A. Yu. Nesterenko, Построение стойких эллиптических кривых для криптографических приложений,
Матем. вопр. криптогр., 2019, том 10, выпуск 2, 135–144

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2019 Т. 10 № 2 С. 135–144

УДК 519.719.2 DOI https://doi.org/10.4213/mvk291

Construction of strong elliptic curves suitable for cryptographic applications

A. Yu. Nesterenko

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

Получено 06.II.2018

Abstract. An algorithm for the construction of elliptic curves satisfying special requirements is presented. The choice of requirements aims to prevent known attacks on the elliptic curve discrete logarithm problem in special cases. The results of practical experiments are discussed, some parameters of concrete elliptic curves are given.

Key words: elliptic curve, discrete logarithm problem, complex multiplication

Построение стойких эллиптических кривых для криптографических приложений

А. Ю. Нестеренко

Московский институт электроники и математики им. А. Н. Тихонова Национального исследовательского университета «Высшая школа экономики» (МИЭМ НИУ ВШЭ), Москва, Россия

Аннотация. Рассматривается новый алгоритм построения эллиптических кривых, параметры которых удовлетворяют ГОСТ Р 34.10-2012, а также ряду дополнительных условий. Эти условия вводятся для противодействия известным атакам на задачу дискретного логарифмирования, использующим специальный вид параметров эллиптических кривых. Приводятся результаты практических вычислений и конкретные эллиптические кривые, удовлетворяющие введенным условиям.

Ключевые слова: эллиптические кривые, задача дискретного логарифмирования, комплексное умножение

Citation: *Mathematical Aspects of Cryptography*, 2019, v. 10, № 2, pp. 135–144 (Russian)

1. Motivation

Let $p > 3$ be a prime. Consider an elliptic curve given in a short Weierstrass form by the equation

$$E_{a,b}: \quad y^2 \equiv x^3 + ax + b \pmod{p}, \tag{1}$$

where $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$. We will say that $E_{a,b}$ is defined over prime field $\mathbb{F}_p$. Let $P = (x, y)$ be a fixed point on $E_{a,b}$ and q is an order of P, i. e.

$$[q]P = \underbrace{P + \cdots + P}_{q \text{ times}} = \mathcal{O},$$

where $\mathcal{O}$ is a neutral element of the group of elliptic curve points. We suppose that q is prime and $q|m$, where $m = |E_{a,b}|$ is a number of all points on the elliptic curve $E_{a,b}$. From Hasse theorem, see [25, Ch. 5], we know that

$$p + 1 - 2\sqrt{p} < m < p + 1 + 2\sqrt{p}.$$

We can define an elliptic curve discrete logarithm problem (ECDLP) as the problem of searching an integer $k \in \mathbb{F}_q^*$ such that $Q = [k]P$ and $Q \in \langle P \rangle$.

To solve this problem (see [5, 28]) we can use Pollard's Rho and Lambda methods [19] or parallel algorithm introduced by van Oorschot and Wiener [16]. These algorithms have the running time $O(\sqrt{q})$ and may be applied to any elliptic curve.

In special cases we can use methods with lower running time. When the condition $m = p$ holds we can use methods of Sato, Araki [22], Smart [26] or Semaev [24] to solve the ECDLP in linear time.

If the multiplicative order of p modulo q is small we may apply MOV-attack (Menezes, Okamoto, Vanstone, see [12]) and solve ECDLP with lower running time using the calculations in multiplicative group of some finite extension of $\mathbb{F}_p$.

In 2016 a new method for solving ECDLP was proposed by Petit, Kosters and Messeng, see [17]. This method is based on solving a system of non-linear polynomials over $\mathbb{F}_p$, generated by Semaev's summation polynomials, and may be applied in case when $p - 1$ is smooth, i. e. $p - 1$ has many small divisors. Nowadays we don't have any practical realizations of this method for some value of p, but in the future this may be done.

At the same time Nesterenko had presented a new method for solving ECDLP wich running time depending on the multiplicative order of secret value k modulo q, see [15]. If t is a divisor of $q - 1$ then solving ECDLP has running time $O(\sqrt{t}\log q)$, hence if $q - 1$ has many small divisors then [15] shows that ECDLP may be efficiently solved for many "weak" values of k.

