一种新的前向安全可证实数字签名方案

秦 波[1] 王尚平[1,2] 王晓峰[1] 罗喜召[3]
[1](西安理工大学理学院 西安 710048)
[2](西安电子科技大学ISN国家重点实验室 西安 710071)
[3](苏州大学计算机科学与技术学院 苏州 215006)
(qinbo-77@163.com)

摘 要 基于前向安全数字签名和可证实数字签名的理论,一种前向安全可证实数字签名的新方案被提出,首次将数字签名的前向安全和可证实的功能结合在一起,并且证实过程应用零知识证明的思想.在因子分解、离散对数及二次剩余问题的困难假设下,系统是安全的.该方案的前向安全保证了即使当前时间段的签名密钥被泄漏,敌手也不能伪造以前的签名,在公钥固定不变的前提下,对密钥进行定期更新.并且由一个半可信任第3方——证实者——来验证签名,从而控制签名有效性的传播,并防止签名者对不利的签名拒绝验证的行为.

关键词 前向安全签名;可证实签名;零知识证明;RSA;数字签名

中图法分类号 TP309

A New Forward-Secure and Confirmer Digital Signature Scheme

QIN Bo[1], WANG Shang-Ping[1,2], WANG Xiao-Feng[1], and LUO Xi-Zhao[3]
[1](*School of Sciences, Xi'an University of Technology, Xi'an* 710048)
[2](*National Key Laboratory on ISN, Xidian University, Xi'an* 710071)
[3](*Computer Science and Technology School, Soochow University, Suzhou* 215006)

Abstract Based on the theory of forward-secure digital signature scheme and confirmer signature scheme, a new forward-secure and confirmer signature scheme is proposed. It is the first time that forward-secure and confirmer are combined in a digital signature scheme. The idea of zero-knowledge proof is used in the confirming process. The scheme is proven to be secure under the assumption of the intractability of factoring and discrete logarithm and quadric remain problems. Forward security of the scheme means that even if the secret key of current time period is compromised, some security remains: it is not possible to forge the signature relating to the past. Secret key is evolved with different period time while the public key is fixed in the life time. And the partially trusted player—conformer could verify the signature who can control the distribution of the verification of the signature and prevent the signer from denying the disadvantageous signature.

Key words forward-secure signature; confirmer signature; zero-knowledge proof; RSA; digital signature

1 引 言

1.1 前向安全问题的提出

普通数字签名具有如下局限性:若签名者的密钥被泄漏,那么这个签名者所有的签名(过去的和将来的)都有可能泄漏.这个局限性影响了签名应该提供的不可否认性.实际上,签名者否认他自己签名最简单的方法就是在Internet上匿名公开自己的密钥,然后声明计算机遭到了入侵.目前各种吊销

收稿日期:2002-05-30;**修回日期**:2002-11-06
基金项目:国家自然科学基金(60273089);陕西省教育厅自然科学研究计划基金(00JK266);西安理工大学青年教师攻读硕士学位科学研究基金(210107)

技术可以阻止用户接受泄漏密钥的签名,然而,即使有了吊销技术,在密钥泄漏前接受签名的用户也不能保证签名者是否足够诚实,能够用新密钥重新进行签名.

为了突破这个局限性,人们提出了很多不同的方法,有许多方法企图避免密钥在一些系统传输中被泄露,通常使用秘密共享. 但是,这种方法耗费巨大,尤其对于单个用户来说实施起来极其昂贵,而且每个系统都可能受到相似的攻击,实际上不会减少危险性. 一个较好的方法是当密钥泄露的时候,减少潜在的损失,即所谓的前向安全[1]. 确保密钥在短期使用时间内是安全的,其主要思想是当前密钥的泄露并不影响以前时间段签名的安全性. 设计这样一个系统的困难之一是在公钥保持不变的情况下能够改变密钥.

