Cryptanalysis of RSA Variants with Modified Euler Quotient

Mengce Zheng[1] Noboru Kunihiro[2] Honggang Hu[1]

[1]University of Science and Technology of China, China

[2]The University of Tokyo, Japan

May 7, 2018

Outline

RSA and Its Variants

The standard RSA cryptosystem.

- $N = pq$ with two distinct prime factors of the same bit-size.
- Public and private keys (e, d) satisfy $ed \equiv 1 \bmod \varphi(N)$.
- Euler's totient function $\varphi(N) = (p-1)(q-1)$.
- Encryption is $C = M^e \bmod N$ and decryption is $C^d \bmod N$.

RSA and Its Variants

The standard RSA cryptosystem.

- $N = pq$ with two distinct prime factors of the same bit-size.
- Public and private keys (e, d) satisfy $ed \equiv 1 \bmod \varphi(N)$.
- Euler's totient function $\varphi(N) = (p-1)(q-1)$.
- Encryption is $C = M^e \bmod N$ and decryption is $C^d \bmod N$.

The RSA variants with modified Euler quotient.

- $N = pq$ with two distinct prime factors of the same bit-size.
- Euler quotient is modified as $\omega(N) = (p^2-1)(q^2-1)$.
- Key pair (e, d) satisfy $ed \equiv 1 \bmod \omega(N)$.

Related Schemes

Three RSA-type variants with modified Euler quotient.

- One is based on singular cubic curves with $y^2 \equiv x^3 + bx^2 \pmod{N}$.
- One is based on the field of Gaussian integers.
- One is based on quadratic field quotients using Lucas sequence.

Related Schemes

Three RSA-type variants with modified Euler quotient.

- One is based on singular cubic curves with $y^2 \equiv x^3 + bx^2 \pmod{N}$.
- One is based on the field of Gaussian integers.
- One is based on quadratic field quotients using Lucas sequence.

Common requirement in the key generation phase.

- RSA modulus $N = pq$ with the same bit-size p and q.
- Public key e satisfies $\gcd(e, (p^2 - 1)(q^2 - 1)) = 1$.
- Private key is $d \equiv e^{-1} \pmod{(p^2 - 1)(q^2 - 1)}$.

Key-Related Attacks

Small private key attack for $d \approx N^{\delta}$ and $e \approx N^{\alpha}$.

- Boneh-Durfee attack on standard RSA shows $\delta < 0.292$ for $\alpha \approx 1$.
- This type attack on target RSA variants is $\delta < 2 - \sqrt{\alpha}$ for $\alpha \geq 1$.

Key-Related Attacks

Small private key attack for $d \approx N^{\delta}$ and $e \approx N^{\alpha}$.

- Boneh-Durfee attack on standard RSA shows $\delta < 0.292$ for $\alpha \approx 1$.
- This type attack on target RSA variants is $\delta < 2 - \sqrt{\alpha}$ for $\alpha \geq 1$.

Multiple private keys attack for $\alpha \approx 1$ with n many keys.

- Takayasu-Kunihiro attack on standard RSA shows $\delta < 1 - \sqrt{\frac{2}{3n+1}}$.
- This type attack on target RSA variants has not been analyzed.

Key-Related Attacks

Small private key attack for $d \approx N^{\delta}$ and $e \approx N^{\alpha}$.

- Boneh-Durfee attack on standard RSA shows $\delta < 0.292$ for $\alpha \approx 1$.
- This type attack on target RSA variants is $\delta < 2 - \sqrt{\alpha}$ for $\alpha \geq 1$.

Multiple private keys attack for $\alpha \approx 1$ with n many keys.

- Takayasu-Kunihiro attack on standard RSA shows $\delta < 1 - \sqrt{\frac{2}{3n+1}}$.
- This type attack on target RSA variants has not been analyzed.

Partial key exposure attack with known leakage of private key.

- This type attack on target RSA variants has not been analyzed.

Lattice-Based Method

Recover small roots of modular equations by lattice reduction algorithm.

