中国科学 F辑: 信息科学 2009 年 第 39 卷 第 2 期: 199～204
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE IN CHINA PRESS

利用二次剩余构造的基于身份的数字签名方案

柴震川, 董晓蕾, 曹珍富*

上海交通大学计算机科学与工程系, 上海 200240
*E-mail: zfcao@cs.sjtu.edu.cn

收稿日期: 2007-03-13; 接受日期: 2007-06-12
国家自然科学基金 (批准号: 60572155, 60673079)、中国高技术研究发展计划 (批准号: 2006AA01Z424) 和国家教育部高等学校博士点基金 (批准号: 20060248008) 资助项目

摘要 近年来, 基于身份的密码学受到了广泛的关注, 基于身份的密码方案大量涌现, 但是其中绝大部分的方案都是基于双线性配对实现的. 因此, 无需配对的基于身份的密码方案一直都是密码界感兴趣的研究方向. 目前, 在利用二次剩余的基础上构造身份签名方案仍然是个未解决的问题, 文中将通过给出一个具体的方案来解决该问题. 首先给出如何有效地计算一个二次剩余的 2^l 次根, 然后由该技巧构造一个具体的基于身份的数字签名方案. 在大整数分解困难问题假设前提下, 提出的方案在随机预言模型下被证明是选择消息和身份安全的.

关键词
基于身份签名
二次剩余
整数分解
随机预言模型
可证安全

1 引言

为了简化证书的管理及降低额外的计算开销, Shamir[1] 在 1984 年提出了基于身份公钥密码学的概念. 按照 Shamir 的思想, 用户不是自己生成一对随机的公私钥对, 而是选择他们的公开可知的身份信息 (比如 Email、电话号码、门牌号码等) 作为公钥, 由一个可信任的私钥分发中心 PKG(private key generator) 按照这些公开可知的身份信息为用户计算出相应的私钥, 并通过秘密渠道分发给用户. 因此, 在基于身份的密码体制下, 通信的一方只需知道对方的 Email、电话号码或者门牌等有明确意义的信息就可以进行加密或签名等密码学操作, 如此可以减去复杂的证书发放和管理机制. 但是直到 2001 年, 基于身份的加密方案 (IBE, identity based encryption) 才被 Boneh 和 Franklin[2] 以及 Cocks[3] 分别实现. 之后, 基于身份的密码体制成为密码学研究的热点, 诸多方案被提出.

现有的大部分基于身份的密码方案是基于 Weil 或者 Tate 配对 [2] 实现的. 由于配对需要很大的计算量, 因此, 构造无需配对的身份密码方案一直都是密码界感兴趣的研究方向. 尽管已有无需配对实现的密码方案, 但是还没有真正基于大整数分解的身份签名方案. 第一个基于身份的数字签名方案是由 Shamir[1] 在 1984 年提出的, 该方案的安全性是基于 RSA 假设, 而 RSA 假设的问题并不等价于大整数分解问题. 之后, Cocks[3] 利用二次剩余构造了一个基于身份的加密方案, 但没有给出签名方案. 近几年, Lee 和 Liao[4] 也提出了不借助于配对的身份数字签名, 但他们的方案是基于离散对数问题的, 而不是分解问题. 这些提出的方案都没有提供可证安全的保证, 所以基于整数分解问题构造有效的可证安全身份签名方案是一项重要的研究课题.

在本文中, 我们首先利用二次剩余的理论构造出一个基于身份的数字签名方案, 然后在随机预言模型下证明该方案是选择消息和身份安全的. 需要指出的是, Qiu 和 Chen[5] 也利用二次剩余构造过身份签名方案, 但是他们的方案需要一个仲裁第三方 (MS, mediated signer) 和用户共同完成签名操作, 因此属于需要仲裁的身份密码体制, 不是我们所讨论的一般概念上的签名方案.

文章组织如下: 在第 2 节, 我们介绍相关基本

概念和工具; 在第 3 节, 我们提出具体方案; 然后在第 4 节给出安全证明; 第 5 节对方案做进一步说明; 第 6 节给出总结.

2 基本概念和工具

本节对一些数学基本概念、结论和工具做一介绍.

