sciendo

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.2478/tmmp-2024-0021
Tatra Mt. Math. Publ. **87** (2024), 67–84

SOLVING ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM ON TWISTED EDWARDS CURVES USING QUANTUM ANNEALING AND INDEX CALCULUS METHOD

Łukasz Dzierzkowski[1] — Michał Wroński [2]

[1]Military University of Technology, Warsaw, POLAND

[2]NASK National Research Institute, Warsaw, POLAND

ABSTRACT. This paper presents an approach to solving the elliptic curve discrete logarithm problem on alternative curve models over prime fields using a quantum annealing and index calculus method. Part of the algorithm, relation searching, is transformed into the Quadratic Unconstrained Boolean Optimization (QUBO) problem and then is efficiently solved using the D-Wave computer by quantum annealing. As Faugère et al. showed, twisted Edwards curves, because of their symmetric shape, allow us to obtain solutions of relations searching step using Groebner basis faster than in the case of Weierstrass curves. Because of symmetries, a system of equations of relations searching step for twisted Edwards curves has many symmetric solutions. Using the Groebner basis and having many system solutions makes it easier to find any of them. The same is true using quantum annealing - it is easier to find any solution to the QUBO problem if many are correct. In this paper, we used this observation to find out that a properly constructed QUBO problem for the relations searching step for twisted Edwards curves allows us to find a solution faster for the same size of the base field than in the case of Weierstrass curves. Using the presented approach, we solved the discrete logarithm problem using quantum annealing and index calculus method for elliptic curve discrete logarithm problem defined on twisted Edwards curve over a field $\mathbb{F}_{1021}$ with order equal to $4 \cdot 241$. It is now the biggest field and size of the group, where the elliptic curve discrete logarithm problem was solved using quantum methods.

© 2024 Mathematical Institute, Slovak Academy of Sciences.
2020 Mathematics Subject Classification: 11T71, 94A60, 14H52, 81P94.
Keywords: cryptology, elliptic curves, ECDLP, quantum annealing, index calculus.
This work was Supported by the Grant DOB/002/RON/ID1/2018 by The National Centre for Research and Development.
Licensed under the Creative Commons BY-NC-ND 4.0 International Public License.

1. Introduction

The dynamic development of quantum computers allows us to solve computationally hard problems, such as factorization, discrete logarithm problem over finite fields, or discrete logarithm problem on elliptic curves. For now, quantum technology makes it possible to overcome issues whose scale may be measured in tens of bits, and thus, it is not a severe danger nowadays. Nevertheless, it is impossible to predict what will happen in the next few months or years, which algorithms may become significantly less safe, and how fast this process will develop.

As general-purpose quantum computers nowadays have limited resources (the biggest quantum computer - IBM Eagle, has 127 physical qubits), quantum annealers offer almost 6,000 physical qubits (see D-Wave Advantage). From this point of view, it is interesting to find out the possibilities of these computers in the context of cryptanalysis for both symmetric and asymmetric ciphers.

The facts above show that quantum annealing is an interesting approach to quantum computing nowadays. There are several papers where cryptanalysis using quantum annealing is performed, for example, integer factorization [10, 15, 21], discrete logarithm problem over prime fields [24], elliptic curve discrete logarithm problem [22], which is described below, and algebraic attacks on block ciphers [6].

This paper focuses on applying quantum annealing to solve the elliptic curve discrete logarithm problem (ECDLP) over prime fields using quantum annealing and twisted Edwards curves. The first application of quantum annealing to the ECDLP using the index calculus method was performed and shown in the paper [22], where the index calculus method on short Weierstrass curves was performed. The biggest difference between [22] and this paper is that we applied twisted Edwards curves this time. Let us note that Faugère et al. in [13] showed that by applying symmetries of twisted Edwards curves, the point decomposition problem (PDP) for twisted Edwards curves, transformed to the system of polynomial equations by applying Semaev summation polynomials, is easier to solve. The main reason for such a fact is that while using the Groebner basis mechanism for solving a system of polynomial equations, the more solutions the system of equations has, the easier it is to find any of them. As shown in [13], applying symmetries of twisted Edwards curve results in finding many equivalent solutions to the system of equations, in opposition to the case of short Weierstrass curves.

The main contribution of this paper is to show that the application of the index calculus method on twisted Edwards curves allows one to speed up computations when quantum annealing to the relations searching step is applied. The reason is similar to the Groebner basis application: it is easier to find one solution among many correct ones than finding the only one being legitimate.

