标准模型下可证安全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.目前大部分本地验证者撤销群签名方案都是在随机预言模型下证明方案的安全性,但是这种理想的预言机在现实世界中是不存在的,构造标准模型下可证安全的群签名方案仍是当前研究的热点课题.本文在Boyen-Waters群签名方案的基础上,提出一个本地验证者撤销群签名方案,并在标准模型下证明了方案的安全性.分析了方案的性能,在满足AES 80比特标准安全条件下,方案在签名元素个数、签名长度方面优于现有标准模型下本地验证者撤销群签名方案.

关键词: 群签名;本地验证者撤销;随机预言模型;标准模型
中图分类号: TP301 **文献标识码:** A **文章编号:** 0372-2112 (2011) 07-1618-06

Provably Secure Group Signature Scheme with Verifier-Local Revocation in the Standard Model

LI Ji-guo, SUN Gang, ZHANG Yi-chen
(*College of Computer & Information Engineering, Hohai University, Nanjing, Jiangsu* 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. However, mostly provably secure group signature relied on the random oracle model that are out of reach in the real world, the designing of provably secure group signature in the standard model is also a hot topic of research in modern cryptography. Based on Boyen-Waters group signature scheme, we propose a group signature scheme with verifier-local revocation, which is proven to be secure in the standard model. The performance of the proposed scheme is analyzed; under the condition of 80-bit AES, our scheme is superior to the existing verifier-local revocation group signatures in the standard model both in the number of signature elements and the length of signature.

Key words: group signature; verifier-local revocation; random oracle model; standard model

1 引言

群签名是Chaum和van Heyst[1]在EUROCRYPT'91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.由于群签名满足正确性、防伪造性、不可链接性、防陷害攻击、抗联合攻击等安全特性,使得其在匿名认证、电子支付、网上投票、电子拍卖[2,3]等方面有着巨大的应用前景.

Ateniese和Tsudik[4]早在1999年就指出,以往的群签名方案都提供了新成员的加入机制,但对群成员的废除问题未加重视,群签名方案应该支持动态的群成员.现实应用中,群组的成员应该是动态的,群组中不仅有新成员的加入,同时还有群成员的撤销.2004年Boneh和Shacham[5]将基于撤销列表这种方法形式化定义为本地验证者撤销(Verifier-Local Revocation,简记为VLR).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,而不需与每个终端用户进行通信.此后,许多VLR群签名方案被提出[6~9].

然而,目前大部分群签名方案都是在随机预言模型下证明方案的安全性.但是随机预言器的实现方式可能会导致方案的不安全[10,11],如哈希函数,往往返回的结

收稿日期:2010-04-20;修回日期:2010-06-06
基金项目:国家自然科学基金(No.60842002,No.60903018);中国博士后基金(No.20100471372);中央高校基本科研业务费专项基金(No.B1020211,No.B103071);江苏省"六大人才高峰"项目;河海大学优秀创新人才支持计划

果并不是随机的.因此随机预言模型是一种理想化的计算模型,随机预言模型下的安全证明只是验证方案设计有效性的一种方法.由于群签名的重要性,有必要研究标准模型下可证安全的群签名方案.Bellare 等[12]最早提出了这样的方案并给出了群签名安全的形式化模型(简记为 BMW 模型),但是方案效率过低,不能在实际中应用.近几年,一些有效的标准模型下可证安全的群签名方案被提出.Ateniese 等[13]、Qin 等[14]基于广义组合/响应模型,提出一类高效的不依赖随机预言的群签名方案,并且可以撤销群成员,但是这一类方案都是可链接的并且安全证明基于新的非常强的交互式假设.Boyen 和 Waters[15,16]、Liang 等[17]和 Wang 等[18]基于 BMW 模型提出一类标准模型下可证安全的群签名方案,但是这一类方案都没有考虑群成员的撤销问题.直到 2009 年,Libert[19]等利用 Groth 和 Sahai[20]提出的非交互证明系统构造了一个标准模型下具有向后无关联性的本地验证者撤销群签名方案,但是方案生成的签名中的元素有 47 个之多,正如作者所说,如果不利用文献[21]中的方法进行压缩,签名长度将达到 1.56kB(1024×8 比特为 1kB).

本文在 Boyen 和 Waters 方案[16](简记为 BW07 方案)的基础上提出一个标准模型下可证安全的本地验证者撤销群签名方案,方案满足正确性、匿名性、可追踪性等安全需求并且具有向后无关联性.虽然本文方案在合数阶群上实现,群签名中的元素都非常长,但签名中的元素只有 6 个.在保证方案满足 AES 80 比特标准安全性的基础上,与未经压缩的 Libert 等方案的签名长度相比较,短了 192 比特.

