密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2015,2(5):390–403

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-81033101

私钥低比特特定泄露下的 RSA 密码分析*

王世雄[1], 屈龙江[1], 李 超[1,2], 付绍静[2]

1. 国防科学技术大学 理学院, 长沙 410073
2. 国防科学技术大学 计算机学院, 长沙 410073
通讯作者: 王世雄, E-mail: wsx09@foxmail.com

摘 要: 基于 Coppersmith 方法, RSA 密码分析取得了许多新结果, 其中包括部分私钥泄露攻击与低解密指数攻击. 现实中侧信道攻击能够泄露私钥的部分比特位, 而部分私钥泄露攻击正是通过泄露的这些比特位来实现对 RSA 密码的破解. 低解密指数攻击则是在解密指数取值较小的条件下来破解 RSA, Boneh 和 Durfee 给出了至今最好的结果. 针对私钥最低几位比特泄露的攻击, 是一类重要的部分私钥泄露攻击, 并且和低解密指数攻击紧密相关. 基于 Coppersmith 方法在模多项式方程求小值解的应用, 以及线性化模方程的技巧, 本文给出了新的针对私钥最低几位比特泄露的攻击结果. 其中线性化模方程的技巧, 来源于 Herrmann 和 May 对于 Boneh 和 Durfee 的低解密指数攻击结果的简化证明. 注意到目前针对私钥最低几位比特泄露的攻击只关注所泄露比特的位数, 而本文还关注所泄露比特的取值. 当所泄露比特的取值满足一定的条件时, 本文的结果改进了 Ernst 等人的攻击结果. 另外 Ernst 等人只考虑了加密指数与 RSA 模基本相等的特殊情况, 本文进一步研究了加密指数小于 RSA 模的一般情况.

关键词: RSA; 最低几位比特泄露; Coppersmith 方法; 格; LLL 算法
中图法分类号: TP918 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000088

中文引用格式: 王世雄, 屈龙江, 李超, 付绍静. 私钥低比特特定泄露下的 RSA 密码分析[J]. 密码学报, 2015, 2(5): 390–403.
英文引用格式: Wang S X, Qu L J, Li C, Fu S J. Cryptanalysis of RSA with special exposed least significant bits of the private key[J]. Journal of Cryptologic Research, 2015, 2(5): 390–403.

Cryptanalysis of RSA with Special Exposed Least Significant Bits of the Private Key

WANG Shi-Xiong[1], QU Long-Jiang[1], LI Chao[1,2], FU Shao-Jing[2]

1. College of Science, National University of Defense Technology, Changsha 410073, China
2. College of Computer Science, National University of Defense Technology, Changsha 410073, China
Corresponding author: WANG Shi-Xiong, Email: wsx09@foxmail.com

Abstract: There are many new results of cryptanalysis of RSA based on Coppersmith's method, which include partial key exposure attacks and low private exponent attacks. With side channel attacks, partial bits of the private key can be exposed, and partial key exposure attacks' aim is to break RSA from these exposed partial bits. Low private exponent attacks on RSA are those targeting at RSA with small private exponent, and Boneh and Durfee

* 基金项目: 国家自然科学基金(61272484,11531002); 国防科技大学科研计划项目(CJ13-02-01); 湖南省自然科学基金(13JJ4005)
收稿日期: 2015-04-27 定稿日期: 2015-09-09

presented the best result known so far. As for the attacks on RSA with exposed least significant bits of the private key, they are important partial key exposure attacks and closely related to low private exponent attacks. Based on Coppersmith's method for finding small roots of modular polynomial equations and the technique of unraveled linearization, this paper presents a new attack with exposed least significant bits of the private key. The technique of unraveled linearization arises from Herrmann and May's elementary proof of Boneh and Durfee's result of low private exponent attacks. Notice that known attacks with exposed least significant bits of the private key only care about how many bits are exposed, while this paper also cares about what the value of each exposed bit is. Under certain condition for the values of the exposed bits, our result improves the result of Ernst et al. Additionally, Ernst et al. only considers the special case where public exponent is roughly equal to RSA modulus, while this paper further studies the general case where public exponent is less than RSA modulus.

Key words: RSA; exposed least significant bits; Coppersmith's method; lattice; LLL algorithm

1 引言

1977 年, 麻省理工学院的 Rivest, Shamir 和 Aldeman 提出了著名的公钥密码算法 RSA[1]. 设 M 为明文, C 为密文, 则加密过程为 $C \equiv M^e \bmod N$, 解密过程为 $M \equiv C^d \bmod N$. 其中 RSA 模 N 为两个大素数 p,q 的乘积, 加密指数 e 与解密指数 d 满足 $e \cdot d \equiv 1 \bmod \varphi(N)$, $\varphi(\cdot)$ 为欧拉函数, 也称 d 为私钥.

RSA 密码的应用非常广泛, 因此密码分析工作也显得十分重要. 在基于格的 RSA 密码分析中, Coppersmith 方法起着关键的作用. Coppersmith 方法通过格基约化算法来解决 v 元模多项式方程(或者 $v+1$ 元整系数多项式方程)求小值解的问题. 最初在 1996 年的欧密会上, Coppersmith 得到了 $v=1$ 时关于模多项式方程、整系数方程的两个结论[2,3], 并在 1997 年总结完善[4]. 单变元模方程方面, 设 δ 次的首一多项式 $f(x) \in \mathbb{Z}[x]$, 以及常数 $X \leqslant N^{1/\delta}$, 那么在关于 $(\log_2 N, 2^\delta)$ 的多项式时间内就可找到满足 $|x_0| \leqslant X$, $f(x_0) \equiv 0 \bmod N$ 的所有整数解 x_0 (文献[4]的推论 1). 双变元整系数方程方面, 设不可约多项式 $p(x,y) \in \mathbb{Z}[x,y]$, δ 为 $p(x,y)$ 中 x 或者 y 的次数的最大值, W 表示 $p(xX, yY)$ 中系数的绝对值的最大值, 其中 $XY \leqslant W^{2/(3\delta)}$, 那么在关于 $(\log_2 W, 2^\delta)$ 的多项式时间内就可找到满足 $|x_0| \leqslant X, |y_0| \leqslant Y, p(x_0, y_0) = 0$ 的所有整数解 (x_0, y_0) (文献[4]的推论 2). 后来, Howgrave-Graham[5]与 Coron[6]分别在 1997 年与 2004 年改进了 Coppersmith 这两个结论的证明方法, 并为学者们广泛应用于 RSA 密码分析中. 一般来说, Coppersmith 方法即指 Howgrave-Graham 与 Coron 的证明方法及其在 $v \geqslant 2$ 情况下的推广. 当 $v \geqslant 2$ 时, 所得的分析结果都是启发式的, 因为此时 Coppersmith 方法要用到相应的结式求解假设.

现实中, 通过错误攻击[7]、时间攻击[8]和能量分析[9]等侧信道攻击, 攻击者能够恢复私钥 d 的部分比特位, 但是难以恢复整个私钥 d. 例如文献[8]中指出, 可以根据 RSA 解密运行时间与私钥 d 取值的相关性, 按照最低位到最高位的顺序, 逐个恢复私钥 d 每一比特位的取值. 因为每次恢复比特位的取值都有失败的风险, 所以恢复的比特位数越多, 成功概率也就越低. 在侧信道攻击的基础上, 一类攻击关注在泄露(即恢复)私钥 d 的多少比特位后, 就能够在多项式时间内破解 RSA 密码. 这类攻击称为针对 RSA 密码的部分私钥泄露攻击, 并且绝大部分都基于 Coppersmith 方法. 1998 年, Boneh, Durfee 和 Frankel 根据文献[3]中的一个推论, 首次提出了部分私钥泄露攻击[10]. 记 MSBs 为最高几位比特(Most Significant Bits), LSBs 为最低几位比特(Least Significant Bits). 设 $N = pq$ 为 n 比特的 RSA 模, 满足 $N^{0.5}/2 < q < p < 2N^{0.5}$. Boneh 等人指出, 泄露 d 的 $n/4$ 的 LSBs, 就可以在关于 n 为多项式、关于 e 为线性的时间内分解 RSA 模 N, 该结果只适用于加密指数 e 取值较小的情况. Boneh 等人的其他结果, 需要泄露 d 的一些 MSBs, 包括 e 的素因子分解式已知与未知两种情况, 不过只适用于 e 大致小于 $N^{1/2}$ 的范围. 与文献[10]一样, 目前部分私钥泄露攻击主要研究的是针对 RSA 密码私钥的 MSBs 泄露攻击或者 LSBs 泄露攻击. 当 e 明显大于 $N^{1/2}$ 时, Boneh, Durfee

