基于数字签名的交互式用户身份鉴别方案 [1]

唐韶华 韦 岗

(华南理工大学计算机系 广州 510640)

摘 要 该文首先利用 Harn 数字签名方案建立了基于身份的交互式用户认证与双向认证方案，并首次将这种基于身份的交互式用户认证方案推广为基于身份的交互式共享认证方案，使得认证系统的 n 名验证者中 t 名以上验证者才能验证用户身份的有效性，从而可以有效地防止认证系统个别管理人员的作弊行为，提高了认证系统的安全级别与可用性。

关键词 数字签名，用户认证，共享认证，基于身份的密码系统

中图号 TN918.1

1 引 言

随着计算机网络的迅速发展，安全问题显得越来越重要，其中的关键技术包括 [1]：安全体系结构、防火墙、数字签名技术等。我们在考虑安全、保密、计费等因素时，需要设置各种安全策略，对于某些特定的资源，只有经授权的合法用户才能访问。而如何正确地鉴别用户的真实身份却是问题的关键，为此，各国专家、学者提出了多种身份鉴别 (也称为用户认证) 方案。

在 1984 年，Shamir 提出了“基于身份的密码系统” [2] 这一概念，在这种系统中，每一用户入网前必须到密钥认证中心 (KAC) 注册，由 KAC 发给用户密钥。这样，用户只需要知道网上另一用户的身份标识就可与之进行保密通信。此后，出现了各种类型的基于身份的密码方案。1986 年，Okamoto 提出了基于身份的密钥分配方案 [3,4]；1988 年 Ohta 扩展了 Okamoto 方案用于身份鉴别 [5]；Tsujii 利用离散对数也提出了基于身份的密码系统 [6,7]；1993 年，Harn 和 Yang 提出了一种可用于身份鉴别、数字签名、密钥分配的密码方案 [8]。国内同行关于身份认证 [9−11]、防火墙技术 [12] 等有关方面也作了大量的研究工作。

然而，如何防止认证系统内部个别管理人员作弊，如何提高认证系统的安全级别与可用性却是各种用户认证方案有待解决的问题。本文首先利用签名与验证速度较快的 Harn 数字签名方案 [13] 构造基于身份的交互式用户认证与双向认证方案，然后再推广为基于身份的交互式共享认证方案，提高了认证系统的安全级别与可用性。

2 Harn 数字签名回顾

Harn[13] 于 1994 年提出了一种基于离散对数的数字签名算法，具有简化签名生成过程、加速签名验证过程等优点。Harn 方案简述如下：p 是一个大素数，α 是 GF(p) 中的一个本原元，f 是单向函数。签名者的密钥为 x，这里 $x \in [1, p-1]$ 且 $\gcd(x, p-1) = 1$，公钥为 $y \equiv \alpha^x (\bmod\ p)$。设 m 为要签发的消息，签名者选择一随机数 $k \in [1, p-1]$，计算 $r \equiv \alpha^k (\bmod\ p)$ 及 $s \equiv x(f(m)+r) - k (\bmod\ p-1)$，则 (r, s) 为签名者关于消息 m 的数字签名。签名验证方程为 $y^{f(m)+r} \equiv r\alpha^s (\bmod\ p)$，如果验证方程成立则签名被接受。

[1] 1999-06-11 收到，1999-11-08 定稿

国家自然科学基金 (69802006) 及广东省自然科学基金 (970849，990598) 资助课题

3 基于身份的用户认证方案

本节将利用 Harn 数字签名方案，结合零知识证明的思想构造基于身份的用户认证方案。一般而言，一个基于身份的密码系统由三个阶段组成：初始化阶段、用户注册阶段和应用阶段。

3.1 初始化

密钥认证中心 KAC 选择一单向函数 f，大素数 p，及 GF(p) 上的本原元 α。p 的选择应满足 $p=2p'+1$，其中 p' 也是一个大素数。KAC 选择一随机数 x 作为自己的秘钥，x 应满足 $x\in[1,p-1]$ 且 $\gcd(x,p-1)=1$，KAC 的公钥为 $y\equiv\alpha^x(\bmod p)$。f,p,α,y 为系统的公开参数。

