实用的本地验证者撤销群签名方案

李继国，孙刚，张亦辰
(河海大学 计算机与信息学院，江苏 南京 210098)

摘 要：本地验证者撤销是一种有效的群成员撤销方法，该方法只需将撤销信息发给验证者而无需签名者的参与。目前本地验证者撤销群签名方案中普遍存在不能防止陷害攻击以及撤销验证计算量与撤销列表长度呈线性增长等问题。为了解决这些问题，并针对群签名在隐私保护证明方面的应用，基于 q-SDH 假设和 DLDH 假设，提出一种实用的本地验证者撤销群签名方案，并在随机预言模型下证明了方案的安全性。分析了方案的效率，并与现有的本地验证者撤销群签名方案进行了比较，分析表明方案的撤销验证计算量与撤销列表长度无关，同时还具有防陷害性和向后无关联性。

关键词：群签名；本地验证者撤销；防陷害性；向后无关联性
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2011)10-0067-11

Practical group signature scheme with verifier-local revocation

LI Ji-guo, SUN Gang, ZHANG Yi-chen
(College of Computer & Information Engineering, Hohai University, Nanjing 210098, China)

Abstract: An efficient approach of member revocation in group signature is verifier-local revocation. In this approach, revocation messages are only sent to signature verifiers, while signers have no involvement. There are some problems in group signature with verifier-local revocation; for example, some group signature schemes do not have exculpability and the computation cost of revocation check is dependent on the length of the revocation list, and so on. In order to solve above problems, and aim at the application of group signatures for enabling privacy-preserving attestation, a practical group signature scheme with verifier-local revocation based on the strong Diffie-Hellman assumption and decision linear Diffie-Hellman assumption, which was proven to be secure in the random Oracle model was proposed. The efficiency of the proposed scheme was analyzed. Compared with the existing verifier-local revocation group signatures, the computation cost of revocation check in the scheme is independent of the length of the revocation list. At the same time, the scheme satisfies exculpability and backward unlinkability.

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

---

收稿日期：2010-05-13；**修回日期**：2010-11-30
基金项目：国家自然科学基金资助项目（60842002, 60903018）；国家高技术研究发展计划（“863”计划）基金资助项目（2007AA01Z409）；中央高校基本科研业务费专项资金资助项目（2009B21114, 2010B07114）；中国博士后基金（20100471373）；江苏省“六大人才高峰”项目（2009182）；河海大学优秀创新人才计划
Foundation Items: The National Natural Science Foundation of China (60842002, 60903018); The National High-Tech Research and Development Program of China (2007AA01Z409); The Fundamental Research Funds for the Central Universities (2009B21114, 2010B07114); China Postdoctoral Science Foundation funded project (20100471373); The “Six Talent Peaks Program” of Jiangsu Province of China (2009182); Program for New Century Excellent Talents in Hohai University

1 引言

群签名是Chaum和van Heyst在EUROCRYPT'91[1]上首先提出的。在群签名中，群成员可以代表群体进行匿名签名，验证者只能验证签名是由群中的成员所签，而不能确定是哪个成员。群签名的匿名性是可撤销的，必要时可通过群管理员打开签名来确定签名者的身份，此外群签名还满足正确性、防伪造性、不可链接性、防陷害攻击、抗联合攻击等安全特性，也正是由于上述这些性质，群签名在匿名认证、电子支付、网上投票等方面有着巨大的应用前景。

现实应用中，签名的群体经常是动态的，群成员是不断增减的，如何安全高效地撤销群成员已经成为制约群签名广泛应用的一个重要问题。最简单的撤销方法就是群中心(或者群管理者)重新生成密钥或证书并分配给群成员，但这需要巨大的计算代价与通信代价。目前主要有 2 类解决方案：一类是基于动态累加器[2~5]，另一类是基于撤销列表[6~14]。前一类方案相比于第二类方案更为高效，然而这类方案有个缺陷：一旦对所有签名者和验证者广播更新后的群公钥信息，之前生成的签名将不能够再验证；第二类方案由群管理员生成一张记录群成员撤销标记的列表，在验证签名时，验证者根据撤销列表进行撤销检查。2004 年，Boneh 和 Shacham[7]将基于撤销列表这种方法形式化定义为本地验证者撤销(VLR, verifier-local revocation)，并提出了一种 VLR 群签名方案。本地验证者撤销是一种有效解决群成员撤销问题的方法，该方法只需将撤销信息发给验证者，而不需要与每个终端用户进行通信，适用于移动环境中。但是文献[8]指出 Boneh-Shacham 方案不具有向后无关联性(BU, backward unlinkability)，这一特性是指即使群成员在某个时刻被撤销了，在该时刻之前的签名仍然保持匿名性。同时文献[8]指出向后无关联性在群签名应用中有着不可或缺的作用，特别当群成员自愿离开群时，理应保持该成员撤销之前所生成签名的匿名性，并引入文献[15]中时间间隔的概念实现了向后无关联性，提出了一种 BU-VLR 群签名方案。之后 Zhou 等[9,10]、Nakanishi 和 Funabiki[11]、魏凌波等[12]在减少签名长度和计算代价基础上，提出了各自的 BU-VLR 短群签名方案。然而上述 VLR 群签名方案[7~9,11,12]都不能防止陷害攻击并且撤销验证计算量与撤销列表长度呈线性增长。张跃宇等[13]以及张京良等[14]提出了一类具有防陷害性且撤销验证计算量与撤销列表长度无关的 VLR 群签名方案，通过群管理者和群成员共同生成群成员私钥，使得方案具有防陷害性；通过验证撤销列表中的值与签名已知量的等同情况，使得撤销验证计算量与撤销列表长度无关。文献[12]指出文献[13]中的方案本身就是相关性的方案，向后无关联性更无从谈起，而这是因为方案中 T_3 的构造($T_3=\tilde{h}_j^{x_i+y_i}$，$x_i$，$y_i$ 是用户加入群时，得到的签名密钥的一部分，此后这 2 个值不变)。类似地，文献[14]中的方案也不具有向后无关联性。2009 年，魏凌波等[16]指出目前本地验证者撤销群签名方案中，公钥长度和撤销列表大小与时间间隔总数线性相关，因此当时间间隔总数比较大时，方案存储空间的开支比较高，并提出一种低耗后向无关联性的本地验证者撤销群签名方案，方案具有较短的公钥长度和撤销列表。文献[16]中所采用的方法具有一般性，现有的本地验证者撤销群签名方案都可以通过该方法实现方案存储空间上的优化。最近，李继国等[17]提出了一个标准模型下安全的本地验证者撤销群签名方案。与同类方案相比，在签名元素个数、签名长度方面具有一定优势。

本文采用文献[7]中的高效撤销思想以及文献[13,14]中防陷害性思想，基于 q-SDH 假设和 DLDH 假设提出一种实用的 VLR 群签名方案，不仅撤销验证计算量与撤销列表长度无关，还具有防陷害性，同时引入时间间隔概念，使得方案具有向后无关联性。本文构造的方案可应用于移动环境中的隐私保护证明。

本文第 2 节介绍预备知识；第 3 节提出了用于隐私保护证明的 BU-VLR 群签名模型以及安全定义；第 4 节提出了实用的 BU-VLR 群签名方案；第 5 节对方案进行了安全分析；第 6 节给出了方案的性能分析与比较；第 7 节总结全文。

2 预备知识

本文方案建立在双线性映射基础上，安全性基于随机预言模型下的 q-SDH 假设和 DLDH 假设。这里简要介绍方案中所使用的双线性映射、困难性假设以及知识签名表示，详见文献[7,11]。

2.1 双线性映射

设 G_1、G_2 都是阶为素数 p 的乘法循环群，g_1 是 G_1 的生成元，g_2 是 G_2 的生成元，φ 是 G_2 到 G_1 的可

计算同态映射，满足 $\varphi(g_2)=g_1$，双线性映射 $e:G_1\times G_2\to G_T$ 满足以下性质：

1) 双映射性。对任意的 $u\in G_1$，$v\in G_2$ 和 $a,b\in Z$，都有 $e(u^a,v^b)=e(u,v)^{ab}$。

2) 非退化性。$e(g_1,g_2)\neq 1_{G_T}$，其中 1_{G_T} 是 G_T 的幺元。

3) 可计算性。存在有效的多项式时间算法计算 e。

称满足上述性质的群 (G_1,G_2) 是一对双线性群，为了更一般化，取 $G_1\neq G_2$。与文献[7~9, 11~14, 16]中方案相同，取 p 是长为 170bit 的素数。

2.2 困难问题假定

定义 1 q-Strong Diffie-Hellman(q-SDH)问题：给定上述的双线性群 (G_1,G_2)，则 (G_1,G_2) 上的 q-SDH 问题是：输入一个元组 $(g_1,g_2,g_2^{\gamma},\cdots,g_2^{(\gamma^q)})$，其中 $\gamma\in Z_p^*$，计算一个数对 $(g_1^{1/(\gamma+x)},x)$，$x\in Z_p^*$。称形如 $(g_1^{1/(\gamma+x)},x)$ 的数对为一个 SDH 对。