2 预备知识

本节简要介绍合数阶上的双线群以及几个困难假设,详见参考文献[16].

2.1 合数阶上的双线性群

设 G, G_T 都是阶为 $n=pq$(p,q 为素数)的乘法循环群,g 是 G 的生成元,双线性映射 $e: G\times G\to G_T$ 满足以下几个性质:

(1)双线性性:对任意的 $u,v\in G$ 和 $a,b\in Z$,都有 $e(u^a,v^b)=e(u,v)^{ab}$.

(2)非退化性:$e(g,g)\neq 1_{G_T}$,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.

2.2 困难性假设

定义 1　CDH 假设　如果不存在一个概率多项式时间算法,在时间 t 内,以至少 ε 的概率解决 CDH 问题,则(ε,t)-CDH 假设成立.

定义 2　子群判定假设　如果不存在概率多项式时间算法解决子群判定问题,则称群 G 上的子群判定假设成立.

定义 3　*l*-HSDH 假设　如果不存在一个概率多项式时间算法,在时间 t 内,以至少 ε 的概率解决 l-HSDH 问题,则群 G_p 上的(l,ε,t)-HSDH 假设成立.

3 算法组成及安全定义

本文提出的标准模型下的 VLR 群签名方案模型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、每个成员 $id\in[1,N]$的签名密钥 $gsk[id]=K_{ID}$以及成员 id 在时间间隔 $j\in[1,T]$的撤销标记 $grt[id][j]=B_{id,j}$.

(2)签名产生算法 Sign($gpk,j,gsk[id],M$):输入群公钥 gpk,时间间隔 j,群成员 id 私钥 $gsk[id]$以及签名消息 M,产生签名 σ.

(3)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.

标准模型下群签名方案还应满足正确性、可追踪性以及匿名性等安全性质,具体定义如下(主要基于文献[12,16,19]):

①**正确性**:对算法 KeyGen(N,T)产生的所有(gpk,gsk,grt)以及所有的 $j\in[1,T]$,RL_j,$id\in[1,N]$和消息 M,满足下面的关系:

$$\mathrm{Verify}(gpk,j,RL_j,\mathrm{Sign}(gpk,j,gsk[id],M),M)$$
$$=Valid\wedge grt[id][j]\notin RL_j.$$

②**可追踪性**:与文献[19]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 $grt[id][j]$可以追踪到签名者.可追踪性要求在多项式时间内,任何群成员或者几个群成员联合,也无法产生一个群签名,能够通过签名验证算法并且群管理员无法通过追踪算法确定真实签名人的身份.根据上述可知,攻击者可以询问任意群成员 id 的密钥 $gsk[id]$,也可以询问任意群成员对任意消息的签名,并向其提供群成员的撤销标记 $grt[id][j]$,其中 $id\in[1,N]$,$j\in[1,T]$.

③**BU-匿名性**:首先挑战者生成相关的群信息,群公钥信息发送给攻击者,保留私钥信息.然后攻击者可以自适应性的询问任意群成员的私钥 $gsk[id]$;任意 j 时间间隔,群成员的撤销标记 $grt[id][j]$;也可以询问任意 j 时间间隔,群成员对任意消息的签名.j_0 时间间隔,攻击者随机选择两个群成员 id_1,id_2 和消息 M 发送给挑战者,挑战者随机选择两个群成员中的一个,生成

相应的合法签名 σ,并发送 σ 给攻击者;攻击者仍可继续询问除 id_1, id_2 以外群成员的私钥,和对任意消息的签名.由于向后无关联性,攻击者也可以询问 j_0 时间间隔之后,群成员 id_1, id_2 的撤销标记.完全匿名性要求不存在概率多项式时间,攻击者能够以不可忽略的高于 1/2 优势,正确猜测消息 M 上的签名 σ 是群成员 id_1 所签还是群成员 id_2 所签,其中 j_0, id_1, id_2, M 由敌手随机选择,并且时间间隔 j_0 之前(包括时间间隔 j_0),攻击者没有询问过群成员 id_1, id_2 的私钥、撤销标记,以及群成员 id_1, id_2 在消息 M 上的签名.

4 本文的方案

基于 BW07 方案,本文提出一个标准模型下可证安全的 VLR 群签名方案.

BW07 方案是在 Waters[22] 方案基础上提出的群签名方案,采用两级分层的签名方式,其中第一层是针对签名者的身份,而第二层是针对待签的消息;然后利用 Groth、Ostovsky 和 Sahai[23] 提出的非交互零知识协议隐藏用户的身份信息、增加方案的不可关联性,将二层签名方案转换成群签名方案.其二层签名方案在自适应选择消息攻击下是不可伪造的,群签名方案在标准模型下是可证安全的,具体证明过程请参考文献[16].

