计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
44(7):1219~1226, 2007

高效撤消成员的前向安全群签名方案

李如鹏[1] 于 佳[1,2] 李国文[1] 李大兴[1]
[1](山东大学网络信息安全研究所 济南 250100)
[2](青岛大学信息工程学院 青岛 266071)
(lirupeng@gmail.com)

Forward Secure Group Signature Schemes with Efficient Revocation

Li Rupeng[1], Yu Jia[1,2], Li Guowen[1], and Li Daxing[1]
[1](*Institute of Network Security*, *Shandong University*, *Jinan* 250100)
[2](*College of Information Engineering*, *Qingdao University*, *Qingdao* 266071)

Abstract How to efficiently revoke group membership and how to cope with key exposure are two important issues in designing group signature schemes. Up to now, there are few group schemes that can resolve the two problems at the same time. The common drawback of the previously proposed scheme is that the computational cost of verifying linearly depends on the number of the revoked group members. The revocation method based on accumulator has common drawback: previously signed signatures can not pass the verifying algorithm under the updated public value after the signer is revoked. Based on the ACJT group signature scheme, two new group signature schemes are proposed. The main trait is that they have efficiently revocable property and forward secure property at the same time. The evolution of secret key in scheme Ⅰ is more efficient. But the size of group public key and the computational cost of signing and verifying in scheme Ⅰ linearly depend on the number of time periods. Scheme Ⅱ adopts another forward secure method and overcomes this defect. Both the schemes tackle the drawback of the revocation method based on accumulator and support retroactively publicly revocable group membership with backward unlinkability. The computational cost of signing and verifying is independent of the number of the current group members and the revoked group members.

Key words group signature; member revocation; forward security; accumulator; backward unlinkability

摘 要 群成员的撤消和如何处理密钥泄漏是设计群签名方案中的两个重要问题,到目前为止,同时解决这两个问题的群签名方案为数不多且尚存在不足. 以ACJT群签名方案为基础,提出了两个新的群签名方案,其最大特点是同时具有高效撤消性和前向安全性. 其中方案Ⅰ具有较高的密钥演化效率,但是群公钥长度、签名和验证算法的计算量和时间段个数线性相关,方案Ⅱ采用了另一种前向安全的思想,克服了方案Ⅰ的不足. 两个方案较好地解决了基于累加器撤消方法存在的缺陷,支持可追溯的公开可撤消群成员身份并且签名具有向后不可联接性,签名和验证算法的计算量均独立于当前群成员个数和被撤消成员的个数.

关键词 群签名;成员撤消;前向安全;累加器;向后不可联接

中图法分类号 TP309

收稿日期:2006-10-26;**修回日期**:2007-02-04
基金项目:国家"八六三"高技术研究发展计划基金项目(2003AA141120,2004AA001260)

群签名的概念[1]由 Chaum 和 van Heyst 提出,在一个群签名方案中,任何群成员均可以匿名的方式代表群对消息进行签名,签名由惟一的群公钥来验证,判断两个签名是否是由同一个群成员所签署在计算上是困难的.在有争议的情况下,签名可以由指定的群管理员"打开",来揭示签名者的身份.群签名可以隐藏内部的组织结构,它有很多应用场合,如电子现金系统、投票协议等.

Ateniese 和 Tsudik 指出了群签名应用中的两个重要问题[2]:成员撤消和如何处理密钥泄漏.随后有很多成员撤消方案被提出,主要的撤消方法有两大类:一类是基于撤消链表的方法[3-4],群管理员公布被撤消成员身份的链表,群成员通过零知识证明的方式来证明签名中含有的身份不等于链表中的任何一个身份.该方法的缺陷是签名长度或者验证算法的计算量和被撤消成员的个数线性相关,随着被撤消成员的增加,验证算法的效率将会降低;另一类比较高效的方法是基于证据的方法,即采用动态累加器[5]来实现,累加器满足伪造一个值在累加器中的证据是困难的.群管理员公布累加值,群成员通过零知识证明的方式来证明他拥有相应于累加值的证据,验证算法的计算量独立于被撤消成员的个数.但是该方法存在这样的缺陷:如果撤消一个成员,那么该成员以前生成的签名用新的累加值验证也将会无效,这样是不符合实际要求的.

数字签名的前向安全性由 Anderson[6]首先提出,用来减少密钥泄漏所造成的损失.在前向安全数字签名方案中,系统的有效时间被划分为离散的时间段,签名和时间绑定在一起,签名密钥通过一个公开的单向函数随着时间进行演化,然后将前一时间段的密钥删除,这样一旦当前时间段的密钥泄漏,之前时间段的签名依然有效.在实际应用中,前向安全的群签名应该支持可追溯的公开可撤消和向后不可联接性[7]:假设成员 A 的密钥在时间段 i 泄漏,在以后的某个时间段 j 发现密钥泄漏,此时群管理员应该撤消成员 A 在时间段 i 以后的成员身份,使得时间段 i 以后 A 的所有签名无效,但时间段 i 之前 A 所有的签名依然有效并且是匿名的和不可联接的.

到目前为止,既能处理密钥泄漏问题,同时又能支持成员撤消的群签名方案为数不多.Song[7]提出了可以同时处理这两个问题的群签名方案,但最大的问题是其验证算法的计算量线性依赖于被撤消成员的个数,并且 Song 方案Ⅰ中签名的向后不可联接性基于一个未被证实的密码学假设——离散对数平方假设.Zhang 等人[8]提出了一个新的支持成员撤消的前向安全群签名方案,虽然效率比较高,但是后来被证明是不安全的[9].

最近,陈少真等人[10]提出了一个有效取消的前向安全群签名体制,也存在验证算法的计算量线性依赖于被撤消成员个数的问题.

