

一种 IND-CCA2 完全匿名的短群签名

张跃宇 陈 杰 苏万力 王育民

(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

摘 要 基于线性假设下的 Cramer-Shoup 加密方案和 SDH 假设,提出一种新的 SDH 问题的零知识证明协议,并基于此协议构造了一种在 Bellare-Micciancio-Warinshi 模型下可证明安全的短群签名方案.该方案具有 IND-CCA2 完全匿名性,允许攻击者在攻击完全匿名性时提问打开预言机.签名的长度仅为 1704bits.

关键词 群签名;完全匿名性;线性 Cramer-Shoup 加密;IND-CCA2 安全;判定线性假设
中图法分类号 TP309

A Short Group Signature with IND-CCA2 Full-Anonymity

ZHANG Yue-Yu CHEN Jie SU Wan-Li WANG Yu-Min

(Key Laboratory of Computer Network and Information Security of Ministry of Education, Xidian University, Xi'an 710071)

Abstract In CRYPTO 2004, a short group signature is proposed by Boneh, Boyen and Shacham, which is based on strong Diffie-Hellman(SDH) assumption and Decision Linear assumption. Thereafter it is denoted BBS. Only chosen plaintext attack(CPA) full-anonymity is achieved in BBS short group signature for CPA secure in linear encryption. In this case, adversary could not query an open oracle. However, when adversaries try to break the notion of chosen ciphertext attack(IND-CCA2) full-anonymity, they have the ability to query an open oracle in the current and strongest security model for group signatures. Hence adversaries can obtain the signer identity of the queried signature. This paper presents a new zero-knowledge protocol for SDH, which based on Cramer-Shoup encryption from the linear assumption. Using this protocol as a building block, a new short group signature is constructed in this paper, which is provable secure in the Bellare-Micciancio-Warinshi model. The scheme is of IND-CCA2-full-anonymity, which allows adversary querying open oracle when trying to attack the anonymity notion. And the signature is only 1704 bits in size.

Keywords group signature; full anonymity; linear Cramer-Shoup encryption; IND-CCA2 secure; decision linear assumption

1 引 言

1991 年 Chaum 和 Heyst 提出了群签名的概

念^[1],群签名允许任何群成员代表群进行匿名签名,如发生争执,群管理员能够揭示签名者的真实身份,同时,区分两个不同的群签名是否来自于同一个人,在计算上是不可行的.近年来,有很多种群签名

收稿日期:2007-05-08;修改稿收到日期:2007-07-25. 本课题得到国家“八六三”高技术研究发展计划项目基金(2007AA01Z435)、国家自然科学基金(60473072)和陕西省自然科学基金计划项目基金(2007F37)资助. 张跃宇,男,1978 年生,博士研究生,讲师,主要研究方向为数字签名与电子商务安全. E-mail:yyzhang@xidian.edu.cn. 陈 杰,女,1979 年生,博士研究生,讲师,主要研究方向为分组密码的分析与设计. 苏万力,男,1963 年生,博士研究生,副教授,主要研究方向为网络与信息安全. 王育民,男,1936 年生,教授,博士生导师,主要研究领域为信息论、编码、密码的理论与应用.

方案被提出,比较著名的有 ACJT 方案^[2],最先在强 RSA 和 DDH 假设下实现了可证明安全的抗联合攻击的群签名.2004 年提出的 BBS 方案^[3],在双线性群上实现了高效的、长度为 1533bits 的签名. Bellare, Micciancio 和 Warinshi(BMW)给出了群签名安全的形式化模型^[4],并首先提出一个在标准模型下可证安全的方案,由于采用的是广义的非交互式零知识证明技术,他们的方案效率较低,所以并不实用. Bellare, Shi 和 Zhang 针对动态群将 BMW 模型作了扩展^[5]. Boneh 和 Shacham 提出一种本地验证者撤销的群签名方案^[6],撤销消息仅发送给签名验证者,而无需与用户通信. Boneh 和 Waters 提出了第一个无需随机预言机模型的可证明安全并且实用的群签名方案^[7],而且该方案只依赖于相对弱的计算假设,即 CDH 假设和他们新引入的子群判定假设. 该方案的缺点是群公钥和签名长度与用户数成对数关系,因此群签名的长度随群大小增长. 由于是在合数阶群上进行签名,表示群签名的每一个元素都非常长,一个完整的群签名通常要数万比特. 2007 年, Boneh 和 Waters 采用新的非交互式零知识证明技术提出一个签名长度为常数的群签名,但该方案依然是在合数阶群上实现的. 上述方案中,有些为了获得更好的效率,模型的安全性被做了一定程度的弱化,例如文献[3,6-8]中的 CPA 完全匿名性,就是 BMW 模型中完全匿名性的弱化,在试图攻破匿名性定义时对攻击者做了限制,不允许提问打开预言机,即不能打开签名以获得签名者的身份.

本文基于 IND-CCA2 安全的线性 Cramer-Shoup 公钥加密方案^[9],设计了一种强 Diffie-Hellman 问题的零知识证明协议,并根据该协议提出了一种新的具有 IND-CCA2 完全匿名性的群签名,允许攻击者在匿名性攻击过程中提问打开预言机,实现了更严格安全定义下的短群签名,签名的长度为 1704bits.

