文章编号:1671-5497(2006)Suppl. 2-0134-05

基于RSA的三次传递不可否认签名方案

裴士辉,赵宏伟

(吉林大学 计算机科学与技术学院,长春 130022)

摘 要:提出了一个新的基于RSA的不可否认签名方案,该方案的确认协议和否认协议是三次传递的,因而提高了效率。该方案同时实现了可转换性,可以把不可否认签名方案转换成通常的RSA数字签名方案。方案在随机问答器模型下证明是安全的,其不可伪造性等同于CDH(Computational Diffie-Hellman)问题;不可分辨性等同于DDH(Decisional Diffie-Hellman)问题;不可扮演性等同于离散对数问题。

关键词:计算机工程;信息安全;不可否认签名;证据不可分辨性;不可伪造性;不可扮演性
中图分类号:TP309 **文献标识码**:A

RSA-based 3-move undeniable signatures scheme

Pei Shi-hui, Zhao Hong-wei
(*College of Computer Science and Technology, Jilin University, Changchun* 130022, *China*)

Abstract: A new RSA-based undeniable signature scheme was proposed which is more efficient because of its 3-move confirmation and disavowal protocols. The scheme is convertable and can be converted into the conventional RSA digital signature scheme. The scheme was proved secure against the active and concurrent attacks in the random oracle model. The existential unforgeability of the proposed scheme is equivalent to the computational Diffie-Hellman problem and its witness indistinguishableness is equivalent to the decisional Diffie-Hellman problem. Its anti-impersonation ability is equivalent to the discrete logarithm problem.

Key words: computer engineering; information security; undeniable signature; witness indistinguishableness; unforgeability; anti-impersonation ability

不可否认签名的概念是1989年由Chaum和Antwerpen首先提出的[1]。对于标准的数字签名,任何人都可以验证签名的有效性,与此不同,不可否认签名的有效性的验证必须经过签名人的允许,通过执行确认协议或否认协议来实现。不可否认签名方案主要应用于发放软件许可[1]、电子现金以及电子选举和拍卖等方面。在过去16年中,人们对不可否认签名进行了广泛的研究,并构造了不同的不可否认签名方案。其中有的方案是基于离散对数问题的[2-5],有的方案是基于RSA协议构建的[6-8],还有的方案是基于身份的对(pairing)加密协议构造的[9]。这些方案的安全性不同,而且各自增加了不同的特性,有的方案增加了可转换性[3,8],有的方案增加了指定验证人的特性,有的方案增加了指定确认人的特性[2,10]。

不可否认签名方案的确认协议和否认协议的

收稿日期:2005-04-13.
基金项目:高等学校博士学科点专项科研基金资助项目(20050183032);吉林省教育厅科学基金项目(2005180、2005181).
作者简介:裴士辉(1969-),男,讲师,博士研究生. 研究方向:应用密码学. E-mail:shihui_pei@sina.com
通讯联系人:赵宏伟(1962-),男,教授,博士生导师. 研究方向:计算机应用. E-mail:zhaohw@jlu.edu.cn.

传递次数直接影响整个方案的效率。目前,基于 RSA 的不可否认签名方案的确认协议至少需要四次传递,而否认协议的传递次数是非固定的。作者在文献[4]和文献[6]的基础上提出了一个新的基于 RSA 的不可否认签名方案,它具有如下特点:①方案的确认和否认协议是三次传递的,即第一次是签名人 S 向验证人 V 传递消息 a;第二次是验证人 V 向签名人 S 传递消息 b;第三次是签名人 S 向验证人 V 传递消息 c。②具有可转换性,可以转换成通常的 RSA 数字签名方案。③对于主动/并发攻击,在随机问答器(random oracle)模型下证明是安全的,其不可伪造性等同于 CDH (Computational Diffie-Hellman) 问题,不可分辨性等同于 DDH (Decisional Diffie-Hellman)问题,不可扮演性等同于离散对数问题。

1　预备知识

1.1　困难性假设

令 $G = <g>$ 是一个有限循环群,g 为其生成元,其阶 $u = \#G$。

假设 1 (DDH 假设) 不存在这样的概率多项式时间算法,该算法能以不可忽略的概率区分出分布 D 和 R,这里,$D = (g, g^x, g^y, g^z)$, $x, y, z \in Z_u$, $R = (g, g^x, g^y, g^{xy})$, $x, y \in Z_u$。

