·安全技术· 文章编号：1000-3428(2018)04-0174-07 文献标志码：A 中图分类号：TP391

一种具有 CDH 问题安全性基于身份的签名方案

陈辉焱[1,2]，刘 乐[2]，张晨晨[2]

（1. 北京电子科技学院 信息安全系，北京 100070；2. 西安电子科技大学 通信工程学院，西安 710071）

摘 要： 严格的安全证明需要较短的安全参数和较高的运行效率。为此，提出一种基于身份的签名方案 IDSSTR，该方案具有可计算 Diffie-Hellman 问题的安全性规约，在线时自然有效，离线阶段也无需额外的条件，且验证过程也不变。为减小签名消息的总长度，给出具有消息恢复功能的 IDSSTR 修改版本。分析结果表明，可计算 Diffie-Hellman 问题的困难性与离散对数问题有着紧密联系，IDSSTR 签名方案可为该困难问题提供安全保证。

关键词： 基于身份的签名；可计算的 Diffie-Hellman 问题；离散对数问题；严格规约；随机预言机模型

中文引用格式： 陈辉焱，刘 乐，张晨晨. 一种具有 CDH 问题安全性基于身份的签名方案[J]. 计算机工程，2018，44(4)：174-180.

英文引用格式： CHEN Huiyan，LIU Le，ZHANG Chenchen. An Identity-based Signature Scheme with CDH Problem Security[J]. Computer Engineering，2018，44(4)：174-180.

An Identity-based Signature Scheme with CDH Problem Security

CHEN Huiyan[1,2]，LIU Le[2]，ZHANG Chenchen[2]

（1. Department of Information Security，Beijing Electronic Science and Technology Institute，Beijing 100070，China；
2. Institute of Communication Engineering，Xidian University，Xi'an 710071，China）

【Abstract】 Tight security proofs need shorter security parameters and better efficiency. Therefor，a new Identity-based Signature（IBS）scheme named IDSSTR is proposed，which has a security specification for Computational Diffie-Hellman（CDH）problems and it is also naturally efficient on-line，no additional conditions is needed for the off-line stage and the verification process is unchanged. In order to shorten the total length of the signed message，a modified version of the IDSSTR with message recovery is goven. Analysis results show that，the difficulty of CDH problem is widely considered to be closely related to the discrete logarithm problem，therefor，the proposed signature scheme provides security assurance for such difficult problems.

【Key words】 Identity-based Signature（IBS）；Computational Diffie-Hellman（CDH）problem；discrete logarithm problem；strict regulations；random oracle model

DOI： 10.3969/j.issn.1000-3428.2018.04.028

0 概述

在实践中使用公钥密码学，最主要的问题是如何提供一种安全的方式将用户与他们的公钥连接起来。目前，解决上述问题的方案是建立一个公钥基础设施，其中由可信实体颁发证书来确定公钥属于某个确定的用户，证书通常包括用户的身份、公钥以及可信的实体签名。若需要安全的通信，2 个用户间首先要交换证书。为了减少实际应用中对用户证书的需求，文献[1]提出基于身份密码学的观点，其思想是用户的公钥可以从任意字符串（邮件地址、连接用户姓名的 IP 地址、社会安全号等）中导出，它以一种明确的方式来验证其身份。这种密码体系需要一种被称为私钥生成器（Private Key Generator，PKG）的可信机构来完成，PKG 的任务是从用户的身份信息中计算用户的私钥。

1984 年以来，许多基于身份的签名（Identity-based Signature，IBS）方案[2-3]被提出。目前，有两种通用的 IBS 构造方法：一种由文献[4]提出，它表明之前提出的大量方案都是其通用构造的实例；另外一种由文献[5]提出，对于签名知识的证明，该方法需要有效的零知识协议，这使得其构造仅仅适用于一部分方案，如 RSA-FDH 和 BLS[6]。

IBS 的安全证明一般都是通过演示一个规约来进行，这种规约证明了如果攻击者 A 能够有效地破解某个 IBS，那么就可以构造出一种算法来破解这种

基金项目： 北京电子科技学院信息安全重点实验室开放基金（2014KF-chy）。

作者简介： 陈辉焱（1968—），男，高级工程师，主研方向为格密码、数字签名；刘 乐、张晨晨，硕士研究生。

收稿日期： 2016-12-26 **修回日期：** 2017-03-10 **E-mail：** 1156038510@qq.com

困难问题,这种评估安全性的技术就是安全性规约。规约质量由敌手抗 IBS 方案破解潜在的棘手问题成功的概率决定。当敌手在时间 t 内运行成功的概率大约等于相同时间内解决潜在困难问题的概率时,则认为安全规约是严格的,否则就认为它是近似规约。

严格的安全证明需要较短的安全参数和更高的效率。针对那些在随机预言机模型下是安全的密码方案或由它们变形[7-8]所得的一些密码方案,为其提供新的安全证明,以及利用严格的安全规约构造新的方案[9-10],已经成为可证明安全领域的一个研究热点。然而,目前在设计具有严格安全规约的 IBS 方案方面还没有明显的进步。文献[11]在 Diffie-Hellman 假设下对方案在严格安全规约范围内通过 Pointcheval 和斯特恩分叉引理给出了证明。文献[12-13]在 Diffie-Hellman 假设下对方案在严格安全规约范围内通过文献[14]的"ID 规约技术"给出了证明。文献[4]针对 IBS 方案的大家族定义了一个框架来提供安全性证明,但是该框架不能提供严格的安全界。文献[5]演示了从任何满足确定条件的数字签名方案到 IBS 方案的转换,并对所得的 IBS 方案给出安全性证明,尽管该安全性证明避免了分叉技术的使用,但它的规约条件仍然比较宽松。