3.2 用户注册

每一用户 U_i 需向 KAC 提交自己的身份标识 ID_i，经 KAC 确认身份后，KAC 为每个 U_i 计算 (r_i,s_i) 如下：

$$r_i\equiv\alpha^{k_i}(\bmod p) \tag{1}$$

$$s_i\equiv x(f(\mathrm{ID}_i)+r_i)-k_i(\bmod p-1) \tag{2}$$

其中 k_i 是随机数，$k_i\in[1,p-1]$。KAC 通过一可靠的信道把 (r_i,s_i) 交给 U_i，其中 s_i 是 U_i 的秘密参数，需保密。U_i 可通过以下验证方程检验 (r_i,s_i) 是否由 KAC 所发：

$$y^{f(\mathrm{ID}_i)+r_i}\equiv r_i\alpha^{s_i}(\bmod p) \tag{3}$$

3.3 用户认证

假设 U_i 须向验证者 V 证实自己的身份，为防止攻击者假冒 V 骗取 U_i 的秘密信息，用户认证方案设计的关键之处在于如何确保用户 U_i 向 V 证实自己身份的同时不致于暴露自己的秘密信息 s_i，这是零知识证明的思想在身份认证方案设计中的应用。本方案属于一种“问答”式 (challenge-response) 的协议，详述如下：

步骤 1 用户 U_i 把 (ID_i,r_i) 发给 V。

步骤 2 V 收到 U_i 的 (ID_i,r_i) 后，选择随机数 v，v 满足 $v\in[1,p-1]$ 且 $\gcd(v,p-1)=1$，并计算

$$w\equiv\alpha^v(\bmod p) \tag{4}$$

然后把 w 发回给 U_i。

步骤 3 用户 U_i 收到 w 以后计算

$$z\equiv w^{s_i}(\bmod p) \tag{5}$$

然后把 z 发回给 V。

步骤 4 V 收到 z 后，验证以下等式是否成立：

$$y^{f(\mathrm{ID}_i)+r_i}\equiv r_iz^{v^{-1}}(\bmod p) \tag{6}$$

如果上述验证方程成立，则说明 U_i 的身份真实。

(6) 式的证明如下：

由 (5) 式可得 $z \equiv w^{s_i} (\mathrm{mod}\ p) \equiv (\alpha^v)^{s_i} (\mathrm{mod}\ p) \equiv (\alpha^{s_i})^v (\mathrm{mod}\ p)$，从而有 $z^{v^{-1}} \equiv \alpha^{s_i} (\mathrm{mod}\ p)$；再由 (3) 式可得 $\alpha^{s_i} \equiv r_i^{-1} y^{f(\mathrm{ID}_i)+r_i} (\mathrm{mod}\ p)$，则有 $z^{v^{-1}} \equiv r_i^{-1} y^{f(\mathrm{ID}_i)+r_i} (\mathrm{mod}\ p)$，从而得 (6) 式。

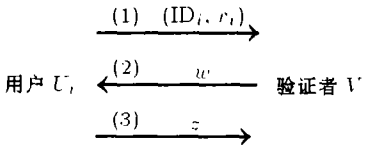

图 1　交互式用户认证协议

上述用户认证协议的执行过程如图 1 所示。

3.4 安全性分析

攻击者可能采用以下几种方法进行攻击:

(1) 任何人均可得到 p, w, z 的值，若试图从方程 $z \equiv w^{s_i} (\mathrm{mod}\ p)$ 中求解 s_i，其计算的困难性等价于计算 GF(p) 中离散对数之困难性。因此，用户 U_i 的秘密信息 s_i 是不会暴露的，攻击者不可能得到 s_i。