2 预备知识

2.1 双线性群^[10]

设 $G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$ 和 G_3 是阶为素数 p 的循环群; ψ 是 G_2 到 G_1 的可计算的同构, $\psi(g_2) = g_1$; e 为可计算的映射 $e: G_1 \times G_2 \rightarrow G_3$, 该映射具有两个性质: (1) 双线性, 即对所有的 $u \in G_1, v \in G_2$ 及 $a, b \in Z$, 有 $e(u^a, v^b) = e(u, v)^{ab}$; (2) 非退化性, 即

$e(g_1, g_2) \neq 1$, 则称群 (G_1, G_2) 是一对双线性群.

2.2 q -SDH 假设^[11]

设 $G = \langle g \rangle$ 是阶数为素数 p 的循环群, 对所有的概率多项式时间算法 A , 概率 $\Pr[A(g, g^\gamma, \dots, g^{(\gamma^q)}) = (g^{1/(\gamma+x)}, x) \wedge x \in Z_p^*]$ 是可忽略的, 其中 $x, \gamma \in Z_p^*$.

2.3 判定线性 Diffie-Hellman(DLDH)假设^[3]

设 $G = \langle g \rangle$ 是阶数为素数 p 的循环群, $u, v, h, \eta \xleftarrow{R} G$, 且 $a, b \xleftarrow{R} Z_p$, 对所有的概率多项式时间算法 A , 概率 $\Pr[A(u, v, h, u^a, v^b, h^{a+b})] - \Pr[A(u, v, h, u^a, v^b, \eta)]$ 是可忽略的.

3 一种 SDH 问题的零知识证明协议

本节中提出的 SDH 问题的零知识证明协议是群签名方案的一个构造模块, 用来证明拥有一个 SDH 问题的解.

设 G, G_T 为阶为素数 p 的循环群, e 为可计算的映射 $e: G \times G \rightarrow G_T$, 取公共参数 $\omega, g, g_1, g_2, g_3 \in G$, 其中 $\omega = g^\gamma, \gamma \in Z_p^*$. 令 $h_1 = g_1^{\tilde{z}_1} g_3^{\tilde{z}_3}, h_2 = g_2^{\tilde{z}_2} g_3^{\tilde{z}_3}, z_1, z_2, z_3 \xleftarrow{R} Z_p$. SDH 对 (A, x) 满足 $e(A, \omega g^x) = e(g, g)$, 其中 $A \in G, x \in Z_p^*$ 且 $A^{x+\gamma} = g$. 下面使用协议 1 证明素数阶群上离散对数的知识.

协议 1.

示证者 Alice 随机选择指数 $\alpha, \beta \xleftarrow{R} Z_p$, 计算 A 的线性 Cramer-Shoup 加密 $T_1 = g_1^\alpha, T_2 = g_2^\beta, T_3 = g_3^{\alpha+\beta}, T_4 = Ah_1^\alpha h_2^\beta$, 然后计算两个辅助值 $\delta_1 = x\alpha, \delta_2 = x\beta$.

Alice 和验证者 Bob 进行满足以下等式的值 $(\alpha, \beta, x, \delta_1, \delta_2)$ 的知识证明:

$$\begin{aligned} g_1^\alpha &= T_1, g_2^\beta = T_2, g_3^{\alpha+\beta} = T_3, \\ T_1^x g_1^{-\delta_1} &= 1, T_2^x g_2^{-\delta_2} = 1, T_3^x g_3^{-\delta_1-\delta_2} = 1, \\ e(T_4, g)^x \cdot e(h_1, g)^{-\delta_1} \cdot e(h_1, \omega)^{-\alpha} \cdot e(h_2, g)^{-\delta_2} \cdot \\ e(h_2, \omega)^{-\beta} &= e(g, g) / e(T_4, \omega). \end{aligned}$$

证明过程如下.

Alice 随机选择 $r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \in Z_p$, 计算 $R_1 \leftarrow g_1^{r_\alpha}, R_2 \leftarrow g_2^{r_\beta}, R_3 \leftarrow g_3^{r_\alpha+r_\beta}, R_4 \leftarrow e(T_4, g)^{r_x} \cdot e(h_1, g)^{-r_{\delta_1}} \cdot e(h_1, \omega)^{-r_\alpha} \cdot e(h_2, g)^{-r_{\delta_2}} \cdot e(h_2, \omega)^{-r_\beta}, R_5 \leftarrow T_1^{r_x} \cdot g_1^{-r_{\delta_1}}, R_6 \leftarrow T_2^{r_x} \cdot g_2^{-r_{\delta_2}}, R_7 \leftarrow T_3^{r_x} \cdot g_3^{-r_{\delta_1}-r_{\delta_2}}$, 然后将 $(T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, R_6, R_7)$ 发送给 Bob. Bob 在 Z_p 中随机选择询问值 c 发送给 Alice. Alice 计算并发送回 $s_\alpha = r_\alpha + c\alpha, s_\beta = r_\beta + c\beta, s_x =$

