文章编号:1000-2367(2017)03-0001-13 DOI:10.16366/j.cnki.1000-2367.2017.03.001

基于格的 RSA 密码分析

李超[a,b], 王世雄[a], 屈龙江[b], 付绍静[a]

(国防科学技术大学 a.计算机学院;b.理学院, 长沙 410073)

摘 要:格在公钥密码分析领域中有着十分重要的地位.1996 年,Coppersmith 以多项式方程求小值解的问题为桥梁,把攻击 RSA 密码体制的问题转换为求格中短向量的问题,开辟了基于格的 RSA 密码分析的研究,他的工作也在后人的简化完善下逐渐形成了 Coppersmith 方法.一方面,关于基于格的 Coppersmith 方法,依次介绍了模多项式方程求小值解的方法、整系数多项式方程求小值解的方法、求解近似公共因子问题的方法,还简单描述了除 Coppersmith 方法外的一种在低维格中寻找最短非零向量的格方法.另一方面,关于 RSA 密码分析,回顾了小加密指数攻击、小解密指数攻击、部分私钥泄露攻击、求解私钥 d 与分解模数 N 的等价性证明、隐式分解问题的分析、素因子部分比特泄露攻击、共模攻击等,并且以 Prime Power RSA,Takagi's RSA,CRT-RSA,Common Prime RSA 为例,介绍了格方法在 RSA 密码变体分析中的应用.

关键词:格;RSA 密码;Coppersmith 方法;LLL 算法

中图分类号:TN918 **文献标志码**:A

基于格的 RSA 密码分析,一般指在给定条件下,把攻击 RSA 密码体制的问题转换为求格中短向量的问题,最后利用格基约化算法进行求解.这方面的开创性工作源于 Coppersmith 在 1996 年关于多项式方程求小值解的工作[1-2],在后人的简化完善下逐渐形成了 Coppersmith 方法,进而构成了基于格的 RSA 密码分析的主要内容.

1 预备知识

1.1 格

格的研究起源于球堆积与覆盖的问题.1611 年,开普勒猜想在容器中堆放同样大的小球,所能达到的最大密度是 $\pi/\sqrt{18}$.为了解决该问题,1840 年前后,高斯引入了格的概念.目前格的研究涉及组合、数论、代数、几何、分析等许多数学领域的理论知识,又在物理学与化学、通信技术、计算机技术、密码学等领域中有着非常重要的应用[3-4].

格 Λ 是 S 维欧氏空间 $\mathbf{R}^s$ 中的一个离散加法子群.等价地说,格 Λ 是 $\mathbf{R}^s$ 中 ω 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 $\Lambda=\mathrm{span}_{\mathbf{Z}}(\vec{b}_1,\vec{b}_2,\cdots,\vec{b}_\omega)=\left\{\sum_{i-1}^{\omega}x_i\vec{b}_i \mid x_i\in\mathbf{Z},i=1,2,\cdots,\omega\right\}$.其中,$s$ 与 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.把基中的向量视为列向量,得到格 Λ 的基矩阵 $\boldsymbol{B}=(\vec{b}_1\quad\vec{b}_2\quad\cdots\quad\vec{b}_\omega)\in\mathbf{R}^{s\times\omega}$.进而定义格 Λ 的行列式为 $\det(\Lambda)=\sqrt{\det(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{B})}$.当 $\omega=s$ 时,Λ 称为满秩格,$\boldsymbol{B}$ 为方阵,从而 $\det(\Lambda)=|\det\boldsymbol{B}|$.

定义格 Λ 的最短非零向量长度为 $\lambda_1(\Lambda):=\min\{\|\vec{b}\| \mid \vec{b}\in\Lambda,\vec{b}\neq\vec{0}\}$.作为格理论中的一个经典困难问

收稿日期:2017-01-14;修回日期:2017-04-10.

基金项目:国家自然科学基金(11531002;61572026);国防科技大学科研计划项目(CJ13-02-01);教育部新世纪人才项目(NCET).

作者简介:李超(1966 -),男,湖南汨罗人,国防科技大学教授,博士生导师,主要研究领域为密码学,E-mail:lichao_nudt@sina.com.

通信作者:王世雄,wsx09@foxmail.com.

题,最短向量问题(Shortest Vector Problem,SVP)即对于给定的格 Λ 寻找 $\vec{v}\in\Lambda$ 使得 $\|\vec{v}\|=\lambda_1(\Lambda)$. 相应地,近似最短向量问题即对于给定的格 Λ 与参数 $r_\omega\geq 1$(r_ω 一般和 ω 有关),寻找 $\vec{v}\in\Lambda,\vec{v}\neq\vec{0}$ 使得 $\|\vec{v}\|\leq r_\omega\cdot\lambda_1(\Lambda)$. 1982 年,文献[5]首次提出了著名的求解近似最短向量问题的 LLL 算法. 输入格 Λ 的一组基后,通过 LLL 算法可以输出一组 LLL-约化基,其中的第一个基向量即为满足近似 SVP 的短向量. LLL 算法是关于格的秩 ω(以及格基向量中分量的比特长度)成多项式时间复杂度的有效算法.

1.2 RSA 密码

RSA 是第一个公钥密码体制,由麻省理工学院的 Rivest,Shamir,Aldeman 在 1978 年提出[6],可以同时用于数据加密和数字签名,是迄今为止最著名的公钥密码算法之一. RSA 的密钥建立过程为:选取两个大素数 p 和 q,计算 $N=pq$ 和欧拉函数 $\varphi(N)=(p-1)(q-1)$,然后选取正整数 e,满足 $e<\varphi(N)$,$\gcd(e,\varphi(N))=1$,并计算正整数 d 使得 $e\cdot d\equiv 1(\bmod \varphi(N))$,最后安全销毁 p,q 和 $\varphi(N)$. 称 N 为 RSA 模数,e 为加密指数,d 为解密指数,也称(N,e) 为公钥,d 为私钥. RSA 的加解密过程为:发信者通过公钥 (N,e) 加密明文 $M(<N)$,得到密文 $C\equiv M^e(\bmod N)$,发送给收信者,收信者再通过私钥 d 解密密文,得到明文 $M\equiv C^d(\bmod N)$.

破解 RSA 密码体制,要在已知 N,e,C 的情况下通过关系式 $C\equiv M^e(\bmod N)$ 求出 M,即在 $\mathbf{Z}_N$ 环中求解 e 次根,通常把该问题称为 RSA 问题. 显然,求解 RSA 问题不比求解 d 困难,求解 d 不比分解 N 困难. 因为分解 RSA 模数 N 意味着破解 RSA 密码体制,所以一般认为 RSA 密码的安全性基于大整数因子分解的困难性. 尽管直接求解 RSA 问题是非常困难的,但是在一些特殊的情况下或者知道一些额外信息的情况下,该问题可以转换为多项式方程求小值解的问题,进而可以转换为求格中短向量的问题,最后利用格基约化算法进行求解.

本文主要介绍以 Coppersmith 方法为主的格方法在 RSA 密码分析以及 RSA 密码变体分析中的应用. 剩余的内容安排如下:第 2 章围绕基于格的 Coppersmith 方法,依次描述模多项式方程求小值解的方法、整系数多项式方程求小值解的方法、求解近似公共因子问题的方法,另外简单描述了除 Coppersmith 方法外的一种需要求解精确 SVP 的格方法;第 3 章是格方法在 RSA 密码分析中的应用,依次介绍小加密指数攻击、小解密指数攻击、部分私钥泄露攻击、求解私钥 d 与分解模数 N 的等价性证明、隐式分解问题的分析、素因子部分比特泄露攻击、共模攻击等;第 4 章以 Prime Power RSA,Takagi's RSA,CRT-RSA,Common Prime RSA 为例,介绍了格方法在 RSA 密码变体分析中的应用;最后在第 5 章进行总结.

2 基于格的 Coppersmith 方法

RSA 密码分析的问题,一定条件下可以转换为多项式方程求小值解的问题. 相应地,基于格的 Coppersmith 方法,则是解决多项式方程(包括 v 元模多项式方程以及 $v+1$ 元整系数多项式方程)求小值解问题的一类方法的统称. Coppersmith 最初在 1996 年得到了 $v=1$ 时的一般结论[1-2],并在 1997 年进行总结完善[7].

后来,Howgrave-Graham[8] 与 Coron[9] 分别在 1997 年与 2004 年改进了 Coppersmith 的证明方法,并被学者们广泛地应用到 RSA 密码分析中. Howgrave-Graham 和 Coron 的方法可以推广到 $v\geq 2$ 的情形,不过此种情形下他们的方法都基于一类结式求解假设,因此结果只能是经验式的(heuristic),需要做实验来验证假设是否成立. 2006 年,Jochemsz 和 May[10] 对改进方法进行了推广与总结,即针对任意 $v\geq 1$ 的情形,给出了两类多项式方程(模多项式方程和整系数多项式方程)求小值解的一般策略(Strategy),主要涉及满秩格的构造方法,包括"基本策略"(Basic Strategy)和"拓展策略"(Extended Strategy). 一般来说,Coppersmith 方法即指 Howgrave-Graham[8],Coron[9] 与 Jochemsz,May[10] 的改进方法.

