

## 一个高效的基于身份签名方案的安全性分析

杨小东<sup>1,2</sup>, 肖立坤<sup>1</sup>, 李雨桐<sup>1</sup>, 陈春霖<sup>1</sup>, 王彩芬<sup>1</sup>

(1. 西北师范大学 计算机科学与工程学院, 兰州 730070; 2. 密码科学技术国家重点实验室, 北京 100878)

**摘 要:** 黄一才等人(密码学报, 2017年第5期)提出一个高效的基于身份签名方案, 并采用混合游戏的方法在标准模型中证明该签名方案是强不可伪造, 其安全性依赖于CDH假设。但是方案的安全性证明存在严重的安全缺陷。为分析该方案的安全性, 构造一个多项式时间区分算法, 以不可忽略的概率区分模拟签名与真实签名的概率分布, 表明模拟游戏和真实游戏是可区分的, 从而说明黄一才方案不能正确地证明该方案是强不可伪造的。设计一个多项式时间算法输出该方案的伪造签名, 挑战者无法利用伪造的签名求解CDH问题。安全性分析结果表明, 该方案的安全性并不能归约到CDH假设, 将其安全性归约到CDH假设的结论是错误的。

**关键词:** 基于身份签名; 可证明安全; 混合游戏; 强不可伪造; 安全性分析

**中文引用格式:** 杨小东, 肖立坤, 李雨桐, 等. 一个高效的基于身份签名方案的安全性分析[J]. 计算机工程, 2018, 44(11): 115-118.

**英文引用格式:** YANG Xiaodong, XIAO Likun, LI Yutong, et al. Security analysis of an efficient identity-based signature scheme[J]. Computer Engineering, 2018, 44(11): 115-118.

## Security Analysis of An Efficient Identity-Based Signature Scheme

YANG Xiaodong<sup>1,2</sup>, XIAO Likun<sup>1</sup>, LI Yutong<sup>1</sup>, CHEN Chunlin<sup>1</sup>, WANG Caifen<sup>1</sup>

(1. College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China;

2. State Key Laboratory of Cryptology, Beijing 100878, China)

**[Abstract]** HUANG Yicai et al (Journal of Cryptologic Research, No. 5, 2017) proposes an efficient identity-based signature scheme, which uses a hybrid game approach to prove that the scheme is strongly unforgeable in a standard model, and its security depends on the Computational Diffie-Hellman (CDH) hypothesis. However, the security of the scheme proves that there are serious security flaws. In order to analyze the security of the scheme, a polynomial-time distinguishing algorithm is constructed to distinguish the probability distribution of simulated signatures from that of real signatures with a non-negligible probability, which indicates that the simulated game and the real game are distinguishable. Therefore, the security proof of the scheme can not prove that the scheme is strong and unfalsifiable. Designing a polynomial time algorithm to output the forged signature of the scheme, the challenger cannot use the forged signature to solve the CDH problem. Security analysis results show that the security of the scheme cannot be reduced to the CDH hypothesis, and the conclusion that the security is reduced to the CDH hypothesis is wrong.

**[Key words]** identity-based signature; provable security; hybrid game; strong unforgeability; security analysis

**DOI:** 10.19678/j.issn.1000-3428.0050253

### 0 概述

在基于身份签名的方案中, 用户的公钥是 Email 地址、电话号码等唯一的身份信息, 而相应的私钥由一个可信的密钥生成中心 (Private Key Generator, PKG) 产生。由于基于身份签名无需数字证书来验证公钥的正确性和用户身份的真实性, 从而解决了传统签名中数字证书的管理和分发开销问题, 因此

被广泛应用于体域网、无线通信等领域<sup>[1]</sup>。

文献[2]提出了基于身份密码体制的思想。文献[3]提出了一个在随机预言模型下安全的基于身份的签名方案。然而, 当用具体的哈希函数实例化理想的预言机时, 在随机预言模型中的安全方案在现实中并不一定是安全的。文献[4]提出了无随机预言机的基于身份签名方案, 其安全性在标准模型中依赖于 CDH (Computational Diffie-Hellman) 假设。