For example, consider the three elliptic curves defined by [18]. All these curves has the form

$$y^2 \equiv x^3 - 3x + b \pmod{p}.$$

The orders of these curves are primes q satifying the condition $q - 1 = t \times q_1$ for some large prime q_1 and composite even integer t. It's clear that t gives us a capacity of "weak" values of k. We present some parameters of these curves in following table.

set	b	p	t
"A"	166	$2^{256} - 617$	$2 \cdot 3 \cdot 7 \cdot 17 \cdot 37 \cdot 127 \cdot 121493 \cdot 5592900119$
"B"	see [18]	$2^{255} + 3225$	$2 \cdot 47336631894758162101$
"C"	32858	see [18]	$2^3 \cdot 3^2 \cdot 5^2 \cdot 47 \cdot 207130852417 \cdot 15398703602419036183$

We see that every curve from [18] has a large set of "weak" keys which makes these curves useless for real security applications.

2. Definitions

On this basis we can lay down conditions on parameters of elliptic curve $E_{a,b}$ which guarantee the impossibility to apply methods referred above.

Definition 1. Let $0 < \alpha < \beta$ are natural numbers. The elliptic curve $E_{a,b}$ defined by the equation (1) is called *strong* elliptic curve if there exists a point $P \in E_{a,b}$ with $|\langle P \rangle| = q$ and the following conditions hold:

1) $m \neq p$,
2) p is safe prime, i. e. $(p-1)/2$ is also prime,
3) $j(E_{a,b}) \not\equiv 0$ or $1728 \pmod{p}$, where
$$j(E_{a,b}) \equiv 1728 \frac{4a^3}{4a^3 + 27b^2} \pmod{p},$$
4) q is safe prime, i. e. $(q-1)/2$ is also prime,
5) $2^\alpha < q < 2^\beta$,
6) for fixed B the condition $p^t \not\equiv 1 \pmod{q}$ holds for all $t = 1, 2, \ldots, B$.

It is clear that conditions of safety for p and q in definition 1 are supplementary to conditions in [10]. We have a situation similar to RSA modulus $N = pq$, where p and q needs to be safe, see [21].

The constants α, β and B may be chosen in different ways. In [10] we can find $\alpha = 254, \beta = 256$ and $B = 31$ or $\alpha = 508, \beta = 512$ and $B = 131$. In [27] we can find another values $\alpha = 224, \beta > \alpha$ and $B = 10^4$.

Also remark that for safe prime p the condition $j(E_{a,b}) \not\equiv 0$ or 1728 gives us inequality $m \neq p + 1$, see [9, Ch.13].

Furthermore, using unproved assumptions we can give more rigorous conditions in terms of theory of complex multiplication on elliptic curves, see [9, 25].

2.1. Complex multiplication

For every elliptic curve $E_{a,b}$ one can define a ring of endomorphisms $\mathrm{End}(E_{a,b}) = \{\tau : E_{a,b} \to E_{a,b}\}$, where τ is morphism and $\tau(\mathcal{O}) = \mathcal{O}$, $\tau(P+Q) = \tau(P) + \tau(Q)$, for any points $P, Q \in E_{a,b}$.

If elliptic curve $E_{a,b}$ comply with conditions of [10], see [9, Ch. 12], then $\mathrm{End}(E_{a,b})$ is isomorphic to some order $o_{\mathbb{K}} \subseteq \mathbb{Z}[\sqrt{-\Delta}] \subset \mathbb{Q}(\sqrt{-d})$, where $d > 1$ is a square free integer and

$$\Delta = \begin{cases} d, & \text{if} \quad d \equiv 1 \pmod 4, \\ 4d, & \text{if} \quad d \equiv 2, 3 \pmod 4. \end{cases}$$

We will say that the order $o_{\mathbb{K}}$ is defined by basis $\{1, \omega\}$, where $\omega \in \mathbb{Z}[-\Delta]$. Let j be a modular function and $\mathbb{H} = \mathbb{Q}(j(\omega), \sqrt{-d})$ be a Hilbert class field.

Following [7] we know that every morphism τ may be represented as map

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

for any point $P = P(x, y) \in E_{a,b}$ and some rational function $f(x) \in \mathbb{H}(x)$. The method of constructing $f(x)$ may be found in [14].

Every ring $\mathbb{Z}[\sqrt{-\Delta}]$ has finite order h of group of classes of ideals called "class number" and $h = [\mathbb{H} : \mathbb{Q}(\sqrt{-d})]$. The value of class number h is crucial for efficiency of arithmetical operations in $\mathbb{H}(x)$.