另外,对于元组(g, g^x, g^y, g^z),如果 $z = xy$,则称其为一个 DH-元组;否则称其为非 DH-元组。

假设 2 (CDH 假设) 已知 $g, g^x, g^y \in G$,不存在这样的概率多项式时间算法,该算法能以不可忽略的概率计算出 $g^{xy} \in G$。

1.2　构造二次剩余子群

令 n 是一个安全的 RSA 模数($n = pq$,其中 $p = 2p' + 1$, $q = 2q' + 1$, p、q、p'、q'都是质数),由阶是 $p'q'$的元素生成的模 n 的二次剩余子群记为 $QR(n)$。$QR(n)$是一个有限循环群,其阶为 $p'q'$。可以根据如下引理构造 $QR(n)$。

引理 1 令 $n = pq$,其中 $p \neq q$, $p = 2p' + 1$, $q = 2q' + 1$,并且 p、q、p'、q'都是质数。Z_n^* 中的元素周期的集合为$\{1, 2, p', q', 2p', 2q', p'q', 2p'q'\}$。特别是当且仅当 $gcd(a \pm 1, n) = 1$ 时[11], $a \in Z_n^*$ 的周期为 $p'q'$或 $2p'q'$。

根据引理 1,可以用如下方法寻找 $QR(n)$的生成元 g:选择 $a \in Z_n^*$,并且 $gcd(a \pm 1, n) = 1$,令 $g = a^2 \bmod n$。那么 $QR(n) = <g>$。

2　新的不可否认签名方案

2.1　方案组成

新的方案分为如下 4 个部分。

(1) 密钥生成: 选取一个安全的 RSA 模数 n, $n = pq$,其中 $p = 2p' + 1$, $q = 2q' + 1$, p、q、p'、q'都是质数。选取 $e \in Z_{\varphi(n)}^*$,并计算 e 的乘逆 d,满足 $ed = 1 \bmod \varphi(n)$; 选取 $g \in_R QR(n)$,并且 g 的周期为 $p'q'$。计算 $y = g^d \bmod n$。选择一个无碰撞 hash 函数 $H: \{0, 1\}^* \rightarrow <g>$。设置公钥为$(n, g, y, H)$,私钥为$(e, d)$。

(2) 签名:输入公钥(n, g, y, H)、私钥(e, d)以及消息 $m \in \{0, 1\}^*$,算法输出签名 $\sigma = H(m)^d \bmod n$。

(3) 确认协议: 签名人使用证据不可区分协议来证明$(g, y, H(m), \sigma)$是一个 DH-元组,其中(m, σ)是有效的消息-签名对。

(4) 否认协议: 签名人使用证据不可区分协议来证明$(g, y, H(m), \sigma)$是一个非 DH-元组,其中(m, σ)是无效的消息-签名对。

2.2　DH-元组的证据不可区分协议

证据不可区分(witness indistinguishable, WI)的概念是由 Feige 和 Shamir 提出的[12]。该类协议通常是一个包含证实人和验证人的双方协议,对于某个 NP 断言,证实人使用几个证据中的一个进行证实,如果验证人无法说出证实人在实际中使用的是哪一个证据,那么协议就称为不可区分的。

在本协议中,证实人使用两个证据中的一个证明一个元组是否为 DH-元组,但验证人无法分辨证实人使用的是哪一个证据,因此是证据不可区分的。

在确认协议中,签名人要向验证人证明$(g, y, H(m), \sigma)$是一个 DH-元组,其中 y 为签名人的公钥,$y = g^d$;σ 为有效的签名 $\sigma = H(m)^d \bmod n$, $H(m) \in <g>$。假设 $H(m) = g^u$,那么上述元组等同于(g, g^d, g^u, g^{ud}),为一个 DH-元组。观察到在元组中有两个证据 d 和 u,证实人在使用证据不可区分协议向验证人证实上述元组是 DH-元组时需要知道 d 或者 u,这里证实人只知道 d,但不知道 u。下面给出具体的三次传递的证据不可区分确认协议。

(1) 证实人随机选取 c_2, $d_2 \in Z_n$,计算 $z_3 = g^{d_2}/H(m)^{c_2} \bmod n$, $z_4 = y^{d_2}/\sigma^{c_2} \bmod n$。再另外随

