Algorithmes arithmétiques pour la cryptologie — 13 février 2018, Paris

A brief overview of pairings attacks

Razvan Barbulescu
CNRS and IMJ-PRG

Notations

Elliptic curves

- equation (in Edwards form): $x^2 + y^2 = c^2(1 + dx^2y^2)$ where $c, d \in K$ and $cd(1 - c^4d) \neq 0$
- group law (when odd cardinality): $(x_1, y_1) + (x_2, y_2) = (\frac{x_1y_2+x_2y_1}{c(1+dx_1x_2y_1y_2)}, \frac{y_1y_2-x_1y_2}{c(1-dx_1x_2y_1y_2)})$
- cardinality (Hasse) :
$$|\#\{(x : y : z) \in \mathbb{P}^2(\mathbb{F}_q) : x^2z^2 + y^2z^2 = c^2(z^4 + dx^2y^2)\} - q - 1| \leq 2\sqrt{q}$$
- scalar product : for any r and P , $[r]P = P + \cdots + P$ (r times)

Finding elliptic curves

Use in cryptography

- Elliptic curves are used in all group-based cryptography : ElGamal, Diffie-Hellman, DSA. They are standardized since 1999.

- Curves are constructed as follows
  - select the good size
  - pick a random prime q of the good size
  - pick random parameters c and d which define a curve E
  - use the Schoof algorithm to compute the cardinality r
  - test primality of r (if desired test primality of $2(q+1)-r$)

Pairings

Definition

- E an elliptic curve over a field K
- r an integer
- P(x,y) a point on E so that $[r]P = (0, c)$ (neutral element).
- μ a unit of Φ_r in the algebraic closure of K

$$e_{E,r,P,\mu} : \begin{array}{ccc} \frac{\mathbb{Z}}{r\mathbb{Z}}P \times \frac{\mathbb{Z}}{r\mathbb{Z}}P & \rightarrow & \mu^{\mathbb{Z}/r\mathbb{Z}} \\ ([a]P, [b]P) & \mapsto & \mu^{ab}. \end{array}$$

Properties of a pairing e

Non-degenerate bilinear map.

Computations of pairings

1. Theorem of Weil (1948): pairings can be defined in terms of divisors, without computing a,b
2. Algorithm of Miller (1985): pairings evaluation is related to a "fast exponentiation" and has a polynomial complexity

Three-party Diffie-Hellman

Problem

Alice, Bob and Carol use a public elliptic curve E and a pairing e with respect to a point P. Each of the participants broadcast simultaneously an information in a public channel. How can they agree on a common key ?

Joux's protocol (2000)

1. Simultaneously, each participant generates a random integer in $[0, r-1]$ and broadcasts a multiple of P:
   - Alice generates a and computes $[a]P$;
   - Bob generates b and computes $[b]P$;
   - Carol generates c and computes $[c]P$;
2. Simultaneously, each participant computes the pairing of the received information and computes the common key:
   - Alice computes $e([b]P, [c]P)^a$;
   - Bob computes $e([c]P, [a]P)^b$;
   - Carol computes $e([a]P, [b]P)^c$;

Common secret key: μ^{abc}.

Embedding degree

Definition

Given E, K and r the embedding degree is the degree of the extension of K which contains an r-th root of unity.

Pariring friendly elliptic curves

Let q be selected so that the discrete logarithm problem is just hard enough in the elliptic curve. Then

- if k is too large, computations are slow (arithmetic in $\mathbb{F}_{q^k}$)
- if k is too small, the discrete logrithm in $\mathbb{F}_{q^k}$ is too easy and the pairing is not safe.

Key sizes

security (bits)	key size RSA $\log_2(q^k)$	key size ECDSA $\log_2 r \approx \log_2 q$	quotient
80	1024	160	6
128	3072	256	12
256	15360	512	30

We need curves such that

- cardinality $r = c \times$ prime with $c \leq 10$
- k donné

CM method

Motivation

Theorem of Köblitz and Balusubramanian : a proportion of $1 - o(1)$ of the curves defined over $\mathbb{F}_q$ have $k \approx q$.

We cannot take random curves, we must find families

Constructing pairings

Given an embedding degree k we construct a pairing-friendly curve E as follows:

1. find q, r and t subject to the CM equations in next slide; they are
   - $\mathbb{F}_q$ is the field of coefficients
   - E has $q + 1 - t$ points
   - E has a subgroup of order r.

