第35卷 第12期 计 算 机 工 程 2009年6月
Vol.35 No.12 Computer Engineering June 2009
·安全技术· 文章编号：1000—3428(2009)12—0103—03 文献标识码：A 中图分类号：TN918.1

一种高效的RSA签名算法

赵耀东，威文峰
（郑州信息工程大学信息工程学院应用数学系，郑州 450002）

摘 要： RSA密码算法是一种广泛应用的公开密钥密码算法。运行该密码算法需要大量的计算资源和存储资源。提出一种快速安全的RSA签名算法以适应计算资源受限的情形。该RSA签名算法基于中国剩余定理，采用较短的私人密钥。分析RSA密码算法的安全性，证明RSA密码算法可以抵抗格攻击。

关键词： RSA算法；格攻击；数字签名

RSA Signature Algorithm with High Efficiency

ZHAO Yao-dong, QI Wen-feng
(Department of Applied Mathematics, School of Information Engineering, Zhengzhou Information Engineering University, Zhengzhou 450002)

【Abstract】 RSA is widely used in public-key cryptosystem. But running this algorithm needs lots of time and memory. This paper proposes a RSA signature algorithm to fit for the devices with low computational power. The new signature algorithm is based on the Chinese Remainder Theorem which has a relative short private key. This paper gives the cryptoanalysis of this algorithm. Results show that the algorithm can resist the lattice attack.

【Key words】 RSA algorithm; lattice attack; digital signature

1 概述

RSA密码算法是一种广泛应用的公开密钥密码算法，它不仅可以用来加密，而且还可以用来进行数字签名[1]。设$N=p\cdot q$为RSA算法的公共模数，e为其公开密钥，d为私人密钥，e, d满足$e\cdot d=1 \bmod (p-1)(q-1)$，其中，$p, q$为一个$n/2$ bit的大素数($n\geqslant 1\ 024$)。若要签名(加密)的消息为m，则签名(加密)后的消息为$m_c=m^e \bmod N$，验证签名(解密消息)则计算$m=m_c{}^d \bmod N$。由于计算模正整数方幂需要耗费大量的计算时间，因此制约了RSA密码算法的执行效率。由此限制了其应用于计算资源有限又需要快速运行算法的环境中，如：保密移动通信设备，Smart卡等。如何加速RSA密码算法并使其占用尽可能少的计算资源(例如存储资源)一直是密码学界研究的热点问题。

但是，1990年M. J. Wiener应用连分数算法证明[2]：当RSA算法中的私钥$d<N^{0.25}$时，可以在多项式时间内恢复出私钥d，而不需要分解模数N，从而说明了使用过短的私人密钥会严重威胁RSA算法的安全性。1999年，D. Boneh和G. Durfee改进了Wiener的结果[3]，证明了当私钥$d<N^{0.292}$时，可以在多项式时间内分解模数N。目前，Boneh–Durfee方法以及由此引出的一系列攻击算法是针对小指数RSA攻击的最有效的攻击算法[4-6]，每一种RSA小指数变形体制均要经受这些攻击算法。

1982年，J. J. Quisquater和C. Couvreur提出了使用中国剩余定理加速RSA解密或者签名的速度[7]。这种RSA算法称之为RSA–CRT。2000年，新加坡学者Guopei Qiao和Kwok-Yan Lam提出了一种面向Smart卡应用的RSA签名算法[8]。该算法在使用中国剩余定理的前提下使用了较短的私钥以期达到加速签名的目的。但是，在2006年的亚密会上[9]，荷兰学者Ellen Jochemsz和德国学者Alexander May攻破了该算法。

本文提出一种新的快速安全的RSA签名算法，该算法使用了较短的私钥，并且应用中国剩余定理加速签名的过程。为了证明所提出的RSA算法的安全性，本文给出针对这种签名算法的格攻击算法。结果表明，RSA算法能够抵抗现有的格攻击算法。

