Partial Key Exposure Attacks on the RSA Cryptosystem

Ellen Jochemsz
TU/e Coding & Crypto Group

SAFE-NL PhD Meeting: December 2nd 2004
Outline

• Basics of the RSA cryptosystem
• What is a partial key exposure attack?
• How can we perform such an attack?
• Results
• Comments, open questions...

Research

In this talk some recent results in this area are sketched.
This research is done together with: Benne de Weger (TU Eindhoven), Alexander May and Matthias Ernst (University of Paderborn).
Basics of RSA

The RSA cryptosystem (1977), invented by Rivest, Shamir and Adleman, was the world’s first (and most successful) public key encryption algorithm.

Public key cryptography:

- **public** encryption key
- **secret** decryption key

We need a mathematical operation which is easy to do one-way (encryption), but hard to do the other way (decryption without the secret information).

Factoring Problem: $N = pq$, where $p$ and $q$ are large primes.

"The obvious mathematical breakthrough would be the development of an easy way to factor large prime numbers" (Bill Gates, The Road Ahead)
Basics of RSA (II)

- $N = pq$, with $p$ and $q$ primes of equal bitsize.

- Encryption: $E(m) \equiv m^e \pmod{N}$, for a chosen encryption key $e$.

- Decryption: $D(c) \equiv c^d \pmod{N}$, for decryption key $d$ satisfying

  $$\frac{e \cdot d - 1}{\phi(N)} = k \cdot \frac{e \cdot d}{N}$$

  where $\phi(N) = (p - 1)(q - 1)$.

- Check: $D(E(m)) \equiv m^{ed} \equiv m^1 \pmod{N}$

Often, $e$ or $d$ is chosen to be small for efficient modular exponentiation, for example: $e = 65537 = 2^{16} + 1 = [10000000000000001]_2$
Attacking RSA

- Factor $N$: Number Field Sieve $\Rightarrow N \approx 2^{1024}$ is still safe
- Exploit implementation/usage errors (i.e. a common modulus, or a common small $e$)
- Recover $d$ when:
  - $d$ is "small" $\left\{egin{array}{l}
  \text{Wiener: } d < N^{0.25} \\
  \text{Boneh/Durfee: } d < N^{0.292}
  \end{array}\right.$
  - $e$ is "small" and the attacker has some partial information on $d$
  - $d$ is "small" and the attacker has some partial information on $d$
Partial Key Exposure Attacks

If the attacker recovers a fraction of $d$, can he recover the whole private key?

**Motivation:**
Implementations can leak bits of $d$ (side-channel attacks, timing attacks)
We assume either MSBs (most significant bits) or LSBs (least significant bits) of $d$ are known to the attacker.

**Result:**
When either $e$ or $d$ is ‘small’, then partial key exposure attacks apply.

**This talk:**
- $d$ is small: $d = N^\beta$, $0 < \beta < 1$.
- MSBs of $d$ are known.
The RSA Key Equation

The exponents $e$ and $d$ satisfy:

$$ed \equiv 1 \mod \phi(N), \text{ where } \phi(N) = (p - 1)(q - 1), \text{ or}$$

$$ed - 1 = k(N - (p + q - 1)) \quad \text{(RSA key equation)}$$

Setting: $d$ is small $\rightarrow d = N^\beta, \ 0 < \beta < 1.$

MSBs of $d$ known $\rightarrow d = \tilde{d} + d_0, \text{ with } d_0 = N^\delta, \ 0 < \delta < \beta.$

$$e(\tilde{d} + x) - 1 = y(N - z) \quad x = d_0 < N^\delta$$

$$y = k < N^\beta$$

$$z = p + q - 1 < N^{1/2}.$$  

Looking for a small root of $f(x, y, z) = ex - Ny + yz + R.$
Finding Small Roots

How to find the small root \((x_0, y_0, z_0) = (d_0, k, p + q - 1)\) of

\[ f(x, y, z) = ex - Ny + yz + R? \]

We use a method of Coppersmith, reformulated by Coron.

Idea:

- Construct two polynomials \(f_1, f_2\) with the same root \((x_0, y_0, z_0)\) that are not multiples of \(f\).
- Use resultant methods to obtain \(x_0, y_0,\) and \(z_0,\) from the three equations.