本文方案依然采用两级分层的签名方式.在 BW07 方案中,利用 Groth、Ostovsky 和 Sahai 提出的非交互零知识协议隐藏用户的身份信息,实现群签名的不可链接性和匿名性,而本文利用文献[24~26]中的非交互式证明系统将文献[16]中的二层签名方案转换成群签名方案.具体方案如下:

(1)KeyGen(N, T):设乘法循环群 $G = < g >$ 的阶为 $n = pq$(p, q 为素数),$e: G \times G \rightarrow G_T$ 是可计算的双线性映射,记 G 的 q 阶子群为 $G_q = < h >$.群管理员随机选择 $\alpha, \omega \in Z_n$,令 $Z = e(g,g)^{\alpha}$,$\Omega = g^{\omega}$;选取 $u, v', v_1, \cdots, v_m \in G$,并对所有 $j \in [1, T]$,选择 $h_j \in G$.则群公钥 $gpk = (g, h, u, v', v_1, \cdots, v_m, h_1, \cdots, h_T, \Omega = g^{\omega}, Z = e(g,g)^{\alpha}) \in G \times G_q \times G^{m+3+T} \times G_T$,群管理员私钥为 $(g^{\alpha}, \omega) \in G \times Z_n$.群管理员为每一个群成员随机选择 $s_{id} \in Z_n$,计算 $K_{ID} = (K_1, K_2, K_3) = ((g^{\alpha})^{1/(\omega + s_{id})}, g^{s_{id}}, u^{s_{id}}) \in G^3$,并对所有 $id \in [1, N]$,$j \in [1, T]$,计算 $B_{id,j} = \hat{h}_j^{s_{id}}$,则群成员的私钥为 $gsk[id] = K_{ID}$,撤销标记为 $grt[id][j] = B_{id,j}$.

(2)Sign($gpk, j, gsk[id], M$):j 时间间隔,给定消息 $M = (\mu_1 \cdots \mu_m) \in \{0,1\}^m$,计算 $\theta = (\theta_1, \theta_2, \theta_3, \theta_4) = (K_1, K_2, K_3(v' \prod_{i=1}^{m} v_i^{\mu_i})^s, g^{-s})$,其中 $s \in_R Z_n$;然后随机选择 $t_1, t_3, \in Z_n$,令 $t_2 = s$,计算 $\sigma_1 = \theta_1 h^{t_1}$,$\sigma_2 = \theta_2^{t_2}$,$\sigma_3 = \theta_3 h^{t_3}$,$\sigma_4 = \theta_4$,最后计算 $\pi_1 = Z^{t_2} e(\theta_1, \Omega)^{1-t_2} e(h^{t_1}, \sigma_2 \Omega)$,$\pi_2 = e(\theta_2, u) e(h, g)^{t_3}$,输出签名 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \pi_1, \pi_2) \in G^6$.

(3)Verify(gpk, j, RL_j, σ, M):

①签名检查:验证 $\pi_1 = e(\sigma_1, \sigma_2 \Omega)$,$\pi_2 = e(\sigma_3, g) e(\sigma_4, (v' \prod_{i=1}^{m} v_i^{\mu_i}))$,如果不等,则拒绝该签名;否则进行下面步骤.

②撤销检查:检查撤销列表 RL_j 中是否存在 $B_{id,j}$ 使得等式 $e(\sigma_2, h_j) = 1/(\sigma_4, B_{id,j})$ 成立,如果存在则拒绝该签名;否则接受签名.

5 方案的安全性分析

5.1 正确性

定理 1 本文方案满足签名的正确性.

证明 对于任意群成员的合法签名 σ 都可以通过验证:

$$
\begin{aligned}
& e(\sigma_1, \sigma_2 \Omega) \\
&= e(\theta_1 h^{t_1}, \sigma_2 \Omega) \\
&= e(\theta_1, \sigma_2 \Omega) e(h^{t_1}, \sigma_2 \Omega) \\
&= e((g^{\alpha})^{1/(\omega + s_{id})}, g^{t_2 s_{id}} g^{\omega}) e(h^{t_1}, \sigma_2 \Omega) \\
&= e((g^{\alpha})^{1/(\omega + s_{id})}, g^{t_2 s_{id}}) e((g^{\alpha})^{1/(\omega + s_{id})}, g^{\omega t_2}) \\
&\quad \cdot e((g^{\alpha})^{1/(\omega + s_{id})}, g^{\omega})^{1-t_2} e(h^{t_1}, \sigma_2 \Omega) \\
&= Z^{t_2} e(\theta_1, \Omega)^{1-t_2} e(h^{t_1}, \sigma_2 \Omega) \\
&\quad \cdot e(\sigma_3, g) e(\sigma_4, (v' \prod_{i=1}^{m} v_i^{\mu_i})) \\
&= e(\theta_3 h^{t_3}, g) e(\theta_4, (v' \prod_{i=1}^{m} v_i^{\mu_i})) \\
&= e(\theta_3, g) e(h^{t_3}, g) e(g^{-s}, (v' \prod_{i=1}^{m} v_i^{\mu_i}) \\
&= e(u^{s_{id}} (v' \prod_{i=1}^{m} v_i^{\mu_i})^s, g) e(g^{-s}, (v' \prod_{i=1}^{m} v_i^{\mu_i})) e(h^{t_3}, g)) \\
&= e(u^{s_{id}}, g) e((v' \prod_{i=1}^{m} v_i^{\mu_i})^s, g) e(g^{-s}, (v' \prod_{i=1}^{m} v_i^{\mu_i})) e(h^{t_3}, g) \\
&= e(g^{s_{id}}, u) e(h^{t_3}, g) = e(\theta_2, u) e(h, g)^{t_3}
\end{aligned}
$$

