第34卷 第15期 计 算 机 工 程 2008年8月
Vol.34 No.15 Computer Engineering August 2008
·安全技术· 文章编号：1000—3428(2008)15—0140—02 文献标识码：A 中图分类号：TP309

标准模型下的安全短签名方案

胡小明，黄上腾
(上海交通大学计算机科学与工程系，上海 200240)

摘 要：提出一个新的短签名方案，证明该签名方案在适应性选择消息下是不可伪造的。将该签名方案的安全性归约到 q-SDH 问题的安全性。对方案的有效性进行分析，将其与目前最新的在标准模型下被证明安全的签名方案进行比较。结果显示，该签名方案更有效，更适合实际应用。

关键词：数字签名；标准模型；双线性对

Secure Short Signature Scheme in Standard Model

HU Xiao-ming, HUANG Shang-teng
(Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】 This paper presents a novel and efficient short signature scheme. It is proven to be existential unforgeable under adaptive chosen message attack. The security of the signature scheme is reduced to the security of the q-SDH problem in the standard model. This paper analyses the efficiency of the signature scheme. Compared with the latest signature schemes secure in the standard model, the signature scheme is more efficient and suitable to be applied in the actual world.

【Key words】 digital signature; standard model; bilinear paring

1 概述

Diffie 和 Hellman 于 1976 年提出了数字签名的概念。在一个数字签名中，一个签名者用自己的私钥产生签名，而任何拥有签名者公钥的用户皆可验证签名的有效性。到目前为止，数字签名已被广泛地用于现实生活中的各个领域，在身份认证、数据完整性、不可否认性以及匿名性等方面有重要应用，其安全性也越来越受到人们的重视。1988 年，Goldwasser 等人给出了数字签名方案安全性的标准概念。如果一个数字签名方案在适应性选择消息攻击下是不可伪造的，它就被认为是安全的。

目前，有 2 种安全证明模型：标准模型和随机预言机模型。标准模型是指安全证明仅仅依赖于标准代数难题。标准模型下的安全也称为真实世界中的安全。随机预言机模型是指安全证明不仅依赖于标准代数难题，而且还依赖于一种很强的假设：存在给定输入，其输出是均匀的这样一种 Hash 函数。但是，根据 Shannon 的熵理论，一个确定的函数不可能“放大”熵，因此，以上假设的 Hash 函数是不可能存在的。在随机预言机模型下安全的公钥密码体制在现实中可能根本就不安全。Canetti 等人就给出了这样一个密码体制，该密码方案在随机预言机模型下是安全的，但无论 Hash 函数如何选择，在现实中根本就不安全。因此，标准模型安全的密码体制成为当前研究的重点。

从 Diffie 和 Hellman 提出第一个数字签名方案以来，已经有很多数字签名方案被提出[1-4]。文献[4]提出了 3 个在标准模型下安全的短签名方案，分别是文献[1-3]的签名方案的改进和提高。本文在文献[5]加密方案的基础上提出了一个标准模型下安全的短签名方案，并与目前最新的 4 个在标准模型下被证明安全的签名方案从计算负担、签名长度和归约基于的复杂性问题 3 方面进行了比较分析。

2 数字签名方案的安全性定义

2.1 安全的数字签名方案

一个数字签名方案由 3 个算法组成：

(1)键产生算法：输入一个安全参数 k，键产生算法输出公钥参数 *params* 和密钥。

(2)签名发布算法：输入密钥和一个消息 m，该算法输出一个签名 σ。

(3)签名验证算法：输入公钥参数 *params*、一个消息 m 和一个签名 σ，输出“接受”或者“拒绝”。

定义 1(正确性) 对于任意的消息 m，如果按照上文描述的数字签名方案产生了一个签名，那么验证者输出的结果肯定是“接受”。

一个数字签名方案的安全性由接下来的一个挑战者和敌人之间的游戏来定义。本文使用一个更强的安全定义。

参数设置：挑战者运行键产生算法，得到公钥参数 *params* 和密钥，然后将 *params* 发送给敌人。

签名询问：敌人能以适应性的方式向挑战者要求最多 q_s 个消息$\{m_1, m_2,\cdots, m_{q_s}\}$的签名。挑战者产生 q_s 个与消息$\{m_1, m_2,\cdots, m_{q_s}\}$对应的签名$\{\sigma_1, \sigma_2,\cdots, \sigma_{q_s}\}$，并发送给敌人。

签名伪造：敌人输出一个伪造的签名(σ^*, m^*)，如果(σ^*, m^*)满足如下的条件，则说明敌人赢了这个游戏：

(1)$(\sigma^*, m^*) \notin \{(\sigma_1, m_1), (\sigma_2, m_2),\cdots, (\sigma_{q_s}, m_{q_s})\}$；

