授权群签名

黄振杰[1,2], 郝艳华[1], 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, 陕西西安 710071; 2. 漳州师范学院计算机科学系, 福建漳州 363000)

摘 要: 现有的群签名方案都假设所有成员拥有相同的权限, 不适用于成员权限不同的情形, 该文提出授权群签名的概念, 并给出一个具体的授权群签名方案. 该文通过在一般群签名上增加一个负责授权的权限管理员和一个授权过程来达到授权群签名. 在所给出的授权群签名方案中, 签名人必须同时使用私钥和授权证书才能签名, 因此只能按所授的权限签名, 验证人则可通过权限公开证书对授权进行验证.

关键词: 数字签名; 群签名; 授权群签名; 匿名性
中图分类号: TN918, TP309 文献标识码: A 文章编号: 0372-2112 (2004) 05-0774-04

Authorized Group Signature

HUANG Zhen-jie[1,2], HAO Yan-hua[1], WANG Yu-min[1]
(1. *National Key Lab of Integrated Service Networks, Xidian University, Xi'an, Shaanxi 710071, China;*
2. *Department of Computer Science, Zhangzhou Teachers College, Fujian, Zhangzhou, Fujian 363000, China*)

Abstract: All the group signature schemes available are supposed that all members have the same right to sign and can not be used in the cases where different members have different rights. To cover this shortage, this paper introduces a concept of the authorized group signature and proposes an authorized group signature scheme to implement it. The authors add a new party, the right manager, and a new procedure, AUTHORIZE procedure to the standard group signatures to achieve the authorized group signatures. In the proposed authorized group signature scheme, the signer can sign a signature only when he knows both a secret key of one group member and a secret certificate so he can sign only in his own right authorized by the right manager, and the verifier can verify the signer's right by verifying the corresponding public certificate.

Key words: digital signature; group signature; authorized group signature; anonymity

1 引言

群签名(group signature)是一种具有可撤消匿名性的数字签名技术, 在群签名中, 群成员可代表群体进行匿名签名, 验证者只能验证签名是由群体中的成员签的, 而不能确知是哪个成员签的, 但必要时可由群管理员打开签名来揭露签名人的身份, 使得签名人不能否认是自己签的名. 群签名同时提供了匿名性和可跟踪性, 其匿名性可为合法用户提供匿名保护, 其可跟踪性又使得可信机构可以跟踪违法行为, 这是许多安全业务所要求的, 以电子现金为例, 一方面要求它和一般现金一样具有匿名性, 另一方面, 为防止利用电子现金进行洗钱等不法行为, 又要求它是可跟踪的, 群签名正好具有这两方面的性质. 可撤消匿名性使得群签名在管理、军事、政治及经济等多个方面有着广泛的应用前景, 因此引起许多研究者的注意[1~7].

群签名的一个典型应用例子是在公司的管理中隐藏公司内部管理层的结构, 如用群签名对交易合同或其他文件签名, 客户或其他验证者只能验证该文件是该公司签名认可的, 而不知道具体是谁签的, 因此不可能从签名中得知公司管理层的更详细情况, 而公司在必要时又可利用群签名的打开功能来揭露某文件签名人的身份, 做到既隐藏管理层结构又可追查责任. 一般来说, 公司管理层的各个成员常有不同的职责和不同的权限, 具有不同权限的经理们都只签署自己权限范围内的文件. 这种签名人权限不尽相同的情况不仅在电子商务中出现, 在电子政务中也常出现, 令人遗憾的是现有的群签名方案都不能适用这种情况, 因为现有的群签名方案都假设所有成员拥有相同的权限, 不能做到按权限签名, 为了克服现有群签名的这个不足, 让每个成员都按其权限签名, 防止越权签名, 本文提出授权群签名的概念, 与一般群签名相比授权群签名增加一个负责授权的权限管理员和一个授权过程, 签名人必须同时使用私钥和授权证书才能签名, 因此只能按所授的权限签名, 验证人则可通过权限公开证书对授权进行验证. 借鉴文[2]群签名方案的思想, 给出了一个授权群签名方案, 与文[2]的方案相比, 方案不仅增加了授权功能, 还将签名的长

收稿日期: 2003-05-22; 修回日期: 2003-12-19
基金项目: 国家自然科学基金(No. 19931010); 国家 973 项目(No. G1999035803)

度缩短了一半, 而签名的长度是群签名效率的一个重要指标[3].

