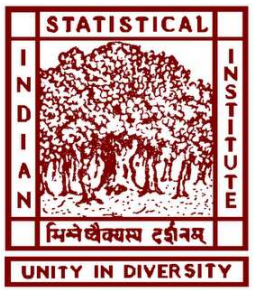
Partial Key Exposure: Generalized Framework to Attack RSA

Santanu Sarkar

Cryptology Research Group
Indian Statistical Institute, Kolkata



12 December 2011

Outline of the Talk

1. RSA - A brief overview
2. Partial Key Exposure attacks on RSA and Factorization
3. Our Work on partial key exposure attack
4. ISO/IEC 9796-2 standard signature scheme
5. Analysis of ISO/IEC 9796-2 standard signature scheme

RSA Public Key Cryptosystem

- Invented by Rivest, Shamir and Adleman in 1977
- Most popular public key cryptosystem
- Used in various Electronic commerce protocols

RSA in a Nutshell

Key Generation

- Choose *big* primes p, q at random
  (generally the primes are considered to be of same bit size)
- Compute RSA modulus $N = pq$, and $\phi(N) = (p-1)(q-1)$
- Find a pair e, d such that $ed = 1 + k\phi(N)$ with $k \geq 1$
- Publish $\langle N, e \rangle$ and keep d private

Encryption: $C \equiv M^e \bmod N$ Decryption: $M \equiv C^d \bmod N$

Partial Key Exposure Attacks

- In Crypto 1996, Kocher proposed timing attack on RSA.
- Given

$$d = \overbrace{10010101\ldots001010}^{t=?}\ldots\ldots\ldots\ldots 010010101001001,$$

find the bound on t such that

"knowing t bits of d yields the factors of N".

Partial Key Exposure

PRINCIPLE:

The fault does not lie in the RSA algorithm, but may reside within its implementation!

Currently known techniques:

- Timing attacks
- Power monitoring attacks
- TEMPEST (or radiation monitoring) attacks
- Acoustic cryptanalysis
- Differential fault analysis
- Observation, Sneaking, Reflection attacks

Factorization: Existing Results

Rivest and Shamir (Eurocrypt 1985)

N can be factored given 2/3 of the LSBs of a prime

$$1001010100\overbrace{10100100101010010011}$$

Coppersmith (Eurocrypt 1996)

N can be factored given 1/2 of the MSBs of a prime

$$\overbrace{100101010010100}100101010010011$$

Boneh et al. (Asiacrypt 1998)

N can be factored given 1/2 of the LSBs of a prime

$$100101010010100\overbrace{100101010010011}$$

Herrmann and May (Asiacrypt 2008)

N can be factored given a random subset of the bits (small contiguous blocks) in one of the primes

$$100\overbrace{1010100}10100\overbrace{1001010100}10011$$

Partial Key Exposure Attacks on RSA

- Boneh et al (Asiacrypt 1998) studied how many bits of d need to be known to factor the RSA modulus N.
  [The constraint in the work of Boneh et al was $e < \sqrt{N}$]

- In Crypto 2003, Blömer and May improved the bound:

$$e < N^{0.725}$$

- Ernst et al (Eurocrypt 2005) further improved the bound:

$$e \text{ may be of size } O(N)$$

Question

What if few contiguous blocks of the d are unknown?

$$d = 1001\ldots01\overbrace{1001101\ldots1010}^{t_1=?}10\ldots\ldots\ldots\ldots01001\overbrace{0101\ldots1001}^{t_2}$$

Our first result

Theorem

Let e be $O(N)$ and $d \leq N^{\delta}$. Suppose the bits of d are exposed except n many blocks, each of size $\gamma_i \log N$ bits for $1 \leq i \leq n$. Then one can factor N in polynomial in $\log N$ but exponential in n time if

$$\sum_{i=1}^{n} \gamma_i < 1 - \frac{1}{2(n+2)} - \frac{n+1}{2(n+2)} \sqrt{4\delta + 1 + \frac{4\delta}{n+1}}.$$