尽管可计算的 Diffie-Hellman (Computational Diffie-Hellman,CDH)假设在技术上比离散对数假设强,但对于各种已被研究的密码群来说,目前并不知道如何通过解决离散对数问题[15]来更快地解决 Diffie-Hellman 问题。此外,一些理论表明在某些群中 CDH 假设与离散对数假设[15]等价。

基于以上问题,本文提出一种新的 IBS 方案 IDSSTR。该方案的签名过程是确定的:用户使用他的部分密钥通过 Schnorr[16]签名方案在消息上计算签名。在随机预言机模型下,IDSSTR 的安全性与 CDH 假设密切相关。此外,不需要额外的信息将 IDSSTR 转换成离线/在线版本。为缩短签名消息的总长度,本文也给出具有消息恢复功能的 IDSSTR 修改版本。

1　预备知识

1.1　IBS 方案

IBS 方案由下列 4 个步骤组成:

1)系统参数建立。该算法通过 PKG 运行,输入安全参数,生成方案的公共参数 *params* 和主密钥。PKG 公布公共参数,自己保存主密钥。

2)私钥提取。给出身份 ID、主密钥和公共参数 *params*,该算法生成 ID 的私钥 d_{ID}。主实体将使用该算法针对参与方案的所有实体来生成私钥,并通过安全渠道将私钥分发给其主人。

3)签名。给出消息 m、身份 ID、私钥 d_{ID}和公共参数 *params*,该算法在 m 上生成 ID 的签名 σ。具有身份 ID 的实体将使用该算法用于签名。

4)验证。给出签名 σ、消息 m、身份 ID 和公共参数 *params*,如果 σ 对于身份 ID 在 m 上是有效的签名,则该算法输出"接受";否则,输出"拒绝"。

IBS 方案安全性已知的最普遍概念是在自适应性选择消息攻击时存在伪造安全,在该模型中,敌手可以让签名者签署除了输出以外的任何消息,如果敌手最终输出一对有效的消息和签名,则敌手赢得游戏。

敌手和挑战者之间的游戏如下:

1)系统参数建立。挑战者运行系统参数建立算法,得到公共参数 *params* 和主私钥 *sk*。敌手可以得到公共参数 *params*,但主私钥 *sk* 由挑战者保管。

2)查询。敌手自适应地制作大量不同的查询给挑战者。每个查询可以是下列中的一种:

(1)哈希查询:挑战者针对请求的输入计算哈希函数值并将该值发送给敌手。

(2)私钥提取查询:敌手可以询问任何身份 ID 的私钥。挑战者通过运行私钥提取算法生成与 ID 对应的私钥 d_{ID},将 d_{ID}作为应答发送给敌手。

(3)签名查询:敌手可以针对身份 ID 和某个消息 m 对挑战者进行签名查询。挑战者首先运行私钥提取算法产生与 ID 对应的私钥 d_{ID},再利用 d_{ID}运行签名算法生成消息 m 的签名 σ,将 σ 作为应答发送给敌手。

3)伪造。敌手最终对消息 m^* 和身份 ID^* 输出一个伪造的签名 σ^*。如果下列条件均成立,则敌手成功:

(1) $Verify(params, ID^*, m^*, \sigma^*) = accept$。

(2)敌手在 ID^* 上没有制造提取查询。

(3)敌手在(ID^*,m^*)上没有制造签名查询。

在上面的游戏中敌手 A 的优势被定义为:

$$AdvSig_{\mathrm{A}} = \Pr[\mathrm{A\ succeeds}] \tag{1}$$

其中,概率是挑战者和敌手在各种能遇到的情况下得到的。

定义 1　如果敌手在时间 t 内最多制造 q_s 个签名查询,q_H 个哈希函数查询,q_e 个私钥提取查询,且 $AdvSig_{\mathrm{A}}$ 至少为 ε,则敌手就可以破解该签名方案。如果一个签名方案在可适应选择消息条件下没有伪造者可以破解它,则认为该签名方案是不可伪造的。

1.2　双线性配对和复杂性假设

定义 3 个阶均为素数 p 的循环乘法群 G_1、G_2和 G_T。g_1、g_2 分别是 G_1、G_2 的生成元。假设存在一个同构 $\psi: G_2 \to G_1$ 满足 $\psi(g_2) = g_1$。令 $\hat{e}: G_1 \times G_2 \to G_T$ 为具有下列属性的双线性映射:

1)双线性。$\hat{e}(u^a, v^b) = \hat{e}(u,v)^{ab}$ 对于所有的 $u \in G_1$、$v \in G_2$、$a, b \in \mathbb{Z}_p$ 均成立。

