CRYPTANALYSIS OF RSA WITH CONSTRAINED KEYS

Abderrahmane Nitaj

Univeristé de Caen, France

September 30, 2005

Outline

- The RSA cryptosystem
- The continued fractions
- Lattices
- Coppersmith’s methods
- Former attacks
- Constrained keys
- The new attack
- Conclusion

RSA Cryptosystem (1978)

- The modulus : $n = pq$, with p and q primes.
- Euler's totient function : $\phi(n) = (p-1)(q-1)$.
- The keys :
  - The public key : e with $\gcd(e, \phi(n) = 1$.
  - The secret key : d inverse of e mod $\phi(n)$.
- Encryption :
  - Plaintext : M with $1 < M < n$.
  - Cyphertext : $C \equiv M^e \pmod{n}$.
- Decryption : Plaintext : $M \equiv C^d \pmod{n}$.

RSA Cryptosystem (1978)

- The modulus : $n = pq$, with p and q primes.
- Euler's totient function : $\phi(n) = (p-1)(q-1)$.
- Public : n, e, C.
- Private : p, q, $\phi(n)$, e, M.
- Equation :

$ed - k\phi(n) = 1$ with unknowns d, k, $\phi(n)$.

The continued fractions

- Setup :
  - $n \in \mathbb{N}$.
  - $e \in \mathbb{N}, \qquad e < n$.
- The problem : find
  - $a \in \mathbb{N}$.
  - $b \in \mathbb{N}$.
  - $\frac{a}{b} \approx \frac{e}{n}$.

The continued fractions

- The Euclid algorithm.
- The continued fraction algorithm.
  - $$\frac{e}{n} = [a_0, a_1, \cdots, a_s] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_s}}}.$$
  - $a =$Numerator$([a_0, a_1, \cdots, a_i])$.
  - $b =$Denominator$([a_0, a_1, \cdots, a_i])$.
- $\frac{a}{b}$ is a convergent of $\frac{e}{n}$.

Legendre's Theorem

- Setup :
  - $n \in \mathbb{N}$.
  - $e \in \mathbb{N}, \qquad e < n$.
  - $a, b \in \mathbb{N}$.
- The problem : Is $\frac{a}{b}$ a convergent of $\frac{e}{n}$?
- Theorem : If $\left|\frac{a}{b} - \frac{e}{n}\right| < \frac{1}{2b^2}$, then $\frac{a}{b}$ is a convergent of $\frac{e}{n}$.

Lattices

- Setup:
  - $v_1, v_2, \cdots v_m \in \mathbb{R}^l, \quad l \geq m$, linearly independents.
  - $L = \mathbb{Z}.v_1 \oplus \mathbb{Z}.v_2 \oplus \cdots \oplus \mathbb{Z}.v_m$.
- Properties:
  - $\dim(L) = m$.
  - $\det(L) = \prod_{i=1}^{m} ||v_i^*||$ (via Gram-Schmidt orthogonalization).

Minkowski's Theorem

- Setup:
  - $v_1, v_2, \cdots v_m \in \mathbb{R}^l, \quad l \geq m$, linearly independents.
  - $L = \mathbb{Z}.v_1 \oplus \mathbb{Z}.v_2 \oplus \cdots \oplus \mathbb{Z}.v_m$.
- The problem: Find a short vector.
- Minkowski's Theorem: $\exists v \in L$ such that $||v|| \leq \sqrt{m}\ \det(L)^{\frac{1}{m}}$.

The LLL algorithm

- Setup: $L = \mathbb{Z}.v_1 \oplus \mathbb{Z}.v_2 \oplus \cdots \oplus \mathbb{Z}.v_m$.
- The problem: Find a short vector.
- The LLL algorithm :
  - Transforms the basis $(v_1, v_2, \cdots v_m)$ into a reduced basis $(v'_1, v'_2, \cdots v'_m)$.
  - Finds a vector v with $||v|| \leq 2^{\frac{m-1}{4}} \det(L)^{\frac{1}{m}}$.
  - In polynomial time in m.

Coppersmith's Theorem

- Setup:
  - $n = pq$.
  - $\tilde{p}$, such that $|p - \tilde{p}| \leq n^{\frac{1}{4}}$.
- Goal: Find p and q.
- Coppersmith's Theorem: If $|p - \tilde{p}| \leq n^{\frac{1}{4}}$, then n can be factored in polynomial time.
  - Finds p et q.
  - Polynomial time in $\log(n)$.

May's extension

- Setup:
  - $n = pq$.
  - $\tilde{P}$, such that $|pu - \tilde{P}| \leq n^{\frac{1}{4}}$.
- Goal: Find p and q.
- May's extension: If $\left|pu - \tilde{P}\right| \leq n^{\frac{1}{4}}$ with $u \not\equiv 0 \pmod{q}$, then n can be factored.
  - Use Coppersmith's Theorem to find pu.
  - Compute $p = \gcd(pu, n)$.
  - Polynomial time in $\log(n)$.