2 预备知识

本节介绍将用到的一些预备知识, 包括变型 ElGamal 加密算法和知识签名.

2.1 变型 ElGamal 加密算法

设 G 是素数 q 阶有限循环群, g 是其生成元, 且使得计算以 g 为底的离散对数是不可行的. 除特别声明外, 本文的所有运算都在 G 中进行. 私钥 x 是在 Z_q 上随机选取的(记为 $x\in_R Z_q$, 下同), 对应的公钥 $z=g^x$, 用变型 ElGamal 加密算法[2]对消息 m 进行加、解密的算法如下:

加密: 随机选取 $r\in_R Z_q$, 密文 $(A, B)=(z^r, g^r m)$;

解密: $m=B/(A^{x^{-1}})=(g^r m)/(g^{rx^{-1}})$.

2.2 知识签名

知识签名可在完成签名的同时证明拥有某个知识, 这里只介绍本文将用到的几个知识签名, 它们都基于离散对数困难性问题.

参数 q, g 如 2.1, 私钥 x 是在 Z_q 上随机选取的, 对应的公钥 $y=g^x$, $H: \{0,1\}^* \to Z_q$ 是一个防碰撞单向 Hash 函数, 符号 $\|$ 表示两个数据串的级联.

定义 1[2]　满足 $c=H(g\|y\|g^s y^c\|m)$ 的数对 (c, s) 称为对消息 m 的以 g 为底 y 的离散对数知识签名, 记为 $SKDL(g, y, m)$.

$SKDL(g, y, m)$ 只有在知道 y 的离散对数 x 的情况下才能计算, 计算方法是: 先随机选取 $r\in_R Z_q$, 然后计算 $c=H(g\|y\|g^r\|m)$ 和 $s=r-cx \pmod q$.

定义 2[2]　满足 $\sum_{i=1}^{n} c_i=H(g\|h\|y_1\|z_1\|\cdots\|y_n\|z_n\|g^{s_1}y_1^{c_1}\|h^{s_1}z_1^{c_1}\|\cdots\|g^{s_n}y_n^{c_n}\|h^{s_n}z_n^{c_n}\|m)$ 的 $2n$ 元组 $(c_1, \cdots, c_n, s_1, \cdots, s_n)$ 称为对消息 m 的 n 对相等离散对数 $\log_g y_1, \log_h z_1; \cdots; \log_g y_n, \log_h z_n$ 之一的知识签名, 记为 $SEQDL\begin{bmatrix} n \\ 1 \end{bmatrix}(g, h, y_1, z_1, \cdots, y_n, z_n, m)$, 简称为 1-out-of-$n$ 相等知识签名.

$SEQDL\begin{bmatrix} n \\ 1 \end{bmatrix}(g, h, y_1, z_1, \cdots, y_n, z_n, m)$ 只有在知道这 n 对相等离散对数 $\log_g y_1, \log_h z_1; \cdots; \log_g y_n, \log_h z_n$ 之一的情况下才能计算, 计算方法是: 以知道 $x_1=\log_g y_1=\log_h z_1$ 为例, 先随机选取 $r, c_2, \cdots, c_n, s_2, \cdots, s_n\in_R Z_q$, 然后计算

$$c_1=H(g\|h\|y_1\|z_1\|\cdots\|y_n\|z_n\|g^r\|h^r\|g^{s_2}y_2^{c_2}\|h^{s_2}z_2^{c_2}\|\cdots\|g^{s_n}y_n^{c_n}\|h^{s_n}z_n^{c_n}\|m)-\sum_{i=2}^{n} c_i,$$

$$s_1=r-c_1x_1 \pmod q.$$

1-out-of-n 相等知识签名具有无条件匿名性, 即任何人正确猜出实际签名人的概率不超过 $1/n$.

2.3 1-out of n 相等知识签名的改进

上述的 1-out-of-n 相等知识签名是一个 $2n$ 元组, 这里我们给出一个改进方案, 它的签名是 $n+1$ 元组, 与原来的签名相比长度缩短了近一半.