**基金项目:** 国家自然科学基金 (61662069, 61562077); 中国博士后科学基金 (2017M610817); 甘肃省科技计划项目 (1506RJZA130); 兰州市科技计划项目 (2013-4-22); 西北师范大学青年教师科研能力提升计划项目 (NWNNU-LKQN-14-7)。

**作者简介:** 杨小东 (1981—), 男, 副教授、博士后, 主研方向为代理重签名; 肖立坤、李雨桐、陈春霖, 硕士研究生; 王彩芬, 教授、博士。

**收稿日期:** 2018-01-23 **修回日期:** 2018-03-21 **E-mail:** y200888@163.com

为了提升该方案的性能,文献[5-6]分别提出了相应的改进方案,但文献[7]发现这些改进的方案无法抵抗伪造攻击。文献[8]提出强不可伪造的基于身份签名方案,不仅能防止攻击者伪造新消息的签名,而且能阻止攻击者利用以前的消息/签名对生成新的合法签名。尽管文献[8]方案提升了基于身份签名方案的安全性,但该方案的计算开销较大,实用性比较差。文献[9]构造了另外一个强不可伪造的基于身份签名方案,但文献[10]发现该方案的安全性证明是错误的。因此,迫切需要研究更安全、更高效的基于身份签名方案。

为了抵抗重放攻击,文献[11]在 2017 年提出了一个高效的基于身份签名方案(下文简称 Huang 方案),具有较短的系统参数和较低的计算开销,并在标准模型中证明了该方案满足强不可伪造性,其安全性可归约到 CDH 假设。Huang 方案的安全性证明采用了基于混合游戏的证明方法,但本文发现该方案的安全性证明存在严重的安全缺陷。首先设计一个多项式时间算法,区分一个签名来自 Huang 方案证明中的模拟游戏还是真实游戏。其次构造一个多项式算法来伪造 Huang 方案的签名,使挑战者利用该算法输出的伪造签名来解决 CDH 问题。

## 1 预备知识

### 1.1 双线性映射

令  $G_1$  和  $G_2$  是 2 个阶为素数  $p$  的循环群,  $g$  是  $G_1$  的一个生成元,如果一个可有效计算的映射  $e: G_1 \times G_1 \rightarrow G_2$  满足以下条件,则称  $e$  是一个双线性映射<sup>[4]</sup>。

1) 双线性: 对任意的  $a, b \in Z_p^*$ , 有  $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$ 。

2) 非退化性:  $e(g, g) \neq 1$ 。

### 1.2 计算复杂度假设

已知  $(g, g^a, g^b) \in G_1^3$ , 这里未知的  $a, b \in Z_p^*$ , 群  $G_1$  上的 CDH 问题是计算  $g^{ab} \in G_1$ 。

**定义 1 (CDH 假设)** 如果没有一个概率多项式时间算法能以不可忽略的概率求解  $G_1$  上的 CDH 问题, 则称 CDH 问题是困难的<sup>[4]</sup>。

### 1.3 基于混合游戏的安全性证明方法

通常直接证明一个密码方案的安全性是非常困难的。为了降低证明密码方案的复杂度, 文献[12]提出了基于混合游戏的安全性证明方法, 并已成为大部分密码方案证明其安全性的主要方法。对于基于身份签名方案, 主要由攻击者和挑战者之间的 2 个安全游戏组成:

1) 真实游戏  $\text{Game}_0$ : 挑战者生成主密钥和系统参数, 并运行实际的算法来响应攻击者发起的密钥询问和签名询问。

2) 模拟游戏  $\text{Game}_1$ : 挑战者首先获得一个困难数学问题的实例, 然后在不知道主密钥的情况下, 通过模拟密钥和签名来响应攻击者发起的密钥询问以及签名询问, 最后利用攻击者伪造的签名来解决困难数学问题的实例。

如果以下 2 个条件成立, 则称基于身份签名的方案是可证明安全的:

1) 没有一个多项式时间算法能以不可忽略的概率区分真实游戏  $\text{Game}_0$  与模拟游戏  $\text{Game}_1$ 。

2) 在模拟游戏  $\text{Game}_1$  中, 如果攻击者伪造了一个合法的签名, 则挑战者能以不可忽略的概率求解困难数学问题。

基于混合游戏的安全性证明方法主要采用了归约的证明思想, 将方案的安全性归约到关联的数学问题的计算困难性。由于求解困难数学问题的概率是可忽略的, 因此在模拟游戏  $\text{Game}_1$  中攻击者能伪造一个合法签名的概率是可忽略的; 而真实游戏  $\text{Game}_0$  与模拟游戏  $\text{Game}_1$  是不可区分的, 所以攻击者在真实游戏  $\text{Game}_0$  中获胜的概率也是可忽略的。因此, 只要方案基于的数学问题是计算困难的, 则可证明相应的基于身份方案是安全的。

## 2 Huang 等人的基于身份签名方案

为了简化表述, 令  $\chi(d): G_1 \rightarrow \{0, 1\}^*$  表示一个映射; 当  $d \in G_1$  的  $x$  轴坐标为奇数时, 设置  $\chi(d) = 1$ ; 当  $d \in G_1$  的  $x$  轴坐标为偶数时, 设置  $\chi(d) = 0$ 。Huang 方案的具体描述如下:

1) 系统初始化。令  $G_1$  和  $G_2$  分别是 2 个阶为素数  $p$  的循环群,  $g$  是  $G_1$  的一个生成元,  $e: G_1 \times G_1 \rightarrow G_2$  是一个双线性映射。PKG 首先选择一个抗碰撞的哈希函数  $H_1: \{0, 1\}^* \rightarrow \{0, 1\}^{n_m}$ , 将任意长度的身份信息映射为一个长度为  $n_m$  的字符串; 然后随机选择  $x_0, x_1, y, v_0, v_1, w, g_2 \in G_1$  和  $s \in Z_p^*$ , 计算  $g_1 = g^s$ ; 最后秘密地保存主密钥  $g_2^s$ , 公开系统参数  $params = (G_1, G_2, e, p, g, g_1, g_2, x_0, x_1, y, v_0, v_1, w, H)$ 。

2) 密钥提取。对于一个用户的身份  $ID \in \{0, 1\}^{n_m}$ , PKG 随机选择  $r_{ID} \in Z_p^*$ , 计算  $d_2 = g^{r_{ID}}$ 。如果  $\chi(d_2) = 1$ , 则令  $x_{r_1} = x_1$ ; 否则, 令  $x_{r_1} = x_0$ 。PKG 输出  $ID$  的密钥  $S_{ID} = (d_1, d_2) = (g_2^s (x_{r_1} y^{ID})^{r_{ID}}, g^{r_{ID}})$ 。

3) 签名。对于消息  $m$ , 身份为  $ID$  的签名者首先选取当前时戳  $T_i$  和一个随机数  $r_m \in Z_p^*$ , 然后计算  $h = T(m) \parallel T_i$  和  $Q_3 = g^{r_m}$ 。如果  $\chi(Q_3) = 1$ , 则令  $v_{r_2} = v_1$ ; 否则, 令  $v_{r_2} = v_0$ 。最后签名者利用自己的私钥  $S_{ID} = (d_1, d_2)$  生成消息  $m$  的签名:

$$\sigma = (Q_1, Q_2, Q_3) = (d_1 (v_{r_2} w^h)^{r_m}, d_2, g^{r_m}) = (g_2^s (x_{r_1} y^{ID})^{r_{ID}} (v_{r_2} w^h)^{r_m}, g^{r_{ID}}, g^{r_m})$$

4) 验证。对于一个消息  $m$  和时戳  $T_i$  的签名  $\sigma = (Q_1, Q_2, Q_3)$ , 如果  $T_i > T_{i-1}$  不成立, 则验证者拒绝接