Using the presented approach, we solved the discrete logarithm problem using quantum annealing and index calculus method for elliptic curve discrete logarithm problem defined on twisted Edwards curve over a field $\mathbb{F}_{1021}$ with order equal to $4 \cdot 241$. It is now the biggest field and size of the group, where the elliptic curve discrete logarithm problem was solved using quantum methods.

2. Alternative models of elliptic curves

A Weierstrass equation can represent any elliptic curve. However, one may want to use some specific properties which are accessible while using an alternative model. To try to solve the ECDLP problem, Montgomery curves and twisted Edwards curves may be used.

2.1. Montgomery curves

In 1987 Peter L. Montgomery introduced a new family of elliptic curves, named later with his surname [18]. The first purpose of these curves was to accelerate Lenstra's ECM factorization method [17]. Now, these curves have a much broader spectrum of use because of their efficient arithmetic.

A Montgomery curve is defined over a field $\mathbb{K}$ by an equation

$$E_M : \; By^2 = x^3 + Ax^2 + x, \tag{1}$$

where A and B are coordinates in $\mathbb{K}, B \neq 0$ and $A^2 \neq 4$. Addition formulas for 2 points P_1 and P_2 lying on the curve are given by equation

$$P_1 \oplus P_2 = (x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3),$$

where

$$\lambda = \begin{cases} (y_2 - y_1) \,/\, (x_2 - x_1) & \text{if } P_1 \neq \pm P_2, \\ \left(3x_1^2 + 2Ax_1 + 1\right) / \left(2By_1\right) & \text{if } P_1 = P_2, \end{cases} \tag{2}$$

$$x_3 = B\lambda^2 - A - x_1 - x_2, \tag{3}$$

$$y_3 = (2x_1 + x_2 + A)\,\lambda - B\lambda^3 - y_1 = \lambda(x_1 - x_3) - y_1. \tag{4}$$

The opposite of a point $P = (x, y)$ is a point $-P = (x, -y)$ and adding 2-torsion point $T_2 = (0, 0)$ to P gives

$$P + T_2 = (1/x, -y/x^2).$$

Because the x-coordinate is invariant under finding the opposite point, the x--coordinate can be used to compute the summation polynomials for Montgomery curves.

2.2. Twisted Edwards curves

In 2007 Edwards curves were proposed by Harold Edwards [12]. The generalized version, twisted Edwards curves, were introduced one year later [2], and this family of curves is isomorphic to the family of Montgomery curves. Since then, they have been deeply analyzed, for example, in [3]. The main interest lies in efficient arithmetic.

A twisted Edwards curve is defined over a field $\mathbb{K}$ of a characteristic greater than 2 by an equation

$$E_{TE}: \; ax^2 + y^2 = 1 + dx^2y^2, \tag{5}$$

where $a, d \neq 0$ and $a \neq d$. If $a = 1$, such a curve is an Edwards curve. Complete addition formulas for any 2 points P_1 and P_2 lying on the curve are given by equation

$$P_1 \oplus P_2 = (x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right). \tag{6}$$

On the twisted Edwards curve, the neutral element is $\mathcal{O} = (0, 1)$, the opposite of a point $P = (x, y)$ is a point $-P = (-x, y)$ and adding 2-torsion point $T_2 = (0, -1)$ to P gives $P + T_2 = (-x, -y)$. Because the y-coordinate is invariant under finding the opposite point, this coordinate can be used to compute the summation polynomials for twisted Edwards curves.

3. Semaev polynomials and index calculus method

This section will describe the most important ideas for using the index calculus method. We begin by describing Semaev polynomials, often used in the relations searching step of the index calculus method. Finally, we describe the most notable approaches to solving ECDLP using the index calculus method.

3.1. Semaev polynomials

Point decomposition problem is defined in the following manner: given a point $R \in E(\mathbb{F}_q)$ and the factor base $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_q) | x \in \mathbb{G}\} \subset E$ find $P_1, \ldots, P_n \in \mathcal{F}$ such that $R = P_1 \oplus \cdots \oplus P_n$. $\mathbb{G}$ is some subset of $\mathbb{F}_q$ field, e.g., for extension fields $\mathbb{F}_{p^n}$ often holds that $\mathbb{G} = \mathbb{F}_q$. If $\mathbb{F}_q$ is a prime field $\mathbb{F}_p$, then $\mathbb{G}$ is often of the form of $\mathbb{G} = \{0, \ldots, \lfloor \sqrt[n]{p} \rfloor\}$. The most notable method for PDP solving is the application of Semaev polynomials. In this section, we describe the general idea of Semaev polynomials and show Semaev polynomials' shape for Montgomery and twisted Edwards curves.

