隐式相关私钥分解问题研究

郑梦策

中国科学技术大学　信息科学技术学院

2020 年 9 月 20 日

报告提纲

报告提纲

RSA 密码算法

- RSA 算法于 1977 年由 Rivest，Shamir 和 Adleman 提出
- RSA 算法的安全性基于大整数分解问题的困难性
- RSA 算法的三个组成算法
  - 密钥生成算法
  - 加密算法
  - 解密算法
- RSA 算法的正确性由欧拉定理确保

RSA 密码算法

- RSA 算法实例的参数：N、p、q、e、d 和 $\varphi(N)$
  - 模数为 $N = pq$，其中 p 和 q 是相同比特长度的大素数
  - 公私钥对为 (e, d) 且满足 $ed \equiv 1 \bmod \varphi(N)$
  - 欧拉函数为 $\varphi(N) = (p-1)(q-1)$
  - 加密操作为 $c = m^e \bmod N$，解密操作为 $c^d \bmod N$
- RSA 算法中的关键等式：$ed \equiv 1 \bmod \varphi(N)$
  - 存在未知正整数 k 使得$ed = k(N + 1 - p - q) + 1$成立
  - 针对求解该关键等式已提出许多攻击
  - 攻击中通常考虑使用较短的私钥

两类典型攻击

- 部分私钥泄露攻击
  - 给定私钥比特的一小部分
  - 例如：$d = \bar{d} + d'$，其中已知高位比特 $\bar{d}$ 和未知低位比特 d'
  - 目标为恢复出完整的私钥 d
- 隐式分解问题
  - 给定可输出素数因子隐式信息的谕言机
  - 例如：$N_1 = p_1 q_1$ 和 $N_2 = p_2 q_2$，其中 p_1, p_2 有相同低位比特
  - 目标为找到 q_1, q_2 且分解 N_1, N_2

研究问题

- 假如攻击者已知私钥的隐式信息?
  - 给定隐式相关私钥的相同高位与低位比特的数目
  - 例如：$d_2 - d_1 = d_{21}D$，其中已知 D 和未知中间位比特 d_{21}
  - 目标为使用给定隐式关系分解 RSA 模数
- 新型研究情形主要出于理论研究兴趣
  - 揭示弱前提下的 RSA 密码算法的脆弱性
  - 延展并丰富 RSA 算法相关的密码分析工作
  - 不完美的随机性可能导致产生隐式相关私钥

隐式相关私钥分解问题

令 $(N_1, e_1, d_1), \ldots, (N_n, e_n, d_n)$ 为 n 对不同的 RSA 密钥对，其中 $N_1, \ldots, N_n$ 为相同比特长度的模数且素数因子也是相同比特长度。给定隐式信息，即私钥 $d_1, \ldots, d_n$ 中某些对应位置存在相同比特，在何种条件下可有效分解相应的 RSA 模数。

我们考虑全规模情形，即 $e_i \approx N$。假设 $d_i \approx N^{\delta}$ 满足隐式关系

$$d_j = d_i + d_{ji}D,\ 1 \leq i < j \leq n,$$

其中已知 D，未知 d_{ji} 表示任意两个未知中间位比特的差异值，且有 $D \approx N^{\gamma}$ 与 $|d_{ji}| \approx N^{\beta}$。

格方法

$$\mathcal{L} = \mathbb{Z}\mathbf{x}_1 + \cdots + \mathbb{Z}\mathbf{x}_n = \left\{ \sum_{i=1}^{n} a_i \mathbf{x}_i : a_i \in \mathbb{Z} \right\}$$

