that this scheme did not satisfy the security of backward unlinkability, and proposed another VLR scheme with the feature of backward unlinkability, i.e., group signatures generated by the same group member is unlinkable except himself and GM, even after this member has been revoked (his/her revocation token is published). In 2006, Zhou and Lin [8] proposed another VLR group signature scheme (ZL06 scheme) based on q-SDH (Strong Diffie-Hellman) assumption and DTDH (Decisional Tripartite Diffie-Hellman) assumption. The scheme in [8] has shorter signature size and lower computation costs than those in [7].

In this paper, we improve ZL06<sup>[8]</sup> VLR group signature scheme. Compared with the original scheme, the proposed scheme not only has the same security, i.e., backward unlinkability (BU-anonymity) and traceability, but also has lower computation costs and shorter signature length.

## Preliminaries

**Definition 1** Bilinear maps:  $G_1 = \langle g_1 \rangle$ ,  $G_2 = \langle g_2 \rangle$ ,  $G'$  are multiplicative cyclic groups of prime order  $p$ .  $\psi$  is an efficiently computed isomorphism from  $G_2$  to  $G_1$ , with  $\psi(g_2) = g_1$ . Then  $e$  is an efficiently computed bilinear map:  $G_1 \times G_2 \rightarrow G'$  if it satisfies: (1) for all  $u \in G_1$ ,  $v \in G_2$  and  $a, b \in \mathbb{Z}$ ,  $e(u^a, v^b) = e(u, v)^{ab}$ , and (2)  $e(g_1, g_2) \neq 1$ .

In this paper, we choose  $G_1 = G_2 = G$ ,  $g_1 = g_2 = g$ .

**Definition 2** ( $q$ -SDH assumption<sup>[5,6]</sup>) For all PPT algorithms  $\mathcal{A}$ , the probability

$\Pr[\mathcal{A}(g, g^\gamma, \dots, g^{\gamma^q}) = (g^{1/\gamma+x}, x)]$  is negligible, where  $x \in \mathbb{Z}_p^*$ ,  $\gamma \in \mathbb{Z}_p^*$ .

**Definition 3** (DTDH assumption<sup>[8]</sup>) For all PPT algorithms  $\mathcal{A}$ , the probability

$|\Pr[\mathcal{A}(g^a, g^b, g^c, g^{abc}) = 0] - \Pr[\mathcal{A}(g^a, g^b, g^c, g^d) = 0]|$  is negligible, where  $a, b, c, d \in \mathbb{Z}_p^*$ .

The model and the security definitions of a VLR group signature scheme with backward unlinkability can be found in [7], we omit it here. We also need the knowledge on signature proof of knowledge (SPK), which can be found in a lot of literatures such as [5]–[8], here, we also omit it.

## Brief Introduction to ZL06 Scheme

ZL06 VLR group signature scheme<sup>[8]</sup> is briefly introduced as follows. Suppose  $n$  is the number of group members,  $T$  is the number of time intervals.

**KEYGEN** ( $n, T$ ): GM selects: a generator  $g$  of  $G$ ,  $\tilde{g}, h_j \in_R G$ , a collision-resistant hash function  $H: \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ ,  $\gamma \in_R \mathbb{Z}_p^*$ ,  $x_i \in_R \mathbb{Z}_p^*$  and computes  $\omega = g^\gamma$ ,  $A_i = g^{1/(\gamma+x_i)}$ ,  $B_{ij} = h_j^{x_i}$ .

The group public key is  $gpk = (g, \tilde{g}, \omega, h_1, \dots, h_T)$ , the private key of member  $i$  is  $gsk[i] = (A_i, x_i)$ , the revocation token of  $i$  at time interval  $j$  is  $grt[i][j] = B_{ij}$ .

**SIGN** ( $gpk, j, gsk[i], M$ ): Group member  $i$  does the followings:

1 Select random  $\alpha, \beta, \delta \in \mathbb{Z}_p^*$ ,  $u \in G$ , compute  $T_1 = A_i \tilde{g}^\alpha$ ,  $T_2 = g^\alpha \tilde{g}^\beta$ ,  $T_3 = h_j^{x_i \delta}$ ,  $T_4 = u^\delta$ .

