基于 DSA 及 RSA 的证实数字签名方案*

王尚平[1,2+], 王育民[2], 张亚玲[1]

[1](西安理工大学 理学院,陕西 西安 710048)

[2](西安电子科技大学 ISN 国家重点实验室,陕西 西安 710071)

A Confirmer Signature Scheme Based on DSA and RSA

WANG Shang-Ping[1,2+], WANG Yu-Min[2], ZHANG Ya-Ling[1]

[1](Science School, Xi' an University of Technology, Xi' an 710048, China)

[2](National Key Laboratory on ISN, Xidian University, Xi' an 710071, China)

+ Corresponding author: Phn: 86-29-2313169, E-mail: spwang@mail.xaut.edu.cn

http://www.xaut.edu.cn

Received 2001-10-17; Accepted 2001-12-05

Wang SP, Wang YM, Zhang YL. A confirmer signature scheme based on DSA and RSA. *Journal of Software*, 2003,14(3):588~593.

Abstract: A confirmer signature scheme is proposed. This scheme is designed according to Camennisch-Michels' confirmer signature model. It is the first time that the widely used digital signature algorithm DSA and famous public key cryptosystem RSA are being used in confirmer signature scheme, and a new method of zero-knowledge proof for denying protocol is used. This scheme can be used in fair electronic contract signing schemes.

Key words: confirmer signature; DSA; RSA; digital signature

摘 要: 提出了一种证实数字签名方案.该方案采用了 Camenisch-Michels 给出的证实数字签名的模型,首次将数字签名专用算法 DSA 和著名的 RSA 公钥加密方案用于证实数字签名方案中,并首次使用了否认零知识证明的新方法.该方案可应用于电子合同的公平签署.

关键词: 证实数字签名;DSA;RSA;数字签名

中图法分类号: TP307 **文献标识码**: A

为了限制数字签名信息的任意传播,Chaum 和 Van Anterwerpen 引进了不可否认数字签名[1],不可否认数字签名只有在得到原始签名者的合作下才可进行验证,签名者能够否认非法数字签名但是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时,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[2]的概念.在证实数字签名的方案中,证实或否认一个签名的功能由一个半可信任的第三方(称为证实者)承担,同时证实者具有转化一个证

* Supported by the National Natural Science Foundation of China under Grant No.60273089 (国家自然科学基金); the Natural Science Research Plan of Education Department of Shanxi Province of China under Grant No.00JK266 (陕西省教育厅自然科学研究计划)

第一作者简介: 王尚平(1963－),男,陕西扶风人,博士,教授,主要研究领域为密码学,电子商务安全.

实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,证实者不能参与数字签名的过程,且证实者应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化为普通的数字签名.例如,一个策略可以是仅对某一个时间内的签名进行验证,或仅对某些特定的人群提交的签名进行验证.

Chaum[2]提出了一个具体的方案,但为非形式模型也未能证明其安全性.随后,Okamoto[3]提出了一个形式模型,且证明了其安全性等价于一个公钥加密,但该方案中证实一个签名不仅需要证实者而且需要签名者的配合.证实数字签名的一个重要的性质是其必须具备"不可见性",即除了证实者,任何人都不能证明一个证实数字签名是否有效.Michel 和 Stadler[4]提出了一个在他们定义下的安全的证实签名的模型.Camennisch 和 Michels[5]也提出了一个较好的证实数字签名的模型,并给出了一个将一般的数字签名和一个公钥加密方案转化为证实签名的方向性的方法,且在 RSA 数字签名[6]和 Cramer-Shoup[7]公钥加密方案的基础上利用零知识证明提出了一个证实数字签名的方案.但 Cramer-Shoup 公钥加密方案中参数较多,且使用得并不广泛,其中证实与否认协议中的零知识证明协议相当复杂,以致其在实际上是不可用的.

