# 一个可公开验证签密方案的密码分析和改进

张串绒[1,2], 肖国镇[1]
(1. 西安电子科技大学综合业务网国家重点实验室, 陕西西安 710071; 2. 空军工程大学电讯工程学院, 陕西西安 710077)

摘 要: 对 Lee等提出的可公开验证签密方案进行了密码分析和改进. 研究了 Lee方案的机密性和不可否认性, 发现 Lee方案的公开验证过程是以泄漏消息的机密性为代价的. 提出对 Lee方案的一个修改方案, 修改方案克服了 Lee方案中存在的安全漏洞, 是一个安全的可公开验证签密方案. 该修改方案的给出有助于"设计可公开验证签密方案"这一公开问题的尽快解决.

关键词: 签密; 认证加密; 公开验证; 机密性
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2006) 01-0177-03

# Cryptanalysis and Improvement of a Signcryption Scheme with Public Verifiability

ZHANG Chuan-rong[1,2], XIAO Guo-zhen[1]
(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Shaanxi, Xi'an 710071, China;
2. Telecom Eng. Institute, Air force Engineering Univ., Shaanxi, Xi'an 710077, China)

**Abstract** Lee's signcryption scheme with public verifiability is cryptoanalyzed and improved. By studying the confidentiality and non-repudiation of Lee's scheme, the fact that the confidentiality of Lee's scheme is lost during its public verification is found. Lee's scheme is modified, and the modification overcomes the security problem in Lee's scheme. So the modified scheme is a security signcryption scheme with public verifiability and it is of great benefit to solve the open problem "design signcryption schemes with public verifiability".

**Key words** signcryption; authenticated encryption; public verify; confidentiality

## 1 引言

数字签名和加密是密码学的两个基本而重要的功能, 其中数字签名具有提供消息完整性、认证性和不可否认性的功能, 而加密则可以提供消息的机密性. 以往, 签名和加密是分开应用的, 然而随着信息传输的网络化, 网上传输的信息往往同时需要认证和加密. 传统上, 实现同时认证和加密的方法是"先签名再加密", 但这种方法计算和传输代价是加密和签名代价的总和, 代价较高. 为了降低代价, 1997年, Zheng[1]提出了签密 (signcryption)的概念, 并给出了两个具体的签密方案. 这两个签密方案能在一个合理的逻辑步骤内同时实现加密和认证两项功能, 且其代价远远低于传统方法. 然而, 由于在签密过程中, 被签密的消息在签名的同时也被加密, 就不能像一般签名那样被公开验证. 随后提出的签密方案, 如文献[2, 3]中的与 Zheng的签密方案一样, 都不具备公开验证功能. 而在如今开放网络 (如 Internet)上的通信、电子商务、电子政务等实际应用中公开验证又是必不可少的. 1998年, 文献[4]以 Zheng的签密方案为基础, 提出了一种签名可公开验证的签密方案 - BD签密方案, 但该方案依然存在效率和安全问题. 为了进一步解决签密的公开验证难题, 2000年, 文献[6]基于 BD方案和文献[5]中的认证加密方案提出了一种可公开验证的签密方案, 简称 Lee方案. 本文对 Lee方案进行密码分析研究, 发现了其中存在的安全问题, 并给出了一个改进方案.

## 2 Lee方案

方案中系统参数 $p$ 是一个大素数, $q$ 是 $p-1$的一个大的素因子, $g\in Z_p^*$ 是 $q$阶元素, $x_a\in Z_q$ 和 $y_a=g^{x_a} \bmod p$ 是 Alice的公钥对, 类似地, $x_b$ 和 $y_b$ 是 Bob的公钥对, $hash$ 是一个单向散列函数, $\|$ 表示级联. 设 Alice要认证加密的发送消息 $m\in Z_p^*$ 给 Bob, 那么, Alice随机选取整数 $k\in Z_q^*$, 计算 $K_1=hash(g^k \bmod p)$, $K_2=hash(y_b^k \bmod p)$, $c=(m\|hash(m\|K_2))K_1K_2 \bmod p$, $s=(k-x_a c)\bmod q$ 并发送 $(c, s)$给 Bob. Bob 接收到 $(c, s)$ 后, 计算 $g^k \bmod p=g^s y_a^{c \bmod q} \bmod p$, $K_1=hash(g^k \bmod p)$, $K_2=hash((g^k)^{x_b} \bmod p)$, $m'$