和 Frankel 的结论不再成立, 为此文献[10]中的一个开放性问题即为如何给出 $e > N^{1/2}$ 情形下的 MSBs 泄露攻击或者 LSBs 泄露攻击. 后来, Blomer 和 May[11]于 2003 年、Ernst 等人[12]于 2005 年, 基于 Coppersmith 方法分别提出了新的部分私钥泄露攻击, 从而解决了文献[10]中的这个开放性问题. 其中文献[12]首次给出了 $e \approx N$ 时的部分私钥泄露攻击. 2009 年, Aono 改进了文献[12]在 LSBs 泄露攻击方面的部分结果[13]. 2010 年, Sarkar 等人则在一定程度上改进了文献[12]中的 MSBs 泄露攻击[14]. 2012 年, Joye 和 Lepoint 提出了针对 $d > N$ 情形下的部分私钥泄露攻击[15]. 2014 年, 黄章杰、胡磊等人提出了针对 RSA 密码 Takagi 变体的部分私钥泄露攻击[16]. Takagi 变体假设 RSA 模 $N = p^j q$, $j \geqslant 1$, 文献[16]中的 LSBs 泄露攻击结果, 在 $j = 1$ 时与文献[12]中的结果是一样的, 所以可以看成文献[12]中的 LSBs 泄露攻击结果在 Takagi 变体上的推广. 注意到目前已知的 LSBs 泄露攻击只关注所泄露比特的位数, 本文进一步还关注所泄露比特的取值. 本文的主要内容, 是在所泄露比特的某些取值情况下改进文献[12]在 LSBs 泄露攻击方面的部分结果.

1990 年, Wiener 利用连分数的方法首次提出了针对 RSA 密码的低解密指数攻击[17]. 1999 年, Boneh 和 Durfee 基于 Coppersmith 方法改进了 Wiener 的结果[18]. 他们指出, 只要解密指数 $d \leqslant N^{1-\sqrt{2}/2-\varepsilon} \approx N^{0.292-\varepsilon}$, 就有可能在多项式时间内分解 RSA 模 N. 这是至今低解密指数攻击中最好的结果. 在文献[18]的正文中, Boneh 和 Durfee 只给出了 $d \leqslant N^{7/6-\sqrt{7}/3-\varepsilon} \approx N^{0.285-\varepsilon}$ 的证明, 而把 $d \leqslant N^{0.292-\varepsilon}$ 的证明放在了附录里, 后者是一个非常繁琐复杂的过程, 并且独立于文献[18]中正文的整体证明思想. 2010 年, Herrmann 和 May 进行了线性化模方程的处理, 进而给出了 $d \leqslant N^{0.292-\varepsilon}$ 的简化证明[19]. 低解密指数攻击可以看作是 LSBs 泄露攻击的一种特殊情况. 如果把文献[18]中低解密指数攻击 $d \leqslant N^{0.285-\varepsilon}$ 的证明方法推广到 LSBs 泄露攻击上, 就能得到文献[12]的相应结果. 本文通过把文献[19]对于低解密指数攻击 $d \leqslant N^{0.292-\varepsilon}$ 的证明方法推广到 LSBs 泄露攻击上, 从而在某些情况下改进文献[12]中相应结果的部分内容.

本文结构如下. 第 2 节首先回顾已知相关工作[12,13,18], 再给出本文结果, 并进行比较. 第 3 节从 LSBs 泄露的条件推导出模方程求小值解的问题, 接着介绍解决求小值解问题的 Coppersmith 方法. 基于此方法, 第 4 节给出本文所构造的格, 并在一系列计算与分析之后证明了本文的攻击结果. 第 5 节通过一些实验, 检验了所涉及的结式求解假设, 同时验证了本文的证明原理. 第 6 节是本文的结论.

2 相关工作及主要结果

在实践中, RSA 模 $N = pq$ 中 p 与 q 的比特位数大致相等, 所以与绝大多数部分私钥泄露攻击一样, 本文假设 $N^{0.5}/2 < q < p < 2N^{0.5}$. 规定 $e = N^{\alpha}$, $d \leqslant N^{\beta}$, N 的比特位数为 n, d 的比特位数为 n_d, 再令 $d = d_1 \cdot 2^r + d_2$, 其中 $0 < r < n_d$, $0 \leqslant d_1 < 2^{n_d - r}$, $0 \leqslant d_2 < 2^r$. 假设现实中, 利用侧信道攻击等手段, 获得了 d_2 与 r, 但 d_1 仍然未知. 定义 $\delta = \log_N 2^r$, 也即 $2^r = N^{\delta}$. 本文所研究的 LSBs 泄露攻击即为, 当 α, β, δ 满足什么条件时, 就能够在多项式时间内分解 RSA 模 N. 本节首先回顾一些已知的相关工作, 然后陈述本文的主要结果. 文献[12,13,18,19]等基本上考虑的都是 $e \approx N$ 的情况, 所以本文重点陈述这种情况, 之后再说明任意 $e < N$ 的情况. 实际上本文所涉及的低解密指数攻击与部分私钥泄露攻击, 当 e 越小时结果越好. 最后指出, 与绝大多数部分私钥泄露攻击一样, 已知结果与本文结果都要用到类似于假设 1(见 3.2 节)的结式求解假设.

2.1 $e \approx N$ 的情况

当 $e \approx N$ 也即 $\alpha \approx 1$ 时, 文献[12,13,18]中结果以及本文结果如图 1 所示. 不妨假设 $d \approx N^{\beta}$. 图 1 横坐标是 β 的取值, 纵坐标是比例 δ/β 的取值, 大致表示所泄露 LSBs 比特数占私钥 d 比特数的比重. 对于针对 RSA 密码私钥的 LSBs 泄露攻击, 在 $\alpha \approx 1$ 情况下, 如果 β, δ 的值使得点 $(\beta, \delta/\beta)$ 落在了线<1>的左方(绿色区域), 或者落在了线<2><3><4>的上方(青蓝色、紫红色、红色区域), 那么基于结式求解假设就能够在多项式时间内分解 RSA 模 N, 其中当点 $(\beta, \delta/\beta)$ 落在线<4>的上方(红色区域)时, 还需满足条件 $d_2 < N^{\beta - 0.5}$.

图 1 中的线<1>, 即为 $\beta=1-\sqrt{2}/2\approx 0.292$, 是指 1999 年 Boneh 和 Durfee 得到的至今最好的低解密指数攻击结果 $\beta\leqslant 0.292-\varepsilon$ [18]. 线<2>指 Ernst 等人在 2005 年的结果, 为文献[12]中的定理 3, 重述如下:

结果 1[12] 符号规定如上文所述. 在假设 1 成立的基础上, 对任意小的 $\varepsilon>0$, 存在大整数 N_0, 使得当 $N>N_0$ 时, 只要

$$\beta-\delta\leqslant\frac{5}{6}-\frac{1}{3}\sqrt{6\beta+1}-\varepsilon \tag{1}$$

成立, 就可以在多项式时间内有效分解 RSA 模 N.

