一个动态的可追踪匿名认证方案

田子建 王继林* 伍云霞
(中国矿业大学信息研究所 北京 100083)
*(浙江财经学院信息学院 杭州 310012)

摘 要：该文提出了一个支持身份追踪的匿名认证方案。该方案有下列优点：(1)用户动态加入和吊销特别方便，管理员仅需在公告牌上公布和删除该成员的相关数据。(2)示证人可以灵活地、主动地选择匿名范围，即他可以任意选取多个合法的用户并说明自己在其中。(3)追踪示证人的具体身份是受限制的，管理员无法单独实现身份追踪，必须和验证者合作才能共同追踪示证人的身份。另外，在抵抗外部攻击和伪装攻击方面，该方案具有任意弹性，明显的优于 Boneh(1999)的 1-弹性方案。

关键词：匿名认证，身份追踪，*k*-弹性
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2005)11-0737-04

A Dynamic Anonymous Authentication Scheme with Identity Escrow

Tian Zi-jian Wang Ji-lin* Wu Yun-xia
(*Information Research Institute, China University of Mining and Technology, Beijing* 100083, *China*)
*(*Information School, of Zhejiang University of Finance and Economics, Hangzhou* 310012, *China*)

Abstract A new anonymous authentication scheme with traceable identity is proposed. This scheme has the following advantages: (1) It is easy for users to dynamically join and leave, the only thing needs to do is manager add or delete the relevant data of users. (2) The prover can unrestrictedly choose a group of users and declare that himself belong to it, so he can choose his anonymous scope initiatively and freely. (3) In the process of trace the identity of prover, the right of manager is restricted, he needs cooperation with the verifiers to reveal the identity of the prover. In the aspect of against outside attack and masking attack, compared with the scheme 1-resilient of Boneh(1999), this scheme can realize arbitrary resilience .

Key words Anonymous authentication, Identity escrow, *k*-resilient

1 引言

匿名技术是实现隐私保护的重要工具，本文研究匿名认证问题：用户希望能够证明自己是某个组织中的成员，但不想暴露其具体身份。

与匿名签名类似，匿名认证可分为无条件匿名认证和可追踪匿名认证。不严格地说，一个认证方案是匿名的，如果示证者不暴露自己的身份而能向验证者证明自己是合法用户；一个匿名认证方案是可追踪的，如果管理员能根据自己的陷门信息和验证者提供的信息能找出示证人的具体身份。设 L 为用户集 Ω 的任一个子集，对 L 来说，一个匿名认证方案对伪装攻击是 k 弹性的，如果不存在 L 中 k 个内部用户能勾结伪装成另一个用户匿名通过认证的情况；一个匿名认证方案对外部攻击是 k 弹性的，如果不存在 k 个外部用户能勾结伪装成 L 中的一个用户成功通过认证的情况。

结合无条件匿名签名[1-3]和群签名的思想，我们提出了一个可追踪的匿名认证方案。该方案的安全性是建立在离散对数问题之上的，在管理员和验证者不勾结的情况下，我们的方案在抵抗外部攻击和伪装攻击方面具有任意弹性，明显地优于文献[4]的 1-弹性方案。

文章按下述方式展开，第 2 节是形式化描述，第 3 节综述有关研究进展，第 4 节介绍我们的方案，第 5 节为安全性和效率分析，第 6 节是结束语。

2004-06-15 收到， 2004-12-16 改回
国家自然科学基金（60073052）和高等学校博士学科点专项基金（20030290019）资助课题

2 匿名认证的形式化描述

一个无条件匿名的认证方案由初始化和认证两个阶段组成，在初始化阶段 INIT 结束后，每个用户获得一对公私钥，在 (P,V) 认证阶段，用户 P 试图向验证者 V 证明其拥有初始化阶段获取的一个合法私钥而不暴露其身份。这里 P 和 V 均为图灵机。

一个无条件匿名的认证方案 $\{\text{INIT},(P,V)\}$ 是安全的，如果它满足：

(1) 正确性　对每个用户:

$U_i \in S, \Pr[(pk_1, pk_2, \cdots, pk_m, sk_i) \leftarrow \text{INIT}(1^k);$

$t \leftarrow (P(sk_i), V)(pk_1, \cdots, pk_m) : \text{OUT}_V(t) = \text{accept}] = 1;$

(2) 完备性　对每个 $U_i \notin S$ 和任一概率多项式时间的算法，其被 V 认可为合法用户的概率:

$\Pr[(pk_1, pk_2, \cdots, pk_m) \leftarrow \text{INIT}(1^k); t \leftarrow (P'(\phi), V)(pk_1, \cdots, pk_m) :$

$\text{OUT}_V(t) = \text{accept}] - 1/2$ 是可忽略的，$P'(\varphi)$ 表示私钥的输入为空串。

(3) 匿名性　对任何用户 $U_i, U_j \in S$ 和任何概率多项式时间的算法 V'，概率空间 $\prod_1$ 和 $\prod_2$ 是一样的，其中

$\prod_1 = [(pk_1, pk_2, \cdots, pk_m, sk_i) \leftarrow \text{INIT}(1^k);$

$t \leftarrow (P(sk_i), V')(pk_1, \cdots, pk_m) : t]$

$\prod_2 = [(pk_1, pk_2, \cdots, pk_m, sk_j) \leftarrow \text{INIT}(1^k);$

$t \leftarrow (P(sk_j), V')(pk_1, \cdots, pk_m) : t]$

与无条件匿名认证方案相比，可追踪匿名认证方案中增加了一个追踪者和一个追踪过程，方案的匿名性一般不针对追踪者。可追踪匿名认证方案的形式化描述可仿上面的形式给出。

3 可追踪匿名认证的有关研究

对无条件匿名认证的最新研究工作可参考文献[5,6]，其中文献[5]通过对前人一些方案的改进，分别给出了一个基于离散对数困难性和用户独立选取 RSA 参数的认证方案。无条件匿名认证方案的计算量和通信量一般都随成员数线性增加。

通过两个不勾结的半可信机构授权的方式，可实现可追踪匿名认证，文献[7]和[8]分别利用 hash 链和盲签名技术给出了相应的方案。但这种方案的前提要求太强。

群签名技术是用来实现可追踪匿名认证的最直接想法[9]。群签名首先由Chaum 和 van Heyst等人[10]提出，目前最好的(能抵抗联合攻击)群签名是由 Ateniese, 等[11]给出的方案。用群签名实现的匿名认证方案中，群管理员可以揭露示证人的真实身份。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。另外基于群签名的这种认证方案很难处理成员用户的吊销问题。

对移动环境下的可追踪匿名认证问题，最近 Shouichi 等人[12]利用随机自归约关系(Random self-redicibility)实现了临时公私钥对的产生并给出了一个匿名认证方案，但这种方案依然有管理员权利过大的问题。

上述方案中，用户不能自由地、主动地选择自己的匿名范围，即他不能匿名地任意选择一个合法的用户子集说明自己是其中一个用户。

可由示证人自由选定匿名子集构成范围但不具有身份追踪的匿名认证方案往往是部分知识证明的具体应用[5,13,14]。值得注意的是 1 out of n 签名[1]和最近提出的环签名[2,3]的思想可用来实现这种匿名认证。

文献[4]利用求高次剩余困难性的假设和零知识证明技术给出了一个可由示证人自由选定匿名子集构成范围且能实现身份追踪的匿名认证方案。但该方案在抵抗外部攻击和伪装攻击方面有严重的缺陷，其基本方案仅具有 1-弹性，作者建议利用有关指纹码技术[15]可提高防止伪装攻击的强度，但这样会严重增加计算量。

4 动态可追踪匿名认证方案

我们借鉴了环签名的思想，提出的方案既能由示证人自由选定匿名子集构成匿名范围，又实现了身份追踪，而且又克服了利用群签名思想等认证方案中管理员权利过大和难吊销用户的缺点。与文献[4]给的方案相比，我们的方案在抵抗外部攻击和伪装攻击方面具有明显的优越性，我们的方案可以实现任意弹性，而文献[4]的方案仅能实现 1-弹性；另外我们方案的通信复杂度也比其低。