2 Generate a signature proof of knowledge  $V$ :

$V = \text{SPK}\{(\alpha, \beta, \delta, x_i, A_i) : T_1 = A_i \tilde{g}^\alpha, T_2 = g^\alpha \tilde{g}^\beta, T_3 = h_j^{x_i \delta}, T_4 = u^\delta, e(A_i, \omega g^{x_i}) = e(g, g)\} (M)$

The group signature on  $M$  signed by group member  $i$  at time interval  $j$  is  $\sigma = (T_1, T_2, T_3, T_4, u, V)$ .

**REVOKE** ( $RL_j, grt[i][j]$ ): If  $i$  is revoked at time interval  $j$ , then  $RL_j \leftarrow RL_j \cup \{B_{ij}\}$ .

**VERIFY** ( $gpk, j, RL_j, \sigma, M$ ): A verifier can check the validity of  $\sigma$  by:

1 Signature check. Check the validity of  $V$ .

2 Revocation check. Check that the signer is not revoked at the interval  $j$ , by checking  $e(T_3, u) \neq e(B_{ij}, T_4)$  for all  $B_{ij} \in RL_j$ .

## Proposed VLR Group Signature Scheme

**The improved Scheme.** Suppose  $n$  is the number of group members,  $T$  is the number of time intervals. The improved ZL06 scheme is following.

**KEYGEN** ( $n, T$ ):

(1) GM selects a generator  $g$  of  $G$ , and  $h_j \in_R G$  for all  $j \in [1, T]$ . Also, selects a collision-resistant hash function  $H: \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ .

(2) GM selects  $\gamma \in_R \mathbb{Z}_p^*$  and computes  $\omega = g^\gamma$ .

(3) GM selects  $x_i \in_R \mathbb{Z}_p^*$ , computes  $A_i = g^{1/(\gamma+x_i)}$  for all group members  $i \in [1, n]$ .

(4) GM calculates  $B_{ij} = h_j^{x_i}$  for all  $i$  and  $j$ .

The group public key is  $gpk = (g, \omega, h_1, \dots, h_T)$ , the private key of member  $i$  is  $gsk[i] = (A_i, x_i)$ , the revocation token of  $i$  at time interval  $j$  is  $grt[i][j] = B_{ij}$ .

$SIGN(gpk, j, gsk[i], M)$ : Hereafter, we assume that  $M$  includes the time interval  $j$  in order to bind the signature to the interval. Group member  $i$  does the followings:

1 Select random  $\alpha, \beta \in Z_p^*$ , compute  $T_1 = A_i g^\alpha, T_2 = g^\beta, T_3 = h_j^{x_i \beta}$ .

2 Set  $\eta = x_i \beta$ , generate a signature proof of knowledge  $V$ :

$$V = SPK\{(\alpha, \beta, x_i, A_i) : T_1 = A_i g^\alpha, T_2 = g^\beta, T_3 = h_j^{x_i \beta}, e(A_i, \omega g^{x_i}) = e(g, g)\}(M)$$

$$= SPK\{(\alpha, \beta, x_i, \zeta, \eta) : T_2 = g^\beta, T_3 = h_j^\eta, e(T_1, \omega) / e(g, g) = (e(g, \omega)^\alpha e(g, g)^\zeta) / e(T_1, g)^{x_i}\}(M)$$

The group signature on  $M$  signed by group member  $i$  at time interval  $j$  is  $\sigma = (T_1, T_2, T_3, V)$ , where  $V$  can be calculated as follows:

Choose  $r_\alpha, r_\beta, r_{x_i}, r_\zeta, r_\eta \in_R Z_p^*$ , and compute

$$R_1 = g^{r_\beta}, R_2 = h_j^{r_\eta}, R_3 = (e(g, \omega)^{r_\alpha} e(g, g)^{r_\zeta}) / e(T_1, g)^{r_{x_i}}, c = H(gpk, M, T_1, T_2, T_3, R_1, R_2, R_3) \text{ and}$$

$$s_\alpha = r_\alpha + c\alpha, s_\beta = r_\beta + c\beta, s_{x_i} = r_{x_i} + c x_i, s_\zeta = r_\zeta + c\zeta, s_\eta = r_\eta + c\eta, \text{ then } V = (c, s_\alpha, s_\beta, s_{x_i}, s_\zeta, s_\eta).$$

$REVOKE(RL_j, gsk[i][j])$ : If  $i$  is revoked at time interval  $j$ , then  $RL_j \leftarrow RL_j \cup \{B_{ij}\}$ .