Wiener's attack

Based on $\phi(n) \approx n$ + continued fractions.

- Setup:
  - $n = pq$.
  - e with $(e < n)$.
  - The equation : $ed - k\phi(n) = 1$.
- Goal: Find d, $k \Longrightarrow \phi(n)$, p, q.
- Wiener's Theorem (1990): If $d < \frac{1}{3}n^{\frac{1}{4}}$, then $\frac{k}{d}$ is a convergent of $\frac{e}{n}$.

The Boneh-Durfee attack

Based on $\phi(n) = n + 1 - (p + q)$ + lattice reduction

- Setup:
  - $n = pq$.
  - e with $(e < n)$.
  - The equation: $ed - k\phi(n) = 1$.
- Goal: Find d, $k \Longrightarrow \phi(n)$, p, q.
- Boneh-Durfee Theorem (1999): If $d < n^{0.292}$, then n can be factored in polynomial time.

Extension attacks

Based on $\phi(n) \approx n \approx n + 1 - 2\sqrt{n}$.

- The equation: $ed - k\phi(n) = 1$.

- Verheul-Van Tilborg (1997) + Dujella (2003): If $d < n^{\frac{1}{4}+\frac{\gamma}{2}}$, then $\frac{k}{d}$ is computable from a convergent of $\frac{e}{n}$.

- de Weger's Theorem (2002): If $d < \frac{n^{\frac{3}{4}}}{|p-q|}$, then $\frac{k}{d}$ is a convergent of $\frac{e}{n+1-2\sqrt{n}}$.

The Blömer-May attack

$\phi(n) \approx n$+Continued fraction + Lattice reduction.

- Setup:
  - $n = pq$, with $(q < p < 2q)$.
  - e, $(e < n)$.
  - The equation $ex + y = k\phi(n)$.
- Goal: Find x, $k \Longrightarrow p$, q.
- Blömer-May Theorem (2004): If $0 < x \leq \frac{1}{3}n^{\frac{1}{4}}$ and $|y| \leq n^{-\frac{3}{4}}ex$, then n can be factored in polynomial time.

The notion of constrained keys (1/2)

- Setup:
  - $e < n = pq$, with $q < p < 2q$.
  - A function F satisfying :
    - (1) $\exists u \in \mathbb{Z},\ F(u) \approx n$.
    - (2) pu or qu is computable from $F(u)$.

- Examples: For a fixed $u_0 \in \mathbb{Q}$.
  - $F(u) = p(q-u)$.
  - $F(u) = \left(p - \frac{u_0}{u}\right)(q-u)$. This includes $\phi(n) = (p-1)(q-1)$.

The notion of constrained keys (2/2)

- (1) $\exists u \in \mathbb{Z},\ F(u) \approx n$.
- (2) pu or qu is computable from $F(u)$.
- Definitions:
  - *Let F be a function satisfying (1) and (2). The public key e is F-constrained if there exist $u \in \mathbb{Z}, X, Y \in \mathbb{N}$ with $\gcd(X, Y) = 1$ such that Y and $|eY - F(u)X|$ are suitably small.*
  - *A public key e is constrained if there exist a function F satisfying (1) and (2) for which e is F-constrained.*

The new attack (1/2)

- Setup:
  - $n = pq$, with $(q < p < 2q)$.
  - e, $(e < n)$.
  - A function F:
    - (1) $\exists u \in \mathbb{Z}$, $F(u) \approx n$.
    - (2) pu or is qu computable from $F(u)$.
- Goal:
  - Find p, q.
  - Equation: $eY - XF(u) = Z$, in X, Y, u, Z.

The new attack (2/2)

- Equation: $eY - XF(u) = Z$, in X, Y, u, Z.
- (1) $\exists u \in \mathbb{Z}$, $F(u) \approx n$.
- (2) pu or pu is computable from $F(u)$.
- The idea
  - $\frac{X}{Y} \approx \frac{e}{F(u)}$.
  - $F(u) \approx n \Longrightarrow \frac{X}{Y}$ is a convergent of $\frac{e}{n}$.
  - $F(u) \approx \frac{eY}{X} \Longrightarrow$ approximation of pu or qu

    $\Longrightarrow$ Coppersmith-LLL-May $\Longrightarrow$ p or q.

Main result: $F_1(u) = p(q-u)$

- Equation: $eY - XF_1(u) = Z$ in X, Y, u, Z.
- Theorem:
  - $n = pq$ with $q < p$.
  - $u \in \mathbb{Z}$ with $1 \leq |u| \leq q - 1$.
  - $p|u| = n^{\frac{1}{2}+\alpha}$.

    If $Y < \frac{1}{2} n^{\frac{1}{4}-\frac{\alpha}{2}} \left(\frac{F_1(u)}{e} \right)^{\frac{1}{2}}$,

    $$|Z| \leq \frac{2n^{\frac{1}{4}} \left(1 - n^{\alpha-\frac{1}{2}}\right) eY}{F_1(u)}$$

    then n can be factored in plynomial time.

