NATIONAL RESEARCH
UNIVERSITY

Constructing of Strong Elliptic Curves Suitable for Cryptography Applications

With Consideration of Russian Standardized Elliptic Curves

Alexey Nesterenko

anesterenko@hse.ru

HSE Tikhonov Moscow Institute of Electronics and Mathematics (MIEM HSE)

May 29th

ECDLP

Let p – prime, elliptic curve in short Weierstrass form:

$$E: \quad y^2 \equiv x^3 + ax + b \pmod{p}, \quad |E| = m = cq,$$

where $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ and q – prime.

Definition

Let $P \in E$, $| < P > | = q$ and $Q \in < P >$. ECDLP is problem of finding $k \in \mathbb{Z}_q$ such $Q = [k]P = \underbrace{P + \cdots + P}_{k \text{ times}}$.

- Complexity of ECDLP for arbitrary elliptic curve is $O(\sqrt{q})$,
- ECDLP ensure the security of:
    1. digital signatures (GOST R 34.10-2012),
    2. key agreement protocols («Echinacea» R 1323565.1.004-2017, RTLS 1.2, SP-FIOT),
    3. public key encryption schemes.

Current Conditions for Elliptic Curve Parameters

since GOST R 34.10 (2001 & 2012)

Let $\alpha \in \{254, 508\}$, $\beta \in \{256, 512\}$.

- $2^\alpha < q < 2^\beta$,
- $m \neq p$ (against Sato, Araki, Smart & Semaev attacks),
- $J(E) \not\equiv 0, 1728 \pmod{p}$, where

$$J(E) \equiv 1728 \frac{4a^3}{4a^3 + 27b^2} \pmod{p}$$

  (against degenerate form of elliptic curve),
- for fixed B the condition $p^i \not\equiv 1 \pmod{q}$ holds for all $i = 1, 2, \ldots, B$, where

$$B = \begin{cases} 31, & \text{if} \quad \beta = 256, \\ 131, & \text{if} \quad \beta = 512. \end{cases}$$

  (against MOV attack)

Attack of Petit, Kosters and Messeng (2016) uses the decomposition

$$p - 1 = \prod_{i=1} p_i^{\alpha_i}.$$

1. applicable if p_i – small,
2. based on solving a system of non-linear polynomials over $\mathbb{F}_p$, generated by Semaev's summation polynomials,
3. nowadays we don't have any practical realizations,
4. but in the future this can be done.

Attack of Nesterenko (CTCrypt 2015) uses the decomposition

$$q - 1 = \prod_{i=1} q_i^{\alpha_i}.$$

1. for every $t | (q-1)$ exists a set $S_t = \{k : \operatorname{ord}_q k = t\}$ and the complexity of ECDLP for every $k \in S_t$ is $O\big(\sqrt{t}\log(q)\big)$,
2. $|S| = \varphi(t)$, where $\varphi()$ is a Euler totient function,
3. if t is small, then keys in S_t are «weak»,
4. checking a «weakness» of k is equal to solving ECDLP and may be applied to standartized elliptic curves,
5. if we choose k randomly from $\mathbb{Z}_q$ the probability of «weakness» is very small,
6. one can construct statistically indistinguishable «weak» keys.

$$p = 2^{256} - 617, \quad a = -3, \quad b = 166.$$

1. decomposition of $p - 1 = s \times p_1$, where $\lceil \log_2(p_1) \rceil = 134$ and

$$s = 2 \times 7 \times 43 \times 9109 \times 87640387787 \times$$
$$\times 16876409960174552741.$$

2. decomposition of $q - 1 = t \times q_1$, where $\lceil \log_2(q_1) \rceil = 186$ and

$$t = 22797749453453903443262 =$$
$$= 2 \times 3 \times 7 \times 17 \times 37 \times 127 \times 121493 \times 5592900119.$$

3. hence exists exactly $t = \sum_{1 \leqslant u \leqslant t, u | t} \varphi(u)$ keys, $2^{70} < t < 2^{71}$, such the complexity of ECDLP's solution for these keys no more than $O(2^{44})$.

$$p = 2^{255} + 3225, \quad a = -3,$$

$$b = 28091019353058090096996979000309560759124368558014865957655842872397301267595.$$

1. decomposition of $p - 1$ is

$$p - 1 = 2^3 \times 11 \times 33797 \times 633062117 \times 434007492324321509 \times$$
$$\times 39607009966486015397 \times 1788843965301779500402446 7.$$

2. decomposition of $q - 1 = t \times q_1$, where $\lceil \log_2(q_1) \rceil = 189$ and

$$t = \color{red}{94673263789516324202} = 2 \times 47336631894758162101.$$

3. hence exists exactly $t = \sum_{1 \leqslant u \leqslant t, u|t} \varphi(u)$ keys, $2^{66} < t < 2^{67}$, such the complexity of ECDLP's solution for these keys no more than $O(\color{red}{2^{42}})$.