5.2 BU-匿名性

本文方案的匿名性证明思路主要基于文献[16].如果 $h \in G$ 且 $h \notin G_q$,那么方案产生的签名统计上独立于签名者身份;如果 $h \in G_q$,那么敌手区分真实环境和模拟环境的概率是可忽略的,因为子群判定问题是困难的.综上所述,方案在子群判定假设下具有 BU-匿名性.

定理 2 如果不存在概率多项式时间敌手,在时间 t 内,以至少 ε_{sub} 的优势解决子群判定问题,则对任意 t'($t \approx t'$)时间敌手 A 攻破匿名性的优势 $Adv_A < 2\varepsilon_{sub}$.

要证明上述定理,我们给出如下两个引理.

引理 1　如果对任意概率多项式时间敌手 A,在时间 t' 内,它区分真实环境和模拟环境的概率是可以忽略的,则 $Adv_A - Adv_{A,S} < 2\varepsilon_{sub}$,其中 $Adv_{A,S}$ 表示模拟环境下敌手 A 攻破匿名性的优势.

证明　假设存在算法 B 模拟挑战者与敌手 A 进行交互,试图解决子群问题.给定 B 以元组 (e, G, G_T, n, h),B 去判断 $h \in G_q$ 还是 $h \notin G_q$.首先 B 按照本文方案中的密钥生成方法选择公共参数生成群信息,然后 B 把群公钥信息发送给敌手 A.不管 h 是否属于 G_q,B 总能回答所有的询问,因为 B 知道群管理员私钥.如果 $h \in G_q$,则模拟环境等同于真实环境.

在某一时间间隔 j^*,敌手 A 选择一个消息 M 和两个身份 id 和 id'.限制条件是时间间隔 j_0 之前(包括时间间隔 j_0),敌手 A 没有询问过群成员 id_1, id_2 的私钥、撤销标记,以及群成员 id_1, id_2 在消息 M 上的签名.B 选择 $id^* \in \{id, id'\}$,并输出 (M, id^*) 的签名,发送挑战签名给 A,A 输出它的猜测.如果 A 猜对了挑战签名的签名者身份,B 输出 1,否则 B 输出 0.我们用 Adv_B 表示模拟者 B 解决子群问题的优势,其中

$$\Pr[h \notin G_q] = \Pr[h \in G_q] = 1/2$$

$$\begin{aligned} Adv_A - Adv_{A,S} &= \Pr[b = 1 \mid h \in G_q] - \Pr[b = 1 \mid h \notin G_q] \\ &= 2\Pr[b = 1, h \in G_q] - 2\Pr[b = 1, h \notin G_q] \\ &= 2Adv_B < 2\varepsilon_{sub} \end{aligned}$$

因此在子群判定假设下,敌手 A 区分真实环境和模拟环境的概率是可以忽略的.

引理 2　对于任意敌手 A,存在 $Adv_{A,S} = 0$.

证明　当 $h \in G$ 且 $h \notin G_q$ 时,敌手 A 不能根据挑战签名猜出签名者的身份,尽管可能用 s_{id} 回答过 (M, id) 和 (M, id') 上的签名询问,即挑战签名在统计上独立于签名者身份.

假设挑战签名为 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \pi_1, \pi_2)$,由于 $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ 被随机选择的 $h^{t_1}, h^{t_3} \in G, t_2 \in Z_n$ 隐藏,因此从签名中看不出签名者的身份信息.我们给出两个签名 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \pi_1, \pi_2)$ 和 $\sigma' = (\sigma_1', \sigma_2', \sigma_3', \sigma_4', \pi_1', \pi_2')$,其中 σ, σ' 分别是关于 (M, id) 和 (M, id') 的签名.

