RSA and Coppersmith Method

宋 凌

2021.06.09

Outline

- RSA
- Relaxed models for attacking RSA
- Intuition
- Coppersmith method
- Application to RSA

RSA

- p,q 为两大素数，N=pq
- $\varphi(N) = (p-1)(q-1)$
- 选择e，gcd(e,$\varphi(N)$)=1,计算d, 满足ed=1 mod $\varphi(N)$
- 公钥：(N,e)
- 私钥：d
- 加密：取m，c=m^e mod n
- 解密：m=c^d mod n

Attacks on the Implementation or the Mathematics.

- Recover the plaintext
- Recover the private key

Relaxed models

- Stereotyped messages (with partial knowledge of m)
- With partial knowledge of p
- With small decryption exponent d
- …

Intuition

Stereotyped messages

$$c = m^e \pmod{N}$$

$$m = m_0 + x_0$$

"The secret key for the day is: desktop "

$$f(x) = c - (m_0 + x)^e \pmod{N}$$

x is small compared to N

Example

$N, e = 3, c$ are known. m has 512 bits where only the least 72 bits are unknown.

$$f(x) = c - (m_0 + x)^e \mod N$$

⬇

$$f(x) = c - (m_0 + x)^3 \mod N$$

f(x) has a small solution but its coefficients are not small.

Solving f(x)

- Factoring N
  - $f(x) \equiv 0 \bmod p$, $f(x) \equiv 0 \bmod q$
  - Then solving f(x) is easy
- But the factorization of N is unknown
- Recall that x is small

$$f(x) = 0 \pmod{N} \text{ with } |x| < X$$

$$\downarrow$$

$$g(x) = 0 \text{ over } \mathbb{Z}$$

Finding integer roots of integer polynomials is **easy**: we can find roots over R using numerical analysis (e.g., Newton's method) and then round the approximations of the roots to the nearest integer.

An intuitive example

- Let N = 17*19 = 323 and let

$$f(x) = x^2 + 33x + 215$$

Find $f(x) \equiv 0 \bmod N$

- $x_0 = 3$ is a solution, but $f(3) \neq 0$ over $\mathbb{Z}$

Property of g(x):

1. $9f(x)$: multiple of f(x)
2. $N(x+6)$: multiple of N

- Define

$$g(x) = 9f(x) - N(x+6) = 9x^2 - 26x - 3$$

$$f(x_0) \equiv 0 \bmod N \Longrightarrow g(x_0) \equiv 0 \bmod N$$

$$\Longrightarrow g(x_0) = 0 \text{ over } \mathbb{Z}$$

$g(x)$ has small coefficients and satisfies $g(3) = 0$. The root can be found using Newton's method over $\mathbb{R}$.

Let's build theorems for it!

Coppersmith Method

Condition to remove "mod"

- Let $M, X \in \mathbb{N}$ and $F(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$
- Suppose $x_0 \in \mathbb{Z}$ is a solution to $F(x) = 0 \bmod M$ such that $|x_0| < X$.
- Associate with F(x) the row vector

$$b_F = (a_0, a_1 X, a_2 X^2, \dots, a_d X^d)$$

Theorem 19.1.2 *(Howgrave-Graham [268]) Let $F(x), X, M, b_F$ be as above (i.e., there is some x_0 such that $|x_0| \le X$ and $F(x_0) \equiv 0 \pmod{M}$). If $\|b_F\| < M/\sqrt{d+1}$ then $F(x_0) = 0$.*

Proof

Theorem 19.1.2 *(Howgrave-Graham [268]) Let $F(x)$, X, M, b_F be as above (i.e., there is some x_0 such that $|x_0| \leq X$ and $F(x_0) \equiv 0 \pmod{M}$). If $\|b_F\| < M/\sqrt{d+1}$ then $F(x_0) = 0$.*