2)非退化性。存在 $u \in G_1$、$v \in G_2$ 使得 $\hat{e}(u,v) \neq 1$。

3)可计算性。对于所有的 $u \in G_1$、$v \in G_2$,都存在一种有效的算法计算 $\hat{e}(u,v)$。

为简单起见,令 $G_1 = G_2$。对于条件 $G_1 = G_2$,可以修改结合超级椭圆曲线的 Weil 和 Tate 配对来创造这样的双线性。

G 是一个由 g 生成的乘法循环群,其阶为素数 p,x 是 $\mathbb{Z}_p^*$ 中的一个随机数,定义 $y = g^x$。所谓离散对数问题,即给出 y 和 g,要求找到 $x \in \mathbb{Z}_p^*$ 使得 $g^x = y$。本文中,以 g 为底,y 的离散对数可以表示为 $DL_g(y) = x$。同时,假设 G 上的离散对数问题是困难的。

定义 2(CDH) 令 G 为一个由 g 生成的循环乘法群,其阶为素数 p。对于 $a,b \in \mathbb{Z}_p$,给出 g、g^a、g^b 计算 $DH_{g,p}(g^a,g^b) = g^{ab}$。如果 $\Pr[A(g,g^a,g^b) = g^{ab}] \geqslant \varepsilon$,则算法 A 在 G 中解决 CDH 问题有 ε 优势,其中概率与生成元 $g \in G$ 和 $a,b \in \mathbb{Z}_p^*$ 的随机选择以及 A 所决定的随机位数有关。

定义 3 如果不存在一个概率多项式时间算法在时间 t 内,以至少 ε 的概率解决群 G 上的 CDH 问题,则认为 (t,ε)-*CDH* 假设成立。

CDH 问题的困难性被广泛地认为与离散对数问题的困难性密切相关。此外,对于离散对数问题是困难的一类群来说,通过文献[15]的结果,可以直接将本文方案与离散对数问题的困难性相联系。

1.3 密码哈希函数

密码哈希函数是具有特定安全属性的哈希函数,适合在各种信息安全应用中作为原语使用,例如身份验证和消息完整性。对于密码哈希函数 H,存在与密码观点相关的 3 个基本属性。

1)原像抵抗性。给出一个哈希值 h,很难找到一个消息 m 使得 $H(m) = h$。缺乏这种属性的密码哈希函数对于原像攻击是很脆弱的。

2)第二原像抵抗性。给出一个输入 m_1,很难找到不同的输入 m_2 使得 $H(m_2) = H(m_1)$。缺乏这种属性的密码哈希函数对于第 2 种原像攻击是很脆弱的。

3)抗碰撞性。很难找到 2 条不同的消息 m_1 和 m_2 使得 $H(m_1) = H(m_2)$,如 m_1 和 m_2 这样的一对值被称为密码哈希碰撞。

2 具有严格安全性规约的 IBS

本文的签名方案 IDSSTR 运行过程如下:

1)系统参数建立。给出安全参数 n,算法运行如下:

(1)选择 2 个阶为素数 p 的乘法循环群 G 和 G_T 使得双线性映射 $\hat{e}: G \times G \to G_T$ 能够构造。

(2)选择一个 G 的随机生成数 g,一个随机数 x,$x \in \mathbb{Z}_p$,计算 $u = g^x$。

(3)选择 3 个密码哈希函数 $H: G \times \{0,1\}^* \to G$,$H_0: G \times \{0,1\}^* \to \mathbb{Z}_p$,$H_1: G \times \{0,1\}^* \to \mathbb{Z}_p$。

(4)设置系统参数 $params = \{G, G_T, \hat{e}, g, u, H, H_0\}$,主密钥 sk 是 x。

2)私钥提取。给定用户的身份 $ID \in \{0,1\}^*$,算法运行如下:

(1)选择一个随机数 $t \in \mathbb{Z}_p$,计算 $v = g^t$。

(2)计算 $h = H(v, ID)$ 和 $f = h^x$。

(3)计算 $r = H_0(f, ID)$。

(4)计算 $y = t + rx \bmod p$。

(5)将对应身份 ID 的私钥 d_{ID} 设置为 $d_{\mathrm{ID}} = (f,y)$。

3)签名。给出身份 ID、d_{ID} 和消息 $m \in \{0,1\}^*$,算法运行如下:

(1)选择一个随机数 $k \in \mathbb{Z}_p$,计算 $v_0 = g^k$。

(2)计算 $c = H_1(v_0, m)$ 和 $w = g^y$。

(3)计算 $s = k + cy \bmod p$。

(4)消息 m 和身份 ID 上的签名 $\sigma = (f,w,s,c)$。

4)验证。给出身份 ID 和消息 m 上的签名 $\sigma = (f,w,s,c)$,算法运行如下:

(1)计算 $r = H_0(f, ID)$。

(2)计算 $h = H(wu^{-r}, ID)$。

(3)验证 $\hat{e}(h,u) = \hat{e}(f,g)$ 和 $c = H_1(g^s w^{-r}, m)$,如果这 2 个等式都成立,则签名 $\sigma = (f,w,s,c)$ 有效;否则,签名无效。

