Modified Gaudry-Schost Algorithm for the Two-dimensional Discrete Logarithm Problem

Maksim Nikolaev

Cryptography Academy of Russian Federation

June 07th, 2019

Plan of talk

- Introduction to DLP and 2-D DLP
- Gaudry-Schost Algorithm
- Modification of algorithm
- Experimental Results

Introduction. Discrete Logarithm Problem

- *Definition 1. Discrete logarithm problem.*
  Given: group $G = \langle P \rangle$, $\mathrm{ord}(P) = r$, $Q \in G$.
  To find: $n \in \{0, ..., r-1\}$ *such, that* $Q = nP$.

Introduction. Discrete Logarithm Problem

- *Definition 1. Discrete logarithm problem.*
  Given: group $G = \langle P \rangle$, $\mathrm{ord}(P) = r$, $Q \in G$.
  To find: $n \in \{0, ..., r-1\}$ *such, that* $Q = nP$.
- *Applications*
  — *Diffie-Hellman Key Exchange;*
  — *ElGamal Cryptosystem*

Introduction. Discrete Logarithm Problem

- Currently, the best known algorithm — *parallelized version of the Pollard rho*.
  Expected running time: $\sqrt{\frac{\pi|G|}{2}}$ group operations in G [Wiener, van Oorschot, 1996].
- *Efficient automorphism*
  orbit of any point under an efficient automorphism can be computed much faster, than group operation
- *Parallel Pollard rho method for groups with efficient automorphisms*
  Expected running time: $\sqrt{\frac{\pi|G|}{2r}}$ group operations in G, where r — order of group of efficient automorphisms [Wiener, Zuccherato, 1999; Duursma, Gaudry, Morain, 1999].

Introduction. 2-D Discrete Logarithm Problem

- *Definition 2. Two-dimensional discrete logarithm problem.*
  Given: group G; $P_1, P_2, Q \in G$, $N_1, N_2 \in \mathbb{N}$, $Q = n_1 P_1 + n_2 P_2$ *or some (unknown)* $n_1 \in \{-N_1, \ldots, N_1\}$, $n_2 \in \{-N_2, \ldots, N_2\}$.
  To find: n_1, n_2 *such that* $Q = n_1 P_1 + n_2 P_2$.

Introduction. 2-D Discrete Logarithm Problem

- *Definition 2. Two-dimensional discrete logarithm problem.*
  Given: group G; $P_1, P_2, Q \in G$, $N_1, N_2 \in \mathbb{N}$, $Q = n_1 P_1 + n_2 P_2$ *or some (unknown)* $n_1 \in \{-N_1, \ldots, N_1\}$, $n_2 \in \{-N_2, \ldots, N_2\}$.
  To find: n_1, n_2 *such that* $Q = n_1 P_1 + n_2 P_2$.
- *Applications*
  — *computing the number of points on genus 2 curves over finite fields;*
  — *DLP for exponents of bounded height.*

Introduction. Applications of 2-D Discrete Logarithm Problem

- efficient automorphisms

$$\varphi : \ \varphi(g) = \lambda g, \ \forall g \in G$$

Group G decomposes into disjoint equivalence classes

$$\{g, \varphi(g), ..., \varphi^k(g)\}$$

Introduction. Applications of 2-D Discrete Logarithm Problem

- *Recomposition*
  Choose $k_1, k_2 \in_R [0, \sqrt{|G|}) \bigcap \mathbb{Z}$, then compute scalar multiplication $kP = k_1 P + k_2 \varphi(P)$, where $k \equiv k_1 + \lambda k_2 \bmod |G|$.
- *Decomposition*
  First, choose k at random, then find k_1, k_2 to compute scalar multiplication.

$$kP = k_1 P + k_2 \varphi(P)$$

$k_1, k_2 \leq C_{GLV} \sqrt{|G|}$

Algorithm of Solving Two-dimensional Discrete Logarithm Problem (Gaudry, Schost, 2004)

- select so-called "tame" and "wild" sets

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

Algorithm of Solving Two-dimensional Discrete Logarithm Problem (Gaudry, Schost, 2004)

- select so-called "tame" and "wild" sets

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

- calculate in parallel two pseudorandom sequences

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \quad (1)$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in T, j = 1, 2, \ldots \quad (2)$$

Algorithm of Solving Two-dimensional Discrete Logarithm Problem (Gaudry, Schost, 2004)

- select so-called "tame" and "wild" sets

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

- calculate in parallel two pseudorandom sequences

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \quad (1)$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in T, j = 1, 2, \ldots \quad (2)$$

- obtain sloution

$$x_k P_1 + y_k P_2 = Q + z_l P_1 + w_l P_2, \quad (3)$$

Algorithm of Solving Two-dimensional Discrete Logarithm Problem (Gaudry, Schost, 2004)

- select so-called "tame" and "wild" sets

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

- calculate in parallel two pseudorandom sequences

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \quad (1)$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in T, j = 1, 2, \ldots \quad (2)$$

- obtain sloution

$$x_k P_1 + y_k P_2 = Q + z_l P_1 + w_l P_2, \quad (3)$$

- average complexity of the Gaudry-Schost algorithm $\Omega = 2.36\sqrt{N}$, $N = (2N_1 + 1)(2N_2 + 1)$ [Galbraith, Ruprai, 2009]