$r_x + cx, s_{\delta_1} = r_{\delta_1} + c\delta_1, s_{\delta_2} = r_{\delta_2} + c\delta_2 \in Z_p$, 最后, Bob 验证以下 7 个等式:

$$g_1^{s_a} \stackrel{?}{=} T_1^c \cdot R_1 \quad (1)$$

$$g_2^{s_\beta} \stackrel{?}{=} T_2^c \cdot R_2 \quad (2)$$

$$g_3^{s_a + s_\beta} \stackrel{?}{=} T_3^c \cdot R_3 \quad (3)$$

$$e(T_4, g)^{s_x} \cdot e(h_1, g)^{-s_{\delta_1}} \cdot e(h_1, \omega)^{-s_a} \cdot e(h_2, g)^{-s_{\delta_2}} \cdot e(h_2, \omega)^{-s_\beta} \stackrel{?}{=} (e(g, g)/e(T_4, \omega))^c \cdot R_4 \quad (4)$$

$$T_1^{s_x} g_1^{-s_{\delta_1}} \stackrel{?}{=} R_5 \quad (5)$$

$$T_2^{s_x} g_2^{-s_{\delta_2}} \stackrel{?}{=} R_6 \quad (6)$$

$$T_3^{s_x} g_3^{-s_{\delta_1} - s_{\delta_2}} \stackrel{?}{=} R_7 \quad (7)$$

如果上述 7 个等式都成立, Bob 接受证明.

定理 1. 协议 1 是诚实验证者在判定线性假设下 SDH 对知识的零知识证明.

定理 1 的证明可以通过以下 3 个引理的证明得出.

引理 1. 协议 1 是完备的, 即验证者总是接受与一个诚实示证者的交互.

证明. 如果 Alice 是一个拥有 SDH 对 (A, x) 的诚实示证者, 并且遵守协议 1 中规定的指令, 那么式(1)~(7)必然成立.

首先, $g_1^{s_a} = g_1^{r_a + ca} = (g_1^a)^c \cdot g_1^{r_a} = T_1^c \cdot R_1$, 所以式(1)成立, 类似地, 有式(2), (3)成立; 然后, $T_1^{s_x} g_1^{-s_{\delta_1}} = (g_1^a)^{r_x + cx} g_1^{-r_{\delta_1} - cx\alpha} = (g_1^a)^{r_x} g_1^{-r_{\delta_1}} = R_5$, 类似地, 有式(6), (7)成立; 最后,

$$e(T_4, g)^{s_x} \cdot e(h_1, g)^{-s_{\delta_1}} \cdot e(h_1, \omega)^{-s_a} \cdot e(h_2, g)^{-s_{\delta_2}} \cdot e(h_2, \omega)^{-s_\beta} = e(T_4, g)^{r_x + cx} \cdot e(h_1, g)^{-r_{\delta_1} - cx\alpha} \cdot e(h_1, \omega)^{-r_a - c\alpha} \cdot$$

$$e(h_2, g)^{-r_{\delta_2} - cx\beta} \cdot e(h_2, \omega)^{-r_\beta - c\beta} = e(T_4, g^x)^c \cdot e(h_1^{-a} h_2^{-\beta}, \omega g^x) \cdot (e(T_4, g)^{r_x} \cdot$$

$$e(h_1, g)^{-r_{\delta_1}} \cdot e(h_1, \omega)^{-r_a} \cdot e(h_2, g)^{-r_{\delta_2}} \cdot e(h_2, \omega)^{-r_\beta}) = e(T_4 h_1^{-a} h_2^{-\beta}, \omega g^x)^c \cdot e(T_4, \omega)^{-c} \cdot (R_4)$$

$$= (e(A, \omega g^x)/e(T_4, \omega))^c \cdot R_4$$

$$= (e(g, g)/e(T_4, \omega))^c \cdot R_4.$$

所以式(4)成立. 因此, 对 Bob 随机选取询问值的所有情况, Alice 的应答都能满足他每一步的验证.

引理 2. 协议 1 的副本在判定线性假设下可以仿真.

证明. 首先描述一个输出协议 1 证明副本的仿真器, 选取 $A \xleftarrow{R} G$, $\alpha, \beta \xleftarrow{R} Z_p$, 令 $T_1 \leftarrow g_1^a$, $T_2 \leftarrow g_2^\beta$, $T_3 \leftarrow g_3^{a+\beta}$, $T_4 \leftarrow Ah_1^a h_2^\beta$. 假设判定线性假设在群 G 上成立, 由仿真器生成的四元组 (T_1, T_2, T_3, T_4) 的分布与任一示证者输出的分布是不可区

分的. 仿真器的剩余部分没有用到知识 A, x, α 或 β , 所以当 T_1, T_2, T_3, T_4 预先指定时仍可以使用. 当预先指定的 T_1, T_2, T_3, T_4 是某个 A 的随机线性 Cramer-Shoup 加密时, 证明副本的剩余部分可以被完美仿真.