Nowadays we don't know a method for solving ECDLP using calculations in the ring $\mathrm{End}(E_{a,b})$. But the construction of endomorphism τ such that $Q = \tau(P)$ is equivalent to solving ECDLP for given point $Q = [k]P$. Based on this considerations we propose to bound a minimal value of h.

This idea was first proposed in Technical Guideline [27], where one can find an appropriate bound $h = 200$. More impulsive conditions were offered in [4]. Bernstein and Lange had stated that the fundamental discriminant Δ of $\mathbb{Z}[\sqrt{-\Delta}]$ should satisfy inequality $|\Delta| > 2^{100}$. This limitation makes calculations in the ring $\mathrm{End}(E_{a,b})$ fully inapplicable for solving ECDLP from practical viewpoint. We hope that inequality $h > 500$ is sufficient.

2.2. Twist of elliptic curve

Recall, see [9, Ch. 13], that twist of elliptic curve $E_{a,b}$ defined over filed $\mathbb{F}_p$ is an elliptic curve $\widehat{E}_{a,b}$ defined over the same field such that:

1) $J(\widehat{E}_{a,b}) = J(E_{a,b})$,
2) $|\widehat{E}_{a,b}| = p + 1 - \delta x$, where $4p = x^2 + dy^2$, $0 < x < 2\sqrt{p}$, and

$$|E_{a,b}| = m_\delta = p + 1 + \delta x, \quad \delta \in \{-1, 1\}. \tag{2}$$

Since $\widehat{E}_{a,b}$ is isomorphic to $E_{a,b}$ over small finite extension of $\mathbb{F}_p$, see [9, 25], we can suppose that ECDLP for $E_{a,b}$ and $\widehat{E}_{a,b}$ has the same complexity. Hence we would to expect that $|\widehat{E}_{a,b}|$ has a large safe prime divisor r.

Note that every safe prime $p > 7$ satisfies the condition $p \equiv 11 \pmod{12}$. Since odd prime $p = 2p_1 + 1$, where $p_1 = 2p_2 + 1$ is also odd prime, we immediately have $p \equiv 3 \pmod 4$.

From the other hand if condition $p \equiv 1 \pmod 3$ holds we have equality $p = 3s+1 = 2p_1+1$ for some natural integer s or $3s = 2p_1$. The last equality doesn't hold since 3 and p_1 are coprime, hence $p \equiv 2 \pmod 3$ and $p \equiv 11 \pmod{12}$.

Consider the orders m_δ and $m_{-\delta}$ of elliptic curve $E_{a,b}$ and its twist $\widehat{E}_{a,b}$. Let p, q be a safe primes and $m_\delta = uq, \quad m_{-\delta} = vr$ for large prime r and natural integers u, v. Suppose also that r is a safe prime; then from (2) we have

$$m_\delta + m_{-\delta} = 2(p+1) = uq + vr \quad \text{and} \quad 11(u+v) \equiv 0 \pmod{12}.$$

The last equation never holds since [10] gives the inequalities $1 \leqslant u \leqslant 4$, $1 \leqslant v \leqslant 4$ and $0 < u+v < 12$. Thus r cannot be a safe if $E_{a,b}$ satisfy definition 1 with α, β from [10].

Definition 2. Strong elliptic curve $E_{a,b}$ defined by equation (1) is called *very strong* elliptic curve if the following conditions holds.

1. The class number h of the ring $\mathbb{Z}[\sqrt{-\Delta}]$ is at least 500, where $\mathrm{End}(E_{a,b}) \subseteq \mathbb{Z}[\sqrt{-\Delta}]$ is a ring of endomorphisms ring of elliptic curve $E_{a,b}$.
2. The order of twist of elliptic curve $E_{a,b}$ have a large prime divisor r where $2^\alpha < r < 2^\beta$ and parameters α, β are defined in definition 1.

In the next section we describe the results of our attempts to construct the elliptic curves satisfying conditions of definition 1 or definition 2.

3. An algorithm

The construction of elliptic curve may be performed in several ways. The first one is based on SEA-algorithm of counting points on elliptic curve, see [23], for which it is necessary to determine the prime p and random coefficients a, b. The generation of random values a, b should continue while the order of elliptic curve does not satisfy conditions of definition 1 or definition 2.

