ISSN 1000-9825 Journal of Software 软件学报 2000,11(10):1333~1337

新型 Rabin 签名方案*

邱卫东 陈克非 白英彩

(上海交通大学计算机科学与工程系 上海 200030)

E-mail: qiuwd@netway.net.cn

摘要 提出一种基于二次剩余问题的新型 Rabin 签名方案.该方案对明文空间几乎没有限制,可能抵抗选择密文攻击,其描述也更为简单,同时还具有更高的实现效率,在签名检验时仅需作一次模乘运算.

关键词 二次剩余,数字签名,Rabin 签名,选择密文攻击.

中图法分类号 TP309

数字签名是人工手动签名的一种电子模拟,自从 1976 年 Diffie 和 Hellman[1]提出数字签名这一概念以后,引起了人们的极大关注,各种数字签名方案也纷纷被提了出来.人们更感兴趣的是可否利用数字签名来解决实际系统中的安全问题,RSA 签名方案[2]的提出证实了数字签名方案在实际中应用的可能性.人们期望数字签名的出现能给我们的系统带来更好的安全解决方案.

Rabin 签名方案[3]是众多数字签名方案中的一种,其安全性是基于求模合数 n 的平方根问题的困难性.Rabin 签名方案由于检验时只需要做一次模乘运算,因此具有很高的检验效率.由 Rabin 签名方案又引出了其他几种数字签名方案,例如,文献[4~6]中的签名方案.

本文提出一种新型的 Rabin 签名方案.该方案更易于描述,并且具有更高的实现效率,同时也比 Rabin 签名方案更安全、更完善.

1 二次剩余

假定 n 为整数,$Z_n^*=\{k\in Z_n|(k,n)=1\}$ 为模 n 的一个乘法群.设 $a\in Z_n^*$,若存在 $x\in Z_n^*$,使得 $x^2\equiv a \bmod n$,则称 a 是模 n 的二次剩余,否则,称 a 为模 n 的二次非剩余.我们用 Q_n 表示模 n 的二次剩余集合,$\overline{Q}_n$ 为模 n 的二次非剩余集合.

设 p 为一奇素数,a 为 Z_p^* 的生成元,对于 $a\in Z_p^*$,可表示为 $a=a^i \bmod p$,当且仅当 i 为偶数时,a 为模 p 的二次剩余.由此有 $|Q_p|=(p-1)/2$,$|\overline{Q}_p|=(p-1)/2$,即 Z_p^* 中一半元素为二次剩余,另一半元素为二次非剩余.

若 p 为一奇素数,a 为一整数,勒让德符号(Legendre symbol)$\left(\frac{a}{p}\right)$ 定义为

$$\left(\frac{a}{p}\right)=\begin{cases}0, & \text{若 } p|a\\ 1, & \text{若 } a\in Q_p\\ -1, & \text{若 } a\in\overline{Q}_p\end{cases}$$

假定 $a,b\in Z$,勒让德符号有以下性质:

- $\left(\frac{a}{p}\right)\equiv a^{(p-1)/2} \bmod p$.

---

* 本文研究得到国家自然科学基金(Nos. 69773013,69973031)和国家 863 高科技项目基金(No. 863-511-030-007 10)资助.作者邱卫东,1973 年生,博士生,主要研究领域为网络安全,电子商务,应用密码学.陈克非,1959 年生,教授,博士生导师,主要研究领域为信息安全,密码学,电子商务.白英彩,1936 年生,教授,博士生导师,主要研究领域为计算机网络,分布式系统,网络安全.

本文通讯联系人:邱卫东,上海 200030,上海交通大学 A9803023 班

本文 2000-05-31 收到原稿,2000-06-30 收到修改稿

• $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$.

• 若 $a\equiv b(\mathrm{mod}\ p)$,则 $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

• $\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$.

• 若 q 为不同于 p 的奇素数,则有 $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)^{(-1)^{(p-1)(q-1)/4}}$.

