第 38 卷 第 24 期
Vol.38 No.24

计 算 机 工 程
Computer Engineering

2012 年 12 月
December 2012

• 安全技术 •

文章编号：1000—3428(2012)24—0108—03 文献标识码：A 中图分类号：TP309.2

一种基于身份的签名方案密码分析与改进

黄 斌[1]，史 亮[2]，邓小鸿[3]

(1. 莆田学院电子信息工程学系，福建 莆田 351100；2. 厦门大学软件学院，福建 厦门 361005；
3. 中南大学信息科学与工程学院，长沙 410083)

摘 要：对李继国等人提出的基于身份的高效签名方案(计算机学报，2009 年第 11 期)进行分析，以一个具体的攻击方法，证明任何攻击者都可以伪造任意消息关于任意身份的有效签名，因此方案不满足存在不可伪造性。通过将原方案中签名的一个分量值固定，并将其作为用户的公钥，使方案在保证效率的同时，满足存在不可伪造性。

关键词：密码学；基于身份的签名方案；数字签名；双线性对；密码分析

Cryptanalysis and Improvement of an Identity-based Signature Scheme

HUANG Bin[1], SHI Liang[2], DENG Xiao-hong[3]

(1. Department of Electronic Information Engineering, Putian University, Putian 351100, China;
2. School of Software, Xiamen University, Xiamen 361005, China;
3. School of Information Science and Engineering, Central South University, Changsha 410083, China)

【Abstract】This paper concludes that the efficient identity-based signature scheme proposed by Li Jiguo et al is insecure, and gives an attack method, which shows that any attacker can forge a valid signature on any message with respect to any identity. Therefore, Li Jiguo's scheme does not satisfy existential unforgeability. By making a component of a signature as user's public key, an improved scheme is proposed, which does not reduce the efficiency of Li Jiguo et al's scheme while satisfying the existential unforgeability.

【Key words】cryptography; identity-based signature scheme; digital signature; bilinear pairings; cryptanalysis

DOI: 10.3969/j.issn.1000-3428.2012.24.026

1 概述

在传统的公钥密码系统中，用户的公钥和该用户的身份之间的关系是通过证书来绑定的，这就带来了证书的管理问题。为了解决该问题，文献[1]提出了基于身份的密码体制。在这种体制中，用户的公钥是由其身份确定的，如 IP 地址或者 E-mail 地址。文献[2]利用 Weil 配对技术提出了第 1 个安全、实用的基于身份的加密方案。然而，该方案只是在随机预言机模型下可证安全的。由于在随机预言机模型下的方案安全性不高，因此构造标准模型下安全的基于身份的密码体制变得非常迫切。文献[3]构造了 2 种在标准模型下安全的基于身份的加密方案，但是方案的效率较低。第 1 个在标准模型下安全的基于身份的高效加密方案是由文献[4]提出的。

在基于身份的签名方面，文献[5]在 Waters 方案的基础上提出了一个标准模型下安全的基于身份的高效签名方案。在该方案的基础上，文献[6]给出了一个更加高效的基于身份的签名方案(下文记为 Li-Jiang 方案)。该方案已广泛应用于一些基于身份的签名方案中，如文献[7-10]的签名方案都以 Li-Jiang 方案为基础的。

本文分析指出 Li-Jiang 方案是不安全的，即攻击者在从未得到任何密钥的情况下，也可以容易地伪造任意消息关于任意身份的有效签名。此外，本文也给出了 Li-Jiang 方案的改进。改进方案不仅满足签名的存在不可伪造性，而且效率与原方案相同。

2 预备知识

2.1 双线性对

令 G、G_T 是 2 个阶均为素数 p 的循环群，定义双线性对为满足以下 3 个性质的映射 $e:G\times G\to G_T$：

(1)双线性性

如果 $a,b\in\mathbb{Z}_p^*$ 且 $g,h\in G$，则 $e\left(g^a,h^b\right)=e\left(g,h\right)^{ab}$。

基金项目：国家自然科学基金资助项目(61103202)；福建星火科技基金资助项目(2010S0017)；莆田市科技基金资助项目(2009G26, 2011G04(2))；瞬态光学与光子技术国家重点实验室 2011 年度开放基金资助项目(SKLST201113)