Heuristic: Are \(f_1\) and \(f_2\) algebraically independent? \(\Rightarrow\) experiments
How to find $f_1$ and $f_2$

Howgrave-Graham

- $h(x, y, z) \in \mathbb{Z}[x, y, z]$, a polynomial, sum of at most $\omega$ monomials,
- $h(x_0, y_0, z_0) \equiv 0 \mod n$ for some $|x_0| < X$, $|y_0| < Y$, $|z_0| < Z$,
- $\|h(xX, yY, zZ)\| < \frac{n}{\sqrt{\omega}}$.

Then $h(x_0, y_0, z_0) = 0$ holds over the integers.

Variations $g_{ijk}$ on $f$ that have the root $(x_0, y_0, z_0) \mod n$ for some $n$:

$$x^i y^j z^k f(x, y, z) \cdot c_{ijk}, \quad nx^i y^j z^k.$$

Find independent linear combinations $f_1(xX, yY, zZ), f_2(xX, yY, zZ)$ of $g_{ijk}(xX, yY, zZ)$, such that they satisfy Howgrave-Graham’s bound.

The choice of $n$ and $c_{ijk}$ should imply that $f_1$ and $f_2$ are not multiples of $f$. 
How to find $f_1$ and $f_2$ (II)

Let the coefficient vectors of $g_{ijk}(xX, yY, zZ)$ be the basis for a lattice $L$.

Lattice $L = \sum_{i=1}^{\omega} \mathbb{Z}b_i$, where $b_i \in \mathbb{R}^\omega$ are basis vectors.

Finding a 'small' basis:
Instead of Gram-Schmidt orthogonalization, we have LLL-reduction.
How to find $f_1$ and $f_2$ (III)

LLL-reduction (Lenstra, Lenstra, Lovasz) = polynomial time algorithm.

Input: basis vectors $\{g_1, \ldots, g_\omega\}$ that span the lattice $L$

Output: reduced basis vectors $\{f_1, \ldots, f_\omega\}$ that also span $L$, with

$$\|f_1(xX, yY, zZ)\| \leq \|f_2(xX, yY, zZ)\| \leq 2^{\frac{\omega}{4}} \det(L)^{\frac{1}{\omega-1}}.$$ 

So, if

$$2^{\frac{\omega}{4}} \det(L)^{\frac{1}{\omega-1}} < \frac{n}{\sqrt{\omega}},$$

then the polynomials $f_1$ and $f_2$ can be found.
Pictures MSB Attacks

Small $d$ and known MSB’s of $d$

Small $e$ and known MSB’s of $d$

Wi = Wiener (1990)
BD = Boneh/Durfee (2000)
BDF = Boneh/Durfee/Frankel (1998)
BM = Blömer/May (2003)
Other attacks = Recent results Ernst/Jochemsz/May/deWeger
Pictures LSB Attacks

Small $d$ and known LSB’s of $d$

Small $e$ and known LSB’s of $d$

Wi = Wiener (1990)
BD = Boneh/Durfee (2000)
BDF = Boneh/Durfee/Frankel (1998)
BM = Blömer/May (2003)
Other attack = Recent result Ernst/Jochemsz/May/deWeger
Comments about the pictures

- Our methods for MSBs known work up to full size $e$ or $d$.

  $\Rightarrow$ If you choose a small $e$ or $d$ (for more efficient computations), be aware of partial key exposure attacks.

- Natural starting points of our methods. This comes from the fact that our method is general: the analysis we apply on the polynomial

  $$f(x, y, z) = ex - Ny + yz + R$$

  also works for other polynomials with the monomials $1, x, y, yz$.

  $\Rightarrow$ lots of old & new cryptanalysis results are special cases.
Conclusion

Be aware of partial key exposure attacks when $e$ or $d$ is small. Take countermeasures (against side-channel attacks) to prevent bits of $d$ from leaking.

Future Research

• The choice of the "shifts" $g_{ijk}$:

$$x^i y^j z^k f(x, y, z) \cdot c_{ijk}, \quad n x^i y^j z^k.$$  

How to choose the ranges of $i$, $j$, $k$ (for general polynomials) is still an open problem.

• Improvement of the areas of attack.

• Other situations, for instance CRT:

$$d_p = d \mod (p - 1)$$
$$d_q = d \mod (q - 1)$$

• ...