2.1 安全性证明

首先,证明不可伪造性。

定理 1 假设 H_1 是密码哈希函数,它具有原像抵抗性,H 和 H_0 作为随机预言机。如果阶为素数 p 的群 G 上的 CDH 假设成立,则该方案在自适应选择消息攻击下是安全的,如果在 q_H 个随机预言机查询、q_e 个提取预言机查询和 q_s 个签名预言机查询的条件下满足:

$$\varepsilon \leqslant \varepsilon' + (q_{sig} + q_e)(q_H + q_{H_0} + 2q_e + 2q_s)/p + (2 + q_H + q_e + q_s)/p \tag{2}$$

$$t \approx t' - O(4q_e + 6q_s + q_H)T \tag{3}$$

则该签名方案是不可伪造的。其中,T 是 G 中求幂的最大时间。

证明:F 是一个伪造者,$(t, q_H, q_{H_0}, q_e, q_s, \varepsilon)$ 破坏本文的构造。

构造一个模拟算法 S,它可以将 (G,g,p) 和 (g^a, g^b) 作为输入。算法 S 使用 F 算法在 t' 步内以 ε' 的概率计算 $CDH_{g,p}(g^a, g^b)$ 函数,其中:

$$\varepsilon \leqslant \varepsilon' + (q_s + q_e)(q_H + q_{H_0} + 2q_e + 2q_s)/p + (2 + q_H + q_e + q_s)/p \quad (4)$$

$$t \approx t' - O(4q_e + 6q_s + q_H)T \quad (5)$$

算法 S 对伪造者 F 模拟运行上述签名方案。算法 S 回答 F 的哈希函数查询、私钥提取查询、签名预言机查询,并将 F 可能的伪造 (m,σ) 转化为 $CDH_{g,p}(g^a,g^b)$ 函数的答案。算法 S 通过提供 (G,g,p) 开始模拟,公钥 $u=g^a$ 作为 F 的输入。算法 S 回应 F 的查询如下:

1)H-预言机查询。S 得到一个 H 查询列表 L,每个条目都是 $(v,ID,d)\in G\times\{0,1\}^*\times\mathbb{Z}_p$ 这种形式。如果伪造者提供一个查询 (v,ID) 作为 H-预言机的输入:

(1)S 检查 L。如果存在条目 $(v,ID,d)\in L$,S 返回 $g^b g^d$ 到 F。

(2)否则,S 检查 L'。L'通过提取预言机和签名预言机生成。如果存在条目 $(v,ID,d)\in L'$,S 返回 g^d 到 F。

(3)若上面的情况都没发生,S 通过在 $\mathbb{Z}_p$ 中随机选择 d,输出 $H(v,ID)$ 作为 $h=g^b g^d$ 并将 (v,ID,d) 放入 L 中,将 g^b 嵌入到它的答案中。

2)H_0-预言机查询。S 得到一个 H_0查询列表 L_0,每个条目都是 $(f,ID,r)\in G\times\{0,1\}^*\times\mathbb{Z}_p$ 这种形式。如果伪造者 F 提供一个新的查询 (f,ID) 作为 H_0-预言机的输入:

(1)S 检查 L_0。如果存在条目 $(f,ID,r)\in L_0$,S 返回 r 到 F。

(2)否则,S 检查 L_0'。L_0'通过提取预言机和签名预言机生成。如果存在条目 $(f,ID,r)\in L_0'$,S 返回 r 到 F。

(3)若上面的情况都没发生,S 在 $\mathbb{Z}_p$ 中随机选择 r,输出 $H_0(f,ID)=r$ 并将 (f,ID,r) 放入 L_0 中。

3)私钥提取查询。S 得到一个提取查询列表 LE,每个条目都是 $(ID,f,y)\in\{0,1\}^*\times G\times\mathbb{Z}_p$ 这种形式。假设伪造者 F 在身份 $ID\in\{0,1\}^*$ 中需要一次提取,算法 S 在不知道主密钥的情况下必须创建一个有效的提取。在这个过程中,S 定义了哈希函数 H 和 H_0 的若干值。因此,算法 S 分别得到 H 和 H_0 的列表 L'和 L_0'。模拟过程如下:

(1)S 检查 LE,如果存在条目 $(ID,f,y)\in LE$,S 返回 (f,y) 到 F。

(2)否则,S 随机选择 $y、r\in\mathbb{Z}_p$,计算 $v=g^y u^{-r}$。

(3)S 随机选择 $d\in\mathbb{Z}_p$,计算 $h=g^d$ 和 $f=g^{ad}$。

(4)设置 $H(v,ID)=h$,$H_0(f,ID)=r$。如果 $H(v,ID)$ 或 $H_0(f,ID)$ 已经被设置,即存在条目 $(v,ID,h')\in L\cup L'$或存在条目 $(f,ID,r')\in L_0\cup L'_0$,则 S 终止;否则,在身份 ID 上生成私钥 $d_{ID}=(f,y)$,将它返回给 F,并分别将 (f,ID,y)、(v,ID,d)、(f,ID,r) 放到 LE、L'和 L_0'中。

4)签名查询。假设伪造者 F 要求身份 $ID\in\{0,1\}^*$和消息 $m\in\{0,1\}^*$上的签名,算法 S 在不知道主密钥的情况下必须创建一个有效的签名组。在这个过程中,S 定义了哈希函数 H 和 H_0的若干值并为签名查询生成了一些私钥。因此,算法 S 得到列表 LE、L'和 L_0'。模拟过程如下:

(1)S 检查 LE。如果存在条目 $(ID,f,y)\in LE$,S 跳到过程(5)。

(2)S 随机选择 $y、r\in\mathbb{Z}_p$,计算 $v=g^y u^{-r}$。

(3)S 随机选择 $d\in\mathbb{Z}_p$,计算 $h=g^d$ 和 $f=g^{ad}$。

(4)设置 $H(v,ID)=h$,$H_0(f,ID)=r$。如果 $H(v,ID)$ 或 $H_0(f,ID)$ 已经被设置,则 S 终止;否则,在身份 ID 上生成私钥 $d_{ID}=(f,y)$,并分别将 (f,ID,y)、(v,ID,d)、(f,ID,r) 放到 LE、L'和 L_0'中。

(5)S 随机选择 $k\in\mathbb{Z}_p$,计算 $v_0=g^k$ 和 $w=g^y$。

(6)S 计算 $c=H_1(v_0,m)$ 和 $s=k+cy$,生成一个有效的签名 $\sigma=(f,w,s,c)$ 并将其返回到 F。

5)伪造。A 输出 $(m^*,ID^*,\sigma^*=(f^*,w^*,s^*,c^*))$ 使得 σ^* 在消息 m^* 和身份 ID^* 上是一个有效的签名,要求 (m^*,ID^*) 未曾在之前的签名预言机查询中被查询过,ID^* 未曾在之前的提取预言机查询中被查询过。其中,如果 $H_0(f^*,ID^*)$ 没有被攻击者查询到 H_0预言机中或通过签名预言机和提取预言机设置,则模拟查询到 H_0 预言机自身。如果 $r^*=H_0(f^*,ID^*)$,$H(w^*u^{-r^*})$ 没有被攻击者查询到 H 预言机中或通过签名预言机和提取预言机设置,则模拟查询到 H 预言机自身。

需要注意的是,S 为 F 提供模拟器,它的分布与 F 在含有签名者的真实交互中的分布相同。为了更清楚地说明这点,本文给出下列解释:

1)H_0预言机和 H 预言机的模拟器较好。

2)考虑到 S 返回的私钥 $d_{\mathrm{ID}}=(f,y)$来回应身份 ID 上的提取查询。ID 上的私钥由 S 构造。很明显,y 和 r 在 $\mathbb{Z}_p$ 上均匀统一分布。计算 $v=g^y u^{-r}$并令 $h=H(v,ID)=g^d$,可以看到 $f=g^{da}$,如同实验中得到的结果。最后,(f,y) 与其在真实实验中的分布相同。

3)考虑到 S 返回的签名 (f,w,s,c)来回应身份 ID 和消息 m 上的签名查询。身份 ID 和消息 m 上的签名由 S 构造。很明显,y 和 r 在 $\mathbb{Z}_p$ 上均匀统一分布。计算 $v=g^y u^{-r}$并令 $h=H(v,ID)=g^d$,可以看到 $f=g^{da}$,如同实验中得到的结果。最后,(f,w,s,c)与其在真实实验中的分布相同。

解决 CDH 问题时假设伪造者 F 返回一个有效的消息、身份和签名组$(m^*,ID^*,\sigma^*=(f^*,w^*,s^*,c^*))$，$(m^*,ID^*)$和 ID^*都未曾在之前的私钥提取查询和签名查询中被查询过。在有效的伪造签名$(m^*,ID^*,\sigma^*=(f^*,w^*,s^*,c^*))$中，需要考虑下列情形：

情形 1 ID^*出现在签名预言机查询中，但存在满足$(ID^*,f',g^{y'})=(ID^*,f^*,w^*)$的$(ID^*,f',g^{y'})\in LE$。假设 A 选择 g^k 并计算 $c^*=H_1(g^k,m^*)$，为了得到 s^*，A 必须计算 $DL_g(g^k(w^*)^{c^*})$。假设 A 选择 c^*，为了生成一个有效的伪造签名$(m^*,ID^*,\sigma^*=(f^*,w^*,s^*,c^*))$，A 必须找到满足 $H_1(g^{s^*}(w^*)^{c^*},m^*)=c^*$的 s^*。如果 s^*以不可忽略的概率被找到，则密码哈希函数 H_1就会很容易受到原像攻击，这与原像抵抗性的概念发生矛盾。因此，这种情况下 A 生成有效伪造签名的概率是可以忽略的。

情形 2 ID^*出现在签名预言机查询中，但存在满足$(ID^*,f',g^{y'})\neq(ID^*,f^*,w^*)$的$(ID^*,f',y')\in LE$。假设 $r^*=H_0(f^*,ID^*)$，$r'=H_0(f',ID^*)$，可以得到 $w^*u^{r^*}\neq w'u^{r'}$。否则，通过 $w^*u^{r^*}=w'u^{r'}$得到 $h^*=H(w^*u^{r^*},ID^*)=H(w'u^{r'},ID^*)=h'$，$f^*=(h^*)^a=(h')^a=f'$，$r^*=H_0(f^*,ID^*)=H_0(f',ID^*)=r'$，$w^*=w'$。因此，在这种情况下，$(w^*u^{r^*},ID^*,h^*)$不能出现在 L'中。