2.1 二次剩余

给定正整数 N, 如果整数 a 满足 $\mathrm{GCD}(a,N)=1$, 并且存在整数 x, 使得 $x^2\equiv a(\mathrm{mod}\ N)$, 那么 a 称为整数模 N 下的二次剩余. 其中, x 称为 a 在模 N 下的平方根. 在这里, GCD() 是最大公约数函数.

令 $N=p\times q$ 是一合数, 其中 p 和 q 是两个素数. 再令 Q_N 表示乘法群 Z_N^* 中所有二次剩余组成的子群. 那么关于 Q_N 的一个重要结论是, Q_N 是一个阶为 $\phi(N)/4=(p-1)(q-1)/4$ 的循环群 [6].

定理 1 令 $N=p\times q$, 其中 p 和 q 是满足 $p=2p'+1$, $q=2q'+1$ 的大素数, p' 和 q' 也是大素数, 若给出 $a\in Q_N$, 则满足

$$a^{2d}\equiv a \mod N,$$

其中 $d=(N-p-q+5)/8$.

证明 由于 $a\in Q_N$, 可知 a 的阶为 $\phi(N)/4=(p-1)(q-1)/4=p'q'$, 所以 $a^{p'q'}\equiv 1 \bmod N$. 又因为 $d=(N-p-q+5)/8=[(p-1)(q-1)+4]/8=[4p'q'+4]/8$, 所以容易得到 $a^{2d}\equiv a^{p'q'+1}\equiv a^{p'q'}a\equiv a \bmod N$.

实际上, 定理 1 提供了一个计算二次剩余 $a\in Q_N$ 的平方根的方法, 即计算 a^d. 需要指出的是, 在不知道 N 因子 p, q 的情况下, 是无法计算平方根的.

下面的引理 [7] 在本文的证明中用来计算平方根.

引理 1 若给出 $\omega\neq 0$, $l>0$, $a\in Q_N$ 和 $X\in Z_N^*$, 满足 $a^\omega\equiv X^{2^l} \bmod N$, $\omega<2^l$, 那么可以有效地计算出 a 的平方根 $y(a=y^2 \bmod N)$.

证明 存在整数 γ, δ, 使得 $\omega=2^\gamma(2\delta+1)$. 由条件可得 $(a^{2\delta+1})^{2^\gamma}\equiv a^\omega\equiv X^{2^l}$, 因此 $a^{2\delta+1}\equiv X^{2^{l-\gamma}} \bmod N$. 令 $y=X^{2^{l-\gamma-1}}/a^\delta \bmod N$, 那么容易得知 y 是 a 的平方根, 因为 $y^2\equiv X^{2^{l-\gamma}}/a^{2\delta}\equiv a \bmod N$. 条件$\omega<2^l$的存在是为了满足$l-\gamma-1\geqslant 0$.

2.2 二次剩余的 2^l 次根

为了分析如何计算二次剩余的 2^l 次根, 我们介绍如下定理.

定理 2 令 $N=p\times q$, $d=(N-p-q+5)/8$, 其中 p, q 是满足 $p=2p'+1$, $q=2q'+1$ 的大素数, p' 和 q' 也是大素数, 若 $a=x^2\in Q_N$, 那么 $a^d\in Q_N$.

证明 令 $p'=2k+1$, $q'=2k'+1$, 其中 k 和 k' 是整数, 那么 $d=(N-p-q+5)/8=[(p-1)(q-1)+4]/8=(4p'q'+4)/8=2kk'+k+k'+1$ 也是整数. 由于 $a^d\equiv x^{2d}\equiv (x^d)^2 \bmod N$, 因此易知, $a^d\in Q_N$.

根据定理 1 和 2, 可知对 $a\in Q_N$ 进行 d 次幂运算得到的平方根依然是二次剩余. 因此, 可以对 $a\in Q_N$ 进行 l 次的 d 幂运算, 求得 a 的 2^l 次根, 而不用担心中间结果会出现二次非剩余. 即, a 的 2^l 次根 s 可以按照如下求解:

$$s=a^{d^l}(\mathrm{mod}N),$$

其中 d^l 是在模 $p'q'$ 下运算. 在不知道模 N 分解的情况下, 是无法计算 2^l 次根的.

2.3 大整数分解问题

大整数分解问题是指: 给定一个 k 比特的合数 N, 其中 N 是两个大素数 p 和 q 的乘积, 输出 p 或 q.