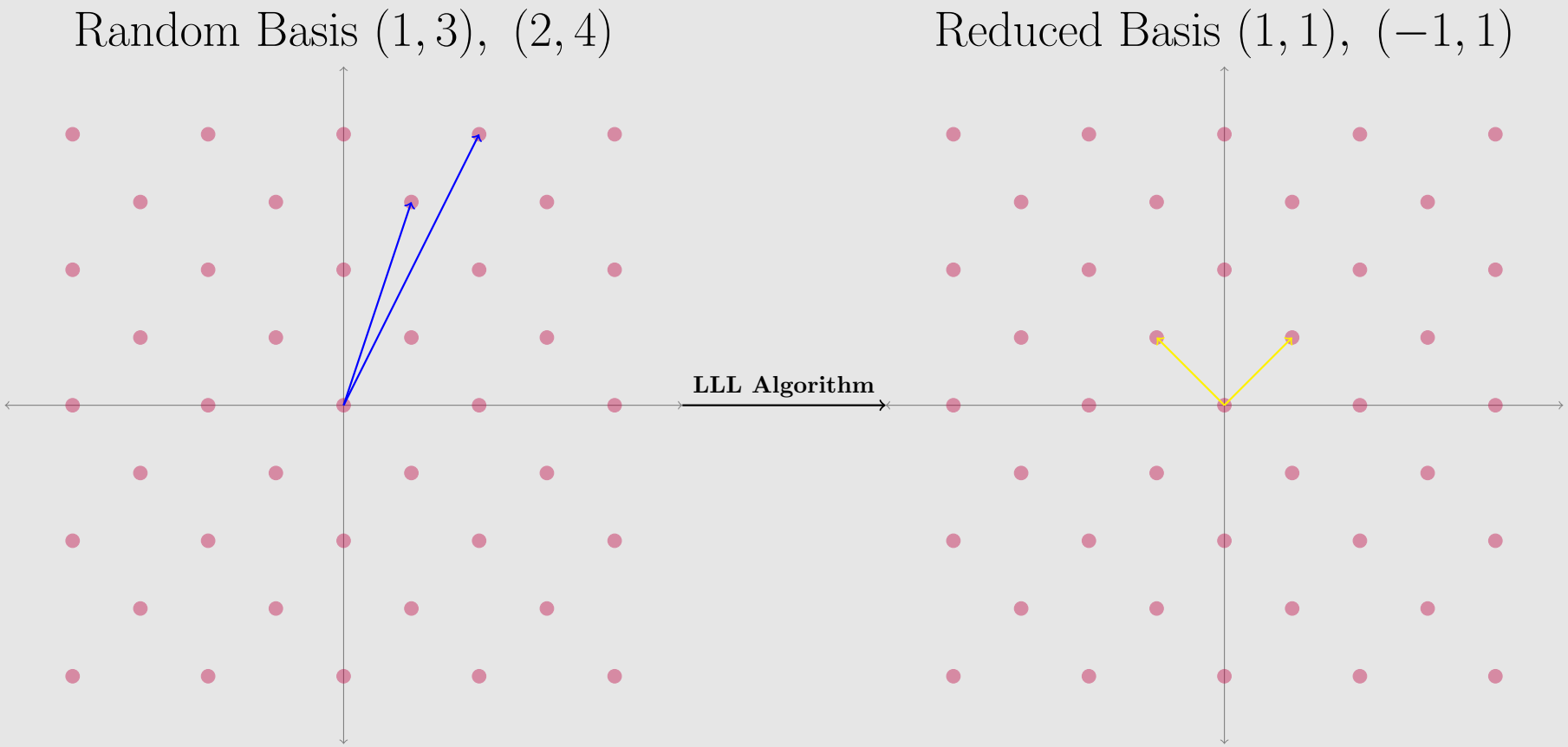
- 格基向量：$\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathbb{R}^n$
- 格基矩阵：$\mathbf{X} = (x_{ij})_{n \times n}$
- 格行列式：$\det(\mathcal{L}) = |\det(\mathbf{X})|$
- 格的维数：$\dim(\mathcal{L}) = n$

