基于 RSA 的证实数字签名方案*

鞠宏伟[1]，李凤银[2]，禹继国[2]，曹宝香[2]
(1. 曲阜师范大学 资产管理处，山东 日照 276826; 2. 曲阜师范大学 计算机科学学院，山东 日照 276826)

摘　要: 验证者要知道一个证实数字签名的有效性,必须得到一个称为证实者的第三方的帮助与合作,签名者的安全性和证实签名的不可见性是一个证实数字签名方案必须具备的两个重要特性。提出了一种完全基于 RSA 的证实数字签名方案,分析表明,该方案是一种安全而高效的证实数字签名实现方案。

关键词: 证实数字签名; 不可否认签名; RSA; 数字签名
中图法分类号: TN918.91　　**文献标识码**: A　　**文章编号**: 1001-3695(2006)01-0093-03

A Confirmer Signature Scheme Based on RSA

JU Hong-wei[1], LI Feng-yin[2], YU Ji-guo[2], CAO Bao-xiang[2]
(1. *Dept. of Assets Management, Qufu Normal University, Rizhao Shandong* 276826, *China;* 2. *Institute of Computer Science, Qufu Normal University, Rizhao Shandong* 276826, *China*)

Abstract: Without the help and cooperation of a designated confirmer, a verifier cannot determine the validity of a confirmer signature. The subscriber's security and the confirmer signature invisibility are characteristic to a confirmer signature scheme. A confirmer signature scheme based on RSA is proposed. It is showed that the new scheme is an implementation of secure and efficient confirmer signature.

Key words: Confirmer Signature; Undeniable Signature; RSA; Digital Signature

为了限制数字签名信息的任意传播,Chaum 和 Van Antwerpen引进了不可否认数字签名。不可否认数字签名只有在得到原始签名者的合作下才可以进行验证,签名者能够否认非法数字签名但不能否认合法的数字签名,因此签名者可控制谁可获得签名有效性的验证。这导致了因签名者可能的不愿意合作或签名者不能被利用而使签名不能被验证的缺点。为了克服这一缺点,Chaum 引进了证实数字签名[3] 的概念。在证实数字签名方案中,签名的证实和否认功能由一个半可信任的第三方(称为证实者)承担,同时证实者具有转换一个证实数字签名为一个普通数字签名(即可被任何人公开验证)的能力。当然,签名者不能参与证实的过程,证实者也不能参与签名的过程;而且证实者应该遵循一定的策略决定对哪些人的证实签名进行证实,或在哪些环境下他可将哪些证实签名转换为普通的数字签名。但 Chaum 提出的证实签名方案是非形式化模型而且也未能证明其安全性。之后,人们提出了各种各样的证实数字签名方案[4~6,8],但这些方案或者不安全,或者非常复杂和低效,以致于在实际上是不可用的。

RSA 密码体制是应用最广泛的公钥密码体制之一,研究基于 RSA 密码体制的高效、安全的证实数字签名方案具有重要的理论和应用价值。鉴于此,本文基于 Canmenisch-Michels 形式化模型和结构,提出一种新颖的完全基于 RSA 密码体制的证实数字签名方案。新方案中的证实与否认协议都是新的交互式的零知识证明协议,在证实或否认一个证实签名时,验证者 V 主动地参与协议的执行与交互,有效地避免了证实签名的可转移性问题。分析表明,在 RSA 的安全假设下,新方案是一种安全、高效、可行的证实数字签名方案。

收稿日期: 2005-01-28; 修返日期: 2005-03-25
基金项目: 国家自然科学基金资助项目(10471078); 教育部高等学校博士学科点专项科研基金资助项目(20040422004); 曲阜师范大学博士科研基金资助项目

1　RSA公钥算法

(1) 密钥生成:

①取两个大素数 p 和 q(保密);

②计算 n(公开) $= pq$, $\phi(n)$(保密) $= (p-1)(q-1)$;

③随机选取整数 e(公开),满足 $gcd(e, \phi(n)) = 1$;

④计算 d(保密),满足 $de \equiv 1 \pmod{\phi(n)}$,则 (e, n) 为公开密钥,d 为私有密钥。

(2) 加密算法。对明文信息 m 加密则执行算法:

$c = E(m) \equiv m^e \pmod{n}$。

(3) 解密算法。对密文信息 c 解密则执行算法:

$m = D(c) \equiv c^d \pmod{n}$。

(4) 数字签名算法。对明文信息 m 进行数字签名则执行算法: $s = H(m)^d \pmod{n}$。

(5) 数字签名验证算法。对数字签名 s 进行验证,则验证等式: $H(m) \equiv s^e \pmod{n}$。

其中,$H(\cdot)$ 是一个公开的安全 Hash 函数(如 SHA-1[2])。

2　证实数字签名模型

定义 1[1]　证实数字签名的参与方有签名者 S、证实者 C 和验证者 V。一个证实数字签名由下列算法构成:

$$CKGS(1^l) \rightarrow (x_s, y_s)$$

(1) 密钥生成算法。设$CKGC(1^l) \rightarrow (x_c, y_c)$是三个概率算

$$CKGV(1^l) \rightarrow (x_v, y_v)$$

法,其中 l 是一个安全参数,(x_s, y_s),(x_c, y_c) 及(x_v, y_v) 分别是签名者 S、证实者 C 及验证者 V 的签名秘密钥和对应的公开钥,即 CKGS, CKGC 和 CKGV 分别为签名者 S、证实者 C 及验证者 V 的密钥生成算法。

(2) 签名算法。签名者 S 对信息 $m \in \{0,1\}^*$ 的概率证实数字签名算法为 $CSig(m, x_s, y_s, y_c) \rightarrow \sigma$。

(3) 证实与否认算法(CverC, CverV)。该算法是在证实者 C 与验证者 V 之间执行的一个签名验证协议。证实者 C 的秘密输入为 x_c,双方的共同输入为(m, σ, y_s, y_c),验证的结果是 1(真)或 0(假)。

(4) 选择可转换算法。算法 $CConv(m, \sigma, y_s, x_c, y_c) \rightarrow s$ 可使证实者在一定的策略下把一个证实签名转换为普通的数字签名。

(5) 普通数字签名验证算法。算法 $coVer(m, s, y_s) \rightarrow (0, 1)$ 可使任何人在输入信息 m,签名 s 及签名者公开钥 y_s 时验证签名。

3 基于 RSA 的证实数字签名方案

基于 RSA 的证实数字签名方案的最大优点是,它所使用的公钥密码体制 RSA 是目前广为使用且已经过大量密码分析的、公认比较安全的密码体制,尽管它的安全性并未得到严格的证明。新方案中设计了一种高效零知识证明协议,保证了签名者的安全和证实签名的不可见性。下面给出完全基于 RSA 的新的证实数字签名方案。

(1) 密钥生成算法

新方案中,CKGS, CKGC 和 CKGV 均取为 RSA 的密钥生成算法,简要描述如下:

①令 $CKGS(1^l) \rightarrow (n_s, e_s, d_s)$,其中,$n_s$ 是两个大素数的乘积,(e_s, n_s) 是签名者 S 的 RSA 公开密钥,d_s 是相应的秘密钥。

②令 $CKGC(1^l) \rightarrow (n_c, e_c, d_c)$,其中,$n_c$ 是两个大素数的乘积,(e_c, n_c) 是证实者 C 的 RSA 公开密钥,d_c 是相应的秘密钥。

③令 $CKGV(1^l) \rightarrow (n_v, e_v, d_v)$,其中,$n_v$ 是两个大素数的乘积,(e_v, n_v) 是验证者 V 的 RSA 公开密钥,d_v 是相应的秘密钥。

此处的 RSA 公钥的真实性和完整性既可以使用 PKI 中的公钥证书来保证,也可以使用其他的物理分发技术来保证,这里不再赘述。同时,关于 RSA 密钥对的生成细节和安全性请查阅文献[7]。