定义 3　满足 $c_{i+1}=H(g\|h\|y_1\|z_1\|\cdots\|y_n\|z_n\|g^{s_i}y_i^{c_i}\|h^{s_i}z_i^{c_i}\|m)$, $i=1, 2, \cdots, n$, $c_{n+1}=c_1$ 的 $n+1$ 元组 $(c_1, s_1, \cdots, s_n)$ 称为对消息 m 的 n 对相等离散对数 $\log_g y_1, \log_h z_1; \cdots; \log_g y_n, \log_h z_n$ 之一的简化知识签名, 记为 $SEQDL\begin{bmatrix} n \\ 1 \end{bmatrix}_S(g, h, y_1, z_1, \cdots, y_n, z_n, m)$, 简称为简化 1-out-of-$n$ 相等知识签名.

上述简化 1-out-of-n 相等知识签名的计算方法为:

(1)随机选取 $r\in_R Z_q$, 并计算 $c_{k+1}=H(g\|h\|y_1\|z_1\|\cdots\|y_n\|z_n\|g^r\|h^r\|m)$.

(2)对 $i=k+1, \cdots, n, 1, \cdots, k-1$, 随机选取 $s_i\in_R Z_q$, 并计算

$$c_{i+1}=H(g\|h\|y_1\|z_1\|\cdots\|y_n\|z_n\|g^{s_i}y_i^{c_i}\|h^{s_i}z_i^{c_i}\|m).$$

(3)最后计算 $s_k=r-x_kc_k \pmod q$.

这里假设签名人知道 $x_k=\log_g y_k=\log_h z_k$.

定理 1　只有知道某个 $x_k=\log_g y_k=\log_h z_k$ 才能计算上述简化 1-out-of-n 相等知识签名.

证明　分两步证明:

(1)签名人得知道 $x_k=\log_g y_k$ 和 $x'_k=\log_h z_k$ 才能签名

虽然在简化 1-out-of-n 相等知识签名 $(c_1, s_1, \cdots, s_n)$ 中只有一个显式的 c_1, 其实还隐含有可从 $(c_1, s_1, \cdots, s_n)$ 计算出的 $(c_2, \cdots, c_n)$, 这些 c_i 根据签名算法所定义的关系首尾相连构成一个圈, 要使 $(c_1, c_2, \cdots, c_n)$ 构成一个圈, $(s_1, \cdots, s_n)$ 中就至少得有一个不能是任选的, 设为 s_k, 它的选择必须使得

$$c_{k+1}=H(g\|h\|y_1\|z_1\|\cdots\|y_n\|z_n\|g^{s_k}y_k^{c_k}\|h^{s_k}z_k^{c_k}\|m),$$

如果我们将上式简记为

$$c_{k+1}=H(^*\|g^{s_k}y_k^{c_k}\|^*) \text{ 或 } c_{k+1}=H(^*\|h^{s_k}z_k^{c_k}\|m),$$

那么就可以发现, 和 Schnorr 签名相类似的, 要求得这样的 s_k, 签名人得知道 $x_k=\log_g y_k$ 和 $x'_k=\log_h z_k$, 否则将面临与伪造 Schnorr 签名相同的困难问题. Schnorr 签名中两个 c 是相等的, 这里虽然两个 c 不相等, 但 c_k 是由 c_{k+1} 通过 Hash 函数确定的, Hash 函数的防碰撞性保证在安全性上这与 Schnorr 签名是一样的.

(2) $x_k=x'_k$

设

$$c_{k+1}=H(g\|h\|y_1\|z_1\|\cdots\|y_n\|z_n\|g^r\|h'\|m),$$

则有　$r=s_k+c_kx_k$, $r'=s_k+c_kx'_k \pmod q$.

如果 $x_k\neq x'_k$, 消去 s_k 得

$$c_k=\frac{r-r'}{x_k-x'_k} \pmod q.$$

因为 H 是防碰撞的, 所以签名人要求得这样的 r, r' 或 g^r, h' 使得由它们确定的 c_{k+1} 经过多次 Hash 后能得到 $c_k=\frac{r-r'}{x_k-x'_k}$ 是不可能的.