2.1 v 元模多项式方程求小值解

v 元模多项式方程求小值解的问题一般描述为:对于 $f(x_1,\cdots,x_v)\in\mathbf{Z}[x_1,\cdots,x_v]$,求出满足 $f(x_1^{(0)},\cdots,x_v^{(0)})\equiv 0(\bmod W)$,$|x_1^{(0)}|<X_1,\cdots,|x_v^{(0)}|<X_v$ 的解 $(x_1^{(0)},\cdots,x_v^{(0)})\in\mathbf{Z}^v$.

当 $v=1$ 时,文献[7]的推论 1 总结了单变元模多项式方程求小值解的结论:设 δ 次首一多项式 $f(x)\in$

$\mathbf{Z}[x]$,常数 $X \leq W^{1/\delta}$,那么在关于 $(\log_2 W, 2^\delta)$ 的多项式时间内就可以找到满足 $f(x^{(0)}) \equiv 0 (\mathrm{mod}\ W)$,$|x^{(0)}| < X$ 的解 $x^{(0)} \in \mathbf{Z}$.

关于求解满足 $f(x^{(0)}) \equiv 0 (\mathrm{mod}\ W)$,$|x^{(0)}| < X$ 的未知整数 $x^{(0)}$,Howgrave-Graham[8]的改进方法的核心思想为:首先构造一个多项式集合 P,使得集合 P 中的任一多项式 $g(x)$ 满足 $g(x^{(0)}) \equiv 0 (\mathrm{mod}\ V)$(其中 V 一般为 W 的幂次),这等同于构造一个格 Λ;然后通过 LLL 算法(或者其他格基约化算法),输出集合 P 中的一个多项式 $h(x)$,满足 $|h(x^{(0)})| < V$;最后联合 $h(x^{(0)}) \equiv 0 (\mathrm{mod}\ V)$ 以及 $|h(x^{(0)})| < V$ 可知 $h(x)$ 满足 $h(x^{(0)}) = 0$,即未知整数 $x^{(0)}$ 为多项式 $h(x)$ 的根,因此可以通过数值方法求出 $x^{(0)} \in \mathbf{Z}$.

当 $v \geq 1$ 时,对于一般的 v 元模多项式方程求小值解问题,Howgrave-Graham[8]给出了一个重要的引理:如果多项式 $h(x_1, \cdots, x_v) \in \mathbf{Z}[x_1, \cdots, x_v]$ 中含有至多 s 个单项式,且存在 $(x_1^{(0)}, \cdots, x_v^{(0)}) \in \mathbf{Z}^v$ 满足 $h(x_1^{(0)}, \cdots, x_v^{(0)}) \equiv 0 (\mathrm{mod}\ V)$,$|x_1^{(0)}| < X_1, \cdots, |x_v^{(0)}| < X_v$ 以及 $\|h(X_1 x_1, \cdots, X_v x_v)\| < V/\sqrt{s}$,那么就在整数意义下得到 $h(x_1^{(0)}, \cdots, x_v^{(0)}) = 0$. 其中 $h(x_1, \cdots, x_n) = \sum a_{i_1, \cdots, i_n} x_1^{i_1} \cdots x_n^{i_n}$ 的范数定义为 $\|h(x_1, \cdots, x_n)\| = \sqrt{\sum |a_{i_1, \cdots, i_n}|^2}$. 与 $v = 1$ 时的核心思想一致,条件 $\|h(X_1 x_1, \cdots, X_v x_v)\| < V/\sqrt{s}$ 一方面蕴含着 $|h(x_1^{(0)}, \cdots, x_v^{(0)})| < V$,从而使得 $h(x_1^{(0)}, \cdots, x_v^{(0)}) = 0$,另一方面意味着 $h(X_1 x_1, \cdots, X_v x_v)$ 对应于所构造的格中的短向量,该短向量通常可以使用 LLL 算法获得. May[11]指出 LLL 算法有如下的结果:输入维数为 s、秩为 ω 的格 Λ 的格基矩阵 $\boldsymbol{B}$ 后,LLL 算法在关于 ω 与 $\boldsymbol{B}$ 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 $\|\vec{v}_i\| \leq 2^{\omega(\omega-1)/4(\omega-i+1)} \det(\Lambda)^{1/(\omega-i+1)}$ $(1 \leq i \leq \omega)$,其中 $\vec{v}_i = (v_{i1}, v_{i2}, \cdots, v_{is})$ 的范数定义为 $\|\vec{v}_i\| = \sqrt{v_{i1}^2 + v_{i2}^2 + \cdots + v_{is}^2}$. 寻找的多项式 $h(x_1, \cdots, x_v)$ 需要满足的条件是 $\|h(X_1 x_1, \cdots, X_v x_v)\| < V/\sqrt{s}$,而 LLL 算法可给出的结果是 $\|\vec{v}_i\| \leq 2^{\omega(\omega-1)/4(\omega-i+1)} \det(\Lambda)^{1/(\omega-i+1)}$,故让若干 $h(X_1 x_1, \cdots, X_v x_v)$ 与诸 $\vec{v}_i$ 建立一一对应的关系后,只要 $2^{\omega(\omega-1)/4(\omega-i+1)} \det(\Lambda)^{1/(\omega-i+1)} < V/\sqrt{s}$ 成立,就可以得到若干多项式 $h(x_1, \cdots, x_v)$ 满足 $h(x_1^{(0)}, \cdots, x_v^{(0)}) = 0$. 当 $v = 1$ 时,可以直接通过数值方法求出 $x_1^{(0)}$. 当 $v \geq 2$ 时,Coppersmith 方法指出可以通过在这些多项式 $h(x_1, \cdots, x_v)$ 之间建立结式依次消元逐渐求出公共解 $(x_1^{(0)}, \cdots, x_v^{(0)}) \in \mathbf{Z}^v$. 当然,结式消元求解只是一个经验式的(heuristic)假设,需要通过实验来验证该假设是否成立.

综上所述,如果结式消元求解假设成立($v = 1$ 时不需要该假设),那么通过 Coppersmith 方法来寻找 v 元模多项式方程的小值解,所需要的条件为 $2^{\omega(\omega-1)/4(\omega-i+1)} \det(\Lambda)^{1/(\omega-i+1)} < V/\sqrt{s}$,在渐进意义下可以简化为 $\det(\Lambda)^{1/\omega} < V \Leftrightarrow \det(\Lambda) < V^\omega$. 该条件实际上最终等价于关于 v 个小值解的上界 $X_1, X_2, \cdots, X_v$ 的不等式.

Coppersmith 方法的基本思想成熟后,后续的工作重心就转变为多项式集合的构造,实际上等同于格的构造. 而优化格的构造,其目的在于最大化小值解的上界,对应到 RSA 密码分析问题时,其实质则是尽可能地弱化攻击需要的条件. 关于格构造方法,Jochemsz 和 May 在文献[10]中,首先给出了一种“基本策略”,并在此基础上给出了“拓展策略”. 按照文献[10]的策略所构造的格,都是满秩格,并且构造的格基方阵为下三角方阵,因此 $\det(\Lambda)$ 的计算也较为简单. 文献[10]的格构造方法,适用于一般情况下的模多项式方程求小值解问题. 针对具体的模多项式方程求小值解问题,有时可以在“拓展策略”的基础之上继续优化格的构造. 例如构造非满秩的格[12],或者采用变量替换的技巧[13].

2.2　$v+1$ 元整系数多项式方程求小值解

$v+1$ 元整系数多项式方程求小值解的问题一般描述为:对于 $f(x_1, \cdots, x_{v+1}) \in \mathbf{Z}[x_1, \cdots, x_{v+1}]$,求出满足 $f(x_1^{(0)}, \cdots, x_{v+1}^{(0)}) = 0$,$|x_1^{(0)}| < X_1, \cdots, |x_{v+1}^{(0)}| < X_{v+1}$ 的解 $(x_1^{(0)}, \cdots, x_{v+1}^{(0)}) \in \mathbf{Z}^{v+1}$.

当 $v = 1$ 时,文献[7]的推论 2 总结了双变元整系数多项式方程求小值解的结论:设不可约多项式 $f(x_1, x_2) \in \mathbf{Z}[x_1, x_2]$,$\delta$ 为 $f(x_1, x_2)$ 中 x_1 的最高次数与 x_2 的最高次数的较大值,M 为 $f(X_1 x_1, X_2 x_2)$ 中系数的绝对值的最大值,其中 $X_1 X_2 \leq M^{2/(3\delta)}$,那么在关于 $(\log_2 M, 2^\delta)$ 的多项式时间内就可找到满足 $f(x_1^{(0)}, x_2^{(0)}) = 0$,$|x_1^{(0)}| < X_1$,$|x_2^{(0)}| < X_2$ 的解 $(x_1^{(0)}, x_2^{(0)}) \in \mathbf{Z}^2$.

