# 一个证实数字签名方案的安全缺陷*

王贵林[1], 卿斯汉[2,3+]

[1](Infocomm Security Department, Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613)

[2](中国科学院 软件研究所,北京 100080)

[3](中国科学院 信息安全技术工程研究中心,北京 100080)

## Security Flaws in a Confirmer Signature Scheme

WANG Gui-Lin[1], QING Si-Han[2,3+]

[1](Infocomm Security Department, Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613)

[2](Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)

[3](Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing 100080, China)

+ Corresponding author: Phn: +86-10-62635150, E-mail: qsihan@ercist.iscas.ac.cn

Received 2003-10-02; Accepted 2003-11-18

**Wang GL, Qing SH. Security flaws in a confirmer signature scheme. *Journal of Software*, 2004,15(5):752~756.**
http://www.jos.org.cn/1000-9825/15/752.htm

**Abstract**: Confirmer signatures are different from standard signatures in the sense that without the help and cooperation of a designated confirmer, a verifier cannot determine the validity of a confirmer signature. But except of the signer, anyone else (including the confirmer) can not generate a valid confirmer signature on behalf of the signer. At the same time, the confirmer cannot cheat verifiers once he is involved in the procedure of signature verification. Furthermore, if it is necessary, the confirmer could convert confirmer signatures into standard ones such that the validity of these converted signatures can be publicly validated. Wang et al. proposed an efficient new confirmer signature scheme based on DSA and RSA, and claimed that their scheme is secure. However, several serious security flaws in their scheme are identified so that their investigation does not succeed.

**Key words**: confirmer signature; undeniable signature; digital signature; information security

**摘 要**: 与普通的数字签名不同,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合作与帮助.但除了签名者,其他任何人(包括证实者)都不能以签名者的名义产生有效的证实签名.同时,只要参与了验证,证实者就不能欺骗验证者.进一步地,在必要的时候,证实者还可以将证实签名转化为普通的数字签名,从而使得任何人都可以验证这些签名的有效性.王尚平等学者提出了一个基于 DSA 和 RSA 的证实数字签名方案,并认为他们的方案是安全而高效的.与现有的具体方案相比,他们的方案确实是高效的.但是,这一方案存在严重的安全缺陷,从而使得他们的尝试是不成功的.

* Supported by the National Natural Science Foundation of China under Grant No.60083007 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035810 (国家重点基础研究发展规划(973))

作者简介: **王贵林**(1968－),男,云南大理人,博士,研究员,主要研究领域为密码学基础及应用;**卿斯汉**(1939－),男,研究员,教授,博士生导师,主要研究领域为信息安全理论和技术.

关键词: 证实数字签名;不可否认签名;数字签名;信息安全
中图法分类号: TP309 文献标识码: A

普通的数字签名都是可以公开验证的(publicly verifiable).也就是说,任何持有数字签名和签名者公钥的人,都可以按照既定的验证算法检查这一比特串是否为该签名者对某一消息的有效签名.但在某些特定的环境下,签名者并不希望他所产生的签名具有这一性质.换句话说,签名者可能更希望能对他所产生的数字签名的可验证性进行控制.这样的例子很多,比如:国家政府、安全和情报部门签署的机密文件,只有特定的官员或机构才能验证它们的真假;只有购买了正版软件的用户才可以验证他使用的软件是某公司开发生产的,从而可以放心地使用而无须担心软件的性能及病毒等安全隐患;两个公司正式合作协议生效前所签订的合作意向及阶段性合同,任何公众(尤其是竞争对手)都无法验证其真伪;只有在遗嘱人去世以后,其亲人才可以验证他所立定的遗嘱.

Chaum 和 van Antwerpen 所引入的不可否认数字签名(undeniable signature)就在某种程度上满足了这种需要[1,2].在这种特殊的数字签名方案中,验证者自己无法区分签名的真与假,只有在签名者的合作与帮助下才能验证签名的有效性.同时,只要参与了验证,签名者就无法欺骗验证者,即他既不能使验证者接受一个无效的签名,也不能让验证者相信一个实际上有效的签名是无效的.但不可否认签名有一个缺点:若签名者主观上不愿意合作或客观上无法合作,他所产生的签名就不能被验证.为此,Chaum 提出了证实数字签名(confirmer signature)的概念[3].在这样的方案中,签名的确认或否认可以由一个称为证实者(confirmer)的第三方来完成.但除了签名者,其他任何人(包括证实者)仍然无法以签名者的名义产生(或伪造)有效的证实签名.进一步地,在必要的时候,证实者还可以将部分或全部证实签名转化为普通的数字签名,从而使得任何人都可以验证这些签名的有效性.另外,一般还假定签名者已经给定了某些验证策略,使得证实者可以决定是否应该与特定的验证者进行关于特定消息的签名的验证,以及在什么条件下,可以将关于哪些消息的证实数字签名转化为普通的数字签名.