若 n 为两个互不相同的奇素数的乘积,$n=pq$,当且仅当 $a\in Q_p$ 且 $a\in Q_q$ 时,$a\in Z_n^*$ 为模 n 的二次剩余,并且有 $|Q_n|=|Q_p|\cdot|Q_q|=(p-1)(q-1)/4$,$|\overline{Q}_n|=3(p-1)(q-1)/4$.

雅可比符号(Jacobi symbol)为勒让德符号的合数模的一般化表示,定义在任意整数 a 和奇整数 n 上.若 $n\geqslant 3$ 为一个奇整数且有素数分解 $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$,则雅可比符号 $\left(\frac{a}{n}\right)$ 定义为

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\cdots\left(\frac{a}{p_k}\right)^{e_k}.$$

同时,我们定义 $J_n=\left\{a\in Z_n^*\ \middle|\ \left(\frac{a}{n}\right)=1\right\}$,用 $\tilde{Q}_n=J_n-Q_n$ 表示模 n 的伪平方根集合.

由文献[5]我们可知如下事实:

(1) 若知道 n 的素数分解,则:

• 存在算法,使得计算雅可比、勒让德符号需要 $O((\log n)^2)$ 比特位操作的运算时间.

• 存在算法,使得找到模素数 p 的平方根需要 $O((\log p)^3)$ 的比特位运算时间.

• 已知 $n=pq$ 的素数分解,存在算法,找到模 n 的平方根需要 $O((\log n)^3)$ 的比特位运算时间.

(2) 若 n 为一合数,且 n 的分解未知,则:

• 除了猜测以外,没有更有效的算法来判断 $a\in J_n$ 是否为模 n 的二次剩余(QRP).

• 求解 QRP 被公认为与整数分解具有相同的困难性.

• 计算 $a\in Q_n$ 的模 $n=pq$ 的平方根与整数分解具有相同的困难性.

BLUM 整数:若 p 和 q 均为模 4 之下与 3 同余的素数,则称 $n=pq$ 为 Blum 整数.

定理 1. $n=pq$,p 和 q 为互不相同的奇素数,若 $(x,n)=1$,则 $x^{(p-1)(q-2)/2}\equiv 1 \bmod n$.

证明:由费尔马小定理和 $(x,p)=1$,我们有 $x^{(p-1)}\equiv 1 \bmod p$,由此可推出 $p\mid(x^{p-1}-1)\mid(x^{\lambda(n)}-1)$,其中 $\lambda(n)=lcm(p-1,q-1)$ 为 $p-1$ 和 $q-1$ 的最小公倍数.同理,我们有 $q\mid(x^{q-1}-1)\mid(x^{\lambda(n)}-1)$.又因为 $(p,q)=1$,我们得到 $pq\mid(x^{\lambda(n)}-1)\mid(x^{(p-1)(q-1)/2}-1)$,即 $x^{(p-1)(q-1)/2}\equiv 1 \bmod n$. □

定理 2. 若 $x\in Q_n$,$n=pq$ 为一个 Blum 整数,则 $x^{(n-p-q+5)/8} \bmod n$ 为 x 模 n 的平方根.

证明:由于 n 为 Blum 整数,p 和 q 模 4 之下与 3 同余,即有 $p=4x_1+3$,$q=4x_2+3$,显然,$8\mid(n-p-q+5)$.另外,由于 $x\in Q_n$,因此存在整数 $y\in Z_n^*$,使得 $y^2\equiv x \bmod n$.由定理 1 可知

$$(x^{(n-p-q+5)/8})^2\equiv(y^2)^{((p-1)(q-1)+1)/4}\equiv y^{(p-1)(q-1)/2}\cdot y^2\equiv x \bmod n.$$ □

定理 3. 若 $x\in J_n$,$n=pq$ 为一个 Blum 整数,则有

$$x^{2d}\equiv\begin{cases}x, & \text{若 } x\in Q_n\\ n-x, & \text{若 } x\in\tilde{Q}_n\end{cases},$$

其中 $d=(n-p-q+5)/8$.