(2)签名验证算法(*params*, σ^*, m^*)=“接受”。

定义 2(不可伪造性) 一个敌人 A 被认为是一个(t, ε, q_s)伪造者，如果 A 在最多使用时间 t、最多要求 q_s 次签名询问

作者简介：胡小明(1978－)，女，博士研究生，主研方向：信息安全，数据库安全；黄上腾，教授、博士生导师

收稿日期：2007-09-07 **E-mail：**huxm@sjtu.edu.cn

下，以至少 ε 的概率赢了上面的游戏，如果没有(t, ε, q_s)伪造者存在，那么一个数字签名方案被认为在适应性选择消息攻击下是不可伪造的。

2.2 困难问题假设

本文提出的签名方案的安全性是以 q-SDH(q-Strong Diffie-Hellman)问题的困难性[1]为基础的。

q-SDH 问题：给定 $q+1$ 个元素$(g, g^{\alpha}, g^{\alpha^2}, \cdots, g^{\alpha^q}) \in G_1^{q+1}$，输出一个 $c \in Z_p^*$ 和$(c, g^{1/(\alpha+c)})$。

定义 3(q-SDH 假设) 如果没有算法可以在时间 t 内以至少 ε 的概率解决群 G_1 下的 q-SDH 问题，那么就认为群 G_1 下 (t, ε, q)-SDH 假设成立。

3 签名方案的提出

设 G_1 和 G_2 是 2 个有同样素数阶的循环群，e 是一个密码学双线性映射 $G_1 \times G_1 \to G_2$。那么提出的签名方案描述如下：

(1)参数产生：签名者随机的选择 2 个生成元 g, $h \in_R G_1$ 和一个随机元素 $x \in_R Z_p$，设置 $g_1 = g^x$。然后，发布公钥参数为 $params = \{g, g_1, h\}$，密钥为 x。

(2)签名发布：假设用户要求一个消息 $m \in Z_p$ 上的签名，那么签名者首先随机地选择一个元素 $r \in_R Z_p^*$，然后计算

$$(\sigma = (hg^{-r})^{\frac{1}{(x-m)}}, r)$$

那么(σ, r)就是消息 m 上的一个签名。签名者将它发送给用户。

(3)签名验证：给定消息 m 上的一个签名(σ, r)，验证者检验如下等式是否满足

$$e(g_1 g^{-m}, \sigma) = e(g,h) \cdot e(g,g)^{-r}$$

如果该等式满足，那么验证者接受该签名，否则拒绝。

注意：$e(g, g)$和 $e(g, h)$能被预计算，然后当作公钥发布，这样验证只需要一个对计算，减少了验证的时间。

3.1 正确性

给定一个 m 消息上的签名(σ, r)，正确性验证如下：

$$e(g_1 g^{-m}, \sigma) = e(g^{x-m}, (hg^{-r})^{\frac{1}{(x-m)}}) = e(g,h) \cdot e(g,g)^{-r}$$

3.2 有效性

本文将提出的签名方案和最近提出的在标准模型下安全的签名方案[1,4]从计算负担、签名长度和归约基于的复杂性问题这 3 方面进行比较。为了方便比较，用 Exp 表示群 G_1 上的一次指数计算，Mul 表示群 G_1 上的一次乘法计算，P 表示群 G_1 上的一次对操作。

(1)计算负担：本文提出的签名方案，在签名阶段需要 2 次指数计算和 1 次乘法计算，不需要任何的对计算，这样大大提高了签名的速度；而在验证阶段需要 2 次指数计算和 3 次对计算。但是能用预计算技术来减少计算负担。如在文献[1]中，将 $e(g, g)$和 $e(g, h)$进行预计算，并作为公钥参数发布，这样在签名验证阶段只需要一个对操作。另外，hg^{-r} 的计算与要签名的消息 m 无关，因此，签名者能事先预计算若干个 hg^{-r} 保存起来。当用户要求签名时，签名者随机取 1 个未使用过的 hg^{-r} 进行签名，这样签名操作只需要一次群 G_1 上的指数计算。这样的预计算技术同样适用于其他的签名方案。在预计算技术下，文献[1]的签名方案一共需要 3 次指数计算、2 次乘法计算和 1 次对计算，文献[4]的签名方案 1 需要 4 次指数计算、3 次乘法计算和 1 次对计算，文献[4]的签名方案 2 需要 3 次指数计算、2 次乘法计算和 2 次对计算，文献[4]的签名方案 3 需要 3 次指数计算、2 次乘法计算和 2 次对计算。因此，本文的签名方案在计算上比其他签名方案更有效。

(2)签名长度：本文提出的签名方案同文献[1]的签名方案、文献[4]的签名方案 1、方案 2 一样均由 2 个元素组成(σ, r)，而文献[4]的签名方案 3 由 6 个元素组成。