但 Chaum 的证实签名方案是非形式化的,且其安全性没有得到证明.随后,Okamoto 提出了一个形式化的模型,并从理论上证明了安全证实签名与安全公钥加密算法的存在性是等价的[4].在 1998 年的欧密会上,Michels 和 Stadler 提出了安全而有效的证实签名的一般性构造方法,并提出了几个效率比较高的具体方案[5].但 Canmenisch 和 Michels 随后的研究表明[6],文献[4,5]提出的安全模型都是有缺陷的,并对 Okamoto 以及 Michels 和 Stadler 提出的具体方案给出了一种称为适应性签名转换的攻击(adaptive signature-transformation attacks).由此,文献[6]中提出了更严格的安全证实签名形式化模型.但他们按照此模型构造出的具体例子却颇为复杂、低效.

注意到 DSA[7]和 RSA[8]是目前使用最广泛的两种数字签名,王尚平等学者在文献[9]中提出了一个基于 DSA 和 RSA 的证实数字签名方案(此后简称为 WWZ 方案).他们的方案虽然采用 Canmenisch-Michels 形式化模型和结构,但与文献[6]所给出的具体方案相比,WWZ 方案中的确认和否认协议是高效的.但本文的研究表明,WWZ 方案存在严重的安全缺陷,从而使得他们的尝试是不成功的.最主要的安全问题在于,该方案中的确认和否认协议都不是零知识的.所以每个与证实者进行过一次验证的验证者都可以恢复出证实数字签名所对应的普通签名,进而可以将签名者的这一 DSA 签名泄漏,或冒充证实者向其他验证者证明该签名的有效性.

本文第 1 节介绍 DSA 数字签名算法.第 2 节回顾 WWZ 证实数字签名方案的几个组成部分.第 3 节给出对 WWZ 方案的安全性分析.更多有关 Canmenisch-Michels 形式化模型和证实数字签名的安全性要求,可以参考文献[6,9].进一步的研究还包括多用户环境下的匿名性[10]和门限方案[11].

## 1 DSA 数字签名算法

本节简要介绍美国国家数字签名算法 DSA[7].设 $(p,q,g)$ 是系统公开参数.其中, $p$ 是一个长为 $l$ 比特的大素数( $512\le l\le 1024$ 且 $64|l$ ); $q$ 是一个长为 160 比特的素数,使得 $q|(p-1)$ ;而 $g$ 为乘法群 $Z_p^*$ 中阶为 $q$ 的元素.签名者 $S$ 选取一个随机数 $x\in_R Z_q^*$ 作为其秘密秘钥,将 $y=g^x \bmod p$ 公布为其公开秘钥.另外,还假设 $H(\cdot)$ 是一个公开的安全 hash 函数(比如 SHA-1)[12].要产生对某个消息 $m\in\{0,1\}^*$ 的签名时,签名者 $S$ 首先随机选取

$k \in_R Z_q^*$,然后利用其秘密秘钥 $x$,按下式计算出签名 $(r,s)$:

$$r=(g^k \bmod p) \bmod q,\quad s=k^{-1}(H(m)+xr) \bmod q \tag{1}$$

验证者 $V$ 可根据以下恒等式是否成立来判定 $(r,s)$ 是否为签名者 $S$ 对消息 $m$ 的签名:

$$r \equiv (g^{H(m)s^{-1} \bmod q} y^{rs^{-1} \bmod q} \bmod p) \bmod q \tag{2}$$

## 2 WWZ 证实数字签名方案回顾

下面逐一介绍 WWZ 证实数字签名方案[9]的 6 个组成部分.

(1) 签名者 $S$ 的秘钥生成算法:与 DSA 相同,即签名者 $S$ 选取 $(p,q,g)$ 为系统公开参数,而置其秘密秘钥/公开秘钥对为 $(x, y=g^x \bmod p)$.

(2) 证实者 $C$ 的密钥生成算法:证实者选取 RSA 模数 $n$ 为两个大素数的乘积,然后置其秘钥对为 $(e,d)$.这里,公开秘钥 $e$ 和秘密秘钥 $d$ 满足 $ed=1 \bmod \varphi(n)$.

