Arithmetic algorithms for cryptology — 16 February 2015, Paris

Recent progress in discrete logarithm[1]

Razvan Barbulescu

CNRS and IMJ-PRG

[1] After the complexity analysis of NFS on the blackboard.

Outline of the talk

- Key sizes
- Special number field sieve
- Automorphisms
- Future development

Security level

Definition

A crypto-system has security s if the best known attack requires 2^s elementary operations.

Utilisation

1. One can choose the fastest crypto-system of a given security level.
2. If symmetric and asymmetric crypto-systems are used together, it is optimal to have the same security level.

Moore's law

Due to the evolution of computers (Moore's law), the same security level can be considered strong at some moment and weak several years later. In 2015, the main levels of security are:

- 80 bits
- 128 bits
- 256 bits.

Key sizes for RSA (1/2)

Complexity

The best algorithm in practice is NFS.

- its complexity is $L_N(1/3, c)^{1+o(1)}$ with $c = \sqrt[3]{64/9} \approx 1.923$; the $o(1)$ term is problematic for extrapolations;
- according to Lenstra and Verheul (Selecting cryptographic key sizes, 2001), the $o(1)$ term has a small derivative, so one can extrapolate on small intervals.
- hence we use the model of complexity $\kappa L_N(1/3, c)$ for some constant κ determined by experiments.

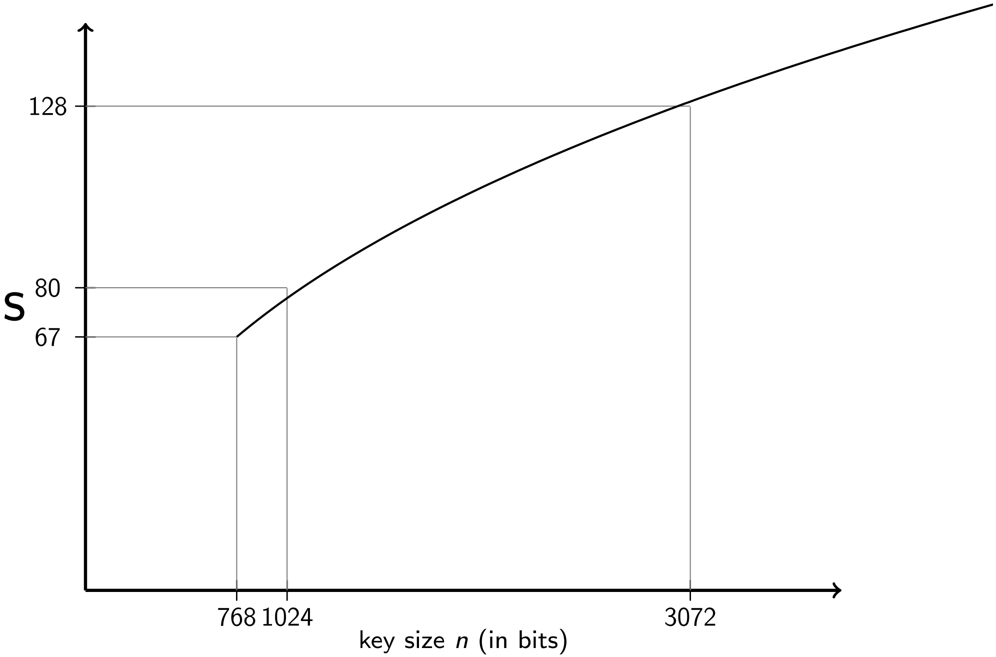
Factorization Record

- RSA challenge, 768 bits;
- 2009, international team (Nancy, Lausanne, Bonn, Tokyo, Amsterdam, Redmond);
- it took 2000 CPU years on 3GHz cores:

$$\log_2(3G \cdot 2000 \cdot 3.15e7) \approx 66.7.$$

$$\boxed{\text{RSA 768 offers 67 bits of security.}}$$

Key sizes for RSA (2/2)



Extrapolation formula

$$2^s = 2^{67} \frac{L_{2^n}(1/3, c)}{L_{2^{768}}(1/3, c)}$$

Key size for DSA and pairings

DSA (discrete log in $\mathbb{F}_p$)

- Same algorithm (NFS), with same parameters, and therefore the same key sizes.
- In 2014, DLP was solved in a field $\mathbb{F}_p$ of 180 decimal digits (Nancy). It took 130 CPU years, to be compared to 5.5 CPU years to factor an RSA module of same size.

Pairings

These crypto-systems must resist to two types of attacks:

- DLP on elliptic curves.
- DLP in fields $\mathbb{F}_{p^k}$ with $k \geq 2$. Until 2014 no records were done, so one uses the key sizes of RSA.

SNFS algorithm

What are the weak keys?