如果 $\sigma_1 = \sigma_1', \sigma_2 = \sigma_2', \sigma_3 = \sigma_3', \sigma_4 = \sigma_4'$,分析 π_1 和 π_1'、π_2 和 π_2' 如下:

$(1)(g^{\alpha})^{1/(\omega + s_{id})} h^{t_1} = (g^{\alpha})^{1/(\omega + s_{id}')} h^{t_1'}, g^{s_{id} t_2} = g^{s_{id}' t_2'}$,

令　$\varepsilon = (\omega + s_{id})/(\omega + s_{id}'), h = g^{\eta}, \eta \in {}_R Z_n$,

则

$$t_1' = t_1 + (\alpha(1-\varepsilon))/(\eta(\omega + s_{id})) (\mathrm{mod} n), t_2' = (s_{id}/s_{id}') t_2.$$

现在证明 π_1' 不能揭示签名者身份,从敌手观点出发,π_1 和 π_1' 满足:

$$\begin{aligned} \pi_1' &= Z^{t_2'} e(g^{\alpha/(\alpha + s_{id}')}, \Omega)^{1 - t_2'} e(h, g^{t_2' s_{id}'} \Omega)^{t_1'} \\ &= e(g, g)^{\alpha \cdot t_2 \cdot s_{id}/s_{id}'} e(g^{\alpha/(\omega + s_{id}')}, g^{\omega})^{1 - t_2 \cdot s_{id}/s_{id}'} \\ &\quad \cdot e(h, g^{t_2 \cdot s_{id}/s_{id}' \cdot s_{id}' g^{\omega}})^{t_1 + (\alpha(1-\varepsilon))/(\eta(\omega + s_{id}))} \\ &= e(g^{\alpha/(\omega + s_{id}')}, g^{\omega})^{t_2 \cdot s_{id}/s_{id}'} e(g^{\alpha/(\omega + s_{id}')}, g^{s_{id}'})^{t_2 \cdot s_{id}/s_{id}'} \\ &\quad \cdot e(g^{\alpha/(\omega + s_{id}')}, g^{\omega})^{1 - t_2 \cdot s_{id}/s_{id}'} \\ &\quad \cdot e(h, g^{t_2 \cdot s_{id}} g^{\omega})^{t_1 + (\alpha(1-\varepsilon))/(\eta(\omega + s_{id}))} \\ &= e(g^{\alpha/(\omega + s_{id}')}, g^{s_{id}'})^{t_2 \cdot s_{id}/s_{id}'} e(g^{\alpha/(\omega + s_{id}')}, g^{\omega}) \\ &\quad \cdot e(h^{t_1}, \sigma_2 \Omega) e(g, g^{t_2 \cdot s_{id}} g^{\omega})^{(\alpha(1-\varepsilon))/(\omega + s_{id})} \\ &= e(g^{\alpha/(\omega + s_{id}')}, g)^{t_2 \cdot s_{id}} e(g^{(\alpha(1-\varepsilon))/(\omega + s_{id})}, g^{t_2 \cdot s_{id}}) \\ &\quad \cdot e(g^{\alpha/(\omega + s_{id}')}, g^{\omega}) e(g^{(\alpha(1-\varepsilon))/(\omega + s_{id})}, g^{\omega}) e(h^{t_1}, \sigma_2 \Omega) \\ &= e(g^{\alpha/(\omega + s_{id})}, g^{s_{id}})^{t_2} e(g^{\alpha/(\omega + s_{id})}, g^{\omega}) e(h^{t_1}, \sigma_2 \Omega) \\ &= Z^{t_2} e(\theta_1, \Omega)^{1 - t_2} e(h^{t_1}, \sigma_2 \Omega) = \pi_1 \end{aligned}$$

$(2) u^{s_{id}} (v' \prod_{i=1}^{m} v_i^{\mu_i})^s h^{t_3} = u^{s_{id}'} (v' \prod_{i=1}^{m} v_i^{\mu_i})^s h^{t_3'}$,

令　$h = u^{\varphi}, \varphi \in {}_R Z_n$,

则　$t_3' = t_3 + (s_{id} - s_{id}')/\varphi$.

现在证明 π_2' 不能揭示签名者身份,从敌手观点出发,π_2 和 π_2' 满足:

$$\begin{aligned} \pi_2' &= e(g^{s_{id}'}, u) e(h, g)^{t_3'} = e(g^{s_{id}'}, u) e(h, g)^{t_3 + (s_{id} - s_{id}')/\varphi} \\ &= e(g^{s_{id}'}, u) e(h, g)^{t_3} e(u, g)^{(s_{id} - s_{id}')} \\ &= e(g^{s_{id}}, u) e(h, g)^{t_3} = \pi_2 \end{aligned}$$

由上述可得 $\pi_1 = \pi_1', \pi_2 = \pi_2'$,尽管模拟者用 s_{id} 生成挑战签名,挑战签名也不会揭示出签名者的身份信息 id,因此可以断定敌手 A 在模拟环境下猜出签名者身份的概率是可以忽略的.综上所述本文方案满足 BU-匿名性.