目前, 大整数分解问题被认为是 (t,ϵ) 困难的, 这就意味着还没有算法能够在多项式时间 t(由安全参数 k 决定) 内以比 ϵ 更大的概率输出 p 或者 q.

2.4 利用多个平方根分解整数

令 $N=pq$, 其中 p, q 是大素数. 再令 a 为模 N 下的二次剩余, s_1 和 s_2 是 a 的两个平方根, 满足 $s_1\neq \pm s_2 \bmod N$. 那么将 (a,s_1,s_2) 输入到如下的函数 Fac(a,s_1,s_2) 中, 则可以得到 N 的分解:

Fac(a,s_1,s_2): 如果 $s_1\equiv \pm s_2 \bmod N$, 输出 “错误”, 否则输出 $\mathrm{GCD}(s_1+s_2,N)$ 或者 $\mathrm{GCD}(s_1-s_2,N)$ 作为 N 的非平凡因子 (p 或 q).

在描述中, 我们省去了对输入合法性的检测, 即检测 $s_1^2\equiv s_2^2\equiv a \bmod N$, 而直接给出了算法的主要思想.

该函数的正确性主要基于以下事实. 给定一个二次剩余 $a\in Q_N$, a 有 4 个主要的平方根: $1<x$, $N-x$, y, $N-y<N$, 满足 $x\neq \pm y \bmod N$. 不失一般性, 我们选取在模 N 下非正负同余的两个根

x,y 作为研究对象. 由于 $x^2 \equiv y^2 \equiv a \bmod N$, 可知 $(x+y)(x-y) \equiv 0 \bmod N$, 因此 $(x+y)(x-y) = kpq$, k 是一个整数. 同时注意到 $x \neq \pm y \bmod N$, 所以 $x+y$ 和 $x-y$ 一定不是 N 的整数倍, 必含有 N 的因子 p, q.

同理, 利用任何满足 $s_1 \neq \pm s_2 \bmod N$ 的平方根对 (s_1, s_2) 都可以分解 N. 但是, 满足 $s_1 \equiv \pm s_2 \bmod N$ 的平方根对却无法用来分解 N. 可以发现, 若任意给定两个 a 的平方根作为输入, 那么函数 Fac() 只有 1/2 的概率输出 N 的分解.

3 方案的构造

在本节中, 我们利用二次剩余的理论构造出一个基于身份的签名方案 IDSig. 方案 IDSig 包括 4 个子算法, IDSig=(Setup, Extract, Sign, Verify), 构造如下:

Setup(k, l) : 接收输入安全参数 (k, l), 该初始化算法由 PKG 按照如下步骤执行:

1) 生成两个随机大素数 $p = 2p' + 1$, $q = 2q' + 1$, 其中 p' 和 q' 也是大素数, 满足 $2^{k-1} \leqslant (p-1)(q-1)$ 和 $pq < 2^k$, 然后计算 $N = p \times q$.

2) 选择 $a \in Z_N^*$, a 的 Jacobi 符号满足 $(a/N) = -1$.

3) 计算 $d = (N - p - q + 5)/8$.

4) 选择两个单向 Hash 函数 $h_1() : \{0,1\}^* \to Z_N^*$ 和 $h_2() : \{0,1\}^* \to \{0,1\}^l$.

该算法执行完后, PKG 的主密钥为 MK=(p, q, p', q', d), 公开参数为

$$\mathrm{PM} = (N, h_1(), h_2(), a, l).$$

Extract(ID, MK, PM): 给定用户身份信息 ID, 该算法由 PKG 运行, 计算用户的私钥 S_{ID} 和对应标签 $(c_1, c_2) \in \{0,1\}^2$ 如下:

1) 计算 $c_1 = \begin{cases} 0, & \text{if } \left(\dfrac{h_1(\mathrm{ID})}{N}\right) = 1, \\ 1, & \text{if } \left(\dfrac{h_1(\mathrm{ID})}{N}\right) = -1. \end{cases}$

2) 计算 $h = a^{c_1} \cdot h_1(\mathrm{ID})$ and

$$c_2 = \begin{cases} 0, & \text{if } \left(\dfrac{h}{p}\right) = \left(\dfrac{h}{q}\right) = 1, \\ 1, & \text{if } \left(\dfrac{h}{p}\right) = \left(\dfrac{h}{q}\right) = -1. \end{cases}$$

令 $H(\mathrm{ID}) = (-1)^{c_2} \cdot a^{c_1} \cdot h_1(\mathrm{ID})$, 则 $H(\mathrm{ID})$ 是模 N 下的二次剩余, 即 $H(\mathrm{ID}) \in Q_N$. 实际上, $H()$ 可认为是一个映射到二次剩余群的 Hash 函数 $H() : \{0,1\}^* \to Q_N$.

