Diversity and Transparency for ECC

Jean-Pierre Flori, Jérôme Plût, Jean-René Reinhard, and Martin Ekerå

ANSSI and NCSA/SW

June 11, 2015

I – Standardization

Need for standardization?

In general, the group of rational points of an elliptic curve behaves as a "generic group": the DLOG problem has **exponential** complexity, provided:

- The curve cardinality includes a *large prime factor* q.
  - Solution: use curves with (almost) prime cardinality.
- The DLOG problem can not be transferred into *weaker* groups.
  - Solution: avoid weak curves.

Applying these solutions is **computationally expensive**: curves can not be generated on demand.

Standardized curves

Year		Curves	Sizes
2000		NIST	192, 224, 256, 384, 521
2005		Brainpool	160, 192, 224, 256, 320, 384, 512
2010		OSCCA	256
2011		ANSSI	256

- Plus a few academic propositions (Curve25519/41417, NUMS, Ed448-Goldilocks, . . .).

Need for a second round?

The first curves were standardized in years 2000 when:

- it was possible to find curves with prime cardinality (SEA algorithm);
- weak classes of curves were identified.

We think that these curves are still secure...

...but new concerns emerged since then:

- what about the generation process? (is there some hidden secret vulnerability?)
- what about side-channel attacks?
- what about scientific progess in related domains (e.g. DLOG in finite fields)?

It is a good time to standardize new curves.

II – Security

Five classes of criteria

1. The **DLOG** problem should be hard.
2. Implementations should be **safe** (e.g. resist *side-channel attacks*).
3. The curve should exhibit no **particularities**.
4. Implementations can be **optimized**.
5. (The curve exhibits **interesting** properties.)

Tradeoffs

Some conditions are **incompatible**: this is a good reason to standardize *different* (families of) curves.

Base field

We only deal with *prime base fields* as we think that *extension fields* introduce more vulnerabilities without valuable properties.

DLOG problem difficulty

- **Large prime subgroup**: Attacks with complexity $O(\sqrt{q})$ exist where q is the largest prime factor of N.

It is mandatory that:

- $q \approx N$ ($\mathcal{P} \approx \frac{1}{\log p}$, costly).
- At best $q = N$ (*no complete addition law!*).

- **Weak curves**: For some curves the DLOG problem can be transferred into a weaker finite field.

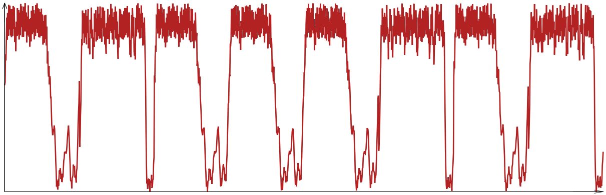
It is mandatory that:

- $\Delta \neq 0$ ($\mathcal{P} \approx 1$, free);
- $N \neq p$ ($\mathcal{P} \approx 1$, free);
- the *embedding degree* must be large ($\mathcal{P} \approx 1$, costly).

Safe implementation

Even though the DLOG problem is *hard* on the curve, implementations might **leak** information.

Example: scalar multiplication using naive "double-and-add" algorithm.



D	A	D	D	D	A	D	A
1		0	0	1		1	

Classical countermeasures

- Against **simple** attacks: avoid branching depending on secret elements.
  - "double-and-add" always;
  - Montgomery ladder.
- Against **differential** attacks: avoid using secrets elements repeatedly.
  - secret *masking*;
  - curve *masking*;
  - point *masking*.

This is not enough: information can still **leak**!

Further countermeasures

Masking inefficiency

Avoid base field with *special prime* cardinality (*no fast reduction!*).

Exceptional cases

Use a curve with a *complete* addition law (*no prime cardinality!*).

Special points

Ensure no points with a *zero coordinate* exist (*no complete addition law!*).

Misbehavior resistance

Subgroup attacks

Ensure no *small subgroups* exist ($\mathcal{P} = 1$ if N is prime, *no complete addition law!*).

Twist attacks

Use a *twist* with prime cardinality ($\mathcal{P} \approx \frac{1}{\log p}$, *does not leverage all checks!*).

Resist attacks to come?

- What if we don't know all classes of **weak** curves?
- Avoid producing too "*special*" curves!
- Verify properties satisfied with $\mathcal{P} \approx 1$ in the sense of the DLOG problem difficulty.
- In particular, some **numbers attached to the curve** should be "*large enough*".