5.3　可追踪性

定理 3　如果存在概率多项式时间敌手,在时间 t 内,以 ε 概率攻破群签名方案的可追踪性,那么就存在时间 $t'(t \approx t')$,敌手以 ε 概率攻破二层签名方案的不可伪造性.

证明　方案可追踪性证明的思路主要基于文献[16].我们可以把群签名方案看作是二层签名方案的扩展,通过在二层签名方案的基础上引入非交互零知识协议,使得群签名方案具有匿名性和不可链接性.这里通过二层签名方案的不可伪造性来证明群签名方案具有可追踪性.

假定存在算法 B 模拟挑战者,通过与敌手 A 进行交互,试图攻破二层签名方案的不可伪造性,它执行以下算法:

在系统参数设置阶段,B 执行二层签名方案的系统参数设置,产生公共参数并公开它们.A 向 B 询问群成员 id 的私钥,B 执行二层签名方案的用户加入算法,得到用户私钥 $K_{ID} = (K_1, K_2, K_3) = ((g^{\alpha})^{1/(\omega + s_{id})}, g^{s_{id}}, u^{s_{id}})$,并发送给 A.A 向 B 询问群成员 id 在 j 时间间隔的

撤销标记,B 计算 $B_{id,j}=\hat{h}_j^{s_{id}}$,并发送给 A. A 向 B 询问群成员 id 在消息 M 上的群签名,B 直接询问二层签名方案的签名预言机,得到 $\theta=(\theta_1,\theta_2,\theta_3,\theta_4)$,然后随机生成 $t_1,t_2,t_3\in Z_n$,计算群签名 $\sigma=(\theta_1 h^{t_1},\theta_2 t_2,\theta_3 h^{t_3},\theta_4, Z^{t_2}e(\theta_1,\Omega)^{1-t_2}e(h^{t_1},\theta_2{}^{t_2}\Omega),e(\theta_2,u)e(h,g)^{t_3})$,显然 σ 为有效的群签名,A 可以利用群公钥和撤销列表来验证 σ 的有效性.

在 j^* 时刻,A 输出身份 id^* 在消息 M^* 上的伪造签名 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\pi_1^*,\pi_2^*)$,要求 A 没有询问过 id^* 的私钥,并且上述签名不是通过询问身份 id^* 在消息 M^* 上的群签名所得到的.验证 $\pi_1{}^*$ 可得:

$$Z^{t_2}e(\theta_1^*,g^{\omega})^{1-t_2}e(h^{t_1},\sigma_2^* g^{\omega})=e(\sigma_1^*,\sigma_2^* g^{\omega})$$

由于

$$\begin{aligned}e(\sigma_1^*,\sigma_2^* g^{\omega})&=e(\theta_1^* h^{t_1},\theta_2^{*t_2}g^{\omega})\\&=e(\theta_1^*,\theta_2^{*t_2}g^{\omega})e(h^{t_1},\theta_2^{*t_2}g^{\omega})\end{aligned}$$

B 生成 $\lambda\equiv 1(\mathrm{mod}p)$ 且 $\lambda\equiv 0(\mathrm{mod}q)$,得到

$e(\sigma_1^*,\sigma_2^* g^{\omega})^{\lambda}=e(\theta_1^*,\theta_2^{*t_2}g^{\omega})^{\lambda}=Z^{\lambda t_2}e(\theta_1^*,g^{\omega})^{\lambda(1-t_2)}$.

则:$e(\theta_1{}^*,\theta_2^{*t_2}g^{\omega})^{\lambda}e(\theta_1^*,g^{\omega})^{\lambda(t_2-1)}=Z^{\lambda t_2}$,

因此:$e(\theta_1^*,\theta_2^*\Omega)^{\lambda t_2}=Z^{\lambda t_2}$.

验证 $\pi_2{}^*$ 可得:

$$\begin{aligned}&e(\theta_2^*,u)e(h,g)^{t_3}\\&=e(\sigma_3{}^*,g)e(\sigma_4{}^*,(v'\prod_{i=1}^{m}v_i^{\mu_i}))\\&\quad\cdot e(\sigma_3{}^*,g)e(\sigma_4{}^*,(v'\prod_{i=1}^{m}v_i^{\mu_i}))\\&=e(\theta_3{}^*,g)e(h^{t_3},g)e(\theta_4{}^*,(v'\prod_{i=1}^{m}v_i^{\mu_i}))\end{aligned}$$

所以 $e(\theta_2{}^*,u)=(\theta_3{}^*,g)e(\theta_4{}^*,(v'\prod_{i=1}^{m}v_i^{\mu_i}))$.

