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 and RSA

Factorization problem

Given: $N = pq$
Find: p, q

RSA problem

Given: $N, e, m^e \bmod N$
Find: $m \in \mathbb{Z}_N$

Secret key problem

Given: N, e
Find: d with $ed = 1 \bmod \phi(N)$

Relations: Secret Key Problem $\Leftrightarrow$ Factoring $\Rightarrow$ RSA

Tackling Factorization/RSA

Goal: Polynomial complexity on Turing machines

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

"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. $f(x_0) = 0 \bmod b$, $b|N$.

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

   $$g(x_0) = 0 \text{ over } \mathbb{Z}.$$

   Sufficient condition: $|g(x_0)| < b^m$.
   Construction of g uses LLL lattice reduction.
3. Solve $g(x)$ over the integers.

Sufficient condition in terms of coefficient vector norm

Lemma Hastad, Howgrave-Graham

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

- $g(x_0) = 0 \bmod b^m$, 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:

$$\begin{aligned} |g(x_0)| &= \left|\sum_{i=0}^{n-1} a_i x_0^i\right| \leq \sum_{i=0}^{n-1} \left|a_i X^i \left(\frac{x_0}{X}\right)^i\right| \\ &\leq \sum_{i=0}^{n-1} |a_i X^i| \leq \sqrt{n} \cdot ||g(xX)|| < b^m \end{aligned}$$

Example: $f(x) = \tilde{p} + x \bmod p$

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.

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

- $\dim(L) = 5, \det(L) = X^{10} N^3$

LLL vector is short enough

LLL outputs coefficient vector v of $g(xX)$ with

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

Neglecting low-order terms yields condition

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

Plugging our values in

$$X^{10}N^3 \leq N^5 \Leftrightarrow X \leq N^{\frac{1}{5}}.$$

In general: The univariate case

Theorem

1. Let N be a composite number of unknown factorization with divisor $b \geq N^{\beta}$.
   $p \geq N^{\frac{1}{2}}$
2. Let $f_p(x)$ be a monic polynomial of degree δ.
   $f_p(x) = \tilde{p} + x, \; \delta = 1$

Then we can find all solutions x_0 for the equation

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

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

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

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

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

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

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

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

$$|x_0| \leq M^{\frac{1}{\alpha^2}} = N^{\frac{1}{\alpha}}.$$

Factoring with arbitrary bits [Herrmann, May 08]

Relaxed Factorization: Arbitrary Bits Known

Given: $N = pq, \tilde{p}, k_1, \ldots, k_r$
Find: p, q

Model polynomial equation as

$$f(x) = \tilde{p} + x_1 2^{k_1} + x_2 2^{k_2} + \ldots + x_r 2^{k_r} \bmod p.$$

Can find the solution whenever

$\ln(2) \approx 69.3\%$ of p'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

n	**pred (bit)**	**exp (bit)**	dim(L)	time (min)
2	**90**	**45/45**	136	25
2	**90**	**87/5**	136	15
3	**56**	**19/19/19**	120	0.3
3	**56**	**52/5/5**	120	0.3
3	**69**	**23/23/23**	286	450
3	**69**	**57/6/6**	286	580
4	**22**	**9/8/8/8**	126	3
4	**22**	**19/5/5/5**	126	4.5

Relaxed RSA Problem

RSA Problem

Given: $N = pq$, $e \in \mathbb{Z}^*_{\phi(N)}$ and $c = m^e \bmod N$

Find: $m \in \mathbb{Z}_N$

- **Relaxation: Small e, m**
  Trivial if $m < N^{\frac{1}{e}}$: Compute $c^{\frac{1}{e}}$.
- **Inhomog. case: Small e, parts of m known**
  C '96: Model as
  $$f(x) = (\tilde{m} + x)^e - c \bmod N.$$
  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.