随机选择询问值 $c \xleftarrow{R} Z_p, s_a \xleftarrow{R} Z_p$, 并令 $R_1 \leftarrow T_1^c / g_1^{s_a}$, 则式(1)成立. α 和 c 选定后, r_a 和 s_a 中选定其中一个, 则另一个也随之确定, 并且一个是均匀随机选择的, 则另一个也必将是均匀随机选择的, 因此 s_a 和 R_1 的分布与实际副本相同. s_β 和 R_2, R_3 的选择也是类似的. 选择 $s_x, s_{\delta_1}, s_{\delta_2} \xleftarrow{R} Z_p$, 并令 $R_5 \leftarrow T_1^{s_x} g_1^{-s_{\delta_1}}, R_6 \leftarrow T_2^{s_x} g_2^{-s_{\delta_2}}, R_7 \leftarrow T_3^{s_x} g_3^{-s_{\delta_1} - s_{\delta_2}}$, 所有被计算的值的分布依然与实际副本一样.

令 $R_4 \leftarrow e(T_4, g)^{s_x} \cdot e(h_1, g)^{-s_{\delta_1}} \cdot e(h_1, \omega)^{-s_a} \cdot e(h_2, g)^{-s_{\delta_2}} \cdot e(h_2, \omega)^{-s_\beta} \cdot e((g, g)/e(T_4, \omega))^{-c}$, 情况也是相同的. 这时仿真器输出的副本为 $(T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, R_6, R_7, c, s_a, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$, 与实际的协议副本相同.

引理 3. 存在一个协议 1 的提取器.

证明. 在协议的第一步, 示证者向验证者发送 $(T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, R_6, R_7)$. 对于不同的询问值 c 和 c' , 示证者的响应分别为 $(s_a, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$ 和 $(s'_a, s'_\beta, s'_x, s'_{\delta_1}, s'_{\delta_2})$, 它们均要满足式(1)~(7). 令 $\Delta c = c - c'$, $\Delta s_a = s_a - s'_a$, $\Delta s_\beta = s_\beta - s'_\beta$, $\Delta s_x = s_x - s'_x$ 和 $\Delta s_{\delta_1} = s_{\delta_1} - s'_{\delta_1}$ 的定义与前面相似. 将上述两组响应值集代入式(1)~(7), 得到上述等式的两个实例.

将等式(1)的两个实例等号两边分别相除, 得 $g_1^{\Delta s_a} = T_1^{\Delta c}$, 由于指数是素数阶群的元素, 对 $g_1^{\Delta s_a} = T_1^{\Delta c}$ 求根运算得 $g_1^{\tilde{a}} = T_1$, 其中 $\tilde{a} = \Delta s_a / \Delta c$. 类似地, 由等式(2)可得 $g_2^{\tilde{\beta}} = T_2$, $\tilde{\beta} = \Delta s_\beta / \Delta c$; 由等式(3)得 $g_3^{a+\tilde{\beta}} = T_3$. 将式(5)的两个实例等号两边分别相除, 得 $g_1^{\Delta s_x} = T_1^{\Delta s_{\delta_1}}$, 代入 $T_1 = g_1^{\tilde{a}}$ 得 $\Delta s_{\delta_1} = \tilde{a} \Delta s_x$. 同理, 由式(6)可得 $\Delta s_{\delta_2} = \tilde{\beta} \Delta s_x$. 最后, 将式(4)的两个实例相除得

$$\begin{aligned} & (e(g, g)/e(T_4, \omega))^{\Delta c} \\ &= e(T_4, g)^{\Delta s_x} \cdot e(h_1, g)^{-\Delta s_{\delta_1}} \cdot e(h_1, \omega)^{-\Delta s_a} \cdot e(h_2, g)^{-\Delta s_{\delta_2}} \cdot e(h_2, \omega)^{-\Delta s_\beta} \\ &= e(T_4, g)^{\Delta s_x} \cdot e(h_1, g)^{-\tilde{a} \Delta s_x} \cdot e(h_1, \omega)^{-\Delta s_a} \cdot e(h_2, g)^{-\tilde{\beta} \Delta s_x} \cdot e(h_2, \omega)^{-\Delta s_\beta}; \end{aligned}$$

令 $\tilde{x} = \Delta s_x / \Delta c$, 对上式两边去 Δc 得

$$\begin{aligned} & e(g, g)/e(T_4, \omega) \\ &= e(T_4, g)^{\tilde{x}} \cdot e(h_1, g)^{-\tilde{a} \tilde{x}} \cdot e(h_1, \omega)^{-\tilde{a}} \cdot e(h_2, g)^{-\tilde{\beta} \tilde{x}} \cdot e(h_2, \omega)^{-\tilde{\beta}} \cdot e(h_1, \omega)^{-\tilde{a}} \cdot e(h_2, \omega)^{-\tilde{\beta}} \end{aligned}$$

$$e(h_2, g)^{-\beta x} \cdot e(h_2, \omega)^{-\beta};$$

令 $\tilde{A} = T_4 h_1^{-a} h_2^{-\beta}$, 可得 $e(\tilde{A}, \omega g^x) = e(g, g)$.

因此提取器得到了 SDH 对 (\tilde{A}, \hat{x}) , 这个对与线性 Cramer-Shoup 加密 (T_1, T_2, T_3, T_4) 中的 SDH 对相同.