我们基于 ACJT 群签名方案[11],提出了两个高效撤消成员的前向安全群签名方案,使用动态累加器来高效地增加和撤消群成员,并解决了目前基于累加器撤消方法中存在的缺陷,采用 Fiat-Shamir 启发式[12]构造知识签名来证明签名者未被撤消并拥有合法密钥.方案Ⅰ采用 Bellare-Miner 方案[13]中前向安全的思想,密钥演化方式为模 n 的平方运算,为了支持可追溯的公开可撤消群成员身份和向后不可联接性,方案Ⅰ在密钥演化的同时,将下一时间段累加值的初始值置为当前的累加值,验证签名时用相应时间段的累加值来验证.方案Ⅰ解决了文献[7,10]方案中验证算法的计算量线性依赖于被撤消成员个数的问题,安全性基于强 RSA 假设、确定 Diffie-Hellman 假设和离散对数假设.不足之处是群公钥长度、签名和验证算法的计算量和时间段个数线性相关.基于相同的安全性假设,方案Ⅱ采用 Itkis-Reyzin 方案[14]中前向安全的思想来实现密钥演化,并为每个群成员生成在每个时间段的加入标记,撤消群成员时对相应的加入标记进行操作.方案Ⅱ同样可以解决验证算法的计算量线性依赖于被撤消成员个数的问题,同时克服了方案Ⅰ的不足,并且提高了成员撤消的效率.

1 方案模型和安全要求

在一个群签名方案中,由群管理员(GM)来负责群成员的加入、撤消和揭示签名者的身份,模型包括如下算法:

系统建立.一个概率算法,输入为一个安全参数,输出为系统参数、群公钥和群管理员的私钥.

成员加入.群管理员和用户之间的交互协议,该协议使得用户得到一个群签名密钥,成为一名群成员.

成员撤消.该算法撤消指定群成员的签名能力.

密钥演化.输入某成员在时间段 i 的群签名密钥,该算法输出在时间段 $i+1$ 的群签名密钥.

签名.输入为群公钥、一个成员的群签名密钥,

消息 m 和时间段 i,该概率算法输出对 m 的群签名 $\langle i, sig\rangle$.

验证. 输入为群公钥、一个群签名 $\langle i, sig\rangle$ 和消息 m,该算法验证 sig 是否是用时间段 i 的群签名密钥所签署的有效群签名.

打开. 输入消息 m、一个对 m 的有效群签名、群公钥和群管理员的私钥,该算法确定签名者的身份.

在 BSZ 模型[15]中,通过一些 Oracle 来模拟敌手的攻击能力,将理想的动态群签名方案应满足的安全特性归纳为 4 点:1)正确性. 群成员所生成的签名验证有效,打开算法能正确地揭示签名者的身份并且给出可接受的证明. 2)匿名性. 对于一个指定消息的签名,如果敌手不能判定是由他所选择的两个成员中哪一个成员所签署,则方案满足匿名性,我们将其扩展为向后不可联接匿名性. 3)可跟踪性. 敌手不能够生成一个 GM 不能揭示其身份的签名,或者 GM 可以揭示其身份但是不能给出一个可接受的证明. 4)抗陷害性. 如果一个成员没有生成某个签名,敌手不能给出一个证明来认定该成员生成了此签名. 此外,在实际应用中,前向安全性、可追溯的公开可撤消和向后不可联接性也被人们所关注.

2 方案描述

2.1 方案Ⅰ

思想:成员 P 加入时,GM 累加其加入标记 e_p,每个时间段设立累加值,成员 P 签名时需要提供 e_p 在该时间段累加值中的证据. 撤消成员时,GM 从对应时间段的累加值中删除 e_p. 设 $\varepsilon>1$, k 和 l_p 为安全参数,定义整数区间 $\Lambda=[2^{\lambda_1}-2^{\lambda_2}, 2^{\lambda_1}+2^{\lambda_2}]$, $\Gamma=[2^{\gamma_1}-2^{\gamma_2}, 2^{\gamma_1}+2^{\gamma_2}]$. 其中 $\lambda_1>\varepsilon(\lambda_2+k)+2$, $\lambda_2>4l_p$, $\gamma_1>\varepsilon(\gamma_2+k)+2$ 和 $\gamma_2>\lambda_1+2$. 无碰撞的 Hash 函数 $H:\{0,1\}^*\rightarrow\{0,1\}^k$. 我们假定每个成员与 GM 间的信道是安全的.

1) 系统建立

GM 随机地选择两个 l_p 位长的素数 p',q' 作为秘密值, $p=2p'+1, q=2q'+1$,设定模为 $n=pq$. 构建 CL 累加器[5],累加函数为 $v=f(u,e)=u^e \bmod n$,累加操作后更新证据的函数同累加函数. 删除函数 $v'=D((p,q),v,e'),(e'\neq e)$,删除 e' 后更新 e 的证据的函数为 $E(u,e,e',v')$. 选择 $a,d,g,h,u\in_R QR_n$, $x\in_R Z^*_{p'q'}$,令 $y=g^x \bmod n$. GM 私钥包括颁发密钥 $ik=(p',q')$,打开密钥 $ok=x$. GM 将系统的有效时间划分为 T 个时间段,设立 T 维变量 $V_{[1..T]}$, $V_j(1\leqslant j\leqslant T)$ 为每个时间段的累加值,V_0 初始值为 u,进入下一时间段时,累加值保持不变,即 $V_{j+1}:=V_j$,群公钥为 $gpk=(n,a,d,g,h,y,V)$,建立两个表 E_{add}:用来存储增加的成员的加入标记,E_{del}:用来存储被撤消的成员的加入标记,其初始值都为空.

2) 成员加入

① 用户 P 选择 $r_u\in_R[0, 2^{\lambda_2}]$, $r\in_R[0,n^2]$,发送 $C_1=g^{r_u}h^r \bmod n$ 给 GM,并证明 C_1 的正确性.

② 如果 $C_1\in QR_n$,GM 随机选择 α, $\beta\in_R[0, 2^{\lambda_2}]$,发送 α, β 给用户 P.

③ 用户 P 计算 $x_p=2^{\lambda_1}+(\alpha r_u+\beta \bmod 2^{\lambda_2})$,发送 GM 值 $C_2=a^{x_p} \bmod n$,并证明:C_2 以 a 为底的对数是由 C_1, α 和 β 正确计算得来的并且在区间 Λ 内.