3) 计算 $H(\mathrm{ID})$ 的 2^l 次根 S_{ID} 如下:

$$S_{\mathrm{ID}} \equiv H(\mathrm{ID})^{d^l} \bmod N.$$

S_{ID} 满足 $S_{\mathrm{ID}}^{2^l} \equiv H(\mathrm{ID}) \bmod N$.

执行完该算法后, PKG 将用户私钥 S_{ID} 以及标签 (c_1, c_2) 通过秘密渠道返回给用户.

Sign$(M, S_{\mathrm{ID}}, c_1, c_2,$ PM): 该签名算法由用户执行, 按照如下操作对消息 M 签名:

1) 随机选取 $r \in Z_N^*$, 计算 $R = r^{2^l} \bmod N$.

2) 计算 $\sigma = h_2(R, M)$.

3) 计算 $Z = rS_{\mathrm{ID}}^{\sigma} \bmod N$.

执行完后, 输出签名 sig=$(Z, \sigma, \mathrm{ID}, c_1, c_2)$.

Verify(PM,sig): 给定一个对于消息 M 的签名 $(Z, \sigma, \mathrm{ID}, c_1, c_2)$, 该签名验证算法按照如下步骤检验签名的合法性:

1) 计算 $H(\mathrm{ID}) = (-1)^{c_2} \cdot a^{c_1} \cdot h_1(\mathrm{ID}) \bmod N$.

2) 检查等式 $\sigma = h_2(Z^{2^l}/H^{\sigma}(\mathrm{ID}), M)$ 是否成立. 如果等式成立, 输出 "签名有效", 否则输出 "签名无效".

由于 $Z^{2^l} = (rS_{\mathrm{ID}}^{\sigma})^{2^l} = r^{2^l} S_{\mathrm{ID}}^{2^l \sigma} = RH^{\sigma}(\mathrm{ID})$, 所以 $h_2(Z^{2^l}/H^{\sigma}(\mathrm{ID}), M) = h_2(R, M) = \sigma$, 由此可见方案是正确的.

4 安全性分析

本节给出方案安全性的证明. 我们首先通过描述攻击模型来定义方案的安全性. 然后, 利用 Pointcheval 和 Stern[8,9] 提出的重放 (rewinding) 技术, 在随机预言模型下证明方案是抵抗存在性伪造攻击安全的.

4.1 攻击模型

为了定义合理的攻击模型, 我们应该假设攻击者拥有最大的自由度, 攻击者的手段应该包括现实中可能的行为. 在我们的模型中, 攻击者可以在对若干身份 ID_i $(i = 1, \ldots, n)$ 进行私钥查询后, 再选择目标身份. 并且攻击者在输出伪造签名前, 可以进行多次签名查询.

为了定义安全性, 我们考虑在攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间进行的交互游戏如下:

1) 挑战者 $\mathcal{C}$ 首先生成 PKG 的公开参数 PM, 然后将 PM 公开给 $\mathcal{A}$.

2) 攻击者 $\mathcal{A}$ 进行如下一系列的查询:

私钥查询: 当收到关于 ID 的私钥查询时, 挑战者 $\mathcal{C}$ 运行 Extract() 产生与 ID 对应的私钥 S_{ID} 以及标签 (c_1, c_2), 然后发送给 $\mathcal{A}$.

签名查询: 当收到关于 ID 在消息 M 上的签名查询时, $\mathcal{C}$ 运行 Sign(), 得到有效签名后, 将签名返还给 $\mathcal{A}$.

Hash 查询: 当收到 Hash 函数的查询时, $\mathcal{C}$ 计算相应的 Hash 值后, 将该值返还给 $\mathcal{A}$.

