CRYPTANALYSIS OF RSA WITH MODULI $N = p^r q$ BASED ON COPPERSMITH METHOD: A SURVEY

Simeng Yuan, Wei Yu, Kunpeng Wang, Xiuxiu Li

State Key Laboratory of Information Security, Institute of Information Engineering, CAS
School of Cyber Security, University of Chinese Academy of Sciences

e-mail: yuansimeng@iie.ac.cn

RESUME OF THE PRESENTER

Simeng Yuan is from Hubei, China. She is currently a Master student at University of Chinese Academy of Sciences where she focuses on lattice-based cryptanalysis of RSA and its variant algorithms. She has a Bachelors degree in information security from Central South University, Hunan, China.

OUTLINE

- Background
  - Coppersmith method
  - RSA with Moduli $N = p^r q$
- Factor RSA Moduli
  - Small Exponent Attacks
  - Partial Key Exposure Attacks
  - Factoring RSA Moduli With Partial Known
- Conclusion and Future Research

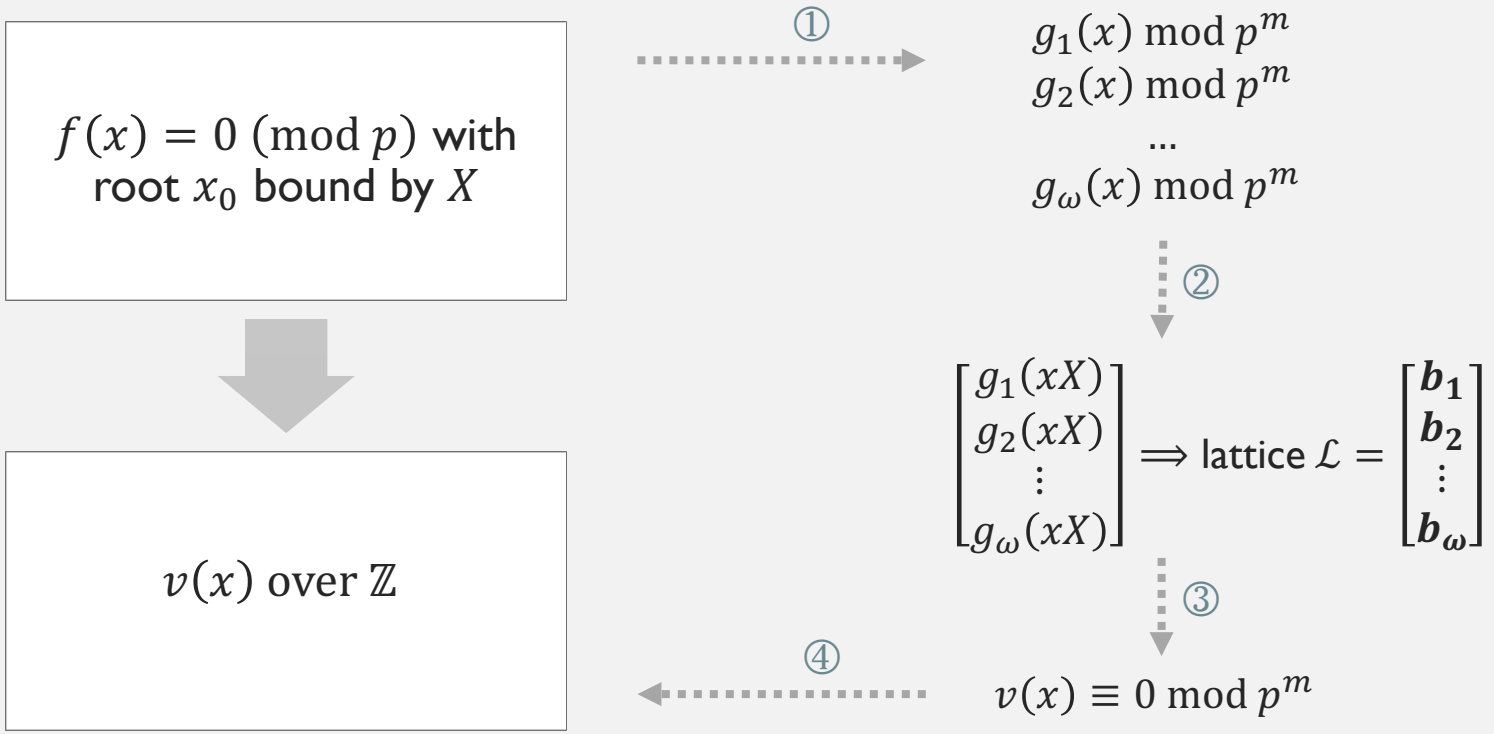
COPPERSMITH METHOD

Coppersmith method can convert the modular equations with large norm into integer equations with small norm by lattice-based algorithm such as LLL algorithm, and the roots of the original equations can be solved over the integers.

