具有前向安全性的可公开验证的签密方案

戚明平，陈建华，何德彪
（武汉大学 数学与统计学院，武汉 430072）

摘 要：已有签密方案大多数不能同时提供可公开验证性和前向安全性。针对此问题，基于求解 Z_p 上离散对数问题的困难性和单向hash函数的不可逆性，给出了一个同时具有前向安全性和可公开验证的签密方案。在该方案中验证不需要接收者的私钥，传输中通过将某一参数隐藏在指数位置，使得到发送者私钥的攻击者不可能得到本次及以前通信者的秘密信息。通过这些方法实现了可公开验证性和前向安全性，弥补了大多数已有签密方案不能同时提供可公开验证性和前向安全性的不足，而且在该方案中认证与消息恢复并未分离，但是在公开验证过程中却无须破坏消息的机密性，这使得本方案具有更高的安全性和更广泛的应用性。

关键词：认证加密；签名；公开验证；机密性；离散对数问题；前向安全；第三方验证
中图分类号：TP309.7 **文献标志码**：A **文章编号**：1001-3695(2014)10-3093-02
doi:10.3969/j.issn.1001-3695.2014.10.051

Signcryption scheme with public verifiability and forward security

QI Ming-ping, CHEN Jian-hua, HE De-biao
(*School of Mathematics & Statistics, Wuhan University, Wuhan* 430072, *China*)

Abstract: Most of existing schemes can't simultaneously provide with public verifiability and forward security. To solve this problem, based on the difficulties of discrete logarithm problem on the cyclic group Z_p and the intractability of reversing a one—way hash function, this paper presented a public verifiable signcryption scheme with forward security. In this scheme, the verification process didn't need the sender's private key, in the transmission, a parameter (r) was hided in the index of g, so attacked who obtained the sender's private key couldn't get any secret information between these participates before this communication. By these methods the scheme achieved public verifiability and forward security and made up the short coming of most existing schemes that can't simultaneously provide with public verifiability and forward security. And furthermore, authentication and message recovery was not separated, but in the process of public verify, the message confidentiality won't be damaged, this made the scheme have higher security and more widely applications.

Key words: authenticated encryption; signature; public verify; confidentiality; discrete logarithm problem; forward security; the third party verification

0 引言

在网络通信中，传送机密消息需要同时保证消息的机密性、可认证性和完整性，实际中实现这一目标的方法是使用密码学中的认证加密方案。所谓的认证加密就是在一个逻辑步骤内同时完成数字签名和消息加密，比传统的先签名后加密所需的计算代价与通信代价要小得多，因此在电子支付、分布式协议中有着广泛的应用。1994年Horster等人[1]首次提出一个被命名为认证加密的方案，但该方案不具有公开可验证性，即只有指定的接收者才能恢复消息并对其进行签名认证，其他任何人都不能验证消息签名的有效性，于是当通信双方发生纠纷、签名者否认签名时，就无法公开验证签名的有效性以作出仲裁。Zheng[2]在1997年提出了一个新的认证加密方案称为签密(signcryption)，它是指在一个单一的逻辑步骤中，同时实现数字签名和对称加密两项功能，并且它的计算代价远比传统先签名后加密的方法低得多。然而文献[3]指出，Zheng的签名方案不具有前向安全性并且也是不能公开验证的。1999年Araki等人[4]提出了一个方案，该方案在必要时可转变为一般的签名方案以实现公开验证。文献[5]指出，在Araki方案中，签名的转变需要签名者的合作且所需额外的计算和传输代价较大，所以当签名者不合作便无法完成签名转换，因而不实用。Ma等人[6]于2003年提出一个可公开验证的认证加密方案，但文献[7,8]证明了其不具有其作者声称的任何一个安全性。之后，为解决上述方案存在的各种问题，在上述方案的基础上，一些具有低通信代价的方案[9~15]被提出。基于对上述认证加密方案的分析研究，本文提出了一个新的安全可靠的可公开验证的签密方案。