Proof Recall the Cauchy–Schwarz inequality $(\sum_{i=1}^{n} x_i y_i)^2 \leq (\sum_{i=1}^{n} x_i^2)(\sum_{i=1}^{n} y_i^2)$ for $x_i, y_i \in \mathbb{R}$. Taking $x_i \geq 0$ and $y_i = 1$ for $1 \leq i \leq n$ one has

$$\sum_{i=1}^{n} x_i \leq \sqrt{n \sum_{i=1}^{n} x_i^2}.$$

Now

$$\begin{aligned} |F(x_0)| &= \left| \sum_{i=0}^{d} a_i x_0^i \right| \leq \sum_{i=0}^{d} |a_i| |x_0|^i \leq \sum_{i=0}^{d} |a_i| X^i \\ &\leq \sqrt{d+1} \|b_F\| < \sqrt{d+1} M / \sqrt{d+1} = M \end{aligned}$$

where the third inequality is Cauchy–Schwarz, so $-M < F(x_0) < M$. But $F(x_0) \equiv 0 \pmod{M}$ and so $F(x_0) = 0$. □

If F(x) does not satisfy the condition

- For our F(x), if $||b_F|| < \mathrm{M}/\sqrt{d+1}$ does not hold, how can we do?

They are multiples of M and all have solution $x = x_0$ mod M

- Consider $d + 1$ polynomials

$$G_i(x) = \mathrm{M}x^i \text{ for } 0 \leq i < d$$

and F(x).

- Let $\mathcal{L}$ be defined with these $d + 1$ polynomials.
- Derive a polynomial with small efficient via LLL algorithm.

If F(x) does not satisfy the condition

- Consider $d+1$ polynomials

$$G_i(x) = \mathrm{M}x^i \text{ for } 0 \le i < d$$

and F(x).

- Each row of B associates with a polynomial.
- $\mathcal{L}$ is spanned by $d+1$ row vectors.

$$B = \begin{pmatrix} M & 0 & \cdots & 0 & 0 \\ 0 & MX & \cdots & 0 & 0 \\ \vdots & & & \vdots & \vdots \\ 0 & 0 & \cdots & MX^{d-1} & 0 \\ a_0 & a_1 X & \cdots & a_{d-1}X^{d-1} & X^d \end{pmatrix}$$

LLL algorithm + Howgrave-Graham's theorem

Theorem 19.1.5 *Let the notation be as above and let $G(x)$ be the polynomial corresponding to the first vector in the LLL-reduced basis for L. Set $c_1(d) = 2^{-1/2}(d+1)^{-1/d}$. If $X < c_1(d)M^{2/d(d+1)}$ then any root x_0 of $F(x)$ modulo M such that $|x_0| \le X$ satisfies $G(x_0) = 0$ in $\mathbb{Z}$.*

M^{1/d^2}

Proof Recall that $\underline{b}_1$ satisfies

$$\|\underline{b}_1\| \le 2^{(n-1)/4}\det(L)^{1/n} = 2^{d/4}M^{d/(d+1)}X^{d/2}.$$

Why?

For $\underline{b}_1$ to satisfy the conditions of Howgrave-Graham's theorem (i.e., $\|\underline{b}_1\| < M/\sqrt{d+1}$) it is sufficient that

$$2^{d/4}M^{d/(d+1)}X^{d/2} < M/\sqrt{d+1}.$$

This can be written as

$$\sqrt{d+1}\,2^{d/4}X^{d/2} < M^{1/(d+1)},$$

$d = 3$,
bound is $M^{1/6}$

which is equivalent to the condition in the statement of the theorem. □

Example

Example 19.1.6 Let $M = 10001$ and consider the polynomial

$$F(x) = x^3 + 10x^2 + 5000x - 222.$$

One can check that $F(x)$ is irreducible, and that $F(x)$ has the small solution $x_0 = 4$ modulo M. Note that $|x_0| < M^{1/6}$ so one expects to be able to find x_0 using the above method. Suppose $X = 10$ is the given bound on the size of x_0. Consider the basis matrix

$$B = \begin{pmatrix} M & 0 & 0 & 0 \\ 0 & MX & 0 & 0 \\ 0 & 0 & MX^2 & 0 \\ -222 & 5000X & 10X^2 & X^3 \end{pmatrix}.$$

Running LLL on this matrix gives a reduced basis, the first row of which is

$$(444, 10, -2000, -2000).$$

The polynomial corresponding to this vector is

$$G(x) = 444 + x - 20x^2 - 2x^3.$$

Running Newton's root-finding method on $G(x)$ gives the solution $x_0 = 4$.