$f(x) \bmod p$

$g(x)$ over $\mathbb{Z}$

COPPERSMITH METHOD



COPPERSMITH METHOD

$f(x) = 0 \pmod{p}$ with root x_0 bound by X

$v(x)$ over $\mathbb{Z}$

① Construct ω new polynomials, which have the same small root as $f(x)$.

② Use the coefficient vectors of $g_i(xX)$ to construct the lattice basis.

③ Apply LLL to the lattice basis, and we can get a short vector $\boldsymbol{v}$, corresponding a polynomial $v(x)$.

④ If $\|\boldsymbol{v}\|$ is small enough ($\det(\mathcal{L}) < p^{m\omega}$), the modular equation can be converted to an integer equation

RSA WITH MODULI
$N = p^r q$

The encryption and decryption of RSA are based on the modular operation of large numbers, so it may be slow in the environment with limited resources. For efficiency, RSA fast variant with moduli $N = p^r q$ has been produced.

$N = pq$

$N = p^r q$

Takagi RSA

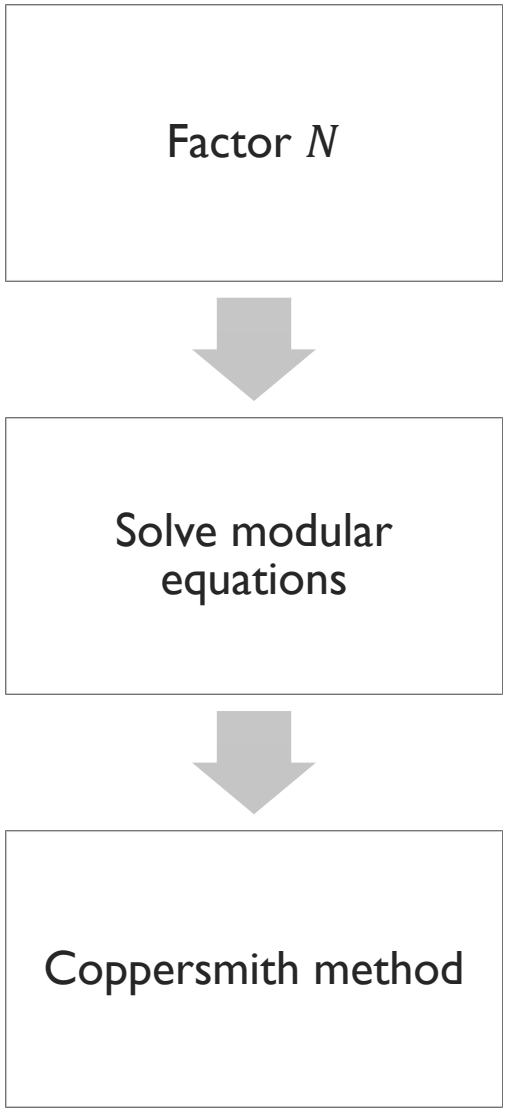
$$ed = 1 \bmod (p-1)(q-1)$$

Prime Power RSA

$$ed = 1 \bmod p^{r-1}(p-1)\,(q-1)$$

FACTOR RSA MODULI

Based on RSA equations, the problem of factoring N can be transformed to the problem of solving modular equation. Then we can use the Coppersmith method to find roots.