④ 如果 $C_2\in QR_n$ 并且以上证明正确,GM 随机选择和以往不同的素数 $e_p\in_R\Gamma$ 为用户 P 的加入标记,计算 $C_{p,0}=(C_2d)^{1/(e_p2^T)} \bmod n$. GM 发送成员证书 $[C_{p,0}, e_p]$ 和值 V_0 给用户 P 作为证据 u_p,更新当前时间段的累加值 $V_0=f(V_0,e_p)$,将加入标记 e_p 存入表 E_{add},维护成员表 $\langle C_{p,0}, e_p\rangle$.

⑤ 用户 P 验证 $C_{p,0}^{e_p2^T}\equiv a^{x_p}d \bmod n$ 和 $V_0\equiv u_p^{e_p} \bmod n$,则私钥为 $(C_{p,0}, e_p, x_p, u_p=V_0)$.

3) 成员撤消

假设在当前时间段 j 撤消成员 P 在时间段 $i(i\leqslant j)$ 以后的成员身份. GM 从时间段 i 到时间段 j 的累加值中删除 e_p, $V_k=D((p,q), V_k, e_p)$, $k=i,i+1,\cdots,j$,并将 e_p 存入表 E_{del}.

4) 密钥演化

成员 P 在时间段 j 的私钥为 $(C_{p,j}, e_p, x_p, u_p)$,在时间段 $j+1$ 的私钥为 $(C_{p,j+1}, e_p, x_p, u_p)$,其中 $C_{p,j+1}=C_{p,j}^2 \bmod n$,则始终有 $(C_{p,j}^{2^{T-j}})^{e_p}=a^{x_p}d \bmod n$ 成立.

5) 更新证据

成员 P 只需要在签名之前更新加入标记 e_p 在累加器中的证据,自上次更新以来,对于表 E_{add} 中新增加的 e_{add},计算 $u_p=f(u_p, \prod e_{add})=u_p^{\prod e_{add}}$;对于表 E_{del} 中新增加的 e_{del},计算 $u_p=E(u_p, e_p, \prod e_{del}, V_j)$,始终有 $V_j=f(u_p,e_p)$ 成立.

6) 签名

成员 P 在时间段 j 的密钥为 $(C_{p,j}, e_p, x_p, u_p)$,过程如下:

① 选择 $w_1,w_2,w_3\in_R\{0,1\}^{2l_p}$,计算承诺值 $A=C_{p,j}y^{w_1} \bmod n$, $B=g^{w_1} \bmod n$, $C_e=g^{e_p}h^{w_1} \bmod n$, $C_u=u_p h^{w_2} \bmod n$, $C_r=g^{w_2}h^{w_3} \bmod n$;

② 选择 $r_1\in_R\pm\{0,1\}^{\varepsilon(\gamma_2+k)}$, r_2, r_4, $r_8\in_R\pm\{0,1\}^{\varepsilon(\gamma_1+2l_p+k+1)}$, $r_3\in_R\pm\{0,1\}^{\varepsilon(\lambda_2+k)}$, r_5, r_6, $r_7\in_R\pm\{0,1\}^{\varepsilon(2l_p+k)}$,计算 $t_1=A^{2^{T-j}r_1}(1/y)^{2^{T-j}r_2}(1/a)^{r_3}$, $t_2=C_u^{r_1}(1/h)^{r_4}$, $t_3=g^{r_5}$, $t_4=B^{r_1}(1/g)^{r_2}$, $t_5=g^{r_1}h^{r_5}$, $t_6=g^{r_6}h^{r_7}$, $t_7=C_r^{r_1}(1/g)^{r_4}(1/h)^{r_8}$, $c=H(j\|a\|d\|g\|h\|y\|A\|B\|C_e\|C_u\|C_r\|t_1\|t_2\|t_3\|t_4\|t_5\|t_6\|t_7\|m)$, $s_1=r_1-c(e_p-2^{\gamma_1})$, $s_2=r_2-ce_pw_1$, $s_3=r_3-c(x_p-2^{\lambda_1})$, $s_4=r_4-ce_pw_2$, $s_5=r_5-cw_1$, $s_6=r_6-cw_2$, $s_7=r_7-cw_3$, $s_8=r_8-ce_pw_3$. 签名为 $sig=(A,B,C_e,C_u,C_r,c,s_1,s_2,s_3,s_4,s_5,s_6,s_7,s_8)$.

7) 验证

① 计算 $c'=H(j\|a\|d\|g\|h\|y\|A\|B\|C_e\|C_u\|C_r\|d^cA^{2^{T-j}(s_1-c2^{\gamma_1})}(1/y)^{2^{T-j}s_2}(1/a)^{s_3-c2^{\lambda_1}} \bmod n\|V_j^cC_u^{s_1-c2^{\gamma_1}}(1/h)^{s_4} \bmod n\|B^cg^{s_5} \bmod n\|B^{s_1-c2^{\gamma_1}}(1/g)^{s_2} \bmod n\|C_e^cg^{s_1-c2^{\gamma_1}}h^{s_5} \bmod n\|C_r^cg^{s_6}h^{s_7} \bmod n\|C_r^{s_1-c2^{\gamma_1}}(1/g)^{s_4}(1/h)^{s_8} \bmod n\|m)$;

② 如果 $c'=c$,并且 $s_1\in\pm\{0,1\}^{\varepsilon(\gamma_2+k)+1}$, s_2, s_4, $s_8\in\pm\{0,1\}^{\varepsilon(\gamma_1+2l_p+k+1)+1}$, $s_3\in\pm\{0,1\}^{\varepsilon(\lambda_2+k)+1}$, s_5, s_6, $s_7\in\pm\{0,1\}^{\varepsilon(2l_p+k)+1}$,则接受签名 sig.

8) 打开

GM 首先验证签名的有效性,然后揭示成员 P 的身份 $C_{p,0}=(A/B^x)^{1/2^j} \bmod n$,GM 同时也证明 $\log_g y=\log_B(A/C_{p,0}^{2^j} \bmod n)$.