定义 2 q-SDH 假设：对所有概率多项式时间算法 A，概率 $\Pr[A(g_1,g_2,g_2^{\gamma},\cdots,g_2^{(\gamma^q)})=(g_1^{1/(\gamma+x)},x):x\in Z_p^*]$ 是可忽略的，则称 (G_1,G_2) 上的 q-SDH 假设成立。

定义 3 Decision Linear Diffie-Hellmen (DLDH)问题：给定上述群 G_2，则群 G_2 上的 DLDH 问题是：已知 $u,v,h,u^a,v^b,h^c\in G_2$，其中 $a,b,c\in {}_RZ_p^*$，如果 $a+b=c$ 则输出 1，否则输出 0。

定义 4 DLDH 假设：对所有概率多项式时间算法 A，概率 $|\Pr[A(u,v,h,u^a,v^b,h^{a+b})=1]-\Pr[A(u,v,h,u^a,v^b,h^c)=1]|$ 是可忽略的，则称群 G_2 上的 DLDH 假设成立。

2.3 签名的知识证明

记号 $SPK\{(x_1,\cdots,x_t):R(x_1,\cdots,x_t)\}(M)$ 表示签名者用秘密值 $x_1,\cdots,x_t$ 对消息 M 签名的一个知识证明，这里 $x_1,\cdots,x_t$ 满足关系式 $R(x_1,\cdots,x_t)$。与文献[7,11]中的方案相同，本文签名的知识证明采用 Fiat-Shamir 方法，即把散列值作为挑战值的一种非交互的零知识证明。

3 模型及安全定义

本文提出的用于隐私保护证明的 BU-VLR 群签名模型是文献[11]中的 BU-VLR 群签名模型的一种扩展。隐私保护证明这一应用在文献[7]中有详细的说明，这里简要介绍其过程：当用户访问 Web 站点时，要用群签名进行私有证明；群签名由用户机器中嵌入的防篡改芯片生成，芯片中内置群密钥；签名验证通过后，用户才可以获得权限访问该 Web 站点。

文献[11]中密钥生成算法以成员个数和时间间隔数目为输入，产生群公钥、群成员私钥和每个成员在每个时间间隔的撤销标记，而本文方案为了防止陷害攻击由群管理员和群成员共同生成群成员私钥，因此单独执行一个成员加入算法来生成群成员私钥。此外还添加了一个成员撤销算法。现有的 VLR 群签名方案在撤销群成员时，只需将群成员的撤销标记添加到撤销列表中，而本文方案的成员撤销算法中以成员的撤销标记和需要访问的 Web 站点信息作为输入，产生撤销信息添加到撤销列表中，进而达到撤销某成员的目的。一个用于隐私保护证明的 BU-VLR 群签名方案主要由以下算法组成。

1) 密钥生成算法 KeyGen(n,T)：输入成员个数 n 和时间间隔数目 T，产生群公钥 gpk 和每个成员 $i\in[1,n]$ 在每个时间间隔 $j\in[1,T]$ 的撤销标记 $grt[i][j]$。

2) 成员加入算法 Join(gpk,i)：用户要加入群成为群成员 i 时，通过与群管理员(GM)交互共同生成群成员 i 的私钥 $gsk[i]$。用户得到群成员私钥，先进行验证，若验证通过则接受该私钥，否则重新发送请求。

3) 签名产生算法 Sign($gpk,j,gsk[i],M,S$)：输入群公钥 gpk、时间间隔 j、群成员 i 私钥 $gsk[i]$、签名消息 $M\in\{0,1\}^*$ 以及 Web 站点信息 $S\in\{0,1\}^*$ (这里可以将 S 看成是 Web 站点网址的任意长比特串)，产生签名 σ。

4) 签名验证算法 Verify(gpk,j,RL_j,σ,M)：输入群公钥 gpk、时间间隔 j、撤销列表 RL_j（j 时间间隔的撤销列表，包含当前时刻的群成员撤销信息)、签名 σ 以及签名消息 M，输出 1 表示签名合法且签名者的撤销信息不在 RL_j 中，反之输出 0。

5) 成员撤销算法 Revocation($grt[i][j],S$)：输入撤销标记 $grt[i][j]$ 和 Web 站点信息 S，产生 j 时间间隔拒绝群成员 i 访问该 Web 站点的撤销信息，并添加到撤销列表 RL_j 中。

用于隐私保护证明的 BU-VLR 群签名方案还应该满足正确性、可追踪性以及 BU-匿名性等安全性质，具体定义如下（主要基于文献[11])。

1) 正确性：对算法 KeyGen(n,T)、Join(gpk,i)

产生的 (gpk, gsk, grt) 以及所有的 $j \in [1,T]$、RL_j、$i \in [1,n]$、消息 $M \in \{0,1\}^*$ 和 Web 站点信息 $S \in \{0,1\}^*$，满足下面的关系：Verify(gpk, j, RL_j， Sign($gpk, j, gsk[i], M, S$), M)=Valid ∧ Revocation($grt[i][j], S$) $\notin RL_j$。

2) 可追踪性：与文献[7,11]中方案相同，本文 BU-VLR 群签名方案采用隐式追踪算法，即对任意时间间隔 j，给定任何一个有效的签名消息对 (σ, M)，群管理员通过 $grt[i][j]$ 可以追踪到签名者。如果攻击者 A 在下面攻击游戏中不能获胜，则称方案满足可追踪性。攻击游戏步骤如下。

建立：挑战者运行 KeyGen(n,T)、Join(gpk, i)，获得 (gpk, gsk, grt)，向 A 提供 gpk, grt，此外设 U 是一个集合，主要用于记录被攻击者询问过密钥的群成员，初始时令其为空集。

询问：在任意时间间隔 $j \in [1,T]$， A 可以向挑战者询问如下。

① 签名询问：A 询问时刻间隔 j，任意群成员 i 对发给任意 Web 站点的任意消息 M 的签名，挑战者计算 $\sigma \leftarrow$ Sign($gpk, j, gsk[i], M, S$)，将 σ 发送给 A。

② 密钥询问： A 询问任意群成员 i 的密钥，挑战者将私钥 $gsk[i]$ 发送给 A 并将 i 添加到集合 U 中。

输出： A 输出 $(M^*, j^*, RL_{j^*}, \sigma^*)$。

如果以下条件同时成立，称 A 攻击成功：

① Verify($gpk, j^*, RL_{j^*}, \sigma^*, M^*$)=valid；

② 追踪 σ^* 到集合 $U \setminus RL_{j^*}$ 外的某个群成员或者追踪失败；

③ σ^* 不是 A 通过在 j^* 时间间隔对发给 Web 站点的消息 M^* 进行签名询问而获得的。

定义 5 如果攻击者 A 最多运行 t 时间，最多通过 q_S 次签名询问和 q_H 次散列询问后以不小于 ε 概率赢得上述攻击游戏，则称攻击者 A $(t, q_H, q_S, \varepsilon)$-—攻破 VLR 群签名方案的可追踪性。

3) BU-匿名性：BU-匿名性是指满足向 j_0 后无关联性的匿名性[11]。如果攻击者 A 在下面攻击游戏中不能获胜，则称方案满足 BU-匿名性。攻击游戏步骤如下。

建立：挑战者运行 KeyGen(n,T)、Join(gpk, i)，获得 (gpk, gsk, grt)，向 A 提供 gpk。

询问：在任意时间间隔 $j \in [1,T]$， A 可以向挑战者询问如下。

① 签名询问：A 询问时刻间隔，任意群成员 i 对发给任意 Web 站点的任意消息 M 的签名，挑战者回应相应的签名。

② 密钥询问： A 询问任意群成员 i 的密钥。

③ 撤销询问：A 询问时刻间隔 j，任意群成员 i 的撤销标记，挑战者回应 $grt[i][j]$。

挑战：A 输出 (M, i_0, i_1, j_0, S) 作为挑战，要求在当前时间间隔之前(包括时间间隔 j_0) A 未询问过群成员 i_0 和 i_1 的密钥以及撤销标记。挑战者随机选取 $\phi \in \{0,1\}$，计算 $\sigma \leftarrow \text{Sign}(gpk, j_0, gsk[i_\phi], M, S)$，将 σ 发送给 A。

限制性询问：除 j_0 时间间隔群成员成员 i_0 和 i_1 的密钥以及撤销标记外， A 可发出任何询问。由于向后无关联性，A 也可以询问时间间隔 j_0 之后群成员 i_0 和 i_1 的撤销标记。

输出： A 输出一比特值 ϕ'，作为对 ϕ 的猜测。

如果 $\phi' = \phi$， A 获胜，其优势定义为 $|\Pr[\phi' = \phi] - 1/2|$。

定义 6 如果攻击者 A 最多运行 t 时间，最多通过 q_S 次签名询问和 q_H 次散列询问后以不小于 ε 概率赢得上述攻击游戏，则称攻击者 A $(t, q_H, q_S, \varepsilon)$—攻破 VLR 群签名方案的 BU-匿名性。