1.2 前向安全数字签名的密钥进化过程的构造

前向安全数字签名实现的一个关键是密钥进化:系统建立初期用户注册获得一个证书,得到公钥 PK 和相应的密钥 SK_0. 将公钥的有效期分为 T 个时段,分别记为 $1,2,3,\cdots,T$. 在有效期内,公钥 PK 是固定的,而密钥随时段不断进化更新. 以 SK_i 记 i 时段的密钥,进入 i 时段时,首先计算 $SK_i = f(SK_{i-1})$,这里 f 是一单向函数,求得 SK_i 后立即删除 SK_{i-1}. 这样即使当攻击者在 i 时段攻入系统获得了 SK_i,还是不能获得 SK_{i-1}, SK_{i-2}, $\cdots$, SK_0,因为它们已被删除且用单向函数进化计算而得. 密钥的进化如下所示:

$$SK_0 \xrightarrow{f} SK_1 \xrightarrow{f} SK_2 \xrightarrow{f} \cdots \xrightarrow{f} SK_T.$$

1.3 可证实数字签名方案的提出

对于普通数字签名,如果知道签名者的公钥,任何人都可以验证签名. 为了限制数字签名有关信息的传播,Chaum 和 van Antwerpen 引入了不可否认签名[2]的概念,而不可否认签名只有在签名者的合作下才可以验证. 当然签名者一定可以否认无效签名,但是,必须不能否认有效签名. 因此,签名者可以控制签名有效性的传播. 但是这样也会出现问题:如果出现不利于签名者的签名,他可以通过拒绝合作而使签名不再具有验证性. Michels 等针对这个问题又提出了可证实签名[3,4]的概念. 这样,证实或否认签名的权力移交给了第 3 方 Confirmor. Confirmor 不参与签名过程,但根据相关协议 Confirmor 决定向谁验证签名的正确性,同时在特定情况下,Confirmor 可以将可证实签名转化成一个普通数字签名.

1.4 可证实数字签名方案的一般模型

在一个可证实签名方案中,有 3 方参与:签名者 S,证实者 C 和验证者 V. 在证实者 C 的帮助下才可验证签名. 可证实签名方案包括以下步骤:

(1) 密钥生成过程

$KG_S(l^l) \rightarrow (x_S, y_S)$: l 是概率算法 KG_S 的参数,生成签名者的签名密钥和公钥对 (x_S, y_S).

$KG_S(l^l) \rightarrow (x_C, y_C)$: l 是概率算法 KG_C 的参数,生成证实者的签名密钥和公钥对 (x_C, y_C).

(2) 签名过程

对一个消息 m 使用概率签名生成算法:$C_{sig}(m, x_S, y_S, y_C) \rightarrow \sigma$,得到签名 σ.

(3) 证实和否认过程

在证实者 C、验证者 V 之间存在一个签名验证协议:

$$(CVerC, CVerV): \langle C_{Ver}(x_c), V_{Ver}() \rangle$$

$$(m, \sigma, y_S, y_C) \rightarrow V \begin{cases} 0 \\ 1 \end{cases}.$$

证实者的秘密输入为 x_C,双方的共同输入为 (m, σ, y_S, y_C),验证结果为 1(真)或 0(假).

(4) 签名转化过程

证实者使用算法:$C_{conv}(m, \sigma, y_S, x_C) \rightarrow s$ 将可证实签名 σ 转化成一个普通签名 s.

(5) 普通签名验证过程

任何人使用算法 $COVer(m, s, y_S) \rightarrow \{0,1\}$,将消息 m,普通签名 s,签名者公钥 y_S 作为输入,可以得到逻辑值,对签名进行验证.

2 基于离散对数知识的前向安全可证实数字签名方案

下面将提出一种使用离散对数知识的前向安全可证实数字签名方案. 新方案的优点是系统的签名公钥短,密钥的进化速度快. 证实者在不泄漏知识(即签名)的前提下向验证者证明 σ 是否是消息 $m \in \{0,1\}^*$ 的证实签名. 并且要求验证的速度快,具有实用性.

2.1 系统的建立

本系统签名算法是基于大群的有效群签名方案[5]及著名的公钥密码体制 RSA 算法[6]构造的证实签名方案.

(1) 签名者初始密钥对的生成

设 p, q 均为大素数,令 $N = pq$,构造群 $G =$

$\langle g\rangle$,使其阶数为 N,即 $ord(g)=N$;将签名密钥的有效期分为 T 个时段,任选 $x_0\in_R Z_N$,令 $y_T=g^{x_0^{2^T}}$,该系统签名者的签名公钥 $PK=\{g,N,y_T\}$,签名者的初始密钥 $SK_0=\{x_0\}$. 即签名者的签名密钥和公钥的初始对$(x_{s0},y_s)=(SK_0,PK)$,其中 $x_{S0}=x_0,y_S=y_T$.