Let E be the elliptic curve defined over some prime finite field $\mathbb{F}_p$. Solving a discrete logarithm problem is equivalent to finding such k that for given points $P, Q \in E(\mathbb{F}_p)$ one has $Q = [k]P \in E(\mathbb{F}_p)$. Semaev proposed in 2004 [20] the index calculus algorithm for the discrete logarithm problem on elliptic curves. Its purpose is to find bounded solutions to modular multivariate polynomial equations obtained from a specific form's elliptic curve summation polynomials. These polynomials have roots when curve points sum to $\mathcal{O}$. According to this fact, for elliptic curves in short Weierstrass form $E/\mathbb{F}_p : y^2 = x^3 + Ax + B$, the 2nd Semaev polynomial is given by

$$f_2(x_P, x_Q) \quad = \quad x_P - x_Q. \tag{7}$$

To find the 3rd Semaev polynomial, we should take into account that we are searching for x-coordinate of some point R for which holds that $R = P + Q$ or $R = P - Q$. So it is equivalent to $x_R = x_{P+Q}$ or $x_R = x_{P-Q}$. To obtain the 3rd Semaev polynomial, we should therefore construct the following polynomial

$$\begin{aligned} f_3(x_P, x_Q, x_R) &= (x_R - x_{P+Q})(x_R - x_{P-Q}) \\ &= x_R^2 - (x_{P+Q} + x_{P-Q})x_R + x_{P+Q}x_{P-Q}. \end{aligned} \tag{8}$$

However, formulas for $x_{P+Q}+x_{P-Q}$ and $x_{P+Q}x_{P-Q}$ for short Weierstrass curves are easy to find. According to [20], the following equalities hold

$$\begin{aligned} x_{P+Q} + x_{P-Q} &= 2\tfrac{(x_P+x_Q)(x_Px_Q+A)+2B}{(x_P-x_Q)^2}, \\ x_{P+Q}x_{P-Q} &= \tfrac{(x_Px_Q-A)^2-4B(x_P+x_Q)}{(x_P-x_Q)^2}. \end{aligned} \tag{9}$$

Therefore it is not challenging to find the 3rd Seamev polynomial as

$$\begin{aligned} f_3(x_P, x_Q, x_R) &= x_Q^2x_R^2 - 2x_Px_Qx_R^2 + x_P^2x_R^2 - 2x_Px_Q^2x_R \\ &\quad -2x_P^2x_Qx_R - 2Ax_Qx_R - 2Ax_Px_R - 4Bx_R + x_P^2x_Q^2 \\ &\quad -2Ax_Px_Q - 4Bx_Q - 4Bx_P + A^2. \end{aligned} \tag{10}$$

For any $m \geq 4$ and $m - 3 \geq k \geq 1$, one can find $f_m(x_P, \ldots, x_m)$ as

$$f_m(x_P, \ldots, x_m) \;=\; \mathrm{Res}\,\mathrm{bl}(f_{m-k}(x_P, \ldots, x_{m-k-1}, x), f_{k+2}(x_{m-k}, \ldots, x_m, x)\big). \tag{11}$$

Value of the $(m+1)$-th summation polynomial $f_{m+1}(x_P, \ldots, x_m, x_R)$ is equal to zero if and only if for $i = \overline{1, m}$ there exists y_i, for which every point of the form (x_i, y_i) lies on the elliptic curve and their sum $\sum_{i=1}^{m}(x_i, y_i) = (x_R, y_R) \in E(\overline{\mathbb{K}})$. Point (x_R, y_R) is obtained by computing $[\alpha]P+[\beta]Q$ for some arbitrary α and β.

3.1.1. Semaev polynomials for Montgomery curves

According to Semaev polynomials' property, they have roots when curve points sum to $\mathcal{O}$. For the Montgomery curve, 2nd Semaev polynomial is the same as for the short Weierstrass curves (7). To obtain 3rd polynomial on the Montgomery curve $E_M/\mathbb{F}_p : by^2 = x^3 + ax^2 + x$, one needs to start with an equation, which fulfills the property below, namely for points $P, Q, R \in E_M$

$$x_R - x_{P+Q})(x_R - x_{P-Q}) = x_R^2 - (x_{P+Q} + x_{P-Q})x_R + x_{P+Q}x_{P-Q} = 0 \quad (12)$$

has to be satisfied. It is easy to obtain equations for $x_{P+Q}+x_{P-Q}$ and $x_{P+Q}x_{P-Q}$ using general Montgomery curve arithmetic

$$\begin{aligned} x_{P+Q} + x_{P-Q} &= \tfrac{2x_P^2x_Q+2x_Px_Q^2+4ax_Px_Q+2x_P+2x_Q}{x_P^2-2x_Px_Q+x_Q^2}, \\ x_{P+Q}x_{P-Q} &= \tfrac{x_P^2x_Q^2-2x_Px_Q+1}{x_P^2-2x_Px_Q+x_Q^2}. \end{aligned} \quad (13)$$