综上所述，ID^*不能出现在签名预言机查询中。

如果上面的情况均不发生，则(v^*,ID^*)存储在 L 中并且 $h^*=H(v^*,ID^*)=g^bg^d$ 对于模拟器 S 中的某些 d 成立。

用算法 S 解决 CDH 问题的概率计算过程如下：

1）在提取预言机模拟器的第（4）步，如果 $H(v,ID)$或 $H_0(f,ID)$已经被设置，则 S 终止。这些输入可以表示为(g^yu^{-r},ID)和(g^{ad},ID)，其中 r、y、d 可以在$\mathbb{Z}_p$ 中随机选择，g 是群 G 的生成元。因为在 $L\cup L'$中最多有 $q_H+q_e+q_s$ 个条目，在 $L_0\cup L_0'$中有 $q_{H_0}+q_e+q_s$ 个条目，碰撞的概率最多为$(q_H+q_{H_0}+2q_e+2q_s)/p$。则这一过程中 S 在模拟器中任何时间内终止的概率最多为 $q_e(q_H+q_{H_0}+2q_e+2q_s)/p$。

2）在签名预言机模拟器的第（4）步，如果 $H(v,ID)$或 $H_0(f,ID)$已经被设置，则 S 终止。这些输入可以表示为(g^yu^{-r},ID)和(g^{ad},ID)，其中 r、y、d 可以在$\mathbb{Z}_p$ 中随机选择，g 是群 G 的生成元。因为在 $L\cup L'$中最多有 $q_H+q_e+q_s$ 个条目，在 $L_0\cup L_0'$中最多有 $q_{H_0}+q_e+q_s$ 个条目，碰撞的概率最多为$(q_H+q_{H_0}+2q_e+2q_s)/p$。则这一过程中 S 在模拟器中任何时间内终止的概率最多为 $q_s(q_H+q_{H_0}+2q_e+2q_s)/p$。

3）NH_0代表伪造者 F 不能在(f^*,ID^*)上查询 H_0 预言机这一事件，NH_0 是伪造者的一部分输出。NH 代表伪造者 F 不能在(v^*,ID^*)上查询 H 预言机这一事件，NH 是伪造者的一部分输出。其中 $r^*=H_0(f^*,m^*)$，$v^*=H_0(w^*u^{-r^*})$。计算概率 $\Pr[NH\vee NH_0]$的上界（$\Pr[NH\vee NH_0]=\Pr[NH\wedge\neg NH_0]+\Pr[NH_0]$）过程如下：

（1）$\Pr[NH\wedge\neg NH_0]$的上界：假设 $r^*=H_0(f^*,m^*)$，计算 $v^*=w^*u^{-r^*}$。如果模拟器在(v^*,ID^*)上查询 H 预言机本身并得到 $h=H(v^*,ID^*)$，h 满足 $h^a=f^*$的概率最多为 $1/p$。

（2）$\Pr[NH_0]$的上界：模拟器 S 在(f^*,ID^*)上查询 H_0 预言机本身并得到 $r^*=H_0(f^*,ID^*)$，$H(v^*,ID^*)$的概率被设置为最大$(q_H+q_e+q_s)/p$，其中$v^*=w^*u^{-r^*}$。如果 $H(v^*,ID^*)$的概率没有被设置，它将通过模拟器被查询且模拟器得到 $h=H(v^*)$。h 满足 $h^a=f^*$的概率为 $1/p$，则 $\Pr[NH_0]$的概率最大值为$(1+q_H+q_e+q_s)/p$。

将上面的概率相加，得出模拟器 S 最小以 $\varepsilon-(q_s+q_e)(q_H+q_{H_0}+2q_e+2q_s)/p-(2+q_H+q_e+q_s)/p$ 的概率解决 CDH 问题。

2.2 效率分析

算法 S 的运行时间指运行伪造者 F 和若干属于 $\mathbb{Z}_p$ 指数的模指数运算时间。每个对应 H 预言机的查询需要 1 次指数运算，每个对应提取预言机的查询需要 4 次指数运算，每个对应签名预言机的查询需要 6 次指数运算。将本文方案与文献[17]方案在计算成本方面进行比较，结果如表 1 所示。其中，$|G|$表示 G 的元素个数（$|G|\geqslant|p|=\lceil\mathrm{lb}(p)\rceil$），计算成本表示为$(a,b,c)$，$a$ 是 G 中的幂数，b 是“哈希到 G”（hash-to-G）操作的次数，c 是 G 中配对的次数。

表 1 2 种方案在循环群 G 上的计算成本比较

算法	签名			验证	提取	假设	严格规约
	离线	在线	和				
SOK-IBS[17]	(0,0,0)	(2,1,0)	(2,1,0)	(0,2,3)	(1,1,0)	多次 CDH	是
IDSSTR	(2,0,0)	(0,0,0)	(2,0,0)	(3,1,2)	(2,1,0)	CDH	是