作者简介：黄 斌(1981－)，男，讲师、硕士，主研方向：信息安全；史 亮，副教授、博士；邓小鸿，博士研究生

收稿日期：2012-02-29 **修回日期：**2012-04-24 **E-mail：**huangbinpt@163.com

(2)非退化性

存在 $g,h\in G$，使得 $e(g,h)\neq 1$。

(3)可计算性

对任意 $g,h\in G$，存在有效算法计算 $e(g,h)$。

2.2 基于身份的签名方案

按照文献[6]的定义，基于身份的签名方案由以下 4 个多项式时间算法构成：

(1)系统建立(Setup)

输入系统安全参数，PKG 产生系统公开参数 *params* 和主密钥 *msk*，然后 PKG 公开 *params*，但保密 *msk*。

(2)密钥提取(Extract)

给定用户身份 u，PKG 利用主密钥 *msk* 计算用户的密钥 d_u，然后 PKG 将 d_u 通过安全通道发给用户。

(3)签名(Sign)

用户得到密钥后，首先验证密钥的正确性。如果密钥通过验证，则签名人 u 利用其密钥 d_u 产生消息 m 的签名 σ。

(4)验证(Verify)

验证者利用系统公开参数 *params* 和签名人的身份 u 对消息 m 的签名 σ 进行验证。

3 Li-Jiang 方案简介

Li-Jiang 方案[6]的具体描述如下：

(1)系统建立(Setup)

令 G、G_T 是 2 个阶为 p 的循环群，g 为 G 的生成元，$e:G\times G\to G_T$ 是一个双线性映射。

首先，PKG 随机选择 2 个单向哈希函数：

$H_1:\{0,1\}^*\to\{0,1\}^{n_u}$

$H_2:\{0,1\}^*\to\{0,1\}^{n_m}$

以及 $a\in\mathbb{Z}_p$、$g_2\in G$，并计算：

$g_1=g^a$

然后，PKG 随机选择 $u'\in\mathbb{Z}_p$、$m'\in G$、n_u 维的向量 $\boldsymbol{U}_v=(u_i)$ 以及 n_m 维的向量 $\boldsymbol{M}_v=(m_i)$，其中，$u_i\in\mathbb{Z}_p$；$m_i\in G$，令：

$z_1=e(g_1,g_2)$

$z_2=e(g,g_2)$

最后，PKG 公开系统参数：

$params=(p,g,g_1,g_2,u',U_v,m',M_v,z_1,z_2)$

并保密系统主密钥 $msk=a$。

(2)密钥提取(Extract)

假定用户的身份 u 是一个长度为 n_u 的比特串(可以用哈希函数 H_1 来实现)，U 是 u 中比特值为 1 的位置的集合。PKG 随机选择 $t\in\mathbb{Z}_p$，计算用户的密钥：

$$d_u=(d_0,d_1)=\left(g_2^{a+t(u'+\sum_{i\in U}u_i)},z_2^t\right)$$

并通过安全信道把密钥发给用户。如果：

$$a+t(u'+\textstyle\sum_{i\in U}u_i)=0 \bmod p$$

则 PKG 返回步骤(1)，重新选择主密钥 a。

(3)签名(Sign)

用户得到密钥 d_u 后，首先对密钥的正确性进行验证：

$$e(g,d_0)=z_1\cdot d_1^{u'+\sum_{i\in U}u_i}$$

如果等式成立，则用户可以确认该密钥是由 PKG 产生的；否则，用户重新向 PKG 询问密钥。如果密钥验证通过，则用户可以对消息签名。假定消息 m 是一个长度为 n_m 的比特串(可以用哈希函数 H_2 来实现)，M 是 m 中比特值为 1 的位置的集合。用户随机选择 $s\in\mathbb{Z}_p$，计算消息 m 的签名为：

$$\sigma=(w,x,y)=\left(d_0\cdot\left(m'\textstyle\prod_{j\in M}m_j\right)^s,g^s,d_1\right)$$

(4)验证(Verify)

验证者用系统公开参数 *params* 和身份 u 对消息 m 的签名 σ 进行验证。如果等式：

$$e(g,w)=z_1\cdot y^{u'+\sum_{i\in U}u_i}\cdot e\left(x,m'\textstyle\prod_{j\in M}m_j\right)$$