2-D Discrete Logarithm Problem: case $\#\langle\varphi\rangle = 2$

- Elliptic curve given by equation $y^2 = x^3 + Ax + B$ over finite field of $p > 3$ elements has efficient automorphism of order 2:

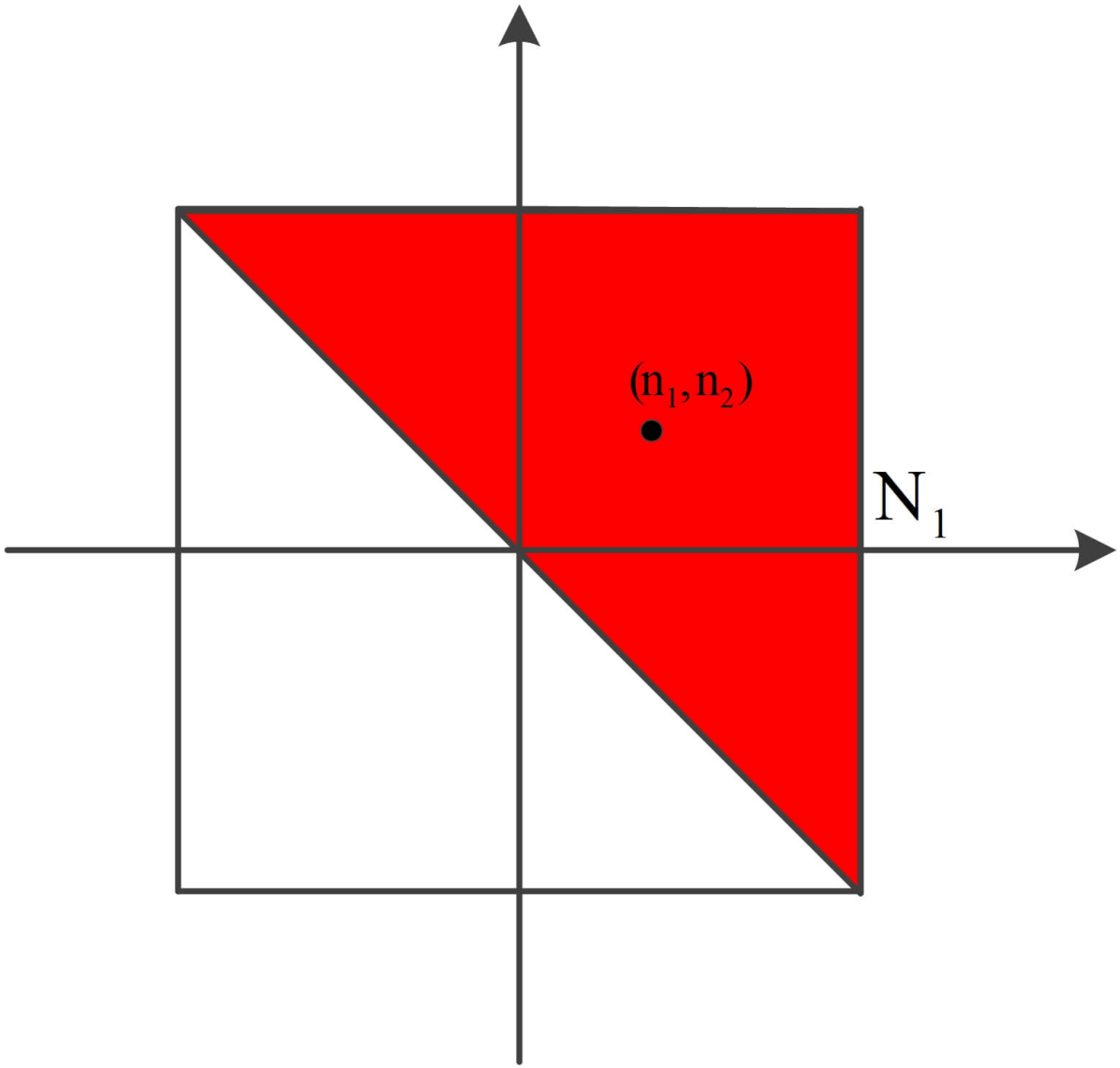
$$\varphi(x, y) = -(x, y) = (x, -y)$$

-

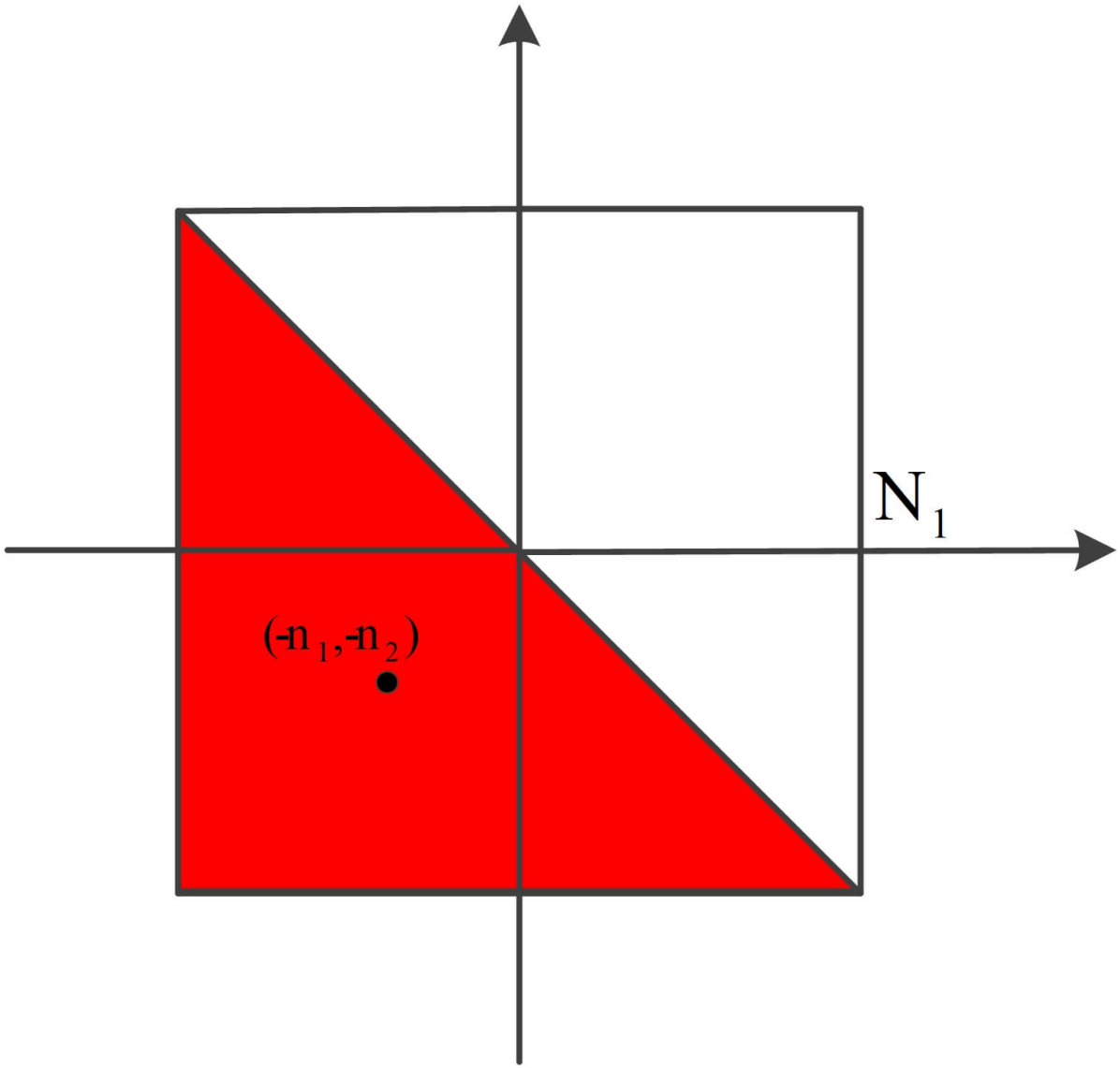
$$\varphi(aP_1 + bP_2) = -aP_1 - bP_2,$$