证明:由定理 2 的证明已经得到,当 $x\in Q_n$ 时,$(x^{(n-p-q+5)/8})^2\equiv x \bmod n$,即 $x^{2d}\equiv x \bmod n$.我们考虑 $x\in\tilde{Q}_n$ 的情况,由 $\tilde{Q}_n$ 的定义可知 $\left(\frac{x}{n}\right)=\left(\frac{x}{p}\right)\left(\frac{x}{q}\right)=1$.另外,当且仅当 $x\in Q_p$ 和 $x\in Q_q$ 时有 $x\in Q_n$.因此,由 $x\in\tilde{Q}_n$ 时可得 $\left(\frac{x}{p}\right)=-1$,$\left(\frac{x}{q}\right)=-1$.

另外,由于 n 为 Blum 整数,$p=4x_1+3$,$q=4x_2+3$,有 $\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}=(-1)^{2x_1+1}=-1$,$\left(\frac{-1}{q}\right)=(-1)^{(q-1)/2}=(-1)^{2x_2+1}=-1$.由此可得 $\left(\frac{-x}{p}\right)=\left(\frac{-x}{q}\right)=1$,即有 $n-x$(或 $-x$)$\in Q_n$,因此,$x^{2d}\equiv(n-x)^{2d}\equiv$

$(n-x) \bmod n$. □

定理 4. 若 $n=pq$,其中 $p\equiv 3 \bmod 8$,$q\equiv 7 \bmod 8$(这样的整数也称为 Williams 整数),则 2 为模 n 的二次非剩余,且雅可比符号 $\left(\frac{2}{n}\right)=-1$. 因此,任何整数 x 乘以 2 或 2^{-1} 都将改变 x 的雅可比符号值.

证明:由于 $p=8x_1+3$,$q=8x_2+7$,根据雅可比符号的性质有 $\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}=-1$,$\left(\frac{2}{q}\right)=(-1)^{(q^2-1)/8}=1$,由此可得 $\left(\frac{2}{n}\right)=\left(\frac{2}{p}\right)\left(\frac{2}{q}\right)=-1$,$\left(\frac{2^{-1}}{n}\right)=\left(\frac{2}{n}\right)^{-1}=-1$. 因此,$\left(\frac{2x}{n}\right)=\left(\frac{2}{n}\right)\left(\frac{x}{n}\right)=-\left(\frac{x}{n}\right)$,$\left(\frac{2^{-1}x}{n}\right)=\left(\frac{2^{-1}}{n}\right)\left(\frac{x}{n}\right)=-\left(\frac{x}{n}\right)$. □

2 新型 Rabin 签名方案

本节我们将提出一种基于二次剩余的数字签名方案. 该方案在 Rabin 签名方案的基础上改造而成,具有简单、安全和更加完善的特性. 方案中 $n=pq$ 为一个 Williams 整数,p 和 q 大小相近,系统的公、私钥分别为 n 和 (p,q).

2.1 新的签名方案之一(NSS1)

(1) 签名的产生:假设 Alice 要给 Bob 的消息 $m\in Z_n$ 签名,签名过程如下:

• 首先测试是否 (m,n) 等于 1,若不为 1 则需重新修改消息 m 的值,否则可能泄漏素数 p 和 q 的值. 事实上,(m,n) 不为 1 的概率是 $\frac{1}{p}+\frac{1}{q}-\frac{1}{n}$,在 n 很大时可以忽略不计;

• 若 $\left(\frac{m}{n}\right)=1$,选择 $a=0$,$\left(\frac{m}{n}\right)=-1$,选择 $a=1$. 这样选择的 a 使得 $2^{-a}m \bmod n\in J_n$,同时选择 $b=0$,当 $2^{-a}m\in Q_n$ 时,$b=1$,若 $2^{-a}m\in\tilde{Q}_n$;

• 计算 $s\equiv(2^{-a}m)^d \bmod n$,其中 $d=(n-p-q+5)/8$;

• 将消息 m 和签名 (s,a,b) 一起发送给 Bob.

(2) 签名检验:Bob 收到 (m,s,a,b) 后,计算等式 $s^2(-1)^b2^a\equiv m \bmod n$ 是否成立,若等式成立,Bob 将接受签名.

定理 5. 对每一个可用的 $m\in Z_n$ 的消息,签名方案中的签名者总能计算出它的签名 (s,a,b).

