私钥 p, q 共享低位比特 RSA 体制的小指数攻击

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

摘　要：本文研究了组成 RSA 模数的两个素数 p 和 q 其低位比特相同，RSA 公开密钥密码系统的安全性。其结果表明若 RSA 模数的两个素因子 p 和 q 共享低位比特，则当私钥 d 较小时这样的体制相对于模数不平衡的 RSA 更易受到攻击。本文的研究结果表明，当组成 RSA 模数的两个素数 p 和 q 仅有少量比特不相同时，使用规模较小的私钥 d 必须十分慎重。

关键词：RSA 密码系统；格攻击；共享低位比特
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2008)06-1453-04

The Attack on RSA with Small Private Key and Primes Sharing Least-Significant Bits

Zhao Yao-dong　　Qi Wen-feng
(*Department of Applied Mathematics*, *Zhengzhou Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: In this paper, the security of RSA system is studied if the private keys p and q share their least significant bits. The result shows that RSA system is more vulnerable in this condition when the private key d is small. So it should be careful to void this kind of weak key.

Key words: RSA cryptosystem; Lattice attack; Least-significant bits

1　引言

自 1978 年提出后，RSA 公钥密码体制一直被广泛的使用。但是，无论是用于加密解密还是用于数字签名，RSA 体制在实现上均存在着速度较低的问题，所以人们一直在寻找 RSA 变形体制，以期加速 RSA 体制的执行效率。最简单的方法是缩短 RSA 体制中的公钥 e 或者是私钥 d 的规模。缩短公钥 e 可以使得加密速度加快，而缩短私钥 d 可以使得签名速度加快。 但是，Wiener 使用连分数的方法证明了当私钥 d 满足 $d < N^{0.25}$ 时，可在多项式时间内由公钥 e 和 N 恢复出私钥 d[1]。1999 年，Boneh 和 Durfee 改进了 Wiener 的结果，将小指数攻击的上界提高到了 $N^{0.292}$。他们使用的方法就是格攻击[2]。他们的方法是基于 Coppersmith 求解模双变元多项式小解的方法[3−5]。 虽然，这种方法是一个启发式的方法，不能被严格的证明。但是在实际的攻击中，它总能成功。

在 1999 年的亚洲密码年会上，Sun，Yang 和 Laih[6]提出了 3 个 RSA 变形体制。他们试图通过使用不平衡的素数 p 和 q(即 p 和 q 的规模相差较大)，使得当使用较小的私钥 d 时，RSA 体制仍然安全。但是，在随后的 2000 年的亚洲密码年会上，Boneh 和 Durfee[7]对这 3 个体制中的两个进行了成功的攻击。他们使用的仍然是格攻击方法。

2001 年，Steinfeld 和 Zheng[8]提出了一种新的 RSA 变形体制。在该体制中组成模数 N 的素数其低位比特相同。设 RSA 密码系统中的模数 $N = pq$，其中 p，q 均为 $n/2$ 比特的素数，则 $|p-q| = r2^{(1/2-\alpha)n}$，$r$ 为一个 αn 比特的奇数，其中 $0 \le \alpha \le 1/2$。 Steinfeld 和 Zheng[9]给出了这种变形 RSA 体制的部分私钥泄漏攻击结果，并证明了当公钥 e 的规模较小时，这种 RSA 变形体制较一般的 RSA 体制更能抵抗部分私钥泄漏攻击。

本文从另一个方面讨论公钥 N 的素因子共享低位比特时的 RSA 变形体制。由于资源的限制，在使用 RSA 做签名时通常会使用较小的私钥 d。但是，通过分析发现当公钥 e 比较大，而私钥 d 比较小时，这种 RSA 变形体制会变得比 p，q 不平衡的 RSA 体制还不安全。需要指出的是，本文的结果适用于所有 $|p-q| = r2^{(1/2-\alpha)n}$，其中 $r = 2^{sn}$，$s \le \alpha$ 的情形。当 $\alpha = 1/2$，$s < 1/2$ 时，本文的结果包含在文献[10]的结果当中。但是， 当 $\alpha = s$ 时，文献[10]的方法并不适用。本文的方法适用于任意 s 的取值。

2　格和格攻击

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

2007-01-25 收到，2007-10-31 改回
国家自然科学基金(60673081)和国家 863 计划项目(2006AA01Z417)资助课题

表示欧几里德范，即若向量 $\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})$，则 $\|\boldsymbol{a}\|=\left(\sum_{i=0}^{n-1}a_i^2\right)^{1/2}$。