$$C(a, b) = \{(a, b), (-a, -b)\}.$$

2-D Discrete Logarithm Problem: case $\#\langle\varphi\rangle = 2$



2-D Discrete Logarithm Problem: case $\#\langle\varphi\rangle = 2$



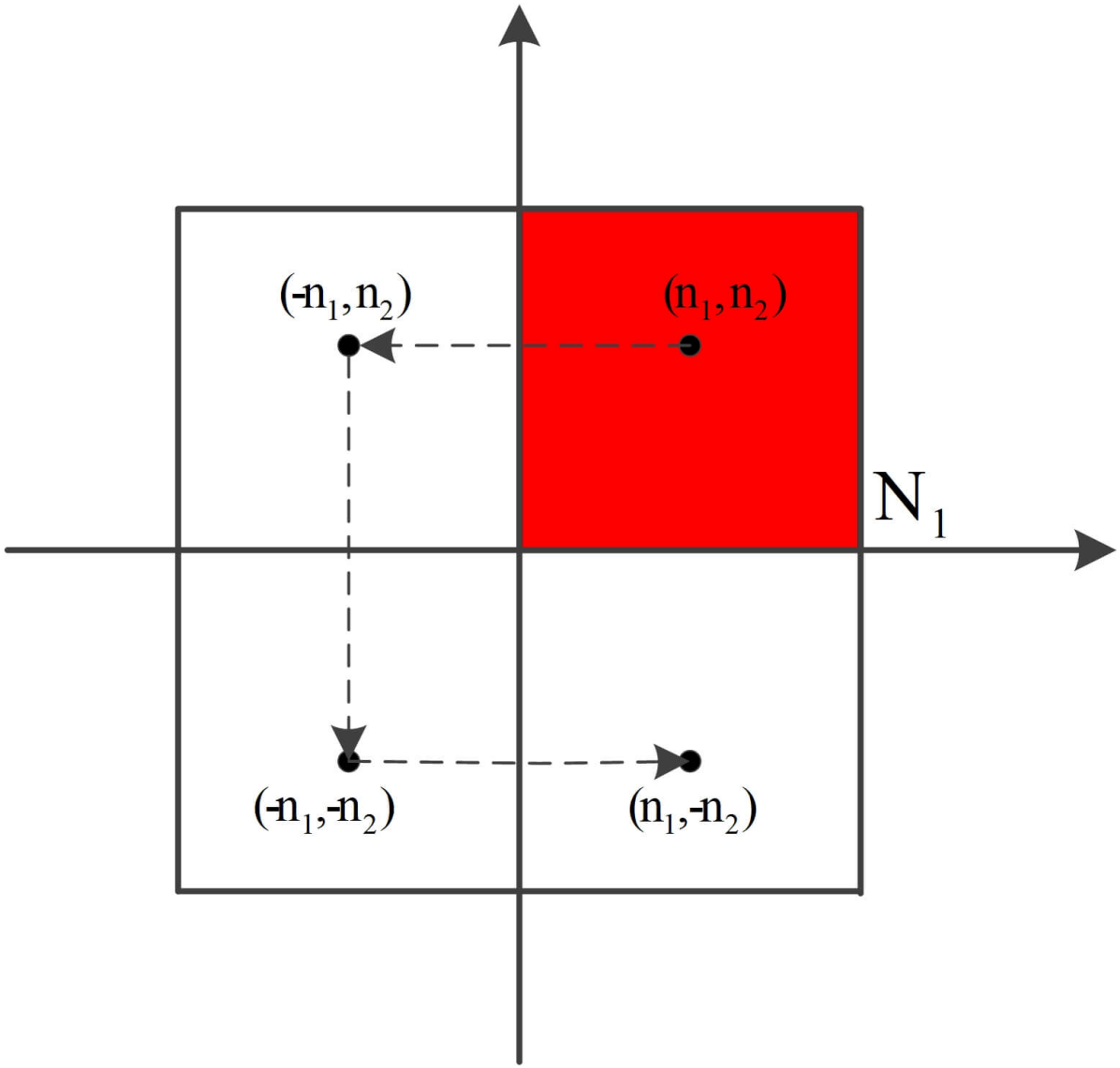
2-D Discrete Logarithm Problem: case $\#\langle\varphi\rangle = 4$

- Prime-order-q subgroup G of elliptic curve given by equation $y^2 = x^3 + Ax$ with $p \equiv 1 \bmod 4$ and $q^2 \nmid \#E$ has efficient automorphism of order 4:
- $\varphi(x, y) = (-x, \alpha y)$, where α — element of order 4 modulo p, λ — root of equation $\lambda^2 \equiv -1 \pmod{q}$
-