Can we do better?

$$B = \begin{pmatrix} M & 0 & \cdots & 0 & 0 \\ 0 & MX & \cdots & 0 & 0 \\ \vdots & & & \vdots & \vdots \\ 0 & 0 & \cdots & MX^{d-1} & 0 \\ a_0 & a_1 X & \cdots & a_{d-1}X^{d-1} & X^d \end{pmatrix}$$

- The bigger X, the better.
- Actually, LLL algorithm + Howgrave-Graham's theorem work well as long as

$$\det(\mathcal{L}) < M^{\text{dim of } L}$$

In the previous theorem, it is $2^{d/4} M^{d/(d+1)} X^{d/2} < M/\sqrt{d+1}$

- Strategies for constructing lattice $\mathcal{L}$
  1. Add rows to $\mathcal{L}$ that contribute less than M to the det
  2. Increase the power of M on the right hand side.

$$\det(\mathcal{L}) < M^{\text{dim}} \implies \det(\mathcal{L}) < \text{bigger modul}us^{\text{dim}}$$

Strategy 1

$$B = \begin{pmatrix} M & 0 & \cdots & 0 & 0 \\ 0 & MX & \cdots & 0 & 0 \\ \vdots & & & \vdots & \vdots \\ 0 & 0 & \cdots & MX^{d-1} & 0 \\ a_0 & a_1X & \cdots & a_{d-1}X^{d-1} & X^d \end{pmatrix}$$

1. Add rows to $\mathcal{L}$ that contribute less than M to the det

Add rows corresponding to $x^iF(x)$ (polynomial multiples of $F(x)$)

$$B = \begin{pmatrix} M & 0 & 0 & 0 & 0 & 0 \\ 0 & MX & 0 & 0 & 0 & 0 \\ 0 & 0 & MX^2 & 0 & 0 & 0 \\ -222 & 5000X & 10X^2 & X^3 & 0 & 0 \\ 0 & -222X & 5000X^2 & 10X^3 & X^4 & 0 \\ 0 & 0 & -222X^2 & 5000X^3 & 10X^4 & X^5 \end{pmatrix}.$$

Exercise 19.1.8 Let $G(x)$ be a polynomial of degree d. Show that taking d x-shifts $G(x), xG(x), \ldots, x^{d-1}G(x)$ gives a method that works for $X \approx M^{1/(2d-1)}$.

Better bound

Strategy 2

2. Increase the power of M on the right hand side.

$$\det(\mathcal{L}) < M^{\mathrm{dim}} \implies \det(\mathcal{L}) < \text{bigger modul}us^{\mathrm{dim}}$$

$$M^{h-1-j} F^j(x) \equiv 0 \bmod M^{h-1}$$

Coppersmith method

Define $G_{i,j}(x) = M^{h-1-j}F^j(x)x^i$ for $0 \leq i < d, 0 \leq j < h$. Note

$$G_{i,j}(x_0) \equiv 0 \bmod M^{h-1}$$

$(d-1)/(d(dh-1)) = \epsilon$

Theorem 19.1.9 *(Coppersmith) Let* $0 < \epsilon < \min\{0.18, 1/d\}$. *Let* $F(x)$ *be a monic polynomial of degree d with one or more small roots* x_0 *modulo* M *such that* $|x_0| < \frac{1}{2}M^{1/d-\epsilon}$. *Then* x_0 *can be found in time, bounded by a polynomial in* d, $1/\epsilon$ *and* $\log(M)$.

Better bound

The proof is similar to the one on slide 17 and thus is omitted here.