受签名;否则,验证者计算  $h = T(m) \parallel T_i$ ,并验证等式:

$$e(Q_1, g) = e(g_2, g_1) e(x_{\tau_1} y^{ID}, Q_2) e(v_{\tau_2} w^h, Q_3)$$

如果上述等式成立,验证者接受  $\sigma$  是一个合法的签名;否则,拒绝  $\sigma$ 。

### 3 Huang 方案的安全性分析

本文通过 2 个定理来分析 Huang 方案<sup>[11]</sup>的安全性,发现 Huang 方案的安全证明不满足 1.3 节的基于混合游戏的安全性证明方法中的 2 个条件。这表明该方案的安全证明存在安全缺陷,进而说明 Huang 方案的安全证明无法正确地证明该方案的强不可伪造性。

**定理 1** 如果一个多项式时间算法 D 允许最多询问  $O(\log_a(\delta^{-1}) q_E^2)$  次签名询问,则 D 能以  $1 - \delta$  的概率区分 Huang 方案的模拟游戏和真实游戏。

证明:当攻击者 A 请求关于消息  $m_i$ 、身份  $ID_i$  和时戳  $T_i$  的签名  $\sigma_i = (Q_{i,1}, Q_{i,2}, Q_{i,3})$  时,挑战者 B 无法生成  $\chi(Q_{i,3}) = 0$  的签名,从而导致  $\chi(Q_{i,3}) = 0$  与  $\chi(Q_{i,3}) = 1$  之间的概率分布存在差异。虽然差异较小,但经过多项式次的签名询问后,这个差异使得 D 能以不可忽略的概率区分  $\chi(Q_{i,3}) = 0$  与  $\chi(Q_{i,3}) = 1$  的 2 种分布。

令  $L$  表示 D 允许询问签名的最大次数,则 D 的具体描述如下:

1) 设置初始值  $c = 0$ 。

2) 对于  $i = 1:L$ , D 每次进行如下操作:

(1) 随机选择一个身份  $ID_i$ , 一个消息  $m_i$  和一个时戳  $T_i$ ;

(2) 向挑战者 B 请求并获得关于  $ID_i, m_i$  和  $T_i$  的签名  $\sigma_i = (Q_{i,1}, Q_{i,2}, Q_{i,3})$ ;

(3) 如果  $\chi(Q_{i,3}) = 1$ , 则设置  $c = c + 1$ 。

3) 如果  $\frac{c}{L} \leq \frac{1}{2} + \frac{1}{8q_E}$ , 则 D 输出与它交互的游戏是真实游戏  $G_0$ ; 否则, 输出与它交互的游戏是模拟游戏  $G_1$ , 这里  $q_E$  是模拟游戏  $G_1$  中攻击者 A 询问密钥的最大次数。

由于 D 仅进行了有限次的签名询问, 因此 D 是基于身份签名方案的安全模型中被允许的攻击者。下面分析 D 成功的概率:

1) 如果 D 与真实游戏  $Game_0$  进行交互, 在实际的签名算法中  $r_{m_i}$  是随机选取的, 则  $\Pr[\chi(Q_{i,3}) = 0] = 1/2, \Pr[\chi(Q_{i,3}) = 1] = 1/2$ 。

2) 如果 D 与模拟游戏  $Game_1$  进行交互, 则挑战者 B 不能生成  $\chi(Q_{i,3}) = 0$  或  $\chi(d_{i,2}) = 0$  的签名。在  $G_1$  中对于  $q_E$  次的密钥询问有概率  $\Pr[\chi(d_{i,2}) = 0] =$

$q_E/2$ , 因此, 在  $G_1$  中:

$$\Pr[\chi(Q_{i,3}) = 0] = \frac{1}{2} (1 - \frac{1}{2q_E})$$

$$\Pr[\chi(Q_{i,3}) = 1] = \frac{1}{2} (1 + \frac{1}{2q_E})$$

令  $X_i$  表示一个随机变量, 对于第  $i$  个签名  $\sigma_i = (Q_{i,1}, Q_{i,2}, Q_{i,3})$ , 设置  $X_i = \begin{cases} 0, \chi(Q_{i,3}) = 0 \\ 1, \chi(Q_{i,3}) = 1 \end{cases}$ 。由于  $\sigma_i$  是随机选取  $ID_i, m_i$  和  $T_i$  生成的, 因此  $\{X_i\}$  是相互独立的。

