Partial Key Exposure Attack on Short Secret Exponent CRT-RSA

ASIACRYPT '21

Alexander May [1]   **Julian Nowakowski** [1]   Santanu Sarkar [2]

[1] Ruhr-University Bochum, Germany

[2] Indian Institute of Technology Madras, India

`eprint.iacr.org/2021/972.pdf`

Short Secret Exponent (CRT-)RSA

RSA:

- Public key: (N, e), where $N = pq$ is the product of two primes.
- Private key: (N, d), where

$$ed \equiv 1 \mod (p-1)(q-1).$$

- Using $d \ll N$ makes the scheme insecure.

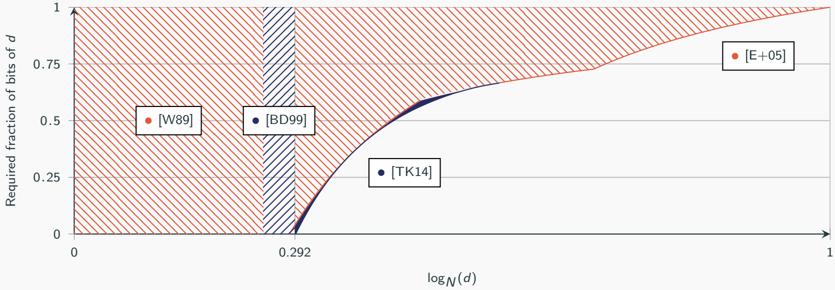
[Wiener'89], [Boneh, Durfee'99]

If $d < N^{0.292}$, then RSA can be broken in polynomial time.

[Ernst, Jochemsz, May, de Weger'05], [Aono'09], [Takayasu, Kunihiro'14]

If $d < N$, then RSA admits for Partial Key Exposure attacks.

Short Secret Exponent (CRT-)RSA



Short Secret Exponent (CRT-)RSA

RSA:

- Public key: (N, e), where $N = pq$ is the product of two primes.
- Private key: (N, d), where

$$ed \equiv 1 \mod (p-1)(q-1).$$

- Using $d \ll N$ makes the scheme insecure.

[Wiener'89], [Boneh, Durfee'99]

If $d < N^{0.292}$, then RSA can be broken in polynomial time.

[Ernst, Jochemsz, May, de Weger'05], [Aono'09], [Takayasu, Kunihiro'14]

If $d < N$, then RSA admits for Partial Key Exposure attacks.

CRT-RSA:

- Public key: (N, e), where $N = pq$ is the product of two primes.
- Private key: (N, d_p, d_q), where

$$ed_p \equiv 1 \mod (p-1),$$
$$ed_q \equiv 1 \mod (q-1).$$

- Open question by Wiener '89:
  Is using $d_p, d_q \ll \sqrt{N}$ insecure?

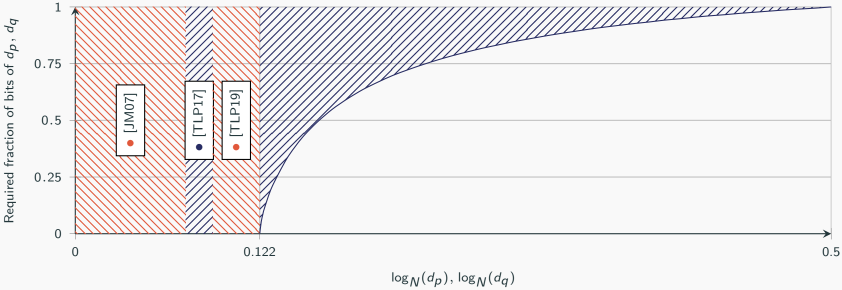
[Jochemsz, May'07], [Takayasu, Lu, Peng'17], [Takayasu, Lu, Peng'19]

If $d_p, d_q < N^{0.122}$, then CRT-RSA can be broken in polynomial time.

Our result

If $d_p, d_q < \sqrt{N}$, then CRT-RSA admits for Partial Key Exposure attacks.