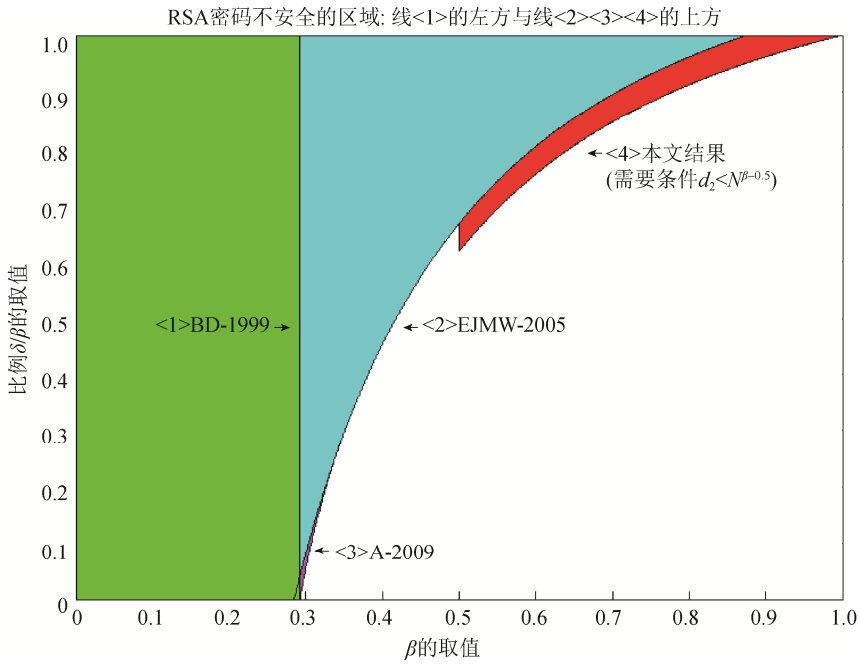


图 1 已知结果与本文结果

Figure 1 Known Results and Our Result

当 $\delta=0$ 时, 根据式(1)得到低解密指数攻击结果 $\beta\leqslant 7/6-\sqrt{7}/3-\varepsilon\approx 0.285-\varepsilon$, 这对应着线<2>左边的起点 $(0.285,0)$ (在线<1>的左方), 另外线<2>右边的终点为 $(0.875,1.0)$. 图 1 中的线<3>在 $0.285<\beta<3/4-\sqrt{21}/12\approx 0.368$ 的范围内改进了结果 1, 具体内容参见 2009 年 Aono 的工作[13]. 线<3>左边的起点为 $(0.292,0)$, 位于线<1>上, 因此文献[18]的结果 $\beta\leqslant 0.292-\varepsilon$ 可以看作是文献[13]的结果的特例. 线<3>右边的终点为 $(0.368,0.358)$, 位于线<2>上, 实际上当 $\beta\geqslant 0.368$ 时, Aono 的结果与结果 1 一样. 对于 $0.5<\beta<1.0$ 的范围, 当所泄露的 d_2 满足一定条件时, 本文给出线<4>对应的如下结果:

定理 1 符号规定如上文所述, 并且要求条件 $d_2<N^{\beta-0.5}$ 成立. 在假设 1 成立的基础上, 对任意小的 $\varepsilon>0$ (或者 $\varepsilon'>0$), 存在大整数 N_0, 使得当 $N>N_0$ 时, 只要

$$\beta-\delta\leqslant\frac{3}{4}-\frac{1}{4}\sqrt{8\beta+1}-\varepsilon \tag{2}$$

$$\Leftrightarrow \quad \beta \leqslant \delta + 1 - \frac{\sqrt{2}}{2}\sqrt{\delta + 1} - \varepsilon' \tag{3}$$

成立, 就可以在多项式时间内有效分解 RSA 模 N.

在定理 1 中, 式(2)与式(3)等价. 式(3)在实际中更有意义. 在本文攻击中, 为了构造相应的格需要知道 N,α,β,δ 的值, 其中 N,α,δ 是已知的, 从式(3)可以得到 β 的一个值, 如果 $d \leqslant N^{\beta}$ 成立, 那么就能实现攻击. 当 $\beta > 0$ 时, 关于式(1)与式(2)的右边, 总有 $5/6 - \sqrt{6\beta + 1}/3 < 3/4 - \sqrt{8\beta + 1}/4$ 成立. 所以在 $d_2 < N^{\beta - 0.5}\left(0.5 < \beta < 1.0\right)$ 的情况下, 定理 1 的结果优于结果 1. 这通过图 1 也可以看出. 当然结果 1 考虑的是一般形式下的私钥泄露攻击, 而本文的定理 1 是一种特殊情况下的私钥泄露攻击, 即还需要条件 $d_2 < N^{\beta - 0.5}$, 而这意味着, 私钥 d 中间位置的一部分比特不仅泄露而且要求为连续的零. 例如当 $\beta = 0.6$ 时, 为了使式(2)成立, 至少大约需要 $\delta = 0.45$, 同时由条件 $d_2 < N^{\beta - 0.5}$ 得到 $d_2 < N^{0.1}$. 这意味着, 共有 $0.6\log_2 N$ 比特位的私钥 d, 需要泄露 $0.45\log_2 N$ 低比特位, 尽管少于结果 1 的 $0.48\log_2 N$ 低比特位, 但是要求私钥 d 从第 $0.1\log_2 N$ 位到第 $0.45\log_2 N$ 位的中间比特均为 0.

若 $\delta = 0$ 即 $r = 0, d_2 = 0$, 意味着 RSA 没有泄露任何的 LSBs, $d_2 < N^{\beta - 0.5}$ 对任意的 β 总是成立的. 此时根据式(3)可以得到 $\beta \leqslant 1 - \sqrt{2}/2 - \varepsilon' \approx 0.292 - \varepsilon'$. 定理 1 在此种情况下的证明, 正是文献[19]对文献[18]中结果的简化证明. 本文考虑 $\delta > 0$ 的情况, 根据 $e \cdot d \equiv 1 \bmod \varphi(N)$ 与 $N = pq$ 可知私钥 d 一定是奇数, 所以 d 的最末位比特一定是 1, 意味着 $d_2 \geqslant 1$. 因此条件 $d_2 < N^{\beta - 0.5}$ 也蕴含着 $\beta > 0.5$. 线<4>左边的起点为 $(0.5, 0.618)$, 右边的终点为 $(1.0, 1.0)$. 注意到线<2>右边的终点为 $(0.875, 1.0)$, 所以定理 1 使得 $0.875 < \beta < 1.0$ 范围下的 LSBs 泄露攻击也成为可能.

2.2 任意 $e < N$ 的情况

对于任意的 $e = N^{\alpha} < N$, 运用文献[12]中定理 3 的证明方法, 可以得到相应的推广结果: 只需要把结果 1 中的式(1)替换为

$$\beta - \delta \leqslant \frac{5}{6} - \frac{1}{3}\sqrt{6(\alpha + \beta) - 5} - \varepsilon \tag{4}$$

即可. 此处略去证明过程. 需要指出的是, 对于 $d \approx N (\beta \approx 1)$ 和任意的 $e = N^{\alpha} < N$, Blomer 和 May 在 2003 年得到的 LSBs 泄露攻击结果(文献[11]的定理 11), 即为式(4)中令 $\beta \approx 1$ 的特殊情况.

对于任意的 $e = N^{\alpha} < N$, 本文的定理 1 也有相应的推广结果, 条件 $d_2 < N^{\beta - 0.5}$ 不变, 只需要把式(2)与式(3)替换为下面的式(5)与式(6)即可:

$$\beta - \delta \leqslant \frac{3}{4} - \frac{1}{4}\sqrt{8(\alpha + \beta) - 7} - \varepsilon \tag{5}$$

$$\Leftrightarrow \quad \beta \leqslant \delta + 1 - \frac{\sqrt{2}}{2}\sqrt{\delta + \alpha} - \varepsilon' \tag{6}$$

同样, 式(5)的结果优于式(4)的结果. 本文接下来, 将针对任意的 $e = N^{\alpha} < N$, 证明定理 1 推广后的结果, 即式(5).

3 模多项式方程求小值解

3.1 LSBs泄露攻击的问题转换

因为 $e \cdot d \equiv 1 \bmod \varphi(N)$, 所以存在一个正整数 k, 使得

$$1=ed-k\varphi(N)=e\left(d_1\cdot 2^r+d_2\right)-k\left[N-\left(p+q-1\right)\right]$$

令 $A=e\cdot d_2-1$，$W=e\cdot 2^r=N^{\alpha+\delta}$，用 W 模去上式得到

$$A-N\cdot k+k\cdot\left(p+q-1\right)\equiv 0 \bmod W$$

其中 $k, p+q-1$ 是未知的. 根据假设 $N^{0.5}/2<q<p<2N^{0.5}$ 以及 $2\varphi(N)>N$, 有

$$0<k=\left(ed-1\right)/\varphi(N)<2ed/N=2N^{\alpha+\beta-1}$$

$$0<p+q-1<p+q<3N^{0.5}$$

至此得到如下的双变元模多项式方程求小值解问题:

$$A-N\cdot x+x\cdot y\equiv 0 \bmod W$$

$$|x|<X=2N^{\alpha+\beta-1}$$

$$|y|<Y=3N^{0.5}$$

类似于文献[19]进行线性化模方程的处理, 令 $u=x\cdot y+A$. 根据条件 $d_2<N^{\beta-0.5}$, 得到 $A=e\cdot d_2-1<N^{\alpha+\beta-0.5}$, 又 $x\cdot y<XY=6N^{\alpha+\beta-0.5}$, 故 $0<u=x\cdot y+A<7N^{\alpha+\beta-0.5}$. 所以, 在 $d_2<N^{\beta-0.5}$ 的情况下, 得到了新的求小值解问题:

$$\begin{aligned}&-N\cdot x+u\equiv 0 \bmod W\\&|x|<X=N^{\alpha+\beta-1}\\&|y|<Y=3N^{0.5}\\&|u|<U=7N^{\alpha+\beta-0.5}\end{aligned}\tag{7}$$