2. apply the complex method (Morain 1990) to construct a curve E corresponding to q,r,t. The cost is $O(h_D^{2+\epsilon})$ where h_D is the class number of $\mathbb{Q}(\sqrt{D})$ (for a random D, $h_D \simeq \sqrt{D}$).

CM equations

k given but some exceptions are allowed

Two primes q and r and a square-free integer D satisfy the CM conditions if

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $q + 1 - t \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Super-singular curves

Idea

Take $t = 0$ and $k = 2$. Indeed,

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$ (true for all r because $\Phi_2(-1) = 0$)
2. $q + 1 - t \equiv 0 \pmod{r}$ (true for any divisor r of $q+1$)
3. $\exists y,\ 4q = Dy^2 + t^2$ (true for any q)

Limits

- if $q = 2$ or $q = 3$ we can have $k \in \{1, 2, 3, 4, 6\}$ (but small characteristic and hence subject to the quasi-polynomial time attack)
- if $q \geq 5$ we have two possibilities
  - $k = 2$ OK
  - $k = 1$ but $q = p^{2s}$ and E or its twist are isomorphic to a pairing of embedding degree 2 defined over p^s ($\mathbb{F}_{(p^{2s})^1 = \mathbb{F}_{(p^s)^2}}$).

Cocks-Pinch

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $q + 1 - t \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

Cocks-Pinch

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $Dy^2 + (t-2)^2 \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

1. replace (2) by an equivalent equation

Cocks-Pinch

CM equations

1. ~~$\Phi_k(t-1) \equiv 0 \pmod{r}$~~
2. $Dy^2 + (t-2)^2 \equiv 0 \pmod{r} \Leftrightarrow (\sqrt{-D}y + (t-2))(\sqrt{-D}y - (t-2) \equiv 0(r)$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

1. replace (2) by an equivalent equation
2. select r so that $r \equiv 1 \mod k$ and $(\frac{-D}{r}) = 1$

Cocks-Pinch

CM equations

1. ~~$\Phi_k(t-1) = 0 \pmod r$~~
2. ~~$Dy^2 + (t-2)^2 = 0 \pmod r \Leftrightarrow (\sqrt{-D}y + (t-2))(\sqrt{-D}y - (t-2) = 0 \pmod r$~~
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

1. replace (2) by an equivalent equation
2. select r so that $r \equiv 1 \mod k$ and $(\frac{-D}{r}) = 1$
3. solve (2) for y

Cocks-Pinch

CM equations

1. ~~$\Phi_k(t-1) = 0 \pmod r$~~
2. ~~$Dy^2 + (t-2)^2 = 0 \pmod r \Leftrightarrow (\sqrt{-D}y + (t-2))(\sqrt{-D}y - (t-2) = 0 \pmod r$~~
3. ~~$\exists y,\ 4q = Dy^2 + t^2$~~

Method

1. replace (2) by an equivalent equation
2. select r so that $r \equiv 1 \mod k$ and $(\frac{-D}{r}) = 1$
3. solve (2) for y
4. solve (3) for q

Dupont-Enge-Morain

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $q+1-t \equiv 0 \pmod{r}$ $a+(t-2)^2 \equiv 0 \pmod{r}$ where $a = Dy^2$
3. $\exists y,\ 4q = Dy^2 + t^2$

Method

1. replace (2) by an equivalent equation
2. compute $R(a) = \mathrm{Res}_t(\Phi_k(t-1), a+(t-2)^2)$; enumerate a's and take
   - r a prime factor of $R(a)$
   - compute $\gcd(\Phi_k(t-1) \bmod r, a+(t-2)^2 \bmod r)$ and obtain t if it is linear
3. solve (3) for q

Sparse families (e.g. MNT)

CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $q + 1 - t \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$ generalized Pell equation (e.g. $X^2 - 3Dy^2 = 24$, where $X = 6x \pm 3$)

Method when $\varphi(k) = 2$ (example when $k = 3$)

1. put $r = \Phi_k(t-1)$, which satisfies (1)
2. put $q = r + t - 1$, which satisfies (2)
3. put $t = t(x)$, t linear, and note that this forces $q = q(x)$, quadratic polynomial q (e.g. $t(x) = -1 \pm 6x$ and $q(x) = 12x^2 - 1$). This transforms (3) into a generalized Pell equation
4. solve the generalized Pell equation to get y and x, and therefor q