Short Secret Exponent (CRT-)RSA



A Simplified Proof for [TLP19]

Coppersmith's Method

Problem (Coppersmith-type problem)

Given:

- Modulus $M \in \mathbb{N}$,
- Bounds $X_1, \ldots, X_k \in \mathbb{Z}_M$,
- Polynomials $p_1, \ldots, p_n \in \mathbb{Z}_M[x_1, \ldots, x_k]$.

Find:

- All common roots $r = (r_1, \ldots, r_k)$ of $p_1, \ldots, p_n$ modulo M with $|r_i| \leq X_i$.

- The smaller $X_1, \ldots, X_k$, the better.

Strategy:

- Fix $m = \text{polylog}(M)$ and define *shift-polynomials*

$$f_{[\mathbf{i},\mathbf{j}]} := p_1^{i_1} \cdot \ldots \cdot p_n^{i_n} \cdot x_1^{j_1} \cdot \ldots \cdot x_k^{j_k} \cdot M^{m-(i_1+\ldots+i_n)}.$$

- Construct triangular lattice basis matrix

$$\mathbf{B} := \left(\vec{f}_{[\mathbf{i},\mathbf{j}]}(X_1 x_1, \ldots, X_k x_k)\right)_{(\mathbf{i},\mathbf{j})}.$$

Heuristic

If the *enabling condition*

$$|\det \mathbf{B}| \lessapprox M^{m \cdot \dim \mathcal{L}(\mathbf{B})}$$

holds, then we can compute all r in polynomial time.

CRT-RSA equations $\mapsto$ Coppersmith-type Problem

- By definition, it holds that

$$\begin{aligned} ed_p &= 1 + k(p-1), \\ ed_q &= 1 + \ell(q-1) \end{aligned}$$

for some $k, \ell \in \mathbb{N}$.

- $d_p, d_q \ll \sqrt{N} \implies k, \ell$ small(-ish).
- Taking the equations modulo e, we obtain polynomials

$$\begin{aligned} f(x_p, y_p, z_p) &= x_p^1 y_p^1 z_p^0 - x_p^1 y_p^0 z_p^0 + x_p^0 y_p^0 z_p^0, \\ g(x_p, y_p, z_p) &= x_p^0 y_p^1 z_p^1 - N x_p^0 y_p^0 z_p^1 - N x_p^0 y_p^0 z_p^0, \\ h(x_p, y_p, z_p) &= (N-1) x_p^1 y_p^0 z_p^1 + N x_p^1 y_p^0 z_p^0 + x_p^0 y_p^0 z_p^1, \end{aligned}$$

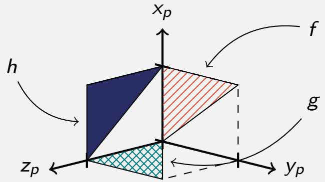
which have a small common root

$$(k, p, \ell - 1)$$

modulo e.

Rule of thumb

1. The polynomials should share as many monomials as possible.
2. In every monomial the degree of each variable should be as low as possible.



Bad news:

- Enabling condition:

$$d_p, d_q < N^{0.250} e^{-0.286} \overset{e \approx N}{<} 1$$

The Geometry of Coppersmith's Method

Is there any information, that we do not use yet?

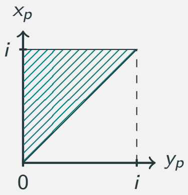
- We know in N a multiple of the unknown p.
- Our polynomials have small coefficients.

Rule of thumb

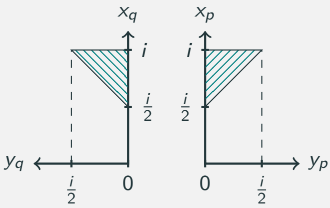
3. The total degree of the shift-polynomials should be as low as possible.
4. The shift-polynomials should have as few monomials as possible.

- Consider the shift-polynomial $f^i(x_p, y_p)$ for some $i \in \mathbb{N}$, which has the root (k, p).
- Multiply shift-polynomial by new variable y_q and replace $y_p y_q \mapsto N$ and $x_p y_q \mapsto (x_q + 1)y_q$.
- The new polynomial in (x_p, x_q, y_p, y_q) has the root $(k, k-1, p, q)$.