从上面的分析过程可知, 在  $Game_0$  中,  $\Pr[X_i = 1] = 1/2$ ; 在  $Game_1$  中,  $\Pr[X_i = 1] = \frac{1}{2} (1 + \frac{1}{2q_E})$ 。为了区分 2 个游戏, D 采样  $L$  个签名来估计  $X_i = 1$  的概率。如果估计值  $\frac{c}{L} \leq \frac{1}{2} + \frac{1}{8q_E}$ , 则 D 猜测与它交互的游戏是真实游戏  $Game_0$ ; 否则, 猜测为模拟游戏  $Game_1$ 。为了提高猜测的正确率, 使用 Chernoff 界<sup>[13]</sup>来估计采样签名的最小个数。令  $\delta$  表示错误的值, 则由 Chernoff 界可得  $\delta = e^{-L(1/8q_E)^2/2}$ , 从而有  $L = O(\log_a(\delta^{-1}) q_E^2)$ 。因此, 如果 D 进行  $L = O(\log_a(\delta^{-1}) q_E^2)$  次签名询问后, 能以  $1 - \delta$  的概率区分 Huang 方案的模拟游戏与真实游戏。特别地, 如果取  $\delta = \frac{1}{4}$ , 则进行  $O(q_E^2)$  次签名询问后, 能以  $\frac{3}{4}$  的概率区分出  $Game_0$  与  $Game_1$ , 即存在一个多项式时间算法 D 能以不可忽略的概率区分 Huang 方案的真实游戏  $Game_0$  和模拟游戏  $Game_1$ 。所以, Huang 方案的安全性证明不满足基于混合游戏证明方法的第 1 个条件。

**定理 2** 如果一个攻击者 A 以不可忽略的概率伪造 Huang 方案的签名, 则存在一个多项式时间算法 F 也以不可忽略的概率伪造 Huang 方案的签名, 但挑战者 B 无法利用算法 F 的伪造签名求解  $G_1$  上的 CDH 问题。

证明: 对于 A 发起的密钥和签名询问, F 首先将相应的询问转交给 B, 然后将 B 的回答作为响应发送给 A, 如图 1 所示。

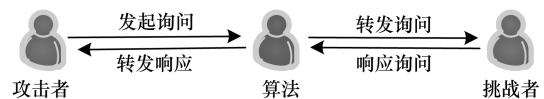


图1 询问-响应流程

令  $\lambda$  是 Huang 方案的安全参数, F 的具体操作描述如下:

1) F 从挑战者 B 获得系统参数  $params$ , 并转发给攻击者 A。

2) F 收到 A 请求的密钥和签名询问后, 首先将

相应的询问转发给挑战者 B,然后将 B 对询问的应答作为响应发送给 A。

3) A 输出一个关于身份  $ID^*$ , 消息  $m^*$  和时戳  $T^*$  的伪造签名  $\sigma^* = (Q_1^*, Q_2^*, Q_3^*)$ 。

4) 如果  $\chi(Q_2^*) = 1$  或  $\chi(Q_3^*) = 1$ , 则 F 将 A 的签名  $\sigma^* = (Q_1^*, Q_2^*, Q_3^*)$  作为自己的伪造签名输出给 B; 否则, F 不输出签名。

由于 F 只是进行 A 和 B 之间询问与响应的转发, 因此在基于身份签名方案的安全模型中, F 是被允许的攻击者。

在签名  $\sigma^* = (Q_1^*, Q_2^*, Q_3^*)$  中,  $\chi(Q_2^*) = 1$  或  $\chi(Q_3^*) = 1$  的概率均为  $1/2$ 。因此, 如果 A 能以不可忽略的概率输出一个伪造的签名, 则 F 也能以不可忽略的概率输出一个伪造的签名。

根据 Huang 方案的安全性证明, 只有  $\chi(Q_2^*) = 0$  且  $\chi(Q_3^*) = 0$  时, B 能从伪造的签名中计算 CDH 问题的实例。但当  $\chi(Q_2^*) = 1$  或  $\chi(Q_3^*) = 1$  时, F 输出一个伪造的签名; 当  $\chi(Q_2^*) = 0$  且  $\chi(Q_3^*) = 0$  时, F 不输出签名。因此, B 无法从 F 伪造的签名中计算 CDH 问题的实例。