(2) 攻击者可能试图在不知道 s_i 的情况下冒充 U_i，方法是收集以往认证过程中的信息，然后试图通过以往的认证信息计算本次认证信息 z。例如攻击者收集了某次认证过程的 $w_1 \equiv \alpha^{v_1} (\mathrm{mod}\ p)$ 及 $z_1 \equiv w_1^{s_i} (\mathrm{mod}\ p)$，然后攻击者向验证者 V 发送 (ID_i, r_i)。根据协议，V 生成询问信息 $w_2 \equiv \alpha^{v_2} (\mathrm{mod}\ p)$，攻击者试图通过 w_1, z_1, w_2 计算 z_2：

$$z_2 \equiv w_2^{s_i} (\mathrm{mod}\ p) \equiv (\alpha^{v_2})^{s_i} (\mathrm{mod}\ p) \equiv (\alpha^{v_1 v_1^{-1} v_2})^{s_i} (\mathrm{mod}\ p) \equiv (\alpha^{v_1 s_i})^{v_1^{-1} v_2} (\mathrm{mod}\ p)$$
$$\equiv (w_1^{s_i})^{v_1^{-1} v_2} (\mathrm{mod}\ p) \equiv z_1^{v_1^{-1} v_2} (\mathrm{mod}\ p)$$

但攻击者想通过 w_1, w_2 求解 v_1, v_2 的困难性等价于计算离散对数。

(3) 若想由公开信息 (ID_i, r_i, y) 及验证方程 $y^{f(\mathrm{ID}_i)+r_i} \equiv r_i \alpha^{s_i} (\mathrm{mod}\ p)$ 求出秘钥 s_i，其计算困难性等价于计算离散对数。

(4) 攻击者可能试图先随机选择一整数 s_i'，然后由方程 $y^{f(\mathrm{ID}_i)+r_i} \equiv r_i \alpha^{s_i'} (\mathrm{mod}\ p)$ 求出 r_i，这是一个极其困难的问题，其计算困难性比求解离散对数还要困难。

(5) 用户 $U_i (i = 1, 2, \cdots, n)$ 中有多人合作试图导出 KAC 的秘钥 x。对于每个 U_i 的 (r_i, s_i)，他们可以构造方程 $s_i \equiv x(f(\mathrm{ID}_i) + r_i) - k_i (\mathrm{mod}\ p-1)$，但由于 k_i, x 均为未知数，而且对于每个 U_i，相应的 k_i 均不相同，因此 x 不能唯一决定。

综上所述，基于公认的“求解离散对数是一计算困难问题”这一前提下，我们的方案是安全的。

3.5 双向认证与密钥交换

我们可以把前面的用户认证方案推广为任意两用户 U_i, U_j 间的双向认证方案。双向认证在电子商务中非常重要，以信用卡购物为例，不仅商家要确认持卡人的真实身份，与此同时，购物者 (持卡人) 也必须确认商家的真实身份，以确保款项付给了真正的商家。U_i, U_j 之间的双向认证的步骤如下:

步骤 1　U_i 选择随机数 v_i，v_i 满足 $v_i \in [1, p-1]$ 且 $\gcd(v_i, p-1) = 1$，计算 $w_i \equiv \alpha^{v_i} (\mathrm{mod}\ p)$，把 $(\mathrm{ID}_i, r_i, w_i)$ 发给 U_j。

步骤 2　U_j 选择随机数 v_j，v_j 满足 $v_j \in [1, p-1]$ 且 $\gcd(v_j, p-1) = 1$，计算 $w_j \equiv \alpha^{v_j} (\mathrm{mod}\ p)$ 及 $z_j \equiv w_i^{s_j} (\mathrm{mod}\ p)$，把 $(\mathrm{ID}_j, r_j, w_j, z_j)$ 发给 U_i。

步骤 3　U_i 验证等式 $y^{f(\mathrm{ID}_j)+r_j} \equiv r_j z_j^{v_i^{-1}} (\mathrm{mod}\ p)$ 是否成立，若等式成立，说明 U_j 身份真实。然后，U_i 计算 $z_i \equiv w_j^{s_i} (\mathrm{mod}\ p)$，并把 z_i 发给 U_j。

步骤 4　U_j 验证等式 $y^{f(\mathrm{ID}_i)+r_i} \equiv r_i z_i^{v_j^{-1}} (\mathrm{mod}\ p)$ 是否成立，若等式成立，说明 U_i 身份真实。