2.2 方案Ⅱ

思想:为了便于成员撤消和密钥演化,为每个成员在每个时间段生成加入标记 $e_{p,i}$ 和撤消标记 $R_{p,i}$ $(0\leqslant i\leqslant T)$,在每个时间段,GM 根据撤消标记来判断是否累加相应的加入标记. 定义整数区间 $\Gamma=[2^{\gamma_1}-(T+1)2^{\gamma_2},2^{\gamma_1}]$, $\Gamma_i=[2^{\gamma_1}-(T-i+1)2^{\gamma_2},2^{\gamma_1}-(T-i)2^{\gamma_2}]$,其中 $0\leqslant i\leqslant T$,其他参数和区间设定同方案Ⅰ. 一个单向的确定算法 EG:输入素数 $e_i\in_R\Gamma_i$,输出一系列互素的素数 $e_j\in\Gamma_j$ $(i\leqslant j\leqslant T)$,对于不同的输入算法生成不同的系列数值,对于 $k\leqslant j$,由 e_j 计算出 e_k 是困难的.

1) 系统建立

同方案Ⅰ,不同的是 u 为累加值,不设 T 维变量 V, $gpk=(n,a,d,g,h,y,u)$. 表 E_{add} 用来存储当前时间段增加的加入标记,表 E_{del} 用来存储当前时间段被删除的加入标记,GM 在每个时间段开始的时候将 E_{add} 和 E_{del} 清空.

2) 成员加入

步骤①~③同方案Ⅰ.

④ 如果 $C_2\in QR_n$ 并且以上证明正确,GM 选择不同的素数 $e_{p,0}\in_R\Gamma_0$,通过算法 EG 输出加入标记 $e_{p,i}\in\Gamma_i$ $(0\leqslant i\leqslant T)$,计算 $b_p=\prod_{0\leqslant i\leqslant T}e_{p,i}$, $v_0=(C_2d)^{1/b_p} \bmod n$, $w_0=\prod_{1\leqslant i\leqslant T}e_{p,i}$, $C_{p,0}=v_0^{w_0} \bmod n$,发送成员证书 $[C_{p,0},e_{p,0}]$, v_0 和证据 $u_p=u$ 给用户 P. GM 更新累加值,$u=f(u,e_{p,0})$,将 $e_{p,0}$ 加入表 E_{add}.

⑤ 用户 P 由 $e_{p,0}$ 计算出 b_p,验证 $C_{p,0}^{e_{p,0}}\equiv a^{x_p}d \bmod n$, $v_0^{b_p}\equiv a^{x_p}d \bmod n$ 和 $u\equiv u_p^{e_{p,0}} \bmod n$,用户 P 存储〈v_0, $e_{p,0}$〉,初始密钥为 $(C_{p,0},e_{p,0},x_p,u_p)$. 撤消标记 $R_{p,t}$ $(0\leqslant t\leqslant T)$ 初始值为 0,$R_{p,t}$ 为 1 表示成员 P 在时间段 t 被撤消,GM 维护成员表〈$C_{p,0}$, $e_{p,0}$, $R_{p,0}$〉.

3) 成员撤消

假设在当前时间段 j 撤消成员 P 在时间段 i $(i\leqslant j)$ 以后的成员身份. 首先删除自时间段 i 后累加的加入标记 $e_{p,k}$ $(i\leqslant k\leqslant j)$:由 $e_{p,0}$,GM 计算 $e_{i,j}=e_{p,i}e_{p,i+1}\cdots e_{p,j}$, $u=D((p,q),u,e_{i,j})$,将 $e_{i,j}$ 存储到表 E_{del};然后 GM 将时间段 j 以后的撤消标记 $R_{p,k}$ $(j+1\leqslant k\leqslant T)$ 置为 1,即在当前时间段 j 以后不再累加成员 P 的加入标记 $e_{p,k}$ $(j+1\leqslant k\leqslant T)$.

4) 密钥演化

假设成员 P 在时间段 j 的密钥为 $(C_{p,j},e_{p,j},x_p,u_p)$,存储的值为〈$v_j$, $e_{p,j}$〉,成员 P 根据 $e_{p,j}$ 计算出 $e_{p,j+1},\cdots,e_{p,T}$, $v_{j+1}=v_j^{e_{p,j}}$, $w_{j+1}=\prod_{j+2\leqslant k\leqslant T}e_{p,k}$, $C_{p,j+1}=v_{j+1}^{w_{j+1}} \bmod n$. GM 根据其撤消标记 $R_{p,j+1}$ 来判断成员 P 在 $j+1$ 时间段是否被撤消,如果未被撤消 $(R_{p,j+1}=0)$,则累加相应的成员加入标记 $e_{p,j+1}$ 将 $u_p=u$ 发给成员 P, $u=f(u,e_{p,j+1})$,则 u_p 为 $e_{p,j+1}$ 在累加值 u 中的证据,将 $e_{p,j+1}$ 加入表 E_{add}. 成员 P 在时间段 $j+1$ 的密钥为 $(C_{p,j+1},e_{p,j+1},x_p,u_p)$,更新〈$v_j$, $e_{p,j}$〉为〈v_{j+1}, $e_{p,j+1}$〉. 始终有 $C_{p,j}^{e_{p,j}}=a^{x_p}d \bmod n$ 成立.

5) 更新证据

方法同方案Ⅰ,并始终有 $u=f(u_p,e_{p,j})$成立.

6) 签名

假设成员 P 在时间段 j 对消息 m 签名,用户密钥为$(C_{p,j},e_{p,j},x_p,u_p)$,过程如下:

① 选择 $w_1,w_2,w_3\in_R\{0,1\}^{2l_p}$,计算承诺值 $A=C_{p,j}y^{w_1} \bmod n$, $B=g^{w_1} \bmod n$, $C_e=g^{e_{p,j}}h^{w_1} \bmod n$, $C_u=u_p h^{w_2} \bmod n$, $C_r=g^{w_2}h^{w_3} \bmod n$;