定义 7 如果一个 VLR 群签名方案在满足正确性的同时不存在算法 $(t, q_H, q_S, \varepsilon)$—攻破方案的可追踪性以及不存在算法 $(t, q_H, q_S, \varepsilon)$—攻破方案的 BU-匿名性则称方案是 $(t, q_H, q_S, \varepsilon)$—安全的。

4 一种实用的 BU-VLR 群签名方案

本文提出的实用的 BU-VLR 群签名方案是在文献[11]中群签名方案的基础上扩展而来，下面简要介绍文献[11]中的群签名方案：方案的群公钥 $gpk = (g_1, \tilde{g}, g_2, h_j, \omega = g_2^{\gamma})$，其中 $g_2 \in G_2, g_1 = \varphi(g_2)$，$\varphi$ 是 G_2 到 G_1 的可计算同态映射， $\tilde{g} \in {}_R G_1$； 对所有 $j \in [1,T]$， 选择 $h_j \in {}_R G_2$； 对所有 $i \in [1,n]$， 群成员 i 私钥为一个 SDH 对 (A_i, x_i)， $A_i = (g_1)^{1/(\gamma + x_i)}$； 群成员 i 在时间间隔 j 的撤销标记为 $B_{ij} = \varphi(h_j)^{x_i}$。群成员 i 在时间间隔 j 生成的群签名由 $T_1 = A_i \tilde{g}^{\alpha}$， $T_2 = \varphi(f)^{\beta + x_i}, T_3 = \varphi(h_j)^{\beta}, \beta \in {}_R Z_p^*$ 以及签名的知识证明 SPK 组成，这里 $f = H_0(gpk, M, r)$ (散列函数 H_0: $G_1 \times G_2 \times \{0,1\}^* \to G_2$， 签名消息 $M \in \{0,1\}^*, r \in {}_R Z_p$)。撤销检查时通过验证 $e(T_2, h_j) = e(BT_3, f)$ 来判断该签名是否为合法群成员所签， $B \in RL_j$。

在构造本文方案时，为了防止群管理员(GM)陷害攻击，由群成员 i 选择的部分私钥 y_i 以及 GM 通过计算发送给群成员的二元组 (A_i,x_i) 共同组成群成员私钥 $gsk[i]=(A_i,x_i,y_i)$，从而使得方案具有防陷害性。在签名生成算法中，利用了文献[12]中的方法构造了 $T_1=A_i^{\alpha},\alpha\in {}_RZ_p^*$，利用文献[7]中的技巧构造了 $f=H_0(gpk,S,r)$，这里 Web 站点信息 $S\in\{0,1\}^*,r\in {}_R\{1,\cdots,k\}$ (与文献[7]中相同，取 $k=128$)，因此每个 Web 站点可能存在的 f 值为 k 个，所以 GM 可以预计算撤销信息 $e(B,f)$ 并添加到撤销列表 RL_j 中，其中 B 为群成员 i 在任意时间间隔 j 的撤销标记 $\varphi(h_j)^{x_i}$。同时用 $\beta y_i,\beta\in {}_RZ_p^*$ 替换上述 $T_2=\varphi(f)^{\beta+x_i},T_3=\varphi(h_j)^{\beta}$ 中的 β 进而构造出本文方案的 $T_3=\varphi(f)^{x_i+\beta y_i},T_4=\varphi(h_j)^{\beta y_i}$，而没有象文献[13]中方案那样，只是用 y_i 去替换 β，使得方案变成相关性方案。撤销检查时，Web 站点通过计算 $e(\varphi(h_j)^{x_i},f)=e(\varphi(f)^{x_i},h_j)=e(T_3,h_j)(1/e(T_4,f))$ (正确性证明见本文具体方案)，然后只需查找撤销列表中是否存在等于 $e(\varphi(h_j)^{x_i},f)$ 的值，从而使得撤销验证计算量与撤销列表长度无关。具体方案由以下算法组成。

1) KeyGen(n,T)：该密钥生成算法以成员个数 n 和时间间隔数目 T 为输入，算法如下。

step1　群管理员(GM)选择一生成元 $g_2\in G_2$，令 $g_1=\varphi(g_2),G_1=\langle g_1\rangle$，其中 φ 是 G_2 到 G_1 的可计算同态映射。选取 $\hat{h},\tilde{g}\in {}_RG_1,h_j\in {}_RG_2$，对所有 $j\in[1,T]$，令 $\hat{h}_j=\varphi(h_j)$。选择 2 个碰撞自由的散列函数 $H_0:G_1\times G_2\times\{0,1\}^*\to G_2,H:G_1\times G_2\times\{0,1\}^*\to Z_p$。

step2　对所有 $i\in[1,n]$，GM 选择 $x_i\in {}_RZ_p^*$，对所有 $i\in[1,n],j\in[1,T]$，计算 $B_{ij}=\hat{h}_j^{x_i}$。

step3　选择 $\gamma\in Z_p^*$，计算 $\omega=g_2{}^{\gamma}\in G_2$，$\gamma$ 仅有 GM 知道。

算法产生群公钥 $pk=(g_1,\hat{h},\tilde{g},g_2,h_1,\cdots,h_T,\omega)$，群成员在每个时间间隔 j 的撤销标记 $grt[i][j]=B_{ij}$，GM 公布群公钥 gpk。

2) Join(gpk,i)：用户需要加入群成为群成员 i 时，选择 $y_i\in {}_RZ_p^*$，计算 $\hat{h}^{y_i}$，同时发送 $\hat{h}^{y_i}$ 给 GM；GM 收到后计算 $A_i=(g_1\hat{h}^{y_i})^{1/(\gamma+x_i)}$，将二元组 (A_i,x_i) 通过安全信道发送给群成员 i，群成员 i 收到后，验证 $e(A_i,\omega g_2{}^{x_i})=e(g_1,g_2)e(\hat{h},g_2)^{y_i}$ 是否成立。如果成立，则接收 (A_i,x_i)，于是群成员 i 的私钥 $gsk[i]=(A_i,x_i,y_i)$，否则重新发送请求。

3) Sign($gpk,j,gsk[i],M,S$)：该签名算法输入为 $gpk=(g_1,\hat{h},\tilde{g},g_2,h_1,\cdots,h_T,\omega)$、当前时间间隔 j，签名者私钥 $gsk[i]=(A_i,x_i,y_i)$，签名消息 $M\in\{0,1\}^*$ 以及 Web 站点信息 $S\in\{0,1\}^*$，算法如下。

step1　选取随机数 $r\in {}_R\{1,\cdots,k\}$，计算：$f=H_0(gpk,S,r)\in G_2,\hat{f}=\varphi(f),\hat{h}_j=\varphi(h_j)$。

step2　选择随机数 $\alpha,\beta\in {}_RZ_p^*$，计算：$T_1=A_i^{\alpha},T_2=\hat{h}^{\alpha}\tilde{g}^{\beta},T_3=\hat{f}^{x_i+\beta y_i},T_4=\hat{h}_j^{\beta y_i}$。

step3　设 $\eta=\alpha y_i,\delta=\beta y_i$，生成知识签名：

$$\begin{aligned}V=SPK\{&(\alpha,\beta,x_i,y_i,\eta,\delta):T_2\\&=\hat{h}^{\alpha}\tilde{g}^{\beta}\wedge 1=T_2^{y_i}(1/\hat{h})^{\eta}(1/\tilde{g})^{\delta}\wedge e(T_1,\omega)\\&=e(g_1,g_2)^{\alpha}e(\hat{h},g_2)^{\eta}(1/e(T_1,g_2)^{x_i})\wedge T_3\\&=\hat{f}^{x_i+\delta}\wedge T_4=\hat{h}_j^{\delta}\}(M)。\end{aligned}$$

step4　选择盲化因子 $r_{\alpha},r_{\beta},r_{x_i},r_{y_i},r_{\eta},r_{\delta}\in {}_RZ_p$，计算：

$$\begin{aligned}&R_1=\hat{h}^{r_{\alpha}}\tilde{g}^{r_{\beta}},\\&R_2=T_2^{r_{y_i}}(1/\hat{h})^{r_{\eta}}(1/\tilde{g})^{r_{\delta}},\\&R_3=e(g_1,g_2)^{r_{\alpha}}e(\hat{h},g_2)^{r_{\eta}}(1/e(T_1,g_2)^{r_{x_i}}),\\&R_4=\hat{f}^{r_{x_i}+r_{\delta}},\\&R_5=\hat{h}_j^{r_{\delta}}。\end{aligned}$$

step5　计算挑战值 $c=H(gpk,j,M,T_1,T_2,T_3,T_4,R_1,R_2,R_3,R_4,R_5),c\in Z_p$。

step6　计算：$s_{\alpha}=r_{\alpha}+c\alpha,s_{\beta}=r_{\beta}+c\beta,s_{x_i}=r_{x_i}+cx_i,s_{y_i}=r_{y_i}+cy_i,s_{\eta}=r_{\eta}+c\eta,s_{\delta}=r_{\delta}+c\delta$，输出签名 $\sigma=(r,T_1,T_2,T_3,T_4,c,s_{\alpha},s_{\beta},s_{x_i},s_{y_i},s_{\eta},s_{\delta})$。

