第 36 卷 第 6 期 计 算 机 工 程 2010 年 3 月
Vol.36 No.6 Computer Engineering March 2010
·安全技术· 文章编号：1000—3428(2010)06—0173—02 文献标识码：A 中图分类号：TP309

基于 ELGamal 数字签名的双向认证方案

胡建军，王 伟，裴东林
(甘肃联合大学数学与信息学院，兰州 730000)

摘 要：针对当前认证方案中普遍存在的认证效率较低和认证过程较复杂等问题，提出一种基于 ELGamal 数字签名的双向认证方案，引入密钥分配中心作为第三方，承担公钥的分发并与认证双方进行通信。分析结果表明，该方案在离散对数问题的基础上提高了难度，在计算量方面优于其他双向认证方案，可广泛用于分布式环境下的身份识别和数字签名。

关键词：数字签名；双向认证；零知识证明；离散对数

Double-way Authentication Scheme Based on ELGamal Digital Signature

HU Jian-jun, WANG Wei, PEI Dong-lin
(College of Mathematic and Information, Gansu Lianhe University, Lanzhou 730000)

【Abstract】 Aiming at the problems of low authentication efficiency and its complex process, a double-way authentication scheme of ELGamal digital signature is proposed. The Key Distribution Center(KDC) is introduced as the third aspect, which distributes the public keys and communicates with both sides. Analysis results show this scheme improves the complexity than discrete logarithm and the computing efficiency is better than others. The scheme may have some comprehensive application in identification and digital signature.

【Key words】 digital signature; double-way authentication; zero-knowledge proof; discrete logarithm

1 概述

认证是确保系统安全的第 1 道关卡，其目的在于识别用户的合法性和真实性。在分布式系统应用中，保证通信双方的合法性、防止伪造和欺骗以及提高认证的效率成为广大学者研究的热点问题。

自文献[1]提出基于身份的密码系统以来，针对身份鉴别的研究逐步开展，如文献[2]提出基于身份的密钥分配方案；文献[3]提出基于离散对数难解性的公开密钥和签名体制；文献[4]给出一个 ELGamal 签名方案的可转换且不可否认的签名方案等；我国学者在身份识别方面也做出了卓有成效的努力，如文献[5]提出一种基于 Harn 数字签名的双向认证访问控制方案；文献[6]提出一种基于不可否认数字签名的用户认证方案；文献[7]提出零知识证明的前向安全不可否认数字签名方案等。

然而，在以上这些认证方案中，存在认证效率较低和过程较为复杂等缺陷，因此，本文提出一种基于 ELGamal 数字签名的双向认证方案。

2 ELGamal 数字签名[3,6]

ELGamal 数字签名方案简述如下：

设 p 是一个大素数，g 为有限域 GF(p)上的非零元素。签名者随机选择一个密钥 x，这里，$x\in[1,p-1]$ 且满足 $\gcd(x,p-1)=1$。

假设 m 为要签名的消息，签名者首先随机选择一个 $k\in[1,p-1]$，则 (g^x,mg^{kx}) 消息就是消息 m 的数字签名。

用户接收到签名消息 (g^x,mg^{kx}) 后，利用私钥 x 验证该消息，因为第三者只知道 g^k 或 g^x，所以无法求出 g^{kx}，从 g^k 或 g^x 计算 k 或 x 是离散对数问题，而求解离散对数十分困难。

3 双向认证方案

认证方案由 2 个部分组成，即注册获取密钥和用户认证。认证的基本思路是用公钥加密、用私钥解密。认证的数学原理为

$$g^{ab}=(g^a)^b=(g^b)^a \tag{1}$$

系统公开 p, g, y 和用户标识 ID，其中，$y=g^x(\mathrm{mod}\ p)$。

3.1 注册[5-6]

