中国科学: 信息科学 2011 年 第 41 卷 第 2 期: 173–180
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS
论 文

RSA 密码系统小 CRT 解密指数的攻击分析

韩立东[①②], 王小云[③], 许光午[③④*]

① 山东大学密码技术与信息安全教育部重点实验室, 济南 250100
② 山东大学数学学院, 济南 250100
③ 清华大学高等研究院, 北京 100084
④ Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53201, USA
* 通信作者. E-mail: gxu4uwm@uwm.edu

收稿日期: 2009–07–16; 接受日期: 2010–03–26
国家自然科学基金 (批准号: 60910118)、国家重点基础研究发展计划 (批准号: 2007CB807902) 和清华大学自主科研计划 (批准号: 2009THZ01002) 资助项目

摘要 本文旨在讨论使用中国剩余定理 (CRT) 表示解密指数的 RSA 系统. 由于中国剩余定理表示可被用来提高计算速度, 这样的系统具有很高的实际应用价值. 文中主要分析当前文献中一个对具有小 CRT 解密指数的 RSA 系统的攻击. 本文指出, 该攻击巧妙地运用了格理论, 但其中某些论断一般是不正确的, 并为此提供了几个反例. 本文改进并完善了这个小 CRT 解密指数的攻击方法.

关键词 RSA 中国剩余定理 密码分析 连分数 格归约

1 引言

在实际应用中, RSA 密码系统 [1] 使用小加密指数或小解密指数加快加密或解密 (签名) 等基本运算. 然而, 一些研究分析表明在使用这些特殊参数时应当十分谨慎. 目前已有一些针对 RSA 小解密指数的攻击分析结果. Lenstra 等 [2] 提出的格归约算法, Coppersmith[3] 求解同余方程小根的技术, 加上经典的数论结果都是公钥密码分析的有力工具.

给定 RSA 模 N 和私钥 d, Wiener[4] 首次提出当 $d < N^{\frac{1}{4}}$ 时 RSA 密码系统是不安全的. Wiener 分析方法的本质是利用了连分数中的 Legendre 定理. 1999 年, Boneh 和 Durfee[5] 在 Coppersmith 的工作基础上把弱密钥 d 的界提高到 $d < N^{0.292}$.

d 的中国剩余定理表示形式如下: d_p, d_q 满足 $d_p = d \pmod{(p-1)}$ 和 $d_q = d \pmod{(q-1)}$. d_p, d_q 称为私钥 (秘密)CRT 指数. 利用私钥 CRT 指数进行解密和签名过程比标准 RSA 系统有效. 此思想是由 Quisquater 和 Couvreur[6] 首先提出. 文献 [3] 建议使用小的私钥 CRT 指数使解密和签名过程更加快速有效. 近年来, 密码学家开始对小的私钥 CRT 指数的 RSA 密码体制进行研究分析. 2002 年 May[7] 给出了对非平衡的素因子 p 和 q 的 RSA 的两种多项式时间攻击算法, 算法成功的条件是 $q < N^{0.382}$. Bleichenbacher 和 May[8] 在 2006 年进一步提高此结果至 $q < N^{0.468}$. 同时对于 RSA 素因子平衡的情况, 文献 [8] 提出一种基于格的攻击方法, 其限制条件是公钥指数 e 比 RSA 模 N 小很多.

引用格式: 韩立东, 王小云, 许光午. RSA 密码系统小 CRT 解密指数的攻击分析. 中国科学: 信息科学, 2011, 41: 173–180

https://engine.scichina.com/doi/10.1360/zf2011-41-2-173

在此方法中，首先利用一个线性关系式构造一个三维格, 然后把问题转变成求解这个三维格的最短向量. 本文以下部分称此攻击为小私钥 CRT 指数攻击. 需要说明的是, 文献 [8] 的分析方法是探索式的, 实现速度非常快. 具体结果是, 当 $d_p, d_q < \min\{\frac{1}{4}(\frac{N}{e})^{\frac{2}{5}}, \frac{1}{3}N^{\frac{1}{4}}\}$ 时, 此攻击方法是有效的. 依照文献 [8] 的结论, 该方法可以攻击文献 [9,10] 设计的 RSA 密码体制变型. 最近, Jochemsz 和 May[11] 对一般的小私钥 CRT 指数 RSA 给出了一个新的攻击结果, 该方法对公钥指数 e 的大小没有限制, 但是要求私钥 CRT 指数都非常小, 即 $d_p, d_q < N^{0.073}$.