4 IND-CCA2 完全匿名的短群签名

设双线性群 G 的生成元为 g , SDH 假设在 (G, G) 上成立, 且线性假设在群 G 上成立, Hash 函数 $H: \{0, 1\}^* \rightarrow Z_p$, IND-CCA2 完全匿名的群签名方案由以下算法组成:

(1) 密钥生成算法 $KeyGen(n)$

算法中的输入参数 n 表示群成员的个数. 选择 $z_1, z_2, z_3 \xleftarrow{R} Z_p$, 令 $g_1, g_2, g_3 \in G$, 使 $h_1 \leftarrow g_1^{z_1} g_3^{z_3}$, $h_2 \leftarrow g_2^{z_2} g_3^{z_3}$, 并令 $\omega = g^\gamma$, 其中 $\gamma \xleftarrow{R} Z_p^*$, γ 仅有密钥分发者知道. 对 $1 \leq i \leq n$, 选择 $x_i \xleftarrow{R} Z_p^*$, 令 $A_i \leftarrow g^{1/(\gamma+x_i)}$, 得到关于用户 i 的 SDH 对 (A_i, x_i) . 群公钥 gpk 为 $(g, g_1, g_2, g_3, h_1, h_2, \omega)$. 用户 i 的私钥 $gsk[i]$ 为 (A_i, x_i) . 群管理员用于追踪签名的密钥 $gmsk$ 为 (z_1, z_2, z_3) .

(2) 签名算法 $Sign(gpk, gsk[i], M)$

该算法的参数为群公钥 gpk , 用户 i 的私钥 $gsk[i]$ 和待签消息 $M \in \{0, 1\}^*$. 用户 i 首先执行协议 1 第一轮中规定的计算, 得到 $T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, R_6, R_7$, 将上述值与消息 M 进行 Hash 运算后获得询问值 c , 即 $c \leftarrow H(T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, R_6, R_7, M)$, 然后执行第三轮规定的计算得到 $s_a, s_\beta, s_x, s_{\delta_1}, s_{\delta_2}$. 最后, 输出签名 $\sigma \leftarrow (T_1, T_2, T_3, T_4, c, s_a, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$.

(3) 验证算法 $Verify(gpk, M, \sigma)$

在此算法中, 给定群公钥 gpk 、消息 M 和群签名 σ , 验证该签名是否为知识 $(A_i, x_i, \alpha, \beta)$ 的有效签名. 验证者根据协议 1 中的式 (1) ~ (7) 重推 $R_1 \sim R_7$: $\tilde{R}_1 \leftarrow g_1^{s_a} / T_1^c$, $\tilde{R}_2 \leftarrow g_2^{s_\beta} / T_2^c$, $\tilde{R}_3 \leftarrow g_3^{s_a+s_\beta} / T_1^c$, $\tilde{R}_5 \leftarrow T_1^{s_x} / g_1^{s_{\delta_1}}$, $\tilde{R}_6 \leftarrow T_2^{s_x} / g_2^{s_{\delta_2}}$, $\tilde{R}_7 \leftarrow T_3^{s_x} / g_3^{s_{\delta_1}+s_{\delta_2}}$, $R_4 \leftarrow (T_4, g)^{s_x} \cdot e(h_1, g)^{-s_{\delta_1}} \cdot e(h_1, \omega)^{-s_a} \cdot e(h_2, g)^{-s_{\delta_2}} \cdot e(h_2, \omega)^{-s_\beta} \cdot (e(g, g) / e(T_4, \omega))^{-c}$, 然后计算 $c \stackrel{?}{=} H(T_1, T_2, T_3, T_4, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5, \tilde{R}_6, \tilde{R}_7, M)$, 如果等式成立则验证者接受.

(4) 签名打开算法 $Open(gpk, gmsk, M, \sigma)$

群管理员在签名打开算法中输入群公钥 $gpk =$

$(g, g_1, g_2, g_3, h_1, h_2, \omega)$ 、消息 M 、群签名 $\sigma = (T_1, T_2, T_3, T_4, c, s_a, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$ 和群管理员追踪密钥 $gmsk = (z_1, z_2, z_3)$, 执行该算法揭示此签名的签名者. 在验证 σ 是有效签名后, 对线性 Cramer-Shoup 加密 T_1, T_2, T_3, T_4 计算 $A \leftarrow T_4 / (T_1^{z_1} T_2^{z_2} T_3^{z_3})$. 群管理员根据用户列表查找 A 所对应的用户 A_i 即可确定签名者身份.

5 签名方案的安全性分析

群签名方案必须满足三个安全属性^[4]: (1) 正确性. 诚实签名者生成的签名能被正确验证和追踪; (2) 完全匿名性. 签名不会泄露它的签名者的身份; (3) 完全可追踪性. 所有的签名, 即使是用户与群管理员合谋生成的签名都要能被打开和追踪. 本文中的群签名的安全性可由以下 3 个定理的证明得出.

定理 2. 本文中的群签名是正确的.

证明. 对于群公钥 $gpk = (g, g_1, g_2, g_3, h_1, h_2, \omega)$ 和某一用户的私钥 $gsk[i] = (A_i, x_i)$, 密钥生成算法确保 $A_i^{x_i+\gamma} = g$, 所以 (A_i, x_i) 是一个 SDH 对. 本文的签名 σ 是第 3 节协议 1 的一个副本, 是关于知识 $(A_i, x_i, \alpha, \beta)$ 的知识证明, 签名验证等价于验证协议副本是正确的, 由引理 1 可知, σ 总是被验证者接受. 由诚实验证者产生的签名中, (T_1, T_2, T_3, T_4) 是 A_i 的线性 Cramer-Shoup 加密, 拥有密钥 (z_1, z_2, z_3) 的群管理员能够解密得出 A_i . 因此任何有效的签名总能被正确打开.