格基约化算法

$$|\mathbf{v}_1|, \ldots, |\mathbf{v}_\ell| \leq 2^{\frac{n(n-1)}{4(n+1-\ell)}} \det(\mathcal{L})^{\frac{1}{(n+1-\ell)}}$$

- LLL 算法于 1982 年由 Lenstra，Lenstra 和 Lovász 提出
- 可在多项式时间内输出格中近似短向量
- 其它优化目标的格基约化算法：L^2 算法，BKZ 算法
- 格基约化算法可应用于公钥密码分析

格基约化算法



格分析技术

- 格分析技术于 1996 年由 Coppersmith 提出
- 将密码分析归约到求解多项式模方程
- 待求解方程来自密码算法的数学原理
- 方程的解与秘密信息（如私钥）相关联
- 恢复出秘密信息从而成功攻破密码算法

格分析技术

$$f(x) = x + a, \quad f(x_0) \equiv 0 \bmod b \ \Rightarrow \ g(x) = 0, \quad |x_0| \leq X$$

1. 函数集合：构造解均为 $x_0 \bmod b^m$ 的 $f_1(x), \ldots, f_n(x)$
2. 格基矩阵：$f_1(xX), \ldots, f_n(xX)$ 的系数向量作为格基向量
3. 格基约化：应用格基约化算法计算出符合条件的 $g(xX)$
4. 方程求解：应用 Gröbner 基方法求解一般整方程 $g(x)$

格分析技术

	1	x	x^2	x^3	x^4	x^5	x^6
f_1	b^6						
f_2	ab^5	b^5X					
f_3	a^2b^4	$2ab^4X$	b^4X^2				
f_4	a^3b^3	$3a^2b^3X$	$3ab^3X^2$	b^3X^3			
f_5	$*$	$*$	$*$	$*$	b^2X^4		
f_6	$*$	$*$	$*$	$*$	$*$	bX^5	
f_7	$*$	$*$	$*$	$*$	$*$	$*$	X^6

- 定义 $f_{i+1}(xX) = f^i(xX)b^{m-i},\ i = 0, \ldots, m$
- 求解条件：$\det(\mathcal{L}) < b^{mn}$

报告提纲

具体情形

- 给定 (N_1, e_1, d_1) 和 (N_2, e_2, d_2) 以及隐式相关私钥 d_1, d_2
  - N_1, N_2 的比特长度相同，表示为 $\log_2 N$
  - $e_1 \approx e_2 \approx N$，即公钥与模数比特长度相近
  - $d_1 \approx d_2 \approx N^{\delta}$ 满足 $d_2 = d_1 + d_{21}D$，$|d_{21}| \approx N^{\beta}$、$D \approx N^{\gamma}$
- 采用基于高斯启发式的分裂技巧
  - 构造由格基矩阵 $\begin{bmatrix} a_0 & e_1 \\ 0 & N_1 \end{bmatrix}$ 生成的 2 维格
  - $d_1 = a_1 c_1 + a_2 c_2$，其中已知 a_1, a_2 和未知 c_1, c_2
  - $|a_1| \approx |a_2| \approx N^{\frac{1}{4}}$ 且 $|c_1| \approx |c_2| \approx N^{\delta - \frac{1}{4}}$

模方程

- 结合 $d_1 = a_1c_1 + a_2c_2$ 和给定隐式关系 $d_2 = d_1 + d_{21}D$
  - $d_2 = a_1c_1 + a_2c_2 + d_{21}D$，其中未知变量 c_1, c_2, d_{21}
  - 将 d_2 代入 RSA 关键等式 $e_2d_2 = k_2(N_2 + 1 - p_2 - q_2) + 1$
  - $e_2(a_1c_1 + a_2c_2 + d_{21}D) - k_2(N_2 + 1 - p_2 - q_2) - 1 = 0$
- 求解含有 4 个变量的多项式函数 f
  - $f(x, y, z, w) := x(y - N_2 - 1) + e_2a_1z + e_2Dw - 1 \bmod e_2a_2$
  - 未知变量：$x = k_2$，$y = p_2 + q_2$，$z = c_1$ 与 $w = d_{21}$
  - 应用线性化技巧令 $u := xy - 1$
  - $\bar{f}(x, z, w, u) := u - (N_2 + 1)x + e_2a_1z + e_2Dw \bmod e_2a_2$
  - $f^*(x, y, z, w) = x(y - N_2 - 1) + e_2a_1z + e_2a_2w - 1 \bmod e_2D$