关于求解满足 $f(x_1^{(0)}, x_2^{(0)}) = 0$,$|x_1^{(0)}| < X_1$,$|x_2^{(0)}| < X_2$ 的未知整数对 $(x_1^{(0)}, x_2^{(0)})$,Coron[9]的改进方法的核心思想为:首先构造一个多项式集合 P,使得集合 P 中的任一多项式 $g(x_1, x_2)$ 满足 $g(x_1^{(0)}, x_2^{(0)}) \equiv 0 (\mathrm{mod}\ R)$(其中 R 为构造的大整数),这同样等同于构造一个格 Λ;然后同样通过 LLL 算法(或者其他格基

约化算法),输出集合 P 中的一个多项式 $h(x_1,x_2)$,使得 $h(x_1^{(0)},x_2^{(0)})=0$,同时保证最初给定的不可约多项式 $f(x_1,x_2)$ 不能整除 $h(x_1,x_2)$,即 $h(x_1,x_2)$ 与 $f(x_1,x_2)$ 是代数无关的;最后通过对 $h(x_1,x_2)$ 与 $f(x_1,x_2)$ 建立结式消元以及数值方法求出公共解 $(x_1^{(0)},x_2^{(0)})\in\mathbf{Z}^2$.

当 $v\geq 1$ 时,对于一般的 $v+1$ 元整系数多项式方程求小值解问题,其原理要比相应的 v 元模多项式方程求小值解问题复杂.同样要求 $v+1$ 元整系数多项式 $f(x_1,\cdots,x_{v+1})$ 不可约,对 $j=1,2,\cdots,v+1$,令 d_j 为 $f(x_1,\cdots,x_{v+1})$ 中变元 x_j 的最高次数,规定 M 为 $f(X_1x_1,\cdots,X_{v+1}x_{v+1})$ 中系数的绝对值的最大值,进而得到 $R:=M\prod_{j-1}^{v+1}X_j^{d_j(m-1)}$,其中 m 为设定的参数.类似于模方程的情况,需要构造一个多项式集合 P,对应一个维数为 s、秩为 ω 的格 Λ.一般情况下 $s=\omega$,即格 Λ 为满秩格.多项式集合 P 中的任一多项式 $g(x_1,\cdots,x_{v+1})$,不但要满足模去 R 后都以 $(x_1^{(0)},\cdots,x_{v+1}^{(0)})$ 为根,而且要求 $g(X_1x_1,\cdots,X_{v+1}x_{v+1})$ 都能被 $\prod_{j-1}^{v+1}X_j^{d_j(m-1)}$ 整除,后者的要求主要为了保证 LLL 算法得到的多项式不是 $f(x_1,\cdots,x_{v+1})$ 的倍式.类似于模多项式方程的分析,通过 Coppersmith 方法来寻找 $v+1$ 元整系数多项式方程的小值解,所需要的条件在渐进意义下可以简化为 $\det(\Lambda)<R^{\omega}$,其中当 $v\geq 2$ 时仍然需要结式消元求解成立的假设.

关于格构造方法,Jochemsz 和 May 在文献[10]中同样给出了"基本策略"与"拓展策略".其中构造的格仍然都是满秩格,并且构造的格基方阵为上三角方阵.考虑到构造格 Λ 时,其对应的多项式集合 P 中的多项式需要同时满足两个条件,即格构造的限制比模方程的情况要多,因此在"拓展策略"基础之上继续优化格构造的难度也较大.比如有时采用变量替换的技巧,因为不能同时满足之前提到的两个条件,所以并不能改进格的构造.

2.3 近似公共因子问题(ACDP)

2001 年,Howgrave-Graham[14] 首次提出了 ACDP(Approximate Common Divisor Problem),即近似公共因子问题:给定 a_0,b_0 以及界 X,Y,C,要求寻找 W,满足 $W>C$,并且存在 x_0,y_0 使得 $W\mid(a_0+x_0),W\mid(b_0+y_0),\mid x_0\mid<X,\mid y_0\mid<Y$.不失一般性可令 $X\geq Y$,当 $Y=0$ 时,Howgrave-Graham 称该问题为 PACDP(Partially Approximate Common Divisor Problem),即部分近似公共因子问题;当 $Y>0$ 时,Howgrave-Graham 称该问题为 GACDP(General Approximate Common Divisor Problem),即一般近似公共因子问题.文献[14]针对 PACDP 与 GACDP 这两个问题,均给出了基于连分数的算法、基于格的算法,而后者实际上为解决模多项式方程求小值解问题的 Coppersmith 方法.与第 2.1 节不同的地方在于,此处模多项式方程中使用的模数 W 是未知的.ACDP 的分析研究有着广泛的应用,例如可以用来解决 RSA 密码分析中的隐式分解问题[15](ImplicitFactorizationProblem),还可以用来构建全同态加密方案[16].

对于模多项式方程中模数 W 未知的情形,文献[14]给出了如下结果:未知数 W 整除已知数 M,并且 $W\geq M^{\gamma}(0<\gamma\leq 1)$,令 $f(x)=x+a_0$,那么在多项式时间内就可以找到满足 $f(x^{(0)})\equiv 0(\mathrm{mod}\ W)$,$\mid x^{(0)}\mid<M^{\gamma^2}$ 的解 $x^{(0)}\in\mathbf{Z}$.从求解思路与格构造方法上来说,模数未知与模数已知两种情形基本相同,只是模数未知的情形增加了一个待优化的参数,从而可以看作模数已知情形的推广.文献[14]针对的是单变元线性方程,2008 年,Herrmann 与 May[17] 针对多变元线性方程,给出了格构造方法与相应的结果;2012 年,Cohn 与 Heninger[18] 则针对联立的单变元线性方程组,给出了格构造方法与相应的结果.之后在 2013 年,Takayasu 与 Kunihiro[19] 进一步优化了文献[17]与文献[18]的格构造方法,从而在小值解上界不平衡的情况下,改进了相应的结果.最后在 2015 年,卢尧等[20] 基于 RSA 密码变体分析的应用需求,通过继续增加参数推广了原来的多项式模未知数求小值解的问题,并且依次针对单变元线性方程、多变元线性方程、联立的单变元线性方程组给出了相应的结果.另外,当多变元线性方程为齐次线性方程时,文献[20]进一步优化了格构造方法.

2.4 其他方法:求解精确 SVP

Coppersmith 方法,构成了基于格的 RSA 密码分析的主要内容.除此之外,仍然存在其他的格方法.例如,RSA 密码分析中的隐式分解问题(Implicit Factorization Problem),最开始的求解方法就是构造二维格或者三维格,然后寻找格中的最短非零向量[21-22].注意到 Coppersmith 方法是在高维格中寻找近似 SVP,而该方法则是在低维格中寻找精确 SVP,所以二者的方法并不相同.文献[21-22]中的方法,需要证明目标向

量为构造的格中的最短非零向量,这在二维格的情况下是可以严格证明的,但是在三维格的情况下只能作为假设提出,并且通过实验验证.针对推广的隐式分解问题,该方法可以构造更高维数的格,不过仍然需要通过实验验证相应的假设.另外,还可以在文献[21－22]方法的基础上,继续使用 Coppersmith 方法弱化攻击所需要的条件[23－26].联合这两种方法,需要运行两次格基约化算法,并且有可能需要通过实验验证两个假设.

3　RSA 密码分析

当 RSA 密码的加密指数 e 比较小时,已知部分明文即可恢复余下的明文;当 RSA 密码的解密指数 d 比较小时,则有可能分解 RSA 模数 N.这些攻击都是 Coppersmith 方法在 RSA 密码分析中的典型应用.作为小解密指数攻击的推广,进一步可以针对 RSA 密码实现部分私钥泄露攻击.除此以外,基于 Coppersmith 方法等格方法还能够进行求解私钥 d 与分解模数 N 的等价性证明,隐式分解问题的分析,素因子部分比特泄露攻击,共模攻击等.

3.1　小加密指数攻击

Coppersmith[1]在 1996 年提出模多项式方程求小值解的方法时,给出的一个直接应用就是小加密指数攻击.文献[1]指出:当加密指数 $e=3$ 时,如果已知明文 M 的 2/3 的比特位,即可恢复整个明文 M.实际上按照第 2.1 节单变元模多项式方程求小值解的结论,对于次数为 e 的模多项式方程 $C\equiv M^e \pmod N$,如果明文 M 的比特位中未知的连续比特位不超过 $1/e$,即可恢复整个明文 M.这也是该攻击需要加密指数比较小的原因.小加密指数情况下还存在其他攻击,例如相关信息攻击[27],针对确定填充的明文的广播攻击[28],针对随机填充的明文的重复加密攻击[7]等等.

