Solving RSA Problems with Lattice Reduction

Alexander May

Faculty for Mathematics
Horst-Görtz Institute
Ruhr-University Bochum

8th Central European Conference on Cryptography
Graz, July 2, 2008
### Factorization problem

<table>
<thead>
<tr>
<th>Given</th>
<th>$N = pq$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find</td>
<td>$p, q$</td>
</tr>
</tbody>
</table>

### RSA problem

<table>
<thead>
<tr>
<th>Given</th>
<th>$N, e, m^e \mod N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find</td>
<td>$m \in \mathbb{Z}_N$</td>
</tr>
</tbody>
</table>

### Secret key problem

<table>
<thead>
<tr>
<th>Given</th>
<th>$N, e$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find</td>
<td>$d$ with $ed = 1 \mod \phi(N)$</td>
</tr>
</tbody>
</table>

**Relations:** Secret Key Problem $\Leftrightarrow$ Factoring $\Rightarrow$ RSA
Tackling Factorization/RSA

**Goal:** Polynomial complexity on Turing machines

- Quadratic Sieve (81) \( \exp(O(\sqrt{\log N \log \log N})) \)
- Elliptic Curve (87) \( \exp(O(\sqrt{\log p \log \log p})) \)
- Number Field Sieve (93) \( \exp(O(\log^{\frac{1}{3}} N \log \log^{\frac{2}{3}} N)) \)

"Relaxed" model: Shor 94
Polynomial complexity on Quantum Turing machines

"Relaxed" problems:
Polynomial complexity for factoring *with a hint.*
- Provide *limited oracle access*
- Model problems as polynomial equations
- Search space: Still exponential size
- Motivation: Side-channel attacks
Different types of oracles

Rivest, Shamir (EC 86):
- Oracle for most significant bits of $p$
- Amount: $\frac{3}{5} \log p$ queries

Maurer (EC 92):
- Oracle for arbitrary questions, oracle answers: yes/no
- Amount: $\epsilon \log p$ for all $\epsilon > 0$

Coppersmith (EC 96):
- Oracle for most significant bits of $p$
- Amount: $\frac{1}{2} \log p$ queries
Modelling as polynomial equations

Given: \( N = pq \)

Find: \( p, q \)

- Polynomial: \( f(x, y) = N - xy \)
- Roots: \( (1, N), (p, q), (q, p), (N, 1) \)

Goal: Find \((x_0, y_0), x_0 \leq X, y_0 \leq Y \) s.t. \( XY \leq N \)

Oracle for most significant bits:

Given: \( N = pq, \tilde{p} \) with \( |p - \tilde{p}| \leq N^{\frac{1}{4}} \)

- Let \( \tilde{q} = \frac{N}{\tilde{p}} \), then \( |q - \tilde{q}| \leq N^{\frac{1}{4}} \)
- Polynomial: \( f(x, y) = N - (\tilde{p} + x)(\tilde{q} + y) \)
- Root: \( (p - \tilde{p}, q - \tilde{q}) \)

Coppersmith 96: Polynomial time for \( XY \leq N^{\frac{1}{2}} \).
Coppersmith’s method

Given: \( f(x), N \in \mathbb{N} \) of unknown factorization
Find: Roots \( |x_0| \leq X \) s.t. \( f(x_0) = 0 \mod b, b | N \).

Outline of the construction

1. Define collection of polynomials \( f_1(x), f_2(x), \ldots, f_n(x) \) with the roots \( |x_0| \leq X \) modulo \( b^m \) for some \( m \).

2. Construct \( g(x) = \sum_{i=1}^{n} a_i f_i \), \( a_i \in \mathbb{Z} \) such that \( g(x_0) = 0 \) over \( \mathbb{Z} \).

Sufficient condition: \( |g(x_0)| < b^m \).

Construction of \( g \) uses LLL lattice reduction.

3. Solve \( g(x) \) over the integers.
Lemma Hastad, Howgrave-Graham

Let \( g(x) \in \mathbb{Z}[x] \) be a polynomial of degree \( n - 1 \) with

- \( g(x_0) = 0 \mod b^m \), where \( |x_0| \leq X \)
- \( ||g(xX)|| < \frac{b^m}{\sqrt{n}} \)

Then \( g(x_0) = 0 \) over the integers.

