第42卷 第10期 西 安 交 通 大 学 学 报 Vol.42 №10
2008年10月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Oct. 2008

具有局部验证者撤销的短群签名方案

张京良[1,2]，李艳平[1,3]，王育民[1]
（1.西安电子科技大学综合业务网国家重点实验室，710071，西安；2.中国海洋大学数学学院，266071，山东青岛；3.陕西师范大学数学与信息科学学院，710062，西安）

摘要：针对局部验证者撤销群签名中如何降低计算量、缩短签名长度等问题，提出了一种具有局部验证者撤销群签名方案.基于强Diffie-Hellman假设和判定性三重Diffie-Hellman假设，通过群管理员与群成员共同生成密钥来实现防陷害性，通过验证撤销列表中的量与某个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，从而避免了双线性运算，克服了以往局部验证者撤销群签名方案的撤销验证计算量与撤销列表长度呈线性增长的缺点.所提方案的签名长度为1 533 b，比已有方案的签名长度缩短了30%～47%.

关键词：群签名；局部验证者撤销；双线性映射
中图分类号：TP309 **文献标志码**：A **文章编号**：0253-987X(2008)10-1250-04

Shorter Group Signatures Scheme with Verifier-Local Revocation

ZHANG Jingliang[1,2], LI Yanping[1,3], WANG Yumin[1]
(1. State Key Laboratory of Integrated Service Networks, Xidian University, Xi′an 710071, China; 2. College of Mathematics, Ocean University of China, Qingdao, Shandong 266071, China; 3. College of Mathematics and Information Science, Shaanxi Normal University, Xi′an 710062, China)

Abstract: Aiming at the intrinsic problems in verifier-local revocation group signatures, such as reducing the computational costs, shortening the signature length and so on, a new verifier-local revocation group signature is proposed based on the strong Diffie-Hellman assumption and the decisional tripartite Diffie-Hellman assumption. In the proposed scheme, a member in the group generates his own private key together with the group manager to realize exculpability, and the computation costs of revocation check are independent of the length of the revocation list by verifying whether the value in the revocation list is equal to some known value in the signing process. The bilinear maps in the revocation check are no longer required, and the shortcoming that the computational costs are linear with the length of the revocation list in the existing verifier-local revocation (VLR) schemes is overcome. The size of a signature in the proposed scheme is just 1 533 bits, and reduces about 30%-47% compared with that of the existing VLR group signatures.

Keywords: group signature; verifier-local revocation; bilinear map

成员撤销是群签名的重要内容，最简单的撤销方法是群管理员给群成员重新分配密钥或证书，这种方法效率太低，更好的方法是对所有签字者及验证者广播公共成员资格信息，但签名者仍得到了一些冗余信息，而局部验证者撤销(VLR)法仅需将撤销信息发送给验证者[1-4].

在上述方法的基础上，基于短群签名的局部验证者撤销方案应运而生[5-10]，但这些方案都有一个共同缺陷，即在签名验证阶段进行撤销验证时，撤销验证的计算量随着撤销列表长度的增加呈线性增长

收稿日期：2007-12-04. 作者简介：张京良(1973—)，男，博士生；王育民(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60473027).

的趋势.

本文基于强 Diffie-Hellman(q-SDH)假设、判定性三重 Diffie-Hellman(DTDH)假设和离散对数(DL)假设，提出了一种新的 VLR 群签名方案. 该方案的撤销验证计算量与撤销列表长度无关，签名长度达到了目前最短的水平.

1　VLR 群签名

设 $G=\langle g\rangle$ 和 G' 是阶为素数 p 的乘法循环群，e 是 $G\times G$ 到 G' 的双线性映射. 本文的安全性假设包括 q-SDH 假设[5-10]、DTDH 假设[8]及 DL 假设[10].

公钥生成算法 KEYGEN(n, T)：假设 n 是群成员个数，T 是时间区间个数，则算法如下.