$VERIFY(gpk, j, RL_j, \sigma, M)$ : A verifier can check the validity of  $\sigma$  by:

1 Signature check. Check the validity of  $V$  as follows.

Given  $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_\zeta, s_\eta)$ , calculate

$$R_1' = g^{s_\beta} / T_2^c, R_2' = h_j^{s_\eta} / T_3^c, R_3' = ((e(g, \omega)^{s_\alpha} e(g, g)^{s_\zeta}) / e(T_1, g)^{s_{x_i}}) (e(g, g) / e(T_1, \omega))^c,$$

validate  $c = H(gpk, M, T_1, T_2, T_3, R_1', R_2', R_3')$ .

2 Revocation check. Check that the signer is not revoked at the interval  $j$ , by checking  $e(T_2, B_{ij}) \neq e(g, T_3)$  for all  $B_{ij} \in RL_j$ .

## Security

*Theorem 1. The proposed VLR group signature scheme satisfies the BU-anonymity in the random oracle model under the DTDH assumption.*

The following lemma implies the above theorem.

*Lemma 1. Suppose adversary  $\mathcal{A}$  breaks the BU-anonymity of the proposed scheme with the advantage  $\varepsilon$  and  $q_H$  hash queries and  $q_S$  signature queries. Then, we can construct  $\mathcal{B}$  that breaks the DTDH assumption with the advantage  $(1/nT - (q_H q_S)/p)\varepsilon$ .*

Intuition: in the proof,  $g^a, g^b, g^c, g^{abc}$  in the DTDH assumption are regarded as  $a = x_i, g^b = h_j, c = \beta$ , and  $g^{abc} = h_j^{x_i \beta}$ . The DTDH assumption means that  $g^{abc} = h_j^{x_i \beta}$  and a random  $g^d$  are indistinguishable, and thus  $T_3 = h_j^{x_i \beta}$  does not reveal any information on private key.

*Proof:* The input of  $\mathcal{B}$  is  $(g, g_1 = g^a, g_2 = g^b, g_3 = g^c, Z)$ , where either  $Z = g^{abc}$  or  $Z = g^d$ , and  $a, b, c, d \in_R Z_p^*$ . The task of  $\mathcal{B}$  is to decide that  $Z$  it is given is  $g^{abc}$  or  $g^d$  by communicating with  $\mathcal{A}$ , as follows.

*Setup:*  $\mathcal{B}$  simulates  $KEYGEN(n, T)$  as follows:

1 picks  $i^* \in_R [1, n]$  and  $j^* \in_R [1, T]$ , furthermore, selects  $\gamma \in_R Z_p^*$ , and computes  $\omega = g^\gamma$ .

2 selects  $r_j \in_R Z_p^*$ , and computes  $h_j = \begin{cases} g^{r_j}, & j \neq j^* \\ g_2 = g^b, & j = j^* \end{cases}$ .

3 For all  $i \in [1, n]$ ,  $\mathcal{B}$  selects  $x_i \in_R Z_p^*$  and computes  $A_i = g^{1/(\gamma + x_i)}$  for all  $i \in [1, n]$  except  $i^*$ . For  $i^*$ , define  $x_{i^*} = a$  and  $A_{i^*} = g^{1/(\gamma + a)}$ , which are unknown for  $\mathcal{B}$  since  $\mathcal{B}$  does not know  $a$ .

4  $\mathcal{B}$  computes  $B_{ij} = h_j^{x_i}$  for all  $i \in [1, n]$  except  $i^*$  and all  $j$ . For  $i^*$ ,  $\mathcal{B}$  sets  $B_{i^*j} = g_1^{r_j} = g^{ar_j} = h_j^a = h_j^{x_{i^*}}$  except for  $j^*$ . For  $i^*$  and  $j^*$ , define  $B_{i^*j^*} = g^{ab} = h_j^{x_{i^*}}$ , which is also unknown for  $\mathcal{B}$  since  $\mathcal{B}$  does not know  $a, b$ .

*Hash queries:* At any time,  $\mathcal{A}$  can query the hash function used in SPK.  $\mathcal{B}$  responds with random values with consistency.