Security proof [Shoup 01]

RSA-OAEP

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

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

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

Idea:

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

RSA Broadcast Attack [Hastad 85]

RSA Broadcast Problem

Given: $c_i = m^{e_i} \bmod N_i$ 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
$$f(x) = \sum_{i=1}^{k} b_i \cdot (x^{e_i} - c_i)x^{\delta - e_i} \bmod N.$$
- We can find all roots m of $f(x)$ provided that
$$m < \min\{N_i\} \leq N^{\frac{1}{k}} \leq N^{\frac{1}{\delta}}.$$

Condition $k \geq \max_i\{e_i\}$

Solve
$$\left|\begin{array}{rcl} x^3 & = & c_1 \bmod N_1 \\ x^3 & = & c_2 \bmod N_2 \\ x^3 & = & c_3 \bmod N_3 \\ x^5 & = & c_4 \bmod N_4 \end{array}\right|$$

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
$$\left| \begin{array}{rcl} x^3 & = & c_1 \bmod N_1 \\ x^3 & = & c_2 \bmod N_2 \\ x^5 & = & c_3 \bmod N_3 \\ x^5 & = & c_4 \bmod N_4 \end{array} \right|$$

A less trivial example

Solve
$$\left| \begin{array}{rcl} x^3 & = & c_1 \bmod N_1 \\ x^3 & = & c_2 \bmod N_2 \\ x^5 & = & c_3 \bmod N_3 \\ x^5 & = & c_4 \bmod N_4 \end{array} \right|$$

Change to
$$\left| \begin{array}{rcl} (x^3 - c_1)^2 & = & 0 \bmod N_1^2 \\ (x^3 - c_2)^2 & = & 0 \bmod N_2^2 \\ x^5 - c_3 & = & 0 \bmod N_3 \\ x^5 - c_4 & = & 0 \bmod N_4 \end{array} \right|$$

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

$$N_1^2 N_2^2 N_3 N_4 > \min\{N_i\}^6$$

Broadcast Reloaded [May, Ritzenhofen 08]

Optimal Broadcast Condition

Given: $c_i = m^{e_i} \bmod N_i$ for $i = 1, \ldots, k$
with $\sum_{i=1}^{k} \frac{1}{e_i} \geq 1$

Find: $m < \min_i\{N_i\}$

- Let $\delta = \mathrm{lcm}\{e_i\}$ 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 $g_i(m) = 0 \bmod N_i^{\frac{\delta}{e_i}}$.
- Compute by CRT
$$f(x) = \sum_{i=1}^{k} b_i \cdot g_i(x) \bmod N.$$
- We can find all roots m of $f(x)$ provided that
$$m < \min\{N_i\} \leq \prod_{i=1}^{k} N_i^{\frac{1}{e_i}} = N^{\frac{1}{\delta}}.$$

Relaxed RSA Secret Key Problem

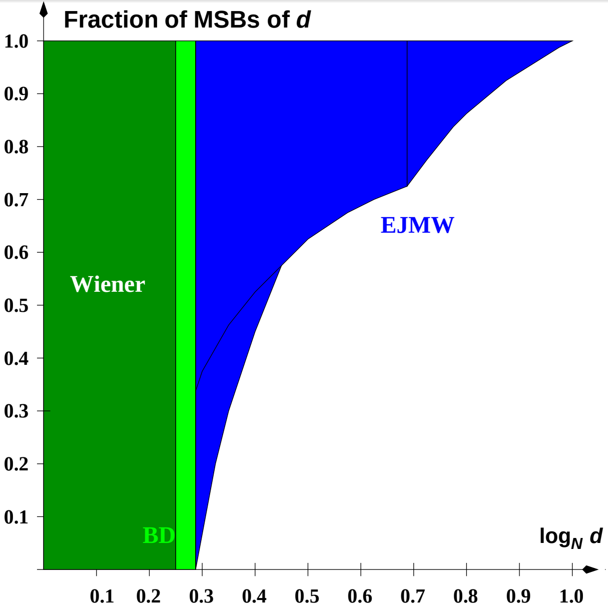
Given: $N = pq$, $e \in \mathbb{Z}^*_{\phi(N)}$

Find: $d \le N^{\frac{1}{4}}$ such that $ed = 1 \bmod \phi(N)$

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

- **mod N (W 90):** $f(x, y) = ex - y \bmod N$ with
$$|x_0 y_0| \approx |dk(p + q - 1)| \le N^{\frac{1}{4}+\frac{1}{4}+\frac{1}{2}}.$$
- **mod e (BD 99):** $f(x, y) = 1 + x(N - y) \bmod e$
  - Linearization yields bound $d \le N^{\frac{1}{4}}$.
  - Using the polynomial structure $d \le N^{0.292}$.