Was generalized by Freeman to $k = 10$, where $\varphi(k) = 4$

Complete families (e.g. BN)

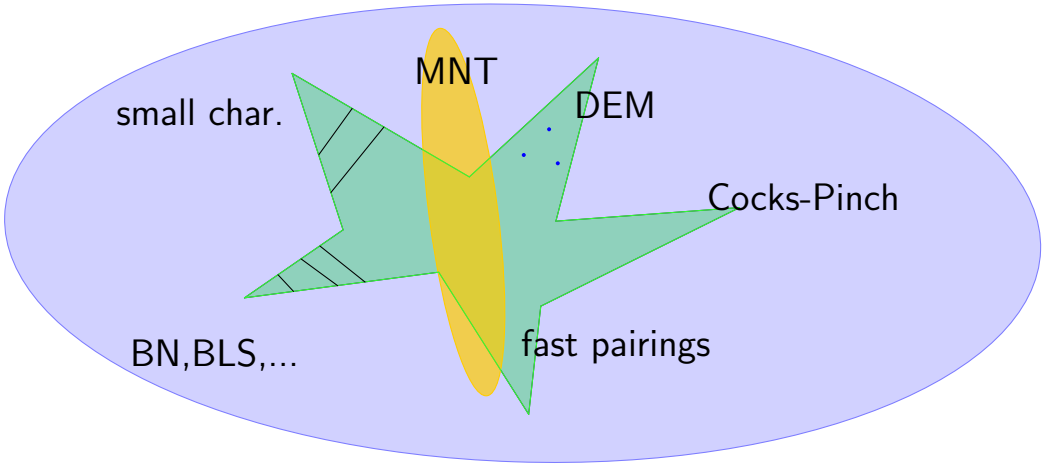
CM equations

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $q+1-t \equiv 0 \pmod{r}$ $Dy^2+(t-2)^2 \equiv 0 \pmod{r}$ $Dy^2+(t-2)^2 \equiv 0 \pmod{r} \Leftrightarrow (\sqrt{-D}y+(t-2))(\sqrt{-D}y-(t-2) \equiv 0(\mod r)$
3. $\exists y,\ 4q = Dy^2+t^2$

1. replace (2) by an equivalent equation
2. - select $r(x) \in \mathbb{Q}[x]$ so that $\mathbb{Q}[x]/r(x)$ contains a root of x^2-D and a root of $\Phi_k(x)$
   - take $t = t(x)$ to be such that $t-1$ is a kth root of unity mod $r(x)$
3. put $y = t(x)/\sqrt{-D}$ which satisfies (2)
4. solve (3) for q

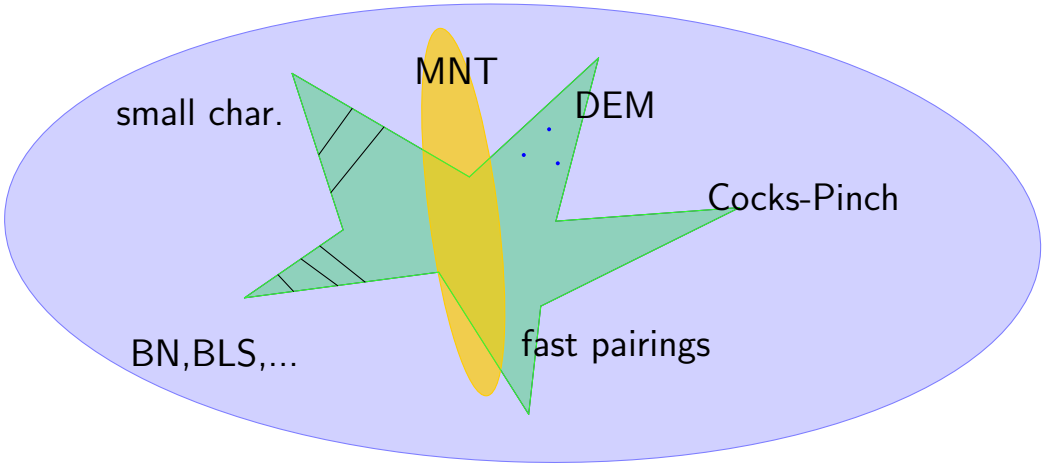
Note that we generate a large number of elliptic curves very quickly.

