# Implicit-Key Attack on the RSA Cryptosystem

Mengce Zheng    Honggang Hu

University of Science and Technology of China

August 11, 2019

# Outline

1. Background
   - Research Problem
   - Lattice-Based Method
2. Proposed Attack
   - Implicit-Key Attack
   - Experimental Results
3. Conclusion

# The RSA Cryptosystem

## Standard RSA instance consists of $N$, $e$, $d$, $\varphi(N)$ parameters

- $N = pq$ with two large 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 key equation of the RSA cryptosystem

- $ed = k(N + 1 - p - q) + 1$ for a positive integer $k$
- Many attacks have been proposed to solve the key equation

# Existing Attacks

## Partial key exposure attack @ ASIACRYPT 1998

- Given a small fraction of the private key bits
- $d = \bar{d} + d_0$ with known MSBs $\bar{d}$ and unknown LSBs $d_0$
- The goal is to reconstruct the entire private key $d$

## Implicit factorization problem @ PKC 2009

- Given an oracle providing implicit information about the primes
- $N_1 = p_1 q_1$ and $N_2 = p_2 q_2$ with $p_1, p_2$ sharing some LSBs
- The goal is to find $q_1, q_2$ and then factor $N_1, N_2$

# New Problem

### Implicit information about the private keys

- $(N_1, e_1, d_1)$ and $(N_2, e_2, d_2)$ with $N_1, N_2$ of the same bit-size
- Given the amounts of shared (unknown) MSBs and LSBs of $d_1, d_2$
- The goal is to factor $N_1$ and $N_2$

### Consider such combined case mainly from theoretical interest

- Disclose the vulnerability of RSA in weaker attack scenario
- Investigate how to further extend existing attacks
- RSA instances may be generated with imperfect randomness

# Lattice-Based Method

Find roots of modular/integer equations by lattice reduction algorithm

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

The crucial condition for extracting the small roots of given equations

$$\det(\mathcal{L}) < R^w$$

# Attack Scenario

Given $(N_1, e_1, d_1)$ and $(N_2, e_2, d_2)$ with implicitly related keys $d_1, d_2$

- $N_1, N_2$ are of the same bit-size denoted by $\log_2 N$
- $e_1 = N^{\alpha_1}, e_2 = N^{\alpha_2}$ are of arbitrary bit-size
- $d_1, d_2 \approx N^{\delta}$ share $\beta_1 \log_2 N$ MSBs and $\beta_2 \log_2 N$ LSBs

Shared MSBs and LSBs $d_{\mathrm{MSB}}, d_{\mathrm{LSB}}$ and different middle bits $\bar{d}_1, \bar{d}_2$

- $d_1 = d_{\mathrm{MSB}} 2^{(\delta-\beta_1)\log_2 N} + \bar{d}_1 2^{\beta_2 \log_2 N} + d_{\mathrm{LSB}}$
- $d_2 = d_{\mathrm{MSB}} 2^{(\delta-\beta_1)\log_2 N} + \bar{d}_2 2^{\beta_2 \log_2 N} + d_{\mathrm{LSB}}$
- Implicit relation: $d_1 - d_2 = (\bar{d}_1 - \bar{d}_2) 2^{\beta_2 \log_2 N} = (\bar{d}_1 - \bar{d}_2) N^{\beta_2}$

# Implicit-Key Attack – (1)

**Apply the key equations and the implicit relation of $d_1, d_2$**

- $e_1 d_1 = k_1(N_1 + 1 - p_1 - q_1) + 1$ and $e_2 d_2 = k_2(N_2 + 1 - p_2 - q_2) + 1$
- $e_2 e_1 d_1 - e_1 e_2 d_2 = e_1 e_2 (d_1 - d_2) = e_1 e_2 (\bar{d}_1 - \bar{d}_2) N^{\beta_2} =$
  $e_2 k_1 (N_1 + 1 - p_1 - q_1) + e_2 - e_1 k_2 (N_2 + 1 - p_2 - q_2) - e_1$

**Find the root of the integer equation in five variables**

- $f(x_1, x_2, x_3, x_4, x_5) = a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_2 x_4 + a_5 x_3 x_5 + a_6$
- Known values: $a_1 = e_1 e_2 N^{\beta_2}$, $a_2 = e_2(N_1 + 1)$, $a_3 = -e_1(N_2 + 1)$, $a_4 = -e_2$, $a_5 = e_1$, and $a_6 = e_2 - e_1$
- Unknown variables: $x_1 = \bar{d}_2 - \bar{d}_1$, $x_2 = k_1$, $x_3 = k_2$, $x_4 = p_1 + q_1$, and $x_5 = p_2 + q_2$

# Implicit-Key Attack – (2)

Figure out the upper bounds on unknown variables

- $X_1 = N^{\delta-\beta}$, $X_2 = N^{\alpha_1+\delta-1}$, $X_3 = N^{\alpha_2+\delta-1}$, $X_4 = X_5 = N^{1/2}$, $X_\infty = N^{\alpha+\delta}$ for $\alpha = \alpha_1 + \alpha_2$ and $\beta = \beta_1 + \beta_2$
- $R = X_\infty X_1^{s-1} X_2^{s-1} X_3^{s-1} X_4^{s-1+t} X_5^{s-1+t}$ for integers $s$ and $t$