函数集合

定义多项式函数 $g_{[i,j,k,l_1,l_2]}$，其中 $s \in \mathbb{Z}_+$ 和 $i,j,k,l_1,l_2 \in \mathbb{N}$

$$g_{[i,j,k,l_1,l_2]}(x,y,z,w,u) := x^i y^j z^{l_1} w^{l_2} \bar{f}^k(x,z,w,u) E^{s-k},\ E = e_2 a_2$$

构造多项式函数集合 $\mathcal{G} := \mathcal{G}_1 \cup \mathcal{G}_2$，$0 \le \tau \le 1$ 为待优化参数

$$\begin{aligned}
\mathcal{G}_1 := \{&g_{[i,0,k,l_1,l_2]}(x,y,z,w,u) : k = 0,\ldots,s; i = 0,\ldots,s-k; \\
&l_1 = 0,\ldots,s-k-i; l_2 = 0,\ldots,s-k-i-l_1.\} \\
\mathcal{G}_2 := \{&g_{[0,j,k,l_1-l_2,l_2-k]}(x,y,z,w,u) : l_1 = 0,\ldots,s; j = 1,\ldots,\tau l_1; \\
&l_2 = 0,\ldots,l_1; k = 0,\ldots,l_2.\}
\end{aligned}$$

方程共同解为 $(k_2,\ p_2+q_2,\ c_1,\ d_{21},\ k_2(p_2+q_2)-1)$ 模 E^s

格基矩阵

- $g_{[i,j,k,l_1,l_2]}(xX, yY, zZ, wW, uU)$ 的系数向量生成格基矩阵
  - X，Y，Z，W 与 U 代表未知变量的上界
  - 格基矩阵可保证是方阵且下三角的
- 例如：$s = 1$，$\tau = 1$ 且 $C := -(N_2 + 1)$ 时的格基矩阵

	1	x	z	yz	w	yw	u	yu
$g_{[0,0,0,0,0]}$	E							
$g_{[1,0,0,0,0]}$		EX						
$g_{[0,0,0,1,0]}$			EZ					
$g_{[0,1,0,1,0]}$				EYZ				
$g_{[0,0,0,0,1]}$					EW			
$g_{[0,1,0,0,1]}$						EYW		
$g_{[0,0,1,0,0]}$		CX	e_2a_1Z		e_2DW		U	
$g_{[0,1,1,0,0]}$	C			e_2a_1YZ		e_2DYW	CU	YU

格行列式

- $\det(\mathcal{L})$ 为格基矩阵对角线项的乘积
  - $\mathcal{G}_1$ 中的对角线项为 $X^i Z^{l_1} W^{l_2} U^k E^{s-k}$
  - $\mathcal{G}_2$ 中的对角线项为 $Y^j Z^{l_1-l_2} W^{l_2-k} U^k E^{s-k}$
  - $\det(\mathcal{L}) = X^{s_x} Y^{s_y} Z^{s_z} W^{s_w} U^{s_u} E^{s_E}$
- $s_x,\ s_y,\ s_z,\ s_w,\ s_u,\ s_E$ 为格基矩阵对角线项的计数总和
  - $s_x = \frac{1}{120} s^5,\ s_y = \frac{\tau^2}{20} s^5$
  - $s_z = s_w = s_u = \frac{1+4\tau}{120} s^5$
  - $s_E = \frac{4+11\tau}{120} s^5$