2 RSA-CRT和格攻击

设格L是由一组线性无关的向量$\boldsymbol{u}_1, \boldsymbol{u}_2,\cdots,\boldsymbol{u}_w$定义的，其中，$\boldsymbol{u}_1, \boldsymbol{u}_2,\cdots, \boldsymbol{u}_w\in Z^n$，$w\leqslant n$，则$L=\{\sum_{i=1}^{w}k_i\boldsymbol{u}_i \mid k_i\in Z\}$。设$\boldsymbol{u}^*_1, \boldsymbol{u}^*_2,\cdots, \boldsymbol{u}^*_w$为对$\boldsymbol{u}_1, \boldsymbol{u}_2,\cdots, \boldsymbol{u}_w$做Gram-Schmidt正交化后所得到的向量。定义格L的行列式为

$$\det(L)=\prod_{i=1}^{w}\|\boldsymbol{u}^*_i\|$$

其中，$\|\cdot\|$表示欧几里德范，即若向量$\boldsymbol{a}=(a_0, a_1,\cdots, a_{n-1})$，则

$$\|\boldsymbol{a}\|=\left(\sum_{i=0}^{n-1}a_i^2\right)^{1/2}$$

若$w=n$，则$\det(L)=|\det(\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_w)|$，此时称格$L$为满秩的。

引理1[10] 设L为向量集$\{\boldsymbol{u}_1, \boldsymbol{u}_2,\cdots, \boldsymbol{u}_w\}$所定义的格，$\{\boldsymbol{b}_1, \boldsymbol{b}_2,\cdots, \boldsymbol{b}_w\}$是对$\{\boldsymbol{u}_1, \boldsymbol{u}_2,\cdots, \boldsymbol{u}_w\}$应用LLL算法所得的向量集，则

$$\|\boldsymbol{b}_1\|\leqslant 2^{w/2}\det(L)^{1/w}$$
$$\|\boldsymbol{b}_2\|\leqslant 2^{w/2}\det(L)^{1/(w-1)}$$

设$h(x_1,x_2,\cdots,x_n)=\sum_{i_j}a_{i_1i_2\cdots i_n}x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}$为一个多变元多项

基金项目： 国家自然科学基金资助项目(60673081)；国家“863”计划基金资助项目(2006AA01Z417)
作者简介： 赵耀东(1979－)，男，博士研究生，主研方向：密码学；威文峰，教授、博士生导师
收稿日期： 2009-01-13 **E-mail：** zhaoyaodong_1979@yahoo.com.cn

式，定义多项式的范为$\| h(x_1,x_2,\cdots,x_n) \|=(\sum_{i_j} a_{i_1 i_2 \cdots i_n}{}^2)^{1/2}$。

引理 2[11] 设 $h(x_1,x_2,\cdots,x_n)=\sum_{i_j} a_{i_1 i_2 \cdots i_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$ 为一个多变元多项式，$a_{i_1,i_2,\cdots,i_n} \in Z$。$h(x_1,x_2,\cdots,x_n)$ 由 w 个单项式相加而成。若：

(1)存在 $x_1^{(0)},x_2^{(0)},\cdots,x_n^{(0)} \in Z$ 满足 $h(x_1^{(0)},x_2^{(0)},\cdots,x_n^{(0)})=0 \bmod e^m$，其中，$x_1^{(0)}<X_1$，$x_2^{(0)}<X_2,\cdots$，$x_n^{(0)}<X_n$，$X_i \in Z$，$i=1,2,\cdots,n$；

(2)$\| h(x_1X_1, x_2X_2,\cdots, x_nX_n)\|<e^m/(w^{1/2})$。

则 $h(x_1,x_2,\cdots,x_n)=0$。

引理 2 说明了如果一个多项式存在小解使得引理中的条件(2)成立，则可将求解模多项式的小解问题转化为求解整数环上多项式的小解问题。

3 RSA-CRT签名算法

由于面向计算资源受限的计算环境的应用，因此 RSA 算法的设计必须从计算复杂性和存储复杂性 2 个方面进行考虑。从计算复杂性方面考虑，RSA 算法应该重点考虑签名速度。从而应用了较短的私钥 d_p, d_q。从存储复杂性方面考虑，应该存储尽可能少的密钥比特。从而令 2 个私钥 d_p, d_q 具有一定的关系。现描述新的签名算法如下：

