On the security properties of the Russian standardized elliptic curves

Vasily D. Nikolaev,
Engineer-analyst,
CryptoPro

Evgeny K. Alekseev, Ph. D., CryptoPro

Stanislav V. Smyshlyaev, Ph. D., CryptoPro

CTCrypt 2017

Elliptic curve generation problem

Why?

- New national digital signature standard adopted in 2012.
- It does not set any parameter set explicitly.

Elliptic curve generation problem

Why?

- New national digital signature standard adopted in 2012.
- It does not set any parameter set explicitly.

How?

- Discussing and obtaining methodics.
- Generating elliptic curves.
- Creating new documents (TC26 Methodical recommendations, Standardization recommendations).

Adopted documents

- RFC 4357. «Additional cryptographic algorithms for use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 algorithms». V. Popov et al.

Adopted documents

- RFC 4357. «Additional cryptographic algorithms for use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 algorithms». V. Popov et al.
- TC26 Methodical recommendations. «Elliptic curve parameters according to GOST R 34.10-2012».
- TC26 Methodical recommendations. «Twisted Edwards curve parameters according to GOST R 34.10-2012».
- RFC 7836. «Guidelines on the cryptographic algorithms to accompany the usage of standards GOST R 34.10-2012 and GOST R 34.11-2012». S. Smyshlyaev et al.

Security analysis in known models was done prior to the adoption of the documents.

Adopted documents

In 2016 a joint document by the WG «Cryptographic protocols and accompanying algorithms» (S. V. Smyshlyaev and V. A. Shishkin) was provided to Rosstandart.

Before that security properties of all curves were revised according to the new security models.

The document was adopted as:
Standardization Recommendations R 50.1.114-2016 «Elliptic curve parameters for cryptographic algorithms and protocols».

Plans to update this document including adding the curves from RFC 4357. «Old» curves will be provided new OIDs with «id-tc26-gost-3410-».

Notation

Curve forms

- Short Weierstrass form $y^2 = x^3 + ax + b$.
- Twisted Edwards form $\varepsilon u^2 + v^2 = 1 + \delta u^2 v^2$.

- $\mathbb{F}_p$ – base field.
- m – the order of the elliptic curve points group.
- q – the order of the prime subgroup of the elliptic curve points group.
- P – base point.

Major approaches

1. Generating curve with pre-selected properties (e.g. CM-method).
2. Iterative curve generation methods.

Iterative methods

1. Random selection.
2. Random value hashing.
3. Partly random methods.
4. Fully determined (rigid) methods.

Iterative methods

All Russian elliptic curves were generated using random value hashing method.

Although sometimes criticized (e.g. BADA55EC), hardly believed to be vulnerable.

How was it done in Russia?

Curve generation algorithm

1. Select p that allows fast arithmetic.
2. Select random *seed*.
3. Put $h = hash(seed)$.
4. Put $k = a^3/b^2 = h$ and $a = -3 \bmod p$ for short Weierstrass and $\varepsilon = 1$ and $\delta = h$ for twisted Edwards curves.
5. Check cryptographic properties. Goto 2 if something is wrong.
6. Select base points, iterating abscissa from 0.

Russian standardized curves

«Old curves»

RFC 4357, 256-bit short Weierstrass

- id-GostR3410-2001-CryptoPro-A-ParamSet
- id-GostR3410-2001-CryptoPro-B-ParamSet
- id-GostR3410-2001-CryptoPro-C-ParamSet

Russian standardized curves

«Old curves»

RFC 4357, 256-bit short Weierstrass

- id-GostR3410-2001-CryptoPro-A-ParamSet
- id-GostR3410-2001-CryptoPro-B-ParamSet
- id-GostR3410-2001-CryptoPro-C-ParamSet

«New curves»

Standardization Recommendations R 50.1.114-2016,

- id-tc26-gost-3410-12-512-paramSetA, 512-bit short Weierstrass
- id-tc26-gost-3410-12-512-paramSetB, 512-bit short Weierstrass
- id-tc26-gost-3410-2012-256-paramSetA, 256-bit twisted Edwards
- id-tc26-gost-3410-12-512-paramSetC, 512-bit twisted Edwards

GOST R 34.10-2001/2012

Some properties are explicitly set by national standards.

1. $2^{254} < q < 2^{256}$ for 256 bit curves and $2^{508} < q < 2^{512}$ for 512 bit curves.
2. P belongs to the curve and $\operatorname{ord} P = q$.
3. $4 \cdot a^3/b^2 + 27 \neq 0$.
4. $b \neq 0$.
5. $a^3/b^2 \neq 0$.

All adopted curves satisfy this condition.

Additive transfers

$(m, p) = 1$

If it is not hold, there exists an efficient isomorphism between G and additive group F_p (Semaev, 1998).

Calculating in $O(ln(p))$ – then solving ECDLP in polynomial time!

All adopted curves satisfy this condition.

Similar results by Satoh-Araki (1998) and Smart (1999).