When we use some pseudo-random function to generate the coefficients a, b with predefined seed value we obtain a deterministic algorithm for constructing pseudo-random elliptic curve. From practical experiments we conclude that probability of successful termination of this algorithm is very small. Therefore we need another deterministic algorithm that will step by step reduce the distance to an expected elliptic curve.

Our algorithm is based on the theory of complex multiplication when we can define a coefficients of elliptic curve relatively simple, when we suppose that prime modulus p and prime order q are known. The algorithm is based on ideas which may be found in [5].

From practical reasons we would find a safe prime p near power of 2. We know many elliptic curves possessing this property, say "E-382" [1], "Curve25519" [3] or "paramsetA" curve from [18]. Such elliptic curves may be efficiently used in cryptographic applications. At the beginning we can construct an elliptic curve in short Weierstrass form (1), where $m = uq$ for small natural integer u and safe prime q satisfying inequalities $2^\alpha < q < p < 2^\beta$. This form of elliptic curve is suitable for digital signature schemes.

If $u = 2$ we can reduce this elliptic curve to the Montgomery form, see [13], for $u = 3$ — to the Hessian form, see [6], and for $u = 4$ — to twisted Edwards form, see [4], of elliptic curve. These forms is more suitable for key agreement protocols and public key encryption.

The algorithm is as follows.

1. We start from maximal odd integer p_0 satisfying the conditions
$$p_0 \equiv 11 \pmod{12}, \quad p_0 < 2^\beta.$$
2. For every number in a decreasing sequence $p_n = p_0 - 12n$, $n = 0, 1, \ldots$, we use twice the Miller–Rabin test, see [20], and check if p_n is a safe prime.
3. For safe prime p_n we try to solve the Cornaccia equation
$$4p_n = x^2 + dy^2 \tag{3}$$
for every square free integer $d = 2, 3, \ldots, d_0$, where d_0 is an appropriate upper bound, say $d_0 = 10^6$, and class number of $\mathbb{Z}[\sqrt{-\Delta}]$ is large.

   Since $p_n \equiv 11 \pmod{12}$ we can, as in [2], consider only d satisfying the condition
$$d \equiv \{2, 7, 10, 11\} \pmod{12}. \tag{4}$$
   This result immediately follows from checking residues of x^2 modulo 12.
4. If we find suitable d satisfying (3), then we calculate
$$m_{-\delta} = p + 1 - x, \quad m_\delta = p + 1 + x,$$
   i. e. the orders of some elliptic curve $E_{a,b}$ and its twist.
5. Now we must check the conditions of definitions 1 or 2 for given values of $m \in \{m_{-\delta}, m_\delta\}$ and safe prime p. If these conditions are satisfied, then we try to construct the coefficients a, b of elliptic curve $E_{a,b}$ using a theory of complex multiplication in the following way.

(a) Let $\omega \in \mathbb{C}$ and $\{1, \omega\}$ is a basis of some order in $\mathbb{Z}[\sqrt{-\Delta}]$. Find a value of $j(\omega)$ where j is a modular function.

(b) Find a polynomial $H_d(x) \in \mathbb{Z}[x]$ for which the equality $H_d(j(\omega)) = 0$ holds and degree of polynomial $H_d(x)$ is equal to the class number h of $\mathbb{Z}[\sqrt{-\Delta}]$. Since $j(\omega)$ is an algebraic integer of degree $2h$ we know that every root of $H_d(x)$ has the same degree and generate the Hilbert class field $\mathbb{H}$ which is a maximal unramified extension of $\mathbb{Q}$ of degree $2h$.

In [5] one can find less complicated method of constructing the Hilbert class field $\mathbb{H}$ based on values of the Weber functions.

(c) Since every root of $H_d(x)$ modulo p gives a value of $j(E_{a,b})$ which denotes as j-invariant of elliptic curve $E_{a,b}$ defined over $\mathbb{F}_p$, we need to find and sort in ascending order all roots of $H_d(x)$ modulo p.

(d) Starting from the minimal root $j(E_{a,b})$ we need to find

$$k \equiv \frac{j(E_{a,b})}{1728 - j(E_{a,b})} \pmod{p}$$

such that $-k^{-1}$ is a quadratic residue modulo p. This condition gives an equality $a = -3$ which is helpful for decreasing the complexity of group operations on elliptic curve.