(1)随机生成 2 个 n/2 bit 的素数 $p=2p_1+1$ 和 $q=2q_1+1$，且$(p_1, q_1)=1$。计算 $N=p \cdot q$。

(2)随机生成 n_p bit 正整数 d_p，$n_p \leqslant n/2$，且$(d_p, p-1)=1$。

(3)计算 $d_q=2^r d_p+1$。

(4)计算 $d_0=(d_p-d_q)p_1^{-1} \bmod q_1$。

(5)计算 $d=d_p+d_0p_1$。

(6)计算 $e=d^{-1} \bmod (p-1)(q-1)$。

现在问题在于如何选取适当的参数使得这种 RSA 算法既能够快速的运行，又能够保证其安全性。一般来说，为了抵御数域筛法的攻击，n 一般取成 1 024 bit。其他参数的选取原则在于能够抵抗现有所有的攻击算法的前提下，尽可能地优化其运行的效率。于是需要找出能够保证这种 RSA 安全性的 n_p 和 r 的最优值。

4 安全性分析

本节将给出针对这种 RSA–CRT 签名算法的 2 种攻击方法用来评估所提出的签名算法的安全性。

4.1 攻击算法 1

由密钥生成算法可知：

$$ed_q \equiv 1 \bmod (q-1)$$

从而存在整数 l，使得：

$$e(2^r d_p+1)=l(q-1)+1$$

两边同时乘以 p 并且模 $2^r e$ 得到：

$$(e-2)p-(l+1)(N-p)+N \equiv 0 \bmod 2^r e$$

从而恢复密钥 p 只需要求同余方程

$$f(x,y) \equiv (e-2)y+x(N-y)+N \equiv 0 \bmod 2^r e$$

的小解$(x_0, y_0)=(-l-1, p)$即可。

由于$|x_0|=(e(2^r d_p+1)-1)/(q-1)<e2^{r+2}d_p/q$，省去小常量可得$|x_0|<N^{1/2+\gamma+\delta}$。于是 x_0, y_0 分别有上界 X, Y 满足：

$$|x_0|<X=N^{1/2+\gamma+\delta}, |y_0|<Y=N^{1/2}$$

为了得到更好的攻击效果，在求解该方程时将增加一个变量 z，其对应的解为 q。并令 $Z=N^{0.5}$，从而在不考虑一些小常量的情况下，有$|z|<Z$，且 $yz=N$。

注 增加变量 z 的目的在于：利用 $yz=N$ 的性质来减少后面所构造格的行列式，从而达到增强攻击效果的目的。

构造如下的多项式集：

$g_{ij}(x, y, z)=(2^r e)^{m-i}x^j z^s f^i(x, y)$，$i=0,1,\cdots,m$；$j=0,1,\cdots,m-i$。

$h_{ij}(x, y, z)=(2^r e)^{m-i}y^j z^s f^i(x, y)$，$i=0,1,\cdots,m$；$j=1,2,\cdots,m-i$。

其中，$m, s \in Z^+$是事先选定的 2 个参数，并且 $s<m$。

现在的目标是寻找 2 个多项式 $h_1(x, y, z)$和 $h_2(x, y, z)$来满足引理 2 的条件。

显然，所构造的多项式集中元素的所有线性组合 $h(x, y, z)$ 均满足：

$$h(x_0, y_0, z_0) \equiv 0 \bmod (2^r e)^m$$

即引理 2 中的第 1 个条件得到满足，其中，$x_0=-l-1$，$y_0=p$，$z_0=q$。从而需要在这些多项式中寻找满足引理 2 中第 2 个条件的多项式。