引理 1[11] 设线性无关的向量集$\{\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_n\}$为 LLL 算法的输入，LLL 算法的输出向量集为$\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\}$。则有

(1) $\|\boldsymbol{b}_i^*\|^2<2\|\boldsymbol{b}_{i+1}^*\|^2$；

(2)若 $\boldsymbol{b}_i=\boldsymbol{b}_i^*+\sum_{j=1}^{i-1}\mu_j\boldsymbol{b}_j^*$，则 $|\mu_j|<1/2,\ i=1,\cdots,n$。

注 1 若 L 为向量集$\{\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_n\}$所定义的格，则引理 1 中的向量集$\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\}$称为格 L 的 LLL 约化基。

引理 2[10] 设 L 为向量集$\{\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_n\}$所定义的格，$\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\}$ 是格 L 的 LLL 约化基，则 $\|\boldsymbol{b}_1\|\le 2^{w/2}\cdot\det(L)^{1/w}$；$\|\boldsymbol{b}_2\|\le 2^{w/2}\det(L)^{1/(w-1)}$。

1996 年 Coppersmith 提出了用于求解模多元多项式小解的方法[3−5]。该方法基于求 LLL 约化基的 LLL 算法。该算法随后由 Howgrave-Graham[12]简化。简化后的算法主要基于下面的引理。

设 $h(x,y,z)=\sum_{i,j,k}a_{i,j,k}x^iy^jz^k$ 为一个含 3 个变元的多项式，定义多项式的范为 $\|h(x,y,z)\|=\left(\sum_{i,j,k}a_{i,j,k}^2\right)^{1/2}$。

引理 3[12] 设 $h(x,y,z)=\sum_{i,j,k}a_{i,j,k}x^iy^jz^k$ 为一个 3 变元的多项式，$a_{ijk}\in\boldsymbol{Z}$。$h(x,\ y,\ z)$由 w 个单项式相加而成。若

(1)存在 $x_0,y_0,z_0\in\boldsymbol{Z}$ 满足 $h(x_0,y_0,z_0)=0 \bmod e^m$，其中 $|x_0|<X$，$|y_0|<Y$，$|z_0|<Z$；$X\in\boldsymbol{Z},Y\in\boldsymbol{Z},Z\in\boldsymbol{Z}$；

(2) $\|h(xX,yY,zZ)\|<e^m/(w^{1/2})$；

则 $h(x_0,y_0,z_0)=0$。

引理 3 说明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。

假设需要求解的模多项式为 $f(x,y,z)=0 \bmod e$，并且有 $g(y,z)=0$。构造如下的多项式集：$h_{u_1,u_2,u_3,v}(x,y,z)=e^{m-v}x^{u_1}y^{u_2}z^{u_3}f^v(x,y,z)$，其中 u_1,u_2,u_3,v 均为正整数。于是若存在 $x_0,y_0,z_0\in\boldsymbol{Z}$ 满足 $f(x_0,y_0,z_0)=0 \bmod e$，则有 $h_{u_1,u_2,u_3,v}(x_0,y_0,z_0)=0 \bmod e^m$。从而由多项式集 $h_{u_1,u_2,u_3,v}\ (x,y,z)$ 线性组合而来的多项式 $h(x,\ y,\ z)$均满足 $h(x_0,y_0,z_0)=0 \bmod e^m$。若由组合而来的多项式满足 $\|h(xX,yY,zZ)\|<e^m/(w^{1/2})$，其中 $X,\ Y,\ Z$ 为 x_0,y_0,z_0 的上界；w 为 $h(x,\ y,\ z)$项数，则由引理 3 可得 $h(x_0,y_0,z_0)=0$。如果可以得到多个满足引理 3 条件的多项式，则可通过做这些多项式的结式求得解(x_0,y_0,z_0)。

求具有较小范的多项式使用的工具即为格约化。将多项式集 $h_{u_1,u_2,u_3,v}(xX,yY,zZ)$ 的系数看作有理数域上的向量，则由这些向量可以构成整数环上的一个格 L。设格 L 的维数为 r，则由引理 2 可得 LLL 算法的第 1 个输出向量和第 2 个输出向量对应的多项式满足：

$\|h_1(xX,yY,zZ)\|\le 2^{r/2}\det(L)^{1/r}$；$\|h_2(xX,yY,zZ)\|\le 2^{r/2}\cdot\det(L)^{1/(r-1)}$。