Finally, the 3rd Seamev polynomial is given by

$$\begin{aligned} f(x_P, x_Q, x_R)_{M,3} &= x_R^2x_P^2 - 2x_R^2x_Px_Q + x_R^2x_Q^2 - 2x_Rx_P^2x_Q \\ &\quad -2x_Rx_Px_Q^2 - 4ax_Rx_Px_Q - 2x_Rx_P \\ &\quad -2x_Rx_Q + x_P^2x_Q^2 - 2x_Px_Q + 1. \end{aligned} \quad (14)$$

Using expression (14), one may transform the searching for equation roots problem into the QUBO problem and then solve it via D-Wave quantum annealer.

3.1.2. Semaev polynomials for twisted Edwards curves

For the twisted Edwards curve, 2nd Semaev polynomial is identical to the short Weierstrass curves (7). To obtain 3rd polynomial on the twisted Edwards curve $E_{TE}/\mathbb{F}_p : ax^2 + y^2 = 1 + dx^2y^2$, one needs to start with an equation, which fulfills the property below, namely, for points $P, Q, R \in E_{TE}$

$$(y_R - y_{P+Q})(y_R - y_{P-Q}) = y_R^2 - (y_{P+Q} + y_{P-Q})y_R + y_{P+Q}y_{P-Q} = 0 \quad (15)$$

has to be satisfied. However, in the case of twisted Edwards coordinates, we will not use the x-line arithmetic as before, but y-line arithmetic because the second one is invariant under involution operation, so both points P and $-P$ have the same value of y coordinate.

It is easy to obtain equations for $x_{P+Q}+x_{P-Q}$ and $x_{P+Q}x_{P-Q}$ using general Montgomery curve arithmetic [11]

$$\begin{aligned} y_{P+Q} + y_{P-Q} &= \tfrac{(2(a-d))y_Py_Q}{{y_P}^2{y_Q}^2d-{y_P}^2d-{y_Q}^2d+a}, \\ y_{P+Q}y_{P-Q} &= \tfrac{(-{y_P}^2{y_Q}^2d+a{y_P}^2+a{y_Q}^2-a)}{({y_P}^2{y_Q}^2d-{y_P}^2d-{y_Q}^2d+a)}. \end{aligned} \quad (16)$$

Finally, the 3rd Seamev polynomial is given by

$$f_{TH,3} = y_R^2 y_P^2 - 2y_R^2 y_P y_Q + y_R^2 y_Q^2 - 2y_R y_P^2 y_Q - 2y_R y_P y_Q^2 - 4a y_R y_P y_Q - 2y_R y_P - 2y_R y_Q + y_P^2 y_Q^2 - 2y_P y_Q + 1. \quad (17)$$

Using expression (17), one may transform the searching for equation roots problem into the QUBO problem and then solve it via D-Wave quantum annealer.

3.2. Index calculus method on elliptic curves

This section presents essential information and methods from the most notable papers on the index calculus method on elliptic curves.

3.2.1. Gaudry-Diem method for ECDLP over field extensions [8], [14]

The most interesting algorithm for ECDLP using index calculus was presented by Gaudry [14] and Diem [9].

Let us consider extension field $\mathbb{F}_{p^m}$ of low degree and large characteristic p and suppose that this field is generated by an irreducible polynomial $f(t)$, which means that $\mathbb{F}_{p^m} = \mathbb{F}_p[t]/\operatorname{bl}(f(t))$.

Let E be an elliptic curve over $\mathbb{F}_{p^m}$ and let $P, Q \in E(\mathbb{F}_{p^m})$. If $(x, y) \in E(\mathbb{F}_{p^m})$, we write that

$$x = x_0 + x_1 t + \cdots + x_{m-1} t^{m-1}$$

and analogously,

$$y = y_0 + y_1 t + \cdots + y_{m-1} t^{m-1}, \quad \text{where} \quad x_i, y_i \in \mathbb{F}_p.$$

The next step is to define the decomposition base $\mathcal{B}$

$$B = \{P = (x, y) \in E : x_1 = \cdots = x_{m-1} = 0\}. \quad (18)$$

Using the Hasse-Weil theorem, one obtains $\#\mathcal{B} \approx p$.