定理 3. 若敌手 A 以优势 ϵ 经 q_S 次签名提问和 q_H 次 Hash 提问攻破本文签名方案的 IND-CCA2 完全匿名性, 则可以构造敌手 B 以优势 $\epsilon/2 - (q_H + q_S)/p^4$ 攻破 DLDH 假设.

证明. 设算法 A 以 (t, q_S, q_H, ϵ) 攻破群签名方案的 IND-CCA2 完全匿名性, 我们构造一个算法 B 以至少 ϵ 的优势攻破线性 Cramer-Shoup 加密的 IND-CCA2 安全. 给算法 B 线性 Cramer-Shoup 加密的公钥 (g, g_1, g_2, g_3) , 由它根据群签名方案的密钥生成算法产生其余的群公钥, 然后算法 B 向算法 A 提供群公钥 $(g, g_1, g_2, g_3, h_1, h_2, \omega)$ 和用户私钥 (A_i, x_i) 以及群管理员密钥 (z_1, z_2, z_3) .

在任何时候算法 A 都可以提问随机预言机 H , 算法 B 以 Z_p 中均匀随机地选择的元素作为应答, 但要保证对相同提问的应答是相同的.

算法 B 要回答算法 A 的所有打开提问, 当算法 A 发出打开提问时, 算法 B 应用解密预言机检验签

名是否有效,然后 B 将签名的加密部分提交解密预言机,从明文中提取签名者身份发送给 A .

算法 A 提出两个群成员标识 i_0, i_1 以及消息 M , 发起用两个群成员标识 i_0, i_1 中的某一个对消息 M 的签名提问. 算法 B 选择随机比特 $b \xleftarrow{R} \{0, 1\}$, 用私钥 $gsk[i_b]$ 生成一个消息 M 的签名, 然后发送给算法 A . A 向打开预言机发起打开提问, 验证签名有效性, 有效性的证明可以通过协议 1 的仿真器模拟, 验证过程在获取随机预言机值时仅以一个可忽略的概率 $(q_H + q_S)/p^4$ 失败, 这时算法 B 中止. 否则说明 $(T_1, T_2, T_3, T_4, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$ 是消息 M 的一个有效签名, 并输出 b 的一个猜测比特 \hat{b} , 采用与文献[12]相同的分析方法, 我们可以得出算法 A 以 $\epsilon/2$ 的优势区分 SDH 对, 此时算法 B 攻破 DLDH, 即敌手 B 以优势 $\epsilon/2 - (q_H + q_S)/p^4$ 攻破 DLDH 假设.

定理 4. 若敌手 A 以优势 ϵ 经 q_S 次签名提问和 q_H 次 Hash 提问攻破本文签名方案的可追踪性, 则可以构造敌手 B 以优势 $(\epsilon - 1/p)^2/(16q_H)$ 解 $(n+1)$ -SDH 实例, 或敌手 B' 以优势 $(\epsilon/n - 1/p)^2/(16q_H)$ 解 n -SDH 实例.

证明. 首先构造一个与赢得完全可追踪性 game 的算法 A 交互的框架.

给定生成元为 g 的群 $G, \omega = g^r \in G$, 以及所有的 $(A_i, x_i), 1 \leq i \leq n$. 对每一个 i , 要么 $x_i = *$, 表示 A_i 所对应的 x_i 未知, 要么 (A_i, x_i) 是 SDH 对, 满足 $e(A_i, \omega g^{x_i}) = e(g, g)$. 选择 $z_1, z_2, z_3 \xleftarrow{R} Z_p^*$, 令 $g_1, g_2, g_3 \in G$, 使 $h_1 \leftarrow g_1^{z_1} g_3^{z_3}, h_2 \leftarrow g_2^{z_2} g_3^{z_3}$, 然后运行算法 A , 给它群公钥 $gpk = (g, g_1, g_2, g_3, h_1, h_2, \omega)$, 群管理员私钥 $gmsk = (z_1, z_2, z_3)$. 我们以如下方式回答它对预言机的提问.

当 A 询问 $(T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, R_6, R_7)$ 的 Hash 值时, 以群 G 中随机选取的元素应答, 要求对相同的提问应答是相同的.

当 A 以索引为 i 的密钥请求消息 M 的签名, 如果 $x_i \neq *$, 根据群签名算法生成密钥为 (A_i, x_i) 的关于消息 M 的签名 σ , 并将 σ 返回给 A . 如果 $x_i = *$, 选取 $\alpha, \beta \in Z_p$; 令 $T_1 \leftarrow g_1^\alpha, T_2 \leftarrow g_2^\beta, T_3 \leftarrow g_3^{\alpha+\beta}, T_4 \leftarrow A_i^* h_1^\alpha h_2^\beta$, 运行协议 1 的仿真器, 返回协议副本为 $(T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, R_6, R_7, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$, 由此副本得到群签名 $\sigma = (T_1, T_2, T_3, T_4, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$. 此外还要填充 Hash 预言机使 $(T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, R_6, R_7, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$ 处的 Hash 值为 c , 如果当前的副本 Hash 值不等于 c , 声明失败并中止.