收稿日期: 2005-03-25; 修回日期: 2005-07-26
基金项目: 国家自然科学重大项目基金 (No. 90104005); "十五"通信预研项目基金 (No. 41001040102)

$= cK_1K_2 \bmod p$, 并验证 $m' = m \| hash(m \| K_2)$. 当出现纠纷时, Bob将 $(K_2, c, s)$给第三方, 第三方计算 $g^k \bmod p = g^s y_a^{c \bmod q} \bmod p$, $K_1 = hash(g^k \bmod p)$, $m' = cK_1K_2 \bmod p$, 验证 $m' = m \| hash(m \| K_2)$.

## 3 Lee方案的安全性分析

一般地, 签密方案应具备机密性、不可伪造性和不可否认性的安全要求[1], Lee方案的不可伪造性是有保证的[6], 下面就其它两个性质进行逐一分析.

### 3.1 关于Lee方案的机密性

就机密性问题, Lee等认为, 除了预定的接收者 Bob外, 其他任何人不可能从 Bob的公钥中恢复出 Bob的私钥, 且也只有接收者 Bob可以恢复出 $K_2$, 因此 Lee方案的安全条件和原 ElGamal加密体系相同, 从而 Lee方案的机密性与原 ElGamal加密体系的相同. 关于这点, 本文认为 Lee等的说法欠妥. 原 ElGamal加密体系仅仅是用于加密目的的, 没有认证的要求, 而 Lee方案是认证加密方案, 它不仅要实现加密还要实现认证, 机密性不仅要体现在加密过程中, 当然也体现在认证过程中, 即认证过程应同样确保秘密信息的不可泄漏. 在 Lee方案中, $K_2$ 显然是保证被签密消息机密性的关键. 然而, 在公开验证阶段却将 $K_2$ 给了第三方. 知道 $K_2$ 的任何人都可算出 $m'$, 从而知道消息 $m$, 因此消息的机密性在这种公开验证中丧失了. 可见 Lee方案的公开验证是以丧失消息机密性为代价的.

### 3.2 关于Lee方案的不可否认性

Lee等在文献[6]中说, 一旦 Bob解密和验证了 $(c, s)$, 任何人可验证 $(K_2, c, s)$的有效性, 因此, 第三方在不知道 Bob的私钥, 也不需用零知识协议的情况下, 解决 Alice和 Bob之间的纠纷在计算上是可能的. 其意思是 Lee方案是可以公开验证的, 因此也是不可否认的. 然而如上所述, Lee方案的公开验证存在严重问题, 该方案的公开验证是失败的, 因此不可否认性也就不能得以实现.

## 4 改进方案

基于 Lee方案机密性和不可否认性问题, 本文提出了对 Lee方案的如下修改方案. 修改方案中的参数 $(E_K, D_k)$是安全的对称加解密算法对, 其余参数与 Lee方案中的相同.

Alice随机选取整数 $k \in Z_q^*$, 计算 $K_1 = hash(g^k \bmod p)$, $K_2 = hash(y_b^k \bmod p)$, $c = E_{K_2}(m)$, $r = hash(K_1, c \bmod p)$和 $s = (k - x_a r) \bmod q$ 并发送 $(c, r, s)$给 Bob. Bob收到 $(c, r, s)$后, 计算 $g^k \bmod p = g^s y_a^r \bmod p$, $K_1 = hash(g^k \bmod p)$, $K_2 = hash((g^k)^{x_b} \bmod p)$, 恢复消息 $m = D_{K_2}(c)$, 并验证 $r = hash(K_1, c \bmod p)$.

当出现纠纷, Alice否认自己的签密时, Bob将 $(c, r, s)$给第三方验证. 第三方计算 $K_1 = hash(g^s y_a^r \bmod p)$, 验证 $r = hash(K_1, c \bmod p)$即可.