(1)群管理员 M_G 选 G 的一个生成元 g 及 $\tilde{g}\in_R G$，并对所有的时间段 $j\in[1,T]$，选 $h_j\in_R G$. 另外，选一抗碰撞的 Hash 函数 $H:\{0,1\}^*\to Z_p^*$，使得 $\gamma\in_R Z_p^*$，并计算 $\omega=g^\gamma$. 那么，群公钥 $k_{GP}=(g,\tilde{g},h_1,\cdots,h_T,\omega)$.

(2)成员 i 选 $y_i\in_R Z_p^*$，将 $\tilde{g}^{y_i}$、$B'_{ij}=h_j^{y_i}$ 发送给 M_G.

(3)M_G 选 $x_i\in_R Z_p^*$，计算 $A_i=(\tilde{g}^{y_i}g)^{1/(\gamma+x_i)}$ 并对所有时间段 j 计算 $B_{ij}=B'^{x_i}_{ij}$，则成员 i 的私钥 $k_{GS}[i]=(A_i,x_i,y_i)$，成员 i 在时间段 j 的撤销标记是 $t_{GR}[i][j]=B_{ij}$.

签名算法 SIGN(k_{GP}, j, $k_{GS}[i]$, m)：为了将签名同时间绑定，需假设消息 $m\supseteq j$，那么成员 i 的工作如下.

(1)随机选择 $\alpha\in Z_p^*$，计算 $T_1=A_i\tilde{g}^\alpha$，$T_2=T_1^{y_i}$，$T_3=h_j^{x_iy_i}$.

(2)令 $\zeta=x_i\alpha$，$\eta=x_iy_i$，生成的知识签名 $V=\mathrm{SPK}\{(\alpha,x_i,y_i,\zeta,\eta)\}=(c,s_\alpha,s_{x_i},s_{y_i},s_\zeta,s_\eta)$，则成员 i 在时间段 j 对消息 m 的群签名 $\sigma=(T_1,T_2,T_3,V)$. 其中，V 的计算方法是：选 $r_\alpha,r_{x_i},r_{y_i},r_\zeta,r_\eta\in_R Z_p^*$，计算 $R_1=(e(\tilde{g},\omega)^{r_\alpha}e(\tilde{g},g)^{r_{y_i}}e(\tilde{g},g)^{r_\zeta})/e(T_1,g)^{r_{x_i}}=e(\tilde{g},\omega^{r_\alpha}g^{r_{y_i}+r_\zeta})/e(T_1,g)^{r_{x_i}}$，$R_2=T_1^{r_{y_i}}$，$R_3=h_j^{r_\eta}$，$c=H(gpk,M,T_1,T_2,T_3,R_1,R_2,R_3)$，$s_\alpha=r_\alpha+c\alpha$，$s_{x_i}=r_{x_i}+cx_i$，$s_{y_i}=r_{y_i}+cy_i$，$s_\zeta=r_\zeta+c\zeta$，$s_\eta=r_\eta+c\eta$，从而获得 $V=(c,s_\alpha,s_{x_i},s_{y_i},s_\zeta,s_\eta)$.

撤销算法 REVOKE (L_{Rj}, $t_{GR}[i][j]$)：如果成员 i 在时间段 j 被撤销，则 $L_{Rj}\leftarrow L_{Rj}\cup\{B_{ij}\}$.

验证算法 VERIFY(k_{GP}, j, L_{Rj}, σ, m)：算法验证内容如下.

(1)签名验证. 给定 $\sigma=(T_1,T_2,T_3,c,s_\alpha,s_{x_i},s_{y_i},s_\zeta,s_\eta)$，计算 $R'_1=((e(\tilde{g},\omega)^{s_\alpha}e(\tilde{g},g)^{s_{y_i}}e(\tilde{g},g)^{s_\zeta})/e(T_1,g)^{s_{x_i}})(e(g,g)/e(T_1,\omega))^c=(e(\tilde{g},\omega^{s_\alpha}\cdot g^{s_{y_i}+s_\zeta})e(g,g)^c)/e(T_1,g^{s_{x_i}}\omega^c)$，$R'_2=T_1^{s_{y_i}}/T_2^c$，$R'_3=h_j^{s_\eta}/T_3^c$. 由此可验证 $c=H(k_{GP},M,T_1,T_2,T_3,R'_1,R'_2,R'_3)$.