(3) 证实数字签名的产生:签名者 $S$ 对消息 $m$ 产生证实数字签名时,首先利用他的秘密秘钥 $x$ 按式(1)计算出一个普通的 DSA 数字签名 $(r,s)$,然后用证实者 $C$ 的公开加密秘钥 $e$ 对 $r$ 和 $s$ 进行加密,即计算 $c_1=r^e \bmod n$, $c_2=s^e \bmod n$. $\sigma=(c_1,c_2)$ 就是签名者 $S$ 产生的对消息 $m$ 的证实数字签名.

(4) 证实数字签名的确认与否认:当验证者 $V$ 持有对某个消息 $m$ 的证实数字签名 $\sigma=(c_1,c_2)$ 时,由于他无法通过解密 $(c_1,c_2)$ 得到 $(r,s)$,所以无法判断 $\sigma$ 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 $\sigma$ 的有效性.证实者 $C$ 首先检查这一请求是否符合证实策略,即是否可以对 $V$ 进行有关消息 $m$ 的证实数字签名验证.若符合,则 $C$ 利用其秘密秘钥 $d$ 解密出 $r$ 和 $s$ : $r=c_1^d \bmod n$, $s=c_2^d \bmod n$.这之后,证实者 $C$ 根据式(2)判断 $(r,s)$ 是否为签名者 $S$ 对消息 $m$ 的 DSA 签名.若是,则执行式(3)给出的知识证明协议,以确认证实数字签名 $\sigma$ 的有效性;否则,执行式(4)给出的知识证明协议以否认 $\sigma$ 的有效性.

$$PK\{\alpha,\beta: c_1=\alpha^e \bmod n \wedge c_2=\beta^e \bmod n \wedge c_1=[(g^{H(m)\beta^{-1}} y^{\alpha\beta^{-1}} \bmod p) \bmod q]^e \bmod n\}(m) \tag{3}$$

$$PK\{\alpha,\beta: c_1=\alpha^e \bmod n \wedge c_2=\beta^e \bmod n \wedge c_1\neq[(g^{H(m)\beta^{-1}} y^{\alpha\beta^{-1}} \bmod p) \bmod q]^e \bmod n\}(m) \tag{4}$$

(a) 确认协议:文献[9]所给出的确认协议式(3)的具体实现如下:证实者 $C$ 任选 $r_1,r_2 \in_R Z_n^*$,计算 $t_1=r_1^e \bmod n$, $t_2=r_2^e \bmod n$ 和 $t_3 \equiv [(g^{H(m)r_2^{-1} \bmod q} y^{r_1 r_2^{-1} \bmod q} \bmod p) \bmod q]^e \bmod n$ 以及如下的 hash 值 $c$ 作为质询(challenge): $c=H(m\|c_1\|c_2\|p\|q\|y\|n\|e\|t_1\|t_2\|t_3)$.然后,$C$ 计算如下的几个值作为应答:

$$s_1=\frac{r_1}{rc} \bmod q,\quad s_2=\frac{r_2}{rc} \bmod q,\quad s_3=(r_1 r_2^{-1}-rs^{-1})/c \bmod q,\quad s_4=H(m)(r_2^{-1}-s^{-1})/c \bmod q \tag{5}$$

最后,证实者 $C$ 将 $(s_1,s_2,s_3,s_4,c)$ 发送给验证者 $V$.为验证证实签名 $\sigma$ 的有效性,$V$ 首先检查是否 $(s_1,s_2,s_3,s_4,c)\in(Z_q)^4\times\{0,1\}^{160}$.若是,则验证者 $V$ 进一步计算出 $t_1'=c_1 s_1^e c^e \bmod n$, $t_2'=c_2 s_2^e c^e \bmod n$ 和 $t_3'=c_1[(g^{cs_4} y^{cs_3} \bmod p) \bmod q]^e \bmod n$,然后检查以下的恒等式是否成立:

$$c \equiv H(m\|c_1\|c_2\|p\|q\|y\|n\|e\|t_1'\|t_2'\|t_3') \tag{6}$$

若式(6)成立,则验证者 $V$ 接受 $\sigma=(c_1,c_2)$ 为签名者 $S$ 产生的对消息 $m$ 的证实数字签名.否则,证实者 $C$ 将被认为是作弊者.

(b) 否认协议:否认协议式(4)的具体实现与上述确认协议类似,此处从略.细节参见文献[9].