(2) 签名者密钥的进化

系统一旦进入 $i(1\leqslant i\leqslant T)$时段,签名者使用拥有的 $i-1$ 时段的密钥 $SK_{i-1}=\{x_{i-1}\}$,计算 $x_i=x_{i-1}^2 \bmod N$ 及 $y_i=g^{x_i}$,则由归纳法可知 $x_i=x_0^{2^i}\bmod N$ 且 $y_i=g^{x_{i-1}^2}$, $y_T=g^{x_0^{2^T}}=g^{x_{i-1}^{2^{T-i+1}}}=g^{x_i^{2^{T-i}}}$,此时立刻从系统中完全删除 $i-1$ 时段的密钥 $SK_{i-1}=\{x_{i-1}\}$,保密 i 时段的密钥 $SK_i=\{x_i\}$,y_i,y_T. 由求离散对数根的困难性可知,由 y_i,y_T 无法获得 x_0,x_{i-1}. 在第 i 时段签名者的签名密钥和公钥对$(x_{Si},y_S)=(SK_i,PK)$,其中 $x_{Si}=x_i,y_S=y_T$.

2.2 证实者密钥对的生成

证实者的密钥对采用 RSA[6]算法的密钥对. N 是两个大素数的乘积,(N,e)是 RSA 公钥,d 是相应的密钥. 证实者的公钥为(N,e),证实者的密钥为 d.

2.3 签名者 S 的签名算法

签名者 S 对消息 $m\in\{0,1\}^*$ 的概率证实数字签名算法 $C_{sig}(m,x_S,y_S,y_C)\to\sigma$ 分为两步:首先,用基于零知识的大群有效群签名方案[5]对消息 m 签名,得到关于消息 m 的签名;然后,用公钥密码体制 RSA 对签名进行加密,得到证实签名.

(1) 基于零知识的大群有效群签名方案的签名

$i(1\leqslant i\leqslant T)$时段签名者对消息 m 的签名为$\langle i,SGN(m,x_{Si}),y_T\rangle$. 其中:$SGN(m,x_{Si})$实际上是以 y_T 为公钥,x_{Si}为密钥的密钥对关于消息 m 的数字签名.

签名过程如下:签名者任选 $k\in_R Z_N$,计算 $c=H(m\parallel g\parallel y_T\parallel i\parallel g^k)$,这里 $H:\{0,1\}^*\to\{0,1\}^l$ 为单向抗碰撞安全哈希函数. 则 $c\in\{0,1\}^l$,令 $s=k-x_{Si}^{2^{T-i}}c\bmod N$,则签名者对信息 m 的签名为$\langle i,SGN(m,x_{Si}),y_T\rangle=\{c,s\}\in\{0,1\}^l\times Z_N$.

(2) 基于 RSA 签名方案的证实签名

得到$\langle i,SGN(m,x_{Si}),y_T\rangle=\{c,s\}\in\{0,1\}^l\times Z_N$ 后,签名者利用公钥密码体制 RSA 对签名$\{c,s\}$进行加密,得到证实签名 $\sigma=(c_1,c_2)$,其中 $c_1=c^e\bmod N,c_2=s^e\bmod N$.

2.4 证实与否认算法

当验证者 V 得到一个消息 $m\in\{0,1\}^*$ 的证实签名 $\sigma=(c_1,c_2)$,要知道其是否有效,需经过证实者 C 的确认. 验证者传递消息 $m\in\{0,1\}^*$ 及签名 $\sigma=(c_1,c_2)$给证实者,证实者首先验证是否符合证实策略,若符合则利用密钥 d 计算 $c=c_1^d\bmod N,s=c_2^d\bmod N$. 证实者验证$\{c,s\}$是否为 m 的签名$\langle i,SGN(m,x_i),y_T\rangle$. 算法如下:证实者计算 $\zeta=H(m\parallel g\parallel y_T\parallel i\parallel g^s y_T^c)$,若 $\zeta=c$,则签名正确,即 $Ver(m,c,s)=1$;否则签名不正确,即 $Ver(m,c,s)=0$.

(1) 若 $Ver(m,c,s)=1$,则 $\sigma=(c_1,c_2)$确实是消息 $m\in\{0,1\}^*$ 的证实签名. 因为验证者 V 并不信任证实者 C,故证实者 C 需向验证者 V 证明这一结论,证实者 C 与验证者 V 执行以下证实协议:

Step1. 证实者 C 计算 $\vartheta=g^s y_T^c$,将 ϑ 传送给验证者.