4) Verify(gpk,j,RL_j,σ,M)：该验证算法输入为 $gpk=(g_1,\hat{h},\tilde{g},g_2,h_1,\cdots,h_T,\omega)$、当前时间间隔 j、撤销列表 RL_j、签名 σ，签名消息 $M\in\{0,1\}^*$。被访问的 Web 站点通过验证签名的有效性来决定该用户是否具有访问权限。

step1　签名检查。

① 计算：$f=H_0(gpk,S,r),\hat{f}=\varphi(f),\hat{h}_j=\varphi(h_j)$。

② 计算：

$$\tilde{R}_1=\hat{h}^{s_{\alpha}}\ \tilde{g}^{s_{\beta}}(1/T_2)^c \tag{1}$$

$$\tilde{R}_2 = T_2^{s_{y_i}} (1/\hat{h})^{s_\eta} (1/\tilde{g})^{s_\delta} \quad (2)$$

$$\tilde{R}_3 = e(g_1, g_2)^{s_\alpha} e(\hat{h}, g_2)^{s_\eta} (1/e(T_1, g_2)^{s_{x_i}})(1/e(T_1, \omega))^c \quad (3)$$

$$\tilde{R}_4 = \hat{f}^{s_{x_i}+s_\delta} (1/T_3)^c \quad (4)$$

$$\tilde{R}_5 = \hat{h}_j^{s_\delta} (1/T_4)^c \quad (5)$$

③ 检查 c 的正确性：$c' = H(gpk, j, M, T_1, T_2, T_3, T_4, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5)$，如果 $c' \neq c$，则拒绝签名，否则执行下面步骤。

step2 撤销检查。

计算 $e(\hat{f}^{x_i}, h_j) = e(T_3, h_j)\ (1/e(T_4, f))$，查询撤销列表中是否存在等于 $e(\hat{f}^{x_i}, h_j)$ 的值，如果不存在，则接受该签名，用户获得访问该 Web 站点的权限，否则拒绝该签名并终止用户访问该 Web 站点。撤销检查的正确性证明如下：

$e(T_3, h_j) = e(\hat{f}^{x_i+\beta y_i}, h_j), e(T_4, f) = e(\hat{h}_j^{\beta y_i}, f) = e(\hat{h}_j, f)^{\beta y_i}$，如果设 $f = h_j^{\zeta} (\zeta \in Z_p^*)$[10]，则 $e(\hat{h}_j, f) = e(\varphi(h_j), h_j)^{\zeta} = e(\hat{f}, h_j), e(T_4, f) = e(\hat{f}, h_j)^{\beta y_i} = e(\hat{f}^{\beta y_i}, h_j)$，所以可得 $e(\hat{f}^{x_i}, h_j) = e(T_3, h_j)(1/e(T_4, f))$。

5) Revocation($grt[i][j], S$)：当需要在时间间隔 j 撤销群成员 i 访问某 Web 站点的权限时，GM 利用撤销标记 $grt[i][j]$ 和该 Web 站点信息 S 计算撤销信息 $e(\hat{h}_j^{x_i}, f)$ 并添加到撤销列表 RL_j 中，这里有 $e(\hat{h}_j^{x_i}, f) = e(\hat{f}^{x_i}, h_j)$。GM 将 RL_j 发送给各个 Web 站点，这样每个 Web 站点保存了一张 $|RL_j| \times k$ 的撤销列表用于撤销检查($|RL_j|$ 表示 j 时间间隔的撤销列表长度)。

定理 1 本文 **BU-VLR** 方案满足签名的正确性。

证明 方案的签名验证算法正确性证明如下。

Web 站点得到签名 $\sigma = (r, T_1, T_2, T_3, T_4, c, s_\alpha, s_\beta, s_{x_i}, s_{y_i}, s_\eta, s_\delta)$，计算：$f = H_0(gpk, S, r), \hat{f} = \varphi(f), \hat{h}_j = \varphi(h_j)$，则有：

$$\tilde{R}_1 = \hat{h}^{s_\alpha} \tilde{g}^{s_\beta} (1/T_2)^c = \hat{h}^{r_\alpha + c\alpha} \tilde{g}^{r_\beta + c\beta} (1/\hat{h}^\alpha \tilde{g}^\beta)^c = \hat{h}^{r_\alpha} \tilde{g}^{r_\beta} = R_1$$

$$\tilde{R}_2 = T_2^{s_{y_i}} (1/\hat{h})^{s_\eta} (1/\tilde{g})^{s_\delta} = T_2^{r_{y_i} + cy_i} (1/\hat{h})^{r_\eta + c\eta} (1/\tilde{g})^{r_\delta + c\delta}$$

$$= T_2^{r_{y_i}} (1/\hat{h})^{r_\eta} (1/\tilde{g})^{r_\delta} (\hat{h}^\alpha \tilde{g}^\beta)^{cy_i} (1/\hat{h})^{c\alpha y_i} (1/\tilde{g})^{c\beta y_i}$$

$$= T_2^{r_{y_i}} (1/\hat{h})^{r_\eta} (1/\tilde{g})^{r_\delta} = R_2$$

$$\tilde{R}_3 = e(g_1, g_2)^{s_\alpha} e(\hat{h}, g_2)^{s_\eta} (1/e(T_1, g_2)^{s_{x_i}})(1/e(T_1, \omega))^c$$

$$= e(g_1, g_2)^{r_\alpha + c\alpha} e(\hat{h}, g_2)^{r_\eta + c\eta} (1/e(T_1, g_2)^{r_{x_i} + cx_i})(1/e(T_1, \omega))^c$$

$$= e(g_1, g_2)^{r_\alpha} e(\hat{h}, g_2)^{r_\eta} (1/e(T_1, g_2)^{r_{x_i}}) e(g_1, g_2)^{c\alpha} \cdot e(\hat{h}, g_2)^{c\eta} (1/e(T_1, g_2)^{cx_i})(1/e(T_1, \omega))^c$$

$$= e(g_1, g_2)^{r_\alpha} e(\hat{h}, g_2)^{r_\eta} (1/e(T_1, g_2)^{r_{x_i}}) e(g_1, g_2)^{c\alpha} \cdot e(\hat{h}, g_2)^{c\alpha y_i} (1/e(T_1, \omega g_2^{x_i}))^c$$

$$= e(g_1, g_2)^{r_\alpha} e(\hat{h}, g_2)^{r_\eta} (1/e(T_1, g_2)^{r_{x_i}}) \cdot e(g_1^\alpha \hat{h}^{\alpha y_i}, g_2)^c (1/e(A_i^\alpha, \omega g_2^{x_i}))^c$$

$$= e(g_1, g_2)^{r_\alpha} e(\hat{h}, g_2)^{r_\eta} (1/e(T_1, g_2)^{r_{x_i}}) \cdot e(g_1^\alpha \hat{h}^{\alpha y_i}, g_2)^c (1/e((g_1\ \hat{h}^{y_i})^{\alpha/(\gamma+x_i)}, g_2^{\gamma+x_i}))^c$$

$$= e(g_1, g_2)^{r_\alpha} e(\hat{h}, g_2)^{r_\eta} (1/e(T_1, g_2)^{r_{x_i}}) \cdot e(g_1^\alpha \hat{h}^{\alpha y_i}, g_2)^c (1/e(g_1^\alpha\ \hat{h}^{\alpha y_i}, g_2))^c$$

$$= e(g_1, g_2)^{r_\alpha} e(\hat{h}, g_2)^{r_\eta} (1/e(T_1, g_2)^{r_{x_i}}) = R_3$$

$$\tilde{R}_4 = \hat{f}^{s_{x_i}+s_\delta} (1/T_3)^c = \hat{f}^{r_{x_i}+cx_i+r_\delta+c\delta} (1/\hat{f}^{x_i+\beta y_i})^c$$

$$= \hat{f}^{r_{x_i}+r_\delta}\ \hat{f}^{cx_i+c\beta y_i} (1/\hat{f}^{x_i+\beta y_i})^c = \hat{f}^{r_{x_i}+r_\delta} = R_4$$

$$\tilde{R}_5 = \hat{h}_j^{s_\delta} (1/T_4)^c = \hat{h}_j^{r_\delta + c\delta} (1/\hat{h}_j^{\beta y_i})^c$$

$$= \hat{h}_j^{r_\delta}\ \hat{h}_j^{c\beta y_i} (1/\hat{h}_j^{\beta y_i})^c = \hat{h}_j^{r_\delta} = R_5$$