**Notation:** \( g(x) = ax^2 + bx + c, g(xX) = aX^2x^2 + bXx + c \)

\[ ||g(xX)|| = ||(aX^2, bX, c)|| \]

**Proof:**

\[
|g(x_0)| = \left| \sum_{i=0}^{n-1} a_i x_0^i \right| \leq \sum_{i=0}^{n-1} \left| a_i X^i \left( \frac{x_0}{X} \right)^i \right|
\]

\[
\leq \sum_{i=0}^{n-1} |a_i X^i| \leq \sqrt{n} \cdot ||g(xX)|| < b^m
\]
Example: \( f(x) = \tilde{p} + x \mod p \)

Collection of polynomials:
- \( N^{2-i}f^i(x) \) for \( i = 0, 1, 2 \)
- \( x^j f^2(x) \) for \( j = 1, 2 \)

All polynomials have small root \( p - \tilde{p} \) modulo \( p^2 \).

\[
B = \begin{pmatrix}
N^2 & NX & X^2 \\
\tilde{p} & 2\tilde{p}X & X^2 \\
0 & \tilde{p}^2X & 2\tilde{p}X^2 & X^3 \\
0 & 0 & \tilde{p}^2X^2 & 2\tilde{p}X^3 & X^4
\end{pmatrix}
\]

- \( \dim(L) = 5, \det(L) = X^{10}N^3 \)
LLL outputs coefficient vector $\mathbf{v}$ of $g(xX)$ with

$$
\| \mathbf{v} \| \leq c^\text{dim}(L) \det(L)^{\frac{1}{\text{dim}(L)}} \leq \frac{p^2}{\sqrt{\text{dim}(L)}}.
$$

Neglecting low-order terms yields condition

$$
\det(L) \leq p^{2\text{dim}(L)}.
$$

Plugging our values in

$$
X^{10} N^3 \leq N^5 \iff X \leq N^{\frac{1}{5}}.
$$
In general: The univariate case

**Theorem**

1. Let $N$ be a composite number of unknown factorization with divisor $b \geq N^\beta$.
   
   $$p \geq N^{1/2}$$

2. Let $f_p(x)$ be a monic polynomial of degree $\delta$.
   
   $$f_p(x) = \tilde{p} + x, \quad \delta = 1$$

Then we can find all solutions $x_0$ for the equation

$$f_p(x) = 0 \mod b \quad \text{with} \quad |x_0| \leq N^{\frac{\beta^2}{\delta}}$$

$$|x_0| \leq N^{\frac{1}{4}}$$

in time $O(\delta^5 \log^9 N)$. 

Alexander May, Ruhr-University Bochum – CECC 2008, Graz
Factoring $N = p^r q$ [BDH99]

Relaxed Factorization: High Bits Known

**Given:** $N = p^r q$, $\tilde{p}$ with $|p - \tilde{p}| \leq N^{\frac{r}{(r+1)^2}}$

**Find:** $p, q$

Model polynomial equation as

$$f(x) = (\tilde{p} + x)^r \mod p^r.$$

Apply Theorem with $\beta = \frac{r}{r+1}$ and $\delta = r$. Find

$$|x_0| \leq N^{\frac{\beta^2}{\delta}} = N^{\frac{r}{(r+1)^2}}.$$

Since $N \approx p^{r+1}$, we need $|p - \tilde{p}| \leq p^{\frac{r}{r+1}}$.

For $r = \Omega \left( \sqrt{\frac{\log N}{\log \log N}} \right)$, $\tilde{p}$ can be guessed in ptime.
Factoring $\leq p$ Computing $d$

**Given:** $N = pq$, $e$, $d$ with $ed < N^2$

**Find:** $p$, $q$

Let $M = ed - 1 = N^\alpha$ for some $\alpha < 2$. Define

$$f(x) = N - x \mod \phi(N)$$

with root $x_0 = p + q - 1 \approx N^{\frac{1}{2}}$. Notice that

$$\phi(N) \approx N = M^{\frac{1}{\alpha}}.$$

Application of Theorem yields

$$|x_0| \leq M^{\frac{1}{\alpha^2}} = N^{\frac{1}{\alpha}}.$$
Relaxed Factorization: Arbitrary Bits Known

**Given:** \( N = pq, \tilde{p}, k_1, \ldots, k_r \)

**Find:** \( p, q \)

Model polynomial equation as

\[
f(x) = \tilde{p} + x_12^{k_1} + x_22^{k_2} + \ldots + x_r2^{k_r} \mod p.
\]

Can find the solution whenever

\[
\ln(2) \approx 69.3\% \text{ of } p \text{'s bits known.}
\]