寻找这些多项式需要用到 L^3 算法。将 $\boldsymbol{g}_{ij}(xX, yY, zZ)$，$i=0,1,\cdots,m$，$j=0,1,\cdots,m-i$ 和 $\boldsymbol{h}_{ij}(xX, yY, zZ)$，$i=0,1,\cdots,m$，$j=1,2,\cdots,m-i$ 相应的系数做成向量，记这些向量所定义的格为 L。对这组向量应用 L^3 算法，则可以得到范较小的多项式，若 L^3 算法输出的前 2 个向量为 $\boldsymbol{h}_1$，$\boldsymbol{h}_2$，并设 $\boldsymbol{h}_1$，$\boldsymbol{h}_2$ 所对应的多项式为 $\boldsymbol{h}_1(xX, yY, zZ)$和 $\boldsymbol{h}_2(xX, yY, zZ)$,则由引理 1 可得：

$$\| \boldsymbol{h}_1(xX, yY, zZ) \| \leqslant \| \boldsymbol{h}_2(xX, yY, zZ) \| < 2^{w/2}\det(L)^{1/(w-1)}$$

其中，w 为 L 的维数；$\det(L)$为格 L 的行列式。

若 $\det(L)$满足：

$$2^{w/2}\det(L)^{1/(w-1)} < (2^r e)^m/(w^{1/2})$$

则可得 $\boldsymbol{h}_1(x, y, z)$和 $\boldsymbol{h}_2(x, y, z)$即为需要的多项式。因为 $w^{1/2}$，$2^{w/2}$ 相对于 $\det(L)$和$(2^r e)^m$ 非常微小，所以在计算中可以不考虑它们。

由此得到结论，若：

$$\det(L) < (2^r e)^{m(w-1)}$$

则可以找到 2 个多项式 $\boldsymbol{h}_1(x, y, z)$和 $\boldsymbol{h}_2(x, y, z)$满足引理 2 中第 2 条件，故 $\boldsymbol{h}_1(x, y, z)$和 $\boldsymbol{h}_2(x, y, z)$满足引理 2 中所有的条件。所以

$$\boldsymbol{h}_1(x_0, y_0, z_0)=\boldsymbol{h}_2(x_0, y_0, z_0)=0$$

从而，通过结式消元可以求解得到 p。

要得到使得不等式 $\det(L)<(2^r e)^{m(w-1)}$成立的条件，需要计算 $\det(L)$和 w。

易验证：适当排列多项式集中的项，可以使得构成格的这组基对应的矩阵为下三角形矩阵。从而计算 $\det(L)$只需要计算对角线上的元素的值即可。

由于 $\boldsymbol{g}_{ij}(xX, yY, zZ)$出现在对角线上的元素为

当 $i \geqslant s$ 时，$(2^r e)^{m-i}X^{i+j}Y^{i-s}$；

当 $i<s$ 时，$(2^r e)^{m-i}X^{i+j}Z^{s-i}$。

从而多项式集$\{g_{ij}(x, y, z) \mid i=0,1,\cdots,m;\ j=0,1,\cdots,m-i\}$对于 $\det(L)$的贡献如下：

$(2^r e)$的个数为 $\sum_{i=0}^{m}\sum_{j=0}^{m-i}(m-i)=m(m+1)(m+2)/3$；

X 的个数为 $\sum_{i=0}^{m}\sum_{j=0}^{m-i}(i+j)=m(m+1)(m+2)/3$；

Y 的个数为 $\sum_{i=s}^{m}\sum_{j=0}^{m-i}(i-s)=(m-s)(m-s+1)(m-s+2)/6$；

Z 的个数为 $\sum_{i=0}^{s-1}\sum_{j=0}^{m-i}(s-i)=s(1+s)(4+3m-s)/6$。

多项式 $\boldsymbol{h}_{ij}(xX, yY, zZ)$出现在对角线上的元素为

当 $i+j \geqslant s$ 时，$(2^r e)^{m-i}X^i Y^{i+j-s}$；

当 $i+j<s$ 时，$(2^r e)^{m-i}X^i Z^{s-i-j}$。

从而多项式集 $\boldsymbol{h}_{ij}(xX, yY, zZ)$对于 $\det(L)$的贡献如下：

$(2^r e)$的个数为 $\sum_{i=0}^{m}\sum_{j=1}^{m-i}(m-i)=m(m+1)(2m+1)/6$；

X 的个数为 $\sum_{i=0}^{m}\sum_{j=1}^{m-i} i=m(m-1)(m+1)/6$；

Y 的个数为 $\sum_{i=0}^{m}\sum_{j=\max\{1,s-i\}}^{m-i}(i-s+j)=(-1+m-s)(m-s)(1+m-s)/3+(m-s)(1+m-s)(s+1)/2$；