综上可得，本文方案的群成员私钥生成算法和签名验证算法都是正确的，所以本文方案是正确的。

定理 2 上述方案中的 V 是关于知识 $(\alpha, \beta, x_i, y_i, \eta, \delta)$ 的一个签名的知识证明，满足关系：$T_1 = (g_1^\alpha \hat{h}^\eta)^{1/(\gamma+x_i)}$, $T_2 = \hat{h}^\alpha \tilde{g}^\beta$, $T_3 = \hat{f}^{x_i+\beta y_i}$, $T_4 = \hat{h}_j^{\beta y_i}$。

证明 在上述方案的 V 中，假设零知识协议有一个提取器[12]，它可以使证明者回到零知识协议的最初阶段，于是由同样的随机输入即相同的 (T_1, T_2, T_3, T_4)，就可以得到 2 个不同的挑战—应答对：$(c, s_\alpha, s_\beta, s_{x_i}, s_{y_i}, s_\eta, s_\delta)$ 和 $(c', s'_\alpha, s'_\beta, s'_{x_i}, s'_{y_i}, s'_\eta, s'_\delta)$，令 $\Delta c = c - c', \Delta s_\alpha = s_\alpha - s'_\alpha, \Delta s_\beta = s_\beta - s'_\beta$，$\Delta s_{x_i} = s_{x_i} - s'_{x_i}$，$\Delta s_{y_i} = s_{y_i} - s'_{y_i}, \Delta s_\eta = s_\eta - s'_\eta, \Delta s_\delta = s_\delta - s'_\delta$。由于 2 个不同的挑战—应答对，可由等式(1)的 2 个不同实例相除得到：$T_2^{\Delta c} = \hat{h}^{\Delta s_\alpha} \tilde{g}^{\Delta s_\beta}$，$T_2 = \hat{h}^{\Delta s_\alpha / \Delta c} \tilde{g}^{\Delta s_\beta / \Delta c}$，令 $\alpha = \Delta s_\alpha / \Delta c, \beta = \Delta s_\beta / \Delta c$；同样可由等式(2) 2 个不同实例相除得到 $T_2^{\Delta s_{y_i}} = \hat{h}^{\Delta s_\eta} \tilde{g}^{\Delta s_\delta}$，因为有 $T_2 = \hat{h}^\alpha \tilde{g}^\beta$，所以 $\hat{h}^{\alpha \Delta s_{y_i}} \tilde{g}^{\beta \Delta s_{y_i}} = \hat{h}^{\Delta s_\eta} \tilde{g}^{\Delta s_\delta}$，可得 $\Delta s_\eta = \alpha \Delta s_{y_i}$, $\Delta s_\delta = \beta \Delta s_{y_i}$；类似地可由等式(3) 2 个不同实例相除得到 $e(T_1, \omega)^{\Delta c} = e(g_1, g_2)^{\Delta s_\alpha} e(\hat{h}, g_2)^{\Delta s_\eta} e(T_1, g_2)^{-\Delta s_{x_i}}$，令 $\eta = \Delta s_\eta / \Delta c, x_i = \Delta s_{x_i} / \Delta c$，则 $e(T_1, \omega) = e(g_1, g_2)^\alpha$

$e(\hat{h},g_2)^{\eta}\ e(T_1,g_2)^{-x_i}$，而 $e(T_1,\omega)e(T_1,g_2)^{x_i}=e(g_1,g_2)^{\alpha}$ $e(\hat{h},g_2)^{\eta}, e(T_1,\omega g_2{}^{x_i})=e(g_1,g_2)^{\alpha}e(\hat{h},g_2)^{\eta}$，令 $\hat{h}=g_1^{\zeta}, T_1=\ g_1{}^{\theta}, \zeta,\theta\in_R Z_p^*$，由 $\omega=g_2{}^{\gamma}$ 可得：$e(g_1{}^{\theta},g_2{}^{\gamma+x_i})=e(g_1,g_2)^{\alpha}e(g_1{}^{\zeta},g_2)^{\eta}, e(g_1,g_2)^{\theta(\gamma+x_i)}$ $=e(g_1,g_2)^{\alpha+\zeta\eta}$，由上式可得 $\theta(\gamma+x_i)=\alpha+\zeta\eta(\mathrm{mod}\,p)$，所以 $T_1=g_1{}^{(\alpha+\zeta\eta)/(\gamma+x_i)}=(g_1{}^{\alpha}\hat{h}^{\eta})^{1/(\gamma+x_i)}$，此外我们由等式(4)、式(5)还可以提取出满足 $T_3=\hat{f}^{x_i+\beta y_i}$ 和 $T_4=\hat{h}_j{}^{\beta y_i}$ 的 y_i 并且有 $\delta=\beta y_i$。

5　安全性分析

5.1　BU-匿名性

定理 3　若攻击者 $A\ (t,q_H,q_S,\varepsilon)$—攻破 VLR 群签名方案的 BU-匿名性，则存在算法 B 以 $(1/nT-q_Sq_H(p+k)/2pk)\varepsilon$ 概率解决 DLDH 困难问题。

证明　证明的主要思路基于文献[11]。假定攻击者 A 在最多 t 时间内，最多通过 q_S 次签名询问和 q_H 次散列询问后以不小于 ε 概率攻破方案的 BU-匿名性，就可以构造一个算法 B 以 $(1/nT-q_Sq_H(p+k)/2pk)\varepsilon$ 概率解决群 G_2 上的 DLDH 困难问题。算法 B 的输入为 $(u,v,h,u^a,v^b,Z)\in G_2{}^6, a,b\in_R Z_p^*, Z=h^{a+b}$ 或 $Z=h^c, c\in_R Z_p^*$，B 通过与 A 交互来区分 Z。可以将 DLDH 困难问题的输入 u,v,h,u^a,v^b,h^{a+b} 看作如下形式：$u=g_2, v=h_j, h=f, u^a=g_2{}^{x_i}, v^b=h_j{}^{\beta y_i}, h^{a+b}=f^{x_i+\beta y_i}$，于是 DLDH 困难问题变成 $h^{a+b}=f^{x_i+\beta y_i}$ 和随机值 h^c 不可区分。

1) 建立：为了不改变文献[11]中 BU-匿名性的攻击模型，给定 B 以同样的模拟能力，这也是为什么在模拟 Join(gpk,i)时由 B 来选择群成员部分私钥 y_i 的原因。在模拟 KeyGen(n,T)，B 首先以一定概率选取最后会被攻击者 A 用来挑战的群成员 i^* 以及时间间隔 j^*，然后将 DLDH 困难问题的输入 u,v,h,u^a,v^b,h^{a+b} 以上述形式模拟成方案的相关参数。

B 模拟 KeyGen(n,T)如下：

① B 选择 $i^*\in_R[1,n], j^*\in_R[1,T]$，设 $g_2=u$, $g_1=\varphi(g_2)$，φ 是 G_2 到 G_1 的可计算同态映射，选取 $\hat{h},\tilde{g}\in_R G_1, r_j\in_R Z_p^*$；当 $j\neq j^*$，计算 $h_j=g_2{}^{r_j}$，当 $j=j^*$，令 $h_{j^*}=v$；对所有 $j\in[1,T]$，都有 $\hat{h}_j=\varphi(h_j)$。

② 当 $i\neq i^*$ 时，B 选择 $x_i\in_R Z_p^*$，当 $i=i^*$ 时，定义 $x_{i^*}=a$，B 不知道 x_{i^*}。对 $i\neq i^*$ 和所有 $j\in[1,T]$，计算 $B_{ij}=\hat{h}_j{}^{x_i}$；对 $i=i^*, j\neq j^*$，计算 $B_{i^*j}=\varphi((u^a)^{r_j})$ $=\varphi(g_2{}^{ar_j})=\hat{h}_j{}^{a}$；对 $i=i^*, j=j^*$，定义 $B_{i^*j^*}=\varphi(v^a)$ $=\hat{h}_{j^*}{}^{x_{i^*}}$，$B$ 无法计算 $B_{i^*j^*}$，因为 B 不知道 a。

③ B 选择 $\gamma\in Z_p^*$，计算 $\omega=g_2{}^{\gamma}\in G_2$。$B$ 获得 $gpk=(g_1,\hat{h},\tilde{g},g_2,h_1,\cdots,h_T,\omega)$, $grt[i][j]=B_{ij}$ (除 $B_{i^*j^*}$ 外)，向 A 提供 gpk。

B 模拟 Join(gpk,i)如下：

对所有 $i\in[1,n]$，B 选择 $y_i\in_R Z_p^*$，当 $i\neq i^*$ 时，计算 $A_i=(g_1\hat{h}^{y_i})^{1/(\gamma+x_i)}$；当 $i=i^*$ 时，定义 $A_{i^*}=(g_1\hat{h}^{y_{i^*}})^{1/(\gamma+x_{i^*})}$，$B$ 无法计算 A_{i^*}，因为 B 不知道 a。B 获得群成员私钥 $gsk[i]=(A_i,x_i,y_i)$，除 A_{i^*} 外。

2) 散列询问：敌手 A 可以任意询问散列函数 H_0 和 H，B 选择随机值作为应答，应答的值前后一致。

3) 询问：在任意时间间隔 j，A 可以进行签名询问，密钥询问和撤销询问。当 $i\neq i^*$，B 知道群成员 i 的密钥，可以正确应答各种询问。当 $i=i^*$，B 模拟挑战者与攻击者 A 交互如下。