成立，则签名有效；反之，签名无效。

本文方案的密钥验证算法和签名验证算法的正确性验证过程如下：

(1)密钥的正确性验证

$$e(g,d_0)=e\left(g,g_2^{a+t(u'+\sum_{i\in U}u_i)}\right)=$$
$$e\left(g,g_2^a\right)\cdot e\left(g,g_2^{t(u'+\sum_{i\in U}u_i)}\right)=z_1\cdot d_1^{u'+\sum_{i\in U}u_i}$$

(2)签名的正确性验证

$$e(g,w)=e\left(g,d_0\cdot\left(m'\textstyle\prod_{j\in M}m_j\right)^s\right)=$$
$$e(g,d_0)\cdot e\left(g,\left(m'\textstyle\prod_{j\in M}m_j\right)^s\right)=$$
$$z_1\cdot d_1^{u'+\sum_{i\in U}u_i}\cdot e\left(g^s,m'\textstyle\prod_{j\in M}m_j\right)=$$
$$z_1\cdot y^{u'+\sum_{i\in U}u_i}\cdot e\left(x,m'\textstyle\prod_{j\in M}m_j\right)$$

4 Li-Jiang 方案的分析和改进

下面先给出一个针对 Li-Jiang 方案的攻击方法，证明该方案是不安全的，然后对该方案进行改进。虽然文献[6]声称 Li-Jiang 方案在自适应选择消息攻击下是存在不可伪造的，但是本文发现该方案甚至不满足签名方案基本的存在不可伪造性。事实上，在该方案中，任何攻击者即使在从未得到任何合法密钥的情况下也可以伪造任意消息关于任意身份的有效签名。具体攻击方法如下：

假设攻击者从未得到任何其他消息的合法签名，他希望伪造消息 m^* 关于身份 u^* 的签名，则可以按照如下过程伪造签名：

(1)选择 2 个随机元素 $w^*,x^*\in G$。

(2)令 U^* 和 M^* 分别为 u^*、m^* 中比特值为 1 的位置的集合，计算：

$b=u'+\sum_{i\in U^*}u_i$

$c=e\left(x^*,m'\prod_{j\in M^*}m_j\right)$

其中，b 是正整数。

(3)计算：

$$y^*=\sqrt[b]{e\left(g,w^*\right)\cdot z_1^{-1}\cdot c^{-1}}$$

(4)输出签名:

$\sigma^* = \left(w^*, x^*, y^*\right)$

由于:

$$z_1 \cdot \left(y^*\right)^{u'+\sum_{i\in U^*} u_i} \cdot e\left(x^*, m'\prod_{j\in M^*} m_j\right) = z_1 \cdot \left(y^*\right)^b \cdot c = z_1 \cdot e\left(g, w^*\right) \cdot z_1^{-1} \cdot c^{-1} \cdot c = e\left(g, w^*\right)$$

即:

$$e\left(g, w^*\right) = z_1 \cdot \left(y^*\right)^{u'+\sum_{i\in U^*} u_i} \cdot e\left(x^*, m'\prod_{j\in M^*} m_j\right)$$

因此攻击者输出的签名:

$\sigma^* = \left(w^*, x^*, y^*\right)$

是有效的，也就是说 Li-Jiang 签名方案不满足存在不可伪造性。

分析发现，导致该方案存在安全漏洞的原因是:

$b = u' + \sum_{i\in U^*} u_i$

是一个正整数。在已知 $e\left(g, w^*\right) \cdot z_1^{-1} \cdot c^{-1}$ 和 b 后，容易得到:

$y^* = \sqrt[b]{e\left(g, w^*\right) \cdot z_1^{-1} \cdot c^{-1}}$

使之满足:

$\left(y^*\right)^b = e\left(g, w^*\right) \cdot z_1^{-1} \cdot c^{-1}$

即:

$e\left(g, w^*\right) = z_1 \cdot \left(y^*\right)^b \cdot c$

为了抵抗本文提出的攻击方法，可以改变用户密钥的生成方式，将其由指数形式改为乘法形式，即将 $g_2^{a+t\left(u'+\sum_{i\in U} u_i\right)}$ 改为 $g_2^a \cdot \left(u'\prod_{i\in U} u_i\right)^t$，相应地，$u', \boldsymbol{U}_v \in G$。但这种改进降低了 Li-Jiang 方案的效率。进一步分析发现，如果令 d_1 为用户公钥的一部分，签名验证等式保持不变，则由 $y = d_1$ 可得新的签名为 $\sigma = (w, x)$。此时，由于 y 为一固定值，因此上述攻击方法失效。同时，由于改进方案只需简单地将 d_1 作为用户公钥的一部分而公开，其他步骤不变，因此方案效率与原方案相同。

5 结束语

基于身份的签名方案是目前的一个研究热点。本文分析指出文献[6]提出的基于身份的高效签名方案是不安全的，因此，使用该方案的其他方案[7-10]也是不安全的。在此基础上对该方案进行改进，使其在满足安全性的同时效率不变。

参考文献

[1] Shamir A. Identity-based Cryptosystems and Signature Schemes[C]//Proceedings of CRYPTO'84. Berlin, Germany: Springer-Verlag, 1985: 47-53.