3) $\mathcal{A}$ 最后输出一个对于消息 M 的签名 $(Z, \sigma, \mathrm{ID}, c_1, c_2)$, 满足 $\mathcal{A}$ 并没有对 ID 进行私钥查询, 且也没有对 M 和 ID 进行签名查询.

若 $\mathcal{A}$ 输出的签名有效, 那么认为 $\mathcal{A}$ 在游戏中获胜. $\mathcal{A}$ 获胜的优势定义为

$$\mathrm{Adv}^{\mathrm{EF}}_{\mathrm{IDSig},\mathcal{A}}(k) = Pr[\text{输出的签名有效}].$$

如果没有攻击者能够在询问至多 q_H 次 Hash 询问, q_{sig} 次签名询问的前提下, 在时间 t 内, 以比 ϵ 更大的优势获得胜利, 那么该基于身份的签名方案就被定义为可抵抗选择消息和身份的存在性伪造攻击的 $(t, q_H, q_{\mathrm{sig}}, \epsilon)$ 安全方案.

4.2 安全性证明

本节利用 Pointcheval 和 Stern[8,9] 提出的重放证明技巧, 证明方案的安全性.

定理 3 如果整数分解问题是 (t', ϵ') 困难的, 那么方案 IDSig 是 $(t, q_{h_2}, q_{\mathrm{sig}}, \epsilon)$ 安全的, 满足

$$\epsilon' \geqslant \frac{(\epsilon - 2^{3-k} q_{\mathrm{sig}}(q_{h_2} + q_{\mathrm{sig}}))^2}{2(q_{h_2}+1)} - \frac{\epsilon - 2^{3-k} q_{\mathrm{sig}}(q_{h_2} + q_{\mathrm{sig}})}{2^{l+1}},$$

$$t' = 2t + O(k^2 l + k^3),$$

其中 (k, l) 是安全参数.

证明 采用反证法的思路进行证明, 假设方案 IDSig 不安全, 也就是说在定义的攻击模型下, 存在一个攻击者 $\mathcal{A}$, 可以不可忽略概率优势攻击方案 IDSig, 那么我们就可以构造算法 $\mathcal{B}$ 来有效地解决整数分解问题. 然而这就与定理中整数分解困难相矛盾, 所以假设不成立, IDSig 是安全的.

现在说明算法 $\mathcal{B}$ 是如何被构造的. $\mathcal{B}$ 的任务是解决一个整数分解问题的实例, 也就是给定一个输入 $N = p \times q$ ($\mathcal{B}$ 不知道 p 和 q), 以不可忽略的概率优势输出 p 或 q.

$\mathcal{B}$ 按照如下的操作模拟 4.1 小节描述的游戏和 $\mathcal{A}$ 交互.

1) $\mathcal{B}$ 选取 Jacobi 符号满足 $(a/N) = -1$ 的整数 $a \in Z_N^*$, 选取整数 $l \geqslant 160$, 然后将参数 (N, a, l) 发送给 $\mathcal{A}$ 作为系统公开参数. $\mathcal{B}$ 同时维护一个签名询问列表和两个 Hash 询问列表.

2) 然后 $\mathcal{B}$ 回答 $\mathcal{A}$ 的一系列询问如下:

h_1- 询问: 为了响应 $\mathcal{A}$ 的 h_1 查询, $\mathcal{B}$ 维护了一个 h_1 列表, 表中的每项是五元组 $\langle \mathrm{ID}, h_1, s, c_1, c_2 \rangle$, 其中 ID 是被询问的身份, h_1 是 $\mathcal{B}$ 的回答, $(c_1, c_2) \in \{0,1\}^2$ 和 $s \in Z_N^*$ 是内部参数. 当 $\mathcal{A}$ 对身份 ID 进行 Hash 查询时, 如果 h_1 列表中含有项 $\langle \mathrm{ID}, h_1, s, c_1, c_2 \rangle$, 那么 $\mathcal{B}$ 将 h_1 作为 Hash 值返回, 否则, $\mathcal{B}$ 选择一个随机数 $s \in Z_N^*$ 和两个随机比特 $(c_1, c_2) \in \{0,1\}^2$, 并将 $h_1 = s^{2^l} / [(-1)^{c_2} a^{c_1}] \bmod N$ 作为答案返回, 然后在 h_1 列表中加入新的项 $\langle \mathrm{ID}, h_1, s, c_1, c_2 \rangle$.

h_2- 询问: 为了响应 $\mathcal{A}$ 的 h_2 查询, $\mathcal{B}$ 维护了一个 h_2 列表, 表中的每项是三元组 $\langle R, M, h_2 \rangle$, 其中 (R, M) 是被询问的信息, h_2 是 $\mathcal{B}$ 的回答.