当 A 询问索引为 i 的用户私钥时, 如果 $x_i \neq *$, 返回 (A_i, x_i) , 否则声明失败并中止. 最后, 如果 A 成功, 它输出一个伪造的消息 M 的群签名 $\sigma = (T_1, T_2, T_3, T_4, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$, 我们使用群管理员密钥 (z_1, z_2, z_3) 打开签名, 得到某个 A_i^* . 如果对所有 i 有 $A_i^* \neq A_i$, 输出 σ ; 否则, 如果对某个 i^* 有 $A_i^* = A_i$, 当 $x_{i^*} = *$, 输出 σ ; 如果 $x_{i^*} \neq *$, 声明失败并中止.

由框架的输出阶段可知, 存在两种类型的伪造算法. 第一类型的伪造者输出一个消息 M 的伪造签名 σ , 该签名被追踪到某个身份 $A^* \notin \{A_1, A_2, \dots, A_n\}$. 第二类型的伪造者输出一个可以被追踪到身份 A^* 的签名, 对于某个 i^* 有 $A^* = A_{i^*}$, 但伪造者并没有就 i^* 询问私钥预言机. 对于一个 $(t, q_H, q_S, n, \epsilon)$ 的第一类型伪造者, 根据 Boneh 和 Boyen 的方法^[10], 我们可由 $(n+1)$ -SDH 实例得到 (g, ω) 和 n 个 SDH 对 (A_i, x_i) , 将这些值应用到交互框架中, 只要 A 伪造成功, 框架就会宣布成功, 所以我们以概率 ϵ 得到第一类型的伪造. 对于一个 $(t, q_H, q_S, n, \epsilon)$ 的第二类型伪造者, 我们可由 n -SDH 实例得到 (g, ω) 和 $n-1$ 个 SDH 对, 这些对的索引分布在 $1 \sim n$ 之间, 对某个在索引 i^* 处空缺的对, 选取 $A_i^* \xleftarrow{R} G, x_i^* \leftarrow *$, $*$ 为占位符, 构成对 (A_i^*, x_i^*) 进行填充. 只有 A 从未就 i^* 提问过私钥预言机, 但却伪造出一个可以追踪到身份 A^* 的签名时, 交互框架才会宣布成功. 所以 A 至少以概率 ϵ/n 输出一个伪造的可以被追踪到用户 i^* 的群签名.

接下来我们用与 BBS 方案相同的方法, 对第一或第二类型的伪造者应用交互框架, 并提取出一个与 SDH 假设矛盾的 SDH 对 (\tilde{A}, \tilde{x}) . 仅当 (T_1, T_2, T_3, T_4) 中被加密的 \tilde{A} 不在那些 x_i 已知的 A_i 之列时, 框架宣布成功. 因此, 提取的 SDH 对 (\tilde{A}, \tilde{x}) 不在那些我们由 n -SDH 实例自己创建的对之内, 并可以被作为 q -SDH 问题的解.

综上所述, 我们可以使用第一类型伪造者以概率 $(\epsilon - 1/p)^2/(16q_H)$ 解 $(n+1)$ -SDH 实例, 或者使用第二类型伪造者以概率 $(\epsilon/n - 1/p)^2/(16q_H)$ 解 n -SDH 实例, 即以优势 $(\epsilon/n - 1/p)(4q_H)$ 攻破判定线性假设, 其中, 伪造类型的猜测概率为 $1/2$.

6 签名方案的性能分析

6.1 签名长度

本文的短群签名方案由 4 个群 G 中的元素和 6 个 Z_p 中的元素组成, 参照文献[10]中所描述的椭圆

曲线族,取 p 为 171bits 的素数,群 G 中的元素为 171bits,则本文群签名的长度为 1704bits.

6.2 计算开销

签名的计算开销主要体现在双线性对运算、指数和多指数运算,尤其以双线性对运算的开销最大,因此分析计算开销时,将指数和多指数运算都归为指数运算.由于双线性对 $e(g, g), e(h_1, g), e(h_1, \omega), e(h_2, g), e(h_2, \omega)$ 和 $e(A, g)$ 均可以预计算,且有 $e(T_4, g) = e(Ah_1^\alpha h_2^\beta, g) = e(A, g) \cdot e(h_1, g)^\alpha \cdot e(h_2, g)^\beta$,使得计算 $e(T_4, g)$ 时无需作双线性对运算,因此在签名生成过程中需要 11 次指数运算,0 次双线性对运算;在验证过程中,根据双线性群的运算性质

可以将 $e(T_4, g)^{s_x} \cdot e(T_4, \omega)$ 合并为 $e(T_4, \omega^f g^{s_x})$,因此需要 7 次指数运算以及 0 次双线性对运算.

6.3 与现有方案的性能比较

本小节将 BBS 短群签名和我们的方案中的具体性能指标在表 1 中分别列出,其中“ME”表示多指数运算,“BM”表示双线性运算.从该表格的各项数据比较中可以看出:本文的方案与 BBS 短群签名相比,长度增加 170bits,而计算开销上总共增加 4 次指数运算.虽然签名长度略有增加,但本文的签名长度依然是比较短的.更为重要的是,以很小的性能代价实现了短群签名更严格安全定义下的完全匿名性.