通过上述步骤，U_i, U_j 间不仅彼此认证了对方的身份，而且可以计算出 U_i, U_j 间的共享密钥，方法如下：U_i 在步骤 3 确认 U_j 身份后，利用自己的秘密信息 s_i, v_i 计算：

$$\begin{aligned} K_{ij} &\equiv z_j^{s_i v_i^{-1}(\bmod p-1)}(\bmod p) \equiv (\alpha^{v_i s_j})^{s_i v_i^{-1}(\bmod p-1)}(\bmod p) \\ &\equiv \alpha^{s_j s_i(\bmod p-1)}(\bmod p) \equiv \alpha^{s_j s_i}(\bmod p) \end{aligned} \tag{7}$$

而 U_j 在步骤 4 确认 U_i 身份后，利用自己的秘密信息 s_j, v_j 计算：

$$\begin{aligned} K_{ji} &\equiv z_i^{s_j v_j^{-1}(\bmod p-1)}(\bmod p) \equiv (\alpha^{v_j s_i})^{s_j v_j^{-1}(\bmod p-1)}(\bmod p) \\ &\equiv \alpha^{s_i s_j(\bmod p-1)}(\bmod p) \equiv \alpha^{s_i s_j}(\bmod p) \end{aligned} \tag{8}$$

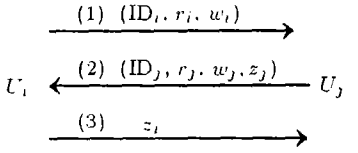

图 2 双向认证与密钥交换

这样，U_i, U_j 间相当于交换了密钥 $K = K_{ij} = K_{ji}$，而且 U_i, U_j 均在确认了对方身份后才计算 K_{ij}, K_{ji} 的。因此，上述方案实现了身份认证与密钥交换。上述双向认证与密钥交换过程如图 2 所示。

4 用户身份鉴别的共享验证方案

受 Harn[14] 等人研究数字签名共享验证方案的启发，我们可以构造用户身份鉴别的共享验证方案 (或称为共享认证方案)，具有如下特征：(1) 认证系统中 (设有 n 名验证者) 的任意 t 人可合作验证用户的身份；(2) 任意 $t-1$ 或少于 $t-1$ 人不能验证用户的身份。共享认证的显著优点为：(1) 可以防止认证系统内部个别管理人员 (验证者) 的作弊；(2) 可提高认证系统的安全级别：对于涉及多个团体和行业的敏感数据的访问，必须经过各团体代表或若干管理人员的同意方可实施，从而可控制和提高认证系统的安全性；(3) 可提高认证系统的可用性：认证系统只要有 t 名以上验证者在场即可提供认证服务，个别验证者缺席或出现别的问题也不致于影响认证服务。本文采用 Shamir 秘密共享方案 [15] 分发共享秘钥。

4.1 初始化

KAC 选择一单向函数 f，大素数 $p, w = (p-1)/2$ 也是大素数，q 是 $w-1$ 的素因子。h_i 是随机数：$0 < h_i < p$，则 $g_i \equiv h_i^{(p-1)/w}(\bmod p)$ 是 GF(p) 中阶为 w 的生成元 ($g_i > 1$)。e 是随机数：$0 < e < w$，则 $\alpha \equiv e^{(w-1)/q}(\bmod \omega)$ 是 GF(w) 中阶为 q 的生成元 ($\alpha > 1$)。KAC 选择随机数 $x(0 < x < q)$ 作为秘钥。由文献 [14] 知，存在 β_i 满足 $g_i^{\alpha^x} \equiv \beta_i^x(\bmod p)$；$U_i$ 的公钥为 $y_i \equiv \beta_i^x \equiv g_i^{\alpha^x}(\bmod p)$。上述参数中，$f, p, w, q, \alpha, g_i, \beta_i$ 为公开参数。

4.2 用户注册

用户注册过程与 3.1 节类似，用户 U_i 提交 ID$_i$ 后，KAC 产生 (r_i, s_i)：$r_i \equiv \beta_i^{k_i}(\bmod p)$ 及 $s_i \equiv x(f(\mathrm{ID}_i) + r_i) - k_i(\bmod w)$，其中 k_i 是随机数。KAC 通过一可靠信道把 (r_i, s_i, y_i, β_i) 传给 U_i。U_i 可通过等式 $y^{f(\mathrm{ID}_i)+r_i} \equiv r_i \beta_i^{s_i}(\bmod p)$ 验证 (r_i, s_i, y_i, β_i) 的有效性。

