学术论文

基于零知识证明的前向安全数字签名方案

王尚平[1,2]，王育民[2]，王晓峰[1]，秦波[1]，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）

摘 要：提出了一种基于零知识证明协议的前向安全数字签名的新方案。新方案在因子分解、离散对数及二次剩余问题困难的假设下，在随机 oracle 模型下是前向安全的。

关键词：数字签名；前向安全；零知识证明

中图分类号：TN309.3 **文献标识码**：A **文章编号**：1000-436X(2003)09-0042-06

A new efficient forward-secure digital signature scheme based on zero-knowledge proof protocol

WANG Shang-ping[1,2], WANG Yu-min[2], WANG Xiao-feng[1], QIN Bo[1], ZHANG Ya-ling[1]

(1. Natural Science Institute, Xi'an University of Technology, Xi'an 710048, China;

2. National Key Lab. on ISN, Xidian University, Xi'an 710071, China)

Abstract: Based on the zero-knowledge proof protocol a new forward-secure digital signature scheme is proposed. The scheme is proven to be forward secure based on the hardness of factoring, discrete logarithm and quadric remain problems in the random oracle model.

Key words: digital signature; forward-secure; zero-knowledge proof

1 引言

数字签名的安全应包括两个方面：一方面是签名方案的安全性，即数字签名方案抗密码分析的安全性；另一方面是签名密钥的安全性，即密钥保管的安全性。前者可通过选用著名的数字签名方案并选用大的安全参数，以保证签名方案的安全性。但是签名密钥的被盗，将会导致灾难性的后果。最常见的防止密钥泄露的解决方法是采用多个服务器对密钥分布式共享方案，包括门限签名方案。但是多个服务器的运行成本较高，并且即使采用了分布式多个

收稿日期：2001-10-08；**修订日期**：2003-04-26

基金项目：国家自然科学基金资助项目（60273089）；陕西省教育厅自然科学研究计划项目（00JK266）

作者简介：王尚平（1963-），男，陕西扶风人，博士，西安理工大学教授，主要研究方向为密码理论与网络安全；王育民（1936-），男，北京人，西安电子科技大学教授、博士生导师，主要研究方向为信息论、信道编码、密码学以及通信网的安全性；王晓峰（1966-），女，河南新乡人，西安理工大学讲师，研究方向为密码理论与电子商务的安全性；秦波（1977-），女，湖北石堰人，硕士，西安理工大学助教，研究方向为密码理论与电子商务的安全性；张亚玲（1966-），女，陕西西安人，西安理工大学副教授，研究方向为软件工程。

服务器，可能由于操作系统的安全漏洞，极有可能使窃密者采用同一手段窃取所有的分布式密钥。因此分布式所能提供的安全性并没有人们想象的那么高。

一旦签名密钥被盗，对手可以任意伪造签名，要求完全的安全性是不可能的，但应考虑将损失减少到最小。前向安全数字签名方案[1]正是这样一种特殊的数字签名方案，要求即使对手在盗得当前时段签名密钥的情况下，对手也不能伪造与签名密钥被盗前时段相关的数字签名，其目的是减少因签名密钥泄露带来的损失。前向安全数字签名的基本方法是将签名密钥的有效期（例如一年）分为 T 个时段（T=365 天，或 T=365×24h），若签名密钥在 i 时段泄露，对手可伪造 i 时段以后的数字签名，但对手不能伪造 i 时段以前的数字签名，即保证以前数字签名的安全性。

前向安全数字签名的思想本质是数字签名安全的风险控制，即将签名密钥被盗后造成的损失尽可能减少。本文提出了一种新的前向安全数字签名方案，新方案使用了零知识数字签名的思想，系统的签名公钥短，密钥的进化速度快，在大合数素数分解[2]、离散对数问题[3]及二次剩余问题[4]困难的安全性假设下，在随机 oracle 模型[5]下是前向安全的。