Application to RSA

Relaxed models

- Stereotyped messages (with partial knowledge of m)
- With partial knowledge of p
- With small decryption exponent d
- …

Stereotyped message attack

$N, e = 3, c$ are known. Higher bits of m are known.

$$f(x) = c - (m_0 + x)^e \mod N$$

↓

$$f(x) = c - (m_0 + x)^3 \mod N$$

We can recover x_0 if $|x_0| < N^{1/3}$

With partial knowledge of p

Theorem 19.4.2 *Let* $N = pq$ *with* $p < q < 2p$. *Let* $0 < \epsilon < 1/4$, *and suppose* $\tilde{p} \in \mathbb{N}$ *is such that* $|p - \tilde{p}| \leq \frac{1}{2\sqrt{2}} N^{1/4-\epsilon}$. *Then given* N *and* $\tilde{p}$ *one can factor* N *in time polynomial in* $\log(N)$ *and* $1/\epsilon$.

Let $F(x) = \tilde{p} + x$. Define h+1 polynomials:

$$N^h, N^{h-1}F(x), N^{h-2}F(x)^2, \ldots, NF(x)^{h-1}, F(x)^h, xF(x)^h, \ldots, x^{k-h}F(x)^h.$$

Take $h \geq \max\{4, 1/4\epsilon\}$, the above thm holds

RSA with small decryption exponent d

$$e \cdot d = 1 \bmod \varphi(N)$$

$$\Longrightarrow e \cdot d = 1 + k \cdot \varphi(N)$$

$$\Longrightarrow k \cdot \varphi(N) + 1 = 0 \bmod e$$

$$\Longrightarrow \underbrace{k}_{x} \cdot (\underbrace{N + 1}_{A} \underbrace{- p - q}_{y}) + 1 = 0 \bmod e$$

$$f(x, y) = x \cdot (A + y) + 1 = 0 \bmod e$$

Bivariate case
-- Condition to remove "mod"

- $h(x,y) = \sum_{i,j} a_{i,j}\, x^i y^j$
- $||h(x,y)||^2 \doteq \sum_{i,j} |\, a_{i,j}^2 \,|$

Fact 4 (HG98). *Let* $h(x,y) \in \mathbb{Z}[x,y]$ *be a polynomial which is a sum of at most* w *monomials. Suppose that*

a. $h(x_0, y_0) = 0 \bmod e^m$ *for some positive integer* m *where* $|x_0| < X$ *and* $|y_0| < Y$*, and*
b. $\|h(xX, yY)\| < e^m/\sqrt{w}$.

Then $h(x_0, y_0) = 0$ *holds over the integers.*

Construct Lattice

$$g_{i,k}(x,y) := x^i f^k(x,y) e^{m-k} \quad \text{and} \quad h_{j,k}(x,y) := y^j f^k(x,y) e^{m-k}.$$

$$0 \le k \le m, 0 \le i \le m-k, 0 \le j \le t, |x_0| < X = e^{\delta}, |y_0| < Y = e^{0.5}$$

	1	x	xy	x^2	x^2y	x^2y^2	y	xy^2	x^2y^3
e^2	e^2								
xe^2		e^2X							
fe	e	eAX	eXY						
x^2e^2				e^2X^2					
xfe		eX		eAX^2	eX^2Y				
f^2	1	$2AX$	$2XY$	A^2X^2	$2AX^2Y$	X^2Y^2			
ye^2							e^2Y		
yfe			$eAXY$				eY	eXY^2	
yf^2			$2AXY$		A^2X^2Y	$2AX^2Y^2$	Y	$2XY^2$	X^2Y^3