KAC 在 GF(q) 中随机选择 $a_i(i = 1, 2, \cdots, t-1)$，构造多项式 $f(z) \equiv x + \sum_{i=1}^{t-1} a_i z^i(\bmod q)$，其中 x 是 KAC 的秘钥。对于认证系统中的 n 名验证者 $V_j(j = 1, 2, \cdots, n)$，假设 V_j 的公开参数为 z_i(如身份标识等)，KAC 向 V_j 分发关于秘钥 x 的部分信息：

$$x_j \equiv \alpha^{f(z_j)}(\bmod w), \qquad j = 1, 2, \cdots, n \tag{9}$$

$V_j(j=1,2,\cdots,n)$ 把 x_j 作为个人密钥保管。此外，为方便起见，在认证系统中还应存放各用户 U_i 的公开参数 g_i, β_i 。

4.3 共享认证

设 V 表示认证系统，$V_1,\cdots,V_n$ 为 V 中 n 名验证者。共享认证步骤如下：

步骤 1　用户 U_i 把 (ID_i,r_i) 发给 V 。

步骤 2　V 收到 U_i 的 (ID_i,r_i) 后，选择随机数 v： $0<v<w$，然后把 $\delta\equiv\beta_i^v(\bmod p)$ 发给 U_i 。参数 v 应作为系统 V 的秘密信息，只有 V 中 t 名以上 V_j 同时在场才能从 V 中取出 v 。

步骤 3　用户 U_i 收到 δ 后，计算 $\eta\equiv\delta^{s_i}(\bmod p)$，然后把 η 发回给 V 。

步骤 4　V 收到 η 后，V 中 t 名验证者合作可计算 α^x 。不失一般性，假设 $V_1,\cdots,V_t$ 合作，则可恢复 α^x：

$$\alpha^x\equiv\alpha^{f(0)}\equiv\alpha^{\left(\sum_{j=1}^{t}f(z_j)\prod_{i=1,i\neq j}^{t}\frac{z_j}{z_j-z_i}\bmod q\right)}\equiv\prod_{j=1}^{t}x_j^{\left(\prod_{i=1,i\neq j}^{t}\frac{z_j}{z_j-z_i}\bmod q\right)}(\bmod w)\quad(10)$$

由 α^x 及 V 中存放的 g_i 可计算 U_i 的公钥 $y_i\equiv g_i^{\alpha^x}(\bmod p)$；然后由系统 V 中取出 v，验证等式

$$\eta^{v^{-1}}r_i\equiv y_i^{f(\mathrm{ID}_i)+r_i}(\bmod p)\qquad(11)$$

是否成立，若等式成立，则说明 U_i 的身份得到证实。

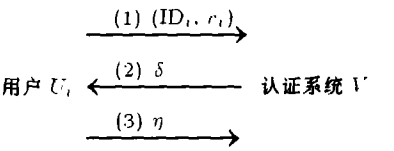

图 3　共享认证协议

(11) 式的证明与 (6) 式的证明类似，从略。上述步骤如图 3 所示。

4.4 安全性分析

攻击者同样可以采用 3.4 节所述的各种攻击方法攻击“共享认证”方案，显然这些攻击方法均不能奏效，这在 3.4 节中已作过详尽分析。此外，共享认证方案还可能面临各种“串谋”攻击，简析如下：

(1) 认证系统 V 中多名验证者 V_j 串谋合作不能得到 KAC 的秘钥 x，也不能得到用户 U_i 的秘钥 s_i 。少于 t 名 V_j 合作不能从 (10) 式计算出 α^x 及 y_i；就算可以计算出 α^x 及 y_i，但从 α^x 求解 x 却是面临求解离散对数之困难问题；由 $y_i\equiv\beta_i^x(\bmod p)$ 求解 x 及由 $\eta\equiv\delta^{s_i}(\bmod p)$ 求解 s_i 也等价于求解离散对数。