(5) 证实数字签名的转化:对于一个有效的证实数字签名 $\sigma=(c_1,c_2)$,若证实者 $C$ 欲将其转化为普通的 DSA 数字签名,只需将 $(c_1,c_2)$ 解密,然后公开 $(r,s)$ 即可.

(6) (普通)数字签名的验证:由于转化后的证实数字签名就是普通的 DSA 数字签名,所以任何验证者都可以用式(2)检查其有效性.

## 3 WWZ 证实数字签名方案的安全缺陷

文献[9]的作者对他们所提出的方案进行了分析,并得出以下结论:在 DSA 数字签名算法和 RSA 加密体制安全的前提下,WWZ 证实数字签名是安全的.而且作者强调,在此方案中,确认和否认协议都是零知识协议,所以

证实者在没有泄漏有关秘密的条件下,可使验证者相信一个待验证的证实数字签名是否有效.但验证者自己却无法对一个待验证的证实数字签名的有效性自行作出判断.另外,作者也认为此方案具有“不可见性”,即系统中只有证实者可以对一个待验证的证实数字签名的有效性作出判断与证明.但我们发现,WWZ 方案并不具备这些原作者所声称的安全性质.下面逐一进行讨论.

(1) 可转移性.首先我们注意到,文献[9]所给出的确认协议和否认协议都是非交互式的知识证明协议.换句话说,验证者 $V$ 并没有实质性地参与协议的执行,而只是被动地对证实者提供的证据进行验证而已.这就意味着,验证者 $V$ 可以将知识证明证据转移给其他任何主体,而该主体也将相信证实者 $C$ 所作出的知识证明.更具体地说,若验证者 $V$ 将确认协议中的证据 $(s_1,s_2,s_3,s_4,c)$ 泄漏(或公开)给某个第三方,则根据式(6),该主体(或任何人)都相信 $\sigma=(c_1,c_2)$ 是签名者 $S$ 所产生的对消息 $m$ 的有效证实数字签名.这是设计概念上的错误.事实上,在不可否认签名和证实数字签名中对签名进行确认或否认时,一般都必须使用非交互的、非诚实验证者零知识证明协议.若要使用非交互式协议,就应该利用由文献[13]提出的指定验证者证据(designated verifier proofs).在这个特殊的非交互式知识证明协议中,验证者相信证明者的证明,但却无法让第三者也相信这一证明,因为验证者自己就可以模拟证明者所提供的证据.另外,由于 WWZ 方案中的确认协议和否认协议都不是零知识的(随后会看到),所以并不能简单地将它们改变为交互式协议就认为是安全的.

(2) 弱不可见性.文献[9]声称 WWZ 方案具有不可见性.也就是说,即使签名者也无法按照确认协议或否认协议对一个待验证的证实数字签名进行成功的确认或否认.但事实并非如此.仔细研究 WWZ 方案的确认协议和否认协议后不难知道,无论在证实数字签名的确认还是否认过程中,证实者 $C$ 既没有使用他所特有的秘密秘钥 $d$,也没有使用他所知道的 RSA 模数 $n$ 的素数因子.证实者 $C$ 所用到的秘密知识仅仅是满足 $c_1=r^e \bmod n$ 和 $c_2=s^e \bmod n$ 的对 $(r,s)$.这说明,任何人(包括签名者 $S$)若知道 $\sigma=(c_1,c_2)$ 所对应的明文 $(r,s)$,就可以扮演证实者的角色对任何验证者 $V$ 作出 $\sigma$ 是否有效的证明.只要签名者 $S$ 愿意,他至少具有对有效签名的确认能力,因为他可以将所产生的(部分或全部)DSA 签名 $(r,s)$ 存储起来.下面我们还会看到,任何与证实者进行过验证的验证者 $V$ 也将具有类似的能力.

(3) 非零知识性.确认(否认)协议的目的是通过验证者和证实者的交互,使验证者相信他所持有的证实签名 $\sigma=(c_1,c_2)$ 是有效的(无效的),但证实者并不泄漏除此以外任何有关 $\sigma$ 的信息.特别地,确认(否认)协议应该保证验证者无法通过与证实者的交互获取满足 $c_1=r^e \bmod n$ 和 $c_2=s^e \bmod n$ 的二元对 $(r,s)$.这是不可否认签名和证实数字签名的最本质、最基本的要求.如果不需要这样特殊的安全性要求,证实者可以直接从 $\sigma=(c_1,c_2)$ 中解密出 $(r,s)$,然后发送给验证者.由此,验证者只需检查 $(r,s)$ 是否满足 $c_1=r^e \bmod n$, $c_2=s^e \bmod n$ 以及式(2)就知道 $\sigma=(c_1,c_2)$ 是否为有效的证实数字签名.但 WWZ 方案中给出的确认和否认协议完全不是零知识的.也就是说,验证者可以从证实者提供的知识证据中恢复出秘密 $(r,s)$.下面仅以确认协议为例进行说明.

