Revisiting Wiener's Attack - New Weak Keys in RSA

Santanu Sarkar
in collaboration with Dr. Subhamoy Maitra

Indian Statistical Institute, Kolkata
subho@isical.ac.in

- Pick two large primes p and q. In general $q < p < 2q$.
- Calculate $N = pq$, $\phi(N) = (p-1)(q-1)$.
- Find e relatively prime to $\phi(N)$.
- Find (using extended Euclidean algorithm) d such that $ed = 1 \bmod \phi(N)$.
- $< e, N >$ is the public key and d is the private (secret) key, $p, q, \phi(N)$ are also kept secret.
- Encryption: $C = M^e \bmod N$, Decryption: $M = C^d \bmod N$.
- Encryption and decryption are the same operation, but the exponent is different.

Example from Wiki

- Take $p = 61$, $q = 53$.
- So, $N = pq = 3233$, $\phi(N) = (p-1)(q-1) = 3120$
- Choose $e > 1$ coprime to 3120, e.g., $e = 17$.
- This gives $d = 2753$. Check
  $17 \cdot 2753 = 46801 = 1 + 15 \cdot 3120$.
- Public key: $< 17, 3233 >$, Private key: 2753
  $61, 53, 3120$ are kept secret.
- Message $M = 123$. Encryption:
  $C = 123^{17} \bmod 3233 = 855$.
- Decryption: $M = 855^{2753} \bmod 3233 = 123$.

RSA Hardness: Based on two problems

- Factoring large integers: if p, q are known, then $\phi(N)$ is known, so d will be known immediately.
  Also if $\phi(N)$ is known, then $(p-1)(q-1) = N - (p+q) + 1$ is known, so $(p+q)$ is known. Since $N = pq$ is known, $(p-q)$ will be known immediately and hence, p, q.
- RSA Problem: It is known that $C = M^e \bmod N$, and both e, N are known. If one can compute e-th root of C modulo N then M will be known immediately.

As of 2005, the largest number factored by general-purpose methods was 663 bits long, using state-of-the-art distributed methods.

Factorization: Time Complexity

The subexponential factorization algorithms, e.g., quadratic sieve, elliptic curve and number field sieve have the time complexities $O\left(exp((1+o(1))\sqrt{\ln N \ln\ln N})\right)$, $O\left(exp((1+o(1))\sqrt{2\ln p \ln\ln p})\right)$, $O\left(exp((1.92+o(1))(\ln N)^{\frac{1}{3}}(\ln\ln N)^{\frac{2}{3}})\right)$ respectively. Since we are considering the primes of the same bit size, the elliptic curve method will not be efficient.

N	$exp((1+o(1))\sqrt{\ln N \ln\ln N})$	$exp((1.92+o(1))(\ln N)^{\frac{1}{3}}(\ln\ln N)^{\frac{2}{3}})$
2^{256}	$2^{43.7}$	$2^{46.6}$
2^{384}	$2^{55.7}$	$2^{56.1}$
2^{512}	$2^{65.9}$	$2^{63.8}$
2^{768}	$2^{83.4}$	$2^{76.4}$
2^{1024}	$2^{98.5}$	$2^{86.6}$

Continued Fraction

- Given a positive rational number $\frac{a}{b}$, a finite Continued Fraction expression of $\frac{a}{b}$ can be written as $q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_m}}}$ or in short $[q_1, q_2, q_3, \ldots q_m]$.
- **Example:** $\frac{34}{99} = 0 + \frac{1}{\frac{99}{34}} = 0 + \cfrac{1}{2 + \frac{31}{34}} = 0 + \cfrac{1}{2 + \cfrac{1}{\frac{34}{31}}} = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{3}{31}}} = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\frac{31}{3}}}} = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{10 + \frac{1}{3}}}}$, and in short $[0, 2, 1, 10, 3]$.

Convergents of a continued fraction

Convergents of a continued fraction expansion of $\frac{a}{b}$:

- Any initial subsequence of $[q_1, q_2, q_3, \ldots q_m]$ is called convergent of continued fraction expansion of $\frac{a}{b}$.
- In above example $[0, 2, 1]$ is one of the subsequence of $[0, 2, 1, 10, 3]$. Note $0 + \frac{1}{2+\frac{1}{1}} = \frac{1}{3}$, close to $\frac{34}{99}$.

Theorem on Continued Fraction(Dirichlet 1842)

Let e, N, t, d are +ve integers with

- $\gcd(e, N) = 1$
- $\gcd(t, d) = 1$ and
- $|\frac{e}{N} - \frac{t}{d}| < \frac{1}{2d^2}$.

Then $\frac{t}{d}$ is one of the convergents of continued fraction expansion of $\frac{e}{N}$.

RSA and Continued Fraction

- RSA equation $ed = 1 + t\phi(N)$
- One may write this equation as $\frac{e}{\phi(N)} - \frac{t}{d} = \frac{1}{d\phi(N)}$
- $|\frac{e}{\phi(N)} - \frac{t}{d}| < \frac{1}{2d^2}$ is satisfied when $2d < \phi(N)$, but $\phi(N)$ is not public.
- We need to get an approximation of $\phi(N)$ for cryptanalysis.