(2) 签名者 S 的证实签名算法

签名者 S 对信息 $m \in \{0,1\}^*$ 的证实数字签名算法 $CSig(m, x_s, y_s, y_c) \rightarrow \sigma$ 分为两步:①利用 RSA 的普通数字签名算法对信息 m 签名,得到关于信息 m 的普通数字签名 $s = H(m)^{d_s} \bmod n_s$;②随机选取 $r_s \in_R Z^*_{n_s}$,利用证实者 C 的 RSA 公钥 (e_c, n_c) 计算

$$c_1 = r_s^{e_c} \bmod n_c, \quad c_2 = [H(r_s) \cdot s]^{e_c} \bmod (n_s \cdot n_c)$$

证实签名 $\sigma = (c_1, c_2)$。

(3) 证实与否认算法(CVerC, CVerV)

当验证者 V 持有对某个信息 $m \in \{0,1\}^*$ 的证实签名 σ 时,由于他无法通过解密 σ 得到 s,也无法通过对 σ 进行运算验证 s 的有效性,所以无法判断 σ 是否为有效的证实数字签名。因此,V 只能向证实者 C 申请验证 σ 的有效性。

验证者 V 首先任意选取一次性随机数 $Nonce \in_R Z^*_{n_v}$,计算 $r_v = H(Nonce \,|\, Timestamp)$,然后使用证实者 C 的公钥 (e_c, n_c) 加密后得到 $R_v = r_v^{e_c} \bmod n_c$,然后将信息 m、证签名 σ 和 R_v 一起发送给证实者 C 提出验证 σ 有效性的请求。

证实者 C 首先检验这一请求是否符合证实策略,即是否可以对 V 进行有关信息 m 的证实数字签名 σ 的验证。若符合,则 C 首先利用其秘密钥 d_c 依次解密 R_v, c_1, c_2,得到

$$r_v = R_v^{d_c} \bmod n_c, \quad r_s = c_1^{d_c} \bmod n_c,$$

$$s = [c_2^{d_c} \bmod n_c] / H(r_s)$$

然后利用签名者 S 的公钥 (e_s, n_s) 验证关于信息 m 的普通数字签名 s 的有效性,即判断式(1)是否成立:

$$s^{e_s} \bmod n_s \equiv H(m) \qquad (1)$$

若式(1)成立,则 $\sigma = (c_1, c_2)$ 是签名者 S 对信息 m 的有效证实数字签名,否则 $\sigma = (c_1, c_2)$ 不是签名者 S 对信息 m 的有效证实数字签名。但由于验证者 V 并不信任证实者 C,C 必须通过执行零知识证明协议向 V 证明 σ 有效或无效。

证实者 C 经过验证知道 σ 的有效性后,执行式(2)给出的零知识证明协议向验证者 V 证实这一结论:

$$ZPK\{\alpha, \beta \,|\, c_1 = \alpha^{e_c} \bmod n_c \cdots c_2 = [H(\alpha) \cdot \beta^{e_c} \bmod n_s \cdot n_c \cdots \beta^{e_s} \bmod n_s \equiv H(m)\} \qquad (2)$$

证实与否认协议的具体实现如下:

①证实者随机选取 $r_1, \cdots, r_l \in_R Z^*_{n_c}$,计算

$$u = r_1^{e_c} \bmod n_c, \; v = r_2^{e_c} \bmod n_c, \; t_i = r_i^{e_s} \bmod n_s, \; (i = 1, \cdots, l)$$

以及如下的 Hash 值 c 作为质询:

$$c = H(m \,|\, c_1 \,|\, c_2 \,|\, n_c \,|\, n_s \,|\, n_v \,|\, u \,|\, v \,|\, t_1 \,|\cdots|\, t_2 \,|\, r_v)$$

②设 c 的二进制表示为

$$c = c[l] \cdots c[2]\, c[1] \in \{0,1\}^l$$

证实者 C 计算以下承诺值:

$$m = \frac{r_1}{r_s \cdot c} \bmod n_c$$

$$n = \frac{r_2}{H(r_s) \cdot s \cdot c} \bmod n_c$$

$$s_i = \begin{cases} r_i \bmod n_s, \text{若 } c[i] = 0 \\ \dfrac{r_i}{s} \bmod n_s, \text{若 } c[i] = 1 \end{cases} \quad (i = 1, \cdots, l)$$