*Signing queries:*  $\mathcal{A}$  can query the signature of member  $i$  at any time interval  $j$ . If  $i \neq i^*$ ,  $\mathcal{B}$  knows  $(A_i, x_i)$ , so  $\mathcal{B}$  computes a signature with the algorithm  $SIGN$  to respond the query as usual. For  $i = i^*$  and  $j \neq j^*$ ,  $\mathcal{B}$  selects  $\beta \in_R Z_p^*$ ,  $T_1 \in_R G$ , computes  $T_2 = g^\beta$ ,  $T_3 = g_1^{r_j \beta} = g^{ar_j \beta} = h_j^{a\beta} = h_j^{x_i^* \beta}$ . For  $i = i^*$  and  $j = j^*$ ,  $\mathcal{B}$  selects  $z \in_R Z_p^*$ ,  $T_1, T_2 \in_R G$ , then computes  $T_3 = g_1^z$ . From the view of  $\mathcal{A}$ , the above choices also satisfy  $T_3 = h_j^{x_i^* \beta}$ , where  $\beta = z/b$ .

Then,  $\mathcal{B}$  computes the simulated SPK  $V = SPK(T_1, T_2, T_3)$  by using the simulator of the perfect zero-knowledge-ness, which includes the backpatch of the hash function. If the backpatch is failure,  $\mathcal{B}$  outputs a random guess  $\omega' \in_R \{0,1\}$  and aborts. Otherwise,  $\mathcal{B}$  responds signature  $\sigma = (T_1, T_2, T_3, V)$  to  $\mathcal{A}$ .

*Revocation queries:*  $\mathcal{A}$  can query the revocation token of  $i$  at time interval  $j$ . If  $i \neq i^*$  or  $j \neq j^*$ ,  $\mathcal{B}$  responds  $B_{ij}$  to  $\mathcal{A}$ ; If  $i = i^*$  and  $j = j^*$ ,  $\mathcal{B}$  outputs a random guess  $\omega' \in_R \{0,1\}$  and aborts.

*Corruption queries:*  $\mathcal{A}$  can query the secret key of  $i$ . If  $i \neq i^*$ ,  $\mathcal{B}$  responds  $(A_i, x_i)$  to  $\mathcal{A}$ ; If  $i = i^*$ ,  $\mathcal{B}$  outputs a random guess  $\omega' \in_R \{0,1\}$  and aborts.

*Challenge:*  $\mathcal{A}$  outputs a message  $M$ , the current time interval  $j$  and two members  $i_0, i_1$  to be challenged.  $\mathcal{B}$  picks  $\phi \in_R \{0,1\}$ . If  $i_\phi \neq i^*$  or  $j \neq j^*$ ,  $\mathcal{B}$  outputs a random guess  $\omega' \in_R \{0,1\}$  and aborts; If  $i_\phi = i^*$  and  $j = j^*$ ,  $\mathcal{B}$  responds the following simulated group signature:  $\mathcal{B}$  regards  $c$  as  $\beta$ , sets  $T_1, T_2 \in_R G$ ,  $T_3 = Z$ , then computes the simulated SPK  $V = SPK(T_1, T_2, T_3)$  by using the simulator of the perfect zero-knowledge-ness. Note that, if  $Z = g^{abc}$ , then,  $T_3 = g^{abc} = h_j^{x_i^* c} = h_j^{x_i^* \beta}$ , thus  $(T_1, T_2, T_3, V)$  is a simulated signature with the same distribution as the real signature; If  $Z = g^d$ , then  $T_2 = g^d$ , thus  $\mathcal{A}$  can decide  $\phi$  only by guessing.

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

As the analysis of lemma 2 in [7], the advantage that  $\mathcal{B}$  guesses  $\omega$ , i.e., the advantage of  $\mathcal{B}$  breaks DTDH assumption is at least  $(1/nT - q_S q_H / p) \varepsilon$ .  $\square$

**Theorem 2.** *The proposed VLR group signature scheme satisfies the traceability in the random oracle model under the  $q$ -SDH assumption.*

The following lemma implies the above theorem.

**Lemma 2.** *Suppose adversary  $\mathcal{A}$  breaks the traceability of the proposed scheme with the advantage  $\varepsilon$  and  $q_H$  hash queries and  $q_S$  signature queries. Then, we can construct  $\mathcal{B}$  that breaks the  $(n+1)$ -SDH assumption with the advantage  $(\varepsilon/n - 1/p)/16q_H$ .*

*Proof:* The process is similar to the lemma 3 in [5], here we omit it.

**Performance and comparison.** We compare the efficiency of the proposed scheme to the original ZL06 scheme. The comparisons are shown in table 1.