Idea of the proof

- d is unknown for n many blocks
- One can write $d = a_0 + a_1 y_1 + \ldots + a_n y_n$, where $y_1, y_2, \ldots, y_n$ are unknown
- $ed = 1 + k(N + 1 - p - q)$
- $ea_0 + ea_1 y_1 + \ldots + ea_n y_n - 1 - k(N + 1 - p - q) = 0$
- We are interested to find the root of the polynomial $f(x_1, \ldots, x_{n+1}, x_{n+2}) = ea_0 + ea_1 x_1 + \ldots + ea_n x_n - 1 + N x_{n+1} + x_{n+1} x_{n+2}$.
- $f(y_1, \ldots, y_n, -k, 1 - p - q) = 0$

Numerical value

δ	$n = 1$	$n = 2$	$n = 3$	$n = 4$
0.30	0.275	0.270	0.267	0.266
0.35	0.246	0.240	0.237	0.234
0.40	0.219	0.211	0.207	0.205
0.45	0.192	0.183	0.179	0.176
0.50	0.167	0.157	0.152	0.148
0.55	0.142	0.131	0.125	0.122
0.60	0.118	0.106	0.100	0.096
0.65	0.095	0.082	0.075	0.071
0.70	0.073	0.059	0.051	0.047
0.75	0.051	0.036	0.028	0.023
0.80	0.030	0.014	0.005	0.000

Table: Numerical upper bound of unknown bits of d for different n.

Asymptotic Case

Lemma

Let e be full bit size and $d \leq N^{\delta}$ with $\delta < 0.75$. Then knowledge of

$$\left(\delta + \frac{\sqrt{1+4\delta}}{2} - 1\right) \log N$$

many bits of d is sufficient to factor N in time polynomial in $\log N$ and exponential in number of unknown blocks of d.

Asymptotic Case

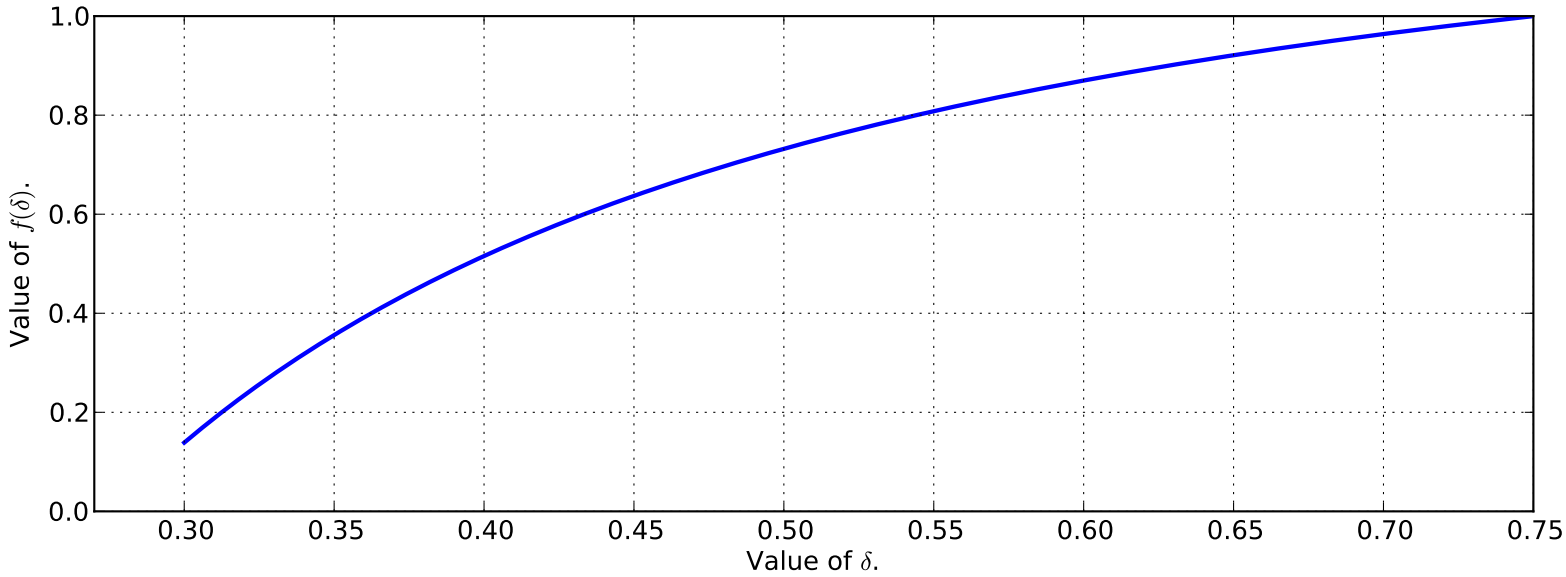


Figure: Partial Key Exposure Attack for d. Plot of $f(\delta) = 1 + \frac{\sqrt{1+4\delta}}{2\delta} - \frac{1}{\delta}$ vs. values of δ.