证明:对于可签名消息 $m\in Z_n$,由于 $(m,n)=1$,则 $\left(\frac{m}{n}\right)\neq 0$,即 $\left(\frac{m}{n}\right)=1$ 或 $\left(\frac{m}{n}\right)=-1$. 由于 n 为 Williams 整数,由定理 4 可知,2 为模 n 的二次非剩余,即 $\left(\frac{2}{n}\right)=-1$. 在签名过程中已知,当 $\left(\frac{m}{n}\right)=1$ 时,$a=0$;当 $\left(\frac{m}{n}\right)=-1$ 时,$a=1$,因此 $\left(\frac{2^{-a}m}{n}\right)=1$. 另外,显然 $(2^{-a}m,n)=1$,由此即有 $2^{-a}m \bmod n\in J_n$. 之后,签名者根据 $2^{-a}m$ 是否为二次剩余来决定 b 是 0 还是 1. 最后,签名者用私钥 d 计算 (s,a,b),$s\equiv(2^{-a}m)^d \bmod n$. □

定理 6. 若签名者和检验签名者按上述过程完成签名协议,检验者可以确信签名的正确性.

证明:若 (m,s,a,b) 为消息 m 的正确签名,则有 $2^{-a}m \bmod n\in J_n$. 由于 n 为 Williams 整数,由定理 3 可知,

$$(2^{-a}m)^{2d}\equiv\begin{cases}2^{-a}m, & \text{若 } 2^{-a}m\in Q_n\\ n-2^{-a}m, & \text{若 } 2^{-a}m\in\tilde{Q}_n\end{cases},$$

即有 $s^2\equiv(-1)^b2^{-a}m \bmod n$. 因此,$s^2(-1)^b2^a\equiv m \bmod n$. □

2.2 新的签名方案之二(NSS2)

众所周知,Rabin 方案对于选择明文攻击是安全的,而对选择密文攻击则完全不安全. 我们在上述新的签名方案中加入一个哈希函数就可以克服这一弱点.

我们让 $h(x)$ 表示安全的单向哈希函数,Alice 对消息 $m\in Z_n$ 进行签名后发送给 Bob. 首先,Alice 计算哈希函数 $h(m)$,然后利用第 2.1 节提出的新的签名方案 NSS1 对 $h(m)$ 进行签名. 签名的结果是 (s,a,b),其中 $a\in\{0,1\}$,正如前面已经说明的,a 的选择使得 $2^{-a}m \bmod n\in J_n$.

$$b=\begin{cases}0, & 2^{-a}h(m)\in Q_n\\ 1, & 2^{-a}h(m)\in \bar{Q}_n\end{cases},$$

$$s\equiv(2^{-a}h(m))^d \bmod n,\ d=(n-p-q+5)/8.$$

检验等式 $s^2(-1)^b2^a\equiv h(m) \bmod n$ 即可判断签名是否正确.

2.3 新的签名方案的安全性分析

当 n 为一个大的合数且分解未知时,计算模 n 的平方根的困难性相当于整数分解[5].本文提出的签名方案的安全性是基于计算模合数 n 平方根的困难性,因此,其安全性分析与 Rabin 方案[3]中的类似.

Rabin 公钥签名方案类似于 RSA 算法,但它的公开指数为 $e=2$,因此,与 RSA 相比,其安全性相同,而签名的检验更为简单.而 Rabin 签名方案对于选择密文攻击完全不安全.同时,Rabin 签名方案还要求签名空间限制在 Q_n 上,因此,消息不能是固定长度的任意比特串,而必须是模 n 的平方根.

本文提出的签名方案首先解决了签名空间问题,任意消息 m(除了 $(m,n)\neq 1$,而这种概率是非常小的,如前所述)均能用本文提出的方案进行签名,而仅仅比 Rabin 方案增加了 a 和 b 两个比特的因子.而且由于 b 是可以由签名验证者算出来的,因此,在协议进行的过程中可以不必传给签名接收方.