The curve should look **generic**.

Numbers attached to a curve

Discriminant of the endomorphism ring

In general, the *discriminant* satisfies $|D_E| \approx p$; therefore, $|D_E| \geq \sqrt{p}$ with $\mathcal{P} \approx 1 - O(1/\sqrt{p})$ (*no pairings, no fast endomorphism!*).

Class number friability

In general, the *class number* h_E has at least a prime divisor $\geq (\log p)^{O(1)}$.

Embedding degree

The *embedding degree* is $\geq p^{1/4}$ with $\mathcal{P} \geq 1 - 1/\sqrt{p}$ (*no pairings!*).

Numbers attached to a curve (II)

Twist cardinality

In general, the *twist cardinality* N' has at least a prime divisor $\geq (\log p)^{O(1)}$.

DLOG in the base field

- The base field cardinality p should be **pseudo-random** (*no fast reduction!*).
- $p - 1$ has a prime divisor $\geq (\log p)^2$ with $\mathcal{P} \geq 1 - 1/\sqrt{p}$.

Summary

	NIST	Brainpool	ANSSI	OSCCA
N prime	✓	✓	✓	✓
p ordinary		✓	✓	✓
Complete law				
Twist secure				
Generic		✓	✓	✓
	NUMS	**Curve25519/41417**	**Ed448-Goldilocks**	
N prime				
p ordinary				
Complete law	✓	✓	✓	
Twist secure	✓	✓	✓	
Generic				

Optimized implementation

- Curves with $N < p$ points (half of them).
- Fast computation of *square roots* ($p \neq 3 \pmod 4$).
- Fast modular *reduction* (special primes, *inefficient masking!*).
- *Small coefficients* for the curve equation (*no genericity!*).
- Specific system of *coordinates* (some entail *no prime cardinality!*).

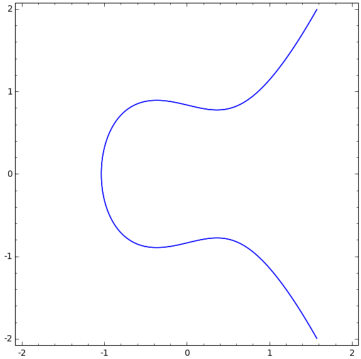
Different criteria for different uses

- The aforementioned criteria are **conflicting**.
- In particular, *tradeoffs* to be made between genericity/speed...
- ...but also between optimization/side-channel security.

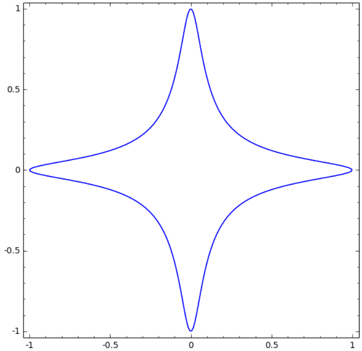
- Only the first class of criteria is mandatory to ensure the *DLOG problem difficulty*.
- The other classes of criteria mostly affect speed and ease of implementation.

Use (and standardize) **different** (families of) curves!

Real zoo

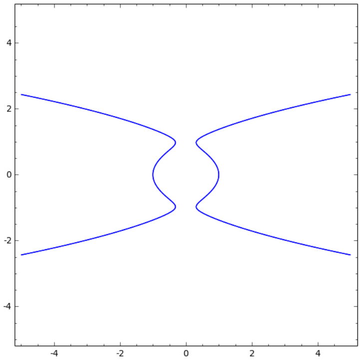


Weierstrass

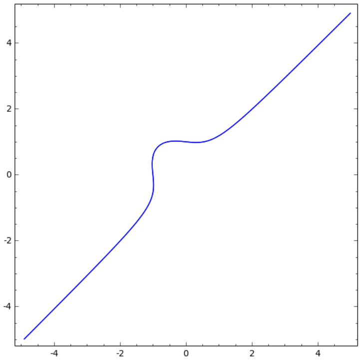


Edwards

Real zoo (II)