③证实者 C 将$(u, v, m, n, s_1, \cdots, s_l, c)$ 发送给 V。

④验证者 V 首先检查是否 $(u, v, m, n, s_1, \cdots, s_l, c) \in (Z_{n_c})^4 \times (Z_{n_s})^l \times \{0,1\}^{160}$,若是,则 V 进一步计算出:

$$u' = c_1 m^{e_c} c^{e_c} \bmod n_c$$

$$v' = c_2 n^{e_c} c^{e_c} \bmod n_c$$

$$t'_i = \begin{cases} s_i^{e_s} \bmod n_s, \text{若 } c[i] = 0 \\ H(m)\, s_i^{e_s} \bmod n_s, \text{若 } c[i] = 1 \end{cases} \quad (i = 1, \cdots, l)$$

接下来首先验证 $u' \equiv u$ 和 $v' \equiv v$ 同时成立,则证明证实者 C 确实拥有签名者 S 对信息 m 的 RSA 数字签名的秘密知识 (r_s, s);否则,认为是证实者 C 在作弊。

验证 $u' \equiv u$ 和 $v' \equiv v$ 同时成立后,进一步检查以下的恒等式是否成立:

$$c = H(m \| c_1 \| c_2 \| n_c \| n_s \| n_v \| u \| v \| t'_1 \| \cdots \| t'_2 \| r_v) \quad (3)$$

若式(3)成立,则验证者 V 接受 $\sigma=(c_1, c_2)$ 为签名者 S 产生的对信息 m 的有效证实数字签名;否则验证者 V 确信 $\sigma=(c_1, c_2)$ 不是签名者 S 产生的对消息 m 的有效证实签名。

(4) 选择可转换算法

证实者在一定的策略下把一个证实签名 σ转换为普通的数字签名的具体算法是证实者 C 告诉验证者 V 信息 $m\in\{0,1\}^*$ 的数字签名 s 即可。

(5) (普通) 数字签名验证算法 $\mathrm{CoVer}(m, s, y_s) \rightarrow (0,1)$

此处取作普通 RSA 数字签名的验证算法,即使用签名者 S 的公钥 (e_s, n_s) 检查以下恒等式是否成立: $s^{e_s} \bmod n_c \equiv H(m)$。

把有关在什么情况下允许证实者证实或否认证实签名的策略作为信息的一部分,对不符合规定的信息证实者拒绝合作,这样可使验证者不能逃避策略的约束。上述方案中的算法都是独立的,即各方都可以独立地运行各自的密钥生成算法,这样使签名者在签名时可选择证实者。

4　性能分析

上述的证实数字签名方案中的证实与否认协议的正确性及有效性通过验证可知是成立的。新方案的设计完全基于 Camennisch 和 Michels 给出的证实数字签名的模型,其核心是证实者与验证者之间的证实与否认协议。本文设计的证实与否认协议是一种交互式的零知识证明协议,所以具有协议的零知识性、证实签名的不可转移性、证实签名的不可见性、签名者的安全性等重要特性。

证实签名 σ中随机数 r_s 的使用,使得不通过解密 c_2 验证 s 的有效性是不可能的。而我们的证实与否认协议是真正的零知识证明协议,任何人(包括签名者)通过与证实者的交互,最多只能获得签名的有效性的证明,而不能获得验证证实签名有效性的秘密信息。因为在 RSA 的安全假设下,攻击者不能从任何承诺值恢复出相应的秘密信息。

由于证实与否认协议是一种真正的交互式协议,验证者主动参与协议的动态执行,即使证实者 C 将他所知道的秘密信息 r_v, r_s, s 统统泄露给 C',C 也不能 C 对证实签名的有效性作出验证,因为 r_v 中时间戳的存在将使得 C 的验证无效,验证者 V 能够及时发现证实者的作弊行为,保证了证实者的安全性和证实签名的不可转移性。

上述协议中,证实者可以对签名者所签的任何符合证实策略的证实签名进行证实,但证实者不能获得有关签名者的签名秘密钥,因为证实者利用自己的证实秘密钥通过对证实签名的作用后仅能获得签名者对 m 通过 RSA 的签名,在 RSA 的安全假设下,签名者的签名秘密钥是安全的,即签名者是安全的。