定理 2　上述简化 1-out-of-n 相等知识签名是无条件匿名和无关联的.

证明　由算法可知 $s_1, s_2, \cdots, s_{k-1}, s_{k+1}, \cdots, s_n$ 都是随机选取的, 由于 r 是随机的, 所以 s_k 也是随机的, 从而 $(s_1, s_2, \cdots, s_n)$ 是随机均匀分布的, 与签名算法从哪点开始无关, 即与

k 无关; c_1 是由 $s_1, s_2, \cdots, s_n$ 决定的, 也与 k 无关, 因此签名是无条件匿名的. 同样地, $c_1, s_1, s_2, \cdots, s_n$ 的随机性保证了签名的无关联性.

3 授权群签名的概念

本节先提出授权群签名的概念, 讨论其组成和安全性要求, 然后给出一个授权群签名方案, 并对其安全性进行分析.

3.1 授权群签名

授权群签名是一种群成员只能按授权代表群体进行签名的群签名, 验证者能验证签名是由获得相应授权证书的群成员签的, 但不能确知是哪个成员签的, 同样地, 必要时群管理员也可打开签名以揭露签名人的身份.

与标准群签名相比, 授权群签名增加了一个权限管理员, 他负责公布权限公开证书, 并把相应的授权证书颁发给指定的群成员, 这由一个新增加的授权过程来完成. 由于授权群签名增加了授权功能, 与标准群签名相对应的几个过程也得作一定的修改, 下面是授权群签名方案的一般组成:

SETUP 建立系统参数, 并产生群管理员、权限管理员和各个群成员的私钥/公钥对 (x_M, y_M), (x_A, y_A) 和 (x_1, y_1), (x_2, y_2), $\cdots$, (x_n, y_n).

AUTHORIZE 这是授权过程, 输入权限描述 W_i 和权限管理员的私钥/公钥对 (x_A, y_A), 输出权限的公开证书 $\tilde{y}_i$ 和授权证书 a_i, 公布公开证书 $\tilde{y}_i$, 秘密传递授权证书 a_i 给被授权的群成员.

SIGN 这是群签名算法, 输入待签消息 m 及所需的权限描述 W_i, 群成员的公钥 $y_1, y_2, \cdots, y_n$, 签名人 s 的私钥 x_s 以及 W_i 所对应的授权证书 a_i, 输出群签名 σ.

VERIFY 这是群签名的验证算法, 输入被签消息 m, 所需的权限描述 W_i 以及 W_i 所对应的公开证书 $\tilde{y}_i$, 群成员的公钥 $y_1, y_2, \cdots, y_n$, 权限管理员的公钥 y_A 和群签名 σ, 输出验证结果"真"或"假".

OPEN 这是群签名的跟踪算法, 输入群签名 σ 和管理员私钥 x_M, 输出签名人的身份 s.

与标准群签名一样, 也可在 **SETUP** 中细分出一个称为 **JOIN** 的过程.

授权群签名应具有如下性质, 其不可伪造性要比标准群签名的强些, 无关联性则弱些:

(1) 不可伪造性(**unforgeability**) 在不知道群成员私钥或没有得到所需授权的条件下, 任何攻击者都不可能成功伪造一个有效的授权群签名.

(2) 匿名性(**anonymity**) 除群管理员之外, 任何人要确定一个给定群签名的实际签名人在计算上是不可行的.

(3) 可跟踪性(**traceability**) 必要时群管理员可以打开一个签名以确定签名人的身份, 而且签名人不能阻止有效签名的打开.

(4) 无关联性(**unlinkability**) 在不打开签名的情况下, 确定两个不同的群签名是否为同一个签名人所签是不可能的, 但两个签名是否为具有同一权限的签名人所签是可知的.

(5) 防陷害性(**exculpability**) 包括群管理员在内的任何人都不能以其他群成员的名义产生有效的群签名.

(6) 抗联合攻击(**coalition-resistance**) 即使一些群成员串通在一起也不能产生一个有效的不能被跟踪的群签名.