本文利用广泛使用的数字签名专用算法 DSA[8]和著名的 RSA 公钥加密方案构造了一种证实数字签名方案,新方案采用了 Camenisch-Michels 给出的证实数字签名的模型,并首次将数字签名专用算法 DSA 用于证实签名方案且具有完全转换性,新方案可应用于电子合同的公平签署.新方案由于数字签名专用算法 DSA 和著名的 RSA 公钥加密方案应用的普遍性,因而更具有实用性和重要性.

1 证实数字签名的模型

本节介绍 Camennisch 和 Michels 给出的证实数字签名的模型.

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

(1) 密钥生成算法:设 $CKGS(1^l)\rightarrow(x_s,y_s)$ 和 $CKGC(1^l)\rightarrow(x_c,y_c)$ 是两个概率算法,其中 l 是一个安全参数,(x_s,y_s) 是签名者的签名秘密钥和对应的公开钥,(x_c,y_c) 是证实者秘密钥和对应的公开钥.即 CKGS 和 CKGC 分别为签名者 S 及证实者 C 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 $CSig(m,x_s,y_s,y_c)\rightarrow s$.

(3) 证实与否认算法:$(CVerC,CVerV)$ 是在证实者 C 与验证者 V 之间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,s,y_s,y_c),验证的结果是 1(真)或 0(假).

(4) 选择可转化算法:算法 $CConv(m,s,y_s,x_c,y_c)\rightarrow s$ 可使证实者在一定的策略下把一个证实签名转化为普通的数字签名,若转化失败,则输出 $\perp$.

(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.

一般地,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应拒绝合作,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,这样可使签名者在签名时可选择证实者.

证实签名的一个重要特性是不可视性,即除证实者以外的任何人都不能证明任意一个证实签名是否有效,对签名者也是如此.证实签名的另一个特性是签名者的安全,即除签名者以外任何人都不能生成一个有效的证实签名,对证实者也是如此.

2 证实数字签名的一般实现

Camennisch 和 Michels 给出了一个将一般的数字签名和一个公钥加密方案转化为证实签名的一般方法,具体如下:设 $SIG=(SKG,Sig,Ver)$ 记一个普通的数字签名方案,其中 SKG 是密钥生成概率算法(输入 1^l,其输出为密钥对(x,y));Sig 是一个签名算法(输入为签名秘密钥 x,相应的公开钥 y,信息 $m\in\{0,1\}^*$,则输出为关于信息 m 的签名 s);Ver 是一个验证算法(输入为信息 m,一个宣称的关于信息 m 的签名 s 及签名者的公开钥 y,输出为 1

当且仅当 s 确实是拥有与 y 对应的秘密钥的签名者对信息 m 的签名).进一步地,设 ENC=(EKG,Enc,Dec)是一个公钥加密方案,当输入一个安全参数时,EKG 的输出为一个密钥对(x',y');当输入公开钥 y'及信息 m'时,Enc 的输出为密文 c;当输入信息密文 c、秘密钥 x'及公开钥 y'时,Dec 的输出为 m'(若密文 c 正确),否则输出⊥.

给定一个适当的普通签名方案 $SIG=(SKG,Sig,Ver)$ 及一个适当的公钥加密方案 ENC=(EKG,Enc,Dec),证实数字签名方案可如下构造:

(1) 分别选择 CKGS(1^l):= SKG(1^l),CKGC(1^l):= EKG(1^l);

(2) 签名者计算 $s:=Sig(x_s,y_s,m)$ 及 $e:=Enc(y_c,s)$,则对信息 $m\in\{0,1\}^*$ 的证实签名为 e;

(3) 证实者和验证者的证实与否认协议 $(CVerC,CVerV)$ 如下:给定一个宣称是信息 m 的证实签字 e,在符合证实策略的情况下,证实者解密 e 得到 $\hat{s}:=Dec(e,x_c,y_c)$.若 $Ver(m,\hat{s},y_s)=1$,证实者告诉验证者该证实签名是有效的,并通过联合零知识证明他知道信息a和b满足:b是与公开钥 y_c 对应的证实秘密钥,且 $a=Dec(e,b,y_c)$ 与 $Ver(m,a,y_s)=1$ 同时成立;否则证实者告诉验证者该证实签名是无效的,并通过联合零知识证明他知道信息a和b满足:b是与公开钥 y_c 对应的证实秘密钥,且 $a=Dec(e,b,y_c)$ 但 $Ver(m,a,y_s)=0$ 同时成立,或解密失败.