(e) The coefficients of constructed elliptic curve $E_{a,b}$ satisfy the equalities

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

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

(f) The coefficients of twist $\widehat{E}_{a,b}$ satisfy the equalities

$$\begin{cases} \widehat{a} \equiv 3k\gamma^2 \pmod{p}, \\ \widehat{b} \equiv 2k\gamma^3 \pmod{p}, \end{cases}$$

where γ is quadratic non-residue modulo p.

Since $p = 12n + 11$ we have $\left(\frac{-1}{p}\right) \equiv -1 \pmod{p}$, where $\left(\frac{\cdot}{\cdot}\right)$ is a Legendre symbol, and $\gamma = \varepsilon c$ is quadratic non-residue modulo p for $\varepsilon \in \{-1, 1\}$. Hence we can take $\widehat{a} = -3$, $\widehat{b} \equiv -b \pmod{p}$ as coefficients of twist $\widehat{E}$.

(g) At last we need to check which of curves: $E_{a,b}$ or $\widehat{E}_{a,b}$, has order with safe prime divisor. For this one can choose a random point P and check its order or ingeniously use the SEA algorithm.

6. After constructing the elliptic curve $E_{a,b}$ we need to give a correct proof that p, q are safe primes.

Note that basic complexity of this algorithm is connected with the solution of equation (3) for every safe prime p_n and all possible values of d.

4. Results of experiments

For computer experiments we choose $\alpha = 254$ and $\beta = 256$. Following (4) we construct a table of $5 \cdot 10^5$ values of d for which class number satisfy $h > 500$. These values started from 72446 and ended by 2811583.

The search phase of algorithm was written by the author in C++ code. The elliptic curve construction phase of algorithm was written in Magma [11] in the following manner.

```
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_p!Modinv( Integers()!(1728 - j_p[1]), p ));
   if JacobiSymbol( Integers()!(-k), p) eq 1 then
      c := Modinv( Modsqrt( Integers()!(-k), p ), p);
      ec := EllipticCurve( [ F_p!(3*k* c^2 ), F_p!(2*k* c^3 )]);
      m := Order(ec);
      if m eq m_δ then
         return true;
         end if;
     end if;
   end for;
```

Using dual core IntelCore i5 processor with 4 Gb of memory we find the following elliptic curves. Let $p = 2^{256} - t$, then

$$E_n : y^2 \equiv x^3 - 3x + 2k\varepsilon c^3 \pmod{p},$$

where

- $k \equiv \frac{j_{p,i}}{1728 - j_{p,i}} \pmod{p}$,
- $j_{p,i}$ is an i-th root of polynomial $H_d(x)$ modulo p, $i = 1, \ldots, h$,
- $c^2 \equiv -k^{-1} \pmod{p}$.

Also the equation $|E_n| = m_\delta = uq$ holds for integer $u \in \{1, 2, 3, 4\}$ and safe prime q, $2^{254} < q < 2^{256}$.

n	t	d	δ	u	h	i	ε	$\log_2 r$
1	4909637	2767810	-1	2	748	5	-1	121
2	5210777	2166070	-1	2	676	2	1	109
3	5460857	640030	-1	2	544	1	1	139
4	17775197	2763419	1	3	792	4	-1	183
5	21924557	2447434	1	2	904	2	-1	202
6	24386669	1904482	1	2	572	2	1	188
7	27679193	2105014	1	2	692	5	-1	242
8	30043733	1449922	1	2	648	2	1	103
9	56522129	1235854	-1	2	512	1	-1	68
10	90054089	935518	-1	2	576	2	1	147

The last column contain a bit size of prime divisor r such that the order of twist $\widehat{E}_n$ satisfy $|\widehat{E}_n| = vr$ and r is a prime integer. Note that elliptic curve E_4 has cofactor $u = 3$ and may be reduced to the Hessian form of elliptic curve. All others curves may be reduced to the Montgomery form.

5. Conclusion

By means of numerical evaluations we found several strong elliptic curves for fixed values $\alpha = 254$ and $\beta = 256$. All these curves satisfy the definition 1, first condition of definition 2 and may be used in cryptographic schemes and protocols.

References

[1] Aranha D., Barreto P., Pereira G., Ricardini J., *A note on high-security general-purpose elliptic curves*, http://eprint.iacr.org/2013/647, 2013.