② 选择 $r_1\in_R\pm\{0,1\}^{\varepsilon(\gamma_2+k-1)}$, $r_2\in_R\pm\{0,1\}^{\varepsilon(\lambda_2+k)}$, r_3, r_4, $r_5\in_R\pm\{0,1\}^{\varepsilon(\gamma_1+2l_p+k+1)}$, r_6, r_7, $r_8\in_R\pm\{0,1\}^{\varepsilon(2l_p+k)}$,计算 $t_1=A^{r_1}(1/y)^{r_3}(1/a)^{r_2}$, $t_2=C_u^{r_1}(1/h)^{r_4}$, $t_3=g^{r_6}$, $t_4=B^{r_1}(1/g)^{r_3}$, $t_5=g^{r_1}h^{r_6}$, $t_6=g^{r_7}h^{r_8}$, $t_7=C_r^{r_1}(1/g)^{r_4}(1/h)^{r_5}$, $c=H(j\|a\|d\|g\|h\|y\|A\|B\|C_e\|C_u\|C_r\|t_1\|t_2\|t_3\|t_4\|t_5\|t_6\|t_7\|m)$, $s_1=r_1-c(e_{p,j}-\gamma)$, $s_2=r_2-c(x_p-2^{\lambda_1})$, $s_3=r_3-ce_{p,j}w_1$, $s_4=r_4-ce_{p,j}w_2$, $s_5=r_5-ce_{p,j}w_3$, $s_6=r_6-cw_1$, $s_7=r_7-cw_2$, $s_8=r_8-cw_3$, 其中 $\gamma=2^{\gamma_1}-(T-j+1/2)2^{\gamma_2}$,签名为 $sig=(A,B,C_e,C_u,C_r,c,s_1,s_2,s_3,s_4,s_5,s_6,s_7,s_8)$.

7) 验证

① 计算 $c'=H(j\|a\|d\|g\|h\|y\|A\|B\|C_e\|C_u\|C_r\|d^cA^{(s_1-c\gamma)}(1/y)^{s_3}(1/a)^{s_2-c2^{\lambda_1}} \bmod n\|u^cC_u^{s_1-c\gamma}(1/h)^{s_4} \bmod n\|B^cg^{s_6} \bmod n\|B^{s_1-c\gamma}(1/g)^{s_3} \bmod n\|C_e^cg^{s_1-c\gamma}h^{s_6} \bmod n\|C_r^cg^{s_7}h^{s_8} \bmod n\|C_r^{s_1-c\gamma}(1/g)^{s_4}(1/h)^{s_5} \bmod n\|m)$;

② 如果 $c=c'$,并且 $s_1\in\pm\{0,1\}^{\varepsilon(\gamma_2+k-1)+1}$, $s_2\in\pm\{0,1\}^{\varepsilon(\lambda_2+k)+1}$, s_3, s_4, $s_5\in\pm\{0,1\}^{\varepsilon(\gamma_1+2l_p+k+1)+1}$, s_6, s_7, $s_8\in\pm\{0,1\}^{\varepsilon(2l_p+k)+1}$,则接受签名 sig.

8) 打开

GM 首先验证签名的有效性,然后揭示成员 P 的身份 $C_{p,j}=(A/B^x) \bmod n$,GM 同时也证明 $\log_g y=\log_B(A/C_{p,j} \bmod n)$.

3 安全性分析

考虑到篇幅限制,我们分析方案Ⅱ的安全性,方案Ⅰ的安全性分析与方案Ⅱ类似且相对简单.

定理 1. 在强 RSA 假设下,方案Ⅱ中签名的交互式协议是关于成员证书和相应成员私钥的统计零知识证明.

证明. 协议的完备性和零知识性容易证明,我们来证明其合理性,即若有两个可接受数组,则可以提取成员密钥. 在交互式的协议中,知识提取器回应两个不同的挑战值,得到两组可接受的值$(j,A,B,C_e,C_u,C_r,c,s_1,s_2,s_3,s_4,s_5,s_6,s_7,s_8)$和$(j,A,B,C_e,C_u,C_r,\tilde{c},\tilde{s}_1,\tilde{s}_2,\tilde{s}_3,\tilde{s}_4,\tilde{s}_5,\tilde{s}_6,\tilde{s}_7,\tilde{s}_8)$. 假设 $\Delta c=\tilde{c}-c$, $\Delta s_1=s_1-\tilde{s}_1$, $\Delta s_2=s_2-\tilde{s}_2$, $\Delta s_3=s_3-\tilde{s}_3$, $\Delta s_6=s_6-\tilde{s}_6$, $\Delta s_7=s_7-\tilde{s}_7$, $\Delta s_8=s_8-\tilde{s}_8$.

由 $t_3\equiv B^cg^{s_6}\equiv B^{\tilde{c}}g^{\tilde{s}_6} \bmod n$,得出 $g^{\Delta s_6}\equiv B^{\Delta c} \bmod n$,让 $\delta_6=gcd(\Delta s_6,\Delta c)$,根据扩展的欧几里德算法,存在 $\alpha_6,\beta_6\in\mathbb{Z}$,满足 $\alpha_6\Delta s_6+\beta_6\Delta c=\delta_6$,则有 $g\equiv g^{(\alpha_6\Delta s_6+\beta_6\Delta c)/\delta_6}\equiv(B^{\alpha_6}g^{\beta_6})^{\Delta c/\delta_6} \bmod n$,如果 $\delta_6<\Delta c$,则 $B^{\alpha_6}g^{\beta_6}$ 是 g 的一个 $\Delta c/\delta_6$ 次根,这和强 RSA 假设相矛盾,所以 $\delta_6=\Delta c$,即存在 $\tau_6\in\mathbb{Z}$ 满足 $\Delta s_6=\tau_6\Delta c$. 因为 $s_6+cw_1=\tilde{s}_6+\tilde{c}w_1$,所以 $\tau_6=w_1$,得出 $C_{p,j}=A/y^{\tau_6} \bmod n$.

由 $t_5\equiv C_e^cg^{s_1-c\gamma}h^{s_6}\equiv C_e^{\tilde{c}}g^{\tilde{s}_1-\tilde{c}\gamma}h^{\tilde{s}_6} \bmod n$,得 $g^{\Delta s_1}\equiv(C_eg^{-\gamma})^{\Delta c}h^{-\Delta s_6}\equiv(C_eg^{-\gamma}h^{-\tau_6})^{\Delta c} \bmod n$,让 $\delta_1=gcd(\Delta s_1,\Delta c)$,根据扩展的欧几里德算法,存在 $\alpha_1,\beta_1\in\mathbb{Z}$,满足 $\alpha_1\Delta s_1+\beta_1\Delta c=\delta_1$,则有 $g\equiv g^{(\alpha_1\Delta s_1+\beta_1\Delta c)/\delta_1}\equiv((C_eg^{-\gamma}h^{-\tau_6})^{\alpha_1}g^{\beta_1})^{\Delta c/\delta_1} \bmod n$,根据强 RSA 假设可得 $\delta_1=\Delta c$,存在 $\tau_1\in\mathbb{Z}$ 满足 $\Delta s_1=\tau_1\Delta c$,由 $s_1+c(e_{p,j}-\gamma)=\tilde{s}_1+\tilde{c}(e_{p,j}-\gamma)$,可得 $e_{p,j}=\gamma+\tau_1$.

