New RSA Vulnerabilities Using Coppersmith's Method

Alex May

Faculty of Computer Science, Electrical Engineering and Mathematics

University of Paderborn

Outline of the talk

- An introduction to Coppersmith's method
- A Generalized Wiener Attack
- Partial Key Exposure Attacks on RSA
- Computing the RSA Secret Key $\equiv_p$ Factoring

A word about lattices

Let $v_1, \ldots, v_n \in \mathbb{Z}^n$ be linearly independent vectors.

$$L := \left\{ x \in \mathbb{Z}^n \mid x = \sum_{i=1}^{n} a_i v_i \text{ with } a_i \in \mathbb{Z}. \right\}$$

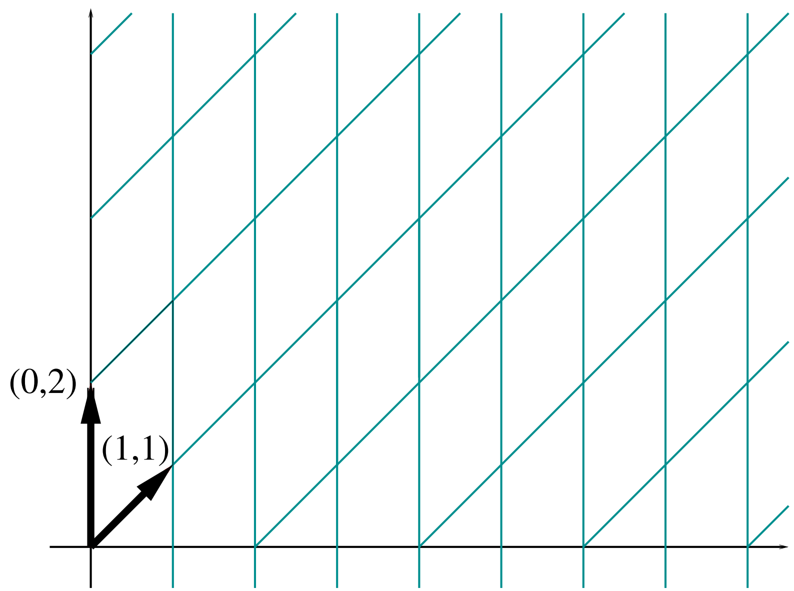


Fig.: Lattice spanned by $\{(0,2),(1,1)\}$

The L^3-algorithm

Theorem[Lenstra, Lenstra, Lovász]: *Let L be a lattice spanned by $v_1, \ldots, v_n$. Then one can find in polynomial time a basis $b_1, \ldots, b_n$ of L with*

$$\|b_1\| \leq 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}}.$$

Coppersmith's method

Problem: Given $f_p(x)$, find all solutions $|x_0| \leq X$ of

$$f_p(x) = 0 \mod p.$$

Coppersmith's method

Problem: Given $f_p(x)$, find all solutions $|x_0| \leq X$ of

$$f_p(x) = 0 \mod p.$$

Idea:

- Collection of polynomials $f_1(x), f_2(x), \ldots, f_n(x)$ with the roots $|x_0| \leq X$ modulo p^m.

- Construct $f(x) = \sum_{i=1}^{n} a_i f_i$, $a_i \in \mathbb{Z}$ such that

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

Sufficient condition: $|f(x_0)| < p^m$.

- Solve $f(x)$ over the integers.

Howgrave Graham's theorem

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

- $f(x_0) = 0 \bmod p^m$, *where* $|x_0| \leq X$
- $||f(xX)|| < \frac{p^m}{\sqrt{n}}$

Then $f(x_0) = 0$ *over the integers.*

Howgrave Graham's theorem

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

- $f(x_0) = 0 \bmod p^m$, *where* $|x_0| \le X$
- $||f(xX)|| < \frac{p^m}{\sqrt{n}}$

Then $f(x_0) = 0$ *over the integers.*

Proof:

$$|f(x_0)| = \left|\sum_{i=0}^{n-1} a_i x_0^i\right| \le \sum_{i=0}^{n-1} \left|a_i X^i \left(\frac{x_0}{X}\right)^i\right|$$

$$\le \sum_{i=0}^{n-1} |a_i X^i| \le \sqrt{n} \cdot ||f(xX)|| < p^m$$

Factoring with high bits known

Theorem[Coppersmith]: *Let* $N = pq$*. Given an approximation* $\tilde{p}$ *of* p *with* $|p - \tilde{p}| \leq N^{\frac{1}{4}-\epsilon}$*, where* $\epsilon > 0$ *arbitrary. Then the factorization of* N *can be found in time polynomial in* $\log N$.