当 $\mathcal{A}$ 对 (R, M) 进行 Hash 查询时, 如果 h_2 列表中含有项 $\langle R, M, h_2 \rangle$, 那么 $\mathcal{B}$ 将 h_2 作为 Hash 值返回, 否则, $\mathcal{B}$ 选择一个随机数 $h_2 \in Z_N^*$, 并将 h_2 作为答案返回, 然后在 h_2 列表中加入新的项 $\langle R, M, h_2 \rangle$.

私钥查询: 当收到关于 ID 的私钥查询时, $\mathcal{B}$ 首先在 h_1 列表中搜索是否存在项 $\langle \mathrm{ID}, h_1, s, c_1, c_2 \rangle$, 若存在, 则返回 $S_{\mathrm{ID}} = s$ 以及 (c_1, c_2), 否则 $\mathcal{B}$ 将如同在 h_1 查询中一样在 h_1 列表中添加包含 ID 的新项, 并返回 $S_{\mathrm{ID}} = s$ 以及 (c_1, c_2).

签名查询: 当收到要求 M 在身份 ID 下的签名时, $\mathcal{B}$ 首先在 h_1 列表中找到包含 ID 项, 并计算 $H_{\mathrm{ID}} = (-1)^{c_2} a^{c_1} h_1(\mathrm{ID})$, 然后随机选取 $Z \in Z_N^*$ 和 $\sigma \in \{0,1\}^l$, 如果 $(R' = Z^{2^l} / H^{\sigma}_{\mathrm{ID}}, M)$ 已经在 h_2 列表中出现, $\mathcal{B}$ 终止游戏, 否则, $\mathcal{B}$ 返回 $(Z, \sigma, \mathrm{ID}, c_1, c_2)$ 作为签名, 并将 $(R' = Z^{2^l} / H^{\sigma}_{\mathrm{ID}}, M, \sigma)$ 添加到 h_2 列表中.

3) $\mathcal{A}$ 最后输出一个对于消息 M^* 的签名 $(Z^*, \sigma^*, \mathrm{ID}^*, c_1, c_2)$, 满足 $\mathcal{A}$ 并没有对 ID^* 进行私钥查询, 且也没有对 M^* 和 ID^* 进行签名查询.

为了分解 N, 我们需要利用重放技术让 $\mathcal{B}$ 重新与 $\mathcal{A}$ 进行第 2 次游戏. 在第 2 次的交互中, 给 $\mathcal{A}$ 与第 1 次交互完全相同的随机输入带, 而 $\mathcal{B}$ 对于 $\mathcal{A}$ 的询问也给出与第 1 次交互完全相同的回答. 直到 $\mathcal{A}$ 对某点进行 h_2 查询, 而该查询在第 1 次游戏中返回值为 σ^* 时, $\mathcal{B}$ 停止输出 σ^*, 而从新选择一个不同的值 $\tau^* \in \{0,1\}^l$ 作为这次该点在 h_2 查询的输出. h_1 的查询不受影响, 两次游戏的输出完全一样.

如果 $\mathcal{A}$ 在第 2 次游戏后, 能输出对于消息 M^* 的签名. 那么 $\mathcal{B}$ 将获得一对签名 $(Z^*, \sigma^*, \mathrm{ID}^*, c_1, c_2)$ 和 $(Z', \tau^*, \mathrm{ID}^*, c_1, c_2)$, 则该签名对满足

$$Z^{*2^l}/H^{\sigma^*}(\mathrm{ID}^*) \equiv Z'^{2^l}/H^{\tau^*}(\mathrm{ID}^*) \bmod N$$
$$\Rightarrow H^{(\tau^*-\sigma^*)}(\mathrm{ID}^*) \equiv (Z'/Z^*)^{2^l} \bmod N,$$

其中 $H(\mathrm{ID}^*) = (-1)^{c_2} \cdot a^{c_1} \cdot h_1(\mathrm{ID}^*)$.