1 本文签密方案

系统参数：p 是一个大素数，q 是 $p-1$ 的一个大素因子，$g \in Z_p^*$ 是 q 阶元素，$x_a \in Z_q^*$ 是发送者Alice的私钥，$y_a = g^{x_a} \bmod p$ 是Alice的公钥。类似地，x_b 和 y_b 分别是接收者Bob的私钥和公钥，$h(\,)$ 是一个强单向散列函数，(E,D) 为安全的对称加、解密对。

1) Alice签密过程

Alice随机选取 $k \in Z_q^*$，并计算 $K = h(y_b^k \bmod p)$，然后计算

收稿日期：2013-10-30；**修回日期**：2013-12-06

作者简介：戚明平(1990-)，男，硕士研究生，主要研究方向为密码与信息安全(766247551@qq.com)；陈建华，男，教授，博导，主要研究方向为椭圆曲线密码、信息安全；何德彪，男，讲师，博士，主要研究方向为密码学、信息安全.

签名(c,R,s)：

$$c=E_K(m)$$

$$r=h(h(m),y_b,g^k \bmod p)$$

$$R=g^r \bmod p$$

$$s=k(r+x_a)^{-1} \bmod q$$

Alice 将对消息 m 的签密密文(c,R,s)发送给接收者 Bob。

2)Bob 解签密过程

Bob 收到 Alice 发来的(c,R,s)先计算：

$$K=h((y_aR)^{sx_b} \bmod p)$$

解密消息：$$m=D_K(c) \tag{1}$$

签名验证：$$R=g^{h(h(m),y_b,(y_aR)^s \bmod p)} \bmod p \tag{2}$$

若式(2)成立，则签名有效，Bob 接受秘密消息和 Alice 的签名。

式(2)的正确性证明如下：

证明 $$g^{h(h(m),y_b,(y_aR)^s \bmod p)} \bmod p=$$

$$g^{h(h(m),y_b,(gr+x_a)^s \bmod p)} \bmod p=$$

$$g^{h(h(m),y_b,g^k \bmod p)} \bmod p=$$

$$g^r \bmod p=R$$

3)第三方验证

当发生纠纷、Alice 否认给 Bob 发送过签密密文时，Bob 可公布 $m'=h(m)$ 以及(c,R,s)，那么任何人都可以通过验证等式(2)的成立与否来证实签名者的签名的有效性。由此可见，接收者 Bob 不用暴露消息明文就可以让任何验证者验证原始签名的有效性。这样既达到了签名可公开验证目的，又保障了消息的机密性不被破坏。

2 安全性分析

本文提出的认证加密方案的安全性是基于下面两个困难性假设：求解 Z_p 上的离散对数问题和单向 hash 函数的不可逆性。

1)本文所给认证加密方案满足前向安全性

证明 假设发送方 Alice 的私钥 x_a 被攻击者所获，攻击者便开始监听 Alice 和 Bob 之间的来往消息，并截获一组密文(c,R,s)，敌手想从 $s=k(r+x_a)^{-1} \bmod q$ 中解出 k，从而解得 $K=h(y_b^k \bmod p)$，可是其中 r 被隐藏在指数位置上，即 $R=g^r \bmod p$ 由 R 计算 r 须解离散对数问题，故可知敌手不能成功。另外敌手利用 $K=h((y_aR)^{sx_b} \bmod p)=h((g^{r+x_a})^{sx_b} \bmod p)=h((y_b^{r+x_a})^s \bmod p)$来求解 K，此时仍然面临求解 r 的问题，由此知敌手依然不能成功，因此本方案具有前向安全性，即使签名密钥被遗漏，也不会影响到密钥遗漏之前所生成的签密密文的安全性。

2)本方案满足不可伪造性

若攻击者想伪造签名密文(c',R',s')使 Bob 验证等式(2)成立，则其要由签密过程中的方程解出某些参数，而要求解这些方程必然会遇到求解离散对数问题或者是单向 hash 函数求逆的问题，显然这是不可能的。

3)本方案满足机密性

攻击者试图恢复消息 m，一方面可从等式 $m=D_k(c)$ 入手，这就需要求出秘密参数 k，而要求出 k 就面临着求解离散对数问题，这是不可能的；另一方面，可从等式 $m'=h(m)$ 入手，这就需要解决单向 hash 函数求逆的问题，这也是不可能的。因此，本方案满足机密性。