2　前向安全的数字签名的相关知识

2.1　前向安全的数字签名中的秘密钥进化过程

前向安全的数字签名的一个重要概念是密钥进化，即系统建立的初期，用户首先创建并注册签明验证公钥 PK，并获得公钥证书并保密相应的初始签明秘密钥，记为 SK_0。公开钥是固定的初始签明而秘密钥则是随时段不断的进化更新，目的在于提供所谓的前向安全性，将公钥的有效期分为 T 个时段，分别记为 1,2,$\cdots T$。在有效期内公钥 PK 保持不变，但是秘密钥随着时段逐步进化更新，以 SK_i 记 i（$1 \leqslant i \leqslant T$）时段的秘密钥，进入 i 时段时，首先计算 $SK_i = f(SK_{i-1})$，这里 f 是一个单向函数，求得 SK_i 后，立即删除 SK_{i-1}。这样当窃密者在 i 时段攻入系统时，可获得 SK_i 但是不能获得 $SK_{i-1}, SK_{i-2}, \cdots SK_0$，因为它们已被删除且 SK_i 是用单向函数进化计算而得的。秘密钥的进化如图 1 所示。

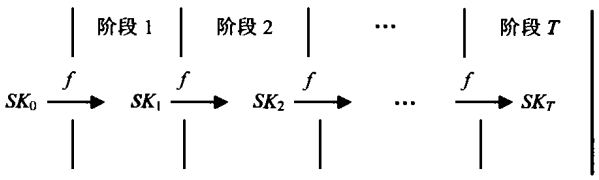

图 1　前向安全数字签名的密钥进化过程

2.2　前向安全的数字签名几种基本解决方案

以下假设采用的数字签名方案（例如，RSA[2,3,6,7]或 DSS 签名方案）中的密钥生成算法为 GEN，签名算法为 SGN，验证算法为 VF。

(1) 长公钥长秘密钥方案：系统建立时，签名者重复执行密钥生成算法产生 T 个密钥对 (p_1,s_1)，(p_2,s_2)，$\cdots(p_T,s_T)$，其中 p_i 为签名验证公钥，s_i 为匹配的秘密钥 $(i=1,2,\cdots T)$。签名者的公开钥为 $PK=(p_1,p_2,\cdots p_T)$，初始秘密钥为 $SK_0=(s_0,s_1,\cdots s_T)$，其中 s_0 为空串。秘密钥的进化过程如下进行，一旦进入 i $(i=1,2,\cdots T)$ 时段，签名者完全删除 s_{i-1}，i 时段的秘密钥为 $SK_i=(s_i,s_{i+1},\cdots s_T)$，$i$ 时段对信息 m 的签名为 $<i,SGN(m,s_i)>$。对信息 m 的签名 $<i,\xi>$ 的验证为检验 $VF(m,p_i,\xi)=1$ 是否成立。该方案显然是前向安全的，但该方案的问题在

于公钥及秘密钥的长度随总的时间段数 T 线性的增长，显然是不可取的。

(2) 短公钥长秘密钥方案：Anderser 提出了上方案的一个改进，其结果为公钥很短，但秘密钥的长度依然随 T 线性增长。签名者同上方案首先产生 T 个密钥对 (p_1,s_1)，(p_2,s_2)，…(p_T,s_T)，并产生一个附加的密钥对 (p,s)，令 $\sigma_i = SGN(i\|p_i,s)$ $(i=1,2,\cdots T)$，然后删除 s。系统的公开钥为 p（短公钥），系统的初始秘密钥为 $SK_0=(s_0,\sigma_0;s_1,\sigma_1;\cdots s_T,\sigma_T)$，其中 s_0,σ_0 为空串。秘密钥的进化过程如下进行，一旦进入 i 时段，签名者完全删除 s_{i-1},σ_{i-1}，i 时段的秘密钥为 $SK_i=(s_i,\sigma_i;s_{i+1},\sigma_{i+1};\cdots s_T,\sigma_T)$，$i$ 时段对信息 m 的签名为 $<i,SGN(m,s_i),p_i,\sigma_i>$，对信息 m 的签名 $<i,(\alpha,q,\sigma)>$ 的验证为检验 $VF(i\|q,p,\sigma)=1$ 及 $VF(m,q,\alpha)=1$ 是否同时成立。该方案提供了前向安全性，但问题在于秘密钥的长度随总的时间段数 T 线性的增长，也是不可取的。

除上述的两个方案外，还有通过证书链使公钥及秘密钥均很短，但代价是签名长度随总的时间段数 T 线性增长的长签名方案，这一点也决定了该方案是实际不可行的。M.Bellare 和 K.Miner 在文献[1]中给出了一个基于二次剩余问题困难性的一种较好的前向安全数字签名方案。