综上所得 $e(\theta_1{}^*,\theta_2{}^*\Omega)=Z$ 且 $e(\theta_2{}^*,u)=(\theta_3{}^*,g)e(\theta_4{}^*,(v'\prod_{i=1}^{m}v_i^{\mu_i}))$,因此$(\theta_1^*,\theta_2^*,\theta_3^*,\theta_4^*)$可以通过两层签名方案的验证等式,所以它们是一个伪造的二层签名,从而 B 攻破了二层签名方案的不可伪造性,定理 3 得证.然而二层签名方案在 l-HSDH 假设下是不可伪造的,因此群签名方案满足可追踪性.

6 性能分析与比较

目前标准模型下本地验证者撤销群签名方案只有 Libert 等方案[19],下面从计算代价、群签名元素个数、群签名长度方面与 Libert 等方案进行分析和比较.

表 1 方案性能比较

签名方案	签名元素个数/个	签名长度/比特(80-bit AES)
Libert 等方案	47	8384
本文方案	6	8192

计算代价:参照文献[16,17],本文方案签名过程需要 4 次双线性运算、5 次指数运算和$(m+6)$次群乘法运算,验证过程需要 3 次双线性运算和 m 次群乘法运算.与 BW07 方案相比,在总的计算代价上只增加了 1 次双线性运算,但少了 10 次指数运算和 9 次群乘法运算.Libert 等方案由于采用文献[20]中的非交互证明系统,引入了复杂的矩阵和向量运算,同时还需进行双线性运算、指数运算和群乘法运算,计算代价巨大.因此本文方案在计算代价方面要低于 Libert 等方案.

群签名元素个数:本文方案生成的签名只有 6 个元素,而 Libert 等方案生成的签名中的元素有 47 个.

群签名长度:本文方案的签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\pi_1,\pi_2)$,包含 4 个 G 中元素和 2 个 G_T 中元素.本文方案在合数阶群上实现,而 Libert 等方案在素数阶群上实现,为了便于比较,我们保证两个方案都满足 AES 80 比特标准安全性,因此素数阶群 G 中的元素长为 160 比特,映射到 G_T 中元素长为 1024 比特;而合数阶群 G 中的元素长为 1024 比特,映射到 G_T 中元素长为 2048 比特,更详细的安全性参数标准参见文献[27,28].所以,Libert 等方案签名长度为 8384 比特(46 个 G 中元素和 1 个 G_T 中元素),而本文方案签名长度为 8192 比特,比 Libert 等方案短了 192 比特.

7 总结

在 BW07 方案基础上,本文提出了一个具有向后无关联性的 VLR 群签名方案,在标准模型下证明了方案的安全性,并与 Libert 等方案进行了比较.然而随着标准安全性要求的提高,本文方案的签名长度将不能够满足实际应用需要,因此下一步工作是在素数阶群上实现标准模型下的 VLR 短群签名方案,并且加强方案的安全性.

参考文献

[1] Chaum D, Van Heyst E. Group signatures[A]. Advances in Cryptology-EUROCRYPT′ 1991[C]. Berlin: Springer-Verlag, 1991.257 – 265.

[2] 姬东耀,王育民.一个基于群签名的安全电子拍卖协议[J].电子学报,2002,30(1):18 – 21.
Ji Dong-yao, Wang Yu-min. A distributed secure electronic auction protocol based on group signatures[J]. Acta Electronica Sinica, 2002, 30(1): 18 – 21. (in Chinese)

[3] 张键红,伍前红,邹建成,王育民.一种高效的群签名[J].电子学报,2005,33(6):1113 – 1115.
Zhang Jian-hong, Wu Qian-hong, Zou Jian-cheng, Wang Yu-min. An efficient group signature scheme[J]. Acta Electronica Sinica, 2005, 33(6): 1113 – 1115. (in Chinese)

[4] Ateniese G, Tsudik G. Some open issues and new direction in group signatures[A]. Proceedings of CRYPTO′ 1999[C]. Berlin: Springer-Verlag, 1999. 196 – 211.

[5] Boneh D, Shacham H. Group signatures with verifier-local revocation[A]. Proceedings of the Computer and Communications Security′2004[C]. New York: ACM Press, 2004. 168 – 177.

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

[7] Zhou Sujing, Lin Dongdai. Shorter verifier-local revocation group signatures from bilinear maps[A]. Proceedings of the Cryptology and Network Security′2006[C]. Berlin: Springer-Verlag, 2006. 126 – 143.