方程求解

- 应用求解条件 $\det(\mathcal{L}) < R^m$，其中 $R = E^s$
  - $X^{s_x} Y^{s_y} Z^{s_z} W^{s_w} U^{s_u} E^{s_E} < R^m$
  - 格维数为 $m = \frac{1+3\tau}{24} s^4$
  - $X^{s_x} Y^{s_y} Z^{s_z} W^{s_w} U^{s_u} E^{s_E} < E^{\frac{1+3\tau}{24} s^5}$
- 代入所有参数并简化后可得基本求解条件
  - $\frac{1}{120} \cdot \xi_x + \frac{\tau^2}{20} \cdot \xi_y + \frac{1+4\tau}{120} \cdot (\xi_z + \xi_w + \xi_u) + \frac{4+11\tau}{120} \cdot \xi_E < \frac{1+3\tau}{24} \cdot \xi_E$
  - ξ_x，ξ_y，ξ_z，ξ_w，ξ_u 与 ξ_E 为解上界与模数的指数表达式
  - $\xi_x + 6\tau^2 \xi_y + (1+4\tau)(\xi_z + \xi_w + \xi_u - \xi_E) < 0$

分析结果 (一)

对于 $f(x,y,z,w) := x(y - N_2 - 1) + e_2 a_1 z + e_2 D w - 1 \bmod e_2 a_2$

$$\xi_x = \delta,\ \xi_y = \frac{1}{2},\ \xi_z = \delta - \frac{1}{4},\ \xi_w = \beta,\ \xi_u = \delta + \frac{1}{2},\ \xi_E = \frac{5}{4}$$

则可推出

$$\delta < \frac{(1-\beta)(1+4\tau) - 3\tau^2}{3 + 8\tau}$$

当优化参数取 $\tau = (\sqrt{177 - 96\beta} - 9)/24$ 时，代入则有不安全界

$$\delta < \frac{25 - 16\beta - \sqrt{177 - 96\beta}}{32}$$

分析结果 (二)

对于 $f^*(x,y,z,w) = x(y - N_2 - 1) + e_2a_1z + e_2a_2w - 1 \bmod e_2D$

$$\xi_x = \delta,\ \xi_y = \frac{1}{2},\ \xi_z = \xi_w = \delta - \frac{1}{4},\ \xi_u = \delta + \frac{1}{2},\ \xi_E = 1 + \gamma$$

则可推出

$$\delta < \frac{(1+\gamma)(1+4\tau) - 3\tau^2}{4 + 12\tau}$$

当优化参数取 $\tau = (\sqrt{\gamma + 2} - 1)/3$ 时，代入则有不安全界

$$\delta < \frac{2\gamma + 3 - \sqrt{\gamma + 2}}{6}$$

隐式相关私钥分解攻击

令 $N_1 = p_1q_1$ 与 $N_2 = p_2q_2$ 为两个比特长度相同的 RSA 模数，其中 p_1，q_1，p_2，q_2 是相同比特长度的大素数。(e_1, d_1)，(e_2, d_2) 为满足下式的加解密指数对：

$$e_1d_1 \equiv 1 \bmod (p_1 - 1)(q_1 - 1),$$
$$e_2d_2 \equiv 1 \bmod (p_2 - 1)(q_2 - 1)$$

假设 $e_1 \approx e_2 \approx N$，$d_1 \approx d_2 \approx N^{\delta}$，其中 N 记为与 N_1，N_2 比特长度相同的整数。给定 $d_2 = d_1 + d_{21}D$ 且 $|d_{21}| \approx N^{\beta}$，$D \approx N^{\gamma}$。那么满足以下条件时，模数 N_1，N_2 可在多项式时间内被分解。

$$\delta < \frac{25 - 16\beta - \sqrt{177 - 96\beta}}{32} \quad \text{或} \quad \delta < \frac{2\gamma + 3 - \sqrt{\gamma + 2}}{6}.$$