Z 的个数为 $\sum_{i=0}^{s-1}\sum_{j=1}^{s-i-1}(s-i-j)=s(-1+s)(1+s)/6$。

设事先选定的 2 个参数 s, m 满足 $s=\sigma m$，于是可得：

$$\det(L)=((2^r e)^4 X^3 Y^{3(1-\sigma)^3+3(1-\sigma)^2\sigma} Z^{\sigma^2(3-\sigma)+\sigma^3})^{m^3(1+o(1))/6}$$

由 $w=(m+1)^2$ 可得，要使不等式 $\det(L)<(2^r e)^{m(w-1)}$成立，只需要：$3(1/2+\gamma+\delta)+(3(1-\sigma)^3+3(1-\sigma)^2\sigma)/2+(\sigma^2(3-\sigma)+\sigma^3)/2<6(1+\gamma)-4(1+\gamma)$。

即若 $\delta<1/6-\gamma/3-(1/2-\sigma+2\sigma^2-\sigma^3)$，则不等式 $\det(L)<(2^r e)^{m(w-1)}$成立，从而可在多项式时间内分解 N。

由于 $s<m$，因此 $0<\sigma<1$。在此范围内，$1/2-\sigma+2\sigma^2-\sigma^3$ 可取得最小值 0.351 8。于是，δ的界可以化简成：

$$\delta<-\gamma/3-0.185\ 1$$

由于δ的值恒为负，因此可以得到结论：攻击算法 1 对本 RSA-CRT 算法无效。

4.2 攻击算法 2

由密钥生成算法可知，存在整数 l, k 使得：

$$2^r e^2 d_p^2+(e^2-e-2^r e)d_p+e l d_p+2^r e k d_p+(e-1)k-l-(e-1)+(N-1)kl=0$$

从而恢复密钥 d_p 仅需要求解多元多项式：

$$f(x,y,z)=2^r e^2 x^2+(e^2-e-2^r e)x+exy+2^r exz+(e-1)z-y-(e-1)+(N-1)yz=0$$

的小解(d, l, k)即可。若 $d<N^{\delta}$, $r<\gamma m$，则有 $l<N^{1/2+\gamma+\delta}$, $k<N^{1/2+\delta}$。令 $X=N^{\delta}$, $Y=N^{1/2+\gamma+\delta}$, $Z=N^{1/2+\delta}$。

2006 年，Ellen Jochemsz 和 Alexander May 在亚密会上给出了如下的结果：

结论 1 设 $f(x,y,z)=a_0+a_1x+a_2x^2+a_3y+a_4z+a_5xy+a_6xz+a_7yz$ 在整数环上存在小解(x_0, y_0, z_0)并且$|x_0|<X$, $|y_0|<Y$, $|z_0|<Z$，并设$\|f(x, y, z)\|_{\infty}=\max\{a_i \mid i=0, 1, \cdots, 7\}$。若

$$X^{7+9\tau+3\tau^2}(YZ)^{5+9/2\tau}<W^{3+3\tau}$$

则可在多项式时间内求得(x_0, y_0, z_0)，其中，$W=\|f(xX, yY, zZ)\|_{\infty}$。

由结论 1 可得要求解方程只需满足：

$$(7+9\tau+3\tau^2)\delta+(1/2+\gamma+\delta)(9/2\tau+5)+(1/2\tau+\delta)(9/2\tau+5)<(\gamma+2+2\delta)(3+3\tau)$$

即

$$3\delta\tau^2+(12\delta+3/2\gamma-3/2)\tau+(11\delta+2\gamma-1)<0$$

取 $\tau=-(4\delta+1/2\gamma-1/2)/2\delta$，得：

$$3(4\delta+1/2\gamma-1/2)^2-6(4\delta+1/2\gamma-1/2)^2-6(4\delta+1/2\gamma-1/2)^2+4\delta(11\delta+2\gamma-1)<0$$