- Monomials of f^i:



- Monomials of $f^i y_q^{\frac{i}{2}}$ after replacing $y_p y_q \mapsto N$ and $x_p y_q \mapsto (x_q + 1)y_q$:



Achieving the Takayasu-Lu-Peng Bound

- By generalizing these ideas we obtain the following enabling condition

$$d_p, d_q < N^{\frac{5}{56}} \approx N^{0.089}.$$

- Adding *extra-shifts* in the variables y_p, y_q yields the Takayasu-Lu-Peng result

$$d_p, d_q < N^{\frac{1}{2} - \frac{1}{\sqrt{7}}} \approx N^{0.122}.$$

Our Partial Key Exposure Attack

First Try

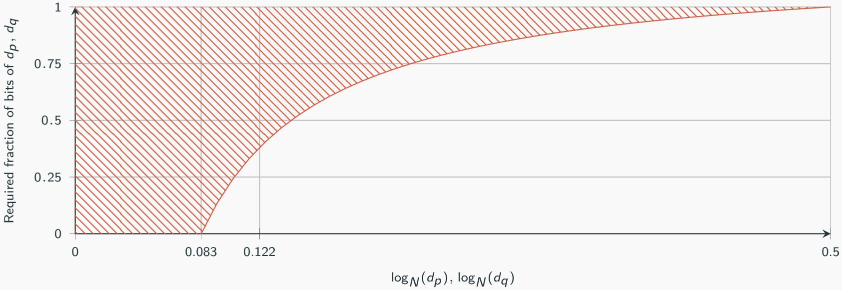
[TLP19] attack:

- CRT-RSA equations yield three polynomials f, g, h, which have the root $(k, p, \ell - 1)$ modulo e.
- Applying Coppersmith's method directly to f, g, h does not work.
- Additional information:
  - We know in N a multiple of the unknown p.
  - Our polynomials have small coefficients.
- Incorporate this information using our geometric view on Coppersmith's method.

Our Partial Key Expsoure attack:

- Knowledge of bits of CRT-exponents gives us three additional polynomials $\widetilde{f}, \widetilde{g}, \widetilde{h}$, which have the desired root $(k, p, \ell - 1)$.
- Applying Coppersmith's method directly to $\widetilde{f}, \widetilde{g}, \widetilde{h}$ does not work.
- Additional information:
  - We know in N a multiple of the unknown p.
  - ~~Our polynomials have small coefficients.~~
- Incorporate this information using our geometric view on Coppersmith's method.

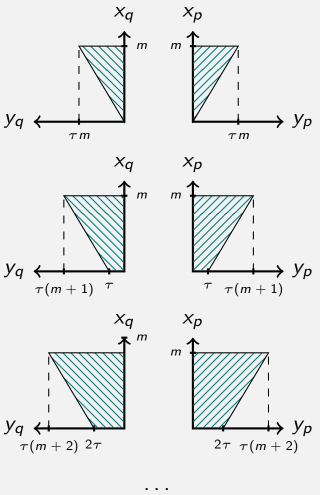
First Try



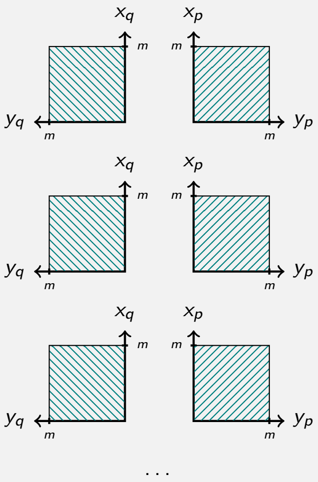
1
0.75
0.5
0.25
0
Required fraction of bits of d_p, d_q
0
0.083
0.122
0.5
$\log_N(d_p)$, $\log_N(d_q)$

Achieving the Takayasu-Lu-Peng Bound

- Set of monomials $\mathcal{M}(m, \tau)$ in Takayasu-Lu-Peng lattice basis matrix:

