一种有效的可转换的认证加密方案

甘元驹[1]，彭银桥[1]，施荣华[2]

(1. 湛江海洋大学信息学院 广东 湛江 524088; 2. 中南大学信息工程学院 长沙 410075)

【摘要】针对一般的认证加密方案存在着当签名者否认签名时，接收者不能使任何验证者证实签名者的诚实性等问题，提出了一种有效的解决方案。该方案与已有的认证加密方案和传统的签名-加密方案相比具有低计算复杂度和低通信代价。并且在该方案中，如果签名者否认自己的签名，接收者在不需签名者的合作下就可将认证加密方案转换为一般签名方案。更重要的是在不暴露消息明文的情况下，任何验证者都可验证签名的有效性。

关 键 词 密码学; 认证加密; 数字签名; 离散对数; 可转换

中图分类号 TP309 文献标识码 A

An Efficient Convertible Authenticated Encryption Scheme

GAN Yuan-ju[1]，PENG Yin-qiao[1]，SHI Rong-hua[2]

(1. College of Information of Zhanjiang Ocean University Guangdong Zhanjiang 524088;
2. College of Information Engineering of CSU Changsha 410075)

Abstract Most previous authenticated encryption schemes have a problem that the recipient can not prove the dishonesty to any verifier if the signer denies his signatures. An efficient solving scheme has been presented in this paper. The new scheme requires less computational costs and lower communication than other previous convertible authenticated encryption schemes and the conventional signature-then-encryption approaches. In the proposed scheme, if the signer repudiates the signature, the recipient can convert this signature into an ordinary one without the cooperation of the signer. Furthermore, the message is not disclosed to any verifier during verification.

Key words cryptography; authenticated encryption; digital signature; discrete logarithm; convertibility

1993年，文献[1]提出了具有消息恢复的新型数字签名方案，该方案是数据加密与数字签名密码技术的结合。在其基础上一些具有低通信代价的认证加密方案被提出[2~4]。在认证加密方案中只有指定的接收者才能恢复消息并进行签名认证，因而其优点在于可以同时实现消息的机密性与完整性，与直接分别使用对消息进行加密和签名方法相比，认证加密在实现消息的机密、完整与认证等功能时需要更小的通信代价与计算量。然而它们不能有效解决签名者否认签名等问题。1999年，首次提出了一种可转换的认证加密方案[5]，该方案如果签名者否认签名，接收者可将认证加密签名转换为一般的签名，使任何人都可以验证签名的有效性，但接收者要实现签名转换需签名者的合作，增加了网络负担和计算量，如果签名者不合作，接收者无法单独完成签名转换[6]。基于此，本文将设计一种有效性的认证加密方案。

收稿日期：2003 – 06 – 16
作者简介：甘元驹(1974 –)，男，硕士，讲师，主要从事电子商务安全、密码协议分析和网络安全方面的研究.

1 方案描述

方案由系统初始化，签名的生成、消息的恢复与验证和签名的转换与验证4个阶段组成。

1.1 系统初始化

可信任中心选择大素数p和q，且$q|p-1$，g是$GF(p)$上阶为q的生成元，一个强单向hash函数$h(\ )$，并公布p，q，g 和 $h()$。每个用户U_i拥有自己的私钥$x_i \in Z_q^*$以及公钥 $y_i = g^{x_i} \bmod p$。假设U_a为签名者，U_b为接收者，m是将被签名的消息。

1.2 签名生成

U_a随机地选择一整数$k \in Z_q^*$，并计算 $v = y_b^k \bmod p$，然后计算签名(r,R,s)：

$$r = mg^{-v} \bmod p \tag{1}$$

$$R = h(h(m) \| r \| g^k) \bmod q \tag{2}$$

$$s = k - x_a R \bmod q \tag{3}$$

式中 “$\|$”表示消息的连接。然后U_a将对消息m的签名(r,R,s)发给接收者U_b。

1.3 消息的恢复与验证

U_b收到U_a的(r,R,s)后，先计算 $v' = (g^s y_a^R)^{x_b} \bmod p$，然后通过方程(4)来恢复消息$m$。

$$m = g^{v'} \cdot r \bmod p \tag{4}$$

方程(4)的正确性证明如下：

证明：

$$v' = (g^s y_a^R)^{x_b} \bmod p = (g^{k - x_a R} y_a^R)^{x_b} \bmod p = (g^k (g^{x_a})^{-R} y_a^R)^{x_b} \bmod p = g^{kx_b} \bmod p$$

因此有 $g^{v'} r \bmod p = g^{(y_b{}^k)} r \bmod p = g^{(y_b{}^k)} m g^{-(y_b{}^k)} \bmod p = m$。当消息$m$恢复后，$U_b$通过方程(5)来验证签名的有效性。

$$R = h(h(m) \| r \| g^s y_a^R) \bmod q \tag{5}$$

方程(5)的正确性证明如下。

证明：

$$h(h(m) \| r \| g^s y_a^R) \bmod q = h(h(m) \| r \| g^{k - x_a R} y_a^R) \bmod q =$$
$$h(h(m) \| r \| g^k y_a^{-R} y_a^R) \bmod q = h(h(m) \| r \| g^k) \bmod q = R$$