$$\varphi(aP_1 + bP_2) = a(\lambda P_1) + b(\lambda^2)P_1 = -bP_1 + aP_2,$$

$$C(a, b) = \{(a, b), (-a, b), (-a, -b), (a, -b)\}.$$

2-D Discrete Logarithm Problem: case $\#\langle\varphi\rangle = 4$



2-D Discrete Logarithm Problem: case $\#\langle\varphi\rangle = 6$

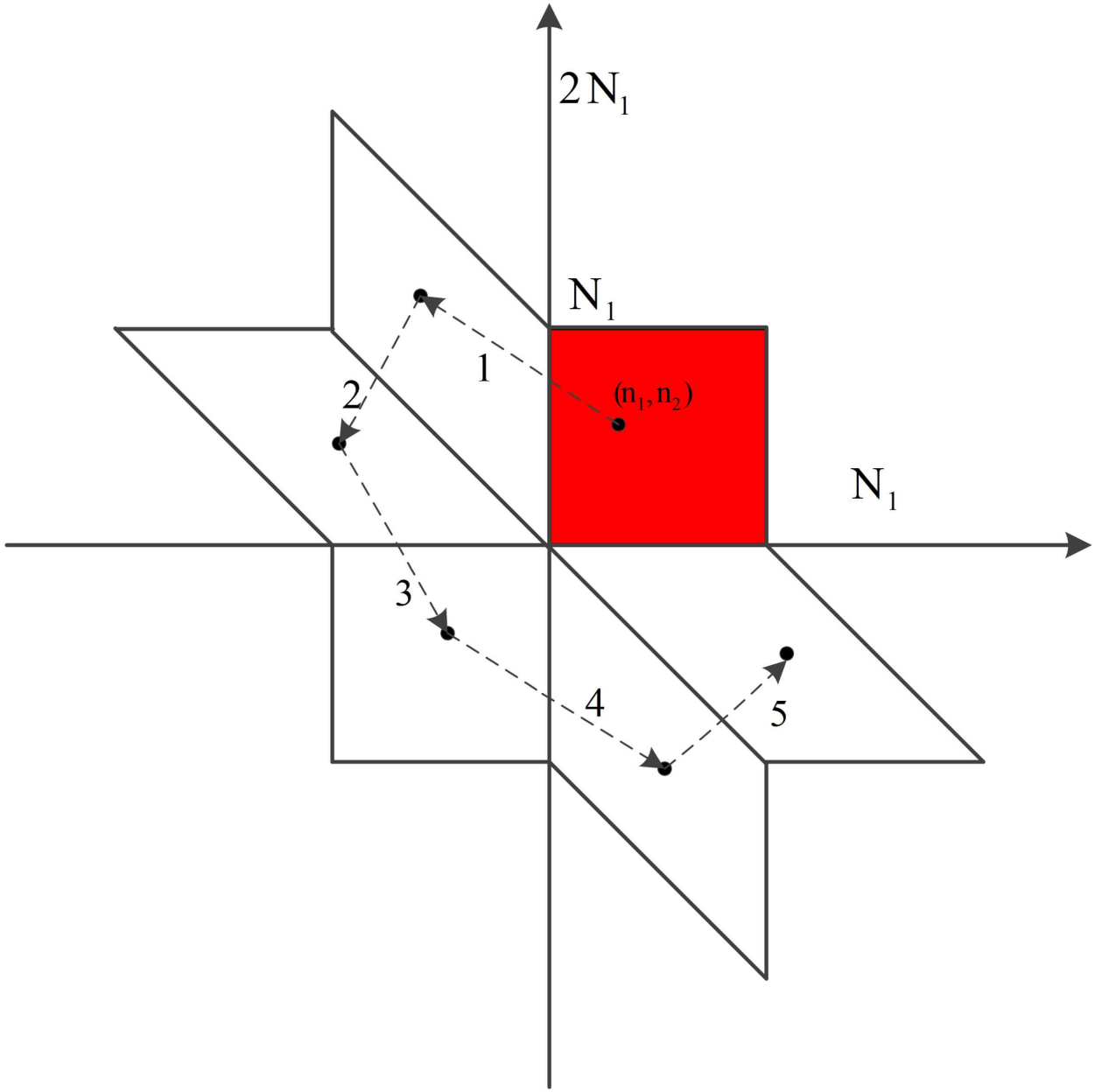
- Prime-order-q subgroup G of elliptic curve given by equation $y^2 = x^3 + B$ with $p \equiv 1 \bmod 3$ and $q^2 \nmid \#E$ has efficient automorphism of order 6:
- $\varphi(x, y) = (\beta x, -y)$, where $\beta \neq 1$ — cube root from 1 modulo p, λ — root of equation $\lambda^2 - \lambda + 1 \equiv 0 \pmod{q}$
-

