Recent Progress on Affine RSA Signature Forgery

Jean-Sébastien Coron (U Lux), David Naccache (ENS)

Mehdi Tibouchi (ENS)

What is an affine RSA forgery?

$$\sigma(m) = \mu(m)^d = (P+m)^d \bmod N$$

Importance: this tells us how malleable the RSA function is.

A thread of papers starting in the 1980s, improved the ratio between the sizes of P and N.

Current record: If P is about 2/3 the size of N then polynomial time forgery is possible.

New Result

Let n be a modulus of size k bits.

We have a polynomial time forgery for the shifted equation:

$$(P+x)(P+2^{k/4}y)=(P+z)(P+2^{k/4}w) \bmod N$$

Where x,y,z,w are all of size k/4 bits

$$(P+x)(P+2^{k/4}y)=(P+z)(P+2^{k/4}w) \bmod N$$

$$(P+x)(P+2^{k/4}y)=(P+z)(P+2^{k/4}w) \bmod N$$

$$\Downarrow$$

$$P\,2^{-k/4}\,(x-z+2^{k/4}(y-w))=wz-xy \bmod N$$

$$(P+x)(P+2^{k/4}y)=(P+z)(P+2^{k/4}w) \bmod N$$

$$\Downarrow$$

$$P\,2^{-k/4}\,(x-z+2^{k/4}(y-w))=wz-xy \bmod N$$

Write $P\,2^{-k/4}=A/B$ as a modular ratio of two k/2 bit numbers.

$$(P+x)(P+2^{k/4}y)=(P+z)(P+2^{k/4}w) \bmod N$$

$$\Downarrow$$

$$P\,2^{-k/4}\,(x-z+2^{k/4}(y-w))=wz-xy \bmod N$$

Write $P\,2^{-k/4}=A/B$ as a modular ratio of two k/2 bit numbers.

Identify $A=wz-xy$ and $B=x-z+2^{k/4}(y-w)$

$$(P+x)(P+2^{k/4}y)=(P+z)(P+2^{k/4}w) \bmod N$$

$$\Downarrow$$

$$P\,2^{-k/4}\,(x-z+2^{k/4}(y-w))=wz-xy \bmod N$$

Write $P\,2^{-k/4}=A/B$ as a modular ratio of two k/2 bit numbers.

Identify $A=wz-xy$ and $B=x-z+2^{k/4}(y-w)$

"read" that $y-w=H$ is the MSB of B and that $x-z=L$ is the LSB of B!

$$(P+x)(P+2^{k/4}y)=(P+z)(P+2^{k/4}w) \bmod N$$

$$\Downarrow$$

$$P\,2^{-k/4}\,(x-z+2^{k/4}(y-w))=wz-xy \bmod N$$

Write $P\,2^{-k/4}=A/B$ as a modular ratio of two k/2 bit numbers.

Identify $A=wz-xy$ and $B=x-z+2^{k/4}(y-w)$

"read" that $y-w=H$ is the MSB of B and that $x-z=L$ is the LSB of B!

Substitute x and simplify:

$$A=wz-(L+z)y \Rightarrow A=(w-y)z-Ly \Rightarrow A=Hz-Ly$$

$$(P+x)(P+2^{k/4}y)=(P+z)(P+2^{k/4}w) \bmod N$$

$$\Downarrow$$

$$P\,2^{-k/4}\,(x-z+2^{k/4}(y-w))=wz-xy \bmod N$$

Write $P\,2^{-k/4}=A/B$ as a modular ratio of two k/2 bit numbers.

Identify $A=wz-xy$ and $B=x-z+2^{k/4}(y-w)$

"read" that $y-w=H$ is the MSB of B and that $x-z=L$ is the LSB of B!

Substitute x and simplify:

$$A=wz-(L+z)y \Rightarrow A=(w-y)z-Ly \Rightarrow A=Hz-Ly$$

Solve mod H to find y. Solve mod L to find z

$$(P+x)(P+2^{k/4}y)=(P+z)(P+2^{k/4}w) \bmod N$$

$$\Downarrow$$

$$P\,2^{-k/4}\,(x-z+2^{k/4}(y-w))=wz-xy \bmod N$$

Write $P\,2^{-k/4}=A/B$ as a modular ratio of two k/2 bit numbers.

Identify $A=wz-xy$ and $B=x-z+2^{k/4}(y-w)$

"read" that $y-w=H$ is the MSB of B and that $x-z=L$ is the LSB of B!

Substitute x and simplify:

$$A=wz-(L+z)y \Rightarrow A=(w-y)z-Ly \Rightarrow A=Hz-Ly$$

Solve mod H to find y. Solve mod L to find z
Using z find x. Using y find w.

$$\mu(m_1) \cdot \mu(m_2) = \mu(m_3) \cdot \mu(m_4) \mod N$$

N = RSA-309

= bdd14965 645e9e42 e7f658c6 fc3e4c73 c69dc246 451c714e b182305b 0fd6ed47
d84bc9a6 10172fb5 6dae2f89 fa40e7c9 521ec3f9 7ea12ff7 c3248181 ceba33b5
5212378b 579ae662 7bcc0821 30955234 e5b26a3e 425bc125 4326173d 5f4e25a6
d2e172fe 62d81ced 2c9f362b 982f3065 0881ce46 b7d52f14 885eecf9 03076ca5

$\mu(m_1)$ = 7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff
ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff fffffff0
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000001
0a22096c f25655f4 104b2971 bc8b4f4f 817e6f4c d0ca8b25 ac5e8377 819e9d23

$\mu(m_2)$ = 7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff
ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff fffffff0
e1bdb579 4ad9e45a 7b17ee62 bf736d1c 8d897862 ce2c3349 72600b8b 44a8d4fb
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

$\mu(m_3)$ = 7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff
ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff fffffff0
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
113271f6 527c0815 fbf55d24 4883207b 827b9fb9 dd3ba8a6 2af1b776 d550a12d

$\mu(m_4)$ = 7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff
ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff fffffff1
0c9ca82a 80d6e82a e84d12a7 6415e27e d6d909da c2331285 aca27f4e 632d1556
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Second New Result

We have a fast subexp forgery for the equation:

$$(P+x)(P+y)=(P+z)(P+w) \bmod N$$

Where x,y,z are all of size k/4 but w is is of size 3k/8

This is based on a completely different technique.

Complexity = pull a factor of size k/8 out of a number of size 3k/8.

Quite technical, uses rational approximation and then LLL.

Come and one of us if interested.