所要求的小值解为

$$(x,y,u)=(x_0,y_0,u_0)=(x_0,y_0,x_0y_0+A)=\left(k,p+q-1,k\left(p+q-1\right)+A\right)$$

当得到 $\left(k,p+q-1,k\left(p+q-1\right)+A\right)$ 的值后, 即可算得 $\left(p+q-1\right)$ 的值, 进而可以很快分解 RSA 模 N. 实际攻击中, 将获得满足式(7)的所有小值解, 从而得到有限个 $\left(p+q-1\right)$ 的备选值, 依次尝试直到分解 RSA 模 N 即可.

3.2 Coppersmith方法

为了获得满足式(7)的所有小值解, 需要引入 Coppersmith 方法. 为此首先介绍格的定义.

定义 1 格是 s 维欧式空间 $\mathbb{R}^s$ 的一个离散加法子群. 等价地说, 格 Λ 是 $\mathbb{R}^s$ 中 $\omega\left(\omega\leqslant s\right)$ 个线性无关的向量 $\vec{b_1},\vec{b_2},\cdots,\vec{b_\omega}$ 的所有整系数线性组合构成的集合, 即

$$\Lambda=\mathrm{span}_{\mathbb{Z}}\left(\vec{b_1},\vec{b_2},\cdots,\vec{b_\omega}\right)=\left\{\sum_{i=1}^{\omega}x_i\vec{b_i}\,|x_i\in\mathbb{Z},i=1,2,\cdots,\omega\right\}$$

其中, s,ω 分别称为格 Λ 的维数与秩, 向量组 $\vec{b_1},\vec{b_2},\cdots,\vec{b_\omega}$ 称为格 Λ 的一组基. 把基中的向量视为行向量, 则可以用矩阵的形式来表示这组基, 得到格 Λ 的基矩阵:

$$\mathcal{B}=\begin{pmatrix}\vec{b_1}\\\vec{b_2}\\\cdots\\\vec{b_\omega}\end{pmatrix}\in\mathbb{R}^{\omega\times s}$$

格 Λ 的行列式定义为 $\det(\Lambda)=\sqrt{\det(\mathcal{B}\mathcal{B}^{\mathrm{T}})}$，这是格 Λ 本身的性质，并不会因为基的选取不同而不同. 本文所涉及的格都满足条件 $s=\omega$，即为满秩格. 此时 $\mathcal{B}$ 为方阵，$\det(\Lambda)=|\det\mathcal{B}|$.

1982 年, Lenstra, Lenstra, Lovasz 三人提出了一种著名的格基约化算法——LLL 算法[20]，其能够在多项式时间内找到格中的短向量. 关于 LLL 算法有如下的事实，证明参见文献[21].

事实 1[21] 设格 Λ 的维数与秩均为 s. 输入 Λ 的一个格基方阵 $\mathcal{B}$，LLL 算法在关于 s 与 $\mathcal{B}$ 中元素比特长度的多项式时间内，可以输出一组 LLL-约化基 $\vec{v}_1,\vec{v}_2,\cdots,\vec{v}_s$，满足

$$\left\|\vec{v}_i\right\|\leqslant 2^{s(s-1)/4(s-i+1)}\det(\Lambda)^{1/(s-i+1)},1\leqslant i\leqslant s$$

其中向量 $\vec{v}_i=(v_{i1},v_{i2},\cdots,v_{is})$ 的范数 $\left\|\vec{v}_i\right\|=\sqrt{v_{i1}^2+v_{i2}^2+\cdots+v_{is}^2}$.

接着介绍 1997 年 Howgrave-Graham 在文献[5]中的一个引理.

引理 1[5] 如果多项式 $h(x_1,x_2,\cdots,x_v)\in\mathbb{Z}[x_1,x_2,\cdots,x_v]$ 中含有至多 s 个单项式，且存在 $(x_1^{(0)},x_2^{(0)},\cdots,x_v^{(0)})\in\mathbb{Z}^v$ 满足下面两个条件:

(1) $h(x_1^{(0)},x_2^{(0)},\cdots,x_v^{(0)})\equiv 0 \bmod V,|x_1^{(0)}|<X_1,\cdots,|x_v^{(0)}|<X_v$;

(2) $\left\|h(X_1x_1,X_2x_2,\cdots,X_vx_v)\right\|<V/\sqrt{s}$ (这里多项式 $g(x_1,x_2,\cdots,x_v)=\sum a_{t_1,t_2,\cdots,t_v}x_1^{t_1}x_2^{t_2}\cdots x_v^{t_v}$ 的范数 $\left\|g(x_1,x_2,\cdots,x_v)\right\|=\sqrt{\sum\left|a_{t_1,t_2,\cdots,t_v}\right|^2}$).

那么就在整数意义上得到 $h(x_1^{(0)},x_2^{(0)},\cdots,x_v^{(0)})=0$.

联合事实 1 与引理 1, 可以分析模多项式方程小值解的上界，此为基于格的 RSA 密码分析中通常采用的 Coppersmith 方法. 下面即以本文考虑的情况 $v=2$ 为例，简要总结 Coppersmith 方法在 v 元模多项式方程求小值解问题的应用过程.

双变元模多项式方程求小值解，即求出满足 $h_0(x_1,x_2)\equiv 0 \bmod W,|x_1|<X_1,|x_2|<X_2$ 的每一个解 $(x_1^{(0)},x_2^{(0)})\in\mathbb{Z}^2$. 设定参数 m，寻找 $\mathbb{Z}[x_1,x_2]$ 的一个子集 Λ^*，使得

$$h(x_1^{(0)},x_2^{(0)})\equiv 0 \bmod W^m,\forall\, h(x_1,x_2)\in\Lambda^*$$

规定 $\mathbb{Z}[x_1,x_2]$ 中一些单项式的排序，使得 Λ^* 中的任意多项式 $h(x_1,x_2)$ 都一一对应于 $\mathbb{R}^s$ 中的一个向量，即为 $h(X_1x_1,X_2x_2)$ 的各项系数按照相应的单项式排序构成的向量. 按照这种一一对应，多项式集合 Λ^* 需要等同于 $\mathbb{R}^s$ 中的一个 s 维满秩格 Λ. 根据事实 1$(i=2)$ 与引理 1$(v=2)$，如果

$$2^{s/4}\det(\Lambda)^{1/(s-1)}<W^m/\sqrt{s} \tag{8}$$

成立，运用 LLL 算法就可以得到两个多项式 $h_1(x_1,x_2)$ 和 $h_2(x_1,x_2)$，它们都在整数意义上以所求的每一个解 $(x_1^{(0)},x_2^{(0)})\in\mathbb{Z}^2$ 为根. 之后 Coppersmith 方法需要如下的假设.

假设 1 对于双变元模多项式方程求小值解的情况，Coppersmith 方法最后通过 LLL 算法获得的两个多项式 $h_1(x_1,x_2)$ 和 $h_2(x_1,x_2)$，可以通过建立结式进行消元求解，从而得到所有的小值解 $(x_1^{(0)},x_2^{(0)})\in\mathbb{Z}^2$.

假设 1 联合其在更多变元情况下的推广，即为结式求解假设，是基于 Coppersmith 方法的 RSA 密码分析中普遍采用的假设. 第 5 节将通过实验来阐释并检验本文结果所涉及到的假设 1.

式(8)等价于

$$\det(\Lambda)T_1(s)<W^{m(s-1)},T_1(s)=2^{s(s-1)/4}s^{(s-1)/2} \tag{9}$$

根据以上分析, 在假设 1 成立的基础下, 利用 Coppersmith 方法解决双变元模多项式方程求小值解问题, 只需要式(9)成立即可.