具体情形

- 多个 RSA 实例 $(N_i, e_i, d_i),\ 1 \le i \le n$
  - $d_j = d_i + d_{ji}D,\ 1 \le i < j \le n$
  - $e_i \approx N,\ d_i \approx N^{\delta}$
  - $D \approx N^{\gamma},\ |d_{ji}| \approx N^{\beta}$
- 采用基于高斯启发式的分裂技巧
  - $d_1 = a_1c_1 + a_2c_2 + \cdots + a_{2n-1}c_{2n-1}$，其中已知 a_i 和未知 c_i
  - $$\begin{bmatrix} a_0 & 0 & \cdots & 0 & e_2 & \cdots & e_n \\ 0 & b_0 & \cdots & 0 & e_2D & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_0 & 0 & \cdots & e_nD \\ 0 & 0 & \cdots & 0 & N_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & N_n \end{bmatrix}$$

模方程

将私钥 d_1 的表达式代入 RSA 算法关键等式中可推出模方程：

$$x(y - N_1 - 1) + e_1 a_1 z_1 + \cdots + e_1 a_{\hat{n}} z_{\hat{n}} - 1 \bmod e_1 a_{\hat{n}+1}$$

解为 $(k_1, p_1 + q_1, c_1, \ldots, c_{\hat{n}})$，记 $\hat{n} = 2n - 2$。

令 $u = xy - 1$ 则有线性模方程

$$f_{\hat{n}}(x, z_1, \ldots, z_{\hat{n}}, u) = u - (N_1 + 1)x + e_1 a_1 z_1 + \cdots + e_1 a_{\hat{n}} z_{\hat{n}} \bmod e_1 a_{\hat{n}+1}$$

解上界分别为

$$X = N^{\delta},\ Y = N^{\frac{1}{2}},\ Z_i = N^{\frac{2n\delta + 2(n-1)\beta - n + 1}{2(2n-1)}},\ U = N^{\delta + \frac{1}{2}}$$

隐式相关私钥分解攻击

根据基本条件 $\det(\mathcal{L}) < R^m$ 且考虑指数上的关系有

$$2\xi_x + (\hat{n}+1)(\hat{n}+2)\tau^2\xi_y + 2(1+(\hat{n}+2)\tau)(\hat{n}\xi_{z_i} + \xi_u - \xi_E) < 0$$

代入解上界与模数的指数表达式后可得

$$\delta < \frac{(2n\tau+1)(n-2(n-1)\beta) - n(2n-1)\tau^2}{2(2n^2\tau+n+1)}$$

选取特定优化参数 τ 后，不安全界为

$$\delta < \frac{2n^3+2n^2+n-1-4n^2(n-1)\beta}{4n^3} - \frac{\sqrt{(2n-1)(6n^3+3n^2-1-8n^2(n-1)\beta)}}{4n^3}$$

实验结果

特定参数设定时，两个实例情形攻击的理论与实验结果对比：

	γ	β	δ_∞	δ_e	s	τ	m
结果 (一)	0.117	0.038	0.350	0.312	6	0.167	225
结果 (一)	0.078	0.092	0.330	0.296	5	0.200	136
结果 (一)	0.023	0.195	0.290	0.274	7	0.143	351
结果 (二)	0.156	0.061	0.307	0.282	5	0.200	136
结果 (二)	0.131	0.101	0.300	0.278	6	0.167	225
结果 (二)	0.117	0.093	0.296	0.272	6	0.167	225

报告提纲

总结

- 关注隐式相关私钥分解问题
  - 存在私钥隐式关系时如何分解 RSA 模数
  - 应用格方法与特定技巧求解多项式模方程
  - 提出隐式相关私钥分解攻击
  - 进行计算机模拟实验验证攻击的正确性与有效性
- 进一步提升与后续工作
  - 更为有效的格构造方式
  - 对一般规模公钥的通用攻击

谢谢!