3 零知识证明的相关知识

3.1 零知识数字签名方案

首先给出一个基于零知识的数字签名方案[7]。设有阶为 N 的循环群 $G=<g>$，即生成元 g 的阶 $ord(g)=N$。假设在群 G 中离散对数是一个困难的问题，使用的单向抗碰撞 Hash 函数为 $H:\{0,1\}^* \to \{0,1\}^l$；设签名者的公开钥为 $y=g^x$，签名者的签名秘密钥为 x；签名者欲对信息 m 进行签名，签名算法 $SGN(m,x)$ 如下：签名者任选 $k\in Z_N$，计算 $c=H(m\|g\|y\|g^k)$，则 $c\in\{0,1\}^l$，令 $s=k-xc \bmod N$，则签名者对信息 m 的签名为 $\{c,s\}\in\{0,1\}^l\times Z_N$；验证者接受到信息 m 的签名 $\{\sigma,\varsigma\}\in\{0,1\}^l\times Z_N$，验证算法 $VF(m,\{\sigma,\varsigma\},y)$如下：若 $\sigma=H(m\|g\|y\|g^{\varsigma}y^{\sigma})$ 成立，则签名正确，令 $VF(m,\{\sigma,\varsigma\},y)=1$；否则令 $VF(m,\{\sigma,\varsigma\},y)=0$，输出错误信息。该数字签名方案在随机 oracle 模型下是安全的。

3.2 离散对数的根相等的零知识证明协议

零知识证明是密码学中的一个基本方法。所谓的零知识证明是指证明者使验证者确信证明者拥有某一个秘密值而证明者没有向验证者泄漏关于该秘密值的任何有用信息。在很多密码方案中，都使用了秘密的零知识证明协议。

下面给出与本文有关的离散对数的知识证明的几个基本协议并介绍有关的记号。阶为 N 的循环群 G 中元素 y 关于基 g 的离散对数 x 的知识证明协议[5,8]记为 $PK\{\alpha:y=g^{\alpha}\}$，具体协议为：证明者随机选 $r\in_R Z_N$，计算 $t=g^r$ 并发送 t 给验证者；验证者随机选一个提问 $c\in_R\{0,1\}^k$ 且发送给证明者；证明者计算 $s:=r-cx \bmod N$ 并发送给验证者；验证者接受证明当且仅当 $g^s y^c=t$ 成立。

结合上面的零知识证明协议，下面给出一个与离散对数的根有关并在下节将用到的零知识证明协议。设证明者的秘密值为 $x\in Z_N$，证明者在不泄露该秘密值的前提下，欲使验证者确信该秘密值同时满足 $y_1=g^{x^{e_1}}$ 及 $y_2=g^{x^{e_2}}$。设使用的单向 hash 函数为 $H:\{0,1\}^*\to\{0,1\}^l$。零知识证明的协议为

$$PK\{\alpha : y_1 = g^{\alpha^{e_1}} \wedge y_2 = g^{\alpha^{e_2}}\}(\Phi) \in \{0,1\}^l \times Z_N^l \times Z_N^l$$

该协议的具体过程为：

证明者首先随机的任选 $r_i \in_R Z_N^*$，$w_i \in_R Z_N^*$（$i = l, l-1, \cdots 2,1$），计算

$$C = H(g \| e_2 \| e_1 \| y_2 \| y_1 \| g^{r_l^{e_1}} \| g^{r_{l-1}^{e_1}} \| \cdots \| g^{r_1^{e_1}} \| g^{w_l^{e_2}} \| g^{w_{l-1}^{e_2}} \| \cdots \| g^{w_1^{e_2}})$$

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

令 $s_{i,1} = \begin{cases} r_i, 若 c[i] = 0 \\ \dfrac{r_i}{x}, 若 c[i] = 1 \end{cases}$，$s_{i,2} = \begin{cases} w_i, 若 c[i] = 0 \\ \dfrac{w_i}{x}, 若 c[i] = 1 \end{cases}$（$i = l, l-1, \cdots, 2,1$）。

则 $PK\{\alpha : y_1 = g^{\alpha^{e_1}} \wedge y_2 = g^{\alpha^{e_2}}\}(\Phi) \triangleq (c[l], \cdots c[1], s_{l,1}, \cdots s_{1,1}, s_{l,2}, \cdots s_{1,2}) \in \{0,1\}^l \times Z_N^l \times Z_N^l$

证明者向验证者传递零知识证明

$$(c[l], \cdots c[1], s_{l,1}, \cdots s_{1,1}, s_{l,2}, \cdots s_{1,2}) \in \{0,1\}^l \times Z_N^l \times Z_N^l$$