Running time is

- polynomial if \( r = \mathcal{O}(\log \log N) \)
- better than NFS if \( r = \mathcal{O}(\log^{\frac{1}{3}} N \log \log^{\frac{2}{3}} N) \)
### Experiments for 512-bit $N$

<table>
<thead>
<tr>
<th>$n$</th>
<th>pred (bit)</th>
<th>exp (bit)</th>
<th>dim($L$)</th>
<th>time (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>90</td>
<td>45/45</td>
<td>136</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>90</td>
<td>87/5</td>
<td>136</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>56</td>
<td>19/19/19</td>
<td>120</td>
<td>0.3</td>
</tr>
<tr>
<td>3</td>
<td>56</td>
<td>52/5/5</td>
<td>120</td>
<td>0.3</td>
</tr>
<tr>
<td>3</td>
<td>69</td>
<td>23/23/23</td>
<td>286</td>
<td>450</td>
</tr>
<tr>
<td>3</td>
<td>69</td>
<td>57/6/6</td>
<td>286</td>
<td>580</td>
</tr>
<tr>
<td>4</td>
<td>22</td>
<td>9/8/8/8</td>
<td>126</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>22</td>
<td>19/5/5/5</td>
<td>126</td>
<td>4.5</td>
</tr>
</tbody>
</table>
Relaxed RSA Problem

RSA Problem

<table>
<thead>
<tr>
<th>Given:</th>
<th>$N = pq$, $e \in \mathbb{Z}_\phi^*(N)$ and $c = m^e \text{ mod } N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find:</td>
<td>$m \in \mathbb{Z}_N$</td>
</tr>
</tbody>
</table>

- **Relaxation:** Small $e$, $m$
  Trivial if $m < N^{1/e}$: Compute $c^{1/e}$.

- **Inhomog. case:** Small $e$, parts of $m$ known
  C ’96: Model as
  \[ f(x) = (\tilde{m} + x)^e - c \text{ mod } N. \]

  Find $x_0 = m - \tilde{m}$ for $|x_0| \leq N^{\frac{\beta^2}{\delta}} = N^{\frac{1}{e}}$.

**Cryptanalysis:** Given an $\frac{e-1}{e}$-fraction, the rest is easy.

**Security:** Recovering an $\frac{e-1}{e}$-fraction must be hard.
RSA-OAEP

Format $m = s \cdot 2^k + t$ with

\[ s = g(r) \oplus (M||0^{k_1}) \quad \text{and} \quad t = h(s) \oplus r \]

Show: CCA2-attacker $\Rightarrow$ RSA-Inverter for $c = m^e$

Idea:

- CCA2-attacker has to query $h$ on $s$.
- Solve $f(t) = (s \cdot 2^k + t)^e - c \mod N$ for $t \leq N^{\frac{1}{e}}$.
- Compute $r = h(s) \oplus t$. Compute $M$ from $s$. 
RSA Broadcast Problem

**Given:** \( c_i = m^{e_i} \mod N_i \) for \( i = 1, \ldots, k \) with \( k \geq \max_i \{e_i\} \)

**Find:** \( m < \min_i \{N_i\} \)

- Let \( N = \prod_{i=1}^{k} N_i \) and \( \delta = \max_i \{e_i\} \).
- Compute by CRT
  
  \[
  f(x) = \sum_{i=1}^{k} b_i \cdot (x^{e_i} - c_i)x^{\delta-e_i} \mod N.
  \]
- We can find all roots \( m \) of \( f(x) \) provided that
  
  \[
  m < \min\{N_i\} \leq N_1^{\frac{1}{k}} \leq N_1^{\frac{1}{\delta}}.
  \]
Condition $k \geq \max_i \{e_i\}$

Solve
\[
\begin{align*}
  x^3 &= c_1 \mod N_1 \\
  x^3 &= c_2 \mod N_2 \\
  x^3 &= c_3 \mod N_3 \\
  x^5 &= c_4 \mod N_4
\end{align*}
\]

Solvable, but $k < \max_i \{e_i\}$.