1. Construct shift polynomials sharing the common roots modulo R;
2. Transform coefficient vectors into a lattice basis matrix B;
3. Calculate short vectors from w-dimensional lattice $\mathcal{L}$;
4. Transform lattice vectors into integer equations;
5. Extract the desired roots of equations over the integers.

A rough condition for extracting the small roots.

$$\det(\mathcal{L}) < R^w \quad \Rightarrow \quad |\det(B)| < R^w$$

Our Results

Small private key attack

Let $N = pq$ with two prime factors p, q of the same bit-size. Let $e \approx N^\alpha, d \approx N^\delta$ be the keys satisfying $ed \equiv 1 \pmod{(p^2-1)(q^2-1)}$. Then N can be efficiently factored if

$$\delta < 2 - \sqrt{\alpha} \quad \text{for} \quad 1 \leq \alpha < 4$$

Our Results

Small private key attack

Let $N = pq$ with two prime factors p, q of the same bit-size. Let $e \approx N^\alpha, d \approx N^\delta$ be the keys satisfying $ed \equiv 1 \pmod{(p^2-1)(q^2-1)}$. Then N can be efficiently factored if

$$\delta < 2 - \sqrt{\alpha} \quad \text{for} \quad 1 \leq \alpha < 4$$

Multiple private keys attack

Given $e_i d_i \equiv 1 \pmod{(p^2-1)(q^2-1)}$ for $1 \leq i \leq n$. Then N can be efficiently factored if

$$\delta < 2 - \sqrt{\frac{4\alpha}{3n+1}} \quad \text{for} \quad \frac{4}{3n+1} < \alpha < 3n+1$$

Our Results

Partial key exposure attack

Let $N = pq$ with two prime factors p, q of the same bit-size. Let $e \approx N^{\alpha}, d \approx N^{\delta}$ be the keys satisfying $ed \equiv 1 \pmod{(p^2-1)(q^2-1)}$. Given $\tilde{d}$ with known MSBs $d_M = N^{\gamma_M}$, LSBs $d_L = N^{\gamma_L}$ and unknown $\hat{d} = N^{\delta-\gamma}$ (for $\gamma = \gamma_M + \gamma_L$) such that $d = d_M M + \hat{d} L + d_L$ for $M := 2^{(\delta-\gamma_M)\log_2 N}$ and $L := 2^{\gamma_L \log_2 N}$. Then N can be efficiently factored if

$$\delta < \frac{3\gamma + 7 - 2\sqrt{3\alpha + 3\gamma + 1}}{3}$$

Small Private Key Attack – (1)

The crucial equation derived from $ed \equiv 1 \bmod \omega(N)$ for $N = pq$.

$$
\begin{aligned}
& ed = k(p^2 - 1)(q^2 - 1) + 1 \\
\Rightarrow \quad & ed = k\left((N+1)^2 - (p+q)^2\right) + 1
\end{aligned}
$$

Small Private Key Attack – (1)

The crucial equation derived from $ed \equiv 1 \bmod \omega(N)$ for $N = pq$.

$$\begin{aligned} & ed = k(p^2-1)(q^2-1)+1 \\ \Rightarrow \quad & ed = k\left((N+1)^2-(p+q)^2\right)+1 \end{aligned}$$

Find solution of the following modular equation.

$$x(y+A)+1 \equiv 0 \pmod{e}$$

- Known: $A = (N+1)^2$ and e.
- Small roots: $x = k$ and $y = -(p+q)^2$.

Small Private Key Attack – (2)

Apply the linearization technique to the crucial modular equation.

$$Ax + z \equiv 0 \pmod{e} \quad \text{for} \quad z := xy + 1$$

Small Private Key Attack – (2)

Apply the linearization technique to the crucial modular equation.

$$Ax + z \equiv 0 \pmod{e} \quad \text{for} \quad z := xy + 1$$

Define shift polynomials $g_{[i,j,k]}(x, y, z)$ for $f(x, y, z) := Ax + z$.

$$g_{[i,j,k]}(x, y, z) := x^i y^j f^k(x, y, z) e^{s-k} = x^i y^j (Ax + z)^k e^{s-k}$$

- s is a fixed positive integer and $i, j, k \in \mathbb{N}$.
- $R = e^s$.

