基于环签名思想的一种类群签名方案

王继林[1,2], 张键红[2], 王育民[2]
(1. 浙江财经学院信息学院, 浙江杭州 310012; 2. 西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071)

摘 要: 群签名方案存在着管理员权利过大的缺点, 而环签名方案又无法追踪签名人的身份, 本文利用环签名的思想提出的一个新的类似群签名的匿名签名方案解决了这一矛盾. 和已有的群签名方案相比, 该方案因保留了环签名的部分特性而具有如下优点: (1) 管理员的权限得到了限制, 他必须和签名接收方合作才能共同追踪签名者的身份; (2) 签名者可以灵活地、主动地选择匿名范围, 即他可以任意选取 d 个合法的公钥说明自己在其中; (3) 用户加入和撤销特别方便, 管理员仅需在公告牌上公布和删除该成员的相关数据.

关键词: 群签名; 离散对数; 环签名
中图分类号: TB11 文献标识码: A 文章编号: 0372-2112 (2004) 03-0408-03

A Group Signature Scheme Based on Ring Signature Idea

WANG Ji-lin[1,2], ZHANG Jian-hong[2], WANG Yu-min[2]
(1. Zhejiang University of Finance and Economics, Zhejiang, Hangzhou 310012, China;
2. National Key Lab of ISN, Xidian University, Xi. an, Shaanxi 710071, China)

Abstract: Traditional group signatures have the demerit that the group manager has the absolute power in revoking the signer. s identity. The unconditional anonymity of ring signature provides chances for the criminals. We give a new group signature scheme based on the idea of ring signature. Compared with the old ones, this scheme has the following advantages: (1) The right of the group manager is restricted, he can only revoke the identity of the signer with the receiver s co-operation. (2) The signer can choose the public keys he wants to realize his anonymous scope. (3) Easy for users to join and leave, it only needs the group manager to add or delete the public key of the corresponding user.

Key words: group signature; discrete logarithm; ring signature

1 引言

群签名是一种重要的匿名签名技术[1], 但这种匿名性是可控制的, 当发生争执时, 群管理员可以揭露签名者的真实身份. 在实际的应用中, 用户希望能够对群管理员的这种特权给以必要的约束, 以防止其滥用职权.

环签名是一种新的匿名签名技术, 因签名中参数 c_i ($i = 1, 2, \cdots, n$) 根据一定的规则首尾相接组成环状而得名. Rivest 等人首先明确提出了这一概念[2] 并在最近引起了人们的重视[3~5]. 环签名不同于群签名, 环签名可以实现无条件匿名, 即无法追踪签名人的身份, 而群签名中群管理员的陷门信息可揭露具体签名者的身份. 环签名的这种无条件匿名性一方面在对信息需要长期保护的一些特殊环境中非常有用, 例如, 即使 RSA 被攻破也须保护匿名的场合.

我们利用环签名的思想提出了一种新的类似群签名的匿名签名方案. 方案一方面说明了可以通过适当的办法把环签名改造成可控制的匿名签名, 另一方面, 这种改造后的匿名签名仍保留着环签名的部分特征, 这些特性主要表现在如下三个方面: (1) 管理员的权限得到了控制, 他必须与签名接收方合作才能共同找出具体签名者, 这一点是群签名的可控匿名性和环签名的无条件匿名性的折衷; (2) 签名者可以灵活地、主动地选择匿名范围, 即他可以任意选取 d 个合法的公钥说明自己在其中, 这是环签名的一个显著特点; (3) 用户加入和撤出特别方便, 管理员只需添加和删除用户的在公告牌上的数据即可完成, 不涉及别的任何参数的改动. 和群签名方案相比, 新的类群签名方案的这些环签名的特征, 使得它在防止群管理员作弊、方便用户加入和撤出和便于签名者选定匿名范围方面具有一定的优势.

2 环签名的研究进展

2.1 环签名及其安全性

我们假定有 n 个用户, 每一个用户 B_i 拥有一个公钥 y_i 和与之对应的私钥 x_i. 环签名是一个能实现签名者无条件匿名的签名方案, 它由下述算法组成:

收稿日期: 2002-10-22; 修回日期: 2003-11-26
基金项目: 国家自然科学基金资助课题(No. 69931010)

签名 Sign(#). 一个概率算法在输入消息 m 和 n 个环成员的公钥 $L=\{y_1, y_2, , , y_n\}$ 以及其中的一个成员的私钥 x_s 后, 对消息 m 产生一个签名 $R=(m, L, c_1, s, , , s_n\}$, 其中 $c_i(i=1, 2, , , n)$ 根据一定的规则首尾相接呈环状.