Boneh-Durfee basis matrix for $m = 2$, $t = 1$

RSA with small decryption exponent d

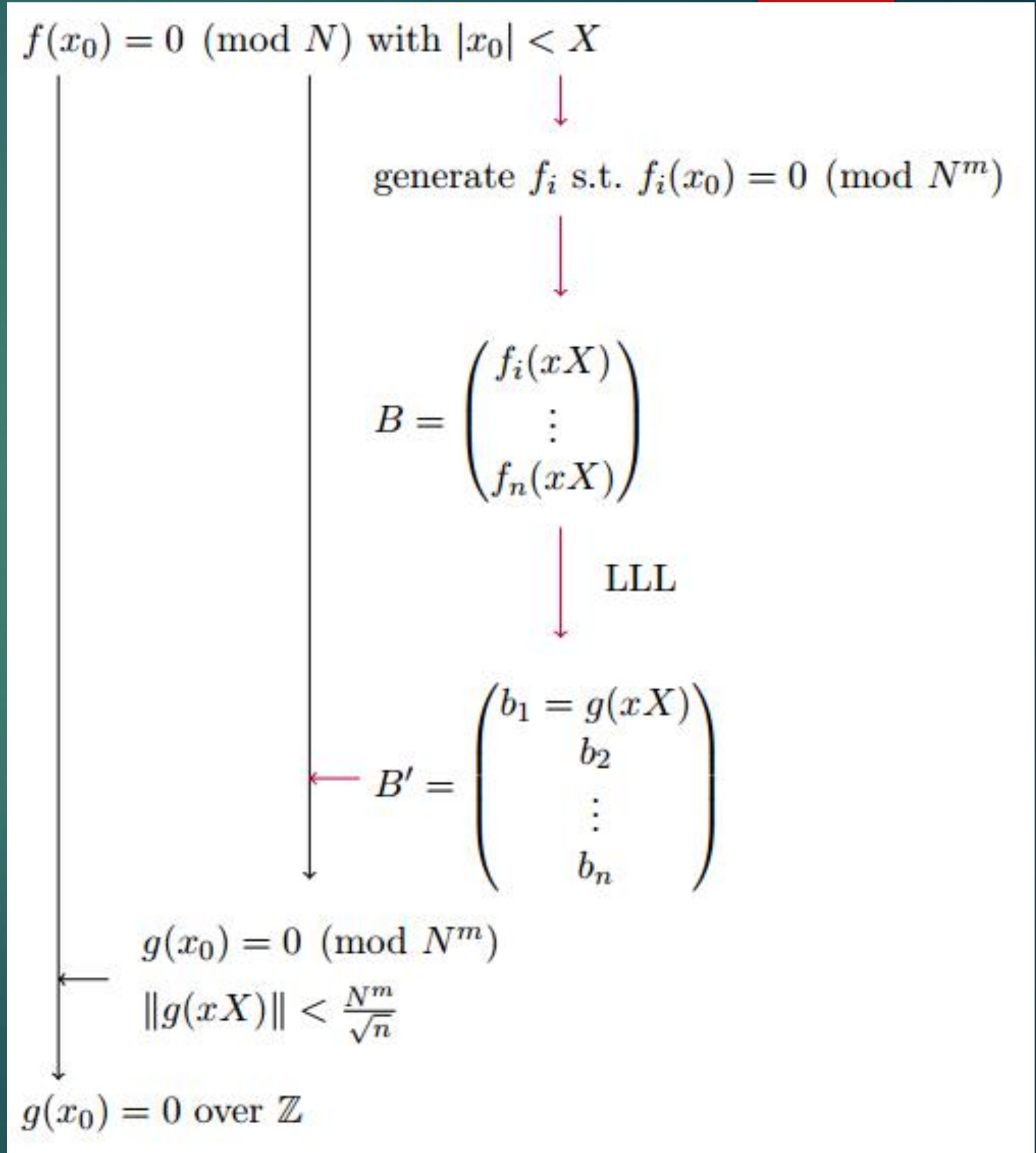
$$k \cdot (N + 1 - p - q) + 1 = 0 \bmod e$$