Small Private Key Attack – (3)

The set of shift polynomials $\mathcal{G} \cup \mathcal{H}$ defined over index sets $\mathcal{I}_{\mathcal{G}}$ and $\mathcal{I}_{\mathcal{H}}$.

$$\mathcal{I}_{\mathcal{G}} := \{(i, j, k) : j = 0; i = 0, \ldots, s; k = 0, \ldots, s - i\}$$
$$\mathcal{I}_{\mathcal{H}} := \{(i, j, k) : i = 0; k = 0, \ldots, s; j = 1, \ldots, \tau k\}$$

- An optimizing parameter $0 \leq \tau \leq 1$ to be determined later.

Small Private Key Attack – (3)

The set of shift polynomials $\mathcal{G} \cup \mathcal{H}$ defined over index sets $\mathcal{I}_{\mathcal{G}}$ and $\mathcal{I}_{\mathcal{H}}$.

$$\mathcal{I}_{\mathcal{G}} := \{(i,j,k) : j = 0; i = 0, \ldots, s; k = 0, \ldots, s-i\}$$
$$\mathcal{I}_{\mathcal{H}} := \{(i,j,k) : i = 0; k = 0, \ldots, s; j = 1, \ldots, \tau k\}$$

- An optimizing parameter $0 \leq \tau \leq 1$ to be determined later.

The coefficient vectors of $g_{[i,j,k]}(xX, yY, zZ)$ generate the basis matrix.

- X, Y and Z denote the upper bounds on the roots (x, y, z).
- $X = N^{\alpha+\delta-2}, Y = N$ and $Z = N^{\alpha+\delta-1}$.

Small Private Key Attack – (4)

Derive final condition and set $\tau = 1 - \delta$ as the optimizing parameter.

$$\Rightarrow \quad \tau^2 + (2\delta - 2)\tau + \alpha + 2\delta - 3 < 0$$
$$\Rightarrow \quad \delta^2 - 4\delta - \alpha + 4 > 0$$

Small Private Key Attack – (4)

Derive final condition and set $\tau = 1 - \delta$ as the optimizing parameter.

$$\begin{aligned} &\Rightarrow \quad \tau^2 + (2\delta - 2)\tau + \alpha + 2\delta - 3 < 0 \\ &\Rightarrow \quad \delta^2 - 4\delta - \alpha + 4 > 0 \end{aligned}$$

Consider the applicable range of α with $0 \leq \tau \leq 1$ and $\alpha + \delta \geq 2$.

$$\delta < 2 - \sqrt{\alpha} \quad \text{for} \quad 1 \leq \alpha < 4$$

Multiple Private Keys Attack – (1)

Given $e_i \approx N^{\alpha}, d_i \approx N^{\delta}$ with $e_i d_i \equiv 1 \pmod{\omega(N)}$ for $1 \leq i \leq n$.

$$\begin{cases} f_1(x_1, y) : = x_1(y + A) + 1 \equiv 0 \pmod{e_1} \\ f_2(x_2, y) : = x_2(y + A) + 1 \equiv 0 \pmod{e_2} \\ \qquad \vdots \\ f_n(x_n, y) : = x_n(y + A) + 1 \equiv 0 \pmod{e_n} \end{cases}$$

- Known: $A := (N + 1)^2$ and e_i for $1 \leq i \leq n$.
- Small roots: $(x_1, x_2, \ldots, x_n, y) = (k_1, k_2, \ldots, k_n, -(p + q)^2)$.

Multiple Private Keys Attack – (2)

Define underlying shift polynomials for each modular equation.

$$g_{i_k,j_k}^{(k)}(x_k,y) := x_k^{i_k-j_k} f_k^{j_k}(x_k,y) e_k^{s-j_k}$$

- $0 \leq j_k \leq i_k \leq s$ and $i_k, j_k \in \mathbb{N}$ for $1 \leq k \leq n$.