SMALL EXPONENT ATTACKS

TAKAGI RSA

Factor N ⇢ $ed = 1 + k(p-1)(q-1)$

↓

Solve modular equations ⇢ $f(x,y,z) = x(y-1)(z-1) + 1 = 0 \pmod{e}$

↓

Coppersmith method

[IKK08] showed that N can be factored in polynomial time, when $\boldsymbol{d} \leq \boldsymbol{N}^{\frac{2-\sqrt{2}}{r+1}}$ using geometric progressive matrices. [TK16] proved the same result based on Coppersmith method.

SMALL EXPONENT ATTACKS

PP-RSA

Factor N ⇢ $ed = 1 + kp^{r-1}(p-1)(q-1)$

↓

Solve modular equations ⇢ $f(x,y,z) = xy^{r-1}(y-1)(z-1) + 1 = 0 \pmod{e}$

↓

Coppersmith method

[LZPL15] proved that one can factor N when $\boldsymbol{d < N^{\frac{r(r-1)}{(r+1)^2}}}$.
[Sar16] studied the small exponent attack of PP-RSA in the case of $\boldsymbol{2 < r < 8}$.

PARTIAL KEY EXPOSURE ATTACKS

TAKAGI RSA

Factor N

Solve modular equations

Coppersmith method

$$e(d_1 M + d_0) = 1 + k(p-1)(q-1)$$

Known MSBs: $f(x_1, x_2, x_3, x_4) =$

$$x_1(x_2 - 1)(x_3 - 1) + 1 + ex_4 = 0 \pmod{ed_1}$$

Known LSBs: $f(x_1, x_2, x_3) =$

$$x_1(x_2 - 1)(x_3 - 1) + 1 - ed_0 = 0 \pmod{eM}$$

[HHX+14] showed that N can be factored in polynomial time, giving about $(1 - \frac{\delta}{\beta})$-fraction of d ($e = N^{\alpha}, d = N^{\beta}$) when

$$\boldsymbol{\delta \leq \frac{7}{4(r+1)} - \frac{1}{4}\sqrt{\frac{24(\alpha+\beta)}{r+1} - \frac{39}{(r+1)^2}} - \epsilon}$$ (for known MSBs)

$$\boldsymbol{\delta \leq \frac{5}{3(r+1)} - \frac{2}{3}\sqrt{\frac{3(\alpha+\beta)}{r+1} - \frac{5}{(r+1)^2}} - \epsilon}$$ (for known LSBs)

PARTIAL KEY EXPOSURE ATTACKS

PP-RSA

Factor N ⇢ $e(d_1M + d_0) = 1 + kp^{r-1}(p-1)(q-1)$

↓

Solve modular equations ⇢ Known MSBs: $f(x) = ex + ed_1 - 1 = 0 \pmod{p^{r-1}}$

Known LSBs: $f(x) = eMx + ed_0 - 1 = 0 \pmod{p^{r-1}}$

↓

Coppersmith method

[EKU15][TK16] proposed the attacks on PP-RSA when the LSBs are known. [Sar16] gave the partial private key exposure attack when $\boldsymbol{r < 8}$ and $\boldsymbol{d < N^{\frac{1}{r+1} + \frac{3r - 2\sqrt{3r+3} + 3}{3(r+1)}}}$

FACTORING RSA MODULI WITH PARTIAL KNOWN

$$N = p^r q$$

Factor N ⇢ $N = (P + \tilde{p})^r q$

↓

Solve modular equations ⇢ $f(x) = (P + x)^r \bmod p^r$

↓

Coppersmith method

[BDH99] showed that N can be factored in polynomial time, when $\frac{1}{r+1}$-fraction of the MSBs bits of p are known. [LZL13] extend it to the case of n unknown bit blocks rather than a consecutive block.

CONCLUSION AND FUTURE RESEARCH

- The selection of parameters needs to be more careful to avoid the above attacks.
- Next, we will research the security of RSA with moduli $N = p^r q^s$ based on Coppersmith method.

THANKS!