本文旨在讨论 RSA 密码体制小私钥 CRT 指数的攻击分析. 证明文献 [8] 的一些论断是不正确的, 并给出了反例. 同时完善了该攻击方法.

本文的结构安排: 第 2 节介绍所需的一些预备知识. 第 3 节介绍 Bleichenbacher 和 May 的小私钥 CRT 指数攻击. 对于小私钥 CRT 指数攻击的几点讨论将在第 4 节提出. 第 5 节给出该攻击方法的完善和改进. 最后的总结是第 6 节的内容.

2 预备知识

2.1 CRT 指数的 RSA 密码算法

在标准 RSA 密码算法中, RSA 模 N 是两个大素数 p 和 q 的乘积, 且满足 $q < p < 2q$. 公钥指数 e 和私钥指数 d 的选取满足

$$ed \equiv 1 \pmod{(p-1)(q-1)}.$$

RSA-CRT 密码体制是 RSA 的一个变型, 即解密时解密指数 d 用私钥 CRT 指数 d_p, d_q 代替, 其中 d_p,d_q 满足

$$ed_p \equiv 1 \pmod{p-1},\ ed_q \equiv 1 \pmod{q-1}.$$

当解密密文 $c = m^e \mod N$ 时, 计算 $m_p = c^{d_p} \pmod{p}, m_q = c^{d_q} \pmod{q}$, 便可以通过中国剩余定理得到明文 $m = (q(q^{-1} \mod p)m_p + p(p^{-1} \mod q)m_q) \pmod{N}$.

2.2 格

定义由线性独立的集合 $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\} \subset \mathbb{R}^n$ 生成的格 $\mathcal{L}$ 是这些向量所有整系数的线性组合构成的集合, 也就是 $\mathcal{L} = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2 + \cdots + \mathbb{Z}\boldsymbol{b}_n$. 设 M 是行向量 $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ 组成的矩阵. $\mathcal{L}$ 的行列式, 记 $\det(\mathcal{L})$, 定义为 $|\det(M)|$.

数的几何理论中的 Minkowski 基本定理指出 $\mathbb{R}^n$ 的任何体积大于 $2^n \det(\mathcal{L})$ 且中心对称的凸集都存在一个非零格点 (见文献 [12]). 这个定理给出格中最短向量 $\boldsymbol{v}$ 的长度的一个上界, 是关于格的行列式和维数的函数, 即 $\|\boldsymbol{v}\| \leqslant \sqrt{n}\det(\mathcal{L})^{\frac{1}{n}}$. 我们称 $B_{\mathcal{L}} = \sqrt{n}\det(\mathcal{L})^{\frac{1}{n}}$ 为 Minkowski 界. 我们知道, 求解格中的最短向量是 NP-hard 问题. 最著名的格基归约算法是由 Lenstra, Lenstra 和 Lovász 给出的 (称为 LLL 算法), 该算法能够在多项式时间内总可以找到一个较短的向量. 更准确的讲, 给定格 $\mathcal{L}$ 的一组格基 $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$, LLL 算法输出另一组基 (称为约化基)$\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$, 满足 $\|\boldsymbol{v}_1\| < 2^{\frac{n-1}{4}}\det(\mathcal{L})^{\frac{1}{n}}$.