Factoring with high bits known

Theorem[Coppersmith]: *Let* $N = pq$. *Given an approximation* $\tilde{p}$ *of* p *with* $|p - \tilde{p}| \leq N^{\frac{1}{4}-\epsilon}$, *where* $\epsilon > 0$ *arbitrary. Then the factorization of* N *can be found in time polynomial in* $\log N$.

Proof: Let $f_p(x) = \tilde{p} + x$ and $X = N^{\frac{1}{4}-\epsilon}$. Then

$$f_p(x_0) = 0 \bmod p \text{ for some } x_0 \text{ with } |x_0| \leq X.$$

Fix an integer m and define

$$\begin{aligned} g_i(x) &= N^{m-i} f_p^i(x) && \text{for } i = 0, \ldots, m \\ h_j(x) &= x^j f_p^m(x) && \text{for } j = 1, \ldots, m. \end{aligned}$$

The lattice L with basis B

$$\left[\begin{array}{cccccccc}
N^m & & & & & & & \\
- & N^{m-1}X & & & & & & \\
\vdots & \vdots & \ddots & & & & & \\
- & - & \cdots & NX^{m-1} & & & & \\
- & - & \cdots & - & X^m & & & \\
\hline
& - & \cdots & - & - & X^{m+1} & & \\
& & & & \ddots & \ddots & \ddots & \\
& & & & - & - & \cdots & X^{2m}
\end{array}\right]$$

- $\dim(L) = n = 2m + 1$
- $\det(L) = N^{\frac{1}{2}m(m+1)} X^{m(2m+1)}$

L^3-vector is short enough

We need

$$||f(xX)|| \leq 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}} < \frac{p^m}{\sqrt{n}}.$$

Neglecting terms that do not depend on N

$$N^{\frac{1}{2}m(m+1)} X^{m(2m+1)} < p^{nm}.$$

L^3-vector is short enough

We need

$$||f(xX)|| \leq 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}} < \frac{p^m}{\sqrt{n}}.$$

Neglecting terms that do not depend on N

$$N^{\frac{1}{2}m(m+1)} X^{m(2m+1)} < p^{nm}.$$

New condition

$$\frac{1}{2}m(m+1) + \left(\frac{1}{4} - \epsilon\right) m(2m+1) < \frac{1}{2}(2m+1)m.$$

The factorization algorithm

INPUT: $N = pq$, $\tilde{p}$ with $|p - \tilde{p}| \leq N^{\frac{1}{4}-\epsilon}$

- Fix an integer m and construct the basis B with the coefficient vectors of $g_i(xX)$ and $h_j(xX)$.
- Let v be the shortest vector found by the L^3-algorithm when applied on input B.
- Let $f(x)$ be the polynomial whose coefficient vector $f(xX)$ is v. Find a root x_0 of $f(x)$ using standard root-finding algorithms.

OUTPUT: $p = \tilde{p} + x_0, q = \frac{N}{p}$

A variation of the theorem

Corollary: *Let* $N = pq$*. Given an approximation* $\tilde{kp}$ *of* kp *with*

$$|kp - \tilde{kp}| \leq N^{\frac{1}{4}},$$

where k *is not a multiple of* q*. Then the factorization of* N *can be found in polynomial time.*

- Take $f_p = \tilde{kp} + x$ instead of $f_p = \tilde{p} + x$.
- Compute $\gcd(N, kp) = p$.

The general theorem

Theorem: *Let*

- N *be a composite number of unknown factorization with divisor* $p \geq N^{\beta}$
- $f_p(x)$ *be a monic polynomial of degree* δ

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

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

in time polynomial in $(\log N, \delta)$.

A Generalized Wiener Attack

RSA setting:

- $N = pq$, where p, q are of the same bitsize
- e, $d \in \mathbb{Z}^*_{\phi(N)}$ satisfying $ed = 1 \bmod \phi(N)$

Main goal:
Given the public information (N, e), find the factorization of N in polynomial time.