根据引理 1, 若令 $a = H(\mathrm{ID}^*), \omega = \tau^* - \sigma^*$, $X = Z'/Z^*$, 那么 $\mathcal{B}$ 可以算出 $H(\mathrm{ID}^*)$ 的平方根 s'.

然后, $\mathcal{B}$ 在 h_1 列表中查找项 $\langle \mathrm{ID}^*, h_1, s, c_1, c_2 \rangle$, 注意到 $s^{2^{l-1}}$ 也是 $H(\mathrm{ID}^*) = (-1)^{c_2} \cdot a^{c_1} \cdot h_1(\mathrm{ID}^*)$ 的一个平方根, 所以如果 $s' \neq \pm s^{2^{l-1}} \bmod N$, 那么通过计算在 2.4 小节中介绍的函数 $\mathrm{Fac}(H(\mathrm{ID}^*), s', s^{2^{l-1}})$, $\mathcal{B}$ 可以最终得到 N 的分解, 否则 $\mathcal{B}$ 输出 "失败". 值得说明的是, s 是由 $\mathcal{B}$ 独立于 $\mathcal{A}$ 选取的 $H(\mathrm{ID}^*)$ 的 2^l 次根, 所以事件 $s' \equiv \pm s^{2^{l-1}} \bmod N$ 的概率为 $1/2$.

为了分解 N, $\mathcal{B}$ 需要和 $\mathcal{A}$ 进行 2 次的游戏交互, 以及一些诸如模 N 上的幂运算等操作, 所以 $\mathcal{B}$ 需要大约 $t' = 2t + O(k^2 l + k^3)$ 的时间分解 N.

令 ϵ' 表示成功分解 N 的概率, ϵ 表示 $\mathcal{A}$ 在真实游戏中获胜 (伪造签名) 的概率, ϵ^* 表示在一次模拟游戏中伪造签名的概率.

在游戏过程中, $\mathcal{B}$ 对 Z 的选取是随机的, 这就可能导致 $Z^{2^l}/H^{\sigma}_{\mathrm{ID}}$ 与 h_2 列表中已经存在的值发生碰撞. 由于 h_2 列表是由 h_2 查询和签名查询过程填充的, 所以这种碰撞的概率是 $(q_{h_2} + q_{\mathrm{sig}})/|Q_N|$, 其中, q_{h_2} 是 h_2 查询最大次数, q_{sig} 是签名查询最大次数. 如果碰撞发生, $\mathcal{B}$ 将终止游戏, 所以在模拟游戏中 $\mathcal{A}$ 获得胜利 (伪造签名) 的概率计算为

$$\begin{aligned}\epsilon^* &= \epsilon - q_{\mathrm{sig}}(q_{h_2} + q_{\mathrm{sig}})/|Q_N| \\ &\geqslant \epsilon - q_{\mathrm{sig}}(q_{h_2} + q_{\mathrm{sig}}) \cdot 2^{3-k}.\end{aligned}$$

令 p_h 是在模拟游戏中, 伪造的签名是基于第 h 次 h_2 查询的概率. 则有

$$\epsilon^* = \sum_{h=1}^{q_{h_2}+1} p_h.$$

令 $p_{h,s}$ 是在给定一个长度为 m 的特定的随机输入带 s 的情况下, 伪造的签名是基于第 h 次 h_2 查询的概率. 则有

$$2^m p_h = \sum_{s \in \{0,1\}^m} p_{h,s}.$$

对一个指定的输入带 s 的, 两次游戏得到的伪造签名都是基于第 h 次 h_2 查询的概率为 $p_{h,s}(p_{h,s} - 2^l)$, 这是因为第 2 轮游戏中对第 h 次 h_2 查询的回答不同与第 1 轮的回答. 令 P_h 为两轮游戏得到的伪造签名都是基于 h 次 h_2 查询的概率, 那么有

$$\begin{aligned}P_h &= \sum_{s \in \{0,1\}^m} 2^{-m} p_{h,s}(p_{h,s} - 2^{-l}) \\ &= 2^{-m}\left(\sum_{s \in \{0,1\}^m} p_{h,s}^2 - 2^{-l} \sum_{s \in \{0,1\}^m} p_{h,s}\right) \\ &\geqslant \frac{2^{-m}(p_h 2^m)^2}{2^m} - 2^{-l} p_h = p_h^2 - 2^{-l} p_h.\end{aligned}$$