(4) 当 $Ver(m,\hat{s},y_s)=1$,即证实签名是有效时,在符合转化策略的情况下,证实者选择转化算法 $CConv(m,e,y_s,x_c,y_c)$ 输出 $Dec(e,x_c,y_c)=s$,得到转换后的签名即普通数字签名 s;否则输出⊥.

(5) 转换后的签名 s 的公开验证算法 $CovVer(m,s,y_s)\hat{=}Ver(m,s,y_s)$.

定理 1[1]. 若上述算法中的数字签名算法 $SIG=(SKG,Sig,Ver)$ 在适应性选择明文攻击下是抗存在伪造攻击的,且公钥加密方案 ENC=(EKG,Enc,Dec)在适应性选择明文攻击下是安全的,则按上述算法构造的证实数字签名方案是安全的且具有签名转化功能.

3 基于数字签名算法 DSA 及公钥加密算法 RSA 的证实数字签名方案

本节给出一个基于美国国家数字签名标准算法 DSA 及著名的公钥密码体制 RSA 算法构造的证实签名新方案.新方案的最大优点是,它所使用的普通数字签名算法 DSA 及公钥密码体制 RSA 均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,尽管它们的安全性并未得到严格的证明.新方案是目前已知文献中首次将数字签名标准算法 DSA 引入到证实数字签名方案中的,因此新方案具有很强的实用性,在新方案中使用了零知识证明,并在零知识证明中首次使用了否认证明方案.

下面用 ENC=(EKG,Enc,Dec)记 RSA 概率公钥加密算法,用 $SIG=(SKG,Sig,Ver)$ 记美国国家数字签名标准算法 DSA,其中 SKG 是密钥生成概率算法,当输入为 1^l,其输出密钥为 (p,q,g,y,x),其中 (p,q,g) 为系统公开参数,p 是 L 位长的大素数,L 在 512~1 024 之间且是 64 的倍数,q 是 160 位长的素数且 $q|(p-1)$,g 是群 Z_p 中阶为 q 的生成元,即 $g^q \bmod p=1$,一般可取 $g=h^{(p-1)/q} \bmod p$,h 是小于 $(p-1)$ 并且使 $h^{(p-1)/q} \bmod p>1$ 的任意数.y 是公开钥,x 是相应的秘密钥,且 $y=g^x \bmod p$;Sig 是签名算法,当输入签名秘密钥 x,相应的公开钥 y,信息 $m\in\{0,1\}^*$,则输出为关于信息 m 的签名 $Sig(m,x,y)=(r,s)$,其中 $r=(g^k \bmod p) \bmod q$,$s=(k^{-1}(H(m)+xr)) \bmod q$,$k$ 是小于 q 的一个随机数,H 是安全 hash 算法 SHA-1[9];Ver 是一个验证算法,当输入为信息 m,一个宣称的关于信息 m 的签名(r,s)及签名者的公开钥 y 时,验证算法 $Ver(m,r,y,s)=1$ 当且仅当(r,s)确实是拥有与 y 对应的秘密钥的签名者对信息 m 的签名,即检验方程式 $r=((g^{H(m)s^{-1} \bmod q}y^{rs^{-1} \bmod q}) \bmod p) \bmod q$ 成立,否则 $Ver(m,r,y,s)=0$.

下面给出一个新的基于公钥密码体制 RSA 及美国国家数字签名标准算法 DSA 的证实数字签名方案.