同理,由 $t_4\equiv B^{s_1-c\gamma}g^{-s_3}\equiv B^{\tilde{s}_1-\tilde{c}\gamma}g^{-\tilde{s}_3} \bmod n$,得出存在 $\tau_3\in\mathbb{Z}$ 满足 $\Delta s_3=\tau_3\Delta c$,由 $t_1\equiv d^cA^{s_1-c\gamma}y^{-s_3}a^{-(s_2-c2^{\lambda_1})}\equiv d^{\tilde{c}}A^{\tilde{s}_1-\tilde{c}\gamma}y^{-\tilde{s}_3}a^{-(\tilde{s}_2-\tilde{c}2^{\lambda_1})} \bmod n$,得出存在 $\tau_2\in\mathbb{Z}$ 满足 $\Delta s_2=\tau_2\Delta c$,由 $s_2+c(x_p-2^{\lambda_1})=\tilde{s}_2+\tilde{c}(x_p-2^{\lambda_1})$,可得 $x_p=2^{\lambda_1}+\tau_2$.

由 t_6 得出 $C_r^{\Delta c}\equiv h^{\Delta s_8}g^{\Delta s_7} \bmod n$,根据强 RSA 假设,存在 $\tau_8=\Delta s_8/\Delta c$, $\tau_7=\Delta s_7/\Delta c$,则有 $C_r=ah^{\tau_8}g^{\tau_7}$,其中 $a^2=1$,并且 $a=\pm1$,否则 $1<gcd(a\pm1,n)<n$,可以分解 n. 由 t_7 得出 $1=C_r^{\Delta s_1+\Delta c\gamma}h^{-\Delta s_5}g^{-\Delta s_4}$,将 C_r 带入,得 $1=a^{\Delta s_1+\Delta c\gamma}h^{(\Delta s_1+\Delta c\gamma)\tau_8}g^{(\Delta s_1+\Delta c\gamma)\tau_7}h^{-\Delta s_5}g^{-\Delta s_4}$,因为 1, g, $h\in QR_n$,所以 $a^{\Delta s_1+\Delta c\gamma}$ 为 1. 由计算离散对数的困难性,得出$(\Delta s_1+\Delta c\gamma)\tau_7\equiv\Delta s_4(\bmod ord(g))$. 由 t_2 得出 $u^{\Delta c}=C_u^{\Delta s_1+\Delta c\gamma}h^{-\Delta s_4}$,进一步有 $u^{\Delta c}=(C_uh^{-\tau_7})^{\Delta s_1+\Delta c\gamma}$,存在 $\hat{e}=\Delta s_1/\Delta c+\gamma=\tau_1+\gamma$,则有 $u=b(C_uh^{-\tau_7})^{\hat{e}}$,其中 $b=\pm1$. 由于 $u\in QR_n$, $-1\notin QR_n$,因此 $b=1$, $u=(C_uh^{-\tau_7})^{\hat{e}}$,所以 C_e 承诺的值 $e_{p,j}$ 被累加到值 u 中. 证毕.

定理 2. 抗联合攻击性. 假设发布的成员证书的个数 K 多项式有界,则在强 RSA 假设下,一个满足的群成员证书 $[C_{p,0}=(a^{x_p}d)^{1/e_{p,0}} \bmod n,\ e_{p,0}]$ 仅能由 GM 生成,其中 $x_p\in\Lambda$, $e_{p,0}\in\Gamma_0$.

我们方案颁发成员证书的方式同 ACJT 方案,该证明参见其定理 1. 前向安全性证明可参见 Song 方案的引理 6. 方案Ⅱ具有正确性:签名的有效性可以通过验证等式验证;由于签名的交互式协议是关于成员证书和相应成员私钥的统计零知识证明,则有效的签名中 A 和 B 一定具有正确的形式,又由定理 2,打开算法总能正确地揭示签名者的身份.

定理 3. 在确定 Diffie-Hellman 假设下以及在随机 Oracle 模型中,方案满足向后不可联接匿名性.

证明. 假设存在一个敌手 A 能在多项式时间内破解方案的向后不可联接匿名性,则可以构造多项式时间算法 B 破解确定 Diffie-Hellman 假设. B 的输入为 $(g,\ g_1=g^{\alpha},\ g_2=g^{\beta},\ Z)$, Z 为 $g^{\alpha\beta}$ 或 g^{γ},其中 $\alpha,\beta,\gamma\in_R Z_{p'q'}$, B 通过和 A 交互来确定 Z. B 建立方案Ⅱ, $gpk=(n,a,d,g,h,y=g_1,u)$, $ik=(p',\ q')$, B 不知道 ok. B 给 A 群公钥 gpk 和 ik. 由 B 通知 A 每个时间段的开始,假设当前时间段为 j, B 可以模拟如下 Oracle[15] 供 A 访问, $CrptU()$:收买某个成员,改变他的成员公钥,准备重新加入群; $SndToI()$:以用户的角色和证书颁发者执行加入协议,设定成员表; $SndToU()$:以证书颁发者的角色和用户执行加入协议,生成成员密钥; $USK()$:得到成员 i 在时间段 j 的密钥; $Wreg()$:改写成员表; $RevokeU()$:撤消时间段 $k(k\leqslant j)$ 后任意成员 i 的身份,将 i 相应的加入标记写入 E_{del}.