Multiplicative transfers

ord p in $\mathbb{F}_q^*$ should not be small.

If the criterion is not met, there exists an efficient isomorphism between G and multiplicative embedding group $\mathbb{F}_{q^t}^*$, $t \in \mathbb{N}$.

Firstly proposed by Menezes-Okamoto-Vanstone, 1993.

All adopted curves satisfy this condition.

CM discriminants

Complex multiplication discriminant should not be small.

If not met then there exist efficient automorphisms that can be used for speedups in Pollard's ρ-method.

SafeCurves require $D > 2^{100}$.
It is met for all the curves except for
id-GostR3410-2001-CryptoPro-B-ParamSet.

Twist security

The «largest» non-trivial quadratic twist group subgroup should be «safe».

One-coordinate Montgomery ladder formulae are equivalent for the curve and it's twist.
We simply check all the already mentioned properties for the twist.

Three curves do not met the requirement.

- id-GostR3410-2001-CryptoPro-A-ParamSet
- id-GostR3410-2001-CryptoPro-C-ParamSet
- id-tc26-gost-3410-12-512-paramSetB

But they also cannot be rewritten in Montgomery form!

Petit-Kosters-Messeng method

F_p^* should not have too many «small» subgroups.

Suppose $p - 1 = p_1 \cdot \ldots \cdot p_s$, where all p_i are primes. Fix $B \in \mathbb{N}$, $k = \log_2(\prod_{j=1}^{n'} p_{i_j}) + 1$, where $p_{i_j} \in \{p_1, \ldots, p_s\}$, $p_{i_j} < B$ and $n = \lfloor \log_2(p) \rfloor$, $m = \lfloor n/k \rfloor$. $d_{max} = max\{4, p_{i_1}, \ldots, p_{i_{n'}}\}$.

Heuristic Estimation

If for every $B < n/4$ the following inequality holds:

$$k + m(\log_2 m - 1) + 2d_{max} \log_2 mn' > n/2,$$

then Petit-Kosters-Messeng method is at least as hard as Pollard's ρ-method.

The main approach

Use factor bases algorithm.

Algorithm

1. $\Omega = \{P_1, \ldots, P_N\}$ – factor base.
2. Build $N + 1$ decompositions with $m \in \mathbb{N}$ points in each.
   $[\alpha_i]P \oplus [\beta_i]Q = \bigoplus_{j=1}^{m} W_j,\ W_j \in \Omega,\ \alpha_i, \beta_i \in_R \{1, \ldots, q-1\}$
3. Build relation matrix.
4. Deduce the value of discrete logarithm using linear algebra.

Building relations

Use summation polynomials (Semaev, 2004).

Definition

$S_i(x_1, \ldots, x_i) \in \mathbb{F}_p[x_1, \ldots, x_i]$, $i \geq 2$, turns to 0 on $x_1, \ldots, x_i \in \mathbb{F}_p \iff \exists y_1, \ldots, y_i \in \overline{\mathbb{F}}_p$: $(x_1, y_1) \in E(\overline{\mathbb{F}}_p), \ldots, (x_i, y_i) \in E(\overline{\mathbb{F}}_p)$ such that $\bigoplus_{j=1}^{i}(x_j, y_j) = O$.

S_2 and S_3 are explicitly defined, other polynomials are given through resultant notation.

All summation polynomials are symmetric and S_i has total degree at most $i \cdot 2^{i-2}$ when $i > 2$.

Factor bases

Ordinary factor bases

When base field is $\mathbb{F}_{p^n}$, select $k \in \mathbb{N}$, such that $1 \leq k \leq n$.

$P \in \Omega \iff x(P) \in V,\ \dim V = k.$

Factor bases

Ordinary factor bases

When base field is $\mathbb{F}_{p^n}$, select $k \in \mathbb{N}$, such that $1 \leq k \leq n$.

$P \in \Omega \iff x(P) \in V,\ \dim V = k.$

Non-trivial factor base.

$P \in \Omega \iff x(P) \in G'$, where $G' = G'_1 \times \cdots \times G'_{n'} \subset \mathbb{F}_p^*$.

Factor bases

Ordinary factor bases

When base field is $\mathbb{F}_{p^n}$, select $k \in \mathbb{N}$, such that $1 \leq k \leq n$.

$P \in \Omega \iff x(P) \in V,\ \dim V = k.$

Non-trivial factor base.

$P \in \Omega \iff x(P) \in G'$, where $G' = G'_1 \times \cdots \times G'_{n'} \subset \mathbb{F}_p^*$.

$$\begin{cases} x_{i,j+1} - x_{i,j}^{p_j} = 0, i = 1, \ldots, m,\ j = 1, \ldots n' - 1 \\ x_{i,n'}^{p_{n'}} - 1 = 0, i = 1, \ldots, m \end{cases} \tag{1}$$

Equation system

The original system.