因此, $\mathcal{A}$ 在两轮游戏中基于同样 h_2 询问得到两个伪造签名的概率为

$$\begin{aligned}\sum_{h=1}^{q_{h_2}+1} P_h &\geqslant \sum_{h=1}^{q_{h_2}+1} p_h^2 - \sum_{h=1}^{q_{h_2}+1} 2^{-l} p_h \geqslant \frac{\epsilon^{*2}}{q_{h_2}+1} - 2^{-l}\epsilon^* \\ &\geqslant \frac{(\epsilon - 2^{3-k} q_{\mathrm{sig}}(q_{h_2} + q_{\mathrm{sig}}))^2}{q_{h_2}+1} \\ &\quad - \frac{\epsilon - 2^{3-k} q_{\mathrm{sig}}(q_{h_2} + q_{\mathrm{sig}})}{2^l}.\end{aligned}$$

由于得到基于相同 h_2 询问的两个伪造签名就可以有 $1/2$ 的概率分解 N (如前所述, 计算 $\mathrm{Fac}(H(\mathrm{ID}^*), s', s^{2^{l-1}})$), 所以 $\epsilon' \geqslant \sum_{h=1}^{q_{h_2}+1} P_h/2$. 结合上式, 定理结论得证.

5 讨论

在本方案中, $h_2()$ 值存在二义性. 从定义上看, $h_2() : \{0,1\}^* \to \{0,1\}^l$ 是一个映射到长度为 l 的比

特串空间上. 然而, $h_2()$ 又充当了数值进行运算 (比如 $Z = rS_{\mathrm{ID}}^{h_2()} \mod N$). 实际上, 该二义性并不影响方案的正确性, 因为 $h_2()$ 不需任何转化就可以当作数值进行运算.

方案参数 l 的选择体现了效率和安全性的折中. 方案中耗时的计算是对某个数进行幂 2^l 计算, 所以 l 应该越小越好, 然而太小的 l 值意味着 $h_2() : \{0,1\}^* \to \{0,1\}^l$ 输出空间小, 导致方案不安全. 所以 l 也不能太小, 可以选取 160.

6 结论

本文首先给出了一个计算二次剩余的 2^l 次根的有效方法, 然后利用该结论构造了一个无需配对实现的基于身份的数字签名方案. 在整数分解问题困难的假设下, 该方案在随机预言模型下被证明为可抵抗选择消息和身份的存在性伪造攻击安全的方案.

参考文献

1 Shamir A. Identity based cryptosystems and signature schemes. In: Advances in Cryptology-Crypto'84. Lecture Notes in Computer Science, Vol 196. Berlin: Springer-Verlag, 1984. 47–53

2 Boneh D, Franklin M. Identity-based encryption from the Weil Pairing. In: Advances in Cryptology-Crypto 2001. Lecture Notes in Computer Science,Vol 2193. Berlin: Springer-Verlag, 2001. 213–229

3 Cocks C. An identity based encryption scheme based on quadratic residues. In: Cryptography and Coding. Lecture Notes in Computer Science, Vol 2260. Berlin: Springer-Verlag, 2001. 360–363

4 Lee W B, Liao K C. Constructing identity-based cryptosystems for discrete logarithm based cryptosystems. J Netw Comput Appl, 2004, 27: 191–199

5 Qiu W D, Chen K F. Identiy oriented signature scheme based on quadratic residues. Appl Math Comput, 2005, 168: 235–242

6 Shoup V. A Computational Introduction to Number Theory and Algebra. Singapore: Cambridge University Press, 2005. 534

7 Abdalla M, Reyzin L. A new forward-secure digital signature scheme. In: Asiacrypt 2000. Lecture Notes in Computer Science, Vol 1976. Berlin: Springer-Verlag, 2000. 116–129

8 Pointcheval D, Stern J. Security proofs for signature schemes. In: Proceedings of Eurocrypt'96. Lecture Notes in Computer Science, Vol 1070. Berlin: Springer-Verlag, 1996. 387–398

9 Pointcheval D, Stern J. Security arguments fot digital signatures and blind signatures. J Cryptol, 2000, 13: 361–396