3.2　小解密指数攻击

1990 年,Wiener[29]基于连分数的方法,首次提出了针对 RSA 密码的小解密指数攻击.1999 年,Boneh 和 Durfee[12]基于 Coppersmith 方法改进了 Wiener 的结果.他们指出,只要解密指数 $d<N^{0.292}$,就有可能在多项式时间内分解 RSA 模数 N.这是至今小解密指数攻击中最好的结果.根据关系式 $e\cdot d\equiv 1 \pmod{\varphi(N)}$ 可知,存在正整数 k 使得 $1=ed-k\varphi(N)=ed-k[N-(p+q-1)]$,模去 e 后即得 $Nk-k(p+q-1)+1\equiv 0 \pmod e$.当 e 约等于 N 时,可得 $0<k<X_1:=2d$;当 p 与 q 的比特位数相等时,可得 $0<p+q-1<X_2:=3N^{0.5}$.令 $f(x_1,x_2)=Nx_1-x_1x_2+1$ 以及 $x_1^{(0)}=k,x_2^{(0)}=p+q-1$.那么文献[12]的工作实际上就是根据 Coppersmith 方法寻找满足 $f(x_1^{(0)},x_2^{(0)})\equiv 0 \pmod e$,$|x_1^{(0)}|<X_1$,$|x_2^{(0)}|<X_2$ 的解 $(x_1^{(0)},x_2^{(0)})\in \mathbf{Z}^2$.这是一个典型的双变元模多项式方程求小值解的问题.只要求出 $x_1^{(0)}=k,x_2^{(0)}=p+q-1$ 即可成功分解 RSA 模数 N.在结式求解假设成立的前提下,在格构造方法上采用文献[10]中的“基本策略”,即可证得实现攻击需要的条件为 $d<N^{0.25}$;进一步采用文献[10]中的“拓展策略”,可以把攻击条件弱化为 $d<N^{0.284}$.而文献[12]在“拓展策略”的基础之上继续突破,通过构造非满秩的格,得到了最终的结果 $d<N^{0.292}$.非满秩格的构造,使得格的行列式的计算非常烦琐.后来在 2010 年,Herrmann 与 May[13]通过变量替换的技巧对原来的方程进行了线性化的处理,得以通过构造满秩格来推导出同样的结果 $d<N^{0.292}$,也即简化了文献[12]中的格构造方法.除了文献[13],还有文献[30－33]也回顾了小解密指数攻击,但是并没有能够改进结果 $d<N^{0.292}$.其中文献[30]给出的结果为 $d<N^{0.29}$,虽然差于文献[12]中的结果,但是实现攻击所需的时间更短.

针对 RSA 密码的小解密指数攻击,在基于格的 RSA 密码分析中占据着核心的地位.许多其他类型的 RSA 密码分析结果,以及大量的 RSA 密码变体分析结果,都可以看作是针对 RSA 密码的小解密指数攻击结果的推广.如果能够改进 $d<N^{0.292}$ 这一结果,那么许多分析结果都有望被改进.

3.3　部分私钥泄露攻击

针对 RSA 密码的部分私钥泄露攻击,即指在已知私钥 d 的部分比特位的条件下去分解 RSA 模 N 或者恢复整个私钥 d.部分私钥泄露情况的出现,来源于现实中针对 RSA 密码的侧信道攻击(Side-Channel Attacks),包括错误攻击[34](Fault Attacks),时间攻击[35](Timing Attacks),能量分析[36](Power Analysis)等等.利用非数学手段的侧信道攻击,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,因此

部分私钥泄露攻击就成了关系到 RSA 密码现实安全的重要问题.

1998 年,Boneh,Durfee 和 Frankel[37] 根据文献[2]中结论的一个推论,首次提出了针对 RSA 密码的部分私钥泄露攻击. 记 MSBs 为最高数位比特(Most Significant Bits),LSBs 为最低数位比特(Least Significant Bits). 设 RSA 模数 $N=pq$ 满足 $N^{0.5}/2<q<p<2N^{0.5}$,文献[37]指出,泄露 d 的 $(\log_2 N)/4$ 的 LSBs,就可以在关于 $\log_2 N$ 为多项式、关于 e 为线性的时间内分解 RSA 模数 N,该结果只适用于加密指数 e 取值较小的情况. 文献[37]中的其他结果,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 $N^{0.5}$ 的范围. 对此,文献[37]提出了一个开放性问题:当 e 充分大于 $N^{0.5}$ 时,是否存在有效的部分私钥泄露攻击? 后来,Blömer 和 May[38] 于 2003 年、Ernst 等人[39] 于 2005 年,基于 Coppersmith 方法分别提出了新的部分私钥泄露攻击,从而肯定地回答了该问题. 其中,文献[39]首次给出了 $e\approx N$ 时的部分私钥泄露攻击,包括私钥 d 的 LSBs 或者 MSBs 泄露情况下的攻击. 2009 年,Aono[40] 改进了文献[39]在 LSBs 泄露攻击方面的部分结果. 2010 年,Sarkar 等人[41] 则在一定程度上改进了文献[39]中的 MSBs 泄露攻击. 2012 年,Joye 和 Lepoint[42] 提出了针对 $d>N$ 情形下的部分私钥泄露攻击. 2014 年,Takayasu 与 Kunihiro[43] 进一步改进了原有的结果. 文献[43]的 LSBs 泄露攻击在 $d<N^{(9-\sqrt{21})/12}$ 时是已知最好的结果,MSBs 泄露攻击则在 $d<N^{9/16}$ 时是已知最好的结果.

部分私钥泄露攻击,可以看作是小解密指数攻击的推广. 这是因为,假设部分私钥泄露攻击中私钥泄露的比特位数为 0,自然会得到相应的小解密指数攻击结果. 例如,把私钥未泄露的情况应用于文献[39]的攻击结果中,会得到 $d<N^{0.284}$ 的小解密指数攻击结果,该结果并没有达到文献[12]中的结果 $d<N^{0.292}$,这也是文献[39]的攻击结果存在改进空间的原因. 以上文献中,在 LSBs 泄露攻击方面,文献[40]首次涵盖了 $d<N^{0.292}$ 的小解密指数攻击结果,而在 MSBs 泄露攻击方面,则是文献[43]首次涵盖了 $d<N^{0.292}$ 的小解密指数攻击结果.

假设在部分私钥泄露攻击中,私钥 d 未泄露部分共分为 n 块. 目前许多研究内容都集中在 LSBs 泄露攻击以及 MSBs 泄露攻击这种 $n=1$ 的情形. 2011 年,Sarkar[44] 研究了针对任意 $n\geq 1$ 的一般情形,从而推广了文献[39]在 LSBs 泄露攻击以及 MSBs 泄露攻击方面的相应结果. 其中,未泄露的块数 n 越多,结果越差. 对于私钥中间数位比特泄露的情况(对应于 $n=2$),之后文献[45]在一定条件下改进了文献[44]中的攻击结果.

3.4 求解私钥与分解模数的等价性证明

根据关系式 $e\cdot d\equiv 1(\mathrm{mod}\ \varphi(N))$ 以及 $\varphi(N)=(p-1)(q-1)$ 可知,如果成功分解 RSA 模数 $N=pq$,那么容易求解出私钥 d 的取值. 反过来考虑,如果成功求解出私钥 d 的取值,那么分解 RSA 模数 $N=pq$ 是否容易? 实际上,该问题存在随机性的多项式时间算法[46]. 2004 年,May[47] 在 $e,d<\varphi(N)$ 并且素因子 p,q 的比特位数相等的条件下,首次给出了确定性的多项式时间算法. 文献[47]的核心内容是通过 Coppersmith 方法解决一个双变元整系数多项式方程求小值解的问题. 之后在 2007 年,Coron 和 May[48] 仅在 $e,d<\varphi(N)$ 的条件下,首次给出了确定性的多项式时间算法,从而解决了 RSA 密码分析中求解私钥 d 与分解模数 N 的等价性证明. 文献[48]的核心内容是通过 Coppersmith 方法解决一个单变元模多项式方程求小值解的问题. 需要注意的是,通过已知的 d 来分解 N 时,文献[48]在模多项式方程中使用的模数是未知的 $\varphi(N)$. 已知 d 的意义在于找到了一个已知数 $ed-1$,使得未知的 $\varphi(N)$ 整除已知的 $ed-1$. 由 $\varphi(N)=(p-1)(q-1)=N-(p+q)+1$ 可知 $x^{(0)}-(N+1)\equiv 0(\mathrm{mod}\ \varphi(N))$,其中 $x^{(0)}=p+q$. 如果素因子 p,q 的比特位数相等,那么 $|x^{(0)}|<3N^{0.5}$. 此时根据第 2.3 节中文献[14]给出的关于单变元线性多项式模未知数求小值解的结论,直接可证分解 N 是多项式可行的. 所以直接应用文献[14]中的结果,即可得到与文献[47]同样的结论. 当素因子 p,q 的比特位数不相等时,文献[48]在上述思路的基础上,进一步证明了求解私钥 d 与分解模数 N 的等价性.

3.5 隐式分解问题的分析

对于两个 RSA 模数 $N_1=p_1q_1$ 与 $N_2=p_2q_2$,假定 N_1 与 N_2 均为 $\log_2 N$ 比特,素因子 q_1 与 q_2 均为 $\alpha\log_2 N$ 比特,素因子 p_1 与 p_2 共享 $t\log_2 N$ 比特. RSA 密码分析中的隐式分解问题(Implicit Factorization Problem)即当 t,α 满足怎样的关系时,可以有效分解 RSA 模数 N_1 与 N_2. 回顾 MSBs 为最高数位比特

(Most Significant Bits),LSBs 为最低数位比特(Least Significant Bits).素因子 p_1 与 p_2 共享的 $t\log_2 N$ 比特,既可以是 MSBs,也可以是 LSBs,还可以是中间数位比特.另外,该问题可以推广到两个以上 RSA 模数的情况.