Standardized Elliptic Curves

parameters set «C» from RFC 4357

$$a = -3, \quad b = 32858.$$

$$p = 70390085352083305199547718019018437841079516630045180471284346843705633502619.$$

1. decomposition of $p - 1 = s \times p_1$, where $\lceil \log_2(p_1) \rceil = 128$ and
$$s = 2 \times 17 \times 37 \times 113 \times 244997 \times \\ \times 704476598345732707758923296\,1.$$
2. decomposition of $q - 1 = tq_1$, where $2^{137} < q_1 < 2^{138}$ and
$$t = 269835642637977294912925317964710600 = 2^3 \times 3^2 \times 5^2 \times \\ \times 47 \times 207130852417 \times 1539870360241903618 3.$$
3. hence exists exactly $t = \sum_{1 \leqslant u \leqslant t, u | t} \varphi(u)$ keys, $2^{117} < t < 2^{118}$, such the complexity of ECDLP's solution for these keys no more than $O(2^{67})$.

$$p = 2^{256} - 617 \quad \text{(as well as RFC 4357 paramsetA)}$$

$$a = 87789765485885808793369751294406841171614589925193456909855962166505018127157$$
$$b = 18713751737015403763890503457318596560459867796169830279162511461744901002515.$$

Elliptic curve has order $m = 4q$ and $q - 1 = tq_1$, where $2^{242} < q_1 < 2^{243}$ and

$$t = 3194 = 2 \times 1597 \times q_1,$$

Hence exists exactly $t = 3194$ keys, $2^{11} < t < 2^{12}$, such the complexity of ECDLP's solution for these keys no more than $O(2^{14})$.

Definition of Strong Elliptic Curves

Note:

p is a *safe* prime, if p is a prime and $\frac{p-1}{2}$ is a prime.

Definition

E is a strong elliptic curve if conditions from GOST R 34.10 holds and p and q are safe primes.

Note:

It's seems like RSA modulus m where $m = pq$ and p, q are safe primes.

Definition of Strong Elliptic Curves

Additional Condition for Endomorphisms Ring. Part I

Every strong elliptic curve has «complex multiplication», i.e.

- Let $P, Q \in E$ and $\tau : E \to E \in End(E)$ endomorphism:

$$\tau(\mathcal{O}) = \mathcal{O}, \quad \tau(P+Q) = \tau(P) + \tau(Q),$$

- Let $\tau, \mu \in End(E)$. We can define $\tau(P) + \mu(P)$ - addition, $\tau(\mu(P))$ - multiplication $\Rightarrow$ End(E) is a ring,
- $End(E)$ is isomorphic to some order $o_{\mathbb{K}} \subseteq \mathbb{K} = \mathbb{Z}[\sqrt{-\Delta}] \subset \mathbb{Q}(\sqrt{-d})$, $\Delta = \begin{cases} d, & \text{if} \quad d \equiv 1 \pmod 4, \\ 4h, & \text{if} \quad d \equiv 2, 3 \pmod 4. \end{cases}$ and $d > 1$ is square free.
- if $P = P(x, y)$ and $\tau \in o_{\mathbb{K}} = \{1, \omega\}$, then

$$\tau(P) = \left(f(x), \frac{y \cdot f'(x)}{\tau} \right), \text{ where } f(x) = \frac{u(x)}{w(x)},$$

$u(x), w(x) \in \mathbb{H} = \mathbb{K}(j(\omega))$, $\deg u(x) = N(\tau)$, and $\tau(P) = [\tau]P$ multiplication on complex number τ.