而且新方案具有不可见性。假设有一个对手,对手握有签名者及证实者的公开钥,并假设该对手掌握签名者的签名秘密钥,该对手可任意创造对任意信息的数字签名,并且可以以任意的模式访问证实与否认算法以及转换算法。但在 RSA 的安全假设下,该对手无法获得验证者 V 的加入时间戳的一次性随机数 r_v,从而使得该对手无法冒充证实者验证证实签名的有效性,即系统中只有证实者可以证实签名的有效性。

新方案还有一个重要特性,那就是签名者对证实者的可选择性。从协议的执行可以看出,签名者可以根据需要选择证实者,此时只需用新选择的证实者的公钥产生证实签名即可。

综上所述,新协议在 RSA 的安全假设下是安全可行的,但由于对 RSA 的安全性尚未有严格的理论证明,只是实际上认为它们是安全的。

5　结束语

证实数字签名方案可用于合同的公平签署,证实者担任半可信任第三方的角色。合同双方都首先对协商好的合同文本进行证实数字签名,当半可信任的第三方即证实者确认双方的签署都为合法签名的情况下,通过证实签名向普通签名的转换协议,将双方的证实签名转换为普通数字签名,即可实现合同的公平签署。本文提出的的证实签名方案基于较为常用的公钥加密体制 RSA,是一种安全而高效的具体实现方案,它的应用将是广泛的。

参考文献:

[1] haum D, Van Antwerpen H. Undeniable Signatures[C]. Proc. of the Advances in Cryptography-CRYPTO'89, LNCS 435, Berlin: Springer-Verlag, 1989. 212-216.

[2] National Institute of Standard and Technology. NIST FIPS PUB 180-1, Secure Hash Standard[EB/OL]. http://csrc.nist.gov/cryptval/html, Washington: Department of Commerce, NIST, 1995.

[3] Chaum D. Designated Confirmer Signatures[C]. Proc. of the Advances in Cryptography-EUROCRYPT'94, LNCS 950, Berlin: Springer-Verlag, 1994. 86-89.

[4] Okamoto T. Designated Confirmer Signatures and Public-key Encryption are Equivalent[C]. Proc. of the Advances in Cryptography-CRYPTO'94, LNCS 839, Berlin: Springer-Verlag, 1994. 61-74.

[5] Michels M, Stadler M. Generic Constructions for Secure and Efficient Confirmer Signature Schemes[C]. Proc. of the Advances in Cryptography-EUROCRYPT'98, LNCS 1403, Berlin: Springer-Verlag, 1998. 406-421.

[6] Camenisch J, Michels M. Confirmer Signature Schemes Secure Against Adaptive Adversaries(Extended Abstract)[C]. Proc. of the Advances in Cryptography-EUROCRYPT'2000, LNCS 1807, Berlin: Springer-Verlag, 2000. 243-258.

[7] Rivest R, Shamir A, Adleman L. A Method of Obtaining Digital Signatures and Public-key Cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[8] 王尚平,王育民,张亚玲. 基于 DSA 及 RSA 的证实数字签名方案[J]. 软件学报, 2003, 14(3): 588-593.

[9] 王贵林,卿斯汉. 一个证实数字签名方案的安全缺陷[J]. 软件学报, 2004, 15(5): 752-756.

[10] 王尚平,王育民,王晓峰,等. 拥有 RSA 数字签名的零知识证明[J]. 通信学报, 2004, 25(1): 30-33.

[11] 秦波,王尚平,王晓峰,等. 一种新的前向安全可证实数字签名方案[J]. 计算机研究与发展, 2003, 40(7): 1016-1020.

[12] 周峰,王尚平,王晓峰,等. 一个新的门限证实数字签名方案[J]. 计算机工程与应用, 2004, 40(21): 146-148.

作者简介:

鞠宏伟(1974-),男,山东日照人,实验师,硕士,主要研究方向为网络与信息安全理论与技术;李凤银(1974-),女,山东荷泽人,讲师,硕士,主要研究方向为计算机网络安全理论与技术、数字签名理论与技术;禹继国(1972-),男,山东泰安人,副教授,博士,主要研究方向为图论与理论计算机科学;曹宝香(1955-),男,山东嘉祥人,教授,主要研究方向为图形图像处理、MIS。