4 主要结果的证明

设 $f(x,y,u)=-N\cdot x+u$. 根据第 3.1 节可知, 对于 $d_2<N^{\beta-0.5}$ 情况下的 LSBs 泄露攻击, 只需要找到满足

$$f(x,y,u)\equiv 0 \bmod W,|x|<X,|y|<Y,|u|<U$$

的小值解 $(x,y,u)=(x_0,y_0,u_0)=(x_0,y_0,x_0y_0+A)=(k,p+q-1,k(p+q-1)+A)$, 其中

$$A=e\cdot d_2-1,\ W=e\cdot 2^r=N^{\alpha+\delta},\ X=2N^{\alpha+\beta-1},\quad Y=3N^{0.5},\ U=7N^{\alpha+\beta-0.5}.$$

4.1 格的构造

下面构造本文攻击所用到的格 Λ, 设 Λ 的格基方阵为 $\mathcal{B}$. 图 2 以分块矩阵的方式给出了格基方阵 $\mathcal{B}$, 其中的 $\mathcal{G}_t,\mathcal{P}_i$ 等表示 $\mathcal{B}$ 中相应位置的子矩阵, 单项式集合 $\mathrm{G}_t,\mathrm{P}_i$ 等以及多项式集合 $\mathrm{G}_t^*,\mathrm{P}_i^*$ 等分别用来辅助说明 $\mathcal{G}_t,\mathcal{P}_i$ 等对应的列与行.

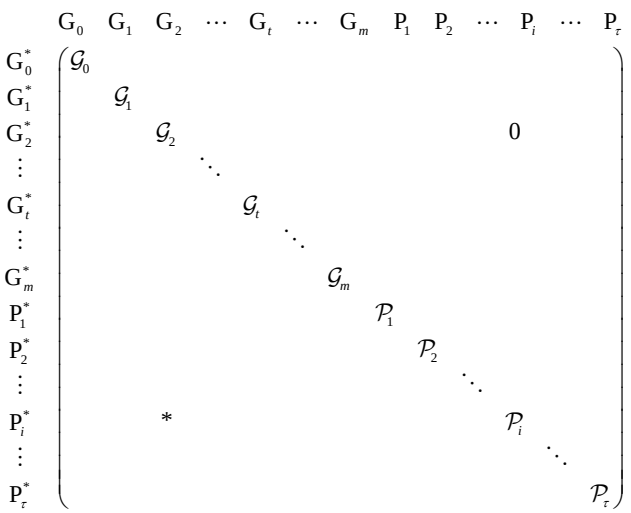


图 2 格基方阵 $\mathcal{B}$

Figure 2 Basis Square Matrix $\mathcal{B}$

设非负整数 m,τ 为待定参数. 对 $t=0,1,2,\cdots,m$ 和 $i=1,2,\cdots,\tau$, 图 2 中的单项式集合 G_t 与 P_i 以及多项式集合 G_t^* 与 P_i^* 定义如下:

$$\mathrm{G}_t=\left\{x^{t-j}u^j\,\middle|\,j=0,1,2,\cdots,t\right\},\ \mathrm{G}_t^*=\left\{x^{t-j}f^jW^{m-j}\,\middle|\,j=0,1,2,\cdots,t\right\}$$

$$\mathrm{P}_i=\left\{y^i\cdot u^j\,\middle|\,j=\theta_i,\theta_i+1,\theta_i+2,\cdots,m\right\},\ \mathrm{P}_i^*=\left\{y^i\cdot f^jW^{m-j}\,\middle|\,j=\theta_i,\theta_i+1,\theta_i+2,\cdots,m\right\}$$

其中 x^0,y^0,u^0,f^0 等都看作 1. 另外, 尽管集合 $\mathrm{G}_t^*,\mathrm{P}_i,\mathrm{P}_i^*$ 的定义还与参数 m 有关, 但是方便起见, 下标中均省去 m. $\mathrm{P}_i,\mathrm{P}_i^*$ 定义中的非负整数 θ_i 是另外一个重要的待定参数, 其的优化选取是改进结果 1 的关键. 定

义总的单项式集合 B 与总的多项式集合 B^* 如下:

$$\mathrm{B}=\mathrm{B}_1\bigcup\mathrm{B}_2,\mathrm{B}_1=\bigcup_{t=0}^{m}\mathrm{G}_t,\mathrm{B}_2=\bigcup_{i=1}^{r}\mathrm{P}_i$$

$$\mathrm{B}^*=\mathrm{B}_1^*\bigcup\mathrm{B}_2^*,\mathrm{B}_1^*=\bigcup_{t=0}^{m}\mathrm{G}_t^*,\mathrm{B}_2^*=\bigcup_{i=1}^{r}\mathrm{P}_i^*$$

接下来在单项式集合 B 上定义一个全序“$\leqslant$”. 任取 $h(x,y,u),h'(x,y,u)\in\mathrm{B}$, 那么 $h(x,y,u)\leqslant h'(x,y,u)$ 当且仅当下述情形之一成立:

(1) $h(x,y,u)\in\mathrm{B}_1, h'(x,y,u)\in\mathrm{B}_2$;

(2) $h(x,y,u)=x^{t-j}u^j\in\mathrm{G}_t\subset\mathrm{B}_1$, $h'(x,y,u)=x^{t'-j'}u^{j'}\in\mathrm{G}_{t'}\subset\mathrm{B}_1$, 并且 $t<t'$ 或者 $t=t', j\leqslant j'$;

(3) $h(x,y,u)=y^j\cdot u^j\in\mathrm{P}_i\subset\mathrm{B}_2$, $h'(x,y,u)=y^{i'}\cdot u^{j'}\in\mathrm{P}_{i'}\subset\mathrm{B}_2$, 并且 $i<i'$ 或者 $i=i', j\leqslant j'$.

类似地, 可以在多项式集合 B^* 上定义全序“$\leqslant^*$”.

现在根据图 2 来说明 $\mathcal{B}$ 的构造. 对于集合 B^* 中的任一多项式 $g(x,y,u)$, 将其展开成单项式相加的形式, 然后根据关系式 $u=xy+A$, 把其中的项 xy 都替换成 $u-A$ 后, 再次展开成单项式相加的形式. 下面的命题 4.1 将证明, 在一些情况下, 忽略系数后这些单项式都属于集合 B. 因此 $g(x,y,u)$ 对应一个行向量, 其分量为 $g(Xx,Yy,Uu)$ 展开后各单项式的系数, 分量的左右顺序, 即由系数对应的单项式的全序“$\leq$”决定. 最后, 由全序“$\leqslant^*$”决定上下顺序, 把集合 B^* 中的多项式对应的行向量进行排列, 就得到了方阵 $\mathcal{B}$.

表 1 $m=2,\tau=2,\theta_1=1,\theta_2=2$ 时的格基方阵 $\mathcal{B}$

Table 1 Basis Square Matrix $\mathcal{B}$ with $m=2,\tau=2,\theta_1=1,\theta_2=2$

	1	x	u	x^2	xu	u^2	yu	yu^2	y^2u^2
W^2	W^2								
xW^2	0	XW^2							
fW	0	*	UW						
x^2W^2	0	0	0	X^2W^2					
xfW	0	0	0	*	XUW				
f^2	0	0	0	*	*	U^2			
yfW	*	0	*	0	0	0	YUW		
yf^2	0	*	*	0	*	*	0	YU^2	
y^2f^2	*	0	*	0	0	*	*	*	Y^2U^2

例如, 当取 $m=2,\tau=2,\theta_1=1,\theta_2=2$ 时, 方阵 $\mathcal{B}$ 如表 1 所示. 接着再以表 1 中的 yfW 为例, 说明多项式与向量的对应关系. 因为 $yfW=y(-Nx+u)W=(-Nxy+yu)W=\left[-N(u-A)+yu\right]W=(NA-Nu+yu)W$, 另外单项式集合 B 中的元素按照全序“$\leqslant$”排列为 $1,x,u,x^2,xu,u^2,yu,yu^2,y^2u^2$, 所以多项式 yfW 对应的向量为 $(NAW,0,-NUW,0,0,0,YUW,0,0)$. 注意到表 1 中的方阵 $\mathcal{B}$ 是一个下三角方阵, 实际上关于方阵 $\mathcal{B}$ 我们有如下结论:

命题 1 如果 $\theta_{i+1}\geqslant\theta_i+1(i=1,2,\cdots,\tau-1)$, 那么 $\mathcal{B}$ 是格基方阵, 且为下三角方阵.