注: 如果某权限只授予一个成员, 那么用该权限所签的多个签名就不是无关联的了, 但签名仍是匿名的; 如果同一成员可授予多个不同的权限, 那么不同权限的签名也不能排除是同一成员所签.

3.2 授权群签名方案

这里提出一个授权群签名方案, 其主要思想是: 在签名之前权限管理员先向群成员授权, 签名时签名人先用群公钥加密自己的公钥和权限公开证书, 然后用 1-out-of-n 相等知识签名证明加密的是某个成员的公钥和特定的权限公开证书, 用离散对数知识签名证明签名人的确知道被加密公钥所对应的私钥和该权限公开证书所对应的授权证书. 具体方案如下:

SETUP 参数 q, g 和 Hash 函数 H 的选择如 2.2. 群管理员、权限管理员和各群成员各自随机选取自己的私钥 x_M, x_A 和 $x_1, x_2, \cdots, x_n$, 计算并公布对应的公钥 y_M, y_A 和 $y_1, y_2, \cdots, y_n$, 这里 $y_* = g^{x_*}$.

AUTHORIZE 设所欲授予的权限描述为 W_i, 权限管理员随机选取 $r_i \in_R Z_q^*$, 计算 $b_i = g^{r_i}$, $\tilde{x}_i = x_A H(W_i \| b_i) + r_i \pmod q$, 公布 $(W_i, b_i, \tilde{y}_i)$, 其中 $\tilde{y}_i = y_A^{H(W_i \| b_i)} b_i$ 为权限 W_i 的公开证书, 并用群成员的公钥加密或通过安全信道将授权证书 $(W_i, b_i, \tilde{y}_i, \tilde{x}_i)$ 秘密传递给所有授予权限 W_i 的群成员, 群成员通过验证 $\tilde{y}_i = g^{\tilde{x}_i} = y_A^{H(W_i \| b_i)} b_i$ 确认该证书.

SIGN 设待签消息为 m, 对其签名需权限 W_i, 签名人为 j, 签名步骤如下:

(a) 用变型 ElGamal 加密算法加密 $\tilde{y}_i y_j$ 得 $(A, B) = (y_M^r, g^r \tilde{y}_i y_j)$, 其中 $r \in_R Z_q$.

(b) 计算简化 1-out-of-n 相等知识签名

$$(c_1, s_1, \cdots, s_n) = SEQDL\begin{bmatrix} n \\ 1 \end{bmatrix}_S (y_M, g, A, \frac{B}{y_1 \tilde{y}_i}, \cdots, A, \frac{B}{y_n \tilde{y}_i}, m \| w_i).$$

(c) 计算离散对数知识签名 $(\bar{c}, \bar{s}) = SKDL(g, B, m \| W_i)$, 先随机选取 $\bar{r} \in_R Z_q$, 然后计算

$$\bar{c} = H(g \| B \| g^{\bar{r}} \| m \| W_i), \quad \bar{s} = \bar{r} - \bar{c}(r + x_j + \tilde{x}_i) \pmod q.$$

授权群签名为 $(A, B, c_1, s_1, \cdots, s_n, \bar{c}, \bar{s})$.

VERIFY 验证 $\tilde{y}_i = y_A^{H(W_i \| b_i)} b_i$, 并验证简化 1-out-of-$n$ 相等知识签名 $(c_1, s_1, \cdots, s_n)$ 和离散对数知识签名 $(\bar{c}, \bar{s})$.

OPEN 群管理员从 (A, B) 解密出实际签名人的公钥 $y_j = \frac{B}{A^{x_M} \tilde{y}_i} = \frac{g^r y_j \tilde{y}_i}{g^{x_M r} \tilde{y}_i}$, 由公钥确定其身份.

几点讨论 (1)如果权限管理员的公钥 y_A 进行过身份注册, 那么在签名验证过程中可以确知是经谁授权的, 这样的授权群签名方案是明授权人授权群签名方案; 如果权限管理员的公钥 y_A 不是授权人注册过的公钥, 而是另外选取的一对私钥/公钥对的公钥, 那么验证人不可能从签名中得到授权人的身份信息, 这样的授权群签名方案是隐授权人授权群签名方案; (2)和代理签名一样, 这里我们假设群成员不会把其所获

得的授权证书再转授他人. 另外, 授权群签名是可跟踪的, 群管理员与权限管理员合作可以确定某个签名是否由有效授权的成员所签. (3) 签名的长度是群签名效率的一个重要指标[3], 本方案的签名是一个 $n+5$ 元组, 与文[2]中的 $2n+4$ 元组相比, 我们的方案将签名长度缩短了近一半.