修改方案以简捷的逻辑结构实现了机密性、不可伪造性和不可否认性, 是一个安全的可公开验证签密方案. 其签名用的是 Schnorr算法, 而 Schnorr签名是可证明安全的, 这也就是说没有人(包括 Bob)能伪造消息 $m$ 的有效签密密文 $(c, r, s)$, 使得 $m = D_{K_2}(c)$, $r = hash(K_1, c \bmod p)$, 其中 $K_1 = hash(g^s y_a^r \bmod p)$, $K_2 = hash((g^s y_a^r)^{x_b} \bmod p)$. 不然的话, Schnorr签名就可伪造. 关于机密性, 除了 Bob, 其他任何人不能从 $(c, r, s)$得到消息, 因为除了 Bob没有人能算出 $K_2$(包括公开验证中). 修改方案也实现了不可否认性, 因为只有 Alice可生成有效的签密密文 $(c, r, s)$, 这点可进行公开验证. 关于效率问题, 除了传输量比 Lee方案仅多了一个 $|hash(\cdot)| = 160$比特, 计算量完全相同. 特别地, 在如上修改方案中, 如果将可由公开信息计算出的 $K_1$ 与 $(c, r, s)$一并给接收者 Bob及第三方验证者, 就可以很小的传输代价换取计算代价的显著提高, 这在特殊的应用环境, 尤其当终端具有较小的计算能力时很适宜.

## 5 结束语

签密作为实现认证加密的一种新技术, 具有高效性的特点, 然而由于签密中被签密的消息在签名的同时也被加密, 由此带来的公开验证问题是急待解决的. 继 Lee方案之后, 文献[7]和[8]也分别提出两个可公开验证的签密方案. 但与 Lee方案类似, 这两个方案的公开验证过程违背了签密的机密性要求. 因此本文给出的 Lee方案的改进方案填补了目前已有可公开验证签密方案的安全漏洞. 该改进方案是一个安全的可公开验证的签密方案, 它的提出有助于"设计可公开验证签密方案"这一公开问题的尽快解决.

参考文献:


[1] Y L Zheng. Signcryption and its applications in efficient public key solutions[A]. LNCS 1397, in Information Security Workshop (ISW'97)[C]. Berlin: Springer-Verlag, 1998. 291-312.

[2] H Petersen, M Michels. Cryptanalysis and improvement of signcryption schemes[J]. IEE Proceedings-Computers and Digital Techniques, 1998, 145(2): 149-151.

[3] W H He, T C Wu. Cryptanalysis and improvement of Petersen-michels signcryption scheme[J]. IEE Proceedings-Computers and Digital Techniques, 1999, 146(2): 123-124.

[4] F Bao, R H Deng. A signcryption scheme with signature directly veriable by public key[A]. LNCS 1431, in PKC'98[C]. Berlin: Springer-Verlag, 1998. 55-59.

[5] P Horster, M Michels, H Petersen. Authenticated encryption schemes with low communication costs[J]. Electronics Letters, 1994, 30(15): 1212-1213.

[6] Mun Kyu Lee, Dong Kyue Kim, Kunsoo Park. An authenticated encryption scheme with public verifiability[A]. 5th Japan-Korea Joint Workshop on Algorithms and Computation[C]. Tokyo, Japan, 2000. 49-56.

[7] D Yum, P Lee. New signcryption schemes based on KCDSA[A]. LNCS 2288, in the 4th International Conference on Information Security and Cryptology[C]. Berlin: Springer-Verlag, 2001. 341-354.

[8] Jun Shin, Kwangsu Lee, Kyungah Shim. New DSA-verifiable signcryption schemes[A]. LNCS 2587, Jun-BICISC 2002[C]. Berlin: Heidelberg: Springer-Verlag, 2003. 35-47.

作者简介:

张串绒　女, 1965年生于陕西眉县, 博士生, 副教授, 现于空军工程大学电讯工程学院任教; 主要研究方向为密码学和信息安全.
E-mail: c. r. zhang@126.com或
crzhang@mail.xidian.edu.cn.

肖国镇　男, 1934年生于吉林四平, 教授, 博导; 主要从事密码学、信息安全等方面的教学与研究.