Main result

Wiener's attack (1990):

Given (N, e), one can factor N provided that

$$d \leq \tfrac{1}{3} N^{\frac{1}{4}}.$$

Blömer, May (2004):

Given (N, e), one can factor N provided that

$$ex + y = 0 \bmod \phi(N) \quad \text{with}$$

$$x \leq \tfrac{1}{3} N^{\frac{1}{4}} \quad \text{and} \quad |y| = \mathcal{O}(N^{-\frac{3}{4}} ex).$$

Main result

Wiener's attack (1990):

Given (N, e), one can factor N provided that

$$d \leq \tfrac{1}{3}N^{\frac{1}{4}}.$$

Blömer, May (2004):

Given (N, e), one can factor N provided that

$$ex + y = 0 \bmod \phi(N) \quad \text{with}$$

$$x \leq \tfrac{1}{3}N^{\frac{1}{4}} \quad \text{and} \quad |y| = \mathcal{O}(N^{-\frac{3}{4}}ex).$$

Notice:

- Wiener's result follows for $x = d$ and $y = -1$
- $d = -\frac{x}{y} \bmod \phi(N)$ for small x and y

Concept of the proof

Write

$$ex + y = k(N + 1 - (p + q)).$$

- Compute x and k via continued fraction of $\frac{e}{N}$.

Concept of the proof

Write

$$ex + y = k(N + 1 - (p + q)).$$

- Compute x and k via continued fraction of $\frac{e}{N}$.
- Compute an approximation of $p + q$:

$$N + 1 - \frac{ex}{k} = p + q + \frac{y}{k}$$

with error $\mathcal{O}(N^{\frac{1}{4}})$, since

$$|y| = \mathcal{O}\left(\frac{ex}{N^{\frac{3}{4}}}\right) \quad \text{and} \quad k = \Omega\left(\frac{ex}{N}\right).$$

Finishing the proof

- An approximation of $p - q$ with error $\mathcal{O}(N^{\frac{1}{4}})$:

$$p - q = \sqrt{(p-q)^2} = \sqrt{(p+q)^2 - 4N}$$

- An approximation of p with error $\mathcal{O}(N^{\frac{1}{4}})$.

Theorem (Coppersmith): *Suppose we are given an approximation of p with error $\mathcal{O}(N^{\frac{1}{4}})$. Then N can be factored in polynomial time.*

The YKLM-scheme (2001)

Key Generation Process:

- Choose small e_r and r.
- Compute $d = e_r^{-1} + r \bmod \phi(N)$.
- Compute $e = d^{-1} \bmod \phi(N)$.

The YKLM-scheme (2001)

Key Generation Process:

- Choose small e_r and r.
- Compute $d = e_r^{-1} + r \bmod \phi(N)$.
- Compute $e = d^{-1} \bmod \phi(N)$.

Observe that

$$e(e_r^{-1} + r) - 1 = 0 \bmod \phi(N).$$

Multiplication with e_r yields

$$e(1 + e_r r) - e_r = 0 \bmod \phi(N).$$

Cryptanalytic result

Theorem: *Let* $N = pq$ *be an RSA modulus with* $p - q \geq cN^{\frac{1}{2}}$. *Let* e *be constructed from* e_r *and* r *satisfying*

$$1 + e_r r \leq \frac{1}{3} N^{\frac{1}{4}} \quad \textit{and} \quad e_r \leq \frac{1}{2} c N^{\frac{1}{4}}.$$

On input (N, e), N *can be factored in polynomial time.*

Partial Key Exposure Attacks

Given an RSA public key (N, e) with $N = pq$. The secret key d satisfies the relation

$$ed = 1 \bmod \phi(N).$$

Question: When does the knowledge of a fraction of the secret key bits suffice to factor N?

Partial Key Exposure Attacks

Given an RSA public key (N, e) with $N = pq$. The secret key d satisfies the relation

$$ed = 1 \bmod \phi(N).$$

Question: When does the knowledge of a fraction of the secret key bits suffice to factor N?

Motivation:

- Side-channel attacks on RSA
- Interesting complexity measure

Previous work

Boneh, Durfee, Frankel 1998:

- Certain results for known MSBs of d when $e < \sqrt{N}$.
- A result for known LSBs of d when $e = \text{poly}(\log N)$.

Previous work

Boneh, Durfee, Frankel 1998:

- Certain results for known MSBs of d when $e < \sqrt{N}$.
- A result for known LSBs of d when $e = \text{poly}(\log N)$.