- Examples of endomorphisms:
  - $[k]P = P + \cdots + P$,
  - Let $P = P(x, y)$. Frobenius endomorphism is $\phi(P) = (x^p, y^p)$ and $N(\phi) = p$.
- Every $\mathbb{Z}[\sqrt{-\Delta}]$ has finite order h of group of classes of ideals, called «class number» and $[\mathbb{H} : \mathbb{K}] = h$, where $\mathbb{H} = \mathbb{K}(j(\omega))$ – Hilbert class field, $\omega \in \mathbb{Z}[-\Delta]$ and j is a modular function.

Definition

E is *very strong* if

1. the class number of $\mathbb{Z}[\sqrt{-\Delta}]$ should[1] be at least $h = 200$.

Note:

Nowadays we don't know a method of solving ECDLP based on theory of complex multiplication. But we know that construction of $\tau \in o_{\mathbb{K}}$ such $Q = \tau(P) = [\tau]P$ is equivalent to solving ECDLP.

[1] Technical Guideline TR-03111. Elliptic curve cryptography. German Federal Office for Information Security. 2007.

Definition

Elliptic curve $\hat{E}$ is a twist of E, $End(E) \subseteq \mathbb{Z}(\sqrt{-\Delta}) \subset \mathbb{Q}(\sqrt{-d})$, if

- $j(\hat{E}) = J(E)$,
- $|\hat{E}| = p + 1 - \delta x$, where $4p = x^2 + dy^2$ and

$$|E| = m_\delta = p + 1 + \delta x, \quad 0 < x < 2\sqrt{p}, \quad \delta \in \{-1, 1\}.$$

Since $\hat{E} \sim E$ over $\mathbb{H}$ we can hope that ECDLP on E has the same complexity as ECDLP on $\hat{E}$.

Definition

E is *very strong* if

2. $\hat{E}$ has order $m_{-\delta} = cr$, $2^\alpha < r < 2^\beta$ and r is safe prime[2].

[2] Similar property was introduced by D.Bernstein for Curve25519 — r must be prime.

Methods of Construction

Basic ways to construct:

1. construct safe prime p,
2. choose one variant from follows:
   2.1 generate random or pseudorandom $a, b \in \mathbb{F}_p$ and evaluate $|E|$ with SEA algorithm,
   2.2 construct safe q and evaluate a, b with theory of complex multiplication.

- The first way has property of «provable pseudorandomness» when

$$a \equiv -3 \pmod{p}, \quad b \equiv Hash(\xi) \pmod{p}$$

  for some ξ and small probability of success.
- We use the second way since he may be described as rigidious algorithm.
- Both ways are exactly deterministic algorithms.

A CM-Theory Algorithm

Step I: Finding appropriate values of p and q for given $0 < \alpha < \beta$

1. Consider a sequence $p_n = p_0 - 12n$, where $p_0 \equiv 11 \pmod{12}$, $p_0 < 2^\alpha$ and $n = 1, 2, \ldots$
2. For every safe prime p_n try to solve Cornaccia's equation

$$4p_n = x^2 + dy^2,$$

   for natural $x, y > 1$ and square free integer $d = 2, 3, 5, 6, \ldots, 10^6$ (this value is algorithm parameter).

3. Define $m_\delta = p + 1 + \delta x$, $\delta \in \{-1, 1\}$, and check

$$m_\delta = cq, \quad 2^\alpha < q < 2^\beta, \quad q - \text{safe}.$$

4. Since $\mathrm{ord}_q p | (q-1) = 2q_1$, q_1 - prime, we check only

$$p^2 \not\equiv 1 \pmod{q}$$

   for GOST R 34.10-2012 conditions (q_1 or $2q_1$ is a MOV degree).

1. Consider $o_{\mathbb{K}} = \{1, \omega\} \subseteq \mathbb{Z}[\sqrt{-\Delta}]$. Let $\eta(z)$ is Dedekind function and $\mathfrak{f}_1(z)$ is Weber function

$$\eta(z) = q^{24} \prod_{n=1}^{\infty}(1 - q^n), \quad \mathfrak{f}_1(z) = \frac{\eta(2z)}{\eta(z)}, \quad \text{where } q = e^{2\pi i z},$$

   then modular function j defined by equation

$$j(z) = \frac{(\mathfrak{f}_1(z)^{24} + 16)^3}{\mathfrak{f}_1(z)^{24}}.$$

2. Since $j(\omega)$ is an algebraic number, $\deg j(\omega) = h$ we can construct polynomial $H_d(x) \in \mathbb{Z}[x]$ for which the equality $H_d(j(\omega)) = 0$ holds and $\deg H_d(x) = h$.
3. Find and sort in ascending order all roots of $H_d(x)$ modulo p.