2009 年,May 与 Ritzenhofen[21]首次提出了上述隐式分解问题,并且针对素因子 p_1 与 p_2 共享 LSBs 的情形,指出只要 $t>2\alpha$ 就可以有效分解 RSA 模数 N_1 与 N_2.文献[21]首先构造了一个二维格,然后证明了当 $t>2\alpha$ 时,(q_1,q_2) 为格中的最短非零向量,最后通过格基约化算法即可得到 q_1 与 q_2,进而分解 N_1 与 N_2.2010 年,Faugère 等人[22]研究了素因子 p_1 与 p_2 共享 MSBs 与共享中间数位比特两种情形.文献[22]通过构造二维格得到共享 MSBs 情形下的攻击结果 $t>2\alpha$,通过构造三维格得到共享中间数位比特情形下的攻击结果 $t>4\alpha$.对于两个以上 RSA 模数的隐式分解问题,文献[21－22]需要构造更高维数的格,并通过格基约化算法得到格中的最短非零向量.需要指出的是,当构造的格的维数大于等于 3 时,文献[21－22]中结果都是经验式的(heuristic),必须通过实验验证相应的结论.

文献[21－22]采用的方法虽然是格方法,但不是 Coppersmith 方法.2011 年,Sarkar 和 Maitra[15]通过研究近似公共因子问题来研究隐式分解问题,把共享 LSBs 与共享 MSBs 两种情形下的结果同时优化到了 $t>2\alpha-\alpha^2$.2013 年,卢尧等人[49]给出了同样的结果,但是当推广到两个以上 RSA 模数的情况时,结果优于文献[15].文献[15,49]本质上都是在研究多项式模未知数求小值解的问题,因此方法上都属于 Coppersmith 方法.2014 年,彭力强等人[23]联合 Coppersmith 方法与文献[21－22]中的方法,把共享 LSBs 与共享 MSBs 两种情形下的结果同时优化到了 $t>4-4\alpha-4(1-\alpha)^{\frac{3}{2}}$.最后在 2015 年,卢尧等人[24]得到了目前最佳的结果 $t>2\alpha-2\alpha^2$.文献[24]实际上采用了两种不同的方法得到了同样的结果,第一种方法是沿用文献[49]的思路并优化其中的格构造方法,第二种方法则是沿用文献[23]的思路并优化其中 Coppersmith 方法部分的格构造方法.

注意共享 $t\log_2 N$ 比特的 p_1 与 p_2 均为 $(1-\alpha)\log_2 N$ 比特,因此 $t<1-\alpha$,而目前最佳的结果需要的攻击条件为 $t>2\alpha-2\alpha^2$.联立这两个不等式即得 $2\alpha-2\alpha^2<1-\alpha$,又 $0<\alpha<1$,最后得到 $0<\alpha<0.5$.所以两个 RSA 模数的隐式分解问题的分析结果,目前只能适用于 RSA 模数的素因子比特位数不平衡的情形.

3.6　其他 RSA 密码分析

Coppersmith 方法等格方法在 RSA 密码分析中还有许多其他的应用.

例如,素因子部分比特泄露攻击,就是 Coppersmith 最初的文献[2]的应用.文献[2]首次给出了双变元整系数多项式方程求小值解的方法,并且据此推得,对于素因子比特位数平衡的 RSA 模数 $N=pq$,只要素因子 p 泄露 50%的比特(均为 MSBs),即可有效分解 N.而之前 1985 年 Rivest 与 Shamir 的结果[50]需要素因子 p 泄露 66.7%的比特.2001 年,Howgrave-Graham[14]给出了单变元线性多项式模未知数求小值解的方法,利用其结论直接可以推得,素因子 p 泄露 50%的比特即可有效分解 RSA 模数 N.假设素因子 p 未泄露的比特共分为 n 块,那么文献[14]要求 $n=1$,即未泄露的比特必须是连续的.通过把文献[14]的方法从单变元推广到多变元,Herrmann 与 May[17]在 2008 年给出了 $n\geq 2$ 时相应的结果.与部分私钥泄露攻击类似,未泄露的块数 n 越多,结果越差.例如 $n=2$ 时,需要素因子 p 泄露 58.6%的比特,当 $n\to\infty$ 时,需要素因子 p 泄露大约 70%的比特.

再如,作为小解密指数攻击的推广,还可以利用 Coppersmith 方法进行共模攻击.假设多个 RSA 密码的加密解密指数对 $(e_1,d_1),(e_2,d_2),\cdots,(e_m,d_m)$ 共用同一个 RSA 模数 N,并且 $d_1,d_2,\cdots,d_m<N^{\beta}$,共模攻击即求得为了分解公共模数 N,β 需要满足的条件.当 $m=1$ 时,即为小解密指数攻击.文献[51－55]研究了共模攻击,其中文献[55]给出了目前最佳的结果 $\beta<1-\sqrt{2/(3m+1)}$.

4　RSA 密码变体分析

为了提高 RSA 密码的加密速度或者解密速度,抑或为了提高 RSA 密码的安全性,人们提出了多种多样的 RSA 密码变体.例如为了提高解密速度,同时保证密码的安全性,Takagi[56]在 1998 年提出可以使用新型的 RSA 模数 $N=p^rq(r\geq 2)$,该方案根据加密解密指数 e,d 的关系定义可以得到两种 RSA 密码变体.第一

种变体采用 $e\cdot d\equiv 1(\mathrm{mod}\ p^{r-1}(p-1)(q-1))$，称之为 Prime Power RSA；第二种变体采用 $e\cdot d\equiv 1(\mathrm{mod}(p-1)(q-1))$，称之为 Takagi's RSA. 也有文献把这两种变体都称为 Prime Power RSA，或者都称为 Takagi's RSA，此处的命名主要为了区分这两种密码变体. 1990 年，Wiener[29] 提出基于连分数的小解密指数攻击之后，又从抵抗小解密指数攻击的角度提出了两种密码变体：CRT-RSA、Common Prime RSA. CRT-RSA 主要是通过中国剩余定理来改进 RSA 密码的解密过程，其中用 $d_p\equiv d(\mathrm{mod}(p-1))$ 以及 $d_q\equiv d(\mathrm{mod}(q-1))$ 取代原来的 d 进行解密. 其中使用 p,q 以及 $d_p\equiv d(\mathrm{mod}(p-1))$，$d_q\equiv d(\mathrm{mod}(q-1))$，取代原来的 d 进行解密. Common Prime RSA 则要求 $p-1$ 与 $q-1$ 有着较大的公共因子，不妨设 $p=2ga+1$，$q=2gb+1$，其中 $\gcd(a,b)=1$，那么在该密码变体中加密解密指数 e,d 的关系定义为 $e\cdot d\equiv 1(\mathrm{mod}2gab)$.

下面分别以 Prime Power RSA，Takagi's RSA，CRT-RSA，Common Prime RSA 为例，介绍基于格的 Coppersmith 方法在 RSA 密码变体分析中的应用.

4.1 Prime Power RSA 的分析

在 Prime Power RSA 中，模数 $N=p^rq(r\geq 2)$，加密解密指数 e,d 满足 $e\cdot d\equiv 1(\mathrm{mod}\ p^{r-1}(p-1)(q-1))$，并且一般默认素因子 p,q 的比特位数是平衡的.

Prime Power RSA 的分析主要是一些小解密指数攻击结果. Takagi[56] 在 1998 年提出该密码变体后，又指出当 $d<N^{\frac{1}{2(r+1)}}$ 时，就可以通过连分数攻击分解模数 N. 之后人们通过 Coppersmith 方法不断进行优化，主要是研究模多项式方程求小值解的问题，分为模数未知与模数已知两种情况. 根据 $e\cdot d\equiv 1(\mathrm{mod}\ p^{r-1}(p-1)(q-1))$，可知存在正整数 k，使得 $e\cdot d-1=kp^{r-1}(p-1)(q-1)$. 在把该方程变成模方程的过程中，既可以选择未知的模数 p，p^{r-1}，又可以选择已知的模数 e. 2004 年，May[57] 通过选择未知模数 p 得到了攻击结果 $d<N^{\frac{r}{(r+1)^2}}$，通过选择未知模数 p^{r-1} 得到了攻击结果 $d<N^{\frac{(r-1)^2}{(r+1)^2}}$. 2015 年，卢尧等人[20] 在选择未知模数 p^{r-1} 的基础之上，在格构造时充分利用 p^r 整除 N 这一信息，把攻击结果改进到了 $d<N^{\frac{r(r-1)}{(r+1)^2}}$. 当选用已知模数 e 时，Sarkar[58-59] 分别在 2014 年和 2015 年给出了新的小解密指数攻击结果. 文献[58-59]的分析过程比较复杂，结果描述也比较烦琐，总体来说，当 r 比较小的时候，可以改进之前的攻击结果.