$$\varphi(aP_1 + bP_2) = a(\lambda P_1) + b(\lambda - 1)P_1 = -bP_1 + (a + b)P_2,$$

$$C(a, b) = \{(a, b), (-b, a + b), (-(a + b), a),$$

$$(-a, -b), (b, -(a + b)), (a + b, -a)\}.$$

2-D Discrete Logarithm Problem: case $\#\langle\varphi\rangle = 6$



Average Complexity

Theorem (Galbraith, Holmes, 2010)

In a random sequence of balls of $C > 1$ different colors k-th ball with probability $r_{k,c}$ is of the color c (independently of previously selected balls) (c=1,2). There exist $N' \in \mathbb{N}$ different boxes. If k-th ball has a color c, then it falls into the i-th box with probability $q_{c,i}(N')$ independently of previous balls. Then the number $Z_{N'}$ of balls allocated before the first occurrence of two balls of different colors in the same urn has the mean

$$\mathbf{M}(Z_{N'}) = \sqrt{\frac{\pi}{2A_{N'}}} + O(N'^{1/4}),$$

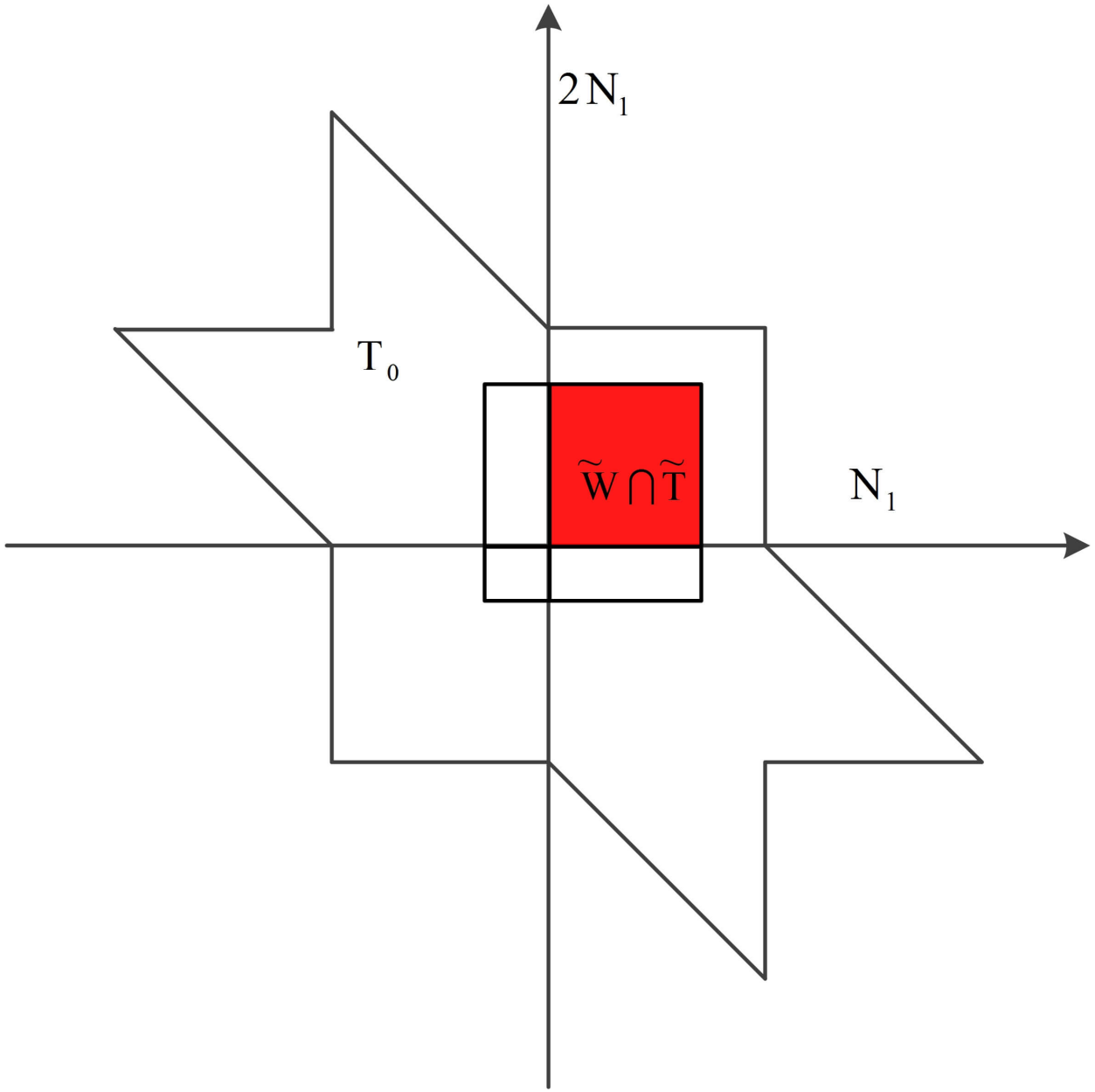
where

$$A_{N'} = \sum_{c=1}^{C} p_c \left(\sum_{c'=1, c \neq c'}^{C} p_{c'} \left(\sum_{i=1}^{N'} q_{c,i} q_{c',i} \right) \right)$$