The proof: $F_1(u) = p(q-u)$ (1/2)

- Equation: $eY - XF_1(u) = Z$ in X, Y, u, Z.
  - $u \in \mathbb{Z}$ with $1 \leq |u| \leq q-1$.
  - $p|u| = n^{\frac{1}{2}+\alpha}$
  - $Y < \frac{1}{2} n^{\frac{1}{4}-\frac{\alpha}{2}} \left(\frac{F_1(u)}{e}\right)^{\frac{1}{2}}$.
  - $|Z| \leq \frac{2n^{\frac{1}{4}} \left(1 - n^{\alpha-\frac{1}{2}}\right) eY}{F_1(u)}$.

The proof: $F_1(u) = p(q-u)$ (2/2)

- Concept of the proof
  - Compute X and Y via the continued fraction expansion of $\frac{e}{n}$.
  - Write $pu = n - \frac{eY}{X} + \frac{Z}{X}$.
  - Compute $\tilde{P} = n - \frac{eY}{X}$.
  - Then $\left|\tilde{P} - pu\right| \leq 2n^{\frac{1}{4}}$.
  - Apply Coppersmith's method to find pu.
  - Compute $p = \gcd(n, pu)$.

The number of $F_1(u)$-constrained keys: $F_1(u) = p(q-u)$

- Equation: $eY - XF_1(u) = Z$ in X, Y, u, Z.
  - $u \in \mathbb{Z}$ with $1 \leq |u| \leq q-1$.
  - $p|u| = n^{\frac{1}{2}+\alpha}$
  - $1 \leq X \leq Y < \frac{1}{2} n^{\frac{1}{4}-\frac{\alpha}{2}}$.
  - $e = \left\lfloor F_1(u)\frac{X}{Y} \right\rfloor + h$ with $\gcd(e, \phi(n)) = 1$.
- Theorem: There are at least $O\left(n^{\frac{3}{4}-\alpha-\varepsilon}\right)$ $F_1(u)$-constrained keys.

The number of F_1-constrained keys: $F_1(u) = p(q-u)$

- Theorem: There are at least $O\left(n^{\frac{3}{4}-\varepsilon}\right)$ F_1-constrained keys.

- Concept of the proof:
  - All $u \in \mathbb{Z}$ with $1 \leq |u| \leq q-1$.
  - $p|u| = n^{\frac{1}{2}+\alpha}$
  - $1 \leq X \leq Y < \frac{1}{2} n^{\frac{1}{4}-\frac{\alpha}{2}}$.
  - $e = \left\lfloor F_1(u)\frac{X}{Y} \right\rfloor + h$ with $\gcd(e, \phi(n)) = 1$.

Example: $F_1(u) = p(q-u)$

- Setup:
  - $n = pq = 941096252089784462564816358 28/331078768267327552 3 \approx 2^{159} \approx 10^{48}$.
  - $e = 847441242103359735969302036883 1/503313484314327 \approx n^{0.95}$.
- Result:
  - The 12th convergent $\frac{X}{Y} = \frac{36482}{4051381}$.
  - Coppersmith-LLL-May with $\tilde{P} = n - \frac{eY}{X}$.
  - $p = 132111069327034363307377 7$.

Analysis of the example

- $q = \frac{n}{p} = 712352308465649934350899.$
- $d = e^{-1} \pmod{\phi(n)} \approx n^{0.97}.$
- Failure of the attacks
  - Wiener+Verheul-Tilborg+Dujella: $d \gg n^{\frac{1}{4}}$.
  - de Weger: $d \gg \frac{n^{\frac{3}{4}}}{p-q}$.
  - Boneh-Durfee: $d \gg n^{0.292}$.
  - Blömer-May: For all convergents $\frac{k}{x}$ of $\frac{e}{n}$, $|ex - k\phi(n)| \gg exn^{-\frac{3}{4}}$.

Conclusion (1/2)

- Techniques for cryptanalysis
  - The continued fraction algorithm
  - Coppersmith's lattice reduction
- Constrained keys
  - Wiener: $d < \frac{1}{3}n^{\frac{1}{4}}$. Constrained with $\phi(n)$.
  - de Weger: $d < \frac{n^{\frac{3}{4}}}{|p-q|}$. Constrained with $\phi(n)$.
  - Boneh-Durfee: $d < n^{0.292}$. Constrained with $\phi(n)$.

Conclusion (2/2)

- Constrained keys
  - Blömer-May: $d \equiv \frac{x}{y}$ with small x and y. Constrained with $\phi(n)$.
  - The new attack: $eY - XF(u) = Z$ with small X, Y and Z. Constrained with $F(u)$.
  - There are at least $O\left(n^{\frac{3}{4}-\varepsilon}\right)$ F_1-constrained keys.