证明: $\mathcal{B}$ 是格基方阵, 即指(1)集合 B^* 中的任意多项式, 其所含的单项式(默认忽略系数)都属于集合 B, 即 $\mathcal{B}$ 作为方阵其构造是合理的; (2)方阵 $\mathcal{B}$ 的行向量是线性无关的. 只需证明 $\mathcal{B}$ 为下三角方阵, 一方面需要先证明(1), 另一方面自然推出(2).

对 $t=0,1,2,\cdots,m$, 任取 $h_1(x,y,u)=x^{t-j}f^jW^{m-j}\in \mathrm{G}_t^*\subset \mathrm{B}_1^*$, 其中 $j=0,1,2,\cdots,t$. 那么 $h_1(x,y,u)$ 所含的单项式为 $x^{t-j_1}u^{j_1}$, $j_1=0,1,2,\cdots,j$, 它们都属于集合 B_1, 并且根据全序"≤"的定义, 最右边的单项式是 $x^{t-j}u^j$.

对 $i=1,2,\cdots,\tau$, 任取 $h_2(x,y,u)=y^i\cdot f^jW^{m-j}\in \mathrm{P}_i^*\subset \mathrm{B}_2^*$, 其中 $j=\theta_i,\theta_i+1,\theta_i+2,\cdots,m$. 那么 $h_2(x,y,u)$ 所含的单项式为 $y^ix^{j-j_1}u^{j_1}$, $j_1=0,1,2,\cdots,j$. 如果 $i\leqslant j-j_1$, 那么

$$y^ix^{j-j_1}u^{j_1}=x^{j-j_1-i}(xy)^iu^{j_1}=x^{j-j_1-i}(u-A)^iu^{j_1}$$

对应的单项式为 $x^{j-j_1-i}u^{j_1+j_2}, j_2=0,1,\cdots,i$. 因为 $0\leqslant(j-j_1-i)+(j_1+j_2)\leqslant m$, 所以这些单项式都属于集合 B_1. 如果 $i>j-j_1$, 那么

$$y^ix^{j-j_1}u^{j_1}=y^{i-(j-j_1)}(xy)^{j-j_1}u^{j_1}=y^{i-(j-j_1)}(u-A)^{j-j_1}u^{j_1}$$

对应的单项式为 $y^{i-(j-j_1)}u^{j_1+j_2}, j_2=0,1,\cdots,j-j_1$. 根据命题 1 的条件 $\theta_{i^*+1}\geqslant\theta_{i^*}+1\left(i^*=1,2,\cdots,\tau-1\right)$, 可以推出 $\theta_i\geqslant\theta_{i-(j-j_1)}+j-j_1$. 联合 $j_2\geqslant 0, j\geqslant\theta_i$, 得到 $j_1+j_2\geqslant j_1=j-(j-j_1)\geqslant\theta_i-(j-j_1)\geqslant\theta_{i-(j-j_1)}$. 这表明这些单项式 $y^{i-(j-j_1)}u^{j_1+j_2}\left(j_2=0,1,2,\cdots,j-j_1\right)$ 都属于 B_2. 类似地根据全序"≤"的定义, 可知 $h_2(x,y,u)$ 所含的单项式中最右边的是 y^iu^j.

综上可知 $\mathcal{B}$ 作为方阵其构造是合理的. 因为 $h_1(x,y,u)=x^{t-j}f^jW^{m-j}$ 所含单项式中最右边的是 $x^{t-j}u^j$, $h_2(x,y,u)=y^i\cdot f^jW^{m-j}$ 所含单项式中最右边的是 y^iu^j, 所以 $\mathcal{B}$ 为下三角方阵, 命题 4.1 得证.

按照之前的规定, Λ 是由格基方阵 $\mathcal{B}$ 生成的满秩格. 根据定义可知, B^* 中任一多项式在模去 W^m 后都以 $(x_0,y_0,u_0)=(k,p+q-1,k(p+q-1)+A)$ 为根, 所以 Λ 中任一向量对应的多项式在模去 W^m 后也都以 $(x_0,y_0,u_0)=(k,p+q-1,k(p+q-1)+A)$ 为根. 格 Λ 满足 Coppersmith 方法的要求. 记 s 为满秩格 Λ 的维数, $s(\mathcal{B})$ 为方阵 $\mathcal{B}$ 的阶, 那么 $s=s(\mathcal{B})$. 另外 $\det(\Lambda)=|\det\mathcal{B}|=\det\mathcal{B}$, $\mathcal{B}$ 是一个下三角方阵, 所以 $\det(\Lambda)$ 等于 $\mathcal{B}$ 中主对角元素的乘积. 下面讨论如何在 $\theta_{i+1}\geqslant\theta_i+1$ 的前提条件下最优化 θ_i 的选取, 然后计算 s 与 $\det(\Lambda)$.

图 2 以分块矩阵的方式给出了格基方阵 $\mathcal{B}$, 其中, 对 $t=0,1,\cdots,m$, 分块方阵

$$\mathcal{G}_t=\begin{pmatrix} X^tW^m & & & & 0\\ & X^{t-1}UW^{m-1} & & & \\ & & X^{t-2}U^2W^{m-2} & & \\ & & & \ddots & \\ * & & & & U^tW^{m-t}\end{pmatrix}$$

对 $i=1,2,\cdots,\tau$, 分块方阵

$$\mathcal{P}_i=\begin{pmatrix} Y^iU^{\theta_i}W^{m-\theta_i} & & & & 0\\ & Y^iU^{\theta_i+1}W^{m-\theta_i-1} & & & \\ & & Y^iU^{\theta_i+2}W^{m-\theta_i-2} & & \\ & & & \ddots & \\ * & & & & Y^iU^m\end{pmatrix}$$

注意到实现攻击所需要的条件为式(9), 另外从下文可知其中的项 $T_1(s)$ 只对最后结果中的 ε 有贡献. 在式(9)中忽略项 $T_1(s)$ 得到 $\det(\Lambda)<W^{m(s-1)}$. 在 P_i 中放入 $y^i\cdot u^j$, P_i^* 中放入 $y^i\cdot f^jW^{m-j}$, 意味着不等式左边 $\det(\Lambda)$ 乘以 $Y^i\cdot U^jW^{m-j}$, 不等式右边 $W^{m(s-1)}$ 乘以 W^m, 为了优化最终结果, 需要 $Y^i\cdot U^jW^{m-j}\leqslant W^m$. 把 $Y=3N^{0.5}$ 粗略看作 $N^{0.5}$, 把 $U=7N^{\alpha+\beta-0.5}$ 粗略看作 $N^{\alpha+\beta-0.5}$, 忽略的系数也只对最后结果中的 ε 有贡献. 在 $Y^i\cdot U^jW^{m-j}\leqslant W^m$ 中代入 Y,U 与 $W=N^{\alpha+\delta}$, 最终推得 $j\geqslant i/2\eta$, 其中 $\eta=0.5-\beta+\delta=0.5-(\beta-\delta)>0$ (在这里指出, 本文的攻击需要条件 $\eta>0$, 攻击结果也自然蕴含了 $\eta>0$, 对于 $\eta\leqslant 0$ 的情况, 按照本文的格构造方法是失效的, 因为想要最优化攻击结果只能取 $\tau=0$, 从而最终得到 $0<\alpha+\beta-1+\varepsilon\leqslant\eta\leqslant 0$ 的矛盾). 注意到 j 为非负整数, 所以 $j\geqslant\lceil i/2\eta\rceil$ (上取整), 这也意味着选取 $\theta_i=\lceil i/2\eta\rceil$. 根据 $\eta<0.5$ 可知, 前提条件 $\theta_{i+1}\geqslant\theta_i+1$ 显然成立.