(1) 签名者 S 的密钥生成算法:令 CKGS(1^l)=SKG(1^l)→ (p,q,g,y,x),其中 (p,q,g) 为系统公开参数,y 是签名者的公开钥,x 相应的签名秘密钥,且 $y=g^x \bmod p$;

(2) 证实者 C 的密钥生成算法:令 CKGC(1^l)= EKG(1^l)→ (n,e,d),其中 n 是两个大素数的乘积,(n,e)是 RSA 公开钥,d 是相应的秘密钥是两个概率算法,证实者的公开钥为(n,e),证实者的秘密钥为 d.

(3) 签名者 S 的签名算法:签名者 S 对信息 $m\in\{0,1\}^*$ 的概率证实数字签名算法 $CSig(m,x_s,y_s,y_c)\to s$ 分为两步.首先利用 DSA 中的普通数字签名算法 Sig 对信息签名,得到关于信息 m 的签名 $Sig(m,x,y)=(r,s)$;然后利用公钥密码体制 RSA 对签名(r,s)进行加密,得到证实签名 $s=(c_1,c_2)$,其中$c_1=r^e \bmod n, c_2=s^e \bmod n$.

(4) 证实与否认算法 $(CVerC,CVerV)$:当验证者 V 得到一个信息 $m\in\{0,1\}^*$ 的证实签名 $s=(c_1,c_2)$ 时,若想知

道其是否有效,须经过证实者 C 的确认.验证者传递信息 $m\in\{0,1\}^*$ 及签名 $s=(c_1,c_2)$ 给证实者.证实者 C 首先检验是否符合证实策略,若符合,则利用秘密钥 d,计算 $r=c_1^d \bmod n, s=c_2^d \bmod n$,利用 DSA 的数字签名验证算法 Ver 验证关于信息 m 的签名(r,s)的有效性.

(4.1) 若 $Ver(m,r,y,s)=1$,则 $s=(c_1,c_2)$ 确实是信息 $m\in\{0,1\}^*$ 的证实签名.因验证者 V 并不信任证实者 C,故证实者 C 须向验证者 V 证明这一结论,证实者 C 与验证者 V 之间执行以下的证实协议:

$$PK\{a,b:c_1=a^e \bmod n\wedge c_2=b^e \bmod n$$
$$\wedge c_1=((g^{H(m)b^{-1} \bmod q}y^{ab^{-1} \bmod q} \bmod p) \bmod q)^e \bmod n\}(m)$$
$$=\{s_1,s_2,s_3,s_4,c\}\in Z_q\times Z_q\times Z_q\times\{0,1\}^{160}.$$

该协议的具体实现如下:

Step1. 证实者 C 任选 $r_1\in_R Z_n^*$, $r_2\in_R Z_n^*$,利用安全 hash 算法 SHA-1 计算:

$$c=H(m\|c_1\|c_2\|p\|q\|y\|n\|e\|r_1^e \bmod n\|r_2^e \bmod n\|((g^{H(m)r_2^{-1} \bmod q}y^{r_1r_2^{-1} \bmod q} \bmod p) \bmod q)^e \bmod n),$$

并且检验 $c\neq 0$;若 $c=0$,重新执行 Step1;

Step2. 证实者 C 计算:

$$s_1=\frac{r_1}{rc}\bmod q,\ s_2=\frac{r_2}{sc}\bmod q,\ s_3=[(r_1r_2^{-1}-rs^{-1})/c]\bmod q,\ s_4=[(H(m)r_2^{-1}-H(m)s^{-1})/c]\bmod q,$$

并传递 $\{s_1,s_2,s_3,s_4,c\}\in Z_q\times Z_q\times Z_q\times Z_q\times\{0,1\}^{160}$ 给验证者;

Step3. 验证者 V 验证等式

$$c=H(m\|c_1\|c_2\|p\|q\|y\|n\|e\|c_1s_1^ec^e \bmod n\|c_2s_2^ec^e \bmod n\|(c_1((g^{cs_4}y^{cs_3} \bmod p) \bmod q)^e \bmod n))$$