机地选取 $r \in Z_n$,并计算 $z_1 = g^r \bmod n$ 和 $z_2 = H(m)^r \bmod n$。然后,把(z_1, z_2, z_3, z_4)发送给验证人。

(2) 验证人随机选取 $c \in Z_n$,并将 c 发送给证实人。

(3) 证实人计算 $c_1 = c - c_2 \bmod p'q'$, $d_1 = r + c_1 d \bmod p'q'$,然后把$(c_1, c_2, d_1, d_2)$发送给验证人。

(4) 验证人检查如下等式是否成立:$g^c = g^{c_1} g^{c_2} \bmod n$, $g^{d_1} = z_1 y^{c_1} \bmod n$, $H(m)^{d_1} = z_2 \sigma^{c_1} \bmod n$; $g^{d_2} = z_3 H(m)^{c_2} \bmod n$, $y^{d_2} = z_4 \sigma^{c_2} \bmod n$。如果上述等式全部成立,则确认$(g, y, H(m), \sigma)$是一个 DH-元组,从而确认签名的有效性。

2.3 非 DH-元组的证据不可区分协议

在否认协议中,签名人要向验证人证明$(g, y, H(m), \sigma)$是一个非 DH-元组,其中 y 为签名人的公钥,$y = g^d$;σ 为无效的签名,$\sigma \neq H(m)^d \bmod n$。假设 $H(m) = g^u$,那么上述元组等同于$(g, g^d, g^u, \sigma \neq g^{ud})$,为一个非 DH-元组。下面给出具体的三次传递的证据不可区分否认协议。

(1) 证实人随机选取 $c_2, d_3, d_4 \in Z_n$,并随机选取 $A_1 \in <g>$,其中 $A_1 \neq 1$,然后计算

$$z_3 = y^{d_3}/(\sigma^{d_4} A_1^{c_2}) \bmod n$$

$$z_4 = g^{d_3}/H(m)^{d_4} \bmod n \text{ 。}$$

再另外随机地选取 $r \in Z_n$,并计算 $A = (H(m)^d/\sigma^r) \bmod n$。

然后,证实人随机地选取 $\alpha, \beta \in Z_n$,并计算

$z_1 = H(m)^{\alpha}/\sigma^{\beta} \bmod n$, $z_2 = g^{\alpha}/y^{\beta} \bmod n$。

最后,把 $(A, A_1, z_1, z_2, z_3, z_4)$发送给验证人。

(2) 验证人首先检查 $A \neq 1$ 和 $A_1 \neq 1$ 是否成立。如果成立,随机地选取 $c \in Z_n$, 并将 c 发送给证实人;否则,退出协议。

(3) 证实人计算 $c_1 = c - c_2 \bmod p'q'$, $d_1 = \alpha + c_1(dr) \bmod p'q'$, $d_2 = \beta + c_1 r \bmod p'q'$,然后把$(c_1, c_2, d_1, d_2, d_3, d_4)$发送给验证人。

(4) 验证人检查如下等式是否成立

$$g^c = g^{c_1} g^{c_2} \bmod n,$$

$H(m)^{d_1}/\sigma^{d_2} = z_1 A^{c_1} \bmod n$, $g^{d_1}/y^{d_2} = z_2 \bmod n$; $y^{d_3}/\sigma^{d_4} = z_3 A^{c_2} \bmod n$, $g^{d_3}/H(m)^{d_4} = z_4 \bmod n$。如果上述等式全部成立,则确认$(g, y, H(m), \sigma)$是一个非 DH-元组,从而确认签名的无效性。

2.4 可转换性

可转换不可否认签名方案允许签名人公布一个值,使用该值可以将不可否认签名转换成所有人都可以自行验证的通常的数字签名。在本方案中,签名人可以公布私钥中的 $e = d^{-1} \bmod \varphi(n)$。这样就把不可否认签名方案转换成具有公钥$(n, e)$的通常的 RSA 数字签名方案。其安全性也与通常的 RSA 数字签名方案相同。

3 安全性

不可否认签名方案的安全性分为不可伪造性、不可分辨性和不可扮演性三个方面。下面分别给出相应的形式化定义和安全分析。

3.1 不可伪造性

为了给出不可伪造性的形式化定义,首先考虑下面的攻击过程:

(1) 令 pk 为伪造者 F 的公钥输入。

(2) 允许 F 进行①签名查询:F 向签名问答器提交消息 m,并得到对 m 的签名 σ;②确认/否认查询:F 提交消息-签名对(m, σ),确认/否认问答器检查(m, σ)的有效性,如果有效,问答器输出位变量 $\mu = 1$,并与 F 一同执行确认协议;否则,问答器输出位变量 $\mu = 0$,并与 F 一同执行否认协议。

(3) 在攻击过程的最后,F 输出一个消息-签名对(m^*, σ^*)。如果 F 输出的消息-签名对(m^*, σ^*)是有效的,同时 m^* 从来没有向签名问答器查询过,则称 F 在攻击过程中获胜。

F 的优势定义为:$Adv(F) = Pr[F \text{ 获胜}]$。

定义 1 如果在上述自适应选择消息攻击过程中,不存在具有不可忽略优势的概率多项式时间(probabilistic polynomial time, PPT)的伪造者 F, 则方案具有不可伪造性。

理论 1 对于主动攻击和并发攻击, 不可否认签名方案的不可伪造性在 random oracle 模型下等同于 CDH 问题。

限于篇幅,关于理论 1 的证明只给出概要的证明过程。需要证明:如果存在一个优势为 ε_F 的伪造者 F,则可以把 F 作为子程序,构造一个解决 CDH 问题的算法 M。

假设 M 的输入为$(g, g^d \bmod n, g^z \bmod n)$。$M$ 配置 F 的公钥为$(n, g, y = g^d, H)$,其中 H 是由 M 模拟的随机问答器。另外 M 也模拟签名问答器和确认/否认问答器。

首先,F 对 M 模拟的随机问答器进行 H 查询,当 F 查询消息 m_i 时,M 以 δ 的概率返回值 $h_i = H(m_i) = g^{v_i}$,以 $1-\delta$ 的概率返回值 $h_i = H(m_i) = (g^z)^{v_i}$,其中 $v_i \in_R Z_n$ 是 M 随机选取的。假设 F 进行 H 查询的次数为 q_H。

然后,F 对 M 模拟的签名问答器进行签名查询。假设 F 对一个消息进行签名查询之前已经进行过 H 查询。F 查询消息 m_i,如果在 H 查询中 M 的对应输出是 $h_i = H(m_i) = g^{v_i}$,那么 M 返回 $\sigma_i = y^{v_i}$ 作为有效的签名(因为 $y^{v_i} = (g^d)^{v_i} = h_i^d = H(m_i)^d$);否则,$M$ 退出并停止解决 CDH 问题。假设 F 进行签名查询的次数为 q_S。

接着,F 按照形式化定义攻击过程中的方法查询由 M 模拟的确认/否认问答器。假设 F 的查询次数为 q_V。

最后,F 输出有效的消息-签名对(m^*, σ^*),其中 m^* 没有查询过签名问答器。假设 F 已经对 m^* 进行过 H 查询并且在第 j 次查询中有 $m^* = m_j$。如果 $h_j = (g^z)^{v_j}$,那么 $\sigma^* = h_j^d = (g^{zv_j})^d$。$M$ 输出 $g^{dz} = (\sigma^*)^{1/v_j}$,并把它作为解决 CDH 问题的结果。

在上述过程中,M 对所有的签名查询都回答的概率为 δ^{q_S},M 输出 $(g^z)^{v_j}$ 的概率为 $1-\delta$,这样,M 不退出的概率为 $\delta^{q_S}(1-\delta)$,其中 δ 的最大值为 $\delta_{\max} = 1 - 1/(q_S+1)$。当 q_S 值增大时,$(1-1/(q_S+1))^{q_S}$ 的值接近于 $1/e$,e 为自然对数的底。因此,M 的优势 ε_M 至少为 $(1/e(1+q_S))\ \varepsilon_F$。

3.2　不可分辨性

不可分辨性是指:已知一个消息-签名对,无法判断其有效性。

为了给出不可分辨性的形式化的定义,首先考虑下面的攻击过程:

(1) 令 pk 为分辨者 D 的公钥输入。

(2) 允许 D 进行像 3.1 节中的伪造者 F 一样进行签名查询和确认/否认查询。

(3) D 输出一个从来没有向签名问答器查询的消息 m^*,并且需要一个对 m^* 的挑战签名 σ^*。其中挑战签名 σ^* 是根据对一个不公开的位变量 b 投硬币来决定的。若 $b=1$,那么 σ^* 由签名问答器产生;否则在签名空间 S 中随机选择 σ^*。

(4) D 继续进行签名查询和确认/否认查询,但是不允许对 m^* 进行签名查询,也不允许对挑战的消息-签名对(m^*, σ^*)进行确认/否认查询。

(5) 在攻击过程的最后,D 输出一个对位变量 b 的猜测 b'。如果 $b' = b$,那么 D 在攻击过程中获胜。D 在攻击过程中的优势为 $Adv(D) = |Pr[b' = b] - 1/2|$。

定义 2　如果在上述自适应选择消息攻击过程中,不存在具有不可忽略优势的概率多项式时间的分辨者 D,则不可否认签名方案具有不可分辨性。

理论 2　对于主动攻击和并发攻击,不可否认签名方案的不可分辨性在 random oracle 模型下等同于 DDH 问题。

理论 2 的证明与理论 1 的证明相似。

3.3　不可扮演性

为了给出不可扮演性的形式化的定义,首先考虑下面的攻击过程:

(1) 令 pk 为扮演者 I 的公钥输入。

(2) I 进入学习阶段,在该阶段进行像 3.1 节中的伪造者 F 一样进行签名查询和确认/否认查询。在该阶段结束后,I 输出一个元组(m^*, σ^*, μ),若 $\mu=1$,表示消息-签名对$(m*, \sigma^*)$是有效的;若 $\mu=0$,表示消息-签名对$(m*, \sigma^*)$是无效的。

(3) I 进入扮演阶段,若 $\mu=1$,对于消息-签名对$(m*, \sigma^*)$,I 以证实人的身份和验证人一同执行确认协议;若 $\mu=0$,对于消息-签名对(m^*, σ^*),I 以证实人的身份和验证人一同执行否认协议。

如果扮演者 I 可以根据 μ 的不同值使验证人相信(m^*, σ^*)的有效性或无效性,那么 I 就在攻击过程中获胜。I 在攻击过程中的优势 $Adv(I) = Pr[I\text{ 获胜}]$。

定义 3　如果在上述自适应选择消息攻击过程中,不存在具有不可忽略优势的概率多项式时间的扮演者 I,则不可否认签名方案具有不可扮演性。

理论 3　对于主动攻击和并发攻击,方案的不可扮演性在 random oracle 模型下等同于离散对数问题。

限于篇幅,关于理论 3 的证明只给出概要的证明过程。需要证明如果存在一个优势为 ε_I 的扮演者 I,那么可以把 I 作为子程序,构造一个解决离散对数问题的算法 M。

假设 M 的输入为$(g, g^d \bmod n)$。M 配置 F

的公钥为$(n, g, y=g^d \bmod n, H)$,其中n为M确定的安全的RSA模数,H是由M模拟的随机问答器。另外,M也模拟签名问答器和确认/否认问答器。

在学习阶段,I进行一系列的查询。如果I对消息m_i进行H查询,M返回值$h_i=H(m_i)=g^{v_i}$,其中$v_i \in_R Z_n$是M随机选取的。如果I对消息m_i进行签名查询,则M返回$\sigma_i=y^{v_i}$作为有效的签名(因为$y^{v_i}=(g^d)^{v_i}=h_i^d=H(m_i)^d$)。假设$I$对一个消息进行签名查询之前已经进行过$H$查询。另外,$I$也可以像形式化定义中的一样,对任意的消息-签名对查询M模拟的确认/否认问答器。学习阶段结束,I输出一个元组(m^*,σ^*,μ)。

然后,I进入扮演阶段。如果$\mu=1$,I和M一同执行确认协议,I作为证实人;M作为验证人,并输入(m^*,σ^*)。第一次传递,M获得I的承诺信息(z_1,z_2,z_3,z_4);第二次传递,M发送挑战值$c \in_R Z_n$;第三次传递,M获得I的返回信息$(c_{11}, c_{12}, d_{11}, d_{12})$。然后$M$重新设置$I$为第一次传递之后的状态,并继续第二次执行确认协议,M发送不同于c的挑战值$c' \in_R Z_n$,并重新运行I得到返回信息$(c_{21}, c_{22}, d_{21}, d_{22})$。