为了对多项式 $h_1(x,y,z)$，$h_2(x,y,z)$ 应用引理 3，需要使得不等式 $2^{(r-1)/2}\det(L)^{1/(r-1)}<e^m(r^{1/2})$ 成立。因为这里所讨论的数的规模通常比 $2^{(r-1)/2}$ 大很多，所以在讨论时通常将这些小因子隐去。于是不等式变为 $\det(L)<e^{m(r-1)}$。

至此，可以得到结论：若所构造的格可以使得上述不等式成立，则可以得到两个多项式满足引理 3。从而，$h_1(x_0,y_0,z_0)=0$，$h_2(x_0,y_0,z_0)=0$。做结式 $g'(y,z)=\mathrm{Res}_x(h_1,h_2)$，若 $g'(y,z)\ne 0$，则结合 $g(y,z)=0$ 可得解 y_0。

注 2 在上面的算法中，假设了由格约化所得的两个多项式结式不为零。找出结式是否为零的充分必要条件是 Coppersmith 方法中遗留的一个公开问题。从而，当应用 Coppersmith 方法求解多项式时，必须使用试验来验证由格约化所得的两个多项式结式是否为零。试验表明由本文构造的格所得到的多项式结式均不为零。故有如下假设。

假设 1 本文中由格约化所得的多项式，其结式不为零。

3 攻击算法

本节将具体考查对公钥 N 的素因子共享低位比特时的 RSA 密码系统的安全性。

假设公钥 $N=pq$ 为一个 n 比特的正整数，其素因子 p 和 q 均为 $n/2$ 比特的素数，并且 p 和 q 的低$(1/2-\alpha)n$ 比特相同。设 RSA 公钥系统的公钥 e 为 $\gamma\ n$ 比特的奇数，私钥 d 为 $\beta\ n$ 比特。由 e 和 d 的关系可得，存在正整数 k 满足 $ed=k(N+1-(p+q))+1$。设 $p-q=r2^{(1/2-\alpha)n}$，其中 r 为一个 $\alpha\ n$ 比特的正整数，则上式变为 $ed=k(N+1-(r2^{(1/2-\alpha)n}+2q))+1$。令 $A=N+1$，$a=2^{(1/2-\alpha)n}$，则 (k,q,r) 为模多项式 $f(x,y,z)=x(A-2y-az)+1 \bmod e$ 的解。从而求解 RSA 私钥 d 的问题就转化为求解 $(x_0,y_0,z_0)\in\boldsymbol{Z}$ 的问题，并使其满足 $f(x_0,y_0,z_0)=0 \bmod e$，且 $|x_0|<X,|y_0|<Y,|z_0|<Z$，其中 $X\cong ed/N\cong N^{\gamma+\beta-1}$，$Y=N^{1/2},Z=N^{\alpha}$。

构造多项式集如下：

$$g_{k,i,b}(x,y,z)=e^{m-k}x^iy^bf^k(x,y,z),\ k=0,\cdots,(m-1),\ i=1,\cdots,(m-k),\ b=0,1;$$

$$h'_{k,j}(x,y,z)=e^{m-k}(az)^jf^k(x,y,z),\ k=0,\cdots,m;\ j=0,\cdots,t;$$

$$h''_{k,j}(x,y,z)=e^{m-k}(y)^jf^k(x,y,z),\ k=0,\cdots,m;\ j=1,\cdots,t;$$

其中 m 和 t 是参数。

注 3 变量 y 和 z 具有关系 $y^2+ayz=N$。故任何类似于 $x^iy^jz^k$ 的项均可由 x^iy^j 和 x^iz^k 线性表示。从而在所构造的多项式中不出现项 $x^iy^jz^k$。事实上，若 $j\ge k$，则 $x^iy^jz^k=x^iy^{(j-k)}(N-y^2)^k/a^k$；若 $j\le k$，$x^iy^jz^k=x^iz^{(k-j)}(N-y^2)^k/a^k$。观察可得 z 的指数下降了，故可再次将方程右边出现的形如 $x^iy^jz^k$ 的项应用 $y^2+ayz=N$ 将其化简至 0。