注意到 P_τ 与 P_τ^* 不能为空集, 也即 $\theta_\tau=\lceil\tau/2\eta\rceil\leqslant m$, 或者 $\tau/2\eta\leqslant m$ (m 为整数). 记 $\xi=\tau/m$, 则 $\tau=\xi m$, $0\leqslant\xi\leqslant 2\eta<1$. 关于格 Λ 的维数 s 与行列式 $\det(\Lambda)$, 在 $m\to\infty$ 的意义下, 经过计算可得

$$\begin{aligned}
s&=\sum_{t=0}^{m}s(\mathcal{G}_t)+\sum_{i=1}^{\tau}s(\mathcal{P}_i)=\sum_{t=0}^{m}(t+1)+\sum_{i=1}^{\xi m}\left(m-\lceil i/2\eta\rceil+1\right)\\
&=\left[\frac{1}{2}m^2+o\left(m^2\right)\right]+\left[\left(-\frac{1}{4\eta}\xi^2+\xi\right)m^2+o\left(m^2\right)\right]\\
&=\left(-\frac{1}{4\eta}\xi^2+\xi+\frac{1}{2}\right)m^2+o\left(m^2\right)
\end{aligned}$$

$$\begin{aligned}
\det(\Lambda)&=\prod_{t=0}^{m}(\det\mathcal{G}_t)\prod_{i=1}^{\tau}(\det\mathcal{P}_i)=\prod_{t=0}^{m}\prod_{j=0}^{t}X^{t-j}U^jW^{m-j}\prod_{i=1}^{\xi m}\prod_{j=\lceil i/2\eta\rceil}^{m}Y^iU^jW^{m-j}\\
&=\left[(XU)^{\frac{1}{6}m^3+o(m^3)}W^{\frac{1}{3}m^3+o(m^3)}\right]\cdot\left[Y^{\left(-\frac{1}{6\eta}\xi^3+\frac{1}{2^2}\xi^2\right)m^3+o(m^3)}U^{\left(-\frac{1}{24\eta^2}\xi^3+\frac{1}{2^2}\xi\right)m^3+o(m^3)}W^{\left(\frac{1}{24\eta^2}\xi^3-\frac{1}{4\eta}\xi^2+\frac{1}{2^2}\xi\right)m^3+o(m^3)}\right]\\
&=W^{\left(\frac{1}{24\eta^2}\xi^3-\frac{1}{4\eta}\xi^2+\frac{1}{2}\xi+\frac{1}{3}\right)m^3+o(m^3)}X^{\frac{1}{6}m^3+o(m^3)}Y^{\left(-\frac{1}{6\eta}\xi^3+\frac{1}{2^2}\xi^2\right)m^3+o(m^3)}U^{\left(-\frac{1}{24\eta^2}\xi^3+\frac{1}{2^2}\xi+\frac{1}{6}\right)m^3+o(m^3)}
\end{aligned}$$

4.2 定理1(推广结果)的证明

回顾本文攻击所需要的条件, 即式(9): $\det(\Lambda)T_1(s)<W^{m(s-1)}$, $T_1(s)=2^{s(s-1)/4}s^{(s-1)/2}$. 把 s 与 $\det(\Lambda)$ 的计算结果代入到式(9)可得:

$$X^{\frac{1}{6}+\frac{o(m^3)}{m^3}}Y^{-\frac{1}{6\eta}\xi^3+\frac{1}{2}\xi^2+\frac{o(m^3)}{m^3}}U^{-\frac{1}{24\eta^2}\xi^3+\frac{1}{2^2}\xi+\frac{1}{6}+\frac{o(m^3)}{m^3}}T_1(s)^{\frac{1}{m^3}}<W^{-\frac{1}{24\eta^2}\xi^3+\frac{1}{2^2}\xi+\frac{1}{6}+\frac{o(m^3)}{m^3}} \tag{10}$$

再把 $X=2N^{\alpha+\beta-1},Y=3N^{0.5},U=7N^{\alpha+\beta-0.5},W=N^{\alpha+\delta}$ 代入到式(10)中得到

$$\lambda(\xi)+\frac{o(m^3)}{m^3}+\log_N T_2(m,\xi)<0 \tag{11}$$

其中

$$\begin{aligned}
&\lambda(\xi)=-\frac{1}{24\eta}\xi^3+\frac{1}{4}\xi^2-\frac{1}{2}\eta\xi+\frac{1}{6}(\alpha+\beta-1-\eta)\\
&\eta=0.5-\beta+\delta=0.5-(\beta-\delta)\\
&T_2(m,\xi)=2^{\frac{1}{6}+\frac{o(m^3)}{m^3}}3^{-\frac{1}{6\eta}\xi^3+\frac{1}{2}\xi^2+\frac{o(m^3)}{m^3}}7^{-\frac{1}{24\eta^2}\xi^3+\frac{1}{2^2}\xi+\frac{1}{6}+\frac{o(m^3)}{m^3}}T_1(s)^{\frac{1}{m^3}}
\end{aligned}$$

为了从式(11)得到尽可能好的结果, 需要最小化式(11)中的 $\lambda(\xi)$. 容易验证 $\lambda(\xi)$ 是关于 ξ 的减函数. 注意到 $0\leqslant\xi\leqslant 2\eta$, 并且可以选取合适的整数 τ,m 使得 $\xi=\tau/m$ 尽可能逼近 2η. 所以在式(11)中令 $\xi=2\eta$, 得到

$$2\eta^2+\eta-(\alpha+\beta-1)-\varepsilon^*>0 \tag{12}$$

其中 $\varepsilon^*=\varepsilon_1+\varepsilon_2$,

$$\varepsilon_1=T^*(m)=6\cdot\frac{o(m^3)}{m^3}=\frac{o(m^3)}{m^3}$$
$$\varepsilon_2=\log_N T_3(m)$$
$$T_3(m)=T_2(m,2\eta)^6$$

如果 $m\to\infty$, 那么 $T^*(m)\to 0$. 因此可以选取足够大的 m, 使得 $|\varepsilon_1|$ 任意小. 固定 m 后, $T_3(m)$ 也被固定, 此时存在足够大的 N, 使得 $|\varepsilon_2|$ 任意小. 所以 $|\varepsilon^*|$ 可以任意小. 根据式(12)以及 $\eta>0$, 得到

$$\eta>-\frac{1}{4}+\frac{1}{4}\sqrt{8(\alpha+\beta)-7}+\varepsilon \tag{13}$$

代入 $\eta=0.5-(\beta-\delta)$ 即得

$$\beta-\delta<\frac{3}{4}-\frac{1}{4}\sqrt{8(\alpha+\beta)-7}-\varepsilon \tag{14}$$

因为 $|\varepsilon^*|$ 可以任意小, 所以只要 m 和 N 足够大, $|\varepsilon|$ 也可以任意地小. 对于式(14), 用 $|\varepsilon|$ 替换 ε (变为原不等式的充分条件), 仍表示为 $\varepsilon(\varepsilon>0)$,再用“≤”代替“<”(因为 ε 的存在而基本无差异), 即得到式(5), 至此证得定理 1 的推广结果.

4.3 关于条件 $d_2<N^{\beta-0.5}$

本文的结果需要条件 $d_2<N^{\beta-0.5}$, 根据 3.1 节可知, 该条件使得

$$0<u=x\cdot y+e\cdot d_2-1<7N^{\alpha+\beta-0.5}=U\approx XY=6N^{\alpha+\beta-0.5}$$

对于一般的 $d_2<N^{\beta-\gamma}$, 如果 $\gamma>0.5$, 基本不会影响 U 的取值, 所以最后的结果仍然为式(5). 对于 $\gamma<0.5$ 的情形, 则 U 的取值由 $7N^{\alpha+\beta-0.5}$ 变为 $7N^{\alpha+\beta-\gamma}$. 这时只需把 η 的取值由 $0.5-(\beta-\delta)$ 改为 $\gamma-(\beta-\delta)$, 按照上文的证明, 最终仍然得到式(13). 在式(13)中代入 $\eta=\gamma-(\beta-\delta)$, 可得式(5)的推广:

$$\beta-\delta\leqslant\gamma+\frac{1}{4}-\frac{1}{4}\sqrt{8(\alpha+\beta)-7}-\varepsilon \tag{15}$$

显然 γ 越小, 对 d_2 的限制越弱, 式(15)的结果也越差. 注意到式(4), 如果有

$$\frac{5}{6}-\frac{1}{3}\sqrt{6(\alpha+\beta)-5}<\gamma+\frac{1}{4}-\frac{1}{4}\sqrt{8(\alpha+\beta)-7}$$

那么当条件 $d_2<N^{\beta-\gamma}$ 对某个 $\gamma<0.5$ 成立时, 式(15)仍然是对式(4)的改进.