https://engine.scichina.com/doi/10.1360/zf2011-41-2-173

2.3 连分数

任何一个正有理数 ξ 都能表示成

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_K}}},$$

其中 a_0 是非负整数, $a_1, a_2, \ldots, a_K$ 是正整数. 这种形式称为 ξ 的有限连分数表示, 记为 $[a_0, a_1, a_2, \ldots, a_K]$. 对于 $j \leqslant K$, 分数 $\frac{\alpha_j}{\beta_j} = [a_0, a_1, a_2, \ldots, a_j]$ 称为 ξ 的第 j 个渐近连分数. 这方面的一个著名结果是, 在分母不大于 β_j 的所有有理数中, $\frac{\alpha_j}{\beta_j}$ 是 ξ 一个最好的逼近值. $\frac{\alpha_j}{\beta_j}$ 称为 ξ 的最佳渐近分数.

另一个关于连分数的有用结论是下面的 Legendre 经典定理.

定理(Legendre) 如果存在一个有理数 $\frac{n}{m}$ 满足 $|\xi - \frac{n}{m}| \leqslant \frac{1}{2m^2}$, 那么, 一定存在 j 使得 $\frac{\alpha_j}{\beta_j} = \frac{n}{m}$.

使用扩展 Euclid 算法可以有效地计算出 ξ 的连分数和两个序列 $\{\alpha_j\}$ 和 $\{\beta_j\}$.

这里我们仅讨论有理数的连分数, 本节中有理数的连分数表示和结论同样可以扩展到实数上. 感兴趣的读者可以参阅文献 [12].

3 小私钥 CRT 指数攻击

首先考虑平衡的 RSA-CRT 密码系统, 即 RSA 模 N 是相同比特长度的素因子 p 和 q 的乘积, 且有 $q < p < 2q$. 公钥指数 e 和 CRT 解密指数 d_p, d_q 满足下列关系式

$$ed_p \equiv 1 \pmod{p-1},\ ed_q \equiv 1 \pmod{q-1}.$$

文献 [8] 中小私钥 CRT 指数攻击是一种探索式的方法, 在条件

$$d_p, d_q < \min\left\{\frac{1}{4}\left(\frac{N}{e}\right)^{\frac{2}{5}}, \frac{1}{3}N^{\frac{1}{4}}\right\} \tag{1}$$

成立下, 可以有效破解 RSA-CRT 密码算法. 下面我们详细介绍小私钥 CRT 指数攻击方法. 设整数 $k, l \in \mathbb{N}$ 满足

$$ed_p = 1 + k(p-1),\ ed_q = 1 + l(q-1). \tag{2}$$

由此, 可以得到等式

$$e^2 d_p d_q + kl(1-N) + e\big(d_p(l-1) + d_q(k-1)\big) = k + l - 1.$$

设

$$\begin{cases} x = d_p(l-1) + d_q(k-1), \\ y = kl, \\ z = k + l - 1, \\ w = d_p d_q, \end{cases} \tag{3}$$

https://engine.scichina.com/doi/10.1360/zf2011-41-2-173

则上式可以转换成一个线性关系式, $ex+(1-N)y+e^2w=z$, 或者, 等价地,

$$(x,y,w)\begin{pmatrix}1 & 0 & e\\ 0 & 1 & 1-N\\ 0 & 0 & e^2\end{pmatrix}=(x,y,z).$$

令

$$L=\begin{pmatrix}4e & 0 & e^{\frac{3}{5}}N^{\frac{2}{5}}e\\ 0 & 4N^{\frac{1}{2}} & e^{\frac{3}{5}}N^{\frac{2}{5}}(1-N)\\ 0 & 0 & e^{\frac{3}{5}}N^{\frac{2}{5}}e^2\end{pmatrix}, \tag{4}$$

今设 $\mathcal{L}$ 是由 L 的行向量生成的格，则有下列结论:

1) 格 $\mathcal{L}$ 的 Minkowski 界为 $B_{\mathcal{L}}=\sqrt{3}\det(L)^{\frac{1}{3}}=4^{\frac{2}{3}}\sqrt{3}e^{\frac{6}{5}}N^{\frac{3}{10}}$.