从而若

$$\delta<1/4(4-2\gamma-(13-10\gamma+\gamma^2)^{1/2})$$

则式(2)成立。

4.3 参数的选取和计算复杂度

显然 n_p 和 r 的选取必须使得上述的 2 个攻击算法无效，但是这还不够，因为攻击者还可以通过遍历 d_p 的高位比特来扩大可以攻击的 n_p 的界。为了抵抗这种攻击，通常会使所选取 n_p 的值超出上述 2 个攻击算法攻击范围 80 bit，以保证算法的安全性。从计算复杂性上考虑，增加 r 的值会延缓计算签名的速度，从而需要选取较小的 r。以 $n=1\ 024$ 为例，可以选取 $n_p=166$, $r=100$。这时$\gamma=0.098$。此时攻击算法 1 的攻击范围是−0.053；攻击算法 2 的攻击范围 0.084，换算成比特数是 86 bit。从而可以确保算法的安全性。

使用攻击算法 2 攻击 Guopei Qiao 和 Kwok-Yan Lam 给出的算法，其攻击范围是 101 bit，从而为了确保其安全性，其 n_p 至少应该为 181 bit，从而在采用相同比特数私钥的情况下，本文的算法要相对安全。

由于计算一次模平方大约相当于计算 0.75 次模乘法，从计算复杂性上分析，完成一次 Qiao–Lam 算法需要计算 $2\times(181\times0.75+w(d_p))=271.5+2w(d_p)$次模乘法，其中，$w(d_p)$表示将 d_p 表示成二进制后“1”的个数。完成一次本文所提出的算法需要计算 $2\times(166\times0.75+w(d_p))+100\times0.75=324+2w(d_p)$次模乘法，略高于 Qiao–Lam 算法。但是，相对于未采用中国剩余定理的普通小指数 RSA 算法，在由于要保证其安全性，私钥至少应该为 $0.292\times1\ 024+80>379$ bit。由于其模数为 1 024 bit，折算成模数为 512 bit 模乘法其计算复杂度至少 $4\times((0.292\times1\ 024+80)\times0.75+w(d))>1\ 137+4w(d)$，远远大于本文方案的计算复杂度。

参考文献

[1] Rivest R, Shamir A, Aldeman L. A Methoed for Obtaining Digital Signatures and Public-key Cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[2] Wiener M J. Cryptanalysis of Short RSA Secret Exponents[J]. IEEE Trans. on Information Theory, 1990, 36(1): 553-558.

[3] Boneh D, Durfee G. Cryptanalysis of RSA with Private Key d Less than N0.292[J]. IEEE Trans. on Information Theory, 2000, 46(4): 1339-1349.

[4] Blömer J, May A. Low Secret Exponent RSA Revisited[C]//Proc. of CALC'01. RI, USA: [s. n.], 2001: 110-125.

[5] May A. Cryptanalysis of Unbalanced RSA with Small CRT-exponent[C]//Proc. of CRYPTO'02. NY, USA: [s. n.], 2002: 242-256.

[6] Bleichenbacher D, May A. New Attack on RSA with Small Secret CRT-exponent[C]//Proc. of PKC'06. NY, USA: [s. n.], 2006: 1-13.

[7] Quisquater J J, Couvreur C. Fast Decipherment Algorithm for RSA Public Key Cryptosystem[J]. Electronic Letter, 1982, 18(1): 905-907.

[8] Qiao Guopei, Lam K Y. RSA Signature Algorithm for Microcontroller Implementation[C]//Proc. of CARDIS'00. NY, USA: [s. n.], 2000: 353-356.

[9] Jochemsz E, May A. A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants[EB/OL]. (2006-10-21). http://dblp.un.-trier.de/db/conf/asiacrypt.

[10] Lenstra A, Lenstra H, Lovasz L. Factoring Polynomials with Rational Coefficients[J]. Mathematiche Annalen, 1982, 261(1): 515-534.

[11] Howgrave-Graham N. Finding Small Roots of Univariate Modular Equations Revisited[C]//Proc. of Cryptography and Coding Conference. London, UK: [s. n.], 1997: 131-142.

编辑　索书志