签名询问：A 询问任意时间间隔 j，群成员 i^* 对发给任意 Web 站点的任意消息 M 的签名，B 模拟签名如下。

当 $j\neq j^*$ 时：

① B 选择 $r\in_R\{1,\cdots,k\}$ 和 $\beta,\zeta\in_R Z_p^*$，令 $f=h_j{}^{\zeta}$, $\hat{f}=\varphi(f)$, $\hat{h}_j=\varphi(h_j)$。

② B 选择 $T_1,T_2\in_R G_1$，计算 $T_3=\hat{f}^{\beta y_{i^*}}B_{i^*j}{}^{\zeta}$ $=\hat{f}^{\beta y_{i^*}}\ \hat{h}_j{}^{x_{i^*}\zeta}=\hat{f}^{x_{i^*}+\beta y_{i^*}}, T_4=\hat{h}_j{}^{\beta y_{i^*}}$。

③ B 利用完备零知识的模拟器，计算模拟的 V（具体过程请参看文献[11,12]）：随机选取 $c,s_\alpha,s_\beta,s_{x_i},s_{y_i},s_\eta,s_\delta\in_R Z_p^*$，利用等式(1)~式(5)，计算相应的 $\tilde{R}_1,\tilde{R}_2,\tilde{R}_3,\tilde{R}_4,\tilde{R}_5$，并定义 $H_0(gpk,S,r)$ $=f, H(gpk,j,M,T_1,T_2,T_3,T_4,\tilde{R}_1,\tilde{R}_2,\tilde{R}_3,\tilde{R}_4,\tilde{R}_5)=c$，输出签名 $\sigma=(r,T_1,T_2,T_3,T_4,c,s_\alpha,s_\beta,\ s_{x_i},s_{y_i},s_\eta,s_\delta)$。如果之前 A 询问过 $H_0(gpk,S,r)$ 或 $H(gpk,j,M,T_1,T_2,T_3,$ $T_4,\tilde{R}_1,\tilde{R}_2,\tilde{R}_3,\tilde{R}_4,\tilde{R}_5)$，则 B 输出一个随机猜测值 $w'\in_R\{0,1\}$ 并终止。这里 $w'=1$，表示 B 猜测 $Z=h^{a+b}$；$w'=0$ 表示 B 猜测 $Z=h^c$。

当 $j=j^*$ 时：

① B 选择 $r\in_R\{1,\cdots,k\}$ 和 $\beta,\zeta\in_R Z_p^*$，令 $f=u^{\zeta},\hat{f}=\varphi(f),\hat{h}_j=\varphi(h_j)$。

② B 选择 $T_1,T_2\in_R G_1$，计算 $T_3=\varphi((u^a)(u^{\beta y_{i^*}})^{\zeta}=\varphi(f^{a+\beta y_{i^*}})=\hat{f}^{x_{i^*}+\beta y_{i^*}}$，$T_4=\hat{h}_j^{\beta y_{i^*}}$。

③ 同 $j\neq j^*$ 情况。

撤销询问：A 询问时间间隔 j，群成员 i^* 的撤销标记，若 $j\neq j^*$ 时，B 回应 B_{i^*j}，否则输出一个随机猜测值 $w'\in_R\{0,1\}$ 并终止。

密钥询问：A 询问群成员 i^* 的密钥，B 输出一个随机猜测值 $w'\in_R\{0,1\}$ 并终止。

4) 挑战：敌手 A 输出消息 M、Web 站点信息 S、时间间隔 j 以及 2 个群成员标识 i_0,i_1，作为他对群签名方案 BU-匿名性的挑战。若 $j\neq j^*$，B 输出一个随机猜测值 $w'\in_R\{0,1\}$ 并终止；否则 B 选取 $\phi\in_R\{0,1\}$。如果 $i_\phi\neq i^*$，B 输出一个随机猜测值 $w'\in_R\{0,1\}$ 并终止，否则 B 模拟群签名如下：

① 选择 $r\in_R\{1,\cdots,k\}$，令 $b=\beta y_{i^*}$，B 不知道该值，同时设 $f=h,\hat{f}=\varphi(f),\hat{h}_{j^*}=\varphi(h_{j^*})$。

② B 选择 $T_1,T_2\in_R G_1$，令 $T_3=\varphi(Z),T_4=\varphi(v^b)=\hat{h}_{j^*}^{\beta y_{i^*}}$，如果 $Z=h^{a+b}$，则 $T_3=\varphi(h^{a+b})=\hat{f}^{x_{i^*}+\beta y_{i^*}}$。

③ 利用完备零知识的模拟器，B 计算模拟的 V，如果之前 A 询问过 $H_0(gpk,S,r)$ 或 $H(gpk,j,M,T_1,T_2,T_3,T_4,\tilde{R}_1,\tilde{R}_2,\tilde{R}_3,\tilde{R}_4,\tilde{R}_5)$，则 B 输出一个随机猜测值 $w'\in_R\{0,1\}$ 并终止；否则，输出签名 $\sigma=(r,T_1,T_2,T_3,T_4,c,s_\alpha,s_\beta,s_{x_i},s_{y_i},s_\eta,s_\delta)$。

5) 限制性询问：唯一限制是 A 不能询问群成员 i_0 和 i_1 的密钥以及在 j^* 时间间隔的撤销标记。

6) 输出：A 输出他的猜测 $\phi'\in_R\{0,1\}$。如果 $\phi=\phi'$，B 输出 $w'=1$，否则输出 $w'=0$。

根据本文 2.2 节给出的 DLDH 假定，计算 B 的猜测优势 $|\Pr[A(u,v,h,u^a,v^b,h^{a+b})=1]-\Pr[A(u,v,h,u^a,v^b,h^c)=1]|$。令 $w=0$ 表示 Z 的输入为 h^c；$w=1$ 表示 Z 的输入为 h^{a+b}；$abort$ 表示事件 B 终止。如果 B 终止，则有 $\Pr[w'=0|abort\wedge w=0]=1/2$，$\Pr[w'=1|abort\wedge w=1]=1/2$，表示如果算法 B 终止且 Z 的输入为 h^c 或 h^{a+b} 的情况下，B 猜测正确的概率为 $1/2$，则猜测错误的概率也为 $1/2$。如果 B 没有终止，当 $w=0$ 时，Z 的输入 h^c 为一随机数，那么敌手 A 只能靠猜测来判断 ϕ，则有 $\Pr[w'=0|\overline{abort}\wedge w=0]=1/2$，表示算法 B 没有终止且 Z 的输入为 h^c 的情况下，B 猜测正确的概率为 $1/2$；当 $w=1$ 时，B 完美模拟真实签名且敌手 A 以 ε 优势猜测正确，则有 $\Pr[w'=1|\overline{abort}\wedge w=1]=1/2+\varepsilon$，表示算法 B 没有终止且 Z 的输入为 h^{a+b} 的情况下，B 猜测正确的概率为 $1/2+\varepsilon$。

综合以上分析，计算 B 的猜测优势如下：

$$
\begin{aligned}
&|\Pr[A(u,v,h,u^a,v^b,h^{a+b})=1]-\Pr[A(u,v,h,u^a,v^b,h^c)=1]|\\
&=|\Pr[w'=1|w=1]-\Pr[w'=1|w=0]|\\
&=|\Pr[w'=1|w=1]-(1-\Pr[w'=0|w=0)|\\
&=|\Pr[abort]\Pr[w'=1|abort\wedge w=1]+\Pr[\overline{abort}]\cdot\\
&\Pr[w'=1|\overline{abort}\wedge w=1]-1+\Pr[abort]\cdot\\
&\Pr[w'=0|abort\wedge w=0]+\Pr[\overline{abort}]\cdot\\
&\Pr[w'=0|\overline{abort}\wedge w=0])|\\
&=|\Pr[abort](1/2+1/2)-1+\Pr[\overline{abort}]((1/2+\varepsilon)+1/2)|\\
&=|\Pr[\overline{abort}]|\varepsilon
\end{aligned}
$$

这里 $\Pr[\overline{abort}]$ 表示事件 B 没有终止的概率：如果 B 没有终止，首先需要选对 i^* 和 j^*，这一概率至少为 $1/nT$，其次减去由于 q_S 次签名询问，A 已询问过 B 产生的散列值，导致 B 终止的概率，这一概率的算术平均值为 $q_Sq_H(p+k)/2pk$，则 $\Pr[\overline{abort}]=1/nT-q_Sq_H(p+k)/2pk$。综上所述，如果敌手 A 在最多 t 时间内，经过 q_S 次签名询问和 q_H 次散列询问后以不小于 ε 概率攻破方案的 BU-匿名性，则可以构造一个算法 B 以 $(1/nT-q_Sq_H(p+k)/2pk)\varepsilon$ 概率解决 DLDH 困难问题，这与 DLDH 假设相矛盾，所以本文方案满足 BU-匿名性。