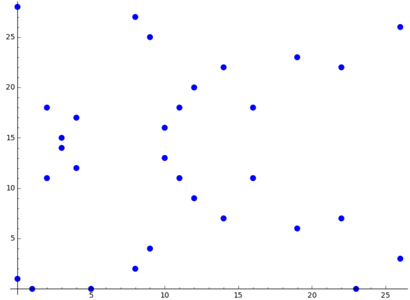


Jacobi

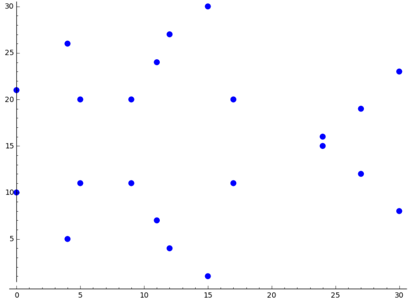


Hess

Finite field zoo

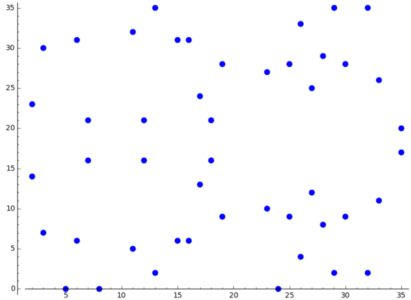


Frog

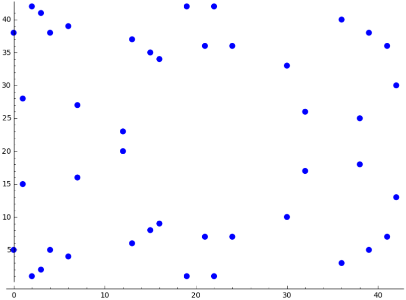


Cockroach

Finite field zoo (II)



Walrus



Bunny

III – Transparency

Architecture

- Provide curves fulfilling a selection of **criteria**...
- ...together with a **certificate** for faster verification of:
  - the number of points,
  - the discriminant and class number properties,
  - the embedding degree.

- A **deterministic** algorithm to sample curves...
- ...and producing a **certificate**:
  - Completely *reproducible* generation process.
  - Either pseudo-random (for genericity) or by enumeration of increasing values (for efficiency).
  - Certify every step, including *rejected* curves.

Cardinality of curves

Prime order

- **Certificate**: (G, q, Π) where $G = 0$ is s.t. $q \cdot G = 0$ with $q \geq p - 2\sqrt{p} + 1$, and Π a primality proof for q.
- *Size* and *verification* in $O(\log^2 p)$, generally only generated once.

Composite order

- **Certificate**: (P, n, c), where $P = 0$ is s.t. $n \cdot P = 0$ with $n < 2(\sqrt{p} - 1)^2$, and c a composition witness for n.
- *Size* in $O(\log p)$, *generation* and *verification* in $O(\log^2 p)$.
- More efficient *verification* using early-abort SEA information about small torsion points.

Example

- *Sampling function* from the **seed** s:
  - $p =$ smallest prime $\geq s$;
  - $g =$ smallest generator of $\mathbb{F}_p^\times$;
  - equations of the form $y^2 = x^3 - 3x + b$, $b = g, g^2, \ldots$.
- *Conditions*:
  - N et N' prime;
  - $\Delta = 0$, $N, N' = p, p + 1$;
  - embedding degrees of E, E' at least $p^{1/4}$;
  - class number $\geq p^{1/4}$.

Certificate

From the seed $s = 2015$: $p = 2017$, $g = 5$,

Curve

```
(2017, -3, 625)
order = 2063, point = (0, 25)
twist_order = 1973
disc_factors = {6043}
class_number = 9, form = (17,3,89)
embedding_degree = 1031, factors = {2, 1031}
twist_embedding_degree = 493, factors = {2, 17, 29}
```

Rejected curves

```
((2017, -3, 5), composite, 2065, witness, 1679, point, (1,258))
((2017, -3, 25), torsion_point, 3, point, (448, 288))
((2017, -3, 125), torsion_point, 2, point, (982, 0))
```

Non-manipulability

- Such a process produces **deterministically** a curve from:
  - a set of *conditions* (including **numerical bounds**),
  - a *sampling function* (including potential **seed**).

No *rigidity* but still **transparency**.

- Only a few *conditions* will actually affect the process:
  - twist security,
  - smoothness bounds.
- When a **seed** is needed, suspicion can be avoided:
  - using a *share-commitment* scheme;
  - using *unpredictable* and *unmanipulable* values (sports results, stock values, lottery results, sunspot observations, ...).

Seed generation

IV – Conclusion

Diversity and Transparency for ECC

Diversity

International standards should:

- not restrict to a single curve or family of related elliptic curves;
- include a “generic” elliptic curve.

Transparency

All details about the generation process should be:

- public and “transparent”;
- annonced before the actual generation.

Questions?