[2] Baier H., Buchmann J., "Efficient construction of cryptographically strong elliptic curves", INDOCRYPT 2000, Lect. Notes Comput. Sci., **1977**, 2000, 191–202.

[3] Bernstein D., "Curve25519: New Diffie-Hellman speed records", PKC 2006, Lect. Notes Comput. Sci., **3958**, 2006, 207–228.

[4] Bernstein D, Lange T., "Faster addition and doubling on elliptic curves", ASIACRYPT 2007, Lect. Notes Comput. Sci., **4833**, 2007, 29–50.

[5] Blake I., Seroussi G., Smart N., *Elliptic Curves in Cryptography*, London Math. Soc. Lecture Notes, **265**, Cambridge: Cambridge Univ. Press, 1999, 204 pp.

[6] Chudnovsky D., Chudnovsky G., "Sequences of numbers generated by addition in formal groups and new primality and factorization tests", *Adv. Appl. Math.*, **7** (1986), 385–434.

[7] Cox D., *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*, N. Y. etc.: J. Wiley and Sons, 1989, 363 pp.

[8] Crandal R., Pomerance C., *Prime Numbers: A Computational Perspective*, 2nd ed.: Springer, 2005.

[9] Husemöller D., *Elliptic Curves*, 2nd ed., Heidelberg etc.: Springer, 2004.

[10] *GOST R 34.10-2012. Information technology. Cryptographic data security. Signature and verification processes of* [*electronic*] *digital signature*, M.: Standardinform, 2012.

[11] Bosma W., Cannon J. (eds.), *Discovering Mathematics with Magma*, Algor. and Comput. in Math., **19**, Heidelberg etc.: Springer, 2006, 364 pp.

[12] Menezes A., Vanstone S., Okamoto T., "Reducing elliptic curve logarithms to logarithms in a finite field", 23rd ACM Symp. Theory of Computing, 1991, 80–89.

[13] Montgomery P.L., "Speeding the Pollard and elliptic curve methods of factorization", *Math. Comp.*, **48**:177 (1987), 243–267.

[14] Nesterenko A. Yu., "Construction of elliptic curves endomorphisms", *Matematicheskie Voprosy Kriptografii*, **5**:2 (2014), 99–102.

[15] Nesterenko A. Yu., "Some remarks on the elliptic curve discrete logarithm problem", *Matematicheskie Voprosy Kriptografii*, **7**:2 (2016), 115–120.

[16] van Oorschot P. C., Wiener M. J., "Parallel collision search with cryptanalytic applications", *J. Cryptology*, **12**:1 (1999), 1–28.

[17] Petit C., Kosters M., Messeng A., "Algebraic approaches for the elliptic curve discrete logarithm problem over prime fields", PKC 2016, **9615**, 2016, 3–18.

[18] Popov V., Kurepkin I., Leontiev S., *RFC4357. 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*, https://www.rfc-editor.org/info/rfc4357, 2006.

[19] Pollard J. M., "Monte Carlo methods for index computation ($mod\ p$)", *Math. Comp.*, **32**:143 (1978), 918–924.

[20] Rabin M. O., "Probabilistic algorithm for testing primality", *J. Number Theory*, **12**:1 (1980), 128–138.

[21] Rivest R. L., Silverman R. D., *Are "strong" primes needed for RSA?*, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.310.4183&rep=rep1&type=pdf, 1999, 23 pp.

[22] Satoh T., Araki K., "Fermat quotients and the polynomial time discrete log algorithm for anomalous curves", *Comm. Math. Univ. Sancti Pauli*, **47** (1998), 81–92.

[23] Schoof R., "Counting points on elliptic curves over finite fields", *J. Théorie des Nombres de Bordeaux*, **7**:1 (1995), 219–254.

[24] Semaev I., "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p", *Math. Comp.*, **67**:221 (1998), 353–356.

[25] Silverman J. H., *The Arithmetic of Elliptic Curves*, Heidelberg etc.: Springer, 1986, 400 pp.

[26] Smart N., "The discrete logarithm problem on elliptic curves of trace one", *J. Cryptology*, **12** (1999), 193–196.

[27] *Technical Guideline TR-03111. Elliptic curve cryptography*: German Federal Office for Inform. Secur., 2007.

[28] Teske E., "Square-root algorithms for the discrete logarithm problem (a survey)". In: "*Public-key cryptography and computational number theory* (*Warsaw, 2000*)", Berlin: de Gruyter, 2001, 283–301.