A 向 B 发送一个消息 M 和两个成员 i_0 和 i_1, i_0, i_1 在当前时间段 j 之前(包括 j)没有被撤消并且其成员密钥未曾被 A 请求过. B 选择 $\phi\in_R\{0,1\}$,由于协议的零知识性,即使不知道 i_ϕ 的成员私钥, B 也可以模拟 i_ϕ 执行签名协议. B 选取 $w_1,w_2,w_3\in_R Z_{p'q'}$, $c\in_R\{0,1\}^k$, $s_1,\cdots,s_8$,计算 $A=C_{i_\phi,j}Z \bmod n$, $B=g_2 \bmod n$, $C_e=g^{e_{i_\phi,j}}h^{w_1} \bmod n$, $C_u=h^{w_2} \bmod n$, $C_r=g^{w_2}h^{w_3} \bmod n$,所模拟的签名协议中值的概率分布和实际协议中的观察在统计上是不可区分的. 由验证协议 B 计算出 $t_1,\cdots,t_7$,通过控制随机 Oracle 让 $H(j\|a\|d\|g\|h\|y\|A\|B\|C_e\|C_u\|C_r\|t_1\|t_2\|t_3\|t_4\|t_5\|t_6\|t_7\|M)=c$, B 将模拟的签名 $sig=(A,B,C_e,C_u,C_r,c,s_1,s_2,s_3,s_4,s_5,s_6,s_7,s_8)$ 发送给 A. 随后, A 可以继续访问以上 Oracle,但在当前时间段 j, $USK()$ 和 $RevokeU()$ 中 i_0 和 i_1 除外. 如果 A 能破解签名的匿名性,则 B 可以判定 Z 为 $g^{\alpha\beta}$,从而破解了确定 Diffie-Hellman 假设. 证毕.

定理 4. 假设发布的成员证书个数 K 多项式有界,在强 RSA 假设下,方案满足可跟踪性.

证明. 假设存在一个敌手 A 能在多项式时间内破解方案的可跟踪性,则可以构造多项式时间算法 B 破解方案的抗联合攻击性. B 建立方案Ⅱ,给 A gpk 和 ok, A 可以访问 $SndToI()$, $USK()$, $CrptU()$ 和 $RevokeU()$,还可以访问 $AddU()$ 增加一个成员. $Rreg()$:读取成员表. 假设 A 和一个诚实的验证者执行签名协议,GM 不能够揭示其签名者的身份. 由于协议具有合理性,所以 B 可以提取知识 $(C_{p,j},e_{p,j},x_p,u_p)$ 满足 $C_{p,j}^{e_{p,j}}=a^{x_p}d \bmod n$ 和 $u=f(u_p,e_{p,j})$,由于敌手 A 没有 ik 并且不能改写成员表,所以如果不能在成员表中找到相应的证书 $\langle C_{p,j},e_{p,j}\rangle$,则 B 生成了一个新的有效的成员证书,从而破解了方案的抗联合攻击性.

定理 5. 在 QR_n 中离散对数问题难解的假设下,方案满足抗陷害性.

证明. 假设存在一个敌手 A 能在多项式时间内破解方案的抗陷害性,则可以构造多项式时间算法 B 破解 QR_n 中离散对数问题. (a,D,n,p',q') 是 QR_n 中离散对数问题的一个实例, B 求解 D 以 a 为底模 n 的离散对数. B 建立方案Ⅱ,生成群公钥 $gpk=(n,a,d=a^r,g,h,y=g^x,u)$,其中 $r,x\in_R Z^*_{p'q'}$, $ik=(p',\ q')$, $ok=x$. B 将 gpk, ik 和 ok 给 A. B 模拟用户集合,设 K 为集合大小的上限. B 选择 $i_h\in_R\{1,\cdots,K\}$,并模拟 $SndToU()$, $Wreg()$, $GSig()$, $USK()$, $CrptU()$ 和 $RevokeU()$ 供 A 访问,其中 $GSig()$ 允许 A 得到成员 $i(i_h$ 除外)对消息 M 的签名, $USK()$ 中访问 i_h 时返回失败. $SndToU(i,Min)$ 中,如果 $i\neq i_h$, B 模拟诚实的用户 i 执行加入协议;如果 $i=i_h$,在加入协议中 B 发送 $C_2=a^{r_h}D$ 给 GM,其中 $r_h\in_R Z_{p'q'}$,通过控制随机 Oracle, B 可以模拟相应的知识证明. 因为 C_2 在 QR_n 中是均匀分布的,所以 A 不会觉察出它和实际协议中值的差别,协议最后得到 i_h 的成员证书 $[C_{i_h,0},\ e_{i_h,0}]$. 假设 A 在时间段 j 能够以 i_h 的身份签名,由于签名协议具有合理性, B 可以提取知识 $(C,\ e,\ x)$,满足 $C^e=da^x \bmod n$,则 $C=C_{i_h,j}$,所以有 $(da^x)^{1/e}=(da^{r_h}D)^{1/e_{i_h,j}}$, $D=a^{(r+x)(e_{i_h,j}/e)-r-r_h}$,由此可以求出 D 的离散对数. 证毕.

4 性能分析

所提出的两个方案都解决了 Song 方案中验证算法的计算量线性依赖于被撤消成员个数的问题,同时也解决了基于累加器撤消方法的缺陷. 算法中的主要运算为模幂、模乘和平方运算,我们分别用 E,M 和 S 表示,k, T 分别表示被撤消成员的个数和时间段个数. 我们主要从签名和验证方面与 Song 方案进行比较(见表 1), Song 方案中签名算法的计算量较小,但是验证算法的计算量与 k 线性相关,特别是在大群体中,随着 k 的增大,验证算法的效率将会明显降低. 我们方案中验证算法的计算量为常量,效率高于 Song 方案. 我们提出的两个方案中,方案Ⅰ中的密钥演化需要一次平方运算,方案Ⅱ中的密钥演化需要 $O(T)$ 次模幂运算,方案Ⅰ密钥演化的效率高于方案Ⅱ,但是方案Ⅰ中签名和验证算法的计算量比方案Ⅱ多执行 $O(T)$ 次平方运算. 在成员撤消方面,方案Ⅰ需要执行 $O(T)$ 次模幂运算,方案Ⅱ只需要一次模幂运算,提高了撤消效率. 方案Ⅰ中群公钥长度、签名和验证算法的计算量和 T 线性相关,在 T 不是很大的情况下较为实用,方案Ⅱ解决了方案Ⅰ的不足,群公钥的长度、签名和验证算法的计算量均独立于时间段个数.