(2)撤销验证. 对所有 $B_{ij}\in L_{Rj}$，通过验证 $B_{ij}\neq T_3$ 来说明签名者在时间段 j 未被撤销.

2　VLR 群签名的安全性

一个 VLR 群签名需满足后向不可联结匿名性(BU-匿名性)和可追踪性[6-10].

定理 1　假设敌手 $\mathcal{A}$ 经过 q_H 次 Hash 询问、q_S 次签名询问后，以优势 ε 攻破方案的 BU-匿名性，则存在算法 $\mathcal{B}$ 能以优势 $(1/(nT)-(q_Hq_S)/p)\varepsilon$ 攻破 DTDH 假设. 从而，在随机预言机模型及 DTDH 假设下，本文 VLR 群签名方案满足 BU-匿名性.

证明　$\mathcal{B}$ 的输入是 $(g,g_1=g^a,g_2=g^b,g_3=g^c,Z)$，其中 $Z=g^{abc}$ 或 $Z=g^d$，$a,b,c,d\in_R Z_p^*$. $\mathcal{B}$ 的任务是，通过与 $\mathcal{A}$ 交互来区分所给的 $Z=g^{abc}$ 或 $Z=g^d$.

首先建立 $\mathcal{B}$，以模拟 KEYGEN(n, T)，步骤如下.

(1)$\mathcal{B}$ 选 $i^*\in_R[1,n]$，$j^*\in_R[1,T]$，$\tilde{g}\in_R G$，$\gamma\in_R Z_p^*$，计算 $\omega=g^\gamma$；选 $r_j\in_R Z_p^*$，计算

$$h_j=\begin{cases}g^{r_j}, & j\neq j^*\\ g_2=g^b, & j=j^*\end{cases}$$

对 $i\in[1,n]$，选 $y_i\in_R Z_p^*$.

当 $i\neq i^*$ 时，$\mathcal{B}$ 取 $x_i\in_R Z_p^*$，计算 $A_i=(\tilde{g}^{y_i}\cdot g)^{1/(\gamma+x_i)}$；当 $i=i^*$ 时，定义 $x_{i^*}=a$，$A_{i^*}=(\tilde{g}^{y_{i^*}}\cdot g)^{1/(\gamma+a)}$，但 $\mathcal{B}$ 并不知道 x_{i^*} 及 A_{i^*}，因为 $\mathcal{B}$ 不知 a.

(2)$\mathcal{B}$ 计算 $B_{ij}=h_j^{x_iy_i}$，$i\neq i^*$；$B_{i^*j}=g_1^{r_jy_{i^*}}=g^{ar_jy_{i^*}}=h_j^{ay_{i^*}}=h_j^{x_{i^*}y_{i^*}}$，$j\neq j^*$. 定义 $B_{i^*j^*}=g^{aby_{i^*}}=h_{j^*}^{x_{i^*}y_{i^*}}$，此值 $\mathcal{B}$ 不知道，因为 $\mathcal{B}$ 不知 a、b.

其次，进行如下询问.

(1)Hash 询问. $\mathcal{A}$ 可在任意时间询问 SPK 中所用的 Hash 值，$\mathcal{B}$ 用随机值应答，保持相同的询问，并用相同的应答.

(2)签名询问. 其一，$\mathcal{A}$ 询问成员 i 在任何时间段 j 的签名. 当 $i\neq i^*$ 时，$\mathcal{B}$ 由于知道 (A_i,x_i,y_i)，故可用签名算法 SIGN 计算出签名，并做应答；当 $i=i^*$，$j\neq j^*$ 时，$\mathcal{B}$ 选 $T_1\in_R G$，计算 $T_2=T_1^{y_{i^*}}$，$T_3=g_1^{r_jy_{i^*}}=g^{ar_jy_{i^*}}=h_j^{ay_{i^*}}=h_j^{x_{i^*}y_{i^*}}$；当 $i=i^*$，$j=j^*$ 时，$\mathcal{B}$ 选 $z,u\in_R Z_p^*$，计算 $T_1=g_2^u$，$T_2=g^{zu}$，$T_3=g_1^z$. 在 $\mathcal{A}$ 看来，同样满足 $T_2=T_1^{y_{i^*}}$，$T_3=$