2.3 离线/在线分析

本质上通过做离线的所有工作有可能使得上述方案瞬间在线签名。本文的签名方案主要分为以下 2 步：

1）离线签名。给出密钥 $x\in\mathbb{Z}_p$。

（1）选择一个随机数 $k\in\mathbb{Z}_p$，计算 $v_0=g^k$。

（2）计算 $w=g^y$。

(3)输出(v_0,m)。

2)在线签名。给出签名消息$m\in\{0,1\}^*$。

(1)计算$c=H_1(v_0,m)$。

(2)计算$s=k+cy \bmod p$。

(3)签名为$\sigma=(f,w,s,c)$。

验证过程与前述相同。这一属性较有用,因为它允许签名者重新计算f进而快速地在线签名,即通过一个模乘运算和模加运算就可以运行一个哈希函数。

3　有限的消息恢复

在带宽有限的环境中,缩短原始消息M附加签名σ的总长度是可行的。缩短签名消息总长度的通用技术是在签名过程中只对消息的一部分进行编码,利用这种技术得到的方案称为具有消息恢复功能的签名方案。现有的具有消息恢复功能的数字签名可以分为 2 种:基于 RSA 的方案[14]和基于离散对数的方案[18]。本节给出 IDSSTR 的一种修改版本,并根据文献[18]提出的技术使其具有消息恢复功能。

IDSSTR 修改版本构造过程如下:

1)系统参数建立。给出安全参数n,算法运行如下:

(1)选择 2 个阶为素数p的乘法循环群G和G_T使得双线性映射$\hat{e}:G\times G\to G_T$能够构造。

(2)选择一个G的随机生成数g,一个随机数x,$x\in\mathbb{Z}_p$,计算$u=g^x$。

(3)选择 4 个密码哈希函数$H:G\times\{0,1\}^*\to G$,$H_0:G\times\{0,1\}^*\to\mathbb{Z}_p$,$H_1:G\to\{0,1\}^{2l}$,$H_2:\{0,1\}^*\to\mathbb{Z}_p^*$。

(4)令$F_1:\{0,1\}^l\to\{0,1\}^l$,$F_2:\{0,1\}^l\to\{0,1\}^l$是 2 个密码哈希函数,其中$\frac{|p|}{2}\leqslant l\leqslant\frac{|p|}{2}+1$。

(5)设置参数$params=\{G,G_T,\hat{e},g,u,H,H_0,H_1,H_2,F_1,F_2\}$,主密钥$sk$是$x$。

2)私钥提取。对于给出的身份串$ID\in\{0,1\}^*$,算法运行如下:

(1)选择一个随机数$t\in\mathbb{Z}_p$,计算$v=g^t$。

(2)计算$h=H(v,ID)$和$f=h^x$。

(3)计算$r=H_0(f,ID)$。

(4)计算$y=t+rx \bmod p$。

(5)将对应身份 ID 的私钥d_{ID}设置为$d_{\mathrm{ID}}=(f,y)$。

3)签名。给出身份 ID、d_{ID}和消息$m\in\{0,1\}^l$,算法运行如下:

(1)选择一个随机数$k\in\mathbb{Z}_p$,计算$v_0=g^k$。

(2)计算$m'=F_1(m)\parallel F_2(F_1(m))\oplus m$和$w=g^y$。

(3)计算$c=H_1(v_0)\oplus m'$。

(4)计算$c'=H_2(c)$。

(5)计算$s=k+c'y \bmod p$。

(6)消息m和身份 ID 上的签名$\sigma=(f,w,s,c)$。

4)验证。给出身份 ID 和消息m上的签名$\sigma=(f,w,s,c)$,算法运行如下:

(1)计算$r=H_0(f,ID)$。

(2)计算$h=H(wu^{-r},ID)$。

(3)计算$c'=H_2(c)$。

(4)计算$v_0=g^s w^{-c'}$。

(5)计算$m'=H_1(v_0)\oplus c$。

(6)计算$m=[m']_l\oplus F_2([m']^l)$。

(7)验证$\hat{e}(h,u)=\hat{e}(f,g)$和$[m']^{k_1}=F_1(m)$,如果这 2 个等式都成立,则签名$\sigma=(f,w,s,c)$有效;否则,签名无效。

其中,$[m']^l$表示m'中最重要的l位,$[m']_l$表示m'中次重要的l位,$a\oplus b$表示字符串a和b的异或计算(XOR)。

备注　为了在身份 ID 上签名一个较长的消息$m(|m|>l)$,m应该分为m_1和m_2两部分,且$|m_2|=l$,$m=m_1\parallel m_2$,$m_1\parallel m_2$表示字符串m_1和m_2的级联。

签名者生成(f,w,s,c)过程如下:

1)选择一个随机数$k\in\mathbb{Z}_p$,计算$v_0=g^k$。

2)计算$m'=F_1(m_2)\parallel F_2(F_1(m_2))\oplus m_2$和$w=g^y$。

3)计算$c=H_1(v_0)\oplus m'$。

4)计算$c'=H_2(c\parallel m_1)$。

5)计算$s=k+c'y \bmod p$。

6)消息m和身份 ID 上的签名$\sigma=(f,w,s,c)$。

对于上面的方案,假设H_1、H_2、F_1、F_2是密码哈希函数,H和H_0是可以给出类似于 IDSSTR 安全证明的随机预言机。

4　结束语

本文提出一种具有严格安全性规约的 IBS 新方案 IDSSTR。IDSSTR 在线时自然有效,离线阶段不需要额外的条件,验证过程也不变。为了缩短原消息M和附加签名σ的总长度,本文同时也提出了一种具有部分消息恢复功能的 IDSSTR 修改版本。因为 CDH 问题的困难性被广泛地认为与离散对数问题的困难性密切相关,因此,本文提出的 IDSSTR 为其提供了安全保证。下一步将对一些基于身份的密码方案提供新的安全证明以及利用严格的安全规约来构造更实用的方案。

参考文献

[1] ADI S. Identity-based cryptosystems and signature schemes[J]. Lecture Notes in Computer Science, 1984, 21(2): 47-53.