验证 Verify(#). 一个确定性算法, 在输入(m, R)后, 若 R 为 m 的环签名输出/ True0, 否则为/ False0.

一个环签名必须满足无条件匿名性和不可伪造性等安全性要求.

无条件匿名性: 攻击者即便非法获取了所有可能的签名者的私钥, 他能确定出真正的签名者的概率不超过 1/ n, 这里 n 为环成员(可能的签名者)的个数.

不可伪造性: 外部攻击者在不知道任何成员的私钥的情况下, 即使能够从一个产生环签名的随机预言模型那得到任何消息 m 的签名, 他也不能成功伪造一个合法签名.

环签名的一个显著特征是签名者的无条件匿名性. 环签名还有另外一个显著特征, 即签名者可以在上述 n 个用户中自由地任意选取 d> 1 个用户(包括自己)产生一个环签名, 也就是说, 签名者可以指定自己的匿名范围, 并且被指定的用户可能不知道自己被包含在其中.

2l2　环签名的研究进展

无条件匿名签名和(t, n)门限签名的思想几乎是和群签名同时出现的, 但把所有可能的签名者的某种信息按一定规则链成环状以达到隐匿具体签名人的想法, 直到最近才由 Rivest 等人正式明确提出并引起人们的重视. Rivest 等人[2]利用对称加密技术和组合函数给出了一个基于 RSA 的高效的环签名方案, 并证明了这个方案在理想的对称加密算法 E(即 E 在任何密钥 k 下都是 $\{0, 1\}^l$ 上的一个随机置换)下满足环签名所要求的安全性.

M Abe, M Ohkuboh 和 K Suzuki 在文[4]中给出了一个简单高效的环签名模型, 这个模型适用于用户持有不同类型的公钥的情况(如有的持有 RSA 型公钥, 有的持有离散对数型公钥), 该模型在随机预言模型下满足环签名的安全性要求.

Fangguo Zhang 和 Kwangjo Kim[5]利用椭圆曲线中的双线性对给出了一个基于身份的环签名方案. 该方案被证明满足前述的安全性要求.

Emmanuel Bresson 等[3]对文[2]中的方案进行了改进, 仅利用 Hash 函数实现了环签名方案, 他们还利用这个基于 RSA 的环签名方案给出了一个基于 RSA 的(t, n)门限环签名方案. 该方案的思想无法适用于基于离散对数的环签名方案的门限推广. 基于离散对数的门限环签名方案和高效的适合任意接入结构的环签名方案还有待于深入研究.

3　基于环签名思想的类群签名方案

我们通过在签名者和接收者之间建立一个匿名连接, 由管理员和接收者分别产生一个秘密参数 t 和 r, 再经由该匿名连接传送给签名者等方式实现了我们的方案. 匿名连接的建立可采用洋葱路由或 Mixnets 等技术, 它是所有匿名应用得以实现的基础平台.

考虑一个基于离散对数的密码系统, 设 p, q 为大素数, 3 g4 为一个生成元为 g 的 Z_p^* 的 q 阶子群, 第 i 个用户 B_i 的私钥为 x_i, 对应的公钥匙 $y_i=g^{x_i}$ modp, Public 为一个发布公钥的公告牌, 所有的用户及其对应的公钥都在其上发布. H: $\{0, 1\}^*$ y Z_q 是一个可公开获得的 hash 函数.

设管理员 GM 管理上述的密码系统和公告牌 Public, 管理员 GM 的私钥为 x_{GM}, 对应的公钥为 y_{GM}. 签名接收者 V 的私钥为 x_V, 对应的的公钥为 y_V. 我们用 $\{x\}_{y_i}$ 表示对消息 x 用 y_i 进行公钥加密, 用 $\{x\}_{x_i}$ 表示对消息 x 用 x_i 进行签名, $E_k(\#)$ 表示用密钥 k 进行某种对称加密(如 DES), Encode(x, L)= $e_x=[\{x\}_{y_1}, \{x\}_{y_2}, , , \{x\}_{y_d}]$, Decode($e_x$, x_k, L)= x= $\{e_x[i]\}x_k$.

用户向管理员注册

用户 B_i 选择并记住一个 t_i, 计算 $p_i=g^{t_i}$ modp, 向 GM 提交(y_i, p_i), 并向 GM 证明他知道对应的 x_i 和 t_i. 当 GM 接收证明后, 它在公告牌上发布用户的身份和对应的(y_i, p_i). GM 在其公告版上发布的有关参数有:

p, q, g, 成员 B_i 及对应的(y_i, p_i);

一个对称加密方案 $E_k(\#)$;

一个可公开获得的 hash 函数 H: $\{0, 1\}^*$ y Z_q.