$$k < N^{0.285} \Longrightarrow d < N^{0.285}$$

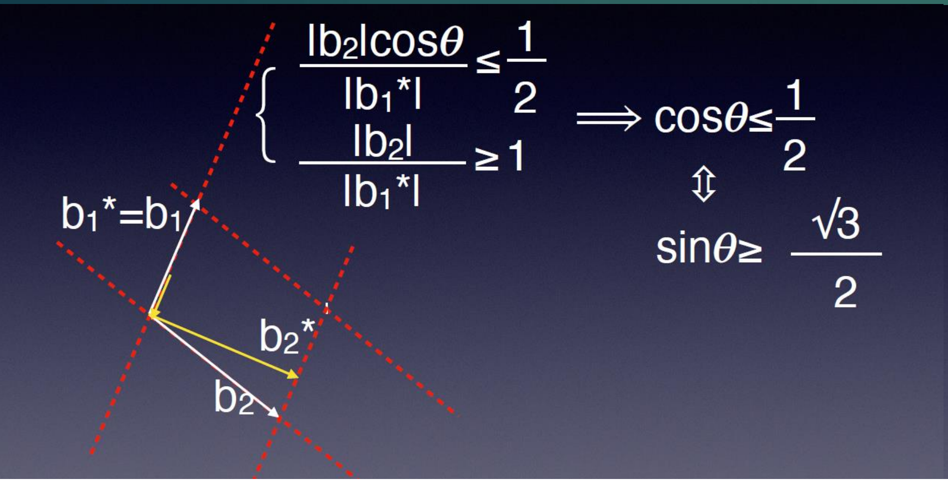
$$e \cdot d = 1 + k \cdot (N + 1 - p - q)$$
$$= k \cdot N + k \cdot (1 - p - q) + 1$$
$$\Longrightarrow e \cdot d \approx k \cdot N$$
$$\Longrightarrow \frac{e}{N} \approx \frac{k}{d}$$

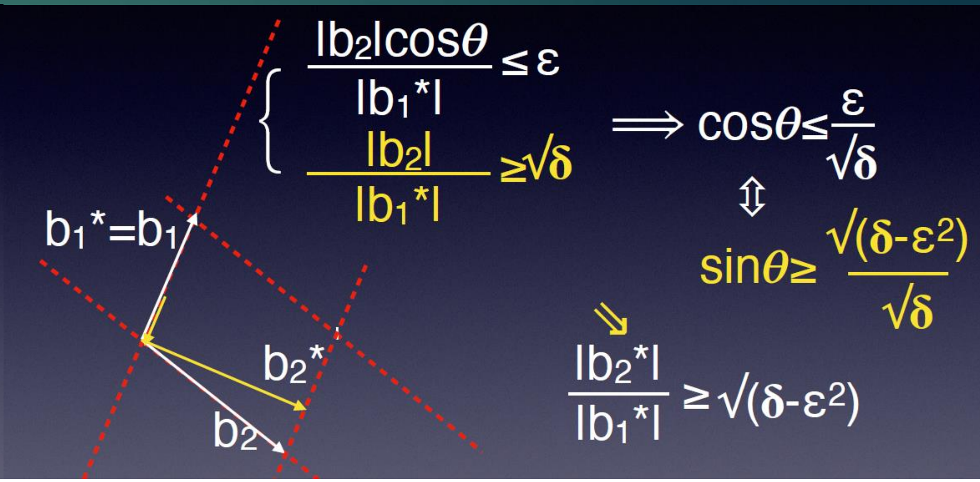
Conclusion

All the cryptanalysis of RSA is carried out under relaxed models.



The bound for b_1





(1.6) **Proposition.** *Let $b_1, b_2, \ldots, b_n$ be a reduced basis for a lattice L in $\mathbb{R}^n$, and let $b_1^*, b_2^*, \ldots, b_n^*$ be defined as above. Then we have*

(1.7) $$|b_j|^2 \leqq 2^{i-1} \cdot |b_i^*|^2 \quad \textit{for} \quad 1 \leqq j \leqq i \leqq n,$$

(1.8) $$d(L) \leqq \prod_{i=1}^{n} |b_i| \leqq 2^{n(n-1)/4} \cdot d(L),$$

(1.9) $$|b_1| \leqq 2^{(n-1)/4} \cdot d(L)^{1/n}.$$

back