Table 1 Computational Cost Comparison of Our Scheme and Song Scheme

表 1 提出的方案与 Song 方案计算量的比较

Scheme	Sign	Verify
Song Ⅰ	20E+17M+$O(T)$S	(22+k)E+13M+(k+1)$O(T)$S
Our Scheme Ⅰ	22E+23M+$O(T)$S	20E+13M+$O(T)$S
Song Ⅱ	10E+9M+7S	(10+k)E+6M+10S
Our Scheme Ⅱ	22E+23M	20E+13M

5 总 结

成员撤消和如何处理密钥泄漏是群签名应用中的两个重要问题,目前还没有方案能同时处理好这两个问题. 本文提出的两个方案都能同时解决这两个问题,方案Ⅱ克服了方案Ⅰ中群公钥长度、签名和验证算法的计算量和时间段个数线性相关的不足. 和已有的同类群签名方案相比,两个方案具有高效撤消性和前向安全性,签名验证算法的计算量独立于被撤消成员个数,本文提出的两个方案具有实际应用价值.

参 考 文 献

[1] D Chaum, E van Heyst. Group signatures [C]. In: Advances in Cryptology—EUROCRYPT '91. Berlin: Springer-Verlag. 1991. 257-265

[2] G Ateniese, G Tsudik. Some open issues and new directions in group signature schemes [C]. In: Financial Cryptography (FC '99). Berlin: Springer-Verlag, 1999. 196-211

[3] E Bresson, J Stern. Efficient revocation in group signatures [C]. In: Public Key Cryptography (PKC '01). Berlin: Springer-Verlag, 2001. 190-206

[4] G Ateniese, G Tsudik, D Song. Quasi-efficient revocation of group signatures [C]. The Financial Cryptography 2002, Bermuda, 2002

[5] J Camenisch, A Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials [C]. In: Proc of Crypto 2002. Berlin: Springer-Verlag, 2002. 61-76

[6] R Anderson. Invited lecture [C]. The 4th ACM Conf on Computer and Communications Security, Zurich, 1997

[7] D X Song. Practical forward secure group signature schemes [C]. In: Proc of the 8th ACM Conf on Computer and Communications Security (CCS 2001). New York: ACM Press, 2001. 225-234

[8] J Zhang, Q Wu, Y Wang. A novel efficient group signature scheme with forward security [C]. In: Proc of Int'l Conf on Information and Communications Security (ICICS '03). Berlin: Springer-Verlag, 2003. 292-300

[9] G Wang. On the security of a group signature scheme with forward security [C]. In: Proc of Int'l Conf on Information Security and Cryptology—ICISC 2003. Berlin: Springer-Verlag, 2003. 27-39

[10] Chen Shaozhen, Li Daxing. An efficient revocable group signature schemes with forward security [J]. Chinese Journal of Computers, 2006, 29(6): 998-1003 (in Chinese)
(陈少真, 李大兴. 有效取消的向前安全群签名体制. 计算机学报, 2006, 29(6): 998-1003)

[11] G Ateniese, J Camenisch, M Joye, *et al*. A practical and provably secure coalition-resistant group signature scheme [C]. In: Advances in Cryptology—CRYPTO 2000. Berlin: Springer-Verlag, 2000. 255-270

[12] A Fiat, A Shamir. How to prove yourself: Practical solutions to identification and signature problems [C]. In: Advances in Cryptology—Crypto '86. Berlin: Springer-Verlag, 1986. 186-194

[13] M Bellare, S Miner. A forward-secure digital signature scheme [C]. In: Advances in Cryptology—CRYPTO '99. Berlin: Springer-Verlag, 1999

[14] G Itkis, L Reyzin. Forward-secure signatures with optimal signing and verifying [C]. In: Advances in Cryptology—CRYPTO 2001. Berlin: Springer-Verlag, 2001. 332-354

[15] M Bellare, H Shi, C Zhang. Foundations of group signatures: The case of dynamic groups [C]. In: CT-RSA 2005. Berlin: Springer-Verlag, 2005. 136-153

Li Rupeng, born in 1976. Since 2004, he has been a Ph. D. candidate in computer science from Shandong University. His main research interests are cryptography and network security.

李如鹏,1976 年生,博士研究生,主要研究方向为密码学、网络安全.

Yu Jia, born in 1976. Received his Ph. D. degree in computer science from Shandong University in 2006. He is a lecturer in Qingdao University. His main research interests are cryptography and network security.

于 佳,1976 年生,博士,讲师,主要研究方向为密码学、网络安全.

Li Guowen, born in 1976. Since 2003, he has been Ph. D. candidate in computer science from Shandong University. His main research interests are cryptography and network security.

李国文,1976 年生,博士研究生,主要研究方向为密码学、网络安全.

Li Daxing, born in 1963. Professor and Ph. D. supervisor in Shandong University. His main research interests are cryptography and network security.

李大兴,1963 年生,教授,博士生导师,主要研究方向为密码学、网络安全.

Research Background

Group signature scheme has many applications such as electronic voting and electronic cash systems. How to cope with key exposure and how to efficiently revoke group membership are two important issues in designing group signature schemes. Up to now, there are few group schemes that can solve the two problems at the same time. And they all have drawbacks. The methods of revocation can be classed into two categories. One is based on revocation list (RL), its complexity of the verifying algorithm linearly depends on the size of RL; the other is based on witness, the verifying algorithm is more efficient than that of RL-based solution. But it has the common drawback: previously signed signatures can not pass the verifying algorithm under the updated public value after the signer is revoked. Based on the ACJT group signature scheme, two new group signature schemes are proposed. The main trait is that they have efficiently revocable property and forward secure property at the same time. Both the schemes tackle the drawback of witness-based solution and support retroactively publicly revocable group membership with backward unlinkability. The computational cost of signing and verifying is independent of the number of the current group members and the revoked group members. Our work is supported by the 863 Project of China (No. 2003AA141120, 2004AA001260).