Defined over $\mathbb{F}_p$, consists of $mn' + 1$ equations with mn' variables:

$$\begin{cases} S_{m+1}(x_{1,1}, \ldots, x_{m,1}, R_x) = 0 \\ x_{i,j+1} - x_{i,j}^{p_j} = 0, i = 1, \ldots, m, \ j = 1, \ldots n' - 1 \\ x_{i,n'}^{p_{n'}} - 1 = 0, i = 1, \ldots, m \end{cases} \quad (2)$$

Maximal degree of equation: $max(B, (m+1) \cdot 2^{m-1})$.

Equation system

The new system.

Defined over $\mathbb{F}_p$.

$$\begin{cases} S_3(x_{1,1}, x_{2,1}, u_1) = 0 \\ S_3(u_i, x_{i+2,1}, u_{i+1}) = 0, \ \ i \in 1, \ldots, m-3 \\ S_3(u_{m-2}, x_{m,1}, R_X) = 0 \\ x_{i,j+1} - x_{i,j}^{p_j} = 0, \ \ i = 1, \ldots, m, \ \ j = 1, \ldots n' - 1 \\ x_{i,n'}^{p_{n'}} - 1 = 0, \ \ i = 1, \ldots, m \end{cases} \tag{3}$$

$mn' + m - 1$ equations with $mn' + m - 2$ variables.
Maximal degree of equation: $max(B, 4)$.

Solving equation system

Solve the system using F_4.

What complexity do we have?

Solving equation system

Solve the system using F_4.

What complexity do we have?

Petit, Kosters and Messeng: «firstfall degree» assumptions seem not to be adequate.

Solving equation system

Solve the system using F_4.

What complexity do we have?

Petit, Kosters and Messeng: «firstfall degree» assumptions seem not to be adequate.

So we try to use some lower bound.

Common complexity estimations

- $T_{ECDLP} = T_{factor} + T_{Sem} + N \cdot P_{PDP}^{-1} T_{trial} + T_{GE}$

Common complexity estimations

- $T_{ECDLP} = T_{factor} + T_{Sem} + N \cdot P_{PDP}^{-1} T_{trial} + T_{GE}$
- $T_{factor} = O(2^{c_1 n^{1/3} \log_2^{2/3} n})$
- $T_{Sem} = O(2^{m^2})$
- $T_{GE} = O(mnN^{\omega'}), \omega' \leq 2$

Common complexity estimations

- $T_{ECDLP} = T_{factor} + T_{Sem} + N \cdot P_{PDP}^{-1} T_{trial} + T_{GE}$
- $T_{factor} = O(2^{c_1 n^{1/3} \log_2^{2/3} n})$
- $T_{Sem} = O(2^{m^2})$
- $T_{GE} = O(mnN^{\omega'}), \omega' \leq 2$
- $P_{PDP} = O(2^{mk-n}/m!)$
- $N = O(2^k)$
- $T_{trial} = O(V^{\omega D_{reg}})$

Regularity degree

What is the value of D_{reg}?

Regularity degree

What is the value of D_{reg}?

No idea, but D_{reg} should be at least as large as the largest degree of polynomial.

Experiments show we are extremely conservative!
$p = 36497 \approx 2^{15}$, $m = 4$, $n' = 4$ and $D_{reg} = 25 \gg 4$.

Complexity estimations

Inequality system

$$\begin{cases} mk = n & (4a) \\ m^2 < n/2 & (4b) \\ 2B < n/2 & (4c) \\ k + m(\log_2 m - 1) + 2d_{max} \log_2 mn' < n/2 & (4d) \end{cases}$$

Complexity estimations

Inequality system

$$\begin{cases} mk = n & \text{(4a)} \\ m^2 < n/2 & \text{(4b)} \\ 2B < n/2 & \text{(4c)} \\ k + m(\log_2 m - 1) + 2d_{max} \log_2 mn' < n/2 & \text{(4d)} \end{cases}$$

The criterion is checked for all divisor sets of $p - 1$ for all Russian curves.

PKM method turns out to have greater complexity then Pollard's ρ for all adopted curves.

On the correctness of criterion

Is the criterion correct? Are there any curves that satisfy it?

On the correctness of criterion

Is the criterion correct? Are there any curves that satisfy it?

Yes, for example NIST P-224 with $p = 2^{224} - 2^{96} + 1$ has such divisor sets.
Are there any real security problems?

On the correctness of criterion

Is the criterion correct? Are there any curves that satisfy it?

Yes, for example NIST P-224 with $p = 2^{224} - 2^{96} + 1$ has such divisor sets.
Are there any real security problems? Still unknown.

Conclusion

- Security properties revised:
  - Compliance with GOST R 34.10-2001/12.
  - Security against additive and multiplicative transfers.
  - CM-security.
  - Twist security.
  - Resistance to Petit-Kosters-Messeng method.
- Russian standardized curves remain secure.

CRYPTOPRO

Thank you for your attention!

Questions?

- Materials, questions, comments:
  - nikolaev@cryptopro.ru
  - alekseev@cryptopro.ru
  - svs@cryptopro.ru