Blömer, May 2003:

- Attack for known MSBs of d when $e < N^{0.725}$.
- Attack for known LSBs of d when $e < N^{\frac{7}{8}}$.
- Attack for known MSBs of $d_p = d \bmod p - 1$ when $e < N^{\frac{1}{4}}$.
- Attack for known LSBs of $d_p = d \bmod p - 1$ when $e = \text{poly}(\log N)$.

Why is d_p interesting ?

Fast RSA decryption:

1. Compute $m^{d_p} \bmod p$.
2. Compute $m^{d_q} \bmod q$.
3. Compute $m^d = CRT(m^{d_p}, m^{d_q}) \bmod N$.

- Method is frequently used and a quasi-standard for smart-cards.
- Smart-cards are highly vulnerable to side-channel attacks.

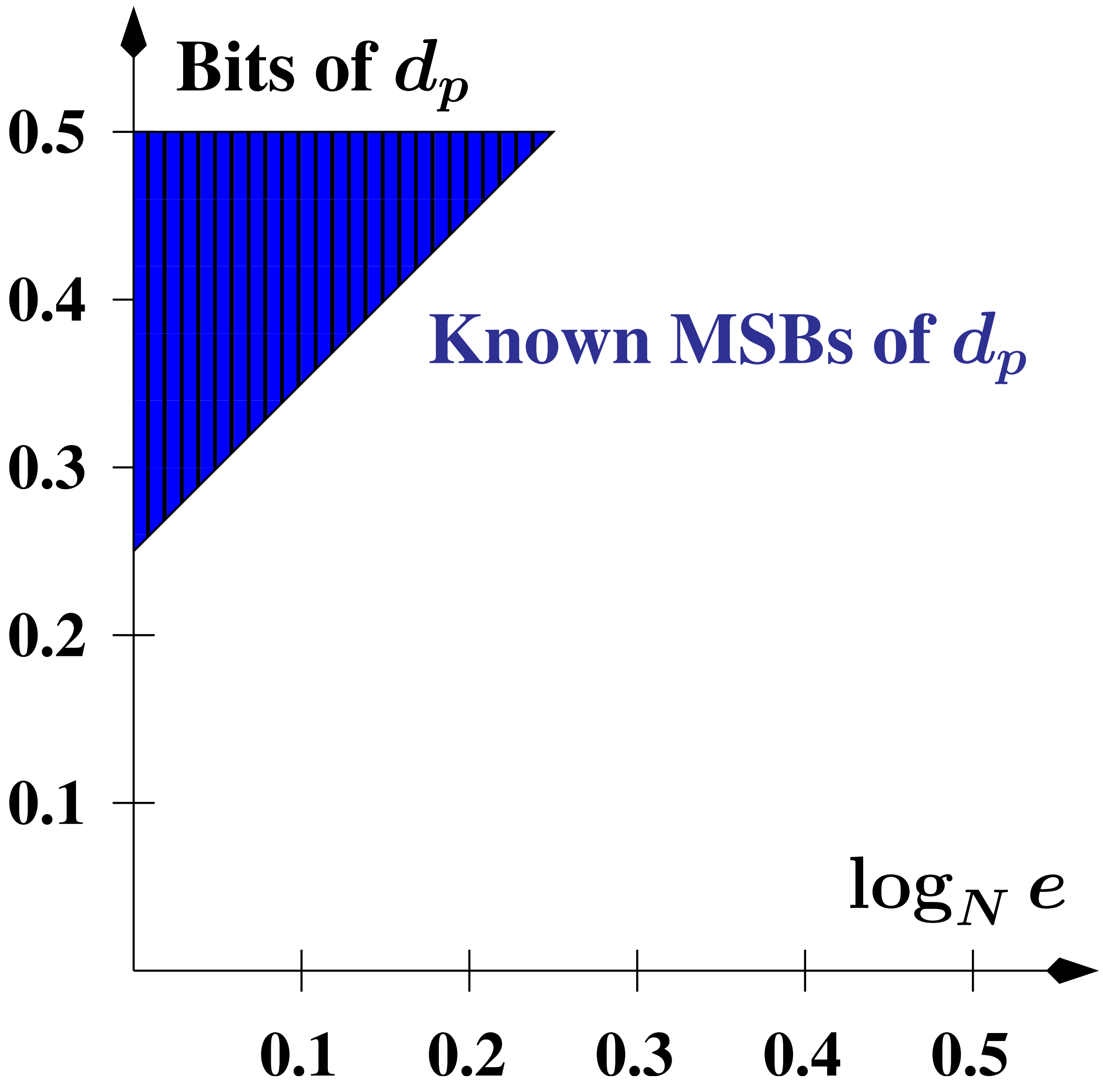
Result for MSBs of d_p

Theorem: *Let (N, e) be an RSA public key with secret key* d *and* $e = N^\alpha$ *for some* $\alpha \in [0, \frac{1}{4}]$. *Furthermore, let* $d_p = d \bmod p - 1$. *Suppose we are given* $\tilde{d}$ *with*

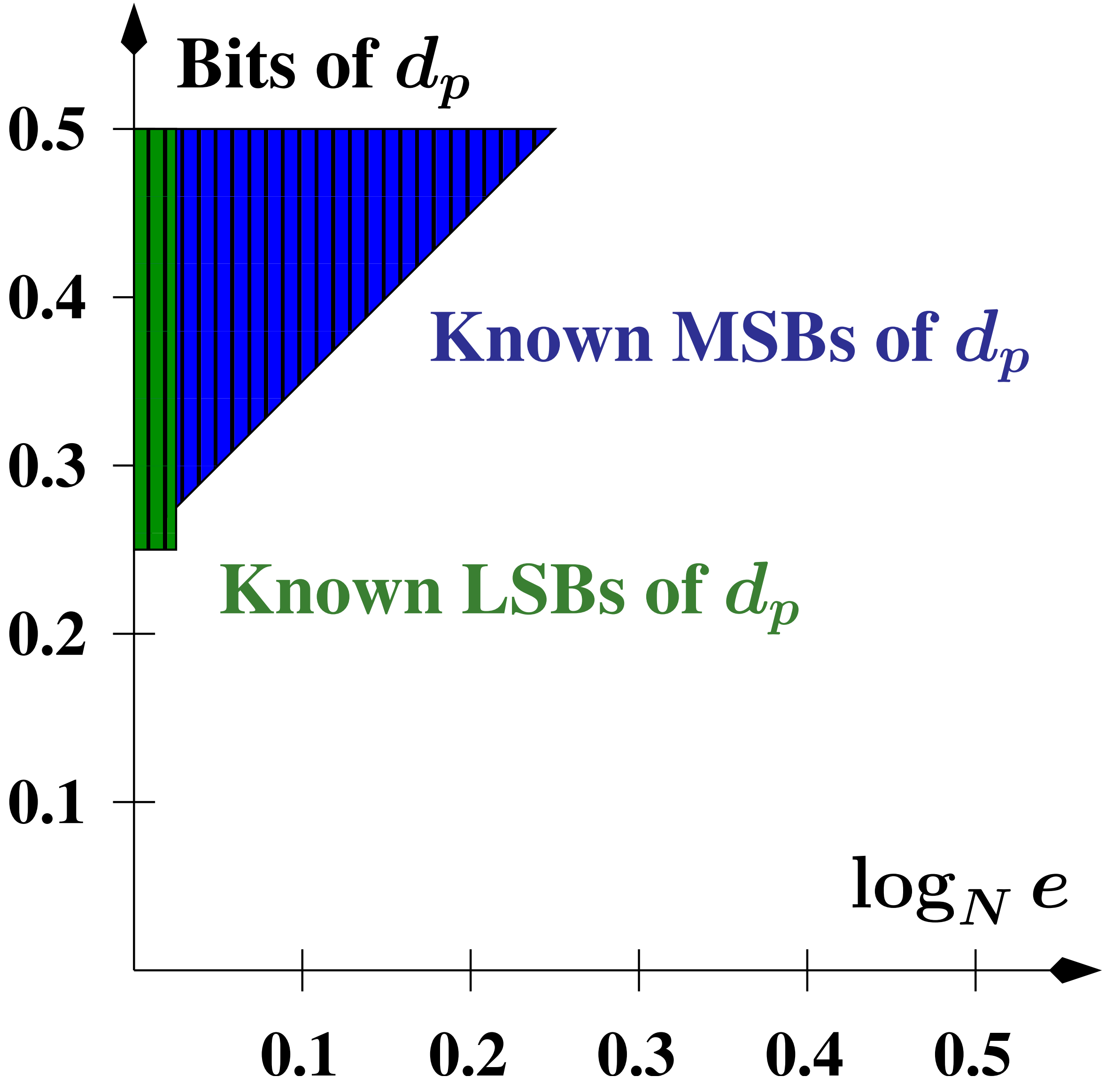
$$|d_p - \tilde{d}| \leq N^{\frac{1}{4} - \alpha}.$$

Then N *can be factored in polynomial time.*

Results for bits of d_p



Results for bits of d_p



Proof of the theorem

We know

$$ed_p - 1 = k(p-1)$$

with $k < e = N^\alpha$.