用户注册过程如图 1 所示。

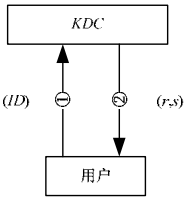

图 1 注册过程

用户首先向密钥分配中心 KDC 提交身份标识 ID，其次 KDC 任选一个数 $k\in[1,p-1]$，且满足 $\gcd(x,p-1)=1$，然后 KDC 利用私钥 x 做如下计算：

$$\begin{cases} r=g^k(\mathrm{mod}\ \ p) \\ s=x\cdot ID-k\cdot r(\mathrm{mod}\ \ p) \end{cases} \tag{2}$$

计算完成后，密钥分配中心将 (r,s) 通过面对面的方式交给用户，然后用户通过式(3)是否成立来验证自己的身份。

基金项目：甘肃联合大学校级基金资助项目(2007-03)
作者简介：胡建军(1971－)，男，讲师、硕士，主研方向：协议工程；王 伟，讲师、硕士；裴东林，副教授
收稿日期：2009-11-04 **E-mail：**hujj518@sina.com

$$y^{ID} = r^r \cdot g^s (\mathrm{mod}\ p) \quad (3)$$

KDC 保存每个注册用户的信息，包括 *ID*, *r* 和 *s* 等，并维护用户注册信息以及承担公钥的分发。

3.2 认证

由于网络中任何 2 个用户的认证过程是相同的，因此下面仅以用户 *IDA* 和用户 *IDB* 为例，说明本文的认证方案，如图 2 所示。

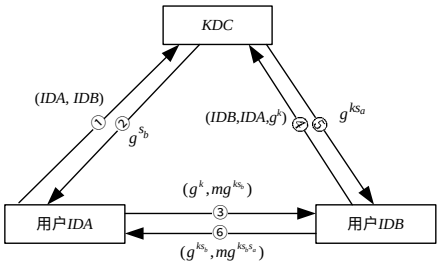

图 2 认证过程

认证过程描述如下：

第 1 步 用户 *IDA* 为获取用户 *IDB* 的公钥 g^{s_b}，向 *KDC* 发送消息 (*IDA*, *IDB*)。

第 2 步 *KDC* 查询用户 *IDB* 的私钥 s_b，并将 g^{s_b} 返回给用户 *IDA*。

第 3 步 用户 *IDA* 任选一个数 k，$k \in [1, p-1]$，计算 $m = IDA \oplus IDB$，然后将 (g^k, mg^{ks_b}) 发送给用户 *IDB*。

第 4 步 用户 *IDB* 利用私钥 s_b 及接收到的消息 g^k 求出 m，再通过计算 $m \oplus IDB$ 求出 *IDA*，即用户 *IDB* 识别出他与用户 *IDA* 进行认证，然后用户 *IDB* 为获取用户 *IDA* 的公钥 g^{s_a} 向 *KDC* 发送消息 (IDB, IDA, g^k)。

第 5 步 *KDC* 查询用户 *IDA* 的私钥 s_a，并将 g^{ks_a} 返回给用户 *IDB*。

第 6 步 用户 *IDB* 将 $(g^{ks_b}, mg^{ks_bs_a})$ 发送给用户 *IDA*。用户 *IDA* 利用私钥 s_a 及接收到的消息 g^{ks_b} 求出 m，通过计算 $m \oplus IDA$ 求出 *IDB*，由于前后 2 次需要认证的用户标识均为 *IDB*，而且前后 2 次用户 *IDB* 的公钥均为 g^{s_b}，从而用户 *IDA* 证实了他确实与用户 *IDB* 在通信。至此，用户 *IDA* 和 *IDB* 实现双向认证。

4 安全性分析

本方案具有如下的安全性：

(1)防止抵赖。因为消息 (g^k, mg^{ks_b}) 只能由私钥 s_b 解出 m，所以消息 $(g^{ks_b}, mg^{ks_bs_a})$ 只能由私钥 s_a 解出 m，除非解决了离散对数的求解问题。