(3)复杂性问题：本文提出的签名方案的安全性能紧归约到 q-SDH 的安全性。虽然文献[1]的签名方案也同样能归约到 q-SDH 的安全性，但是它的归约不是很紧。而文献[4]的签名方案 1~方案 3 的安全性需要更多的困难问题假设。

本文方案与其他签名方案的比较如表 1 所示。

表 1 本文方案与其他签名方案的比较

签名方案	计算负担	签名长度	复杂性问题
文献[1]的方案	3Exp + 2Mul + 1P	2	q-SDH assumption
文献[4]的方案 1	4Exp + 3Mul + 1P	2	q-SDH, SSPIR, assumption
文献[4]的方案 2	3Exp + 2Mul+ 2P	2	PSR assmuption
文献[4]的方案 3	3Exp + 2Mul+ 2P	6	q-whLRSW assumption
本文方案	2Exp + 1Mul + 1P	2	q-SDH assumption

4 安全分析

定理 如果(t, ε, q)-SDH 假设在群 G_1 上成立，那么提出的数字签名方案在(t', ε', q_s)适应性选择消息攻击下是不可伪造的，其中，$q > q_s$；$t' = t - O(qq_s\rho)$；$\varepsilon' \le \varepsilon + (2q-1)/p \approx \varepsilon$；$\rho$ 表示群 G_1 上的一次指数计算的时间。

证明 假设存在一个敌人 A，在(t', ε', q_s)下伪造了一个提出的签名方案的有效签名。使用 A 建立一个算法 B，使得 B 能在最多使用时间 t、至少概率 ε 下解决 q-SDH 问题，这与假设矛盾。

B 取一个随机的 q-SDH 实例$(g, g_1, \cdots, g_q)$，其中，$g_i = g^{\alpha^i}$，并且 B 不知道 α 的值。B 的目标是找到一个 $c \in Z_p^*$ 并输出$(c, g^{1/(\alpha+c)})$。为了达到这个目的，B 必须能模拟签名者与 A 进行交互。B 的模拟过程如下：

(1)参数设置：B 随机地产生一个 q 次多项式 $f(x) \in Z_p[x]$，并设置 $h = g^{f(\alpha)}$，h 能从$(g, g_1, \cdots, g_q)$计算得到。B 将公钥参数 $params = \{g, g_1, h\}$发送给 A。因为 g, α 和 $f(x)$都是随机的，所以公钥参数 $params$ 的分布与实际的签名者建立的公钥参数的分布一致。

(2)签名询问：A 能要求以适应性的方式对 B 进行 q_s 次签名询问。B 用如下方法回答：

假设 A 要求消息 m 上的一个签名。B 首先判断是否 $m = \alpha$，如果 $m = \alpha$，那么 B 马上使用 α 解决 q-SDH 问题。否则，B 设置 $F(x)$是一个$(q-1)$次多项式$(f(x)-f(m))/(x-m)$。B 计算 $r = f(m)$和 $\sigma = g^{F(\alpha)}$。显然(σ, r)是一个有效的签名，这是因为：

$$\sigma = g^{F(\alpha)} = g^{\frac{(f(\alpha)-f(m))}{(\alpha-m)}} = (hg^{-f(m)})^{\frac{1}{(\alpha-m)}}$$

(3)签名伪造：最后，A 输出一个消息 m^*上的有效的伪造签名(σ^*, r^*)，也就是说该签名满足验证等式 $e(g_1 g^{-m^*}, \sigma^*) = e(g,h)e(g,g)^{-r^*}$。因为 $h = g^{f(\alpha)}$ 和 $g_1 = g^{\alpha}$，所以 $e(g, \sigma^{*(\alpha-m^*)}) = e(g, g^{(f(\alpha)-r^*)})$，从而 $\sigma^* = g^{(f(\alpha)-r^*)/(\alpha-m^*)}$。

使用多项式除法，$(f(\alpha)-r^*)$能被写为$(f(\alpha)-r^*) = \gamma(\alpha)(\alpha-m^*) + \gamma_{-1}$，其中，$\gamma(\alpha) = \sum_{k=0}^{q-1} \gamma_i \alpha^k$；$\gamma_{-1} \in Z_p$。从而得到$(f(\alpha)-r^*)/(\alpha-m^*) = \gamma(\alpha) + \gamma_{-1}/(\alpha-m^*)$和 $g^{\gamma(\alpha)+\gamma_{-1}/(\alpha-m^*)} = \sigma^*$。如果 $\gamma_{-1} = 0$, B 将放弃。否则，B 计算 $g^{1/(\alpha-m^*)} = (\sigma^* g^{-\gamma(\alpha)})^{1/\gamma_{-1}} = (\sigma^* g^{-\sum_{k=0}^{q-1}\gamma_i \alpha^k})^{1/\gamma_{-1}}$。

（下转第 158 页）