Experimental Results

n	δ	$\sum_{i=1}^{n} \gamma_i$	LD	Time (Sec.)
2	0.30	0.200	55	99.69
2	0.35	0.145	55	107.94
2	0.40	0.095	55	114.12
2	0.45	0.060	55	122.82
2	0.50	0.045	55	114.23
2	0.55	0.010	55	99.68
3	0.30	0.195	91	911.31
3	0.35	0.140	91	901.11
3	0.40	0.090	91	1002.15
3	0.45	0.040	91	914.22

Table: Experimental results for $n = 2$ and $n = 3$ with 1024 bit N.

Partial information of k

- When d_0 known,

$$ed = 1 + k(N + 1 - p - q) \text{ and } d = d_0 + d_1$$

- We can estimate for k as:

$$k_0 = \lfloor \frac{ed_0 - 1}{N} \rfloor$$

- Accuracy: If $|d - d_0| < N^{\gamma}$, we will have

$$|k - k_0| < 4N^{\lambda}$$

where $\lambda = \max\{\gamma, \delta - \frac{1}{2}\}$.

- We use partial information of k in our second result

Numerical values

$\lambda = 0.25$

δ	γ_1	$\sum_{i=1}^{2} \gamma_i$	$\sum_{i=1}^{3} \gamma_i$
0.30	0.1424	0.1408	0.1400
0.40	0.1424	0.1408	0.1400
0.60	0.1424	0.1408	0.1400
0.75	0.1424	0.1408	0.1400
0.80	0.1101	0.1092	0.1087
0.85	0.802	0.0797	0.0794
0.90	0.0521	0.0519	0.0518
0.95	0.0255	0.0254	0.0254

Table: Numerical upper bound of unknown bits of d for different n using the partial knowledge of k.

Signature scheme: CRT-RSA

- CRT-RSA is used to devise one of the most popular digital signature schemes
  1. $s_p = m^{d_p} \bmod p$
  2. $s_q = m^{d_q} \bmod q$
- Signature s can be computed using CRT with s_p and s_q
- Fault in $s_q \Rightarrow \gcd(s^e - m, N) = p$

ISO/IEC 9796-2 signature scheme

- Encoded message: $\mu(m) = 6A_{16} \,||\, m[1] \,||\, H(m) \,||\, BC_{16}$, where $m = m[1] \,||\, m[2]$ is split into two parts, $m[2]$ is data
- Signature: $\left(\mu(m)^d \bmod N, m[2]\right)$
- Faulty signatures s such that
  1. $s^e = \mu(m) \mod p$
  2. $s^e \neq \mu(m) \mod q$
- Coron et al. (CHES 2010): Unknown part is small, one can factor N
- They also consider two faulty signatures occur for two different primes

Our Result: Two faulty signature

- Two faulty signatures s_1, s_2 such that
  1. $s_1^e = \mu(m_1) \mod p$ and $s_1^e \neq \mu(m_1) \mod q$
  2. $s_2^e \neq \mu(m_2) \mod p$ and $s_2^e = \mu(m_2) \mod q$
- We get the upper bound $N^{0.30}$ of unknownn part
- Coron et al. obtained the upper bound $N^{0.167}$

Experimental Results

$\log N$	Unknown: $m[1]$	$H(m)$	LD	Time (Sec)
1024	74	160	36	21.71
2048	278	160	36	98.18
2048	180	256	36	95.05

Table: Experimental results when two faults occur with p and q.

In first two case previous bound was 12 and 182.

Summary

- We consider the partial key exposure attack on RSA
- Existing results: single contiguous block of unknown bits of the secret exponent
- we study partial key exposure attacks on RSA where the number of unexposed blocks in the decryption exponent is more than one
- We also study an ISO/IEC 9796-2 standard signature scheme with two faulty signatures for different primes

Open Problem

- Need to study the factorization of N with more than 2 signatures, some are faulty modulo p and others faulty modulo q


Thank You!