Compute $\tilde{kp} = e\tilde{d} - 1$. Then

$$\begin{aligned} |kp - \tilde{kp}| &= |e(d_p - \tilde{d}) + k| \\ &\leq N^{\frac{1}{4}} + N^\alpha \leq 2N^{\frac{1}{4}}. \end{aligned}$$

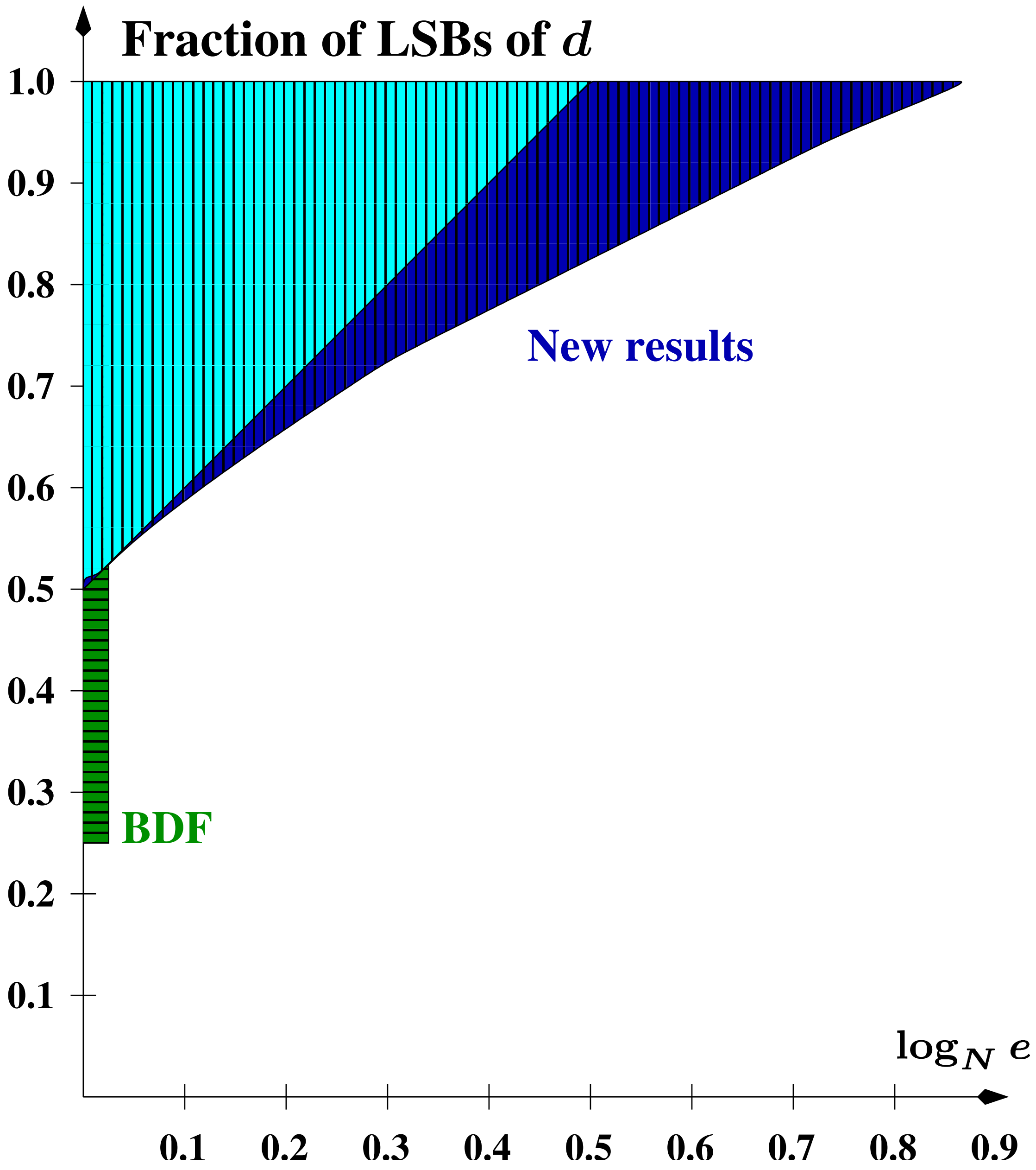
Results for LSBs of d

Heuristic: *Let* (N, e) *be an RSA public key with* $\alpha = \log_N(e) \le \frac{7}{8}$. *Let* d *be the secret key. Suppose we are given* d_0, M *satisfying* $d = d_0 \bmod M$ *with*

$$M \ge N^{\frac{1}{6}+\frac{1}{3}\sqrt{1+6\alpha}+\epsilon}.$$

Then N *can be factored in polynomial time.*

Known LSBs of d



The bivariate case