Multiple Private Keys Attack – (2)

Define underlying shift polynomials for each modular equation.

$$g^{(k)}_{i_k,j_k}(x_k, y) := x_k^{i_k - j_k} f_k^{j_k}(x_k, y) e_k^{s-j_k}$$

- $0 \leq j_k \leq i_k \leq s$ and $i_k, j_k \in \mathbb{N}$ for $1 \leq k \leq n$.

Define shift polynomials by Minkowski sum based construction.

$$g_{i_1,\ldots,i_n,j}(x_1, \ldots, x_n, y) := \sum_{j_1+\cdots+j_n=j} a_{j_1,\ldots,j_n} g^{(1)}_{i_1,j_1} g^{(2)}_{i_2,j_2} \cdots g^{(n)}_{i_n,j_n}$$

- $R = (e_1 \cdots e_n)^s$.

Multiple Private Keys Attack – (3)

Chosen $a_{j_1,\ldots,j_n}$ leads to each diagonal entry of basis matrix.

$$X_1^{i_1} \cdots X_n^{i_n} Y^j e_1^{s-i_1} \cdots e_n^{s-i_n}$$

- $X_1 = \cdots = X_n = N^{\alpha+\delta-2}$ and $Y = N$.

Multiple Private Keys Attack – (3)

Chosen $a_{j_1,\ldots,j_n}$ leads to each diagonal entry of basis matrix.

$$X_1^{i_1}\cdots X_n^{i_n} Y^j e_1^{s-i_1}\cdots e_n^{s-i_n}$$

- $X_1 = \cdots = X_n = N^{\alpha+\delta-2}$ and $Y = N$.

The shift polynomials are defined over the index set $\mathcal{I}$.

$$\mathcal{I} := \{(i_1,\ldots,i_n,j) : 0 \le i_1, i_2, \ldots, i_n \le s; 0 \le j \le (2-\delta)\sum_{k=1}^{n} i_k\}$$

- To choose as many helpful polynomials as possible.

Multiple Private Keys Attack – (4)

Derive final condition for multiple private keys attack case.

$$\Rightarrow \quad -(3n+1)(2-\delta)^2 + 4\alpha < 0$$

$$\Rightarrow \quad \delta < 2 - \sqrt{\frac{4\alpha}{3n+1}}$$

Multiple Private Keys Attack – (4)

Derive final condition for multiple private keys attack case.

$$\Rightarrow \quad -(3n+1)(2-\delta)^2 + 4\alpha < 0$$
$$\Rightarrow \quad \delta < 2 - \sqrt{\frac{4\alpha}{3n+1}}$$

Consider the applicable range of α with $\delta > 0$ and $\alpha + \delta > 2$.

$$\frac{4}{3n+1} < \alpha < 3n+1$$

Partial Key Exposure Attack – (1)

Given N and $e \approx N^{\alpha}$ and a known approximation $\tilde{d}$ of $d \approx N^{\delta}$.

$$d = \tilde{d} + \hat{d}L = d_M M + \hat{d}L + d_L$$

- $M := 2^{(\delta-\gamma_M)\log_2 N}$ and $L := 2^{\gamma_L \log_2 N}$.
- $|\hat{d}| < N^{\delta-\gamma}$ for $\gamma := \gamma_M + \gamma_L$.

Partial Key Exposure Attack – (1)

Given N and $e \approx N^{\alpha}$ and a known approximation $\tilde{d}$ of $d \approx N^{\delta}$.

$$d = \tilde{d} + \hat{d}L = d_M M + \hat{d}L + d_L$$

- $M := 2^{(\delta-\gamma_M)\log_2 N}$ and $L := 2^{\gamma_L \log_2 N}$.
- $|\hat{d}| < N^{\delta-\gamma}$ for $\gamma := \gamma_M + \gamma_L$.

Focus on the following integer equation.

$$f(x, y, z) := 1 - e\tilde{d} + eLx + y((N+1)^2 + z)$$

- Small roots: $x = -\hat{d}$, $y = k$ and $z = -(p+q)^2$.