1.4 签名的转换与验证

如果U_a否认对消息m的签名，U_b可以公布 $m' = h(m)$ 以及(r,R,s)，那么任何人都可以通过方程(6)的成立与否，来证实签名者签名的有效性。由此可见，接收者不必暴露消息明文，就可让任何验证者验证原始签名的有效性。

$$R = h(m' \| r \| g^s y_a^R) \bmod q \tag{6}$$

2 安全性分析

方案的安全性是基于密码学中两个假设：强单向hash函数的不可逆和求解离散对数的困难性，因而方案在这两个假设下是安全的。下面讨论该方案可能受到的攻击：

攻击 1　攻击者试图得到签名者或接收者的私钥。

攻击者不可能从方程(3)中得到签名者的私钥，因方程中有两个未知变量 x_a 和k，要想得到k的值，攻击者必须解决离散对数难题。同样攻击者不可能从方程(4)中得到接收者U_b的私钥。

攻击 2　攻击者试图伪造用户U_a的认证加密签名。

为了伪造一个签名满足方程(4)，攻击者首先应知道U_a和U_b共享的密钥，如 $y_{ab} (= y_a{}^{x_b} = y_b{}^{x_a} \bmod p)$，但从攻击1可知，攻击者是不可能知道$U_a$和$U_b$的私钥，也就不可能知道$U_a$和$U_b$共享的密钥，从而也就不可能伪造$U_a$的认证加密签名。

攻击 3　攻击者试图伪造转换签名。

攻击者可能会先选择参数r, R, m'，然后从方程(6)中求出s；或先选择r, s, m'从方程(6)中求出R，然而，攻击者不可能成功，除非解决了离散对数难题和单向hash函数的求逆。

攻击 4 攻击者试图从U_a的签名中恢复消息出 m。

从方程 v' 和(4)可以知，只有知道签名者或接收者的私钥，才能恢复消息m，然而从攻击1可知，攻击者不可能成功。

攻击 5 在没有转换签名前，攻击者试图验证签名。

要验证方程(6)，必须先知道消息 m'，从攻击4可知,攻击者不能求出消息m，也就不可能知道 m'，从而也就不能在转换签名前验证签名。

攻击 6 攻击者试图从转换签名中得知消息明文。

从转换签名中可知 $m' = h(m)$，要想从方程中求出m，攻击者必须解决强单向hash函数的求逆。

3 性能分析

假定T_v，T_m，T_e，T_h分别为求逆时间、模乘时间、模指数时间和求hash函数时间。$|N|$表示整数N的比特位长。方案在计算复杂性、签名的存储量与文献[5, 6]方案的比较结果如表1所示。表中，存在$|p|>|q|$，$T_e > T_m > T_v > T_h$等关系，方案的签名长度和转换签名时间与文献[6]的方案相当，但优于文献[5]的方案，在消息恢复时间和转换签名验证时间上都优于文献[5,6]的方案。因而方案在计算复杂度和存储量等方面上都是相对较优的。

表1 方案比较

	文献[5]的方案	文献[6]的方案	本文的方案
签名长度	$2\|p\|+\|q\|$	$\|p\|+2\|q\|$	$\|p\|+2\|q\|$
消息恢复时间	$5T_m+3T_e$	$3T_h+4T_m+3T_e$	$2T_m+3T_e$
转换签名时间	$2T_v+4T_m+2T_e$	0	0
转换签名验证时间	$T_v+4T_m+3T_e$	$2T_h+3T_m+2T_e$	$2T_h+T_m+2T_e$

4 结束语

在本文的方案中，接收者只需在正常的过程的恢复和验证签名的有效性，当签名者否认签名时，接收者不需签名者的合作就可单独将这认证加密方案转换为一般签名，并且不必暴露消息内容就可使任何验证者验证签名的有效性。该方案在计算复杂度和通信量方面都比较优于已有的方案。

参 考 文 献

[1] Nyberg K, Rueppel R A. A new signature scheme based on the DSA giving message recovery[R]. Proceeding of the First ACM Conf on computer and Communications Security, Fairfax, VA, 1993

[2] Horster P, Michels M, Petersen H. Authenticated encryption schemes with low communication costs[J]. Electron Letters 1994, 30(15): 1 212-1 213

[3] Lee W B, Chang C C, Yang WP. Authenticated encryption schemes without using a one way function[J]. Electron Letter, 1995, 31(19): 1 656-1 657

[4] Chen K. Authenticated encryption schemes based on Quadratic residue[J]. Electron Letter, 1998, 34(22): 2 115-2 116

[5] Araki S, Uehara S, Imamura K. The limited verifier signature and its application[J]. ICICE Transactions on Fundamentals 1999, E82-A(1): 63-68

[6] Wu T S, Hsu C L. Convertible authenticated encryption scheme[J]. Journal of System and Software, 2002, 62(6): 205-209

编 辑 漆 蓉