*Size of signature:* the proposed signature  $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_\zeta, s_\eta)$  includes 3 elements from  $G$ , 6 elements from  $Z_p$ . As in [5]-[8],  $p$  is 170 bits, elements of  $G$  are 171bits, thus the size of proposed signature is 1533 bits.

*Computations:* In our signing algorithm,  $R_3 = (e(g, \omega)^{r_\alpha} e(g, g)^{r_\zeta}) / e(T_1, g)^{r_{x_i}}$ . This can be computed as  $R_3 = (e(g, \omega)^{r_\alpha} e(g, g)^{r_\zeta - ar_{x_i}}) / e(A_i, g)^{r_{x_i}}$ . Thus, all bilinear map computations ( $e(g, \omega)$ ,  $e(g, g)$  and  $e(A_i, g)$ ) can be pre-computed. So, the signature generation requires 6 multi-exponentiations (denoted by ME).

In the verification,  $R_3' = ((e(g, \omega)^{s_\alpha} e(g, g)^{s_\gamma}) / e(T_1, g)^{s_{x_i}}) (e(g, g) / e(T_1, \omega))^c$ . This can be computed as  $R_3' = ((e(g, \omega)^{s_\alpha} e(g, g)^{s_\gamma + c}) / e(T_1, g)^{s_{x_i} \omega^c})$ , the bilinear map computations ( $e(g, \omega)$  and  $e(g, g)$ ) can be pre-computed. So, the verification requires 3 multi-exponentiations (denoted by ME) and  $(2 + |RLj|)$  bilinear maps (denoted by BM).

Table 1 Comparison (ME denotes multi-exponentiations, BM denotes bilinear map)

Scheme	Size of Signature (bits)	Costs of Signing	Costs of Verification	BU
ZL06	2215	11ME + 2BM	7ME + (3 +  RLj )BM	yes
Ours	1533	6ME	3ME + (2 +  RLj )BM	yes

From table 1, we can see that the size of signature of our scheme reduces about 31% than that of ZL06 scheme, also, our scheme has lower computation costs.

## Conclusion

In this paper, we propose a new VLR group signature scheme with backward unlinkability based on q-SDH assumption and DTDH assumption. The proposed scheme has lower computation costs and shorter signature length than ZL06 scheme, and can be applicable to mobile environments such as IEEE 802.1x [9].

## References

- [1] Chaum D., Van Heyst E., Group signatures, in: Donald W. Davies (Ed.), Advances in Cryptology- EUROCRYPT'91, LNCS 547, Springer-Verlag, Berlin, 1991, pp. 257-265.
- [2] Bresson E., Stern J., Efficient revocation in group signatures, in: G. Goos, J. Hartmanis, J. van Leeuwen (Eds.), Public Key Cryptography-PKC 2001, LNCS 1992, Springer-Verlag, Berlin, 2001, pp. 190-206.
- [3] Lan Nguyen, Accumulators from bilinear pairings and applications, in: Alfred Menezes (Ed.), CT-RSA'05, LNCS 3376, Berlin, 2005, pp. 275-292.
- [4] G. Ateniese, D. Song, and G. Tsudik, Quasi-efficient revocation in group signatures, In: Rebecca N. Wright (Ed.), Financial Cryptography'02, LNCS 2357, Springer-Verlag, Berlin, 2002, pp. 183-197.
- [5] Boneh D., Shacham H., Group signatures with verifier-local revocation, In: B. Pfitzmann, P. Liu(Eds.), Proceedings of the 11th ACM conference on Computer and communications security-CCS'04, ACM Press, New York, 2004, pp. 168-177.
- [6] Dan Boneh, Xavier Boyen, and Hovav Shacham, Short group signatures, In: M. Franklin (Eds.), CRYPTO'04, LNCS 3152, Springer-Verlag, Berlin, 2004, pp. 45-55.
- [7] Nakanishi T., Funabiki N., Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps, in: K. Roy (Ed.), Advances in Cryptology-ASIACRYPT 2005, Springer-Verlag, Berlin, 2005, pp. 533-548.
- [8] Zhou S., Lin D., A short group signature with verifier-local revocation and backward unlinkability, Cryptology ePrint Archive: Report 2006/100, (2006).
- [9] Herry Z. K., Kalvein R., Silvester T., Gregorius K., Wireless sensor network for landslide monitoring in Nusa Tenggara Timur, TELCOMNIKA. Vol.9 No.1 (2011) 9-18.