使用 $g_{k,i,b}(xX,yY,zZ)$， $h'_{k,j}(xX,yY,zZ)$ 和 $h''_{k,j}(xX,yY,zZ)$ 的系数构造格 L。即将这些多项式的系数看作整数环上的向量，格 L 即为由这些向量生成的格。对格 L 使用 LLL 算法求得两个向量 $\boldsymbol{h}_1, \boldsymbol{h}_2$，设其对应的多项式分别为 $h_1(xX,yY,zZ)$，$h_2(xX,yY,zZ)$，则 $h_1(xX,yY,zZ)$ 和 $h_2(xX,yY,zZ)$ 均满足 $h_1(x_0,y_0,z_0)=0 \bmod e^m$， $h_2(x_0,y_0,z_0)=0 \bmod e^m$， $x_0=k, y_0=q, z_0=r$。当 $h_1(xX,yY,zZ)$ 和 $h_2(xX,yY,zZ)$ 的范足够小时，由引理 3 可得 $h_1(x_0,y_0,z_0)=0$，$h_2(x_0,y_0,z_0)=0$。由于 $az=N/y-y$，从而可以得到两个多项式 $H_1(x,y)$ 和 $H_2(x,y)$ 满足 $H_1(x_0,y_0)=0$， $H_2(x_0,y_0)=0$，其中 $(x_0,y_0)=(k,q)$。做 $H_1(x,y)$ 和 $H_2(x,y)$ 的结式 $h(y)=\mathrm{Res}_x(H_1,H_2)$，则 $h(y)$ 以 y_0 为根。求解这个多项式即可求得模数 N 的因子 q。

下面说明在何种条件下，才能使得 LLL 算法输出的两个多项式满足引理 3 的条件。由上一节的说明可得当所构造的格满足式(1)时，引理 3 的条件才会满足

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

其中 w 为格 L 的维数。

由所构造的格可得， 调整所有多项式中项的顺序可以使得形如表 1 的矩阵成为下三角形。 从而计算 $\det(L)$只需要计算这个矩阵对应的对角线上的元素即可。 这个矩阵对角线上含有 X 的数目为 $\mathrm{num}_x=m(m+1)(4m+3t+5)/6+m(m+1)t/2$; 含有 Y 的数目为 $\mathrm{num}_y=m(m+1)(m+2)/6+t/2+mt+m^2t/2+t^2/2+mt^2/2$。含有 Z 的数目为 $\mathrm{num}_z=(m^3-m)/6+(m+1)t/2+(m+1)mt/2+m(m+1)/2+t^2(m+1)/2$，含有 e 的数目 num_e 与 num_x 相同。其具体证明过程略。从而，$\det(L)=(eX)^{\mathrm{num}_x}Y^{\mathrm{num}_y}Z^{\mathrm{num}_z}=N^{(2\gamma+\beta-1)\mathrm{num}_x+\mathrm{num}_y/2+\alpha\mathrm{num}_z}$。又因为格 L 的维数为$(m+1)\cdot(m+2t+1)$，故式(1)变为

$$(2\gamma+\beta-1)\mathrm{num}_x+\mathrm{num}_y/2+\alpha\mathrm{num}_z < \gamma m((m+1)(m+2t+1)-1)$$

设 $t=\tau m$ ， 于是 $\mathrm{num}_e=\mathrm{num}_x=(4+6\tau)m^3/6+o(m^3)$ ； $\mathrm{num}_y=(1+3\tau+3\tau^2)m^3/6+o(m^3)$ ； $\mathrm{num}_z=(1+3\tau+3\tau^2)m^3/6+o(m^3)$。从而式(1)成立的充分必要条件变为

$$(2\gamma+\beta-1)((4+6\tau)m^3/6+o(m^3))+(1/2)((1+3\tau+3\tau^2)m^3/6+o(m^3))+\alpha((1+3\tau+3\tau^2)m^3/6+o(m^3)) < \gamma((1+2\tau)m^3+o(m^3))$$

对充分大的 m，要使得上式成立只需要满足下面的不等式

$$(8(2\gamma+\beta-1)+1+2\alpha-12\gamma)+(12(2\gamma+\beta-1)+3+6\alpha-24\gamma)\tau+(3+6\alpha)\tau^2<0$$

上式中 $\tau=-(6\alpha+12\beta-9)/(6+12\alpha)$ 取最小值。最小值为 $(12+24\alpha)(2\alpha+8\beta+4\gamma-7)-(6\alpha+12\beta-9)^2$。故式(1)成立只需要 $-144\beta^2+(48\alpha+312)\beta+(12\alpha^2-36\alpha+96\alpha\gamma+48\gamma-165)<0$。所以当

$$\beta<((48\alpha+312)-((48\alpha+312)^2+576(12\alpha^2-36\alpha+96\alpha\gamma+48\gamma-165))^{1/2})/288 \tag{2}$$