Summary



- Pinch-Cocks constructs all the fast pairings, but it is never in the fast case.
- Sparse families (e.g. MNT) construct many pairings but $k = 2$ and they are not fast for the ≥ 80 bits of security.
- Dupond-Enge-Morain offers a very small number of pairings, which might be target of subsequent attacks, impossible to tune them to be faster in practice.

Summary



- Pinch-Cocks constructs all the fast pairings, but it is never in the fast case.
- Sparse families (e.g. MNT) construct many pairings but $k = 2$ and they are not fast for the ≥ 80 bits of security.
- Dupond-Enge-Morain offers a very small number of pairings, which might be target of subsequent attacks, impossible to tune them to be faster in practice.

We are left with small char and parametrized families (e.g. BN, BLS).

Discrete logarithm problem (DLP)

DLP

Given P and $[a]P$ find a.

Generic algorithm

A combination of Pohlig-Hellman reduction and Pollard's rho solves DLP in a generic group G after $O(\sqrt{r})$ operations, where r is the largest prime factor of $\#G$.

Relation to pairings

A pairing $e : \langle P \rangle \times \langle P \rangle \to K(\mu)$ is safe only if

1. DLP in $E[r]$ is hard; (DLP on elliptic curves) **if** $\log_2 \#G = n$, **cost**$=2^{\frac{n}{2}}$
2. DLP in $K(\mu)$ is hard. (DLP in finite fields) **if** $\log_2 \#K(\mu) = n$, **cost**$\approx \exp(\sqrt[3]{n})$

Small characteristic

Chronology

- December 2012: Joux creates "pinpointing" using Frobenius. The idea works for any prime power q but he uses it for primes.

Small characteristic

Chronology

- December 2012: Joux creates "pinpointing" using Frobenius. The idea works for any prime power q but he uses it for primes.
- February 2013: In the same time Joux and, in parallel, Göloğlu, Granger, McGuire, Zumbrägel apply the idea to $q = 2^k$ and find logs of factor base in polynomial time.

Small characteristic

Chronology

- December 2012: Joux creates "pinpointing" using Frobenius. The idea works for any prime power q but he uses it for primes.
- February 2013: In the same time Joux and, in parallel, Göloğlu, Granger, McGuire, Zumbrägel apply the idea to $q = 2^k$ and find logs of factor base in polynomial time.
- In the same paper, Joux introduces techniques to reduce global time to $L(1/4)$ and for degree 2 polys he uses a factor base which has few instead of small elements.

Small characteristic

Chronology

- December 2012: Joux creates "pinpointing" using Frobenius. The idea works for any prime power q but he uses it for primes.
- February 2013: In the same time Joux and, in parallel, Göloğlu, Granger, McGuire, Zumbrägel apply the idea to $q = 2^k$ and find logs of factor base in polynomial time.
- In the same paper, Joux introduces techniques to reduce global time to $L(1/4)$ and for degree 2 polys he uses a factor base which has few instead of small elements.
- June 2013: Barbulescu, Gaudry, Joux, Thomé use this latter idea to create the quasi-polynomial algorithm.

Small characteristic

Chronology

- December 2012: Joux creates "pinpointing" using Frobenius. The idea works for any prime power q but he uses it for primes.
- February 2013: In the same time Joux and, in parallel, Göloğlu, Granger, McGuire, Zumbrägel apply the idea to $q = 2^k$ and find logs of factor base in polynomial time.
- In the same paper, Joux introduces techniques to reduce global time to $L(1/4)$ and for degree 2 polys he uses a factor base which has few instead of small elements.
- June 2013: Barbulescu, Gaudry, Joux, Thomé use this latter idea to create the quasi-polynomial algorithm.
- October 2013: ECRYPT forbids pairings of small characteristic.

Small characteristic

Chronology

- December 2012: Joux creates "pinpointing" using Frobenius. The idea works for any prime power q but he uses it for primes.
- February 2013: In the same time Joux and, in parallel, Göloğlu, Granger, McGuire, Zumbrägel apply the idea to $q = 2^k$ and find logs of factor base in polynomial time.
- In the same paper, Joux introduces techniques to reduce global time to $L(1/4)$ and for degree 2 polys he uses a factor base which has few instead of small elements.
- June 2013: Barbulescu, Gaudry, Joux, Thomé use this latter idea to create the quasi-polynomial algorithm.
- October 2013: ECRYPT forbids pairings of small characteristic.
- 2014-2016 practical improvements and second quasi-poly algorithm (Joux, Pierrot, Menezes, Adj, Kleinjung, Oliveira-H., Rodriguez-Henriquez, Granger, Zumbrägel).