[2] XUN Yi. An identity-based signature scheme from the weil pairing[J]. IEEE Communications Letters, 2003, 7(2): 76-78.

[3] BARRETO P S L M, MCCULLAGH N, QUISQUATER J J. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]//Proceedings of International Conference on Theory and Application of Cryptology and Information Security. Washington D. C., USA: IEEE Press, 2005: 515-532.

[4] BELLARE M, NAMPREMPRE C, NEVEN G. Security proofs for identity-based identification and signature schemes[M]. Berlin, Germany: Springer, 2004.

[5] KUROSAWA K, HENG S H. From digital signature to ID-based identification/signature[C]//Proceedings of International Workshop on Public Key Cryptography. Berlin, Germany: Springer, 2004: 248-261.

[6] DAN B, BEN L, HOVAV S. Short signatures from the weil paring[J]. Journal of Cryptology, 2004, 17(4): 297-319.

[7] CORON J S. Optimal security proofs for PSS and other signature schemes[C]//Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2002: 272-287.

[8] GE S. Tight proofs for signature schemes without random Oracles[C]//Proceedings of International Conference on Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2011: 189-206.

[9] 卢 超, 钱海峰. 标准模型下的在线/离线多签名方案[J]. 计算机应用研究, 2010, 27(9): 3514-3517.

[10] 胡国政, 洪 帆. 标准模型中可证安全的签名方案[J]. 武汉理工大学校报, 2009, 31(15): 130-134.

[11] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[12] 刘振华, 张襄松, 田绪安, 等. 标准模型下基于身份的具有部分消息恢复功能的签名方案[J]. 北京工业大学学报, 2010, 36(5): 654-658.

[13] WANG Z, CHEN H. Emerging directions in embedded and ubiquitous somputing[M]. Berlin, Germany: Springer, 2007.

[14] BELLARE M, ROGAWAY P. The exact security of digital signatures: how to sign with RSA and Rabin[C]//Proceedings of International Conference on Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 1996: 399-416.

[15] MAURER U M, WOLF S. The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms[J]. SIAM Journal on Computing, 1998, 28(5): 1689-1721.

[16] SCHNORR C P. Efficient identification and signatures for smart cards[M]. Berlin, Germany: Springer, 1989.

[17] LIBERT B, QUISQUATER J J. The exact security of an identity based signature and its applications[EB/OL]. [2016-11-25]. https://eprint.iacr.org/2004/102.pdf.

[18] ABE M, OKAMOTO T. A signature scheme with message recovery as secure as discrete logarithm[J]. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 2001, 84(1): 197-204.

编辑 吴云芳

(上接第 173 页)

[9] 叶永宏, 武东英, 陈 扬. 一种基于细粒度污点分析的逆向平台[J]. 计算机工程与应用, 2012, 48(28): 90-96.

[10] 史大伟, 袁天伟. 一种粗细粒度结合的动态污点分析方法[J]. 计算机工程, 2014, 40(3): 12-17.

[11] 宋 铮, 王永剑, 金 波, 等. 二进制程序动态污点分析技术研究综述[J]. 信息网络安全, 2016(3): 77-83.

[12] RODRÍGUEZ R J, ARTAL J A, MERSEGUER J. Performance evaluation of dynamic binary instrumentation frameworks[J]. IEEE Latin America Transactions, 2015, 12(8): 1572-1580.

[13] REDDI V J, JANAPA V, SETTLE A, et al. PIN: a binary instrumentation tool for computer architecture research and education[C]//Proceedings of Workshop on Computer Architecture Education. New York, USA: ACM Press, 2004: 1-7.

[14] 王 乾. 基于动态二进制分析的关键函数定位技术研究[D]. 郑州: 信息工程大学, 2012.

[15] 孔德光, 郑 烇, 帅建梅, 等. 基于污点分析的源代码脆弱性检测技术[J]. 小型微型计算机系统, 2009, 30(1): 78-82.

[16] 黄 昭. 一种改进的动态污点分析模型[D]. 武汉: 华中科技大学, 2011.

[17] WU Weimin, GUO Chaowei, HUANG Zhiwei, et al. Vulnerability exploitation technology of structured exception handling based on windows[J]. Computer Engineering, 2012, 38(20): 5-8.

[18] ZHANG Yufeng, CHEN Zhenbang, WANG Ji, et al. Regular property guided dynamic symbolic execution[C]//Proceedings of the 37th IEEE International Conference on Software Engineering. Washington D. C., USA: IEEE Press, 2015: 643-653.

编辑 顾逸斐