Change condition to:
There exists a subset $S$ of $k$ polynomials s.t.

\[ k \geq \max_{i \in S} \{e_i\}. \]
A less trivial example

Solve

\[
\begin{align*}
  x^3 &= c_1 \mod N_1 \\
  x^3 &= c_2 \mod N_2 \\
  x^5 &= c_3 \mod N_3 \\
  x^5 &= c_4 \mod N_4
\end{align*}
\]
A less trivial example

Solve

\[
\begin{align*}
  x^3 &= c_1 \mod N_1 \\
  x^3 &= c_2 \mod N_2 \\
  x^5 &= c_3 \mod N_3 \\
  x^5 &= c_4 \mod N_4 
\end{align*}
\]

Change to

\[
\begin{align*}
  (x^3 - c_1)^2 &= 0 \mod N_1^2 \\
  (x^3 - c_2)^2 &= 0 \mod N_2^2 \\
  x^5 - c_3 &= 0 \mod N_3 \\
  x^5 - c_4 &= 0 \mod N_4 
\end{align*}
\]

CRT: \( f(x) \) of degree 6 with root modulo

\[
N_1^2 N_2^2 N_3 N_4 > \min\{N_i\}^6
\]
Optimal Broadcast Condition

**Given:** \( c_i = m^{e_i} \mod N_i \) for \( i = 1, \ldots, k \)
with \( \sum_{i=1}^{k} \frac{1}{e_i} \geq 1 \)

**Find:** \( m < \min_i \{N_i\} \)

- Let \( \delta = \text{lcm}\{e_i\} \) and \( N = \prod_{i=1}^{k} N_i^{\frac{\delta}{e_i}} \).
- Let \( g_i(x) = (x^{e_i} - c_i)^{\frac{\delta}{e_i}} \) with \( g_i(m) = 0 \mod N_i^{\frac{\delta}{e_i}} \).
- Compute by CRT
  \[
  f(x) = \sum_{i=1}^{k} b_i \cdot g_i(x) \mod N.
  \]
- We can find all roots \( m \) of \( f(x) \) provided that
  \[
  m < \min\{N_i\} \leq \prod_{i=1}^{k} N_i^{\frac{1}{e_i}} = N^{\frac{1}{\delta}}.
  \]
RSA Secret Key Problem

Relaxed RSA Secret Key Problem

**Given:** \( N = pq, \ e \in \mathbb{Z}_{\phi(N)}^* \)

**Find:** \( d \leq N^{\frac{1}{4}} \) such that \( ed = 1 \mod \phi(N) \)

**RSA equation:** \( ed = 1 + k(N - (p + q - 1)) \)

- **mod \( N \) (W 90):** \( f(x, y) = ex - y \mod N \) with
  \[ |x_0y_0| \approx |dk(p + q - 1)| \leq N^{\frac{1}{4} + \frac{1}{4} + \frac{1}{2}}. \]

- **mod \( e \) (BD 99):** \( f(x, y) = 1 + x(N - y) \mod e \)
  - Linearization yields bound \( d \leq N^{\frac{1}{2}} \).
  - Using the polynomial structure \( d \leq N^{0.292} \).
RSA with Small Exponent $d$

Fraction of MSBs of $d$

$\log_N d$

Wiener

BD

EJMW
Chinese Remainder Theorem: Compute $m = c^d \mod N$ via

$$
\begin{align*}
  c &= m^d \mod p \\
  c &= m^d \mod q
\end{align*}
$$

Relaxed Problem: Small CRT-Exponents

Given: $N = pq$, $e \in \mathbb{Z}_\phi(N)^*$
Find: $d = (d_p \mod p - 1, d_q \mod q - 1)$ small

- Bleichenbacher, May ’06: Small $e$
  - Linearization attack
  - Cryptanalysis of two RSA-variants
- Jochemsz, May ’07: $d_p, d_q \leq N^{0.073}$
  - Uses polynomial structure
**Setting:** $d_q \leq d_p$ small, $p$, $q$ of same bit-size

Look at

\[
\begin{align*}
ed_p &= 1 + k(p - 1) \\
ed_q &= 1 + \ell(q - 1)
\end{align*}
\]

with $k, \ell \leq \frac{ed_p}{\sqrt{N}}$. Rewrite as

\[
\begin{align*}
ed_p + k - 1 &= kp \\
ed_q + \ell - 1 &= \ell q
\end{align*}
\]

Multiply

\[
e^2 d_p d_q + e(d_p(\ell - 1) + d_q(k - 1)) + (1 - N)k\ell = k + \ell - 1
\]
Experiments for JM-attack