[8] 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 Jing-liang, Li Yan-ping, Wang Yu-min. Shorter group signatures scheme with verifier-local revocation[J]. Journal of Xi′an Jiaotong University, 2008, 42(10): 1250 – 1253. (in Chinese)

[9] Wei Lingbo, Wu Chuankun, Zhu Tingge. Backward unlinkability and verifier-local revocation group signature scheme with lower cost[J]. Journal of Software, 2009, 20(7): 1977 – 1985.

[10] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols[A]. Proceedings of the 1st ACM Conference on Communications and Computer Security[C]. New York: ACM Press, 1993. 62 – 73.

[11] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4): 557 – 594.

[12] Bellare M, Micciancio D, Wainschi B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions[A]. Advances in Cryptology-EUROCRYPT′2003[C]. Berlin: Springer-Verlag, 2003. 614 – 629.

[13] Ateniese G, Camenisch J, Hohenberger S, de Medeiros B. Practical group signature without random oracles[OL]. http://eprint.iacr.org/2005/385.

[14] Qin Bo, Wu Qianhong, W Susilo, Mu Yi, Wang Yuming, Jiang Zhengtao. Short group signature without random oracles[J]. Journal of Computer Science and Technology, 2007, 22(6): 805 – 821.

[15] Boyen X, Waters B. Compact group signature without random oracles[A]. Advances in Cryptology-EUROCRYPT′ 2006[C]. Berlin: Springer-Verlag, 2006. 427 – 444.

[16] Boyen X, Waters B. Full-domain subgroup hiding and constant-size group signature[A]. Advances in Public Key Cryptogaphy(PKC′2007)[C]. Berlin: Springer-Verlag, 2007. 1 – 15.

[17] Liang Xiaohui, Cao Zhenfu, Shao Jun, Lin Huang. Short group signature without random oracles[A]. ICICS′ 2007[C]. Berlin: Springer-Verlag, 2007. 69 – 82.

[18] Wang Shaohui. Modification and improvement on group signature scheme without random oracles[A]. International Symposium on Electronic Commerce and Security′2008[C]. Washington: IEEE Computer Society. 462 – 466.

[19] Libert B, Vergnaud D. Group signatures with verifier-local revocation and backward unlinkability in the standad model[A]. CANS′2009[C]. Berlin: Springer-Verlag, 2009. 498 – 517.

[20] Groth J, Sahai A. Efficient non-interactive proof systems for bilinear groups[A]. Advances in Cryptology-EUROCRYPT′ 2008[C]. Berlin: Springer-Verlag, 2008. 415 – 432.

[21] Scott M, Barreto P. Compressed pairings[A]. Advances in CRYPTO′ 2004[C]. Berlin: Springer-Verlag, 2004. 140 – 156.

[22] Waters B. Efficient identity-based encryption without random oracles[A]. Advances in Cryptology-EUROCRYPT′ 2005[C]. Berlin: Springer-Verlag, 2005. 114 – 127.

[23] Groth J, Ostrovsky R, Sahai A. Perfect non-interactive zero knowledge for NP[A]. Advances in Cryptology-EUROCRYPT′2006[C]. Berlin: Springer-Verlag, 2006. 339 – 358.

[24] Groth J. Fully anonymous group signatures without random oracles[A]. Advances in Cryptology-ASIACRYPT′ 2007[C]. Berlin: Springer-Verlag, 2007. 164 – 180.

[25] Delerablee C, Pointcheval D. Dynamic fully anonymous short group signatures[A]. Advances in Vietcrypt′2006[C]. Berlin: Springer-Verlag, 2006. 193 – 210.

[26] 马海英,石振国,顾翔.标准模型下的高效短群签名[J].计算机应用,2009,29(8):2220 – 2222.
Ma Hai-ying, Shi Zhen-guo, Gu Xiang. Short group signature with high efficiency under standard model[J]. Journal of Computer Applications, 2009, 29(8): 2220 – 2222. (in Chinese)

[27] Koblitz N, Menezes A. Pairing-based cryptography at high security levels[A]. Cryptography and coding′2005[C]. Berlin: Springer-Verlag, 2005. 13 – 36.

[28] Freeman M D. Converting pairing-based cryptosystems from composite-order groups to prime-order groups[OL]. http://crypto.rd.francetelecom.com/events/eurocrypt2010/program, 2010-05-31.

作者简介

李继国　男,1970 年生于黑龙江富裕,博士,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、可信计算等.
E-mail: ljg1688@163.com

孙　刚　男,1985 年生于江苏淮安,硕士,主要研究领域为密码学理论与技术.

张亦辰　女,1971 年生于黑龙江齐齐哈尔,学士,讲师,主要研究领域为密码学理论与技术.