因为从 F 的构造过程可知, F 是 Huang 方案的一个合法攻击者, 所以 Huang 方案的安全性并不能规约到 CDH 问题的困难性, 从而使得 Huang 方案的安全性证明不满足基于混合游戏证明方法的第 2 个条件。

综合定理 1 和定理 2 很容易发现, Huang 方案的安全性证明存在严重的安全缺陷, 无法从理论上证明 Huang 方案的安全性。

## 4 结束语

Huang 等人设计了一个具有较短系统参数的基于身份签名方案, 并在标准模型中证明该方案是强不可伪造的。本文对该方案进行安全性分析, 发现其安全性证明并不满足基于混合游戏证明方法的 2 个条件, 从而表明将 Huang 方案的安全性规约到 CDH 假设的结论是错误的。即存在一个多项式时间算法能区分 Huang 方案的真实游戏和模拟游戏, 挑战者无法利用攻击者伪造的签名求解 CDH 问题。Huang 方案的安全性证明存在缺陷的主要原因是采用了安全性较低的 Boneh 和 Boyen 方案<sup>[14]</sup>。此外, Huang 方案无法抵抗量子计算攻击<sup>[15-16]</sup>。因此, 如何构造具有更短系统参数且抗量子计算攻击的基于身份签名方案, 仍需要进一步研究。

## 参考文献

- [1] HU C, LI H, HUO Y, et al. Secure and efficient data communication protocol for wireless body area networks[J]. IEEE Transactions on Multi-Scale Computing Systems, 2016, 2(2): 94-107.
- [2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Proceedings of Advances in Cryptology-Crypto'84. Washington D. C., USA: IEEE Press, 1984: 47-53.
- [3] PATERSON K G. ID-based signatures from pairings on elliptic curves[J]. Electronics Letters, 2002, 38(18): 1025-1026.
- [4] PATERSON K G, SCHULDT J C N. Efficient identity-based signatures secure in the standard model[C]//Proceedings of Australasian Conference on Information Security and Privacy. Sydney, Australia: [s. n.], 2006: 207-222.
- [5] 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.
- [6] 谷 科, 贾维嘉, 姜春林. 高效安全的基于身份的签名方案[J]. 软件学报, 2011, 22(6): 1350-1360.
- [7] 禹 勇, 李继国, 伍 玮, 等. 基于身份签名方案的安全性分析[J]. 计算机学报, 2014, 37(5): 1025-1029.
- [8] TSAI T T, TSENG Y M, HUANG S S. Efficient strongly unforgeable ID-based signature without random oracles[J]. Informatica, 2014, 25(3): 505-521.
- [9] KWON S. An identity-based strongly unforgeable signature without random oracles from bilinear pairings[J]. Information Sciences, 2014, 276: 1-9.
- [10] LEE K, LEE D H. Security analysis of an identity-based strongly unforgeable signature scheme[J]. Information Sciences, 2014, 286: 29-34.
- [11] 黄一才, 张星昊, 郁 滨. 高效防重放体域网 IBS 方案[J]. 密码学报, 2017, 4(5): 447-457.
- [12] SHOUP V. Sequences of games: a tool for taming complexity in security proofs[EB/OL]. [2017-12-20]. <https://www.researchgate.net>.
- [13] SSHOUP V. A computational introduction to number theory and algebra[M]. Cambridge, USA: Cambridge University Press, 2009.
- [14] BONEH D, BOYEN X. Efficient selective-ID secure identity-based encryption without random oracles[C]//Proceedings of Conference on Theory and Applications of Cryptographic Techniques. Washington D. C., USA: IEEE Press, 2004: 223-238.
- [15] LIU Z, CHOO K K R, GROSSSCHADL J. Securing edge devices in the post-quantum internet of things using lattice-based cryptography[J]. IEEE Communications Magazine, 2018, 56(2): 158-162.
- [16] 冯超逸, 赵一鸣. 基于理想格的证明安全数字签名方案[J]. 计算机工程, 2017, 43(5): 103-107.

编辑 索书志