是否成立,若成立,则相信 $s=(c_1,c_2)$ 确实是信息 $m\in\{0,1\}^*$ 的证实签名,否则输出错误信息;

(4.2) 若 $Ver(m,r,y,s)=0$,即证实者 C 计算 $r=c_1^d \bmod n, s=c_2^d \bmod n$,但是 $r\neq((g^{H(m)s^{-1} \bmod q}y^{rs^{-1} \bmod q}) \bmod p) \bmod q$,则 $s=(c_1,c_2)$ 不是信息 $m\in\{0,1\}^*$ 的证实签名.因验证者 V 并不信任证实者 C,故证实者 C 须向验证者 V 证明这一结论.证实者 C 和验证者 V 执行下面否认协议:

$$PK\{a,b:c_1=a^e \bmod n\wedge c_2=b^e \bmod n\wedge c_1\neq$$
$$((g^{H(m)b^{-1} \bmod q}y^{ab^{-1} \bmod q} \bmod p) \bmod q)^e \bmod n\}(m)\{s_1,s_2,s_3,s_4,s_5,c,c_0\}\in Z_q\times Z_q\times Z_q\times Z_q\times Z_q\times\{0,1\}^{160}\times Z.$$

该协议的具体步骤为

Step1. 证实者 C 任选 $r_1\in_R Z_n^*$, $r_2\in_R Z_n^*$, $r_3\in_R Z_n^*$,利用安全 hash 算法 SHA-1 计算:

$$c=H(m\|c_1\|c_2\|p\|q\|y\|n\|e\|r_1^e \bmod n\|r_2^e \bmod n\|r_3^e \bmod n\|((g^{H(m)r_2^{-1} \bmod q}y^{r_1r_2^{-1} \bmod q} \bmod p) \bmod q)^e \bmod n).$$

Step2. 证实者 C 计算 $r_0=((g^{H(m)s^{-1} \bmod q}y^{rs^{-1} \bmod q}) \bmod p) \bmod q$,计算承诺:

$$c_0=r_0^e \bmod n;\ s_1=\frac{r_1}{rc}\bmod q,\ s_2=\frac{r_2}{sc}\bmod q,\ s_3=\frac{r_3}{r_0c}\bmod q,$$
$$s_4=[(r_1r_2^{-1}-rs^{-1})/c]\bmod q,\ s_5=[(H(m)r_2^{-1}-H(m)s^{-1})/c]\bmod q,$$

并传递 $\{s_1,s_2,s_3,s_4,s_5,c,c_0\}\in Z_q\times Z_q\times Z_q\times Z_q\times Z_q\times\{0,1\}^{160}\times Z_q$ 给验证者;

Step3. 验证者 V 验证 $c_1\neq c_0$ 成立,而且

$$c=H(m\|c_1\|c_2\|p\|q\|y\|n\|e\|c_1s_1^ec^e \bmod n\|c_2s_2^ec^e \bmod n\|c_0s_3^ec^e \bmod n\|(c_0((g^{cs_5}y^{cs_4} \bmod p) \bmod q)^e \bmod n))$$

成立,则验证者 V 确信 $s=(c_1,c_2)$ 不是信息 $m\in\{0,1\}^*$ 的证实签名.否则输出错误信息;

(5) 选择可转化算法的数字签名,证实者在一定策略下把一个证实签名 $s=(c_1,c_2)$ 转化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(r,s)即可,其中 $r=c_1^d \bmod n, s=c_2^d \bmod n$.若转化失败,则输出$\perp$.

(6) (普通)数字签名验证算法 $CoVer(m,sig,y_s)\to\{0,1\}$ 只要取 DSA 中的数字签名验证算法 Ver 即可.