<table>
<thead>
<tr>
<th>$N$</th>
<th>$d_p, d_q$</th>
<th>pred</th>
<th>asym</th>
<th>dim</th>
<th>LLL-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 bit</td>
<td>10 bit</td>
<td>&lt; 0</td>
<td>73</td>
<td>56</td>
<td>61 sec</td>
</tr>
<tr>
<td>1000 bit</td>
<td>13 bit</td>
<td>&lt; 0</td>
<td>73</td>
<td>95</td>
<td>1129 sec</td>
</tr>
<tr>
<td>1000 bit</td>
<td>15 bit</td>
<td>2</td>
<td>73</td>
<td>115</td>
<td>13787 sec</td>
</tr>
<tr>
<td>2000 bit</td>
<td>20 bit</td>
<td>&lt; 0</td>
<td>146</td>
<td>56</td>
<td>255 sec</td>
</tr>
<tr>
<td>2000 bit</td>
<td>27 bit</td>
<td>&lt; 0</td>
<td>146</td>
<td>95</td>
<td>1432 sec</td>
</tr>
<tr>
<td>2000 bit</td>
<td>32 bit</td>
<td>4</td>
<td>146</td>
<td>115</td>
<td>36652 sec</td>
</tr>
<tr>
<td>5000 bit</td>
<td>52 bit</td>
<td>&lt; 0</td>
<td>365</td>
<td>56</td>
<td>1510 sec</td>
</tr>
<tr>
<td>5000 bit</td>
<td>70 bit</td>
<td>&lt; 0</td>
<td>365</td>
<td>95</td>
<td>18032 sec</td>
</tr>
<tr>
<td>10000 bit</td>
<td>105 bit</td>
<td>&lt; 0</td>
<td>730</td>
<td>56</td>
<td>3826 sec</td>
</tr>
<tr>
<td>10000 bit</td>
<td>140 bit</td>
<td>&lt; 0</td>
<td>730</td>
<td>95</td>
<td>57606 sec</td>
</tr>
</tbody>
</table>
How far can we improve?

<table>
<thead>
<tr>
<th>Problem</th>
<th>Relaxed</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factoring</td>
<td>$</td>
<td>p - \tilde{p}</td>
</tr>
<tr>
<td>RSA</td>
<td>$</td>
<td>m - \tilde{m}</td>
</tr>
<tr>
<td>$d$</td>
<td>$d \leq N^{0.292}$</td>
<td>$N$</td>
</tr>
<tr>
<td>$d_p, d_q$</td>
<td>$d_p, d_q \leq N^{0.073}$</td>
<td>$N^{1/2}$</td>
</tr>
</tbody>
</table>
How far can we improve?

<table>
<thead>
<tr>
<th>Problem</th>
<th>Relaxed</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factoring</td>
<td>$</td>
<td>p - \tilde{p}</td>
</tr>
<tr>
<td>RSA</td>
<td>$</td>
<td>m - \tilde{m}</td>
</tr>
<tr>
<td>$d$</td>
<td>$d \leq N^{0.292}$</td>
<td>$N$</td>
</tr>
<tr>
<td>$d_p, d_q$</td>
<td>$d_p, d_q \leq N^{0.073}$</td>
<td>$N^{\frac{1}{2}}$</td>
</tr>
</tbody>
</table>

**Polynomial**

\[
f(x, y) = N - (\tilde{p} + x)(\tilde{q} + y)
\]

**Bound**

\[
XY \leq N^{\frac{1}{2}}
\]

\[
f(x, y) = N - (\tilde{p} + x)y
\]

\[
f(x, y) = N - xy
\]
### Problem

<table>
<thead>
<tr>
<th>Problem</th>
<th>Relaxed</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factoring</td>
<td>$</td>
<td>p - \tilde{p}</td>
</tr>
<tr>
<td>RSA</td>
<td>$</td>
<td>m - \tilde{m}</td>
</tr>
<tr>
<td>$d$</td>
<td>$d \leq N^{0.292}$</td>
<td>$N$</td>
</tr>
<tr>
<td>$d_p, d_q$</td>
<td>$d_p, d_q \leq N^{0.073}$</td>
<td>$N \frac{1}{2}$</td>
</tr>
</tbody>
</table>

### Polynomial

<table>
<thead>
<tr>
<th>Bound</th>
<th>$XY \leq N \frac{1}{2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f(x, y) = N - (\tilde{p} + x)(\tilde{q} + y)$</td>
<td>$XY \leq N \frac{3}{4}$</td>
</tr>
<tr>
<td>$f(x, y) = N - (\tilde{p} + x)y$</td>
<td>$XY \leq N^{1-\epsilon}$</td>
</tr>
<tr>
<td>$f(x, y) = N - xy$</td>
<td></td>
</tr>
</tbody>
</table>
• Relaxed problems: Interesting results

• Duality: Cryptanalysis vs. Security

• Ongoing progress

• Many open problems
  • Finding an optimal collection
  • Giving best bounds
  • Provability in multivariate case

• Can we eventually solve general instances?