Wiener's attack: IEEE-IT 1990

- Consider N (publicly available) as an approximation of $\phi(N)$.
- $|\frac{e}{N} - \frac{t}{d}| < \frac{1}{2d^2}$, when $d \leq \frac{1}{3}N^{\frac{1}{4}}$.
- In this case $\frac{t}{d}$ will be known, so $\phi(N) = \frac{ed-1}{t}$ will be known and hence p, q.

Wiener's attack (example)

- Consider $N = 160523347$ and $e = 60728973$.
- The continued fraction expansion of $\frac{e}{N}$ is as follows: $[0, 2, 1, 1, 1, 4, 12, 102, 1, 1, 2, 3, 2, 2, 36]$.
- Few convergents of $\frac{e}{N}$ are $0, \frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{3}{8}, \frac{14}{37}, \ldots$.
- Take each of them and try.
- As example, $\frac{t}{d} = \frac{1}{2}$, then $\phi(N) = \frac{ed-1}{t} = 60728973 * 2 - 1 = 121457945$ which gives $p = \frac{39065403}{2} - \frac{\sqrt{1526105069459021}}{2}$, which is not correct.

Wiener's attack (example)

- Proceeding in this way, consider $\frac{t}{d} = \frac{14}{37}$.
- Then $\phi(N) = \frac{ed-1}{t} = \frac{60728973*37-1}{14} = 160498000$.
- This gives, $p = 12347, q = \frac{N}{p} = 13001$.

Extension of Wiener's attack (de Weger, AAECC 2002)

- Generally primes of same bit lengths are considered, i.e., $q < p < 2q$.
- This gives, $N - \frac{3}{\sqrt{2}}\sqrt{N} + 1 < \phi(N) < N - 2\sqrt{N} + 1$.
- In Wiener's attack $\phi(N)$ is replaced by N, de Weger improved the result considering $N - 2\sqrt{N} + 1$ as an approximation of $\phi(N)$ and studying the CF expression of $\frac{e}{N-2\sqrt{N}+1}$. This approximation works better when p and q are close.
- We replace$\phi(N)$ by $N - \frac{3}{\sqrt{2}}\sqrt{N} + 1$ to get better result when p and $2q$ are close.

Our Contribution

Our first result:

l positive integer, $q > \frac{2l+2}{4l+1}p$, $2q - p = N^{\gamma}$ and $d = N^{\delta}$. One can factor N in polynomial time provided

$$\delta < \frac{3}{4} - \gamma - \tau,$$

where $2\tau > (\log \frac{4l}{\frac{3}{\sqrt{2}}+2})\frac{1}{\log N}$.

- Compute t and d via continued fraction of $\frac{e}{N+1-\frac{3}{\sqrt{2}}\sqrt{N}}$ in this case.
- Note when $2q - p$ is bounded then the limit of d beyond $N^{0.3}$.

Our second result:

N can be factored when $d < \frac{1}{2}N^{\delta}$ and e is $O(N^{\frac{3}{2}-2\delta})$ for $\delta \leq \frac{1}{2}$

- Compute t and d via continued fraction of $\frac{e}{N+1-\frac{3}{\sqrt{2}}\sqrt{N}}$.
- We remove the constraint on the difference between the primes.
- Instead an upper bound on e is considered.

Coppersmith's Theorem: Eurocrypt 1996

Let

- N be a composite number of unknown factorization with divisor $p \geq N^{\beta}$,
- $f_p(x)$ be a monic polynomial of degree s (x^s has coefficient 1).

Then one can find all solutions x_0 for the equation $f_p(x) = 0 \bmod p$ with $|x_0| \leq N^{\frac{\beta^2}{s}}$ in time polynomial in $(\log N, s)$. The proof requires the application of LLL algorithm.

Factoring with high bits known

Let $N = pq$ with $q < p < 2q$. Suppose we know an integer P with $|p - P| \leq N^{\frac{1}{4}}$. Then N can be factored in polynomial time using previous theorem.

Weak Keys

- The ideas of Wiener (CF based) and Coppersmith (LLL based) have been exploited together to find weak keys of RSA.
- (Blömer and May, PKC 2004) The primes p, q can be found in polynomial time for every N, e satisfying $ex + y = 0 \bmod \phi(N)$, with $0 < x \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{p-q}$ and $|y| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$.

Our Result

Let l be a positive integer such that $l > \frac{2(\frac{3}{\sqrt{2}}+2)}{\frac{3}{\sqrt{2}}-2\epsilon}$, where $\epsilon > \frac{2q-p}{\phi(N)N^{\frac{1}{4}}}$. Let $q > \frac{2l+2}{4l+1}p$. Suppose e satisfies the equation $ex + y = k\phi(N)$, for $k > 0$. Then N can be factored in $O(poly(\log(N)))$ time when $0 < x \leq \sqrt{\frac{3}{4l}}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{2q-p}$ and $|y| \leq \frac{2q-p}{\phi(N)N^{\frac{1}{4}}}ex$.

proof:

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

- Compute x and k by continued fraction of $\frac{e}{N-\frac{3}{\sqrt{2}}\sqrt{N}+1}$
- Compute an approximation of $p + q$:

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

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

$$| y | = O(N^{\gamma-\frac{5}{4}}ex)$$

Proof

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

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

- Find an approximation of p with error $O(N^{\frac{1}{4}})$.
- **Coppersmith's result:** Suppose we are given an approximation p with an error $O(N^{\frac{1}{4}})$.Then N can be factored in polynomial time.
- The number of such e is $\Omega(N^{\frac{3}{4}-\varepsilon})$.

Thank You