及相关的公共信息 y_1 及 y_2。

验证者的验证过程如下：首先计算

$$u_{i,1} = \begin{cases} g^{s_{i,1}^{e_1}}, 若 c[i] = 0 \\ y_1^{s_{i,1}^{e_1}}, 若 c[i] = 1 \end{cases}，\quad u_{i,2} = \begin{cases} g^{s_{i,2}^{e_2}}, 若 c[i] = 0 \\ y_2^{s_{i,2}^{e_2}}, 若 c[i] = 1 \end{cases}（i = l, l-1, \cdots 2,1）$$

验证等式 $(c[l], \cdots c[1]) \stackrel{?}{=} H(g \| e_2 \| e_1 \| y_2 \| y_1 \| u_{l,1} \| u_{l-1,1} \| \cdots \| u_{1,1} \| u_{l,2} \| u_{l-1,2} \| \cdots \| u_{1,2})$

若成立则证明者的证明正确，若不成立则给出验证失败的信息。

以上是关于离散对数的根的一个零知识证明的协议，更多的关于零知识证明的相关知识可参阅文献[7]。

4　基于零知识证明的前向安全数字签名方案

下面将提出一种新的使用零知识数字签名思想的前向安全数字签名方案，新方案的目标是要求系统的签名公钥短，密钥的进化速度快。

4.1　系统的建立

设 p, q 均为大素数，令 $N = pq$。构造群 $G = < g >$ 使其阶为 N，即 $ord(g) = N$；任选 $x_0 \in_R Z_N^*$，令 $y_T = g^{x_0^{2^T}}$；系统的前向签名公开钥 $PK = \{g, N, y_T\}$，将前向签名密钥的有效期分为 T 个时段，系统的初始秘密钥 $SK_0 = \{x_0\}$。

4.2　秘密钥的进化

系统一旦进入 $i(1 \leqslant i \leqslant T)$ 时段，签名者利用拥有的 $i-1$ 时段的秘密钥 $SK_{i-1} = \{x_{i-1}\}$，计算

$x_i = x_{i-1}^2 \bmod N$ 及 $y_i = g^{x_i}$，则由归纳法有 $x_i = x_0^{2^i} \bmod N$ 且 $y_i = g^{x_{i-1}^2}$，$y_T = g^{x_0^{2^T}} = g^{x_{i-1}^{2^{T-i+1}}}$，计算零知识证明 $PK\{\alpha : y_i = g^{\alpha^2} \wedge y_T = g^{\alpha^{2^{T-i+1}}}\}(\Phi)$。此时立即从系统中完全删除 $i-1$ 时段的秘密钥 $SK_{i-1} = \{x_{i-1}\}$，保密 i 时段的秘密钥 $SK_i = \{x_i\}$，保留 y_i 及零知识证明 $PK\{\alpha : y_i = g^{\alpha^2} \wedge y_T = g^{\alpha^{2^{T-i+1}}}\}(\Phi)$。

4.3 前向安全的数字签名算法

$i(1 \leqslant i \leqslant T)$ 时段签名者对信息 m 的前向安全数字签名为

$$< i, SGN(m, x_i), y_i, \ PK\{\alpha : y_i = g^{\alpha^2} \wedge y_T = g^{\alpha^{2^{T-i+1}}}\}(\Phi) >$$

其中：在 i 时间段对信息 m 的签名数字（如 3.1 节所示）$SGN(m, x_i) = \{c, s\} \in \{0,1\}^l \times Z_N$。实际计算为，签名者任选 $k \in_R Z_N$，计算 $c = H(m \| g \| y_i \| g^k)$，则 $c \in \{0,1\}^l$，令 $s = k - x_i c \bmod N$。

此时注意到对信息 m 的签名实际由两部分组成，$SGN(m, x_i)$ 实际上是以 y_i 为公钥以 x_i 为秘密钥的密钥对关于信息 m 的数字签名，剩余的零知识证明 $PK\{\alpha : y_i = g^{\alpha^2} \wedge y_T = g^{\alpha^{2^{T-i+1}}}\}(\Phi)$（如 3.2 节所示）实际上是保证 y_i 结构合法性的证明，$y_i = g^{\alpha^2}$ 保证了 y_i 结构的正确性，注意到系统公钥 $y_T = g^{x_0^{2^T}} = g^{x_{i-1}^{2^{T-i+1}}}$，故 $y_T = g^{\alpha^{2^{T-i+1}}}$ 与 $y_i = g^{\alpha^2}$ 的同时成立保证了 y_i 进化的正确性。