2) $(x,y,w)L=(4ex,4N^{\frac{1}{2}}y,e^{\frac{3}{5}}N^{\frac{2}{5}}z)$.

3) 如果 w,x,y 和 z 满足关系式 (3), 那么格向量 $(4ex,4N^{\frac{1}{2}}y,e^{\frac{3}{5}}N^{\frac{2}{5}}z)$ 的长度小于 Minkowski 界 $B_{\mathcal{L}}$.

文献 [8] 提出下述探索式假设, 对于格 $\mathcal{L}$, 长度小于 Minkowski 界 $B_{\mathcal{L}}$ 的格向量是唯一的. 因此, 利用 LLL 算法得到的短向量一定是 $(4ex,4N^{\frac{1}{2}}y,e^{\frac{3}{5}}N^{\frac{2}{5}}z)$, 其中 x,y 和 z 满足关系式 (3). x,y 和 z 可以通过这个向量计算得到, 从而分解 RSA 模. 文献 [8] 同时提供了上述结论的实验数据, 其中私钥 CRT 指数和公钥指数的取值范围分别是 $d_p,d_q<2^{200}$ 和 $e<2^{512}$.

4 小私钥 CRT 指数攻击的几点说明

在本节中, 我们指出上述格 $\mathcal{L}$ 中长度小于 Minkowski 界 $B_{\mathcal{L}}$ 的非零短向量是唯一的这种探索式假设在一般情况下不成立. 下面分两种情形讨论:

$$\min\left\{\frac{1}{4}\left(\frac{N}{e}\right)^{\frac{2}{5}},\frac{1}{3}N^{\frac{1}{4}}\right\}=\frac{1}{3}N^{\frac{1}{4}},$$

和

$$\min\left\{\frac{1}{4}\left(\frac{N}{e}\right)^{\frac{2}{5}},\frac{1}{3}N^{\frac{1}{4}}\right\}=\frac{1}{4}\left(\frac{N}{e}\right)^{\frac{2}{5}}.$$

第一种情形等价于 $e\leqslant(\frac{3}{4})^{\frac{5}{2}}N^{\frac{3}{8}}$. 在这种情况下, 向量 $(4ex,4N^{\frac{1}{2}}y,e^{\frac{3}{5}}N^{\frac{2}{5}}z)$ 不再是唯一长度小于 Minkowski 界 $B_{\mathcal{L}}$ 的非零向量. 下面我们给出证明.

记 $e=N^{\alpha}$, 那么 $\alpha<\frac{3}{8}$. 格 $\mathcal{L}$ 的 Minkowski 界可以写成 $B_{\mathcal{L}}=4^{\frac{2}{3}}\sqrt{3}N^{\frac{6}{5}\alpha+\frac{3}{10}}$.

断言 1 $4e^2<B_{\mathcal{L}}$.

实际上,

$$\frac{4e^2}{B_{\mathcal{L}}}<\frac{N^{2\alpha}}{N^{\frac{6}{5}\alpha+\frac{3}{10}}}=N^{\frac{4}{5}\left(\alpha-\frac{3}{8}\right)}<1.$$

断言 2 $(4e^2,0,0)$ 是格 $\mathcal{L}$ 中的一个向量.

实际上, 如果我们记 $L(i)$ 是矩阵 L 中第 i 个行向量, 那么 $(4e^2,0,0)=eL(1)-L(3)$. 因此, 在这种情况下我们找到了一个非零向量 $(4e^2,0,0)$, 其长度小于 Minkowski 界 $B_{\mathcal{L}}$. 显然, 此向量不同

https://engine.scichina.com/doi/10.1360/zf2011-41-2-173

于向量 $(4ex, 4N^{\frac{1}{2}}y, e^{\frac{3}{5}}N^{\frac{2}{5}}z)$. 同时, 需要指出的是, 多数情况下 LLL 算法求出的第一个短向量都是 $(4e^2, 0, 0)$(用 Shoup 的 NTL 数论函数库 [13] 编程实现). 此外, 还有更多长度小于 Minkowski 界 $B_{\mathcal{L}}$ 的向量, 如 $\lambda_1(4e^2, 0, 0) + \lambda_2(4ex, 4N^{\frac{1}{2}}y, e^{\frac{3}{5}}N^{\frac{2}{5}}z)$, 其中 λ_1, λ_2 是某些整数.