时有式(1)成立。

至此，对充分大的 m，通过优化 t 可以得到可以求取的公钥 d 的最大规模。具体结果可以有下面的两个表来形象地说明。表 1 的第 1 行是 γ 的取值，第 1 列是 α 的取值，其他元素表示的是当 γ 和 α 取相应的值时， β 的上界。表 2 是 p,q 不平衡的变形 RSA 公钥体制的格攻击结果，其第 1 行是 γ 的取值，第 1 列是 $\min\{\log_N(p),\log_N(q)\}$。

4　结束语

由此可以得到结论， 若构成 RSA 模数 N 的素数 p 和 q 满足其低位比特相同的条件， 则 RSA 密码算法的安全性较普通的小私钥指数的 RSA 密码算法要弱， 其更易受到格攻击。从而，使用这种密码算法时应当谨慎。

表 1　p, q 共享低位比特时的攻击结果

	$\gamma=1.0$	0.9	0.86	0.8	0.7	0.6	0.55
$\alpha=0.5$	0.284	0.323	0.339	0.363	0.406	0.451	0.475
0.4	0.319	0.356	0.371	0.395	0.435	0.479	0.501
0.3	0.355	0.390	0.405	0.427	0.466	0.507	0.529
0.25	0.375	0.409	0.423	0.444	0.482	0.522	0.544

表 2　p, q 不平衡时的攻击结果

	$\gamma=1.0$	0.9	0.86	0.8	0.7	0.6	0.55
$\min\{\log_N(p),\log_N(q)\}=0.5$	0.284	0.323	0.339	0.363	0.406	0.451	0.475
0.4	0.296	0.334	0.350	0.374	0.415	0.460	0.483
0.3	0.334	0.369	0.384	0.406	0.446	0.487	0.510
0.25	0.364	0.398	0.412	0.433	0.471	0.511	0.532

参 考 文 献

[1] Wiener M. Cryptanalysis of short RSA secret exponents. *IEEE Trans. on Information Theory*, 1990, 36(3): 553–558.

[2] Boneh D and Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Trans. on Information Theory*, 2000, 46(4): 1339–1349.

[3] Coppersmith D. Finding a small root of a univariate modular equation. Eurocrypt 96, Saragossa, Spain, 1996, LNCS 1070: 155–165.

[4] Coppersmith D. Finding a small root of a bivariate integer equation; factoring with high bits known. Eurocrypt 96, Saragossa, Spain, 1996, LNCS 1070: 178–189.

[5] Coppersmith D. Finding small solutions to small degree polynomials. CalC 2001, Providence, RI, USA, 2001, LNCS 2146: 178–189.

[6] Sun H M, Yang W C, and Laih C S. On the design of RSA with short secret exponent. Asiscrypt 1999, Singapore, 1999, LNCS 1716: 150–164.

[7] Durfee G and Nguyen P Q. Cryptanalysis of the RSA schemes with short secret exponent from Asiscrypt'99. Asiscrypt 2000, Kyoto, Japan, 2000, LNCS 1976: 14–29.

[8] Steinfeld R and Zheng Y L. An advantage of low-exponent RSA with modulus primes sharing least significant bits.CT-RSA 2001, San Francisco, CA, USA, 2001, LNCS 2020: 52–62.

[9] Steinfeld R and Zheng Y L. On the security of RSA with primes sharing least significant bits. *Applicable Algebra in Engineering Communication and Computing*, 2004, 15(3): 179–200.

[10] Weger B D. Cryptanalysis of RSA with small prime difference. *Applicable Algebra in Engineering Communication and Computing*, 2003, 13: 17–28.

[11] Lenstra A, Lenstra H, and Lovasz L. Factoring Polynomials with rational coefficients. *Mathematiche Annalen*, 1982, 261: 515–534.

[12] Howgrave-Graham N. Finding small roots of univariate modular equations revisited. Cryptography and Coding, UK, 1997, LNCS 1355: 131–142.

赵耀东： 男，1979 年生，博士生，研究方向为密码学.

戚文峰： 男，1963 年生，教授，博士生导师，主要研究方向为有限域、密码学.