3.3 安全性分析

不可伪造性　方案中相等知识签名 $SEQDL\left[\begin{matrix}n\\1\end{matrix}\right]_S(y_M, g, A, \frac{B}{\tilde{y}_1}, \cdots, A, \frac{B}{\tilde{y}_n}, m \| W_i)$ 保证 (A, B) 是对某个群成员的公钥 y_j 与权限 W_i 的公开证书 $\tilde{y}_i$ 之积进行加密而来的, 知识签名 $SKDL(g, B, m \| W_i)$ 保证签名人的确知道 (A, B) 中被加密的公钥所对应的私钥 x_j 和权限 W_i 所对应的授权证书 $\tilde{x}_i$, 也就是说, 要计算一个有效的授权签名, 签名人需同时拥有一个群成员的私钥和消息所要求的授权证书, 否则将得求 $g^{\tilde{r}}B^{-\tilde{c}}$ 关于 g 的离散对数, 即伪造签名的难度等价于解离散对数的困难性, 方案中参数的选择保证求离散对数是不可行的, 因此签名是不可伪造的; 匿名性和无关联性　变型 ElGamal 加密算法、简化 1-out-of-n 相等知识签名和离散对数知识签名都是概率算法, 其随机性和定理 2 一起保证了本方案的匿名性和无关联性; 可跟踪性　这由打开功能保证; 防陷害性　上面的分析同样可知, 在不知道签名所包含公钥的相应私钥的情况下要完成签名需求关于 g 的离散对数, 而签名所包含公钥又是可跟踪的, 因此陷害是不可行的; 抗联合攻击　如上分析, 方案中的相等知识签名 $SEQDL\left[\begin{matrix}n\\1\end{matrix}\right]_S$ 保证 B 中恰好加密了一个成员的公钥, 而打开功能又能解密出签名所包含的公钥, 因此任何有效签名都是可跟踪的.

4 结论

群签名因其具有可撤消匿名性而在许多领域有潜在的应用, 但已有的群签名方案都不能做到按所授权限签名, 为满足实际应用中成员按所授权限签名的需要, 本文提出了授权群签名的概念, 并给出了一个具体的授权群签名方案.

参考文献:

[1] Chaum D, et al. Group signatures [A]. Advances in Cryptology —— Eurocrypt' 91 [C]. Berlin: Springer-Verlag, 1992. 257- 265.

[2] Camenisch J. Efficient and generalized group signatures [A]. Advances in Cryptology —— Eurocrypt' 97 [C]. Berlin: Springer-verlag, 1997. 465- 479.

[3] Camenish J, et al. A group signature scheme with improved efficiency [A]. Advances in Cryptology ——Asiacrypt' 98 [C]. Berlin: Springer-verlag, 2000. 160- 174.

[4] Ateniese G, et al. Some open issues and new directions in group signatures [A]. Financial Cryptography-FC' 99 [C]. Berlin: Springer-verlag, 1999. 196- 211.

[5] Bresson E, et al. Efficient revocation in group signature [A]. Public Key Cryptography —PKC2001 [C]. LNCS 1992, Berlin: Springer-Verlag, 2001. 190- 206.

[6] Xia S, et al. A group signature scheme with strong separability [J]. Journal of Systems and Software, 2002, 60(3): 177- 182.

[7] Li Z, et al. Security of tseng-Jan's group signature schemes [J]. Information Processing Letters, 2000, 75(5): 187- 189.

作者简介:

黄振杰　男, 1964 年 11 月生于福建龙海市, 现为西安电子科技大学博士研究生, 漳州师范学院副教授, 主要研究兴趣是电子商务安全和网络安全.

郝艳华　女, 1976 年 4 月生于河南新乡市, 现为西安电子科技大学博士研究生, 主要研究兴趣是(超)椭圆曲线密码体制与电子商务安全.