1999 年，Boneh 等人[60] 研究了模数 $N=p^rq(r\geq 2)$ 的分解问题. 他们指出，只要素因子 p 泄露 $1/(r+1)$ 比特，即可在多项式时间内分解 N. 如果 r 的数量级达到 $\log_2 p$，那么只需要素因子 p 泄露常数个比特，而这些比特也可以通过穷搜的方法获得. 因此模数 $N=p^rq(r\geq 2)$ 中不能使用过大的 r. Boneh 等人的结果实际上是素因子部分比特泄露攻击，与文献[14]类似，采用的是单变元线性多项式模未知数求小值解的方法. 之后在 2005 年，Blömer 与 May[61] 通过研究双变元整系数多项式方程求小值解的问题，改进了文献[60]的上述结果. 研究 $N=p^rq(r\geq 2)$ 的分解问题，源于 $N=p^rq$ 不仅应用在 Prime Power RSA、Takagi's RSA 两种密码变体中，还应用在 ESIGN[62] 与 EPOC[63] 中. 除此之外，还有针对 $N=p^rq^s$ 的分解问题的研究[64-65].

4.2 Takagi's RSA 的分析

在 Takagi's RSA 中，模数 $N=p^rq(r\geq 2)$，加密解密指数 e,d 满足 $e\cdot d\equiv 1(\mathrm{mod}(p-1)(q-1))$，同样默认素因子 p,q 的比特位数是平衡的.

小解密指数攻击方面，Itoh，Kunihiro 与 Kurosawa[66] 在 2008 年，通过推广文献[12]中的方法，得到了目前最佳的结果 $d<N^{\frac{2-\sqrt{2}}{r+1}}$. 实际上当 $r=1$ 时，就得到了文献[12]中的结果 $d<N^{0.292}$. 之后在 2016 年，Takayasu 与 Kunihiro[67] 按照文献[13]的思路，通过引入变量替换的技巧，简化了文献[66]中的格构造方法.

部分私钥泄露攻击方面，黄章杰等人[68] 相继给出了 LSBs 泄露攻击、MSBs 泄露攻击、中间数位比特泄露攻击的结果. 其中 LSBs 泄露攻击的结果，当 $r=1$ 时即为文献[39]中的相应结果. MSBs 泄露攻击的结果与中间数位比特泄露攻击的结果相同，但是 MSBs 泄露攻击的结果，当 $r=1$ 时劣于文献[39]中的相应结果. MSBs 泄露攻击中得到的是整系数多项式方程，而文献[68]把之当作模多项式方程进行处理，尽管方便之后变量替换技巧的引入，但是因为没有充分利用信息从而导致了较差的结果.

除此之外，Kunihiro 与 Kurosawa[69] 在 2007 年推广了文献[48]中的格构造方法，针对该密码变体给出了求解私钥与分解模数的等价性证明. 文献[69]构造的格基方阵不是下三角方阵，因此 Kunihiro 与 Kurosa-

wa 通过引入新的技巧来重点解决格的行列式的计算问题.

4.3 CRT-RSA 的分析

在 CRT-RSA 中,使用 p,q 与 $d_p \equiv d(\mathrm{mod}(p-1)),d_q \equiv d(\mathrm{mod}(q-1))$,取代原来的 d 进行解密. 收到密文 C 之后,计算 $M_p \equiv C^{d_p}(\mathrm{mod}\ p),M_q \equiv C^{d_q}(\mathrm{mod}\ q)$,之后通过中国剩余定理得到整数 M,满足 $M \equiv M_p(\mathrm{mod}\ p),M \equiv M_q(\mathrm{mod}\ q)$. 可以验证 M 满足 $M \equiv C^d(\mathrm{mod}\ N)$,即为所要的明文.

CRT-RSA 的意义在于,一方面可以使得 d_p,d_q 很小从而提高解密速度,另一方面可以使得 d 较大从而抵抗针对 RSA 密码的小解密指数攻击. 然而,之后人们又开始考虑 d_p,d_q 很小时 CRT-RSA 的安全性问题,即针对 CRT-RSA 的小解密指数攻击. 2002 年,May[70] 研究了 p,q 的比特位数不平衡的情况. May 基于多项式模方程求小值解情形下的 Coppersmith 方法,依次给出了 $q < N^{0.382}$ 情形下与 $q < N^{0.375}$ 情形下的两种小解密指数攻击. 2006 年,Bleichenbacher 与 May[71] 给出了适用于 $q < N^{0.468}$ 情形下的小解密指数攻击. 另外,针对 p,q 的比特位数平衡的情况,Bleichenbacher 与 May 指出当 $d_p,d_q < \min\{(N/e)^{0.4},N^{0.25}\}$ 时,即可根据 Coppersmith 方法分解 CRT-RSA 的模数 N. 2007 年,Jochemsz 与 May[72] 同样针对 p,q 的比特位数平衡的情况,指出当 $d_p,d_q < N^{0.073}$ 即可根据 Coppersmith 方法分解模数 N,这个界与加密指数 e 无关. 2010 年,Herrmann 与 May[13] 回顾了 Jochemsz 与 May 的工作,尽管在理论上没能改进 Jochemsz 与 May 的结果,但是因为所构造的格的维数更低,所以在实验中时间代价低,运行效率高.

针对 CRT-RSA 还存在部分私钥泄露攻击. 2003 年,Blömer 与 May[38] 在研究针对 RSA 密码的部分私钥泄露攻击时,也研究了针对 CRT-RSA 的攻击. 假设 $d_p \approx p$,并且加密指数 e 非常小,为 $\log_2 N$ 的多项式数量级,那么 Blömer 与 May 指出,只要 d_p 或者 d_q 泄露的比特为 LSBs 且达到 50%,就足够分解模数 N. 当 d_p 或者 d_q 泄露的比特为 MSBs 时,Blömer 与 May 的攻击适用于 $e < N^{0.25}$. 2009 年,Sarkar 与 Maitra[73] 研究了 d_p,d_q 较小并且同时泄露 MSBs 的情况,他们的方法实际上为文献[72]中小解密指数攻击方法的推广. 2014 年,卢尧等人[74] 回顾了文献[38]中的工作. 对于 d_p 或者 d_q 泄露 MSBs 的情况,他们在 d_p,d_q 较小的情形下,改进了文献[38]中的结果;对于 d_p 或者 d_q 泄露 LSBs 的情况,他们的攻击改进了文献[38]中的结果,并且适用于 $e < N^{0.375}$. 2015 年,Takayasu 与 Kunihiro[75] 继续改进了上述部分私钥泄露攻击. 无论 d_p 或者 d_q 是泄露 MSBs 还是泄露 LSBs,Takayasu 与 Kunihiro 的攻击都适用于 $e < N^{0.375}$,并且在结果上优于文献[38]与文献[74]. 对于 d_p,d_q 同时泄露 MSBs 的情况,Takayasu 与 Kunihiro 改进了文献[73]的结果. 文献[73]只适用于较小的 d_p,d_q,而他们的攻击也适用于 $d_p,d_q \approx N^{0.5}$,并且加密指数 e 的适用范围也达到了 $e < N$. 类似的,Takayasu 与 Kunihiro 也研究了 d_p,d_q 同时泄露 LSBs 的情况. 2016 年,Takayasu 与 Kunihiro[76] 通过深入挖掘格构造方法,进一步研究了 d_p 或者 d_q 泄露 LSBs 泄露的情况. 他们的攻击在 $e < N^{0.375}$ 的情况下所需泄露的 d_p 或者 d_q 的比特位数最少,优于之前所有的结果.

4.4 Common Prime RSA 的分析

在 Common Prime RSA 中,模数 $N = pq$ 选择必须使得 $p-1$ 与 $q-1$ 有着较大的公共因子. 不失一般性,可设 $p = 2ga+1,q = 2gb+1$,其中 a 与 b 互素,即 $\gcd(a,b) = 1$. 加密解密指数 e,d 满足关系式 $e \cdot d \equiv 1(\mathrm{mod}2gab)$. 如果 $g \simeq N^{\gamma}$,那么 $2gab \simeq N^{1-\gamma}$. 下面仅给出针对 Common Prime RSA 的小解密指数攻击,其中设 $e \simeq N^{1-\gamma},d \simeq N^{\beta}$.

1990 年,Wiener[29] 基于连分数攻击,指出当 $\beta < \frac{1}{4} - \frac{1}{2}\gamma$ 时,即可在多项式时间内分解 N. 2006 年,Hinek[77] 回顾了文献[29]中的工作,并且给出了两类格攻击. Hinek 的结果表明,当 $\beta < \gamma^2$ 或者 $\beta < \frac{2}{5}\gamma$ 时,N 会在多项式时间内被分解. 紧接着,Jochemsz 与 May[10] 从另外一个角度研究了文献[77]中的方程,改变了方程中的未知变元,进而把结果改进到了 $\beta < \frac{1}{4}(4+4\gamma-\sqrt{13+20\gamma+4\gamma^2})$. 2013 年,Sarkar 与 Maitra[78] 又提出两种改进的小解密指数攻击,第一种攻击适用于 $\gamma \leq 0.051$,第二种攻击适用于 $0.051 < \gamma \leq 0.208\ 7$. 在以上的小解密指数攻击中,当 $\gamma \geq 0.208\ 7$ 时,Jochemsz 与 May[10] 的结果是最好的. 到 2015 年,卢尧等[20] 基于其得到的多项式模未知数求小值解的新结论,指出只要 $\beta < 4\gamma^3,\gamma > \frac{1}{4}$ 即可分解 N. 当 $\gamma \geq$

0.387 2 时,卢尧等人的工作再次改进了 Jochemsz 与 May[10] 的结果. 并且随着 γ 的增大,改进越明显,例如 γ 逼近 0.5 时,把 β 的界从原来最佳的 0.275 2 改进到了 0.5.