5 实验

类似于其他基于 Coppersmith 方法的部分私钥泄露攻击, 定理 1 建立在假设 1 成立的基础上. 为了检验假设 1 同时验证本文的证明原理, 我们在软件 SAGE 5.0 上通过编程做了许多实验. 设备为一台拥有 3.20GHz Intel 双核处理器、4GB 内存的台式机, 并在其上通过安装虚拟机建立了 Linux Fedora 16 的操作系统, 从而让软件 SAGE 5.0 得以运行.

在每次实验中，首先选择私钥LSBs泄露的RSA密码参数，即选择参数 N,β,δ,d_2 以及 $\alpha\approx 1$，使这些参数满足定理 1 中的条件. 然后再选择参数 m,τ 和 $\theta_1,\theta_2,\cdots,\theta_\tau$，建立格基方阵 $\mathcal{B}$，作为 LLL 算法的输入. 运行 LLL 算法后可以得到一组 LLL-约化基，取前两个向量，即得到对应的两个多项式 $h_1(x,y,u)$ 和 $h_2(x,y,u)$，二者都在整数意义上以 $(x_0,y_0,u_0)=(k,p+q-1,k(p+q-1)+A)$ 为根. 由关系式 $u=xy+A$ 可以消去 u，得到 $g_1(x,y)=h_1(x,y,xy+A)$ 和 $g_2(x,y)=h_2(x,y,xy+A)$. 接着建立 $g_1(x,y)$ 和 $g_2(x,y)$ 的结式消去 x，得到 $g_{12}(y)=\mathrm{Res}_x(g_1,g_2)$. 如果假设 1 成立，那么 $g_{12}(y)$ 应该是非零多项式，因此通过求根的数值算法就可以找到 $g_{12}(y)$ 的所有整数根，其中就包含 y_0. 进一步可以通过把 y_0 的备选值(即 $g_{12}(y)$ 的所有整数根)逐个代入 $g_1(x,y)$ 或 $g_2(x,y)$ 的方式得到 x_0 的所有备选值. 不过在实际中得到 $y_0=(p+q-1)$ 的备选值，就可以逐个尝试进而分解 RSA 模 N.

在我们的实验中，假设 1 总是成立的，进而总是可以成功分解 RSA 模 N. 针对定理 1 的一些实验结果如表 2 所示.

表 2 当条件 $d_2<N^{\beta-0.5}$ 满足时定理 1 的一些实验结果

Table 2 Some Experimental Results of Theorem 1 under condition $d_2<N^{\beta-0.5}$

N (bits)	β	δ	m	τ	$\theta_1,\theta_2,\cdots,\theta_\tau$	$s=\dim(\Lambda)$	$\log_2(\det(\Lambda))$	LLL 算法时间(s)
2000	0.8009	0.7844	8	7	2,3,4,5,6,7,8	73	2.081×10^6	1751.000
1000	0.7227	0.6907	6	5	2,3,4,5,6	43	4.351×10^5	25.370
1500	0.7031	0.6698	5	4	2,3,4,5	31	3.871×10^5	8.966
2000	0.6693	0.6053	7	6	2,3,4,5,6,7	57	1.278×10^6	389.800
1000	0.6266	0.5556	5	4	2,3,4,5	31	2.407×10^5	4.877
1500	0.5504	0.4370	6	4	2,3,4,6	41	5.292×10^5	45.620

6 结论

Herrmann 和 May 通过线性化模方程的处理，给出了低解密指数攻击 $d\leqslant N^{0.292-\varepsilon}$ 的简化证明[19]. 本文通过把文献[19]的证明方法推广到部分私钥泄露攻击中，提出了新的 LSBs 泄露攻击. 本文的攻击在 $d_2<N^{\beta-0.5}$ 的情况下改进了 Ernst 等人[12]的 LSBs 泄露攻击. 另外，文献[12]中的 LSBs 泄露攻击只考虑了 $e\approx N$ 的情况，针对任意 $e<N$ 的情况，本文指出了文献[12]的推广结果以及本文攻击的推广结果，后者仍然是前者在情况 $d_2<N^{\beta-0.5}$ 下的改进. 最后，本文对于一般的 $d_2<N^{\beta-\gamma}$ 给出了相应的攻击结果并进行了简要分析.

References

[1] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120–126.

[2] Coppersmith D. Finding a small root of a univariate modular equation[C]. In: Advances in cryptology—EUROCRYPT '96. Springer Berlin Heidelberg, 1996: 155–165.

[3] Coppersmith D. Finding a small root of a bivariate integer equation; factoring with high bits known[C]. In: Advances in cryptology—EUROCRYPT'96. Springer Berlin Heidelberg, 1996: 178–189.

[4] Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities[J]. Journal of Cryptology, 1997, 10(4): 233–260.

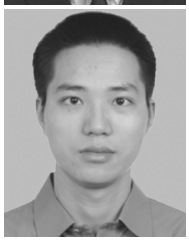
[5] Howgrave-Graham N. Finding Small Roots of Univariate Modular Equations Revisited[M]. Crytography and Coding. Springer Berlin Heidelberg, 1997: 131–142.
[6] Coron J S. Finding small roots of bivariate integer polynomial equations revisited[C]. In: Advances in Cryptology—EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 492–505.
[7] Boneh D, DeMillo R A, Lipton R J. On the importance of checking cryptographic protocols for faults[C]. In: Advances in Cryptology—EUROCRYPT '97. Springer Berlin Heidelberg, 1997: 37–51.
[8] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]. In: Advances in Cryptology—CRYPTO '96. Springer Berlin Heidelberg, 1996: 104–113.
[9] Kocher P, Jaffe J, Jun B. Differential power analysis[C]. In: Advances in Cryptology—CRYPTO '99. Springer Berlin Heidelberg, 1999: 388–397.
[10] Boneh D, Durfee G, Frankel Y. An attack on RSA given a small fraction of the private key bits[C]. In: Advances in Cryptology—ASIACRYPT '98. Springer Berlin Heidelberg, 1998: 25–34.
[11] Blömer J, May A. New partial key exposure attacks on RSA[C]. In: Advances in Cryptology—CRYPTO 2003. Springer Berlin Heidelberg, 2003: 27–43.
[12] Ernst M, Jochemsz E, May A, et al. Partial key exposure attacks on RSA up to full size exponents[C]. In: Advances in Cryptology—EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 371–386.
[13] Aono Y. A new lattice construction for partial key exposure attack for RSA[C]. In: Public Key Cryptography—PKC 2009. Springer Berlin Heidelberg, 2009: 34–53.
[14] Sarkar S, Gupta S S, Maitra S. Partial key exposure attack on RSA–improvements for limited lattice dimensions[C]. In: Progress in Cryptology-INDOCRYPT 2010. Springer Berlin Heidelberg, 2010: 2–16.
[15] Joye M, Lepoint T. Partial key exposure on RSA with private exponents larger than N [C]. In: Information Security Practice and Experience. Springer Berlin Heidelberg, 2012: 369–380.
[16] Huang Z, Hu L, Xu J, et al. Partial key exposure attacks on Takagi's variant of RSA[C]. In: Applied Cryptography and Network Security. Springer International Publishing, 2014: 134–150.
[17] Wiener M J. Cryptanalysis of short RSA secret exponents[J]. IEEE Transactions on Information Theory, 1990, 36(3): 553–558.
[18] Boneh D, Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$ [C]. In: Advances in Cryptology—EUROCRYPT '99. Springer Berlin Heidelberg, 1999: 1–11.
[19] Herrmann M, May A. Maximizing small root bounds by linearization and applications to small secret exponent RSA[C]. In: Public Key Cryptography—PKC 2010. Springer Berlin Heidelberg, 2010: 53–69.
[20] Lenstra A K, Lenstra H W, Lovász L. Factoring polynomials with rational coefficients[J]. Mathematische Annalen, 1982, 261(4): 515–534.
[21] May A. New RSA vulnerabilities using lattice reduction methods[D]. University of Paderborn, 2003.

作者信息

王世雄(1991–), 硕士生在读. 主要研究领域为密码学.
E-mail: wsx09@foxmail.com

屈龙江(1980–), 博士, 教授. 主要研究领域为密码学.
E-mail: ljqu_happy@hotmail.com

李超(1966–), 博士, 教授, 中国密码学会理事. 主要研究领域为密码学.
E-mail: lichao_nudt@sina.com



付绍静(1984–), 博士, 副教授. 主要研究领域为密码学.
E-mail: shaojing1984@163.com