$h_{j^*}^{x_{i^*}y_{i^*}}$，其中 $y_{i^*}=z/b$. 其二，$\mathcal{B}$ 模拟 Hash 输出，计算出 T_1、T_2、T_3 的模拟知识签名 $V=\mathrm{SPK}(T_1,T_2,T_3)$. 若 Hash 输出值与上一次询问值相同，则 $\mathcal{B}$ 退出并输出一随机猜测值 $\omega'\in_R\{0,1\}$，否则 $\mathcal{B}$ 对 $\mathcal{A}$ 的应答是模拟签名 $\sigma=(T_1,T_2,T_3,V)$.

(3)撤销询问. $\mathcal{A}$ 询问成员 i 在时间段 j 时的撤销标志. 若 $i\neq i^*$ 或 $j\neq j^*$，$\mathcal{B}$ 以 B_{ij} 作为对 $\mathcal{A}$ 的应答；若 $i=i^*$ 且 $j=j^*$，则 $\mathcal{B}$ 输出一随机猜测 $\omega'\in_R\{0,1\}$，并退出.

(4)贿赂询问. 首先 $\mathcal{A}$ 询问成员 i 的私钥. 若 $i\neq i^*$，$\mathcal{B}$ 以 (A_i,x_i,y_i) 作为应答；若 $i=i^*$，$\mathcal{B}$ 输出一随机猜测 $\omega'\in_R\{0,1\}$ 并退出.

再次进行挑战. $\mathcal{A}$ 输出消息 m、时间段 j 和 2 个成员 i_0、i_1. $\mathcal{B}$ 选 $\varphi\in_R\{0,1\}$，若 $i_\varphi\neq i^*$ 或 $j\neq j^*$，$\mathcal{B}$ 输出一随机猜测值 $\omega'\in_R\{0,1\}$ 并退出；若 $i_\varphi=i^*$ 且 $j=j^*$，$\mathcal{B}$ 生成挑战签名，即将 c 当作 y_{i^*}，选 $r\in_R Z_p^*$，令 $T_1=g^r$，$T_2=g_3{}^r$，$T_3=Z$，并计算模拟知识签名 $V=\mathrm{SPK}(T_1,T_2,T_3)$. 可见，若 $Z=g^{abc}$，则 $T_1=g^r$，$T_2=g_3{}^r=g^{cr}=T_1{}^c=T_1{}^{y_{i^*}}$，$T_3=g^{abc}=h_{j^*}{}^{x_{i^*}c}=h_{j^*}{}^{x_{i^*}y_{i^*}}$，$(T_1,T_2,T_3,V)$ 是一分布同真实签名的模拟签名；若 $Z=g^d$，则 $T_3=g^d$，此时 $\mathcal{A}$ 只能靠猜测来判断 φ.

最后 $\mathcal{A}$ 输出 $\varphi'\in\{0,1\}$. 若 $\varphi=\varphi'$，$\mathcal{B}$ 输出 $\omega'=1$（指 $Z=g^{abc}$），否则 $\mathcal{B}$ 输出 $\omega'=0$（即 $Z=g^d$）.

采用类似于文献[8]中的分析方法，可得 $\mathcal{B}$ 猜出 ω 的优势即为攻破 DTDH 假设的优势，至少为 $(1/nT-q_Sq_H/p)\varepsilon$.

定理 2 假设敌手 $\mathcal{A}$ 经过 q_H 次 Hash 询问、q_S 次签名询问后，以优势 ε 攻破方案的可追踪性，则存在算法 $\mathcal{B}$ 能以优势 $(\varepsilon/(2n)-1/p)^2/(32\times q_H)$ 攻破 $(n+1)$ 次 q-SDH 假设或以优势 $(\varepsilon/(2n)-1/p)^2/(32\times q_H)$ 攻破 DL 假设.