5 结 论

本文从格方法与分析应用两个方面介绍了基于格的 RSA 密码分析. 从格方法上来说,有在高维格中求解近似 SVP 的 Coppersmith 方法,也有在低维格中求解精确 SVP 的其他方法. 从分析应用上来说,有针对 RSA 密码的多种类型的分析结果,也有针对多种 RSA 密码变体的分析结果. Coppersmith 方法一直是基于格的 RSA 密码分析的主要方法,它研究的是针对多项式方程求小值解的问题,当其基本思想成熟后,工作重心就转变为格的构造. RSA 密码分析结果被不断改进,正是源于格的构造被不断优化. 在 RSA 密码分析中,小解密指数攻击占据着核心的地位,诸如针对 RSA 密码的部分私钥泄露攻击、共模攻击,以及针对各种 RSA 密码变体的小解密指数攻击等,都可以看作是针对 RSA 密码的小解密指数攻击的推广. 目前最佳的攻击结果需要的条件仍然是 $d < N^{0.292}$,如果能够改进这一结果,那么许多分析结果都有望被改进. 另外,在 Coppersmith 方法中,除了两种最初的多项式方程求小值解问题之外,后来的多项式模未知数求小值解的问题也十分重要,目前求解私钥 d 与分解模数 N 的等价性证明、隐式分解问题的分析、素因子部分比特泄露攻击等的最佳结果也正来源于该问题的研究. 最后,与其他大部分分析应用中可以分解模数不同,小加密指数攻击不但需要除了加密指数较小以外的其他条件,而且只能恢复明文,不能分解模数.

尽管基于格的 RSA 密码分析有着十分丰富的结果,但是 RSA 密码在选取合理参数的情况下仍然是非常安全的. 例如,一般在选取 $N = pq$ 时都会要求 p,q 的比特位数平衡,此时就基本足以抵抗来自隐式分解问题分析的攻击(该攻击的前提是 p,q 的比特位数不平衡);再如,如果不特意强调提高加密解密速度,在随机选取加密解密指数的情况下,一般都会满足 $e,d \simeq N$,此时就足以抵抗小加密指数攻击、小解密指数攻击,以及部分私钥泄露攻击(该攻击的前提是 e,d 不能同时大). 目前通过不断优化 Coppersmith 方法中的格的构造,在 RSA 密码分析结果上获得的改进都是比较微弱的. 而且诸如小解密指数攻击中的 $d < N^{0.292}$ 等核心结果的改进,也成了基于格的 RSA 密码分析中的瓶颈问题.

参 考 文 献

[1] Coppersmith D. Finding a small root of a univariate modular equation[J]. International Conference on Theory & Applicatio,1996,1070:155-165.

[2] Coppersmith D. Finding a small root of a bivariate integer equation; factoring with high bits known[J]. International Conference on Theory & Applicatio,1996,1070:178-189.

[3] Conway J H,Sloane N J A. Sphere packings,lattices and groups[M]. Berlin:Springer Science & Business Media,2013.

[4] Martinet J. Perfect lattices in Euclid Spaces[J]. Grundlehren Der Mathematischen Wissenschaften,2003,327(4):67-108.

[5] Lenstra A K,Lenstra H W,Lovász L. Factoring polynomials with rational coefficients[J]. Mathematische Annalen,1982,261(4):515-534.

[6] 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.

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

[8] Howgrave-Graham N. Finding small roots of univariate modular equations revisited[J]. Prol Crytography and Coding,1997,1355:131-142.

[9] Coron J S. Finding small roots of bivariate integer polynomial equations revisited[J]. Advances in Cryptology-EUROCRYPT 2004,2004,3027:492-505.

[10] Jochemsz E,May A. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants[J]. Springer Berlin Heidelberg,2006,4284:267-282.

[11] May A. New RSA vulnerabilities using lattice reduction methods[D]. Paderborn:University of Paderborn,2003.

[12] Boneh D,Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$ [J]. Information Theory IEEE Transactions on,2000,46(4):1339-1349.

[13] Herrmann M,May A. Maximizing small root bounds by linearization and applications to small secret exponent RSA[J]. International

Conference on Public Key Cryptogr,2010,6056:53-69.
[14] Howgrave-Graham N. Approximate integer common divisors[M]. Berlin:Springer,2001:51-66.
[15] Sarkar S,Maitra S. Approximate integer common divisor problem relates to implicit factorization[J]. IEEE Transactions on Information Theory,2011,57(6):4002-4013.
[16] Van Dijk M,Gentry C,Halevi S,et al. Fully homomorphic encryption over the integers[J]. Advances in Cryptology - EUROCRYPT 2010. DOI:10.1007/978-3-642-13190-5_2.
[17] Herrmann M,May A. Solving linear equations modulo divisors:On factoring given any bits[J]. International Conference on the Theory & Applic,2008,5350:406-424.
[18] Cohn H,Heninger N. Approximate common divisors via lattices[EB/OL]. [2016-12-13]. http://www.microsoft.com/en-us/research/video/approximate-common-divisors-via-lattices/.
[19] Takayasu A,Kunihiro N. Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors[C]//Australasian Conference on Information Security and Privacy. Berlin:Springer,2013:118-135.
[20] Lu Y,Zhang R,Peng L,et al. Solving linear equations modulo unknown divisors:revisited[M]. Berlin:Springer,2015:189-213.
[21] May A,Ritzenhofen M. Implicit factoring:On polynomial time factoring given only an implicit hint[M]. Berlin:Springer,2009:1-14.
[22] Faugère J C,Marinier R,Renault G. Implicit factoring with shared most significant and middle bits[C]//Public Key Cryptography-PKC 2010. Berlin:Springer,2010:70-87.
[23] Peng L,Hu L,Xu J,et al. Further improvement of factoring RSA moduli with implicit hint[C]//Progress in Cryptology-AFRICACRYPT 2014. Berlin:Springer,2014:165-177.
[24] Lu Y,Peng L,Zhang R,et al. Towards optimal bounds for implicit factorization problem[C]//Selected Areas in Cryptography-SAC 2015. Berlin:Springer,2015:462-476.
[25] Peng L,Hu L,Lu Y,et al. Implicit Factorization of RSA Moduli Revisited[C]//International Workshop on Security-IWSEC 2015. Berlin:Springer,2015:67-76.
[26] Peng L,Hu L,Lu Y,et al. Cryptanalysis of Dual RSA[J]. Designs,Codes and Cryptography,2017,83(1):1-21.
[27] Coppersmith D,Franklin M,Patarin J,et al. Low-exponent RSA with related messages[C]//Advances in Cryptology-EUROCRYPT 1996. Berlin:Springer,1996:1-9.
[28] Hastad J. Solving simultaneous modular equations of low degree[J]. SIAM Journal of Computing,1988,17(2):336-341.
[29] Wiener M J. Cryptanalysis of short RSA secret exponents[J]. IEEE Transactions on Information Theory,1990,36(3):553-558.
[30] Blömer J,May A. Low secret exponent RSA revisited[C]//Cryptography and Lattices. Berlin:Springer,2001:4-19.
[31] Kunihiro N. Solving generalized small inverse problems[C]//Australasian Conference on Information Security and Privacy. Berlin:Springer,2010:248-263.
[32] Kunihiro N,Shinohara N,Izu T. A unified framework for small secret exponent attack on RSA[C]//International Workshop on Selected Areas in Cryptography. Berlin:Springer,2011:260-277.
[33] Kunihiro N. On optimal bounds of small inverse problems and approximate GCD problems with higher degree[C]//International Conference on Information Security. Berlin:Springer,2012:55-69.
[34] Boneh D,DeMillo R A,Lipton R J. On the importance of checking cryptographic protocols for faults[C]//Advances in Cryptology-EUROCRYPT 1997. Berlin:Springer,1997:37-51.
[35] Kocher P C. Timing attacks on implementations of Diffie-Hellman,RSA,DSS,and other systems[C]//Advances in Cryptology-CRYPTO 1996. Berlin:Springer,1996:104-113.
[36] Kocher P,Jaffe J,Jun B. Differential power analysis[C]//Advances in Cryptology-CRYPTO 1999. Berlin:Springer,1999:388-397.
[37] Boneh D,Durfee G,Frankel Y. An attack on RSA given a small fraction of the private key bits[C]//Advances in Cryptology-ASIACRYPT 1998. Berlin:Springer,1998:25-34.
[38] Blömer J,May A. New partial key exposure attacks on RSA[C]//Advances in Cryptology-CRYPTO 2003. Berlin:Springer,2003:27-43.
[39] Ernst M,Jochemsz E,May A,de Weger B. Partial key exposure attacks on RSA up to full size exponents[C]//Advances in Cryptology-EUROCRYPT 2005. Berlin:Springer,2005:371-386.
[40] Aono Y. A new lattice construction for partial key exposure attack for RSA[C]//Public Key Cryptography-PKC 2009. Berlin:Springer,2009:34-53.
[41] Sarkar S,Gupta S S,Maitra S. Partial key exposure attack on RSA - improvements for limited lattice dimensions[C]//Progress in Cryptology-INDOCRYPT 2010. Berlin:Springer,2010:2-16.
[42] Joye M,Lepoint T. Partial key exposure on RSA with private exponents larger than N[C]// Information Security Practice and Experience. Berlin:Springer,2012:369-380.
[43] Takayasu A,Kunihiro N. Partial key exposure attacks on RSA:achieving the boneh-durfee bound[C]//International Workshop on Selected Areas in Cryptography. Berlin:Springer International Publishing,2014:345-362.