成员用户的撤消过程

如果需要撤消某个成员用户, 管理员只需在公告牌上删除该用户的数据即可.

成员用户 B_k 的签名过程

签名者 B_k 希望给接收者 V 发送一个签名, 他首先在 GM 发布的公钥中任选一些公钥(包括他自己), 构成本次匿名签名的匿名群 L, 为了方便叙述, 不妨假定 $L=\{y_1, y_2, , , y_d\}$, 然后分别从 GM 与 V 那里匿名获取参数 t 和 r, 最后执行签名 Sign(S_k, p_k, r, t).

参数 t 和 r 按如下方式获得:

B_k 与 V 建立匿名连接, 按照对称加密方案 $E_k(\#)$ 对密钥的要求任选一个 h, 把 $\{h, L\}_{y_V}$ 送给 V. V 解密出 h 和 L 后, 把 $\{h, L\}_{y_{GM}}$ 送给 GM. GM 解密 h 和 L, 为本次签名随机产生一个 $t\ I\ Z_q^*$ 在数据库中记录(h, t), 把 $E_h[\{Encode(t, L)\}_{x_{GM}}, \{p_1^t, p_2^t, , , p_d^t\}_{x_{GM}}]$ 送给 V. V 为本次签名随机产生一个 $r\ I\ Z_q^*$ 在自己的秘密数据库中记录(h, r), 把 $E_h[\{Encode(t, L)\}_{x_V}, \{Encode(t, L)\}_{x_{GM}}]$ 送给 B_k. B_k 分别用 Decode(e_r, x_k, L) 和 Decode(e_t, x_k, L) 解密出 t 和 r, 并经过检查 $e_r \stackrel{?}{=}$ Encode(Decode(e_r, x_k, L), L) 和 $e_t \stackrel{?}{=}$ Encode(Decode(e_t, x_k, L), L) 验证解密是否正确.

签名过程 Sign(B_k, p_k, r, t) 如下:

Sign(B_k, p_k, r, t)

(1) A a^R Z_q, $c_{k+1}=H(m, g^A k \text{mod} p)$,

(2) for i= k+ 1, , , d, 1, , , k- 1

do s_i a^R Z_q, and c_{i+1} a H(m, $g^{s_i}(p_k^{tr}y_i)^{c_i}$ mod p),

(3) s_k a A- ($t_k$tr+ x_k) c_k mod q,

(4) returnR= (h, m, L, p_k^{tr}, c_1, s_1, s_2, , , s_d)

接收方验证过程

接收方通过下面的Verify(R)算法, 计算 C_j 是否构成一个环状结构决定签名是否合法.

(1) p_k^{tr} 检查: 对 GM 给的 $E_h[\{Encode(t, L)\}_{x_{GM}}, \{p_1^t, p_2^t, \cdots, p_d^t\}_{x_{GM}}]$, 找出$\{p_1^t, p_2^t, \cdots, p_d^t\}$, 计算其中每一项的 r 次幂, 检查 p_k^{tr} 是否在其中, 如在, 则执行 2, 否则/ Reject0;

(2)环检查: for i = 1, 2, , , d, c_{i+1} a H (m, $g^{s_i}(p_k^{tr}y_i)^{c_i}$ modp),

If $c_{d+1} = c_1$ then return / Accept0

else return / Reject0

管理员与签名接收者合作恢复用户身份的过程:

签名接收者 V 根据h 提供r, 管理者 GM 根据 h 提供t, 然后可以通过计算 L 中每个用户 B_i 对应的 p_i 的tr 次幂, 找出对应 p_k^{tr} 的 p_k, 从而可有 GM 确定签名人的身份.

4 安全性分析和计算量

定理 1 在无法建立 p_k^{tr} 和 p_k 对应的情况下, 上述签名方案满足无条件匿名性.

证明 方案中除了签名者 B_k 的 s_k 外, 其余的 s_i 都是在 Z_q 上随机选取的. 由于 A是在 Z_q 上均匀选取的, s_k 在 Z_q 上的分布是均匀的. 对于固定的 m 和 p_k^{tr}, (s_1, s_2, , , s_d) 有 q^d 种等可能的取值, 而 c_1 完全由 m 和(s_1, s_2, , , s_d) 唯一确定. 因此, 从(c_1, s_1, s_2, , , s_d)本身判断出具体为哪个签名者的签名是不可能的. 在无法建立 p_k^{tr} 和 p_k 对应的情况下, 由于签名结构呈环状, 即便所有人的私钥泄露也无法确定具体签名者. 因而上述方案满足无条件匿名性.