一般地,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

息证实者应拒绝合作,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 基于 RSA 及 DSA 的证实数字签名算法的安全性分析

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,而且新方案的设计完全是第 2 节所指出的利用一个数字签名方案和一个公钥加密体制构造证实签名的一个具体实现.新方案的核心是设计证实者与验证者之间的证实与否认协议.若 $s=(c_1,c_2)$ 确实是信息 $m\in\{0,1\}^*$ 的证实签名,证实协议使用了三步式的零知识证明方法,这里的知识是指利用 DSA 对信息 m 的普通数字签名(r,s),证实者利用自己的秘密钥通过对证实签名的计算可获得该知识,但是应注意到,证实者并不能直接对信息 m 进行 DSA 数字签名,证实者在没有泄露有关该知识的条件下使验证者确信证实签名是正确的.若 $s=(c_1,c_2)$ 不是信息 $m\in\{0,1\}^*$ 的证实签名,证实者须向验证者证明证实者计算 $r=c_1^d \bmod n, s=c_2^d \bmod n$,但是 $r\neq((g^{H(m)s^{-1}\bmod q}y^{rs^{-1}\bmod q})\bmod p)\bmod q$ 这一事实.这里使用了否认协议,否认协议使用了一个新的方法,这在零知识证明中首次被使用.这里引进了承诺量 $c_0=r_0^e \bmod n$,其中 $r_0=((g^{H(m)s^{-1}\bmod q}y^{rs^{-1}\bmod q})\bmod p)\bmod q$,并且注意到,若 $s=(c_1,c_2)$ 确实是信息 $m\in\{0,1\}^*$ 的证实签名,此时由 DSA 数字签名验证算法可知, $r=((g^{H(m)s^{-1}\bmod q}y^{rs^{-1}\bmod q})\bmod p)\bmod q$,必有 $r_0=r$从而$c_0=c_1$,这样否认协议中验证者通过验证 $c_1\neq c_0$,并且

$$c=H(m\|c_1\|c_2\|p\|q\|y\|n\|e\|c_1s_1^ec^e \bmod n\|c_2s_2^ec^e \bmod n\|c_0s_3^ec^e \bmod n\|(c_0((g^{cs_5}y^{cs_4} \bmod p)\bmod q)^e \bmod n))$$

成立,保证了 $r\neq((g^{H(m)s^{-1}\bmod q}y^{rs^{-1}\bmod q})\bmod p)\bmod q$ 而且 c_0 具有正确的 $c_0=r_0^e \bmod n$ 的形式.

在上述协议中,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信息 m 通过 DSA 的签名,在假设 DSA 安全的条件下,签名者的签名秘密钥是安全的,即签名者是安全的.实际上,迄今为止还未见到对 DSA 的存在伪造签名攻击,DSA 目前是实际安全的.

在上述的协议中,证实者也是安全的,即新方案中的证实签名方案具有“不可见性”.假设有一个对手,对手掌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,并且可以以任意的神喻模式访问证实与否认算法 $(CVerV,CVerV)$ 以及转化算法 $CConv(m,s,y_s,x_c,y_c)\rightarrow(r,s)$,该对手也难于获得证实者的证实秘密钥的任何信息,因为证实签名实际上是利用 RSA 公钥密码体制对 DSA 数字签名加密,若假设 RSA 是安全的,则证实者是安全的,即系统中只有证实者可以证实签名的有效性以进行确认.

因此,新协议在 DSA 数字签名算法及 RSA 安全的假设下是安全可行的.但由于对 DSA 数字签名算法及 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 小 结

证实数字签名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化协议,将双方的证实签名转化为数字签名,即可实现合同的公平签署.本文提出的证实签名方案实现了利用较为常用的数字签名算法 DSA 及公钥加密体制 RSA 构造证实签名方案的设想,它的应用将是广泛的.但是它的安全性是建立在 DSA 及 RSA 安全的基础上的,如何构造理论上安全的证实签名方案将需要进一步的深入研究.