4. Every root j_p means as j-invariant of elliptic curve E over $\mathbb{F}_p$, hence find first k, such $-k^{-1}$ is quadratic residue modulo p, where

$$k \equiv \frac{j_p}{1728 - j_p} \pmod{p}.$$

5. The coefficients a, b is satisfy to equalities

$$\begin{cases} a \equiv 3ku^2 \equiv -3 \pmod{p}, \\ b \equiv 2ku^3 \pmod{p}, \end{cases}$$

where $u < p - u$ and $u^2 \equiv -k^{-1} \pmod{p}$.

6 Since $p = 12n + 11$ we have $\left(\frac{-1}{p}\right) \equiv -1 \pmod{p}$ then u or $-u$ is non quadratic residue modulo p (one can write εu, $\varepsilon \in \{-1, 1\}$) and

$$\hat{a} = -3, \quad \hat{b} \equiv -b \pmod{p}$$

is a coefficients of twist $\hat{E}$.

7. Using SEA algorithm one can check which curve has order $m_\delta = cq$.

Algorithm realization

with Magma code example

- Step I was written by author in C++ code.
- Step II was written by author in Magma like this

```
𝔽_p := GF(p);
R<x> := PolynomialRing(𝔽_p);
fp := R!HilbertClassPolynomial(Δ);
for j_p in Roots(fp) do
  k := j_p[1]*(F!Modinv( Integers()!(1728 - j_p[1]), p ));
  if JacobiSymbol( Integers()!(-k), p) eq 1 then
    c := Modinv( Modsqrt( Integers()!(-k), p ), p);
    ec := EllipticCurve( [K!(3*k*c^2), K!(2*k*c^3)]);
    m := Order(ec);
    if m eq m_δ then
      return true;
    end if;
  end if;
end for;
```

- Dual core IntelCore i5 processor with 4 Gb Memory and some days of calculations.

Results of practical experiments
Statistics

For fixed $\alpha = 254$, $\beta = 256$.
We test all integers $p = 2^{256} - t$, where

$$p \equiv 11 \pmod{12} \quad \text{and} \quad 5 \leq t < 100.000.000 = 10^8.$$

We found:

- 116014 — primes,
- 879 — safe primes,
- 22 — «strong» elliptic curves,
- 7 — elliptic curves, with classs number $h > 200$,
- 0 — very «strong» curves.

Results of practical experiments

Elliptic Curves

$$E : y^2 \equiv x^3 - 3x + 2k\varepsilon u^3 \pmod p, \quad p = 2^{256} - t, \quad |E| = m_\delta,$$

where

- $m_\delta = p + 1 + \delta x = cq$, $4p = x^2 + dy^2$, $2^{254} < q < 2^{256}$,
- $k \equiv \frac{j_{p,j}}{1728 - j_{p,i}} \pmod p$, $j_{p,i}$ – i-th root $H_d(x)$ modulo p,
- $u^2 \equiv -k^{-1} \pmod p$, deg $H_d = h$, $\delta, \varepsilon \in \{-1, 1\}$.

number	t	d	δ	c	h	i	ε	$log_2 r$
4	5460857	640030	-1	2	544	1	1	139
9	34771673	338062	1	2	224	1	-1	58
14	48208517	580907	-1	3	240	1	1	117
16	57688733	760618	1	2	446	2	-1	184
18	63233777	939262	1	2	272	2	1	78
19	78045197	822155	-1	3	308	2	1	88
21	90054089	935518	-1	2	576	2	1	147

where $|\hat{E}| = m_{-\delta} = \hat{c}r$, r — greater prime.

Let $m_{+1} = p + 1 + x = 2q$ and $m_{-1} = p + 1 - x = 2r$, $q > r \Rightarrow$

Question:

How to find $q + r = p + 1$, where p, q, r — safe primes.

$$\begin{aligned} 3 + 5 &= 7 + 1 \\ 5 + 7 &= 11 + 1 \\ 7 + 13 &= 19 + 1 \\ 13 + 11 &= 23 + 1 \\ 17 + 31 &= 47 + 1 \\ &\dots \end{aligned}$$

No more found for $5 \le q, r < 10^8$:((

Thank You for Attention! Questions?