定理 2 p_k^{tr} 和 p_k 对应关系的建立, 只有靠管理员 GM 和签名接收者 V合作才能实现.

证明 由于 t 和r 的随机性, 很显然, 在不知道 t 和 r 的情况下, 直接通过 p_k^{tr} 找到对应的 p_k 不可能的, 因为这必须求解离散对数问题. 在寻找 p_k^{tr} 对应的 p_k 上, 管理员和签名接收者因每人掌握一个秘密比其它人更具有优势, 我们只需证明上述二者任何一方无法单独建立起 p_k^{tr} 和 p_k 的对应.

管理员GM 能够利用自己的 t 计算出L 中所有 y_i 的 p_i^t, 但在不知 r 的情况下, 要通过 p_k^{tr} 找到对应的 p_k^t 也必须求解离散对数问题, 签名接收者的情况与之类似.

综合定理 1 和定理 2 我们得出, 在管理员和签名接收者不勾结的情况下, 上述签名方案能够实现签名者匿名. 管理员无法单独找出具体签名者, 因而本方案对管理员的权限进行了有效限制.

定理 3 在管理员不与伪造者串通的情况下, 上述签名方案满足群签名的不可伪造性.

证明 一个攻击者要伪造上述签名, 他必须要获取 t 和 r, 但 V 和GM 传送的 t 和r 只有L 中成员才能解密, 所以我们只要证明 L 中的一个成员不能冒充别的成员签名即可.

L 中的内部攻击者 B_i 要伪造 B_k 的签名, 他必须使用 B_k 对应的 p_k 来构成签名, 为使签名中的 c_i 按照规则呈环状结构, 他最终需要知道 p_k 对应的 t_k, 但在管理员不与伪造者串通的情况下, 这也是不可能的.

定理 4 上述签名方案能够抵御一致性攻击.

证明 这个结论是显然的, 因为签名者每次签名用的 t 和r 都不相同, 而 t 和r 又是随机选取的, 故不能判定两个签名是否为同一个人的.

我们的方案中, 在 t 和r 决定后, 签名和验证主要花费在 d 个 c_i 的计算上, 而每个 c_i 的计算量其实就是 Schnorr 签名的计算量. 签名长度也线性依赖于 d. 值得注意的是, 方案中 d 是由签名者自由决定的, d 越大, 匿名范围越广, 但计算量和签名长度也就越大, 签名者可以根据需要在计算量和匿名性方面进行灵活地选择.

5 结束语

群签名方案中存在群管理员权利过大的缺点, 而环签名方案又无法追踪签名者. 本文利用环签名的思想给出的新的类似群签名的匿名签名方案解决了这一矛盾. 其基本思想是通过让管理员和签名接收者分别产生一个秘密数传送给签名者, 签名者利用这些秘密数和自己的一个秘密数产生一个环签名. 这种签名方案是群签名和环签名思想的折衷. 它基本上是一个群签名方案, 但同时保留了环签名的某些特征. 签名者在安全性和计算量上可以根据自己的需要进行灵活选择.

参考文献:

[1] D Chaum, E van Heyst. Group signatures[A]. LNCS 547, Proc of Eurocrypt 91[C]. Berlin: Springer2Verlag, 1992. 257- 265.

[2] R L Rivest, A Shamir, Y Tauman. How to leak a secret[A]. LNCS 2248, Proc of Asiacrypt01[C]. Berlin: Springer2Verlag, 2001. 552- 565.

[3] Emmanuel Bresson, Jacques Stern, Michael Szydlo. Threshold ring signatures for adhoc groups[A]. LNCS 2442, Cryptology2002[C]. Berlin: Springer2Verlag, 2002. 465- 480.

[4] M Abe, M Ohkubo, K Suzuki. 1out 2of2n signatures from a variety of keys[A]. LNCS 2501, Asiacrypt 2002[C]. Berlin: Springer2Verlag, 2002. 415- 423.

[5] Fangguo Zhang, Kwangjo Kim. ID2based blind signature and ring signature from pairings[A]. LNCS 2501, Asiacrypt 2002[C]. Berlin: Springer2Verlag, 2002. 533- 574.

作者简介:

王继林 男, 1965 年生于河南柘城, 西安电子科技大学博士生, 副教授, 研究方向为电子商务安全.

张键红 男, 1975 年生于河北石家庄, 西安电子科技大学博士研究生, 研究方向为群体密码技术.