文献 [8] 中的变量 x, y 和 z 的取值范围本质上是与不等式 $e < N^{\frac{3}{8}}$ 有关的 (文献 [8] 第 9 页). 因此 x, y 和 z 的界决定格 $\mathcal{L}$ 的构造. 很自然的问题就是, 能否完善一下格 $\mathcal{L}$ 的构造使得当 $e < N^{\frac{3}{8}}$ 时, 文献 [8] 的思想还能有效. 下面我们将讨论此问题.

记 $e = N^{\alpha}$, 假设 $\alpha < \frac{3}{8}$ 和 $d_p, d_q < \frac{1}{3}N^{\frac{1}{4}}$. 我们有下面结论

$$k < \frac{ed_p}{p-1} < \frac{N^{\alpha}\frac{1}{3}N^{\frac{1}{4}}}{N^{\frac{1}{2}}} = \frac{1}{3}N^{\alpha-\frac{1}{4}}, \quad l < \frac{ed_q}{q-1} < \frac{N^{\alpha}\frac{1}{3}N^{\frac{1}{4}}}{\frac{1}{2}N^{\frac{1}{2}}} = \frac{2}{3}N^{\alpha-\frac{1}{4}}.$$

由上, 可得变量 x, y 和 z 的界:

$$x < \frac{1}{3}N^{\alpha}, \quad y < \frac{2}{9}N^{2\alpha-\frac{1}{2}}, \quad z < N^{\alpha-\frac{1}{4}}. \tag{5}$$

按照文献 [8] 的方法, 构造

$$L' = \begin{pmatrix} a & 0 & ce \\ 0 & b & c(1-N) \\ 0 & 0 & ce^2 \end{pmatrix},$$

其中 a, b 和 c 的取值待定. 设 $\mathcal{L}'$ 是由矩阵 L' 的行向量生成的格.

$\mathcal{L}'$ 的 Minkowski 界是 $B_{\mathcal{L}'} = \sqrt{3}\big(abcN^{2\alpha}\big)^{\frac{1}{3}}$. 其中 $(ax, by, cz) = (x, y, w)L'$, 也就是说, (ax, by, cz) 是格 $\mathcal{L}'$ 的一个向量. 类似文献 [8] 的方法, 选取 a, b 和 c 满足

1) $\|(a\frac{1}{3}N^{\alpha}, b\frac{2}{9}N^{2\alpha-\frac{1}{2}}, cN^{\alpha-\frac{1}{4}})\| < B_{\mathcal{L}'}$ (此处利用关系式 (5) 的界),

2) $a\frac{1}{3}N^{\alpha} \approx b\frac{2}{9}N^{2\alpha-\frac{1}{2}} \approx cN^{\alpha-\frac{1}{4}}$.

取 $a = 3N^{\gamma}, b = \frac{9}{2}N^{\frac{1}{2}+\gamma-\alpha}, c = N^{\frac{1}{4}+\gamma}$, 其中 $\gamma \geqslant 0$, 可满足上述两个条件.

由于 $\alpha < \frac{3}{8}$, 不等式 $ae = 3N^{\alpha+\gamma} < \frac{3\sqrt{3}}{\sqrt[3]{2}}N^{\gamma+\frac{1}{4}+\frac{\alpha}{3}} = B_{\mathcal{L}'}$ 成立. 也就是说, 除了向量 (ax, by, cz), $(ae, 0, 0) = (e, 0, -1)L'$ 也是格 $\mathcal{L}'$ 的有效短向量. 因此我们还是不能得到唯一性结论.