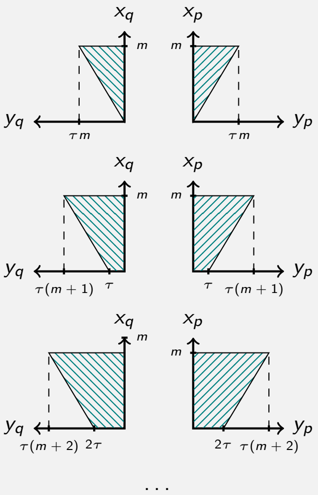


- Set of monomials $\widetilde{\mathcal{M}}(m)$ in our lattice basis matrix:

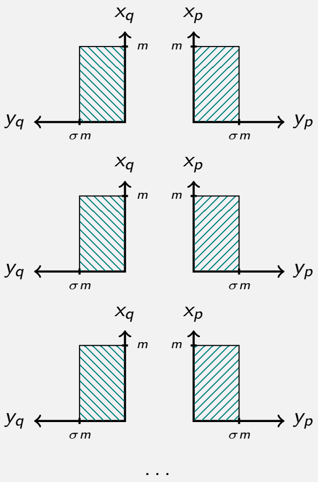


Achieving the Takayasu-Lu-Peng Bound

- Set of monomials $\mathcal{M}(m, \tau)$ in Takayasu-Lu-Peng lattice basis matrix:

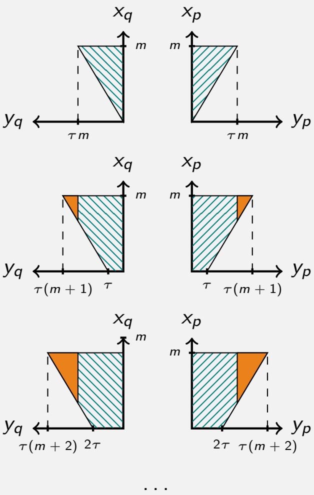


- Set of monomials $\widetilde{\mathcal{M}}(m, \sigma)$ in our lattice basis matrix:

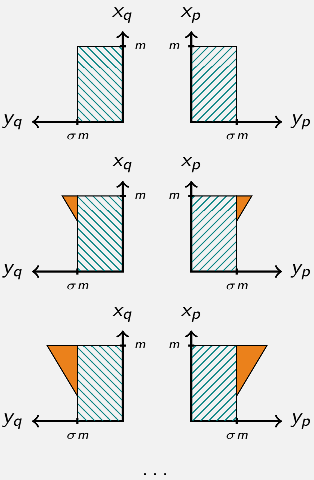


Achieving the Takayasu-Lu-Peng Bound

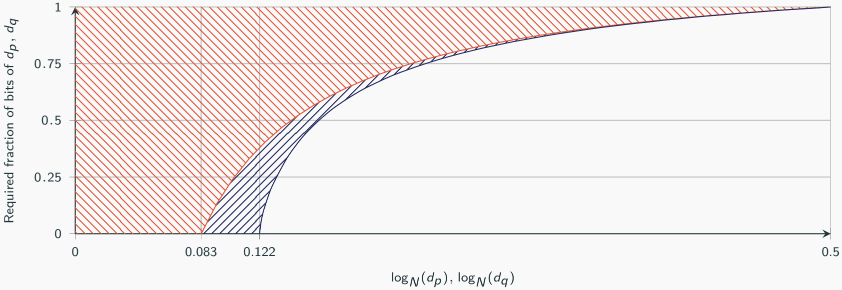
- Set of monomials $\mathcal{M}(m,\tau)$ in Takayasu-Lu-Peng lattice basis matrix:



- Set of monomials $\widetilde{\mathcal{M}}(m,\sigma,\tau)$ in the combined lattice basis matrix:



Achieving the Takayasu-Lu-Peng Bound



Conclusion and Open Question

Conclusion:

- Simplified proof for [TLP19].
- First Partial Key Exposure attack on Short Secret Exponent CRT-RSA.
- A geometric view Coppersmith's method can provide deeper insights.

Open question:

- Our attack so far works only for exposed LSBs. Does there exist a similar MSB-type Partial Key Exposure attack?