Theorem(Howgrave-Graham): *Let $f(x, y)$ be a polynomial that is a sum of at most ω monomials. Suppose that*

- $f(x_0, y_0) = 0 \bmod p^m$, *where* $|x_0| \leq X$, $|y_0| \leq Y$
- $\|f(xX, yY)\| < \frac{p^m}{\sqrt{\omega}}$.

Then $f(x_0, y_0) = 0$ *holds over the integers.*

The bivariate case

Theorem(Howgrave-Graham): *Let $f(x, y)$ be a polynomial that is a sum of at most ω monomials. Suppose that*

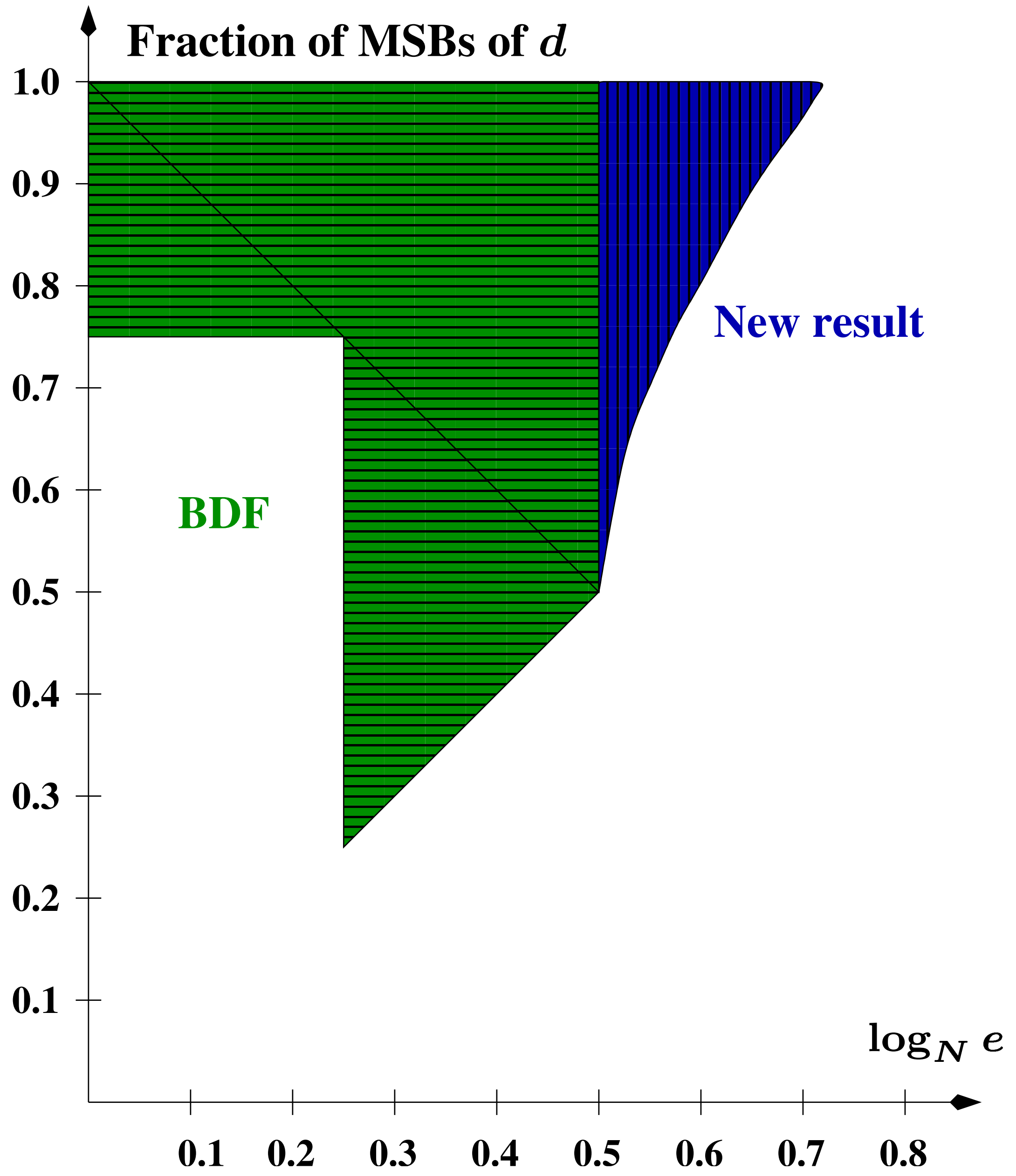
- $f(x_0, y_0) = 0 \bmod p^m$, *where* $|x_0| \leq X$, $|y_0| \leq Y$
- $\|f(xX, yY)\| < \frac{p^m}{\sqrt{\omega}}$.