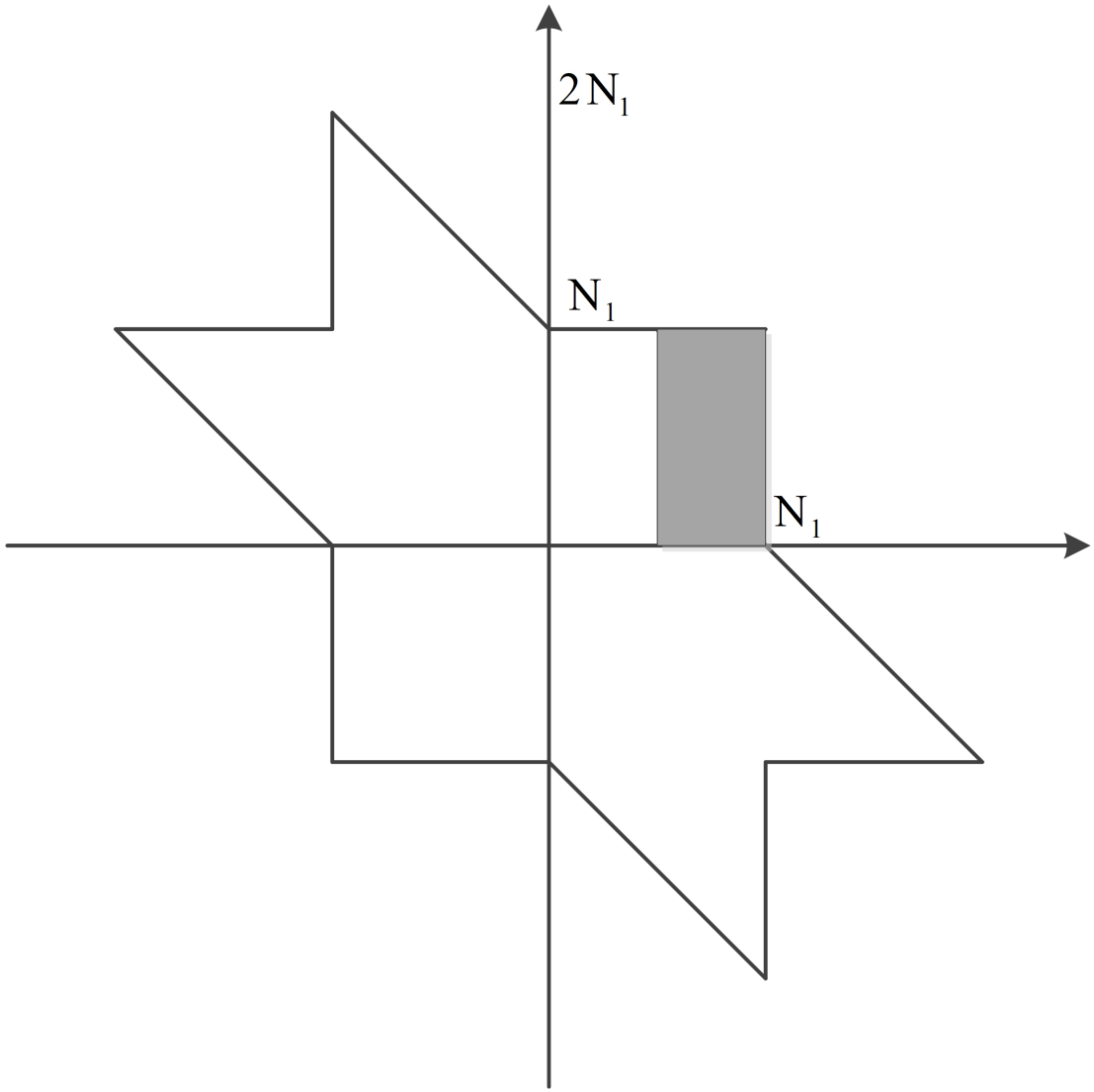
Average Complexity

- case $\#\langle\varphi\rangle = 2$: $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ group operations in G
  speedup: $\sqrt{2}$
- case $\#\langle\varphi\rangle = 4$: $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ group operations in G