RSA with Small Exponent d



CRT-RSA problem

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

$$\left| \begin{array}{lcl} c & = & m^d \bmod p \\ c & = & m^d \bmod q \end{array} \right| .$$

Relaxed Problem: Small CRT-Exponents

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

Find: $d = (d_p \bmod p - 1, d_q \bmod q - 1)$ 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

Modelling as polynomial

Setting: $d_q \leq d_p$ small, p, q of same bit-size

Look at

$$\left| \begin{array}{rcl} ed_p & = & 1 + k(p-1) \\ ed_q & = & 1 + \ell(q-1) \end{array} \right|$$

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

$$\left| \begin{array}{rcl} ed_p + k - 1 & = & kp \\ ed_q + \ell - 1 & = & \ell q \end{array} \right|$$

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

N	d_p, d_q	pred	asym	dim	LLL-time
1000 bit	10 bit	< 0	73	56	61 sec
1000 bit	13 bit	< 0	73	95	1129 sec
1000 bit	15 bit	2	73	115	13787 sec
2000 bit	20 bit	< 0	146	56	255 sec
2000 bit	27 bit	< 0	146	95	1432 sec
2000 bit	32 bit	4	146	115	36652 sec
5000 bit	52 bit	< 0	365	56	1510 sec
5000 bit	70 bit	< 0	365	95	18032 sec
10000 bit	105 bit	< 0	730	56	3826 sec
10000 bit	140 bit	< 0	730	95	57606 sec

How far can we improve?

Problem	**Relaxed**			**General**
Factoring	$\lvert p - \tilde{p} \rvert$	$\leq$	$N^{\frac{1}{4}}$	$N^{\frac{1}{2}}$
RSA	$\lvert m - \tilde{m} \rvert$	$\leq$	$N^{\frac{1}{e}}$	N
d	d	$\leq$	$N^{0.292}$	N
d_p, d_q	d_p, d_q	$\leq$	$N^{0.073}$	$N^{\frac{1}{2}}$

How far can we improve?

Problem	Relaxed			General
Factoring	$\lvert p-\tilde{p}\rvert$	$\leq$	$N^{\frac{1}{4}}$	$N^{\frac{1}{2}}$
RSA	$\lvert m-\tilde{m}\rvert$	$\leq$	$N^{\frac{1}{e}}$	N
d	d	$\leq$	$N^{0.292}$	N
d_p, d_q	d_p, d_q	$\leq$	$N^{0.073}$	$N^{\frac{1}{2}}$

Polynomial	**Bound**
$f(x,y) = N - (\tilde{p}+x)(\tilde{q}+y)$	$XY \leq N^{\frac{1}{2}}$
$f(x,y) = N - (\tilde{p}+x)y$	$XY \leq N^{\frac{3}{4}}$
$f(x,y) = N - xy$	

How far can we improve?

Problem	Relaxed			General
Factoring	$\lvert p - \tilde{p}\rvert$	$\leq$	$N^{\frac{1}{4}}$	$N^{\frac{1}{2}}$
RSA	$\lvert m - \tilde{m}\rvert$	$\leq$	$N^{\frac{1}{e}}$	N
d	d	$\leq$	$N^{0.292}$	N
d_p, d_q	d_p, d_q	$\leq$	$N^{0.073}$	$N^{\frac{1}{2}}$

Polynomial	**Bound**
$f(x,y) = N - (\tilde{p}+x)(\tilde{q}+y)$	$XY \leq N^{\frac{1}{2}}$
$f(x,y) = N - (\tilde{p}+x)y$	$XY \leq N^{\frac{3}{4}}$
$f(x,y) = N - xy$	$XY \leq N^{1-\epsilon}$

Summary

- 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?**