证明 首先 $\mathcal{B}$ 已知 $g,\omega=g^\gamma$ 且有 n 个对 (A_i,x_i). 对于 $i\in[1,n]$，选 $y_i\in_R Z_p^*$，并用 $s_i=1$ 表示 (A_i,x_i) 是一个 SDH 对，用 $s_i=0$ 表示 $\mathcal{B}$ 知道 x_i 但其对应的 A_i 不知道. 另外，对于 $j\in[1,T]$，选 $\tilde{g},h_j\in_R G$，计算 $B_{ij}=h_j{}^{x_iy_i}$. 告知 $\mathcal{A}$ 公钥为 $k_{GP}=(g,\tilde{g},h_1,\cdots,h_T,\omega)$，其撤销标记是 $t_{GR}=(B_{11},\cdots,B_{nT})$.

其次进行如下询问.

(1)Hash 询问. $\mathcal{A}$ 可在任意时间询问 SPK 中所用的 Hash 值，$\mathcal{B}$ 用随机值应答，并保持询问相同、应答相同.

(2)签名询问. $\mathcal{A}$ 询问成员 i 在任何时间段 j 的签名. 当 $s_i=1$ 时，$\mathcal{B}$ 知道 (A_i,x_i,y_i)，所以可用 SIGN 算法计算出签名，并将结果作为应答；当 $s_i=0$ 时，$\mathcal{B}$ 选 $T_1\in_R G$，计算 $T_2=T_1{}^{y_i}$，$T_3=h_j{}^{x_iy_i}$，然后模拟 Hash 输出，计算出模拟知识签名 $V=\mathrm{SPK}(T_1,T_2,T_3)$，而 $\mathcal{B}$ 对 $\mathcal{A}$ 的应答是模拟签名 $\sigma=(T_1,T_2,T_3,V)$.

(3)贿赂询问. $\mathcal{A}$ 询问成员 i 的私钥. 若 $s_i=0$，则 $\mathcal{A}$ 退出；若 $s_i=1$，$\mathcal{B}$ 以 (A_i,x_i,y_i) 应答.

最后 $\mathcal{A}$ 输出一个包含有私钥 A^* 的伪造签名 $\sigma^*=(T_1{}^*,T_2{}^*,T_3{}^*,V^*)$，但应用签名算法隐含的打开算法，可识别出签名成员. 若识别失败（识别出的成员不包含在所有成员之中），则输出 σ^*；若识别正确（识别出了某个成员），则当 $s_i=0$ 时输出 σ^*，而当 $s_i=1$ 时 $\mathcal{A}$ 退出.

采用类似于文献[10]的方法知，$\mathcal{B}$ 可以优势 $(\varepsilon/(2n)-1/p)^2/(32\times q_H)$ 攻破 $(n+1)$ 次 SDH 假设或以优势 $(\varepsilon/(2n)-1/p)^2/(32\times q_H)$ 攻破 DL 假设.

综上，在随机预言机模型及 q-SDH 假设、DL 假设下，本文 VLR 群签名方案满足可追踪性.

3 性能及比较

签名长度 本文方案的签名 $\sigma=(T_1,T_2,T_3,c,s_\alpha,s_{x_i},s_{y_i},s_\alpha,s_\eta)$ 中包含了 G 中 3 个元素、Z_p 中 6 个元素. 与文献[5-10]相同，取 $p=170$ b，G 中元素为 171 b，则本文方案的签名长度为 1 533 b.

计算量 生成签名需要 6 个复合模指数 e_M 及 2 个双线性映射 m_B 计算，验证过程需要进行 $3e_M$ 和 $3m_B$ 次. 若先对 $e(\tilde{g},\omega)$、$e(\tilde{g},g)$、$e(g,g)$ 进行预算，则生成签名的计算量为 $6e_M+1m_B$，验证过程的计算量为 $3e_M+1m_B$.

本文方案与向后不可关联性的 VLR 群签名方案的性能比较如表 1 所示.

表 1 性能比较

方案	签名长度/b	生成签名计算量	验证过程的计算量
文献[6]	2 893	$10e_M+4m_B$	$6e_M+(6+\lvert L_{Rj}\rvert)m_B$
文献[8]	2 215	$10e_M+2m_B$	$6e_M+(3+\lvert L_{Rj}\rvert)m_B$
文献[9]中方案3	2 213	$8e_M+3m_B$	$7e_M+(4+\lvert L_{Rj}\rvert)\ m_B$
文献[10]	1 533	$6e_M+3m_B+I$	$4e_M+(6+\lvert L_{Rj}\rvert)\ m_B+I$
本文	1 533	$6e_M+1m_B$	$3e_M+1m_B$

注：I 表示同构.