下面讨论第二种情况. 其条件等价于 $e \geqslant \big(\frac{3}{4}\big)^{\frac{5}{2}}N^{\frac{3}{8}}$. 对于这种情形, 我们给出一个具体的反例.

例子 选择 RSA 素因子的取值为 p =60533767506702857778226345956 11 和 q=429635953330562760947457097763. 那么

$$N = 26007482911432925508673390792563530751567080608803719771819 3.$$

公钥 e 和私钥 CRT 指数 d_p, d_q 分别为: e = 37860564280586716144375 3; d_p = 975677548627; d_q = 697573817543.

从上述例子中, 很容易验证 $d_p, d_q < \frac{1}{4}(\frac{N}{e})^{\frac{2}{5}}$.

按照关系式 (4) 构造矩阵 L, 然后生成相应的格 $\mathcal{L}$. 可以得到 LLL 算法计算出格 $\mathcal{L}$ 中的短向量是长度小于 Minkowski 界 $B_{\mathcal{L}}$ 的. 然而, 此短向量不是 $(4ex, 4N^{\frac{1}{2}}y, e^{\frac{3}{5}}N^{\frac{2}{5}}z)$, 其中 x, y, z 满足关系式 (3). 实际上, 格 $\mathcal{L}$ 的 LLL 归约基的 3 个向量都不是我们想要的短向量. 这也表明了集合 $\{\boldsymbol{v} \in \mathcal{L} : \|\boldsymbol{v}\| < B_{\mathcal{L}}\}$ 含有多于一个非零向量.

https://engine.scichina.com/doi/10.1360/zf2011-41-2-173

5 小私钥 CRT 指数攻击的完善

第 4 节中, 我们指出小私钥 CRT 指数攻击方法在一般情况下不能找到正确的解. 本节主要目的是完善此攻击方法. 对于特殊情况 $\alpha < \frac{3}{8}$ 和 $d_p, d_q < \frac{1}{3}N^{\frac{1}{4}}$, 还可以利用连分数方法求解此问题.

由前一节分析, 格 $\mathcal{L}$ 中长度小于 $B_{\mathcal{L}}$ 的非零短向量是不唯一的. 也就是说, 利用 LLL 算法求解格 $\mathcal{L}$ 的短向量不一定是 $(4ex, 4N^{\frac{1}{2}}y, e^{\frac{3}{5}}N^{\frac{2}{5}}z)$. 因此也就不一定得到 d_p 和 d_q.

记 $\boldsymbol{v}_0 = (4ex, 4N^{\frac{1}{2}}y, e^{\frac{3}{5}}N^{\frac{2}{5}}z)$. 可以看出 $\boldsymbol{v}_0$ 一定是格 $\mathcal{L}$ 约化基的 3 个向量的线性组合. 所以可以执行下列运算:

1. 选择一个适当的正整数 M;

2. 用 LLL 算法计算格 $\mathcal{L}$ 的约化基 $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3\}$;

3. 对每一个线性组合 $\boldsymbol{v} = a_1\boldsymbol{b}_1 + a_2\boldsymbol{b}_2 + a_3\boldsymbol{b}_3$, 其中 $|a_i| \leqslant M$, 设 $\boldsymbol{v} = (4ex, 4N^{\frac{1}{2}}y, e^{\frac{3}{5}}N^{\frac{2}{5}}z)$, 从 $\boldsymbol{v}$ 中计算出 x, y, z;

4. 验证 x, y, z 能否根据关系式 (3) 得到 d_p, d_q 并且分解 N.

在探索式假设下, M 的取值可以比较小 (例如 $M = 2^{10}$). 我们的实验数据支持这一假设.