从第一次执行的确认协议中,M获得如下关系:$g^{d_{11}}=z_1 y^{c_{11}} \bmod n$, $H(m^*)^{d_{11}}=z_2(\sigma^*)^{c_{11}} \bmod n$。从第二次执行的确认协议中,$M$获得如下关系:$g^{d_{21}}=z_1 y^{c_{21}} \bmod n$, $H(m^*)^{d_{21}}=z_2(\sigma^*)^{c_{21}} \bmod n$。由此可得

$$g^{d_{11}-d_{21}} = y^{c_{11}-c_{21}} \bmod n \quad (1)$$

$$H(m^*)^{d_{11}-d_{21}} = (\sigma^*)^{c_{11}-c_{21}} \bmod n \quad (2)$$

由于$y=g^d \bmod n$,$\sigma^*=H(m^*)^d$,M可以从式(1)或式(2)中得到$d=\dfrac{d_{11}-d_{21}}{c_{11}-c_{21}} \bmod p'q'$,从而解决了离散对数问题。

如果$\mu=0$,I和M一同执行否认协议,同样可以得到d(过程略)。

综上,M解决离散对数问题的优势ε_M和I的优势ε_I近似相同。

4 结束语

第一次提出了基于RSA的三次传递的不可否认签名方案。该方案同时实现了可转换性,签名人公布私钥中的$e=d^{-1} \bmod \varphi(n)$,能把不可否认签名方案转换成通常的RSA数字签名方案。方案在random oracle模型下证明是安全的,其不可伪造性在CDH假设下是安全的;不可分辨性在DDH假设下是安全的;不可扮演性在离散对数假设下是安全的。

参考文献:

[1] Chaum D, Van Antwerpen H. Undeniable signatures [C]// Advances in Cryptology-CRYPTO'89, LNCS 435. Berlin: Springer-Verlag, 1989.

[2] Chaum D. Designated confirmer signatures[C]// Advances in Cryptology-EUROCRYPT'94, LNCS 950. Berlin: Springer-Verlag, 1995.

[3] Michels M, Stadler M. Efficient convertible undeniable signature schemes[C]// Selected Areas in Cryptography-SAC'97. Berlin: Springer-Verlag, 1997.

[4] Kurosawa K, Heng S. 3-move undeniable signature scheme[C]// Advances in Cryptology-EUROCRYPT 2005, LNCS 3494. Berlin: Springer-Verlag, 2005.

[5] Camenisch J, Michels M. Confirmer signature schemes secure against adaptive adversaries[C]// Advances in Cryptology-EUROCRYPT'00, LNCS 1870. Berlin: Springer-Verlag, 2000.

[6] Gennaro R, Krawczyk H, Rabin T. RSA-based undeniable signatures[C]// Advances in Cryptology-CRYPTO'97, LNCS 1294. Berlin: Springer-Verlag, 1997.

[7] Galbraith S, Mao W, Paterson K G. RSA-based undeniable signatures for general moduli[C]// Topics in Cryptology-CT-RSA'02, LNCS 2271. Berlin: Springer-Verlag, 2002.

[8] Galbraith S W. Invisibility and anonymity of undeniable and confirmer signatures[C]// Topics in Cryptology-CT-RSA'03, LNCS 2612. Berlin: Springer-Verlag, 2003.

[9] Libert B, Quisquater J. Identity based undeniable signatures[C]// Topics in Cryptology-CT-RSA'04, LNCS 2964. Berlin: Springer-Verlag, 2004.

[10] Okamoto T. Designated confirmer signatures and public key encryption are equivalent[C]// Advances in Cryptology-CRYPTO'94, LNCS 839. Berlin: Springer-Verlag, 1994.

[11] Ateniese G, Camenisch J, Joye M, et al. A practical and provably secure coalition-resistant group signature scheme[C]// Advances in Cryptology-CRYPT0 2000, LNCS 1880. Berlin: Springer-Verlag, 2000.

[12] Feige U, Shamir A. Witness indistinguishable and witness hiding protocols[C]// ACM Symposium on Theory of Computing-STOC'90. New York: ACM Press, 1990.