由表 1 可见，本文方案的签名长度最短，计算量

最小，尤其是验证阶段的计算量与撤销列表长度无关，它克服了以往 VLR 群签名方案的验证计算量随撤销列表长度呈线性增长的问题.

4　结束语

本文提出了一种 VLR 群签名方案，其在 q-SDH 假设和 DTDH 假设下，满足向后不可关联性和可追踪性. 与已有 VLR 群签名方案相比，所提方案的签名长度最短，计算量最小，可应用于 IEEE802.1x 等移动环境.

参考文献：

[1] CHAUM D. Group signatures [C]// Workshop on the Theory and Application of Cryptographic Techniques Proceedings. Berlin, Germany: Springer-Verlag, 1992: 257-265.

[2] BRESSON E, STERN J. Efficient revocation in group signatures [C] // Proceedings of 4th International Workshop on Practice and Theory in Public Key Cryptosystems. Berlin, Germany: Springer-Verlag, 2001: 190-206.

[3] BONEH D, BOYEN X, SHACHAM H. Short group signatures [C]// Proceedings of 24th Annual International Cryptology Conference. Berlin, Germany: Springer-Verlag, 2004: 41-55.

[4] BOYEN X, WATERS B. Full-domain subgroup hiding and constant-size group signatures [C]// Proceedings of 10th International Conference on Practice and Theory in Public-Key Cryptography. Berlin, Germany: Springer-Verlag, 2007: 1-15.

[5] BONEH D, SHACHAM H. Group signatures with verifier-local revocation [C]// Proceedings of the ACM Conference on Computer and Communications Security. New York, USA: ACM, 2004: 168-177.

[6] NAKANISHI T, FUNABIKI N. Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps [C] // Proceedings of 11th International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer-Verlag, 2005: 533-548.

[7] NAKANISHI T, FUNABIKI N. Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps [J]. IEICE Trans on Fundamentals of Electronics, 2007, E90-A (1): 65-74.

[8] ZHOU Sujing, LIN Dongdai. A short group signature with verifier-local revocation and backward unlinkability [EB/OL]. [2006-10-11]. http://eprint.iacr.org/2006/100.pdf.

[9] ZHOU Sujing, LIN Dongdai. Shorter verifier-local revocation group signatures from bilinear maps [C]// Proceedings of 5th International Conference on Cryptology and Network Security. Berlin, Germany: Springer-Verlag, 2006: 126-143.

[10] NAKANISHI T, FUNABIKI N. A short verifier-local revocation group signature scheme with backward unlinkability [J]. IEICE Trans on Fundamentals of Electronics, 2007, E90-A(9): 1793-1802.

（编辑　苗凌）

西安交通大学国家重点实验室在评估中喜获佳绩

据国家重点实验室官方网站消息，科技部公布了 2008 年工程与材料领域国家及部门重点实验室评估结果. 西安交通大学动力工程多相流国家重点实验室继 2003 年重点实验室评估被评为优秀类实验室后，今年再一次被评为优秀类实验室，其他 4 个参评实验室被评为良好类实验室.

今年科技部对 54 个工程与材料领域国家和部门重点实验室组织了评估，其中工程领域 34 个，材料领域 20 个；国家重点实验室 50 个，部门实验室 4 个. 经过现场评估和复评，最终产生了 9 个优秀类实验室，其中工程领域 5 个，材料领域 4 个；产生了 43 个良好类实验室，其中工程领域 28 个，材料领域 15 个. 西安交通大学共有 5 个实验室参评，其中工程领域的 4 个分别是动力工程多相流国家重点实验室、机械制造系统工程国家重点实验室、电力设备电气绝缘国家重点实验室和强度与振动教育部重点实验室，材料领域的是金属材料强度国家重点实验室.

（来源：西安交大科技在线 http://www.xjtust.com）