Small characteristic

Chronology

- December 2012: Joux creates "pinpointing" using Frobenius. The idea works for any prime power q but he uses it for primes.
- February 2013: In the same time Joux and, in parallel, Göloğlu, Granger, McGuire, Zumbrägel apply the idea to $q = 2^k$ and find logs of factor base in polynomial time.
- In the same paper, Joux introduces techniques to reduce global time to L(1/4) and for degree 2 polys he uses a factor base which has few instead of small elements.
- June 2013: Barbulescu, Gaudry, Joux, Thomé use this latter idea to create the quasi-polynomial algorithm.
- October 2013: ECRYPT forbids pairings of small characteristic.
- 2014-2016 practical improvements and second quasi-poly algorithm (Joux, Pierrot, Menezes, Adj, Kleinjung, Oliveira-H., Rodriguez-Henriquez, Granger, Zumbrägel).
- Two 128 bit pairings are broken in char 2 (Granger, Kleinjung, Zumbrägel 2014) and 3 (Canales-Martínez, Cortés, Menezes, Oliveira, Rivera-Zamarripa and Rodríguez-Henríquez 2016).

The case of $\mathbb{F}_p^k$ with non-small characteristic p

Chronology

- 2000: Schirokauer creates a variant of NFS where integers are replaced by complex numbers of the form $a + ib$ where a and b are integers. He asks if this applies to parametrized primes (SNFS).

The case of $\mathbb{F}_p^k$ with non-small characteristic p

Chronology

- 2000: Schirokauer creates a variant of NFS where integers are replaced by complex numbers of the form $a + ib$ where a and b are integers. He asks if this applies to parametrized primes (SNFS).
- 2013: Joux and Pierrot create a method of polynomial selection for classical NFS which has a better asymptotic complexity.

The case of $\mathbb{F}_p^k$ with non-small characteristic p

Chronology

- 2000: Schirokauer creates a variant of NFS where integers are replaced by complex numbers of the form $a + ib$ where a and b are integers. He asks if this applies to parametrized primes (SNFS).
- 2013: Joux and Pierrot create a method of polynomial selection for classical NFS which has a better asymptotic complexity.
- 2015: Barbulescu, Gaudry, Guillevic and Morain create a method of polynomial selection for arbitrary form when $k = 2$ and $k = 3$.