另外,新的签名方案之二(NSS2)对于选择密文攻击是安全的.对 Rabin 签名的选择密文攻击可以描述如下:攻击者首先随机选取整数 $x\in Z_n$,并且计算 $m=x^2 \bmod n$;如果攻击者能够成功地骗取签名者对 m 进行签名,他将能够以 1/2 的概率从签名 s 和 x 中破解 n 的分解.因为签名者不知道 x,所以对 m 的签名 s 若不同于 x,即 $s\neq\pm x \bmod n$,则可从 $\gcd(x\ \ s,n)$ 得到 n 的素数因子.

上面的攻击方法对于 NSS2 来讲无法成立,因为即使攻击者能够骗取签名者对消息 m 进行签名,除非他知道 n 的素数分解或者能求解哈希函数的逆,否则,他也无法同时知道 m 的平方根 $\sqrt{m}$ 和 $h^{-1}(m)$.

下面,我们来分析其他几种可能的攻击手段:

· 给定 x 和 $s\equiv x^2 \bmod n$,寻找 m 使得 $h(m)=s$.这相当于求哈希函数的逆,在计算上是不可行的.

· 给定 m 及其哈希函数值 $y=h(m)$(相当于一个随机数),要找出签名 s(即求 $2^{-c}y$ 的平方根)相当于二次剩余问题.

· 在没有其他信息的情况下,要找到 (x,y,z) 使得 $x^2\equiv y \bmod n$,$y=h(z)$ 在计算上是不可行的.我们知道,y 是由 z 唯一决定的,确定 x,得到 y 要找 z 使得 $y=h(z)$ 相当于求安全哈希函数的逆;若先确定 z,得到 y 求 x 则相当于二次剩余问题.

· 给定 (x_0,y_0,z_0),$x_0^2\equiv y_0 \bmod n$,$y_0=h(z_0)$,构造 (x,y,z) 使得 $x^2\equiv y \bmod n$,$y=h(z)$ 也成立.一种可能的攻击是找到 $z\neq z_0$,但 $x=x_0$,$y=y_0$,若 $h(x)$ 为安全哈希函数,这种攻击在计算上是不可行的;另一种攻击方法是找到 $x^2\equiv x_0^2\equiv y \bmod n$ 且 $x\neq x_0 \bmod n$,这意味着 $x+x_0$ 和 $x-x_0$ 其中的一个为 n 的素数因子,这样一来就相当于分解了合数 n,显然这是不成立的.

· 除了上述攻击以外,没有其他办法能够找出正确的 (x,y,z) 对.因此,我们说新的签名方案 NSS2 是安全的.

3 结束语

我们针对 Rabin 签名方案的不足,对其进行了改进和完善.改进的方案首先解决了可签名消息空间的问题,即不论消息是否为二次剩余均可签名,这样就使签名方案更为实用.另外,改进后的签名方案还能克服 Rabin 方案中可能受到选择密文攻击的弱点,使得签名系统在安全性上有很大的提高.

参考文献

1 Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Informations Theory, 1976,22(6):644~654

2 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978.21(2):120~127

3 Rabin M O. Digitalized signatures and public key functions as intractable as factorization. Technical Report, MIT/LCS/

TR-212, MIT Laboratory for Computer Science, 1979
4 Chen K. Authenticated encryption scheme based on quadratic residue. Electronics Letters, 1998,34(22):2115~2116
5 Menezes A J, Oorschot van P, Vanstone S A. Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, 1997
6 Nyang D, Song J. Fast digital signature scheme based on the quadratic residue problem. Electronics Letters, 1997,33(3): 205~206

A New Rabin Signature Scheme

QIU Wei-dong CHEN Ke-fei BAI Ying-cai

(*Department of Computer Science and Engineering Shanghai Jiaotong University Shanghai* 200030)

Abstract In this paper, a modified Rabin signature scheme is presented based on quadratic residue problem. The main advantage of the modified scheme is simpler to describe and more efficient to implement, there is no limitation or plain test space, especially only one modular multiplication is required for verification, and it is secure against chosen-ciphertext attack.

Key words Quadratic residue, digital signature, Rabin signature, chosen-ciphertext attack.