In the next step, it is necessary to choose random values $\alpha, \beta \in \overline{0, \#E(\mathbb{F}_{p^m}) - 1}$ and compute $R = [\alpha]P + [\beta]Q$, which should be decomposed as $P_1 + \cdots + P_m = R$, where $P_1, \ldots, P_m \in \mathcal{B}$.

It results in reducing the problem of relation searching to solving a multivariate system of m variables. Such a solution may be efficiently found using the Groebner basis over $\mathbb{F}_p$. Finally, one has to factorize the resulting polynomial in $\mathbb{F}_p[x]$. The cost of finding one relation is polynomial to $\log p$ and exponential to m.

After some improvements, the whole Gaudry-Diem algorithm's final cost is equal to $O(p^{2-\frac{2}{m}})$. It is worth to emphasize that there is a constant in the complexity that depends exponentially on m.

3.2.2. Algebraic approach by Petit et al. [19], [16]

Petit, Kosters, and Messeng proposed an algebraic approach to solve ECDLP over prime fields. They constructed the decomposition base $\mathcal{B}$ of size $p^{\frac{1}{m}}$ and used algebraic or rational map L, for which two conditions have to be satisfied:

- $\#\{x \in \mathbb{F}_p : L(x) = 0\} \approx \#\left\{x \in \overline{\mathbb{F}_p} : L(x) = 0\right\} \approx p^{\frac{1}{m}}$,
- map L may be represented as a composition of maps L_j of low degrees.

Using the construction presented above, they considered the following system of equations to solve

$$\begin{cases} f_{m+1}(x_P, \ldots, x_m, x_R) = 0, \\ L_j(x_{i,j}) = x_{i,j+1}, 1 \leq i \leq m, 1 \leq j \leq r-1, \\ L_r(x_{i,r}) = 0, 1 \leq i \leq m, \end{cases} \tag{19}$$

where each variable x_i is decomposed as

$$x_i = x_{i,1}, L_1(x_{i,1}) = x_{i,2}, \ldots, L_{r-1}(x_{i,r-1}) = x_{i,r}, L_r(x_{i,r}) = 0. \tag{20}$$

The presented method has the following advantages:

- most solutions of System (19) are defined over $\mathbb{F}_p$,
- all the polynomial equations in System (19) have low degrees, so System (19) may be efficiently solved using the Groebner basis algorithm.

Disadvantages:

- the algorithm may be applied only when $p-1$ has a large smooth factor, or we can efficiently construct an elliptic curve $E'/\mathbb{F}_p$, whose order has a large smooth factor.

3.2.3. Variant of Amadori et al. [1], [16]

In this approach, it is required to find a single solution of the equation

$$P_1 + \cdots + P_m = R = [\alpha]P + [\beta]Q.$$

The decomposition base is given by $\mathcal{B} = \{\pm R \in E(\mathbb{F}_p) : R = [\alpha]P + [\beta]Q\}$, for randomly chosen $0 \leq \alpha, \beta \leq n-1$, where $n = \mathrm{Ord}(P)$. It is worth noting that both points R and $-R$ are included in the decomposition base. The size of the decomposition base is then $\#\mathcal{B} \approx p^{\frac{1}{m}}$.

Now let $f(x) = \prod_{v \in V}(x - v)$ be the polynomial generating the vanishing ideal of $V \subset \mathbb{F}_p$ for a variable x. The original system that has to be solved is given by

$$\begin{cases} f_m(x_P, \ldots, x_m) = 0, \\ f(x_1) = 0, \\ \cdots \\ f(x_m) = 0. \end{cases} \tag{21}$$

If any solution is found, we can obtain a relation $P_1 + \cdots + P_m + R = \mathcal{O}$, where $P_1, \ldots, P_m \in \mathcal{B}$. From the construction of the decomposition base, each point P_i is equal to $[\alpha_i]P + [\beta_i]Q$ for some known α_i, β_i. Therefore, it is possible to find linear congruence $[\gamma]P = [\delta]Q$ and solve ECDLP.