4.4 前向安全数字签名的验证算法

设验证者得到一个 $i(1 \leqslant i \leqslant T)$ 时段对信息 m 的前向安全数字签名为

$$< i, \{\sigma, \varsigma\}, y_i, \ PK\{\alpha : y_i = g^{\alpha^2} \wedge y_T = g^{\alpha^{2^{T-i+1}}}\}(\Phi) >$$

验证者首先验证零知识证明 $PK\{\alpha : y_i = g^{\alpha^2} \wedge y_T = g^{\alpha^{2^{T-i+1}}}\}(\Phi)$ 的正确性，若错误则输出失败信息；若正确则继续验证与 i 时间段公钥 y_i 对应的秘密钥 $\{x_i\}$ 对 m 的数字签名 $\{\sigma, \varsigma\}$ 的正确性，验证算法 $VF(m, \{\sigma, \varsigma\}, y_i)$ 如下：若 $\sigma = H(m \| g \| y_i \| g^{\varsigma} y_i^{\sigma})$ 成立，则签名正确，令 $VF(m, \{\sigma, \varsigma\}, y_i) = 1$，验证者接受信息 m 在 i 时间段的签名 $\{\sigma, \varsigma\} \in \{0,1\}^l \times Z_N$，验证结束；否则令 $VF(m, \{\sigma, \varsigma\}, y_i) = 0$，输出验证失败信息。

5 基于零知识证明的前向安全数字签名方案的安全性

上述的基于零知识证明的前向安全数字签名方案中，系统的安全性假设包括三个方面：1) 在系统建立时涉及到大合数素数分解的困难性，这一点完全与 RSA 的安全性假设一致，目前取 N 为 1024bit 是基本安全的；2) 在系统建立时涉及到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众多密码系统采用的安全性假设；3) 在秘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。在以上三个基本安全假设下，所提的方案显然是前向安全的。在数字签名的过程中使用了离散对数的根相等的零知识证明，该证明在随机 oracle 模型下是安全的。故上述方案在随机 oracle 模型下是前向安全的。

6 结束语

信息系统的安全不仅仅是一个技术的安全，而且涉及到系统的安全管理过程，它应该是一个动态的过程。数字签名的安全也是这样，因此在数字签名方案设计之初，应考虑到安全风险的控制与规避，前向安全数字签名正是考虑到了签名密钥在运行过程中泄漏时，如何减少损失，使对手即使在盗得系统签名秘密钥的情况下，也不能伪造以前时段的数字签名，因此可以说，前向安全数字签名是信息安全的风险控制的措施之一，也将成为数字签名的一个重要的研究方面。

参考文献：

[1] BELLARE M, MINER S. A forward-secure digital signature scheme[A]. Advances in Cryptology-CRYPTO'99, Lecture Notes in Compute Science[C]. Spring-Verlag, 1999.431-448.

[2] RIVEST R, SHAMIR A, ADLMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of ACM , 1978, 21(2):120-126.

[3] POINCTCHEVAL D, STERN J. Security proof for signature schemes[A]. Advances in Cryptology-EUROCRYPTO'96, Lecture Notes in Compute Science Vol.1070[C]. Spring-Verlag, 1996. 387-398.

[4] GOLDWASSER S, MICLIS. Probabilistic encryption[J]. Journal of computer and system, 1984, 28(2):270-299.

[5] BELLARE M, ROGAAWAY P. Random oracles are practical: a paradigm for designing efficient protocols[A]. Proceedings of the First Annual Conference on Computer and Communications Security[C]. 1993.1-20.

[6] BELLARE M, ROGAAWAY P. The exact security of digital signatures: How to sign with RSA and Rabin[A]. Advances in Cryptology-EUROCRYPTO'96, Lecture Notes in Compute Science[C]. Spring-Verlag, 1996. 399-416.

[7] CAMENISCH J, STADLER M. Efficient group signatures schemes for large groups[A]. Advances in Cryptology-CRYPT'97, Lecture Notes in Compute Science[C]. Berlin: Springer-Verlag, 1997.410-423.

[8] POINCTCHEVAL D, STERN J. Security arguments for digital signatures[J]. Journal of Cryptology, 2000, 113(3):361-396.