5.2 可追踪性

定理 4 若攻击者 A (t,q_H,q_S,ε)—攻破群签名方案的可追踪性，则存在算法 B 以 $(\varepsilon-1/p)/(4q_H)$ 概率解决(n+1)-SDH 困难问题，或以 $(\varepsilon/n-1/p)/(4q_H)$ 概率解决 n-SDH 困难问题。

证明 证明的主要思路基于文献[11]。假定攻击者 A 在最多 t 时间内，最多通过 q_S 次签名询问和 q_H 次散列询问后以不小于 ε 概率攻破方案的可追踪性，即攻击者 A 伪造出一个签名而群管理员通过撤销标记追踪不到真正的签名人或者追踪失败，则可以构造一个算法 B 以 $(\varepsilon-1/p)/(4q_H)$ 概率解决(n+1)-SDH 困难问题，或以 $(\varepsilon/n-1/p)/(4q_H)$ 概率解决 n-SDH 困难问题。

1) 建立：假设给定 B 以 $(g_1, g_2, \omega = g_2^{\gamma})$ 和 n 个群成员密钥对 (A_i, x_i, y_i)。对每个 $i \in [1,n]$，如果 (A_i, x_i, y_i) 已知，设 $s_i = 1$；如果 x_i, y_i 已知而 A_i 未知，设 $s_i = 0$。B 选取 $\tilde{g} \in {}_R G_1, \zeta \in {}_R Z_p^*$，计算 $\hat{h} = g_1^{\zeta}$；对每个 $i \in [1,n], j \in [1,T]$，B 选取 $h_j \in {}_R G_2$，计算 $B_{ij} = \hat{h}_j^{x_i}$。$(g_1, g_2, \omega = g_2^{\gamma})$ 下的 SDH 对为 $(\overline{A}_i, x_i)$，其中 $\overline{A}_i = A_i^{1/(\zeta y_i + 1)}$。

则 B 获得 $gpk = (g_1, \hat{h}, \tilde{g}, g_2, h_1, \cdots, h_T, \omega)$，$grt = (B_{11}, \cdots, B_{nT})$，$gsk[i] = (A_i, x_i, y_i)$（当 $s_i = 0$ 时，A_i 未知），向 A 提供 gpk, grt。B 模拟挑战者与 A 交互如下。

2) 散列询问：敌手 A 可以任意询问散列函数 H_0 和 H，B 选择随机值作为应答，应答的值前后一致。

3) 签名询问：敌手 A 询问时刻间隔 j，任意成员 i 对发给 Web 站点的任意消息 M 的签名。如果 $s_i = 1$，因为 B 知道密钥 (A_i, x_i, y_i)，所以可以正确应答；如果 $s_i = 0$，选取 $r \in {}_R Z_p, \beta \in {}_R Z_p^*, T_1, T_2 \in {}_R G_1$，计算 $f = H_0(gpk, S, r), T_3 = \hat{f}^{x_i + \beta y_i}$，$T_4 = \hat{h}_j^{\beta y_i}$，同时利用完备零知识的模拟器，计算模拟的 V (BU-匿名性的证明中有其简要过程)，如果之前 A 询问过散列值 $H_0(gpk, S, r)$ 或 $H(gpk, j, M, T_1, T_2, T_3, T_4, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5)$，则 B 失败并终止，反之输出 $(r, T_1, T_2, T_3, T_4, V)$，这里 $V = (c, s_\alpha, s_\beta, s_{x_i}, s_{y_i}, s_\eta, s_\delta)$。

4) 密钥询问：敌手 A 询问成员 i 的密钥，如果 $s_i = 1$，B 以秘密钥 (A_i, x_i, y_i) 作为应答，若 $s_i = 0$，B 失败并终止。

5) 输出：敌手 A 输出一个含有秘密钥 A_i 伪造的签名 $\sigma^* = (r^*, T_1^*, T_2^*, T_3^*, T_4^*, V^*)$。通过 B_{ij} 可以追踪群成员身份，如果伪造的成员身份不在群中，即身份追踪失败，则输出签名 σ^*；如果身份追踪到某成员 i 且 $s_i = 0$，则输出签名 σ^*；否则终止。

在上面的伪造活动中，存在 2 种类型的伪造：一是伪造不属于任何一个群成员 i 的签名；二是伪造某个群成员 i 的签名。

下面分析这 2 种伪造类型成功的概率：

给定一个 q-SDH 的实例 $(g_1', g_2', (g_2')^{\gamma}, \cdots, (g_2')^{\gamma^q})$，利用文献[18]中的方法，可以得到 $(g_1, g_2, \omega = (g_2)^{\gamma})$ 和 $q-1$ 个 SDH 对 $(\overline{A}_i, x_i)$ 满足 $e(\overline{A}_i, \omega (g_2)^{x_i}) = e(g_1, g_2)$。另一方面，任何一个不同于上面 $q-1$ 个 SDH 对的 $(\overline{A}, x)$ 都是该 q-SDH 困难问题的一个解。

伪造类型 1：从一个(n+1)-SDH 实例中，可以得到 $(g_1, g_2, \omega = (g_2)^{\gamma})$ 和 n 个 SDH 对 $(\overline{A}_i, x_i)$。A 运行上面的询问，输出一个用 $(A_{i'}, x_{i'}, y_{i'})$ 得到的签名，这里有 $\overline{A}_{i'} = A_{i'}^{1/(\zeta y_{i'} + 1)}$ 且 $\overline{A}_{i'} \neq \overline{A}_i, i \in [1,n]$。$A$ 以优势 ε 伪造成功。

伪造类型 2：从一个 n-SDH 实例中，可以得到 $(g_1, g_2, \omega = (g_2)^{\gamma})$ 和 $n-1$ 个 SDH 对 $(\overline{A}_i, x_i)$，对这 $n-1$ 个 SDH 对设 $s_i = 1$。对于未分布的那个随机数 i'，选取 $x_{i'}, y_{i'} \in {}_R Z_p^*$（$\overline{A}_{i'}$ 未知）且令 $s_{i'} = 0$。A 运行上面的询问，则仅当 A 未询问成员 i' 的密钥且伪造的签名含有 $\overline{A}_{i'}^{(\zeta y_{i'} + 1)}$，才会成功。$i'$ 的值与 A 的观测值相独立，因此 A 伪造成员 i' 的签名成功的概率至少为 ε / n。

下面分析怎样构造出另一个 SDH 对。

对于相同的消息 M 和时间间隔 j，重新运行上述的攻击活动，则 V 中的承诺相同而挑战-应答不同，根据定理 2，可以获得元组 $(\alpha^*, \beta^*, x^*, y^*, \eta^*, \delta^*, T_1^*, T_2^*, T_3^*, T_4^*)$ 使得 $T_1^* = (g_1^{\alpha^*} \hat{h}^{\eta^*})^{1/(\gamma + x^*)}$，$T_2^* = \hat{h}^{\alpha^*} \tilde{g}^{\beta^*}$，$e(T_3^*, h_j) = e(\varphi(h_j)^{x^*} T_4^*, f)$，并且对于所有 i，有 $x^* \neq x_i$。同文献[11]，根据 *forking* 引理[19]，这一成功的概率至少为 $(\varepsilon' - 1/p)^2 / (16 q_H)$，这里 ε' 表示 A 伪造成功的概率。如果存在 $\alpha^* + \zeta \eta^* = 0 (\mathrm{mod}\, p)$，则终止；否则计算：$T_1^* = (g_1^{\alpha^*} \hat{h}^{\eta^*})^{1/(\gamma + x^*)} = (g_1^{\alpha^*} g_1^{\zeta \eta^*})^{1/(\gamma + x^*)} = (g_1^{\alpha^* + \zeta \eta^*})^{1/(\gamma + x^*)}$，因为有 $\alpha^* + \zeta \eta^* \neq 0 (\mathrm{mod}\, p)$，则 $(T_1^*)^{1/(\alpha^* + \zeta \eta^*)} = g_1^{1/(\gamma + x^*)}$，于是获得另一个 SDH 对 $(\overline{A}^*, x^*)$，$\overline{A}^* = (T_1^*)^{1/(\alpha^* + \zeta \eta^*)}$。如果令 ε'' 表示 A 成功伪造签名，且存在元组 $(\alpha^*, \beta^*, x^*, y^*, \eta^*, \delta^*, T_1^*, T_2^*, T_3^*, T_4^*)$ 使得 $\alpha^* + \zeta \eta^* \neq 0 (\mathrm{mod}\, p)$ 的概率，则有：对于第 1 类伪造，存在算法 B 以 $(\varepsilon'' - 1/p)^2 (16 / q_H)$ 概率解决(n+1)-SDH 假设；对于第 2 类伪造存在算法 B 以 $(\varepsilon'' / n - 1/p)^2 (16 / q_H)$ 概率解决 n-SDH 假设，正确猜测 A 所使用伪造类型的概率为 1/2。如果 $\varepsilon'' \geqslant \varepsilon / 2$，则存在算法 B 以 $(\varepsilon - 1/p)^2 (4 / q_H)$ 概率攻破(n+1)-SDH 假设，或以 $(\varepsilon / n - 1/p)^2 (4 / q_H)$ 概率攻破 n-SDH 假设，这与 q-SDH 假设相矛盾，因此本文的方案具有可追踪性。