For each size of number N, one computes the optimal value of the non-linear polynomial f used in NFS. For $N \approx 2^{1024}$ the optimal degree is 6 or 7. If a number N can be written as $N = P(u)$ with P a polynomial and $u \approx N^{1/d}$, then N is an SNFS number.

Complexity

- NFS on SNFS numbers has complexity $L_N(1/3, c/\sqrt[3]{2})$ where $c = \sqrt[3]{64/9}$.
- One can show that an SNFS key of size $2t$ has the same security as an RSA key of size t.
- The record for SNFS numbers is 1024 and took CPU time comparable to RSA 512.

SNFS by error?

Test if SNFS

```
Require: integer $N$ and degree $d$
Ensure: YES/NO an NFS number, and polynomial $f$
for $(f_d, \dots, f_0)$ do
    Find the integer roots $\mathcal{R}$ of $\sum f_i x^i - N$
    if $\mathcal{R} \neq \emptyset$ then
        return YES and $\sum_{i=0}^{d} f_i x^i$
    end if
end for
return NO
```

Complexity

The computation of integers roots has a polynomial complexity. One computes the roots modulo a small prime, say 17, then lifts the solutions mod 17^2, 17^3, etc. Since the largest root is smaller than $\sum_{i=0}^{d-1} |f_i|$, it is enough to lift the solution $\log(\|f\|_\infty)$ times.

SNFS in pairings

The BN pairings

Some pairings, e.g. the Barreto-Naehrig pairings, rely on the difficulty of DLP in fields $\mathbb{F}_{p^k}$ with $k > 1$ and p is an SNFS number.

SNFS in $\mathbb{F}_{p^k}$

- In 2013 Joux and Pierrot Some pairings, e.g. the Barreto-Naehrig pairings, rely on the difficulty of DLP in fields $\mathbb{F}_{p^k}$ with $k > 1$ and p is an SNFS number. The second constant in the complexity is divided by $\sqrt[3]{2}$.
- In 2014, B., Gaudry and Kleinjung announced a second algorithm.

The case of Kummer extensions

DLP in fields $F_q[x]/\langle x^{q-1}-\mu\rangle$

We have $x^q=\mu x$ and then, for any $a\in\mathbb{F}_q$

$$\begin{aligned}(x-a)^q &= x^q-a^q\\ &= \mu x - a\\ &= \mu(x-a/\mu).\end{aligned}$$

Taking discrete logs, we have

$$q\log(x-a)=\log(\mu)+\log(x-a/\mu)=\log(x-a/\mu)$$

because the logs of constants is 0 (previous lecture).

Advantage

We keep $q-1$ times less logarithms in the factor base, so a speed-up of

- $q-1$ in the relation collection stage;
- $(q-1)^2$ in the linear algebra stage.

Automorphisms in general

Automorphisms in other fields

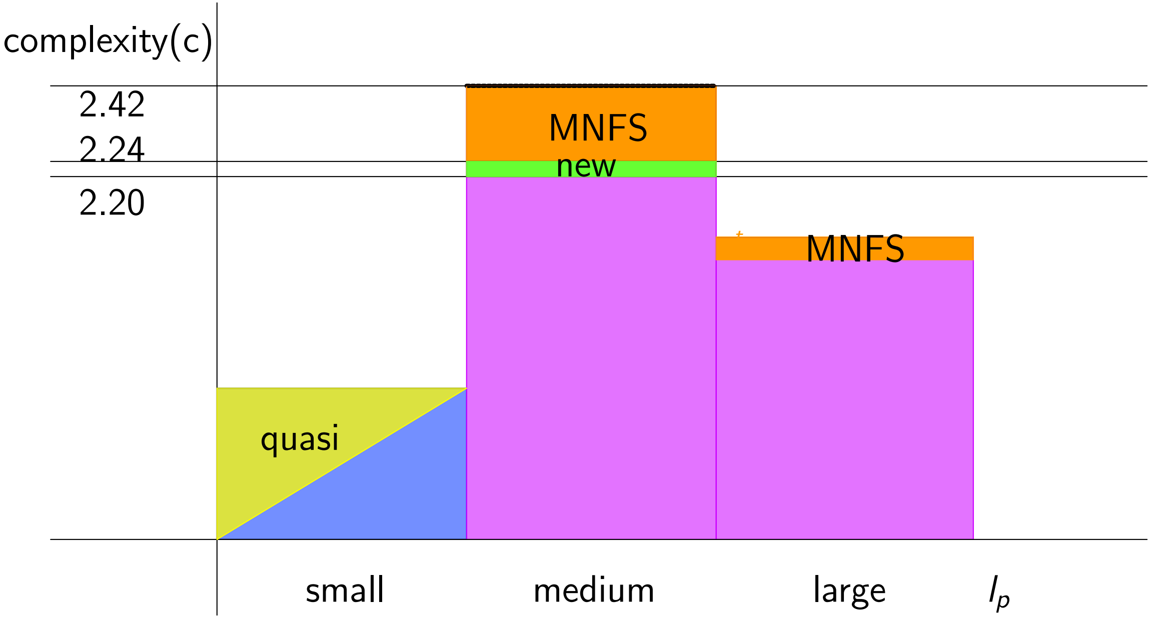
- In $\mathbb{F}_{p^k}$ using NFS we have a speed-up of k (JLSV 2006);
- In $\mathbb{F}_{q^{k\ell}}$, where q is a power of 2 or 3, using FFS we have a speed-up of k.