在确认协议中,证实者 $C$ 是根据式(5)来准备知识证据 $(s_1,s_2,s_3,s_4,c)$ 的.由式(5)中的第 2 项,我们有 $r_2=s_2sc \bmod q$.将此表达式代入式(5)中的第 4 项,可以得到 $s$ 的值.利用由此得到的 $s$ 值以及由式(5)中的第 1 项导出的 $r_1=s_1sc \bmod q$,就可以从式(5)中的第 3 项得到 $r$ 的值.具体地说,验证者利用证实者 $C$ 提供的知识证据 $(s_1,s_2,s_3,s_4,c)$,可以按如下表达式恢复出 $(r,s)$ 的值:

$$r=css_3(s_1s_2^{-1}-1)^{-1} \bmod q,\quad s=H(m)(s_2^{-1}c^{-1}-1)s_4^{-1}c^{-1} \bmod q. \tag{7}$$

得到 $(r,s)$ 的值以后,验证者 $V$ 既可以将签名者 $S$ 的普通 DSA 数字签名 $(r,s)$ 泄漏给其他人,也可以冒充证实者 $C$ 向其他验证者证明 $\sigma=(c_1,c_2)$ 是有效的证实数字签名.类似地,在否认协议中,验证者利用知识证据 $(s_1,s_2,s_3,s_4,s_5,c,c_0)$,也可按下式恢复出 $(r,s)$ 的值:

$$r=css_4(s_1s_2^{-1}-1)^{-1} \bmod q,\quad s=H(m)(s_2^{-1}c^{-1}-1)s_5^{-1}c^{-1} \bmod q. \tag{8}$$

这说明 WWZ 方案中作为证实数字签名核心部分的确认和否认协议都是不安全的.要改进该方案,就必须重新给出既安全又高效的确认和否认协议.安全的协议有,如文献[6],但不高效.设计高效的协议也很容易,但难以保证安全性.而密码学的精髓和困难就在于如何对安全和效率进行平衡与折衷.如何为 WWZ 证实数字签名方案给出安全而高效的确认和否认协议是一个有待进一步研究的问题.

**References**:

[1] Chaum D, van Antwerpen H. Undeniable signatures. In: Proc. of the Advances in Cryptography–CRYPTO'89. LNCS 435, Berlin: Springer-Verlag, 1989. 212~216.

[2] Chaum D. Zero-Knowledge undeniable signatures. In: Proc. of the Advances in Cryptography–EUROCRYPT'90. LNCS 473, Berlin: Springer-Verlag, 1991. 458~464.

[3] Chaum D. Designated confirmer signatures. In: 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. In: 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. In: 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). In: Proc. of the Advances in Cryptography–EUROCRYPT 2000. LNCS 1807, Berlin: Springer-Verlag, 2000. 243~258.

[7] National Institute of Standard and Technology. Digital signature standard. NIST FIPS PUB 186, Washington: Department of Commerce, NIST, 1994.

[8] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978,21(2):120~126.

[9] Wang SP, Wang YM, Zhang YL. A confirmer signature scheme based on DSA and RSA. Journal of Software, 2003,14(3):588~593 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/588.pdf

[10] Galbraith SD, Mao W. Invisibility and Anonymity of undeniable and confirmer signatures. In: CT-RSA 2003. LNCS 2612, Berlin: Springer-Verlag, 2003. 80~97.

[11] Wang G, Qing S, Wang M, Zhou Z. Threshold undeniable RSA signature scheme. In: Information and Communications Security (ICICS 2001). LNCS 2229, Berlin: Springer-Verlag, 2001. 221~232.

[12] National Institute of Standard and Technology. Secure hash standard. NIST FIPS PUB 180-1, Washington: Department of Commerce, NIST, 1995. http://csrc.nist.gov/cryptval/shs.html

[13] Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications. In: Proc. of the Advances in Cryptography–EUROCRYPT'96. LNCS 1070, Berlin: Springer-Verlag, 1996. 143~154.

**附中文参考文献**:

[9] 王尚平,王育民,张亚玲.基于 DSA 及 RSA 的证实数字签名方案.软件学报,2003,14(3):588~593.http://www.jos.org.cn/1000-9825/14/588.pdf