上面的讨论可以应用到一般情况, $d_p, d_q < \min\{\frac{1}{4}(\frac{N}{e})^{\frac{2}{5}}, \frac{1}{3}N^{\frac{1}{4}}\}$. 接下来, 考虑 $\alpha < \frac{3}{8}$ 和 $d_p, d_q < \frac{1}{3}N^{\frac{1}{4}}$ 的情形. 我们的想法类似于 Galbraith 等 [9] 的方法, 是一种不同的求解方法. 下面具体描述该方法, 其本质是利用连分数方法的逼近原理.

关系式 $xe + y(1-N) + we^2 = z$ 可以转换成

$$\frac{e}{N-1} - \frac{y}{x+we} = \frac{z}{(N-1)(x+we)}. \tag{6}$$

又因为 $z < N^{\alpha-\frac{1}{4}}$, $k < \frac{1}{3}N^{\alpha-\frac{1}{4}}$, $l < \frac{2}{3}N^{\alpha-\frac{1}{4}}$, $x + we$ 满足

$$\begin{aligned} x + we &= d_p(l-1) + d_q(k-1) + ed_pd_q = d_p(l-1) + d_qkp \\ &< \frac{1}{3}N^{\frac{1}{4}}\frac{2}{3}N^{\alpha-\frac{1}{4}} + \frac{1}{3}N^{\frac{1}{4}}\frac{1}{3}N^{\alpha-\frac{1}{4}}2N^{\frac{1}{2}} < \frac{1}{4}N^{\left(\frac{5}{4}-\alpha\right)-2\left(\frac{3}{8}-\alpha\right)} < \frac{1}{4}N^{\left(\frac{5}{4}-\alpha\right)}. \end{aligned}$$

由方程 (6), 我们有

$$\begin{aligned} \frac{e}{N-1} - \frac{y}{x+we} &= \frac{z}{(N-1)}\frac{1}{(x+we)} < \frac{N^{\alpha-\frac{1}{4}}}{N}\frac{1}{(x+we)}\frac{N}{N-1} \\ &= \frac{1}{N^{\frac{5}{4}-\alpha}}\frac{1}{(x+we)}\frac{N}{N-1} < \frac{1}{4(x+we)^2}\frac{N}{N-1} < \frac{1}{2(x+we)^2}. \end{aligned}$$

由 Legendre 定理知, $\frac{y}{x+we}$ 是 $\frac{e}{N-1}$ 的渐近连分数表示. 也就是, 对于某个 j,

$$\frac{y}{x+we} = \frac{\alpha_j}{\beta_j}. \tag{7}$$

α_j 和 β_j 可以由 e 和 $N-1$ 通过扩展 Euclid 算法计算得出. 现在考虑关系式 (7), 分两种情况讨论:

情况 1 如果 $\gcd(y, x+we) = 1$, 则 $y = \alpha_j, x+we = \beta_j$. 然后得到 z 的值, $z = (x+we)e+y(1-N)$. 因为

$$x = d_p(l-1) + d_q(k-1) < \frac{1}{3}N^{\alpha} < N^{\alpha} = e,$$

计算 $x + we$ 模 e, 就可得到 x 和 w.

x, y, z 和 w 值已知, k, l 和 d_p, d_q 由 (3) 确定, 从而可以通过关系式 (2) 恢复出 p 和 q.

https://engine.scichina.com/doi/10.1360/zf2011-41-2-173

情况 2 $\gcd(y, x+we) = \gamma > 1$. 对于某个常数 c, $\gamma < c$ 以很大的概率成立 (我们的实验数据没有出现 $\gamma > 100$). 对于 $i = 2, 3, \ldots, c-1$ 和 $\frac{e}{N-1}$ 的所有渐近连分数 $\frac{\alpha_j}{\beta_j}$, 计算 $y = i\alpha_j, x + we = i\beta_j$, 然后求解 k, l 和 d_p, d_q 所有可能的值进行验证. 通过分析, 该方法会以很大概率找到正确的解.