The case of $\mathbb{F}_p^k$ with non-small characteristic p

Chronology

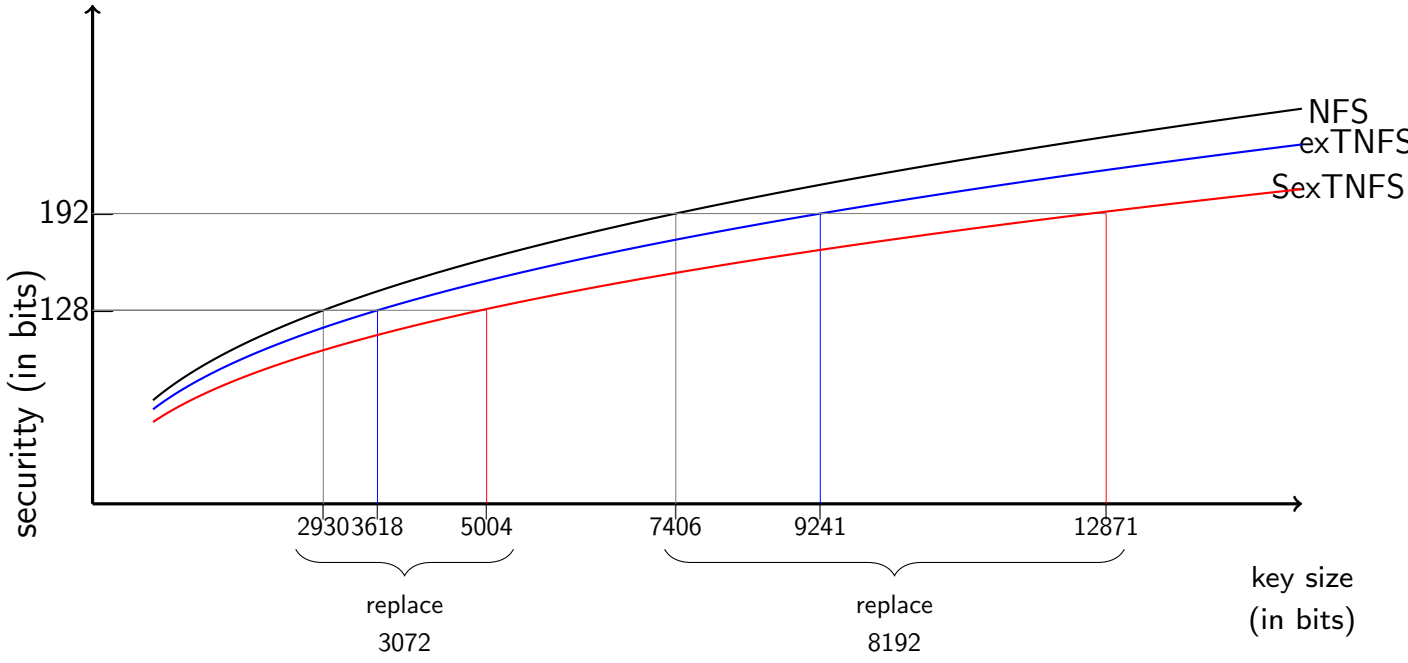
- 2000: Schirokauer creates a variant of NFS where integers are replaced by complex numbers of the form $a + ib$ where a and b are integers. He asks if this applies to parametrized primes (SNFS).
- 2013: Joux and Pierrot create a method of polynomial selection for classical NFS which has a better asymptotic complexity.
- 2015: Barbulescu, Gaudry, Guillevic and Morain create a method of polynomial selection for arbitrary form when $k = 2$ and $k = 3$.
- 2015: Barbulescu, Gaudry, Kleinjung rehabilitate Schirokauer's TNFS.