在我们的认证方案中，有一个管理者负责用户的注册和吊销，他同时负责用户的追踪；被称为“示证者”的用户在认证时向“验证者”证明自己是合法的用户。

我们通过由管理员和验证者分别产生一个秘密参数 t 和 r，示证人利用 t 和 r 以及自己的私钥等构成环签名的方式实现了我们的方案。

4.1 参数假定

设 p,q 为大素数，$<g>$ 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 $y_i = g^{x_i} \bmod p$，Public 为一个发布公钥的公告牌。

设管理员 GM 管理上述公告牌 Public，管理员 GM 的私钥为 x_{GM}，对应的公钥为 y_{GM}。验证者 V 的私钥为 x_V，对应的的公钥为 y_V。管理员和验证者的公私钥可以不是基于离散对数的。我们用 $\{x\}_{y_1}$ 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 AES) $\text{Encode}(x, L) = e_x = [\{x\}_{y_1}, \{x\}_{y_2}, \cdots,$

$\{x\}_{y_d}]$, Decode$(e_x, x_k, L) = x = \{e_x[i]\}_{x_k}$。$\overset{R}{\Leftarrow}$表示任意选取。

4.2 用户向管理员注册

用户 B_i 选择并记住一个 t_i，计算 $p_i = g^{t_i} \bmod p$，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 $H: \{0,1\}^* \to Z_q$。

4.3 用户吊销过程

已经成为成员的用户如果想吊销，只需向管理员申请，管理员在公告牌上删除该用户的数据即可。

4.4 成员用户 B_k 的认证过程

示证人 B_k 希望匿名地向验证者 V 证明自己是公告牌上发布的合法用户，他首先在 GM 发布的公钥中任选一些公钥(包括他自己的公钥)，构成本次的匿名集 L，为了方便叙述，不妨假定 $L = \{y_1, y_2, \cdots, y_d\}$，然后分别从 GM 和 V 那里匿名获取参数 t 和 r，最后产生一个环签名 $S(B_k, p_k, r, t) = \sigma = (h, L, p_k^{tr}, c_1, s_1, s_2, \cdots, s_d)$ 送给验证者供其验证。验证者通过 Verify(σ) 算法，计算 c_j 是否构成一个环状结构决定示证者是否合法。

(1) 参数 t 和 r 按如下方式获得　B_k 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 $t \in Z_q^*$ 在自己的秘密数据库中记录 (h, t)，把 $E_h[\{\text{Encode}(t, L)\}_{x_{GM}}, \{p_1^t, p_2^t, \cdots, p_d^t\}_{x_{GM}}]$ 送给 V。V 为本次签名随机产生一个 $r \in Z_q^*$ 在自己的秘密数据库中记录 (h, r)，把 $E_h[\{\text{Encode}(r, L)\}_{x_V}, \{\text{Encode}(t, L)\}_{x_{GM}}]$ 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。

(2) $S(B_k, p_k, r, t)$ 的计算如下：$S(B_k, p_k, r, t)$

(a) $\alpha \overset{R}{\Leftarrow} Z_q$，$c_{k+1} = H(g_k^{\alpha} \bmod p)$

(b) for $i = k+1, \cdots, d, 1, \cdots, k-1,$

do $s_i \overset{R}{\Leftarrow} Z_{q_i}$，and $c_{i+1} \Leftarrow H(g_i^{s_i} (p_k^{tr} y_i)^{c_i} \bmod p)$

(c) $s_k \Leftarrow \alpha - (t_k tr + x_k) c_k \bmod q$

(d) return $\sigma = (h, L, p_k^{tr}, c_1, s_1, s_2, \cdots, s_d)$

(3) 验证者 V 的 Verify(σ) 算法：　Verify(σ)