References:

[1] Chaum D, van Antwerpen H. Undeniable signatures. In: Brassard G, ed. Proceedings of the Advances in Cryptology (CRYPTO' 89). LNCS 435, Berlin: Springer-Verlag, 1990. 212~216.

[2] Chaum D. Designated confirmer signatures. In: De Santis A, ed. Proceedings of the Advances in Cryptology (EUROCRYPT' 94). LNCS 950, Berlin: Springer-Verlag, 1994. 86~89.

[3] Okamoto T. Designated confirmer signatures and public-key encryption are equivalent. In: Desmendt YG, ed. Proceedings of the Advances in Cryptology (CRYPTO' 94). LNCS 839, Berlin: Springer-Verlag, 1994. 61~74.

[4] Michels M, Stadler M. Generic constructions for secure and efficient confirmer signature schemes. In: Nyberg K, ed. Proceedings of the Advances in Cryptology (EUROCRYPT' 98). LNCS 1403, Berlin: Springer-Verlag, 1998. 406~412.

[5] Camenisch J, Michels M. Confirmer signature secure against adaptive adversaries. In: Preneel B, ed. Proceedings of the Advances in Cryptology (EUROCRYPT 2000). LNCS 1807, Berlin: Springer-Verlag, 2000. 243~258.

[6] 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.

[7] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk H, ed. Proceedings of the Advances in Cryptology (CRYPTO' 98). LNCS 1462, Berlin: Springer-Verlag, 1998. 13~25.

[8] National Institute of Standards and Technology. Digital signature standard. NIST FIPS PUB 186, Department of Commerce, NIST, 1994.

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

全国第 13 届网络与数据通信学术会议(NDCS13)

征 文 通 知

本届会议旨在推动开放系统及其互联技术、开放式网络技术和数据通信技术的发展。会议由中国计算机学会开放系统专委会和网络与数据通信专委会联合主办、大连理工大学电子与信息工程学院承办、大连市计算机学会协办，定于 2003 **年** 10 **月在大连市同** 2003 **年全国开放式分布与并行计算学术会议联合举行。有关信息如下：**

一、征文范围

开放系统及其互联技术，新一代网络体系结构与协议，网络智能化，网络管理，网络信息系统模型，网络计算与应用，网络环境下的信息安全，无线通信网络，电子商务系统以及光纤通信等技术。

二、征文要求

(1) **论文应是未正式发表的，或者未正式等待刊发的研究成果；**

(2) **论文格式仿照《计算机研究与发展》刊物的格式，应包含题目、摘要、关键词、正文和参考文献；**

(3) **论文中、英文均可，一般不超过** 5000 **字，一律用** Word2000 **格式排版，提供** A4 **激光打印稿一式两份，并随寄软盘；**

(4) **邮寄论文时，须在信封左下角或** Email **主题中注明**"NDCS13"**；**

(5) **经程序委员会审查合格的论文，将收入论文集，在自然科学核心刊物集中发表或者推荐到适当刊物发表；**

(6) **论文一律寄给大连地区联系人。论文自留底稿，恕不退稿。**

三、重要日期与联系方式

(1) **论文须在** 2003 **年** 6 **月** 30 **日之前寄达，录用通知将在** 2003 **年** 7 **月** 15 **日发出。**

(2) **联系方式**:

- **大连地区联系人**:**郭禾、单慧英**

地址: **大连理工大学计算机系系统结构教研室 邮编**: 116023 **电话**: 0411–4708497

E-mail: dpcs2003@dlut.edu.cn

- **北京地区联系人**:**陈炳从(中国计算机学会开放系统专委会主任)**

通信地址: **北京** 619 **信箱** 63 **号 邮编**: 100083 **联系电话**: 010–62311951

- **石云(网络与数据通信专委会秘书长)**

通信地址: **北京宣武门西大街** 131 **号国家邮政局信息技术局 邮编**: 100808 **联系电话**: 010–66419786

(3) **会议主页**: http://hefeng.dlut.edu.cn/DPCS2003