Then $f(x_0, y_0) = 0$ *holds over the integers.*

Problem: How to find (x_0, y_0) ?

Heuristically: Construct two polynomials $f_1(x, y)$, $f_2(x, y)$ with root (x_0, y_0) and compute $\mathrm{Res}_y(f_1, f_2)$.

Known MSBs of d



RSA and Factoring

Easy:

Factoring $N \Rightarrow$ Computing the secret key d

Rivest, Shamir and Adleman (1978):

Computing $d \;\Rightarrow\;$ Factoring N in
probabilistic polynomial time

RSA and Factoring

Easy:

Factoring $N \Rightarrow$ Computing the secret key d

Rivest, Shamir and Adleman (1978):

Computing $d \;\Rightarrow\;$ Factoring N in probabilistic polynomial time

New result:

Computing $d \;\Leftrightarrow\;$ Factoring N in deterministic polynomial time (provided that $ed < N^2$)

Constructing the polynomial

Let us look at

$$ed = 1 + k(N - (p + q - 1)).$$

This can be written as

$$N - (p + q - 1) = \frac{ed - 1}{k}$$

Constructing the polynomial

Let us look at

$$ed = 1 + k(N - (p + q - 1)).$$

This can be written as

$$N - (p + q - 1) = \frac{ed - 1}{k}$$

We obtain an univariate polynomial

$$f(x) = -x + N$$

with the root $x_0 = p + q - 1 \leq N^{\frac{1}{2}}$ modulo $\frac{ed-1}{k}$.

Recall: The general theorem

Theorem: *Let*

- M *be a composite number of unknown factorization with divisor* $b \geq M^{\beta}$
- $f_b(x)$ *be a monic polynomial of degree* δ

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

$$f_b(x) = 0 \bmod b \quad \textit{with} \quad |x_0| \leq M^{\frac{\beta^2}{\delta}}$$

in time polynomial in $(\log M, \delta)$.

Recall: The general theorem

Theorem: *Let*

- M *be a composite number of unknown factorization with divisor* $b \geq M^{\beta}$
- $f_b(x)$ *be a monic polynomial of degree* δ

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

$$f_b(x) = 0 \bmod b \quad \textit{with} \quad |x_0| \leq M^{\frac{\beta^2}{\delta}}$$

in time polynomial in $(\log M, \delta)$.

- Let $M = ed - 1 = N^{\alpha}$, $\alpha \leq 2$.
  We have $b = \frac{ed-1}{k} \approx N$: $\beta = \frac{1}{\alpha}$ and $\delta = 1$.
- Therefore $x_0 = p + q - 1 \leq M^{\frac{\beta^2}{\delta}} = N^{\frac{1}{\alpha}}$.

Conclusions & Open Problems

- Coppersmith's method is very useful for cryptanalysis
- Interestingly, it has also been applied to prove the security of schemes.
- How can we make the multivariate approach rigorous?
- Are there further applications/improvements?