(2) 假冒的 U_i 与认证系统中少于 t 名 V_j 串谋合作也不能假冒成功。首先，假冒的 U_i 不知道 s_i，因而不能正确计算 $\eta\equiv\delta^{s_i}(\bmod p)$，也就不能通过验证方程 (11) 式的检验；再者，V 中多名 V_j 的串谋合作也不能得到真正 U_i 的秘钥 s_i 。因此，假冒的 U_i 与 V 中个别验证者串谋也不能伪造认证数据 η 。

综上所述，本文提出的共享认证方案是安全的。

5 结束语

Harn 数字签名方案 [13] 具有签名生成过程简单、签名验证速度快等优点，本文利用 Harn 方案 [13]，结合零知识证明的思想构造了基于身份的用户认证方案与双向认证方案，并首次将这种基于身份的交互式用户认证方案推广为基于身份的交互式共享认证方案，提高了认证系统的安全级别及可用性。本文还对上述各种方案的安全性进行了分析，在“求解离散对数是一计算困难问题”这一公认的安全性假设前提下，本文的方案是安全的。

参 考 文 献

[1] 李昊, Internet 的经验与挑战, 见, 石冰心主编, 中国教育和科研计算机网的研究与发展 (第一卷), 武汉, 华中理工大学出版社, 1996, 6–16.

[2] A. Shamir, Identity-based cryptosystem and signature schemes, In Proc. Crypto'84, Santa Barbara, CA, Springer-Verlag, 1984, 47–53.

[3] E. Okamoto, Proposal for identity-based key distribution systems, Electron. Lett., 1986, 22(24), 1283–1284.

[4] E. Okamoto, K. Tanaka, Key distribution system based on identification information, IEEE J. Select. Areas. Commun., 1989, 7(4), 481–485.

[5] K. Ohta, Efficient identification and signature schemes, Electron. Lett., 1988, 24(2), 115–116.

[6] S. Tsujii, ID-based cryptosystem using discrete logarithm problem, Electron. Lett., 1987, 23(24), 1318–1320.

[7] S. Tsujii, T. Itoh, An ID-based cryptosystem based on the discrete logarithm problem, IEEE J. Select. Areas. Commun., 1989, 7(4), 467–473.

[8] L. Harn, S. B. Yang, ID-based cryptographic schemes for user identification, digital signature, and key distribution, IEEE J. Select. Areas.Commun., 1993, 11(5), 757–760.

[9] 刘建伟, 王育民, 肖国镇, 基于 Krypto Knight 的移动用户认证协议, 电子学报, 1998, 26(1), 93–97.

[10] 周智, 胡正名, 个人通信网中的身份认证技术, 通信学报, 1997, 18(1), 37–41.

[11] 徐胜波, 武传坤, 王新梅, 移动通信网中的认证与密钥分配, 电子学报, 1996, 24(10), 105–110.

[12] 林晓东, 杨义先, 马严, 等, Internet 防火墙系统的设计与实现, 通信学报, 1998, 19(1), 65–69.

[13] L. Harn, New digital signature scheme based on discrete logarithm, Electron. Lett., 1994, 30(5), 396–398.

[14] L. Harn, Digital signature with (t, n) shared verification based on discrete logarithms, Electron. Lett., 1993, 29(24), 1002–1003.

[15] A. Shamir, How to share a secret, Comm. of ACM, 1979, 22(11), 612–613.

ID-BASED INTERACTIVE USER AUTHENTICATION SCHEMES USING DIGITAL SIGNATURE

Tang Shaohua Wei Gang

(*Dept. of Computer Sci. and Eng., South China Univ. of Tech., Guangzhou* 510640, China)

Abstract A kind of ID-based interactive user authentication and two-way authentication schemes are presented in this paper and extended to form a new ID-based interactive shared authentication scheme, which enables more than t out of n verifiers in authentication system to validate a user's identity, such that the cheating trick of few administrators in the authentication system can be prevented, thus the security class and the availiability of the authentication system are improved.

Key words Digital signature, User authentication, Shared authentication, ID-based cryptosystem

唐韶华: 男, 1970 年生, 博士, 华南理工大学计算机系副教授, 主要研究方向为电子商务的安全, 网络与信息安全, 计算机网络等.

韦 岗: 男, 1963 年生, 华南理工大学电子与通信工程系教授, 博士生导师; 主要研究方向为通信理论、信息处理等.