下面解释为什么 γ 通常很小. 首先观察关系式 $xe + y(1-N) + we^2 = z$, 可以得到

$$\gcd(y, x+we) \big| \gcd(y, z).$$

因为 $y = kl, z = k + l - 1$, 假设 $\gamma = \gamma_k\gamma_l$, 其中 $\gamma_k | k, \gamma_l | l$(实际中, 可取 k, l 为互素二数). 这就使得 $\gamma_k | l-1, \gamma_l | k-1$. 因此,

$$\gamma_k | \gcd(k, l-1) \text{ and } \gamma_l | \gcd(k-1, l).$$

这意味着, 大多数情况下 γ_k 和 γ_l 都很小. 同样, 就分解而言, $k, l < N^{\alpha - \frac{1}{4}}$ 也是很小的.

6 结论

本文主要讨论了私钥 CRT 指数 RSA 密码体制的安全性. 我们得出在条件 (1) 下, 文献 [8] 构造的格中小于 Minkowski 界 $B_{\mathcal{L}}$ 的向量不是唯一的, 分析完善了文献 [8] 的攻击方法. 当 $e < N^{\frac{3}{8}}$ 时, 给出了类似于 Galbraith, Heneghan 和 McKee 的方法, 利用了连分数的经典 Legendre 定理有效实现 RSA 模 N 的分解.

参考文献

1 Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM, 1978, 21: 120–126

2 Lenstra A K, Lenstra H W, Lovász L. Factoring polynomial with rational coefficients. Math Ann, 1982, 261: 515–534

3 Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J Crypto, 1997, 10: 233–260

4 Wiener M. Cryptanalysis of short RSA secret exponents. IEEE Trans Inf Theory, 1990, 36: 553–558

5 Boneh D, Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans Inf Theory, 2000, 46: 1339–1349

6 Quisquater J J, Couvreur C. Fast decipherment algorithm for RSA public-key cryptosystem. Electr Lett, 1982, 18: 905–907

7 May A. Cryptanalysis of unbalanced RSA with small CRT-exponent. In: Proceeding of Crypto 2002. LNCS 2442. Berlin: Springer-Verlag, 2002. 242–256

8 Bleichenbacher D, May A. New attacks on RSA with small secret CRT-exponents. In: Proceeding of PKC 2006. LNCS 3958. Berlin: Springer-Verlag, 2006. 1–13

9 Galbraith S D, Heneghan C, McKee J F. Tunable balancing of RSA. In: Proceeding of ACISP 2005. LNCS 3574. Berlin: Springer-Verlag, 2005. 280–292

10 Sun H M, Wu M E. An approach towards RSA-CRT with short public exponent. Cryptology ePrint Archive, 2005/053

11 Jochemz E, May A. A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$. In: Proceeding of Crypto 2007. LNCS 4622. Berlin: Springer-Verlag, 2007. 395–411

12 Hua L K. Introduction to Number Theory. Berlin: Springer-Verlag, 1982

13 Shoup V. NTL: a library for doing number theory. Available at http://www.shoup.net/ntl/index.html

https://engine.scichina.com/doi/10.1360/zf2011-41-2-173

On an attack on RSA with small CRT-exponents

HAN LiDong[1,2], WANG XiaoYun[3] & XU GuangWu[3,4*]

1 *Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan* 250100*, China;*
2 *School of Mathematics, Shandong University, Jinan* 250100*, China;*
3 *Institute for Advanced Study, Tsinghua University, Beijing* 100084*, China;*
4 *Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI* 53201*, USA*
*E-mail: gxu4uwm@uwm.edu

Abstract This paper concerns the RSA system with private CRT-exponents. Since Chinese remainder representation provides efficiency in computation, such system is of some practical significance. In this paper, an existing attack to small private CRT-exponents is analyzed. It is indicated that this attack makes nice use of lattice in RSA analysis, but some argument does not hold in general. Several counterexamples are constructed. Refinements and more precise statements of the attack are given.

Keywords RSA, CRT, cryptanalysis, continued fraction, lattice reduction

https://engine.scichina.com/doi/10.1360/zf2011-41-2-173