(2)防止伪造。假如用户 *IDC* 代替用户 *IDA*，则用户 *IDC* 向用户 *IDB* 发送 (g^u, mg^{us_b})，其中，$u \in [1, p-1]$，用户 *IDB* 收到消息后能够识别出 *IDA*，因此，用户 *IDB* 将会把消息 $(g^{ks_b}, mg^{ks_bs_a})$ 发送给用户 *IDC*，然而用户 *IDC* 无法解出 m，因为用户 *IDC* 无法取得私钥 s_a，从而用户 *IDC* 伪造成用户 *IDA* 失败。

(3)防止欺骗。假如用户 *IDC* 代替用户 *IDB*，则用户 *IDC* 无法取得前后一致的消息 g^k，由于用户 *IDC* 向用户 *IDA* 发送的 $g^{ks_as_c}$ 是用户 *IDC* 先前获取的，不是新的 *KDC* 执行 $(g^k)^{s_c}$ 操作，因此用户 *IDC* 代替用户 *IDB* 失败。

5 各认证方案分析比较

表 1 列出本文方案与各参考文献中方案的量化比较结果。

表 1 各认证方案比较

操作	文献[5]方案	文献[6]方案	文献[7]方案	文献[8]方案	本文方案
指数运算	10	5	8	10	6
求余运算	8	5	6	10	0
异或运算	0	0	0	0	3
查询运算	0	0	0	0	2
传输次数	3	3	4	4	6
双方认证	是	否	是	是	是

从表 1 可以看出，若采用文献[6]方法进行双方认证，则衡量指标为 10,10,0,0,3。本文方案优点如下：

(1)提高运行效率

本方案减少了复杂度为 $O(n)$的指数运算，避免了复杂度为 $O(n(\log n))$的求余运算，由复杂度为 $O(\log n)$的查找运算和复杂度为 $O(n/m)$(同时可执行 m 位信息)的异或运算替代。根据分析：$O(\log n) \le O(n/m) < O(n) < O(n(\log n))$成立。与执行效率最优的方案[8]相比减少了 8 次高复杂度运算，仅增加 5 次低复杂度运算和 2 次传输，在高性能传输情况下，传输速度与运算不属同一量级。因此，方案从整体上降低了运算复杂度，提高了运行效率。

(2)提高认证的安全性

用户无需其他用户的公钥信息，且双方认证的完成基于 *IDA*, *IDB* 和 *KDC* 三方的通信，窃密者需截获 3 条链路信息才有可能破解，从而在离散对数问题上又增加了难度，使得系统的安全性更高。

6 结束语

本文提出一种基于 ELGamal 数字签名的双向认证方案，其特点有：(1)利用复杂度低的运算代替复杂度高的运算，从而提高了执行效率；(2)在不影响执行效率的前提下，引进第三方提高了系统的安全性。可以广泛应用于分布式环境下的身份鉴别和数字签名。

参考文献

[1] Shamir A. Identity-based Cryptosystem and Signature Schemes[C]// Proc. of Crypto'84. Santa Barbara, CA, USA: [s. n.], 1984.

[2] Okamoto E, Tanaka K. Key Distribution System Based on Identification Information[J]. IEEE Journal on Select Areas Commun., 1989, 7(4): 481-485.

[3] Elgamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms[J]. IEEE Trans. on Info. Theory, 1985, 31(4): 469-472.

[4] Boyar J, Chaum D, Damgurd I, et al. Convertible Undeniable Signatures[C]//Proc. of Crypto'90. [S. l.]: Springer-Verlag, 1990.

[5] 施荣华. 一种基于 Harn 数字签名的双向认证访问控制方案[J]. 计算机学报, 2001, 24(4): 400-403.

[6] 张 席, 林 强. 一种基于不可否认数字签名的用户认证方案[J]. 计算机工程, 2000, 26(8): 146-147.

[7] 王晓峰, 王尚平. 零知识证明的前向安全不可否认数字签名方案[J]. 计算机工程, 2007, 33(8): 27-29.

[8] 左为平, 王彩芬. 基于改进的 ELGamal 签名的双向认证方案[J]. 微计算机信息, 2007, 23(12): 81-82.

编辑 陈 文