表 1 现有 VLR 群签名方案的性能比较

签名方案	签名长度/比特	签名过程计算量	验证过程计算量	BU	防陷害性
文献[7]	1 192	8ME+2BM	6ME+(3+2|RL|)BM	NO	NO
文献[8]	2 893	11ME+4BM	7ME+(4+|RL_j|)BM	YES	NO
文献[9]	2 557	11ME+2BM	7ME+(2+2|RL_j|)BM	YES	NO
文献[11]	1 533	8ME+2BM	4ME+(3+|RL_j|)BM	YES	NO
文献[12]	1 363	8ME+1BM	5ME+(2+|RL_j|)BM	YES	NO
文献[13]	1 533	8ME+2BM	5ME+3BM	NO	YES
文献[14]	1 533	7ME+2BM	4ME+3BM	NO	YES
文献[16]	1 363	8ME+1BM	5ME+(2+|RL_j|)BM	YES	NO
本文方案	1 881	11ME+2BM	7ME+4BM	YES	YES

6 性能与比较

签名长度：本文方案的签名为 $\sigma=(r,T_1,T_2,T_3,T_4,c,s_\alpha,s_\beta,s_{x_i},s_{y_i},s_\eta,s_\delta)$，其中包含了 4 个 G_1 中元素 T_1,T_2,T_3,T_4，7 个 Z_p 中元素 $c,s_\alpha,s_\beta,s_{x_i},s_{y_i},s_\eta,s_\delta$ 以及一个 7bit 长度的 r。p 是长为 170bit 的素数，G_1 中元素长为 171bit，因此本文方案的签名长度为 1 881bit。

计算代价：定义 ME 为指数(包括多指数)运算，BM 为双线性运算，因为同态映射的计算代价接近于 ME[7]，所以也记为 ME。本文方案签名过程需要 11ME 和 2BM，在验证过程需要 7ME 和 4BM，验证过程计算量与撤销列表长度无关。

表 1 给出了现有 VLR 群签名方案的性能比较，主要是从签名长度、签名及验证过程计算量、是否具有 BU 性和防陷害性方面加以比较。表中签名及验证过程计算量的估算参照文献[7]的标准，这也是为什么表中某些方案的计算量会和其在原文中得出的计算量略有不同的原因(表中 $|RL|$ 表示撤销列表长度，$|RL_j|$ 表示时间间隔 j 的撤销列表长度)。

签名长度方面，本文方案并不占优，文献[12]中方案的签名长度是目前本地验证者撤销群签名方案中签名长度最短的。此外，魏等对文献[11]中的方案进行改进，使得方案的签名长度只有 1 193bit。签名过程计算量方面，本文只比计算量最小的，文献[12]中的方案多 1BM，因为在实际计算中，ME 计算量和 BM 计算量比起来是可以忽略不计的。同理，在验证过程计算量方面，本文也只比计算量最小的，文献[14]中的方案多 1BM。同时只有本文方案和文献[13,14]中的方案能够使得撤销验证计算量与撤销列表长度无关，其他方案在撤销验证计算量方面都是与撤销列表长度线性相关的，这也是本地验证者撤销群签名方案的最大缺点。最后，在向后无关联性和防陷害性方面，只有本文方案能够同时满足。这 2 个性质在群签名方案的实际应用中有着很重要的作用。(注：这里没有列出文献[10]中方案参与性能比较，是因为文献[10]中的 3 个方案都是基于新的安全假设，所以不好与现有 VLR 群签名方案进行比较)

综上所述，本文方案不仅验证过程计算量与撤销列表长度无关，而且具有向后无关联性和防陷害性，这是目前 VLR 群签名方案所不能同时满足的。但是本文方案为了预计算撤销信息会使得部分签名变的可链接[7]：当群成员发给同一个 Web 站点的两个签名中使用了相同的 r 时，该 Web 站点可以测试出这两个签名来自同一个用户。但在一些实际应用中，以此来获得高效撤销还是可以接受的(本文中 $k=128$，也仅有不足1% 的签名变得可链接)。

7 结束语

本文提出了一个实用的 BU-VLR 群签名方案，方案的安全性建立在随机预言模型下的 q-SDH 假设和 DLDH 假设之上，并且满足防陷害性和向后无关联性。该方案在移动环境中的隐私保护证明方面有着广泛的应用前景。

参考文献：

[1] CHAUM D, HEYST V E. Group signatures[A]. Advances in Cryptology-EUROCRYPT'1991[C]. Berlin: Springer-Verlag, 1991. 257-265.

[2] CAMENISCH J, LYSYANSKAYA A. Dynamic accumulators and application to efficient revocation of anonymous credentials[A]. Ad-

vances in Cryptology-CRYPTO'2002[C]. Berlin: Springer-Verlag, 2002. 61-76.

[3] TSUDIK G, XU S. Accumulating composites and improved group signing[A]. Advances in Cryptology- ASIACRYPT' 2003[C]. Berlin: Springer-Verlag, 2003. 269-286.

[4] NGUYEN L. Accumulators from bilinear pairings and applications[A]. Proc of the CT-RSA'2005[C]. Berlin: Springer-Verlag, 2005. 275-292.

[5] JIN H M, WONG D S, XU Y L. Efficient group signature with forward secure revocation[A]. SecTech' 2009[C]. Berlin: Springer-Verlag, 2009. 124-131.

[6] ATENIESE G, SONG D, TSUDIK G. Quasi-efficient revocation in group signatures[A]. Proc of the Final Cryptology' 2002[C]. Berlin: Springer-Verlag, 2003. 183-197.

[7] BONEH D, SHACHAM H. Group signatures with verifier-local revocation[A]. Proc of the Computer and Communications Security'2004[C]. New York: ACM Press, 2004. 168-177.

[8] NAKANISHI T, FUNABIKI N. Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps[A]. Advances in Cryptology-ASIACRYPT'2005[C]. Berlin: Springer- Verlag, 2005. 533-548.

[9] ZHOU S J, LIN D D. A shorter group signature with verifier-local revocation and backward unlinkability[EB/OL]. http://eprint.iacr.org / 2006/100.

[10] ZHOU S J, LIN D D. Shorter verifier-local revocation group signatures from bilinear maps[A]. Proc of the Cryptology and Network Security 2006[C]. Berlin: Springer-Verlag, 2006. 126-143.

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

[12] 魏凌波, 武传坤, 周苏静. 具有向后无关性的本地验证撤销群签名方案[J]. 计算机研究与发展, 2008, 45(8): 1315-1321.
WEI L B, WU C K, Zhou S J. A new verifier-local revocation group signature with backward unlinkability [J]. Journal of Computer Research and Development, 2008, 45(8): 1315-1321.

[13] 张跃宇, 庞辽军, 苏万力等. 一种高效的本地验证者撤销群签名方案[J]. 西安电子科技大学学报(自然科学版), 2007, 34(5): 818-822.
ZHANG Y Y, PANG L J, SU W L, *et al*. Efficient group signature scheme with verifier-local revocation[J]. Journal of Xidian University, 2007, 34(5): 818-822.

[14] 张京良, 李艳平, 王育民. 具有局部验证者撤销的短群签名方案[J]. 西安交通大学学报, 2008, 42(10): 1250-1253.
ZHANG J L, LI Y P, WANG Y M. Shorter group signatures scheme with verifier-local revocation[J]. Journal of Xi'an Jiaotong University, 2008, 42(10): 1250-1253.

[15] SONG D. Practical forward-secure group signature schemes[A]. Proc of the Computer and Communications Security'2001[C]. New York: ACM Press, 2001. 225-234.

[16] WEI L B, WU C K, ZHU T G. Backward unlinkability and verifier-local revocation group signature scheme with lower cost[J]. Journal of Software, 2009, 20(7): 1977-1985.

[17] 李继国, 孙刚, 张亦辰. 标准模型下可证安全的本地验证者撤销群签名方案[J]. 电子学报, 2011,20(7):1618-1623.
LI J G, SUN G, ZHANG Y C. Provably secure group signature scheme with verifier-local revocation in the standard mode[J]. Acta Electronica Sinica, 2011,20(7):1618-1623.

[18] BONEH D, BOYEN X. Short signature without random oracles[A]. Advances in Cryptology-EUROCRYPT' 2004[C]. Berlin: Springer-Verlag, 2004. 56-73.

[19] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-96.

作者简介：

李继国（1970-），男，黑龙江富裕人，博士，河海大学教授、博士生导师，主要研究领域为信息安全、密码学理论与技术。

孙刚（1985-），男，江苏淮安人，河海大学硕士生，主要研究领域为密码学理论与技术。

张亦辰（1971-），女，黑龙江齐齐哈尔人，河海大学博士生、讲师，主要研究领域为密码学理论与技术。