Remark

A similar situation, and speed-up, occurs for elliptic curves discrete logarithm when

- The curves admits a group isomorphism.
- The curve has torsion points of small order (e.g. P such that $2P = 0$).

Complexities of DLP in $\mathbb{F}_Q$ when $p = L_Q(l_p)$



Polynomial selection for $\mathbb{F}_p$

Polynomial selection by rational reconstructon (JLSV 2006)

```
Require: $p$ prime and $n$ integer
Ensure: $f, g, \varphi$ with $f, g \in \mathbb{Z}[x]$ irreducible and $\varphi = \gcd(f \bmod p, g \bmod p)$ in $\mathbb{F}_p[x]$
  irreducible of degree $n$
  Select $f_1(x)$, $f_0(x)$, two polynomials with small integer coefficients,
  $\deg f_1 < \deg f_0 = n$
  repeat
      Choose $a \geq \lceil \sqrt{p} \rceil$
      $(u, v) \leftarrow$ a rational reconstruction of $a$ modulo $p$
      $f \leftarrow f_0 + a f_1$
      $g \leftarrow v f_0 + u f_1$
  until $f$ is irreducible in $\mathbb{F}_p[x]$
  return $(f, g, \varphi = g \bmod p)$
```

Example

Take $p = 1000001447$, $n = 4$, and $a = 44723 \geq \lceil \sqrt{p} \rceil$. One has $f = (x^4 - 6x^2 + 1) - 44723(x^3 - x)$ and $g = 22360(x^4 - 6x^2 + 1) - 4833(x^3 - x)$ with $u/v = 4833/22360$ a rational reconstruction of a modulo p.

Conjugation method (1/2)[2]

Example

- We target $\mathbb{F}_{p^4}$ with $p = 1000010633$.
- We try integers $a = -2, -3, \dots$ until a is a square but not a fourth power in $\mathbb{F}_p$. We find $a = -9$.
- We set $f = x^8 - a = x^8 + 9$ which is irreducible over $\mathbb{Z}$. Observe that by construction, f has two degree 4 conjugate irreducible factors $f = (x^4 - \sqrt{a})(x^4 + \sqrt{a})$.
- We set $\varphi = x^4 - \sqrt{a}$ which, due to the choice of a, belongs to $\mathbb{F}_p[x]$ and is irreducible.
- We continue by computing a rational reconstruction (u, v) of $\sqrt{a}$ modulo p: $u \cdot v^{-1} \equiv \sqrt{a} \mod p$; here $u = -58281$ and $v = 24952$.
- Finally we set $g = vx^4 - u = 24952x^4 + 58281$ of norm $\|g\|_\infty \sim \sqrt{p}$.
- Note that we respect the condition $\varphi = \gcd(f \mod p, g \mod p)$.

[2] Eurocrypt 2015

Conjugation method (2/2)

```
Require: $p$ prime and $n$ integer
Ensure: $f, g, \varphi$ with $f, g \in \mathbb{Z}[x]$ irreducible and $\varphi = \gcd(f \bmod p, g \bmod p)$ in $\mathbb{F}_p[x]$ irreducible of degree $n$
repeat
    Select $g_1(x), g_0(x)$, two polynomials with small integer coefficients, $\deg g_1 < \deg g_0 = n$
    Select $\mu(x)$ a quadratic, monic, irreducible polynomial over $\mathbb{Z}$ with small coefficients
until $\mu(x)$ has a root $\lambda$ in $\mathbb{F}_p$ and $\varphi = g_0 + \lambda g_1$ is irreducible in $\mathbb{F}_p[x]$
$(u, v) \leftarrow$ a rational reconstruction of $\lambda$
$f \leftarrow \mathrm{Res}_Y(\mu(Y), g_0(x) + Y g_1(x))$
$g \leftarrow v g_0 + u g_1$
return $(f, g, \varphi)$
```

Timings

Algorithm	relation collection	linear algebra	total
NFS-IF	5 years	5.5 months	5.5 years
NFS-DL(p)	50 years	80 years	130 years
NFS-DL(p^2)	157 days	18 days (GPU)	0.5 years

Table : Comparison of running time for integer factorization (NFS-IF), discrete logarithm in prime field (NFS-DL(p)) and in quadratic field (NFS-DL(p^2)) of same global size 180 dd.