[2] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[C]//Proceedings of CRYPTO'01. Berlin, Germany: Springer-Verlag, 2001: 213-229.

[3] Boneh D, Boyen X. Efficient Selective-ID Secure Identity-based Encryption Without Random Oracles[C]//Proceedings of EUROCRYPT'04. Berlin, Germany: Springer-Verlag, 2004: 223-238.

[4] Waters B. Efficient Identity-based Encryption Without Random Oracles[C]//Proceedings of EUROCRYPT'05. Berlin, Germany: Springer-Verlag, 2005: 114-127.

[5] Paterson K, Schuldt J. Efficient Identity-based Signatures Secure in the Standard Model[C]//Proceedings of ACISP'06. Berlin, Germany: Springer-Verlag, 2006: 207-222.

[6] 李继国, 姜平进. 标准模型下可证安全的基于身份的高效签名方案[J]. 计算机学报, 2009, 32(11): 2130-2136.

[7] 于义科, 郑雪峰. 标准模型下基于身份的高效动态门限代理签名方案[J]. 通信学报, 2011, 32(8): 55-63.

[8] 于义科, 郑雪峰, 韩晓光, 等. 一种标准模型下基于身份的高效门限代理签名方案[J]. 计算机应用研究, 2011, 28(3): 1136-1141.

[9] 冀会芳, 韩文报, 刘连东. 新的标准模型下基于身份的代理签名方案[J]. 计算机科学, 2011, 38(8): 88-91.

[10] 李 聪, 闫德勤, 郑宏亮. 标准模型下高效安全的基于身份多签密方案[J]. 计算机应用, 2012, 32(4): 957-959.

编辑 张 帆

(上接第 107 页)

参考文献

[1] Elias P, Feinstein A, Shannon C E. A Note on the Maximum Flow Through a Network[J]. IRE Trans. on Information Theory, 1956, 2(4): 117-119.

[2] Ahlswede R, Cai N, Li S Y R, et al. Network Information Flow[J]. IEEE Trans. on Information Theory, 2000, 46(1): 1204-1216.

[3] Wu Y, Chou P A, Kung S Y. Information Exchange in Wireless Networks with Network Coding and Physical Layer Broadcast[R]. Redmond, USA: Microsoft Research, Technical Report: MSR-TR-2004-78, 2004.

[4] Zhang S, Liew S C, Lam P. Physical-layer Network Coding[C]// Proc. of the 12th Annual International Conference on Mobile Computing and Networking. New York, USA: [s. n.], 2006: 358-365.

[5] Zhang S, Liew S C, Lam P. On the Synchronization of Physical-layer Network Coding[C]//Proc. of the 2006 IEEE Information Theory Workshop. [S . 1.]: IEEE Press, 2006: 404-408.

[6] Ong L, Kellett C M, Johnson S J. Capacity Theorems for the AWGN Multi-way Relay Channel[J]. IEEE Transactions on Information Theory, 2012, 58(9): 5761-5769.

[7] Make D. Paired Carrier Multiple Access(PCMA) for Satellite Communications[C]//Proc. of Pacific Telecommunications Conference. Honolulu, USA: [s. n.], 1998: 787-791.

[8] 吕 凌, 于宏毅. 物理层网络编码分组的机会中继[J]. 电子与信息学报, 2009, 3(7): 1767-1770.

[9] Katti S, Gollakota S, Katabi D. Embracing Wireless Interference: Analog Network Coding[C]//Proc. of ACM SIGCOM'07. Kyoto, Japan: ACM Press, 2007.

[10] Gacanin H, Adachi F. Broadband Analog Network Coding[J]. IEEE Trans. on Wireless Communication, 2010, 9(5): 1577-1583.

编辑 索书志