Partial Key Exposure Attack – (2)

Apply Jochemsz-May strategy to solve integer equations.

- Set a suitable integer $R := WX^{s-1}Y^{s-1}Z^{s-1+\tau s}$ as the modulus.
- $X = N^{\delta-\gamma}$, $Y = N^{\alpha+\delta-2}$, $Z = N$ and $W = N^{\alpha+\delta}$.
- A fixed positive integer s and an optimizing parameter $\tau \geq 0$.
- $f'(x, y, z) := (1 - e\tilde{d})^{-1} f(x, y, z) \pmod{R}$.

Partial Key Exposure Attack – (2)

Apply Jochemsz-May strategy to solve integer equations.

- Set a suitable integer $R := WX^{s-1}Y^{s-1}Z^{s-1+\tau s}$ as the modulus.
- $X = N^{\delta-\gamma}$, $Y = N^{\alpha+\delta-2}$, $Z = N$ and $W = N^{\alpha+\delta}$.
- A fixed positive integer s and an optimizing parameter $\tau \geq 0$.
- $f'(x,y,z) := (1-e\tilde{d})^{-1} f(x,y,z) \pmod{R}$.

The shift polynomials $g_{[i,j,k]}(x,y,z)$ are defined as follows.

$$g^{\mathcal{G}}_{[i,j,k]}(x,y,z) := x^i y^j z^k f'(x,y,z) X^{s-1-i} Y^{s-1-j} Z^{s-1+\tau s-k}$$
$$g^{\mathcal{H}}_{[i,j,k]}(x,y,z) := x^i y^j z^k R$$

- An optimizing parameter $\tau \geq 0$ and $i,j,k \in \mathbb{N}$.

Partial Key Exposure Attack – (3)

The set of shift polynomials by $\mathcal{G} \cup \mathcal{H}$.

$$\mathcal{G} := \{g^{\mathcal{G}}_{[i,j,k]}(x, y, z) : (i, j, k) \in \mathcal{I}_{\mathcal{G}}\}$$
$$\mathcal{H} := \{g^{\mathcal{H}}_{[i,j,k]}(x, y, z) : (i, j, k) \in \mathcal{I}_{\mathcal{H}} \setminus \mathcal{I}_{\mathcal{G}}\}$$

Two index sets $\mathcal{I}_{\mathcal{G}}$ and $\mathcal{I}_{\mathcal{H}}$ are defined as follows.

$$\mathcal{I}_{\mathcal{G}} := \{(i, j, k) : i = 0, \ldots, s-1; j = 0, \ldots, s-1-i; k = 0, \ldots, j+\tau s\}$$
$$\mathcal{I}_{\mathcal{H}} := \{(i, j, k) : i = 0, \ldots, s; j = 0, \ldots, s-i; k = 0, \ldots, j+\tau s\}$$

Partial Key Exposure Attack – (4)

Derive final condition and set $\tau = \frac{1+\gamma-\delta}{2}$ as the optimizing parameter.

$$\Rightarrow \quad 3\tau^2 + (3\delta - 3\gamma - 3)\tau + \alpha + 2\delta - \gamma - 3 < 0$$

$$\Rightarrow \quad \delta < \frac{3\gamma + 7 - 2\sqrt{3\alpha + 3\gamma + 1}}{3}$$

Conclusions

Key-related attacks on RSA variants with modified Euler quotient $\omega(N)$.

- Small private key attack with a precise applicable range of α.
- Multiple private keys attack that extends to n many keys.
- Partial key exposure attack is analyzed for the first time.

Conclusions

Key-related attacks on RSA variants with modified Euler quotient $\omega(N)$.

- Small private key attack with a precise applicable range of α.
- Multiple private keys attack that extends to n many keys.
- Partial key exposure attack is analyzed for the first time.

Further improvement and combined scenario remain as future work.

- To improve for given only the most or the least significant bits.
- To analyse partial key exposure attack with multiple key pairs.

Thank You!