  speedup: $\sqrt{4}$
- case $\#\langle\varphi\rangle = 6$: $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ group operations in G
  speedup: $\sqrt{4}$

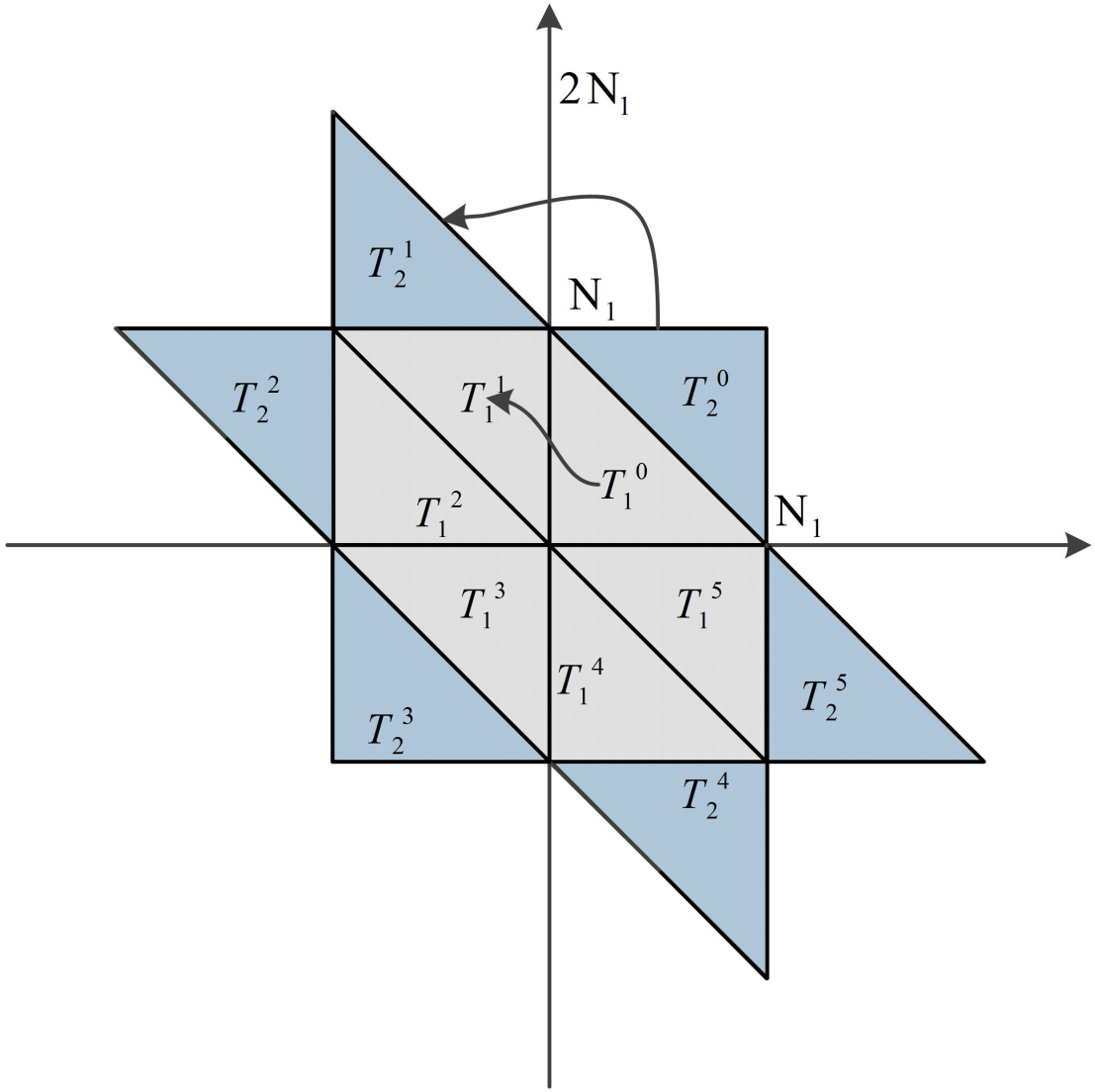
2-D Discrete Logarithm Problem: case $\#\langle\varphi\rangle = 6$