表 1 短群签名方案性能比较

签名方案	签名长度/bits	签名过程计算量	验证过程计算量	匿名性
文献[3]	1533	8ME+0BM	6ME+0BM	CPA full-anonymity
本文方案	1704	11ME+0BM	7ME+0BM	IND-CCA2 full-anonymity

7 结 论

本文基于 IND-CCA2 安全的线性 Cramer-Shoup 公钥加密方案,设计了一种 SDH 问题的零知识证明协议,并根据该协议提出了一种新的具有 IND-CCA2 完全匿名性的群签名,签名的长度为 1704bits,签名算法需要 11 次多指数运算,而验证算法需要 7 次多指数运算.与 BBS 方案相比,签名长度和计算开销增长很少,但却实现了更为严格的完全匿名性安全定义.

参 考 文 献

[1] Chaum D, Heyst E V. Group signatures//Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques. Brighton, UK, 1991: 257-265

[2] Ateniese G, Camenisch J, Joye M, Tsudik G. A practical and provably secure coalition-resistant group signature scheme//Proceedings of the 20th Annual International Cryptology Conference. California, USA, 2000: 255-270

[3] Boneh D, Boyen X, Shacham H. Short group signatures//Proceedings of the 24th Annual International Cryptology Conference. California, USA, 2004: 41-55

[4] Bellare M, Micciancio D, Warinschi B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumption//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Warsaw, Poland, 2003: 614-629

[5] Bellare M, Shi H, Zang C. Foundations of group signatures: The case of dynamic groups//Proceedings of the Cryptographers' Track at the RSA Conference 2005. California, USA, 2005: 136-153

[6] Boneh D, Shacham H. Group signatures with verifier-local revocation//Proceedings of the 11th ACM Conference on Computer and Communications Security. Washington DC, USA, 2004: 168-177

[7] Boyen X, Waters B. Compact group signatures without random oracles//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. St. Petersburg, Russia, 2006: 427-444

[8] Boyen X, Waters B. Full-domain subgroup hiding and constant-size group signatures//Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, 2007: 1-15

[9] Shacham H. A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive: Report 2007/074. <http://eprint.iacr.org/2007/074.pdf>

[10] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing//Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia, 2001: 514-532

[11] Nakanishi T, Funabiki N. Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps//Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security. Chennai, India, 2005: 533-548

[12] Delerablée C, Pointcheval D. Dynamic fully anonymous short group signatures//Proceedings of the 1st International Conference on Cryptology in Vietnam. Hanoi, Vietnam, 2006: 193-210



ZHANG Yue-Yu, born in 1978, Ph. D. candidate, lecturer. His current research interests include digital signature and electronic commerce security.

Her current research interests include design and analysis of block cipher.

SU Wan-Li, born in 1963, Ph. D. candidate, associate professor. His current research interests include network and information security.

WANG Yu-Min, born in 1936, professor and Ph. D. supervisor. His current research interests include information theory, coding, theory and application of cryptography.

CHEN Jie, born in 1979, Ph. D. candidate, lecturer.

Background

This research is supported by the National High Technology Research and Development Program (863 Program) of China (2007AA01Z435), the National Natural Science Foundation of China under grant No. 60473072, and the Natural Science Basic Research Plain in Shaanxi Province of China (2007F37).

This paper focuses on the field of full-anonymity of group signature. The research group has done much research work in the design of group signature scheme and other related work of electronic auction. Group signatures, introduced by Chaum and van Heyst, allow any member of a certain group to sign a message on behalf of the group, but the signer remains anonymous within the group. Since then, there have been several works on this subject. In 2000, based on a novel use of the DDH assumption combined with the Strong-RSA assumption, Ateniese, Camenisch, Joye and Tsudik present a scheme with constant signature size. This scheme has a resistance to attacks by coalitions of users. In CRYPTO 2004, the scheme of Boneh, Boyen and Shacham takes about 1533 bits for achieving an RSA-1024 security level. It is the shortest GS in the random oracle model. But only chosen plaintext attack (CPA) full-anonymity is achieved in this

short group signature. Bellare, Micciancio, and Warinschi (BMW) introduced a modern formalism for static groups. Their definition models a primitive of a relaxed group signature as it requires a key-issuing center to generate all keys in the system and distributes them to the group manager and group members. Since they use generic Non-Interactive Zero Knowledge techniques, their scheme is too inefficient to be useful in practice. Bellare, Shi and Zhang strengthened the security model to include dynamic enrollment of members. Recently, two schemes secure in the standard model are proposed by Boyen and Waters, but the anonymity of those schemes relies on the adversary not being able to see any opening of group signatures. The authors present a new zero-knowledge protocol for SDH, which based on Cramer-Shoup encryption from the linear assumption. Using this protocol as a building block, a new short group signature is constructed in this paper, which is provable secure in the Bellare-Micciancio-Warinschi model. The scheme is of IND-CCA2-full-anonymity, which allows adversary querying open oracle when trying to attack the anonymity notion. And the signature is only 1704 bits in size.