(a) p_k^{tr} 检查：对 GM 给的 $E_h[\{\text{Encode}(t, L)\}_{x_{GM}}, \{p_1^t, p_2^t, \cdots, p_d^t\}_{x_{GM}}]$，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 “Reject”

(b) 环检查：for $i = 1, 2, \cdots, d$，$c_{i+1} \Leftarrow H(g_i^{s_i} (p_k^{tr} y_i)^{c_i} \bmod p)$, If $c_{d+1} = c_1$ then return “Accept”

else return “Reject”

4.5 管理员与验证者合作恢复出示证人身份

验证者 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 确定示证人的身份。

5 安全性和效率分析

定理 1　在无法建立 p_k^{tr} 和 p_k 对应的情况下，上述认证方案满足匿名性。

证明　方案中除了示证人 B_k 的 s_k 外，其余的 s_i 都是在 Z_q 上随机选取的。由于 α 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}，$(s_1, s_2, \cdots, s_d)$ 有 q^d 种等可能的取值，而 c_1 完全由 m 和 $(s_1, s_2, \cdots, s_d)$ 唯一确定。因此，从 $(c_1, s_1, s_2, \cdots, s_d)$ 本身判断出具体为哪个示证人的签名是不可能的。在无法建立 p_k^{tr} 和 p_k 对应的情况下，由于 $c_j (j = 1, 2, \cdots, d, 1)$ 结构呈环状，即便所有人的私钥泄露也无法确定具体示证人。因而上述方案满足匿名性。　证毕

定理 2　p_k^{tr} 和 p_k 对应关系的建立，只有靠管理员 GM 和验证者 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 是不可能的，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，管理员和验证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，验证者的情况与之类似。　证毕

综合定理 1 和定理 2 我们得出，在管理员和验证者不勾结的情况下，上述认证方案能够实现示证人匿名。管理员无法单独找出具体示证人，因而本方案对管理员的权限进行了有效限制。

定理 3　在管理员和验证者不勾结的情况下，上述认证方案对伪装攻击和外部攻击均具有任意弹性。

证明　外部攻击者和伪装攻击者要假冒 L 中某个用户进行认证，就必须要获取 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 中的任意多个成员不能冒充别的成员成功通过即可。

L 中的内部攻击者要成功假冒 B_k 进行认证，他必须使用 B_k 对应的 p_k 来计算 σ，为使 σ 中的 c_j 呈环状结构，他们最终需要知道 p_k 对应的 t_k，但这需要解离散对数，在计算上是不可能的。　证毕

定理 4　上述认证方案能够抵御一致性攻击(两次认证是否来自同一个用户的)。

证明 这个结论是显然的，因为示证人每次提交的 σ 用的 t 和 r 都不相同，而 t 和 r 又是随机选取的，故不能判定两次认证是否为同一个示证者的。 证毕

我们的方案中，在 t 和 r 决定后，认证和验证主要花费在 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。σ 的长度也线性依赖于 d 。值得注意的是，方案中的 d 是由示证人自由决定的。d 越大，匿名范围越广，但计算量和提交数据的长度也就越大。示证人可以根据需要在计算量和匿名性方面进行灵活地选择。

与文献[4]所给的方案相比，我们方案的通信复杂度要低，仅经过一轮即完成认证，由于文献[4]采用了复杂的零知识证明技术，其通信需要多轮才能完成；两个方案的计算量都线性依赖于 d ，但我们的方案在抵抗外部攻击和伪装攻击方面具有任意弹性。

6 结束语

以前的可追踪匿名认证方案中存在难以吊销用户的缺点，而很多可由示证人自由指定匿名集的认证方案又无法追踪示证人。本文结合环签名的思想给出的新的匿名认证方案解决了这一矛盾。其基本思想是通过让管理员和签名验证者分别产生一个秘密数传送给示证人，示证人利用这些秘密数和自己的一个秘密数产生一个含有环型的 c_i 的 σ 送给验证者。这种认证方案是本质上群签名和环签名思想的折衷。示证人在安全性和计算量上可以根据自己的需要进行灵活选择。该方案在抵抗外部攻击和伪装攻击方面具有任意弹性。

参 考 文 献

[1] Abe M, Ohkubo M, Suzuki K. 1-out–of-*n* signatures from a variety of keys[A]. Asiacrypt 2002, Queenstown, New Zealand, 2002, LNCS Vol.2001: 415 – 423.