2-D Discrete Logarithm Problem: case $\#\langle\varphi\rangle = 6$



2-D Discrete Logarithm Problem: case $\#\langle\varphi\rangle = 6$



Pseudorandom walks

A distinguished point is an element of the group G which has a particular feature that is easily checked and confirmed. Let S_{dp} – number of distinguished points and

$$\frac{S_{dp}}{|G|} = \theta$$

$m_s \in \mathbf{N}, m_s > 1$, hash-function $\psi : G \to \{1, ..., m_s\}$, functions $F, F_1, ..., F_{m_s} : G \to G$ such that

$$F(u) = \begin{cases} F_1(u), \text{ if } \psi(u) = 1 \\ F_2(u), \text{ if } \psi(u) = 2 \\ \vdots \\ F_{m_s}(u), \text{ if } \psi(u) = m_s \end{cases}$$

For start point $u_0 \in_R G$ sequence $u_0, u_1 = F(u_0), ..., u_{i+1} = F(u_i), ...$ is called *pseudorandom walk*.

2-D Pseudorandom walks

Theorem (Cofman, Flajolet, Flatto and Hofri)

Let $y_0, y_1, \ldots, y_k$ be a symmetric random walk that starts at the origin ($y_0 = 0$) and takes steps uniformly distributed in $[-1, +1]$ then the expected maximum excursion is

$$\mathbb{E}(max\{|y_i| : 0 \leq i \leq k\}) \leq \sqrt{\frac{2k}{3\pi}} + O(1)$$

$$F_i(u) = u + \gamma_i, where$$

$$\gamma_i = \zeta_i^{'} P_1 + \zeta_i^{''} P_2, \ \ i = 1, .., n_s,$$

$$\zeta_i^{'}, \zeta_i^{''} \in_R \{-2M, ..., 2M\}, M \in \mathbb{Z}.$$

Results of the paper

- $$T_1^0 = \{(a; b) : 0 \le a \le N_1,\ 1 \le b \le N_1 - a\},$$
$$T_2^0 = \{(a; b) : 0 \le a \le N_1,\ N_1 - a + 1 \le b \le N_1\},$$
$$\widetilde{W}_k = \{-\frac{kN_1}{2} + n_1, \ldots, \frac{kN_1}{2} + n_1\} \times \{-\frac{kN_1}{2} + n_2, \ldots, \frac{kN_1}{2} + n_2\}.$$

- $$x_i P_1 + y_i P_2, \begin{cases} (x_i, y_i) \in T_1^0, & \text{with probability } p_3 \\ (x_i, y_i) \in T_2^0, & \text{with probability } p_4 = 1 - p_3 \end{cases}, \ i = 1, 2, \ldots,$$

Results of the paper

- $\mathbf{M}(Z_{N'}) \leq (1+\varepsilon(k))\frac{1}{8}\sqrt{\frac{\pi}{2}}\left(\frac{3}{\sqrt{p_3}}+\frac{1}{\sqrt{p_4}}\right)\sqrt{N}$
- To find: $x_0 = \arg\min\limits_{x\in(0;1)} f(x)$

$$= \arg\min_{x\in(0;1)}\left(\frac{3}{\sqrt{x}}+\frac{1}{\sqrt{1-x}}\right) = \frac{9}{10}-\frac{3\sqrt[3]{3}}{10}+\frac{3^{2/3}}{10} \approx 0.67533$$

- Then for $p_3 = 0.67533,\ p_4 = 0.32467$

$$\mathbf{M}(Z_{N'}) \leq (1+\varepsilon)0.847\sqrt{N} + O_\varepsilon(N^{\frac{1}{4}})$$

Results of the paper

Theorem

Let G be a prime-order-q subgroup of an elliptic curve E defined over a finite prime field $GF(p)$ by the equation $y^2 = x^3 + B$ with $p \equiv 1 \pmod 3$, $q^2 \nmid \#E$; φ is an automorphism of the group G, $\varphi(x, y) = (\beta x, -y)$, where $\beta \neq 1$ is the cube root of 1 modulo p; λ is the root of the equation $\lambda^2 - \lambda + 1 \equiv 0 \pmod q$ such that $\varphi(x, y) = \lambda(x, y)$. Then for any $\varepsilon > 0$ there exists an algorithm for solving the two-dimensional discrete logarithm problem in G with average complexity $(1 + \varepsilon)0.847\sqrt{N} + O_\varepsilon(N^{\frac{1}{4}})$ group operations (with $N_1 = N_2$, $P_2 = \varphi(P_1)$ and (n_1, n_2), chosen uniformly at random), where $N = 4N_1N_2, N \to \infty$.

Experimental results

Table: experemental results for ellitic curve *secp256r1*

"wild" set parametrization, k	N=36000000, number of experiments=3000	error, %
0.1	0.85554	0.18
0.2	0.88164	1.69
0.3	0.86710	1.11
0.4	0.89328	0.76
0.5	0.88997	0.68
0.6	0.91167	0.67
0.7	0.91322	0.18
0.8	0.92575	0.19
0.9	0.93778	0.54
1.0	0.93880	0.27

Questions

Thanks for attention!