Step2. 验证者 V 计算 $\zeta=H(m\parallel g\parallel y_T\parallel i\parallel\vartheta)$. 验证 $\zeta=c$ 是否成立,若成立则相信 $\sigma=(c_1,c_2)$确实是消息 $m\in\{0,1\}^*$ 的证实签名,否则输出错误信息.

(2) 若 $Ver(m,c,s)=0$,则 $\sigma=(c_1,c_2)$不是消息 $m\in\{0,1\}^*$ 的证实签名. 即证实者计算 $\zeta=H(m\parallel g\parallel y_T\parallel i\parallel g^s y_T^c)$,但是 $\zeta\neq c$. 在证实者 C 将 $\vartheta(\vartheta=g^s y_T^c)$传送给验证者 V 之前,因为验证者 V 并不信任证实者 C,故证实者 C 必须首先向验证者 V 证明 $\vartheta=g^s y_T^c$ 中的(c,s)为 $\sigma=(c_1,c_2)$(其中 $c_1=c^e\bmod N,c_2=s^e\bmod N$) 中的$(c,s)$. 即零知识证明协议:

$$PK\{\alpha,\beta\mid c_1=\alpha^e\wedge c_2=\beta^e\wedge\vartheta=g^\alpha y_T^\beta\}\Leftrightarrow$$

$$PK\{\alpha,\beta\mid c_1=\alpha^e\wedge c_2=\beta^e\wedge c_3=g^\alpha\wedge(\frac{\vartheta}{c_3})=y_T^\beta\wedge c_3^{c_1}=g^{\alpha^{e+1}}\}\Leftrightarrow$$

$$PK\{\alpha,\beta\mid c_1=\alpha^e\wedge c_3^{c_1}=g^{\alpha^{e+1}}\wedge c_2=\beta^e\wedge(\frac{\vartheta}{c_3})^{c_2}=y_T^{\beta^{e+1}}\}.$$

该协议的具体过程为证明者首先随机地任选 $r_i\in_R Z_N,u_i\in_R Z_N(i=0,1,\cdots,l)$,计算

$$\omega=H(r_0^e\parallel t_1^*\parallel\cdots\parallel t_l^*\parallel u_0^e\parallel k_1^*\parallel\cdots\parallel k_l^*)=\omega[1],\omega[2],\cdots,\omega[l]\in\{0,1\}^l,\text{其中}$$

$$t_i^*=g^{r_i^{e+1}},\ r_i\in_R Z_N,r_0\in_R Z_N,$$

$$k_i^*=y_T^{u_i^{e+1}},\ u_i\in_R Z_N,u_0\in_R Z_N.$$

令

$$s_i=\begin{cases}r_i,若\ \omega[i]=0\\ \dfrac{r_i}{\alpha},若\ \omega[i]=1\end{cases},(i=1,\cdots,l),s_0=\frac{r_0}{\alpha\omega},$$

$$q_i=\begin{cases}u_i,若\ \omega[i]=0\\ \dfrac{u_i}{\beta},若\ \omega[i]=1\end{cases},(i=1,\cdots,l),q_0=\frac{u_0}{\beta\omega}.$$

证明者向验证者传递零知识证明:

$$(\omega[1],\cdots,\omega[l],s_0,s_1,\cdots,s_l,q_0,q_1,\cdots,q_l)\in\{0,1\}^l\times Z_N^{l+1}\times Z_N^{l+1}.$$

验证者的验证过程如下,首先计算:

$$t_i=\begin{cases}g^{s_i^{e+1}},若\ \omega[i]=0\\ (c_3^{c_i})^{s_i^{e+1}},若\ \omega[i]=1\end{cases},i=1,\cdots,l,$$

$$k_i=\begin{cases}g^{q_i^{e+1}},若\ \omega[i]=0\\ (\dfrac{\vartheta}{c_3})^{c_2q_i^{e+1}},若\ \omega[i]=1\end{cases},i=1,\cdots,l.$$

验证等式$(\omega[1],\omega[2],\cdots,\omega[l])=H(c_1s_0^e\omega^e\|t_1\|\cdots\|t_l\|c_2q_0^e\omega^e\|k_1\|\cdots\|k_l)$是否成立.若成立则证明证实者诚实,可以进行以下否认协议;否则终止否认协议.