Define two monomial sets $S$ and $T$ for integers $s \geq 1$ and $t \geq 0$

$$S = \bigcup_{0 \leq j_4, j_5 \leq t} \left\{ x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4+j_4} x_5^{i_5+j_5} \,\middle|\, x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \text{ is a monomial of } f^{s-1} \right\}$$

$$T = \bigcup_{0 \leq j_4, j_5 \leq t} \left\{ x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4+j_4} x_5^{i_5+j_5} \,\middle|\, x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \text{ is a monomial of } f^{s} \right\}$$

# Implicit-Key Attack – (3)

Define the shift polynomials $g$ and $g'$ according to $S$ and $T$

$$g : x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} f' X_1^{s-1-i_1} X_2^{s-1-i_2} X_3^{s-1-i_3} X_4^{s-1+t-i_4} X_5^{s-1+t-i_5} \quad \text{for } x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in S$$

$$g' : x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} R \text{ for } x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in T \backslash S$$

Coefficient vectors of $g(x_i X_i), g'(x_i X_i)$ generate a basis matrix $B$

- $B$ is a square and triangular matrix
- $\det(\mathcal{L}) = \det(B)$ is the product of diagonal elements

# Implicit-Key Attack – (4)

Apply the crucial condition $\det(\mathcal{L}) < R^w$ in lattice-based method

- $\prod_{j=1}^{5} X_j^{s_j} < X_\infty^{s_g}$ for $s_j = \sum_{x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} x_5^{i_5} \in T \setminus S} i_j$ and $s_g = |S|$

Obtain final condition for conducting implicit-key attack ($\tau = t/s$)

$$\delta < \frac{(\alpha+\beta-1)(1+10\tau+20\tau^2) - 10\tau^2 - 30\tau^3}{4+30\tau+40\tau^2} - \frac{\alpha}{2} + 1$$

Set the optimal value of $\tau$ when it is the only positive root of

$$120x^4 + 180x^3 + (86 - 20\alpha - 20\beta)x^2 + (16 - 8\alpha - 8\beta)x - \alpha - \beta + 1 = 0$$

# Main Result

**Implicit-Key Attack**

Let $N_1 = p_1q_1, N_2 = p_2q_2$ be two RSA moduli of the same bit-size, and $p_1, q_1, p_2, q_2$ be primes of the same bit-size. Let $e_1, d_1, e_2, d_2$ satisfy $e_1d_1 \equiv 1 \bmod \varphi(N_1)$ and $e_2d_2 \equiv 1 \bmod \varphi(N_2)$, such that $e_1 = N^{\alpha_1}$, $e_2 = N^{\alpha_2}$ and $d_1, d_2 \approx N^{\delta}$. Suppose that $d_1$ and $d_2$ share $\beta_1 \log_2 N$ MSBs and $\beta_2 \log_2 N$ LSBs. Then $N_1, N_2$ can be factored in polynomial time if

$$\delta < \frac{(\alpha+\beta-1)(1+10\tau+20\tau^2)-10\tau^2-30\tau^3}{4+30\tau+40\tau^2} - \frac{\alpha}{2} + 1,$$

where $\alpha = \alpha_1 + \alpha_2$, $\beta = \beta_1 + \beta_2$ and $\tau$ is the only positive root of

$$120x^4 + 180x^3 + (86 - 20\alpha - 20\beta)x^2 + (16 - 8\alpha - 8\beta)x - \alpha - \beta + 1 = 0.$$

# Experimental Results

Randomly generate 1024-bit moduli and implicitly related keys

Table: The comparison of theoretical and experimental results on $\delta$

| $\log_2 N = 1024$ | | | Dim= 6 | | Dim= 21 | | Dim= 56 | |
|---|---|---|---|---|---|---|---|---|
| $\beta_1$ | $\beta_2$ | $\delta_t$ | $\delta_e$ | Time | $\delta_e$ | Time | $\delta_e$ | Time |
| 0.043 | 0.043 | 0.271 | 0.259 | 0.004s | 0.264 | 0.623s | 0.270 | 47.59s |
| 0.064 | 0.101 | 0.291 | 0.280 | 0.004s | 0.286 | 0.621s | 0.291 | 47.17s |
| 0.107 | 0.142 | 0.312 | 0.300 | 0.004s | 0.307 | 0.682s | 0.311 | 37.23s |
| 0.150 | 0.150 | 0.325 | 0.315 | 0.005s | 0.321 | 0.522s | 0.325 | 32.02s |

# Conclusion

**Focus on a new attack scenario concerning implicitly related keys**

- Factor RSA moduli using implicit information about private keys
- Apply lattice-based method for solving integer equations
- Verify the validity of implicit-key attack by numerical experiments

**Further improvements remain as future work**

- More efficient lattice construction for implicit-key attack
- Similar attacks on the RSA cryptosystem in practice

**Thank You!**

**Q & A**