[44] Sarkar S. Partial key exposure: Generalized framework to attack RSA[C]//Progress in Cryptology-INDOCRYPT 2011. Berlin: Springer, 2011: 76-92.

[45] Wang S, Qu L, Li C, Fu S. A New Attack on RSA with Known Middle Bits of the Private Key[J]. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2015, 98(12): 2677-2685.

[46] Stinson D R. Cryptography: theory and practice[M]. 2nd edition. Florida: CRC press, 2002.

[47] May A. Computing the RSA secret key is deterministic polynomial time equivalent to factoring[C]//Advances in Cryptology-CRYPTO 2004. Berlin: Springer, 2004: 213-219.

[48] Coron J S, May A. Deterministic polynomial-time equivalence of computing the RSA secret key and factoring[J]. Journal of Cryptology, 2007, 20(1): 39-50.

[49] Lu Y, Zhang R, Lin D. Improved bounds for the implicit factorization problem[J]. Advances in Mathematics of Communications, 2013, 7(3): 243-251.

[50] Rivest R L, Shamir A. Efficient factoring based on partial information[C]//Advances in Cryptology-EUROCRYPT 1985. Berlin: Springer, 1985: 31-34.

[51] Howgrave-Graham N, Seifert J P. Extending Wiener's attack in the presence of many decrypting exponents[C]//Secure Networking-CQRE [Secure] 1999. Berlin: Springer, 1999: 153-166.

[52] Sarkar S, Maitra S. Cryptanalysis of RSA with two decryption exponents[J]. Information Processing Letters, 2010, 110(5): 178-181.

[53] Sarkar S, Maitra S. Cryptanalysis of RSA with more than one decryption exponent[J]. Information Processing Letters, 2010, 110(8): 336-340.

[54] Aono Y. Minkowski sum based lattice construction for multivariate simultaneous Coppersmith's technique and applications to RSA[C]//Information Security and Privacy. Berlin: Springer, 2013: 88-103.

[55] Takayasu A, Kunihiro N. Cryptanalysis of RSA with Multiple Small Secret Exponents[C]//ACISP. Berlin: Springer, 2014: 176-191.

[56] Takagi T. Fast RSA-type cryptosystem modulo $p^k q$ [C]//Advances in Cryptology-CRYPTO 1998. Berlin: Springer, 1998: 318-326.

[57] May A. Secret Exponent Attacks on RSA-type Schemes with Moduli $N = p^r q$ [C]// Public Key Cryptography-PKC 2004. Berlin: Springer, 2004: 218-230.

[58] Sarkar S. Small secret exponent attack on RSA variant with modulus $N = p^r q$ [C]//Designs, Codes and Cryptography, 2014, 73(2): 383-392.

[59] Sarkar S. Revisiting prime power RSA[J]. Discrete Applied Mathematics, 2015, 203: 127-133.

[60] Boneh D, Durfee G, Howgrave-Graham N. Factoring $N = p^r q$ for large r [C]//Advances in Cryptology-CRYPTO 1999. Berlin: Springer, 1999: 326-337.

[61] Blömer J, May A. A tool kit for finding small roots of bivariate polynomials over the integers[C]//Advances in Cryptology-EUROCRYPT 2005. Berlin: Springer, 2005: 251-267.

[62] Fujioka A, Okamoto T, Miyaguchi S. ESIGN: An efficient digital signature implementation for smart cards[C]//Advances in Cryptology-EUROCRYPT 1991. Berlin: Springer, 1991: 446-457.

[63] Okamoto T, Uchiyama S. A new public-key cryptosystem as secure as factoring[C]//Advances in Cryptology-EUROCRYPT 1998. Berlin: Springer, 1998: 308-318.

[64] Lim S, Kim S, Yie I, et al. A generalized Takagi-cryptosystem with a modulus of the form $p^r q^s$ [C]//. Progress in Cryptology-INDOCRYPT 2000. Berlin: Springer, 2000: 283-294.

[65] Coron J S, Faugére J C, Renault G, et al. Factoring $N = p^r q^s$ for Large r and s [C]//Topics in Cryptology-CT-RSA 2016. Berlin: Springer, 2016: 448-464.

[66] Itoh K, Kunihiro N, Kurosawa K. Small secret key attack on a variant of RSA (due to Takagi)[C]//Topics in Cryptology-CT-RSA 2008. Berlin: Springer, 2008: 387-406.

[67] Takayasu A, Kunihiro N. How to Generalize RSA Cryptanalyses[C]//Public Key Cryptography-PKC 2016. Berlin: Springer, 2016: 67-97.

[68] Huang Z, Hu L, Xu J, et al. Partial key exposure attacks on Takagi's variant of RSA[C]//Applied Cryptography and Network Security. Berlin: Springer International Publishing, 2014: 134-150.

[69] Kunihiro N, Kurosawa K. Deterministic polynomial time equivalence between factoring and key-recovery attack on Takagi's RSA[C]//Public Key Cryptography-PKC 2007. Berlin: Springer, 2007: 412-425.

[70] May A. Cryptanalysis of unbalanced RSA with small CRT-exponent[C]//Advances in Cryptology-CRYPTO 2002. Berlin: Springer, 2002: 242-256.

[71] Bleichenbacher D, May A. New attacks on RSA with small secret CRT-exponents[C]//Public Key Cryptography-PKC 2006. Berlin: Springer, 2006: 1-13.

[72] Jochemsz E, May A. A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$ [C]//Advances in Cryptology-

CRYPTO 2007. Berlin: Springer, 2007: 395-411.

[73] Sarkar S, Maitra S. Partial key exposure attack on CRT-RSA[C]//International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2009: 473-484.

[74] Lu Y, Zhang R, Lin D. New partial key exposure attacks on CRT-RSA with large public exponents[C]//International Conference on Applied Cryptography and Network Security. Berlin: Springer International Publishing, 2014: 151-162.

[75] Takayasu A, Kunihiro N. Partial key exposure attacks on CRT-RSA: better cryptanalysis to full size encryption exponents[C]//International Conference on Applied Cryptography and Network Security. Berlin: Springer International Publishing, 2015: 518-537.

[76] Takayasu A, Kunihiro N. Partial key exposure attacks on CRT-RSA: general improvement for the exposed least significant bits[C]//International Conference on Information Security. Berlin: Springer International Publishing, 2016: 35-47.

[77] Hinek M J. Another look at small RSA exponents[C]//Topics in Cryptology-CT-RSA 2006. Berlin: Springer, 2006: 82-98.

[78] Sarkar S, Maitra S. Cryptanalytic results on Dual CRT and Common Prime RSA[J]. Designs, Codes and Cryptography, 2013, 66(1/2/3): 157-174.

Lattice-Based Cryptanalysis of RSA Cryptosystem

Li Chao[a,b], Wang Shixiong[a], Qu Longjiang[b], Fu Shaojing[a]

(a. College of Computer Science; b. College of Science,
National University of Defense Technology, Changsha 410073, China)

Abstract: Lattice plays an important role in the field of cryptanalysis of public key cryptosystem. In 1996, Coppersmith introduces new ways of finding small roots of polynomial equation. According to his work, from the problem of some attacks on RSA cryptosystem, one can derive the problem of finding short vectors in lattice. Lattice-based cryptanalysis of RSA cryptosystem thus begins to attract attentions, and the method has been developed into "Coppersmith's method" after some reformulations and extensions. On the one hand, about lattice-based Coppersmith' method, this paper introduces the methods of finding small roots of modular polynomial equation and integer polynomial equation, and the method of solving approximate common divisor problem. Besides, another lattice method which needs to find the shortest vector in a low-dimension lattice is also presented. On the other hand, about the cryptanalysis of RSA cryptosystem, this paper summarizes small public exponent attack, small private exponent attack, partial key exposure attack, deterministic polynomial-time equivalence of computing the private key d and factoring the modulus N, cryptanalysis of the implicit factorization problem, partial prime factor exposure attack, and cryptanalysis of RSA with multiple exponents and the same modulus. Moreover, we take Prime Power RSA, Takagi's RSA, CRT-RSA and Common Prime RSA for examples, and introduce cryptanalysis of RSA variants by means of lattice methods.

Keywords: lattice; RSA cryptosystem; Coppersmith's method; LLL algorithm

[责任编辑　陈留院]