The case of $\mathbb{F}_p^k$ with non-small characteristic p

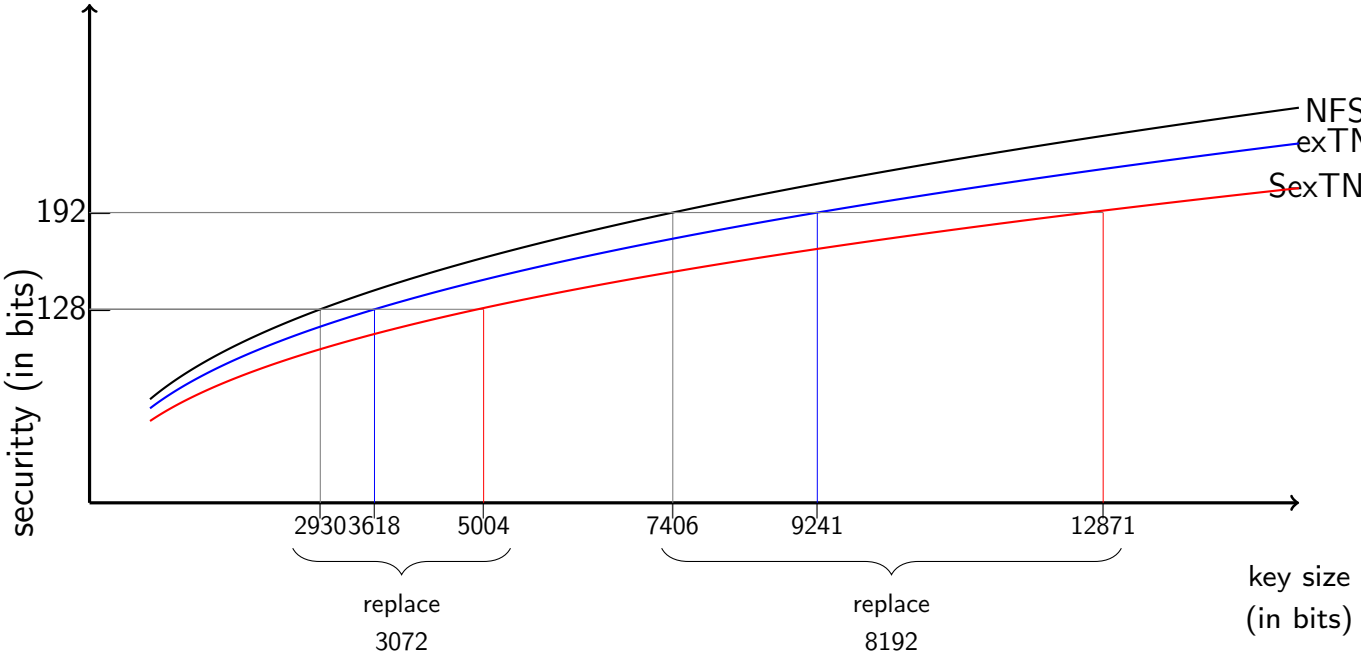
Chronology

- 2000: Schirokauer creates a variant of NFS where integers are replaced by complex numbers of the form $a + ib$ where a and b are integers. He asks if this applies to parametrized primes (SNFS).
- 2013: Joux and Pierrot create a method of polynomial selection for classical NFS which has a better asymptotic complexity.
- 2015: Barbulescu, Gaudry, Guillevic and Morain create a method of polynomial selection for arbitrary form when $k = 2$ and $k = 3$.
- 2015: Barbulescu, Gaudry, Kleinjung rehabilitate Schirokauer's TNFS.
- 2015-2016: Kim and later Barbulescu combine TNFS and the recent methods of polynomial selection to obtain very good asymptotic complexities when k has a factor 2 or 3 and, particularly good when additionally p has parametrized form.

Change of keysizes by ignoring o(1)



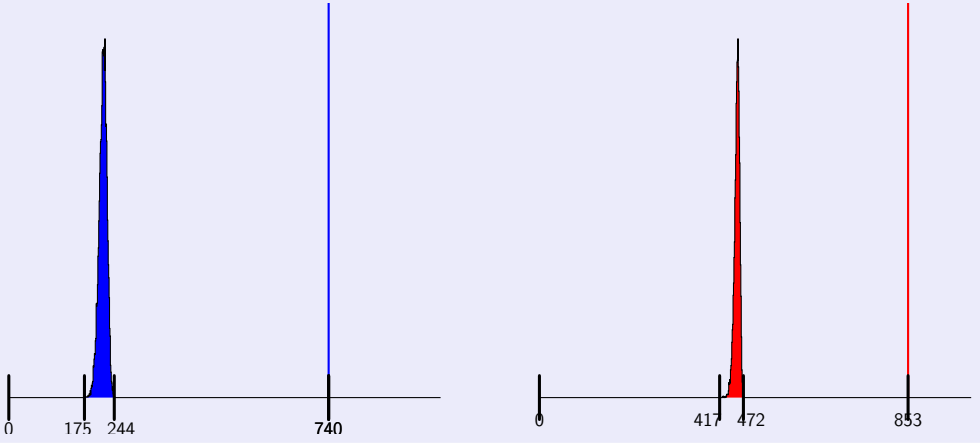
Change of keysizes by ignoring o(1)



This suggests that for BN one has to replace 3072 by 5004.

Updating keysizes (joint work with S. Duquesne)

Unpreciseness of a previous work: Menezes, Sarkar, Singh 2016



New key sizes

Family	$\log_2(p^k)$	κ	A	$\log_2 B$
obsolète sizes	3072			
BN	5534	2	1145	74.00
BLS12	5530	2	1098	73.65
KSS16	$\approx 4400^*$	1	9	76.5
KSS18	$\approx 4300^*$	1	9	76

*: curve side is weaker, we need 5410 and resp. 6257 bits.

Conclusion

- Only small char and parametrized pairings have been considered for industrial application.
- New attacks in small char. lead ECRYPT to forbid small characteristic.
- New attacks in non-small char demand to update the key sizes.
- The practical improvements of NFS which have asted over 30 years transformed $o(1)$ from positive to negative and made the new attacks practical.
- Records are likely to come but they will take years, and delay the standardization of pairings.

Conclusion

- Only small char and parametrized pairings have been considered for industrial application.
- New attacks in small char. lead ECRYPT to forbid small characteristic.
- New attacks in non-small char demand to update the key sizes.
- The practical improvements of NFS which have asted over 30 years transformed $o(1)$ from positive to negative and made the new attacks practical.
- Records are likely to come but they will take years, and delay the standardization of pairings.

Post quantun alternatives might be introduced.