证实者C与验证者V之间执行以下否认协议:

Step1. 证实者C将ϑ(这里$\vartheta=g^sy_T^c$)传送给验证者V.

Step2. 验证者V计算$\zeta=H(m\|g\|y_T\|i\|\vartheta)$,验证$\zeta=c$是否成立.若不成立则相信$\sigma=(c_1,c_2)$不是信息$m\in\{0,1\}^*$的证实签名,否则输出错误信息.

2.5 选择可转化的数字签名

证实者C在一定的策略下把一个证实签名$\sigma=(c_1,c_2)$转化为普通数字签名的具体算法是:证实者C告诉验证者V消息$m\in\{0,1\}^*$的数字签名(c,s)即可,其中$c=c_1^d\bmod N$,$s=c_2^d\bmod N$.若转化失败,则输出错误信息.

2.6 (普通)数字签名验证算法 $COVer(m,s,y_S)\to\{0,1\}$

将消息m,普通签名(c,s),签名者公钥$y_S=y_T$作为输入,计算$\zeta=H(m\|g\|y_T\|i\|g^sy_T^c)$,若$\zeta=c$,则签名正确,即$Ver(m,c,s)=1$;否则签名不正确,即$Ver(m,c,s)=0$.

关于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消息的一部分,对不符合规定的消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根据需要选择证实者.

3 新方案的安全性分析

上述的前向安全可证实数字签名方案的系统安全性假设包括3个方面:首先,在系统建立时基于循环群上离散对数问题的困难性,并且该假设也是零知识证明的基础,离散对数问题是目前多密码系统采用的安全性假设;其二,在密钥进化的过程中涉及到了模N下二次剩余问题的困难性,该假设也是数字签名前向安全的基本保证;其三,因为证实签名用的是RSA算法,基于大合数素数分解的困难性,这一点与RSA的安全性假设一致.在以上3个基本假设下,所提方案显然是前向安全且可证实的.

4 结 论

上述新方案的协议与算法的正确性与有效性通过验证可知是成立的,而且其设计是利用离散对数知识构造前向安全签名和一个公钥加密体制构造证实签名的一个具体实现,该方案核心是简单方便地完成了密钥的进化,实现了前向安全和证实者进行验证这两个功能.

这个证实协议实为零知识证明协议,其主动权掌握在证实者手中,使证实者可以根据证实策略决定对哪些人的证实签名进行证实,例如,一个策略可以是仅对某一个时间段内的签名进行验证,或对某些特定的人群提交的签名进行验证.在证实的过程中,由于离散对数问题的困难性,证实者并没有泄漏要保密的知识.由于使用了哈希函数,所以在预计算处理的基础上速度快,具有实用价值.

参 考 文 献

1 M Bellare, S K Miner. A forward-secure digital signaure scheme. In: Proc of the CRYPTO'99. Berlin: Springer-Verlag, 1999. 431~448

2 D Chaum, H van Antwerpen. Undeniable signatures. In: Proc of the CRYPTO'89. Berlin: Springer-Verlag, 1990. 212~216

3 J. Camenisch, M Michels. Confirmer signature secure against adaptive adversaries. In: Proc of the EUROCRYPT'2000. Berlin: Springer-Verlag, 2000. 243~258

4 M Michels, M Stadler. Generic constructions for secure and

efficient confirmer signature schemes. Int'l Conf on Theory and Application of Cryptographic Techniques, Espoo, 1998

5 J Camenisch, M Stadler. Efficient group signatures schemes for large groups. In: Proc of the CRYPTO'97. Berlin: Springer-Verlag, 1997. 410～423

6 Bruce Schneier. 吴世忠等译. 应用密码学:协议、算法与C源程序. 北京:机械工业出版社, 2000
(Bruce Schneier. Translated by Wu Shizhong *et al*. Applied Cryptography Second Edition: Protocols, Algorithms, and Sources Code in C. Beijing: China Machine Press, 2000)

秦 波 女,1977 年生,硕士研究生,主要研究方向为密码学理论与网络安全.

王尚平 男,1963 年生,博士,教授,主要研究方向为密码学理论与网络安全.

王晓峰 女,1966 年生,讲师,主要研究方向为信息安全与密码理论.

罗喜召 男,1978 年生,硕士,主要研究方向为信息安全与密码理论.