[2] Rivest R L, Shamir A, Tauman Y. How to leak a secret[J]. In C. Boyd, editor, Proc. of Asiacrypt01, Gold Coast, Australia, December 2001, LNCS Vol.2248, Springer-Verlag, 2001: 552 – 565.

[3] Emmanuel Bresson, Jacques Stern, Michael Szydlo. Threshold ring signatures for Ad-hoc groups[A]. Cryptology-2002. August,18-22, 2002, Santa Barbara, California, USA. http://citeseer.nj.nec.com/bresson02threshold.html

[4] Boneh D, Franklin M. Anonymous authentication with subset queries. In Proceedings of the 6th ACM Conference on Computer and Communications Security, New York, NY, USA, 1999: 113 – 119.

[5] Lee C H, Deng Xiaotie, Zhu Huafei. Design and security analysis of anonymous group identification protocols. Public Key Cryptography, February 2002, Paris, France, LNCS Vol.2274, Springer-Verlag Berlin Heidelberg, 2002: 188 – 198.

[6] Eliane Jaulmes, Guillaume Poupard. On the security of homage group authentication protocol FC2001, Cayman Islands, British West Indies, Feb. 19-22, 2001, LNCS Vol.2339: 106 – 116.

[7] Kim Jongseong，Choi Soogil，Kim Kwangjo, *et al.*. Anonymous authentication protocol for dynamic groups with power-limited devices. SCIS 2003, Hamamatsu, Japan.http://cites eer.nj. nec. com/kim03anonymous.html.

[8] Wang Changjie, Leung Ho-fung. An anonymous and secure continuous double auction scheme for internet retails market. 37th Hawaii International Conference on System Sciences, Big Island, HI, USA, January 5-8, 2004, http://csdl.computer.org/comp /proceedings/hicss/2004/2056/07/205670180babs.htm

[9] Kilian J, Petrank E. Identity escrow proceedings. Advances in Cryptology: Crypto'98 http://external.nj.nec.com/ homepages/ joe/ web-papers.html

[10] Chaum D, Van Heyst E. Group signatures. In D. W. Davies, editor, Proc. of Eurocrypt '91, Brighton, U.K, April 1991, LNCS Vol. 547, Springer-Verlag, 1992: 257 – 265.

[11] Ateniese G, Camenisch J, Joye M, *et al.*.A pratical and provably secure coalition-resistant group signature scheme, In Advances in Cryptology- CRYPTO 2000, Santa Barbara, California, USA, August 20-24, 2000, LNCS Vol.1880: 255 – 270.

[12] Hirose S, Yoshida S. A user authentication scheme with identity and location privacy. Information Security and Privacy : 6th Australasian Conference, Sydney, Australia, July 11-13, 2001, LNCS Vol.2119: 235 – 246.

[13] Cramer R, Damgard I, Schoenmakers B. Proofs of partial knowledge and simplified design of witness hiding protocols. 14th Annual International Crytology Conference, Santa Barbara, California, USA, August 21-25, 1994, LNCS Vol.839: 174 – 187.

[14] Feige A, Shamir. Witness indidtinguishable and witness hiding protocols[A]. In Proceedings of the, Twenty-Second Annual ACM Symposium on Theory of Computing , Maryland, United States, April 1990: 416 – 426.

[15] Boneh D, Shaw J. Collusion-secure fingerprinting for digital data. In Prot of 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27-31, 1995: 452 – 465.

田子建： 男，1964 年生，讲师，博士，研究方向为编码理论与信息安全.

王继林： 男，1965 年生，教授，博士后，研究方向为电子商务的安全技术.

伍云霞： 女，1967 年生，博士后，研究方向为信息安全.