4)本方案满足不可否认性，即本方案是可公开验证的

不可否认性是指签密消息的发送者不能否认他曾经发送过的签密消息。也就是说，第三方可以在安全可信的基础上证明发送方的确发送过这个消息，并且在证明的过程中消息接收者无须泄露自己的私钥，便可实现签密方案的不可否认性证明。在本文的签密方案中，当发生纠纷、Alice 否认给 Bob 发送过签密密文时，Bob 可将 $m'=h(m)$ 以及(c,R,s)发送给任意第三方验证，第三方通过计算 $r=h(m',y_b,(y_aR)^s \bmod p)$然后再验证 $R=g^r \bmod p$ 是否成立来作出判断。显然，验证过程中无须明文 m 和接收者的私钥。因此，该签密方案可公开验证，并且验证时不会破坏消息的机密性。

3 结束语

可转变认证加密方案是为了解决认证加密中的公开验证问题提出的。当出现纠纷、签名者否认自己的签名时，可将可转变认证加密方案中的签名转变为一般签名来实现公开验证。但当消息的机密性不容破坏时，已有文献的大多数方案就不再适用。本文提出的认证加密方案恰好弥补了这方面的不足：一方面它可广泛地运用于当一个签名者想对签名的消息对公众保密，例如从银行进行电子支付，并且该支付对其他人是保密的；另一方面当通信双方发生纠纷时，接收者可以在不破坏消息机密性的前提下实现公开验证。同时，本方案具备前向安全性，这在一定程度上强化了签密方案的安全性能。

参考文献：

[1] HORSTER P, MICHEL M, PETERSEN H. Authenticated encryption schemes with low communication costs[J]. Electronics Letters, 1994, 30(15):1212-1213.

[2] ZHENG Yu-liang. Signcryption and its applications in efficient public key solutions [C] //Proc of International, Information Security Workshop. Berlin: Springe-Verlag, 1997: 291-312.

[3] 张申绒,张彤,肖国镇. 前向安全可公开验证签名方案[J]. 计算机工程与应用,2006,42(21): 103-104.

[4] ARAKI S, UEHARA S, IMAMURA K. Convertible limited verifier signature based on horster's authenticated encryption[C]//Proc of Symposium on Cryptography and Information Security. 1998: 32-36.

[5] WU T S, HSU C L. Convertible authenticated encryption scheme[J]. The Journal of Systems and Software, 2002, 62(3):205-209.

[6] MA Chang-she, CHEN Ke-fei. Publicly verifiable authenticated encryption[J]. Electronics Letters,2003,39(3):281-282.

[7] SHAO Zu-hua. Cryptanalysis of publicly verifiable authenticated encryption[EB/OL]. (2003-09-09)[2005-04-22]. http://eprint.iacr.org/2003/189/.pdf.

[8] WANG Gui-lin, FENG Bao, MA Chang-she, *et al*. Efficient authenticated encryption with public verifiability[C]//Proc of the 60th IEEE Vehicular Technology Conference on Wireless Technologies for Global Security. 2004: 3258-3261.

[9] 甘元驹,彭银桥,施荣华. 一种有效的可转换的认证加密方案[J]. 电子科技大学学报,2005,34(2):172-174.

[10] 张申绒,傅晓彤,肖国镇. 对两个可转变认证加密方案的分析和改进[J]. 电子与信息学报,2006,28(1):151-153.

[11] 李艳平,张京良,王玉民. 改进的前向安全的认证加密方案[J]. 东南大学学报:自然科学版,2007,37 (S1):20-23.

[12] 于永,慕朝晖. 一种基于前向安全的可公开验证签密方案[J]. 计算机应用与软件,2010,27(1):284-285.

[13] 张建航,胡予濮,齐新社. 具有前向安全性和公开可验证性的签密方案[J]. 计算机应用研究,2011,28(2):733-734,737.

[14] 黎仁峰. 混合签密体制的设计与实现[D]. 成都:电子科技大学,2013.

[15] 雷咏,杨世平. 基于 PKI 的签密体制[J]. 通信技术,2013,46(1):43-46.