In an improved variant, the decomposition base $\mathcal{B}$ is partitioned into m partitions with almost the same sizes $\mathcal{B} = \bigcup_{i=1}^{m} \mathcal{B}_i$ and $\#F_i \approx \#F_j$, for $i \neq j$. For each $q \leq i \leq m$, let V_i denote the set of x-coordinates of points in the partition $\mathcal{B}_i$. Now, one should consider a system

$$\begin{cases} f_m(x_P, \ldots, x_m) = 0, \\ f_1(x_1) = 0, \\ \ldots \\ f_m(x_m) = 0, \end{cases} \tag{22}$$

where $f_i(x)$ is the polynomial generating the vanishing ideal of V_i for every $1 \leq i \leq m$. The degree of every $f_i(x)$ equals to $\#V_i$, which is equal approximately to $\frac{\#V}{m}$ and $\#V_i \approx \#V_j$ for $i \neq j$. In this case, the size s of the decomposition base should fulfill $s \geq mp^{\frac{1}{m}}$.

3.2.4. Improvements of Kudo et al. [16]

Kudo et al. [16] presented three improvements to accelerate the variant of Amadori et al. [1]. They considered the following improvements:

- adoption of the hybrid approach, which is an adaptation of the idea of Bettale et al. [4] to solve multivariate systems over finite fields,
- using symmetries in the hybrid approach, where the symmetry of $f_3(x_1, x_2, x_R)$ is used. Making substitution $t_1 = x_1 + x_2$ and $t_2 = x_1 x_2$, the polynomial f_3 may be rewritten as $f_3'(t_1, t_2, x_R)$, which has total degree 2, comparing to the total degree 4 of polynomial f_3,
- solving system via GCD computation, where efficient computation of $\mathrm{GCD}(f_3(x_1, x_Q, x_R), f(x_1)) \in \mathbb{F}_p[x_1]$ is used.

These three improvements significantly accelerate the variant of Amadori even though this method's complexity is at least $p^{\frac{2}{3}}$, compared to the complexity $p^{\frac{1}{2}}$ of Pollard's rho and baby step - giant step methods.

4. D-Wave and QUBO

This section is mainly based on work [5]. Quantum computing lets us develop new approaches to classically computational hard problems. Many classical methods for the cryptanalysis of both symmetric and asymmetric ciphers can

be transformed to the problem of solving a large system of multivariate polynomial equations. To obtain a solution in such a case, one has to perform two general steps: the first is to represent the problem as a system of multivariate polynomial equations, and the second is to solve the created system.

Because the application of quantum annealing requires the transformation of the problem to the quadratic unconstrained binary optimization (QUBO) problem (or equivalent, e.g., Ising), we start from the formal definition of the QUBO problem.

QUBO is a combinatorial optimization problem in which the cost function $f(x)$ is defined on an n-dimensional binary vector space $\mathbb{B}^n$ onto $\mathbb{R}$, as follows:

$$\text{QUBO}: \min \ f(x) = x^t Q x.$$

In the equation above, x is a vector of binary variables, and Q is an upper diagonal matrix of real weights.

The variables are binary, $x_i^2 = x_i$, so the cost function can be represented as follows:

$$\text{QUBO}: \min \ f(x) = \sum_i Q_{i,i} x_i + \sum_{i<j} Q_{i,j} x_i x_j.$$

Solving the QUBO model is, in general, an NP-hard problem. Nowadays, quantum annealing, which aims to find the global minimum of the cost function in the solution space, gives promising results. The quantum annealing device is implemented in D-Wave systems. The biggest D-Wave Advantage has 5,760 qubits and can solve dense QUBO problems with up to 20,000 binary variables and sparse QUBO problems with up to 1,000,000 binary variables.

So, the obtained QUBO problem may be solved using quantum annealing. The method presented in [5] is as follows. At first, one has to obtain algebraic equations describing a given problem. After obtaining polynomial equations over finite fields (for simplicity, let us assume that the problem is defined over some prime finite field $\mathbb{F}_p$) of the given problem, each equation f has to be transformed to the equation with Boolean variables and integer coefficients, which can be written as $f' = f - pk$. k is an integer for which $k \leq \lfloor \frac{f_{\max}}{p} \rfloor$, and $f_{\max}$ is maximal value which polynomial f can have. It is worth noting that k has to be then written as the sum of Boolean variables

$$k = \sum_{i=0}^{\text{bl}(f_{\max})-1} 2^i k_i + f_{\max} + 1 - 2^{\text{bl}(f_{\max}-1)}, \tag{23}$$

where $bl(x)$ is the bit-length of integer x.

In the next step, which takes place after the transformation of given equations, obtained equations should be linearized. After this operation, one obtains $f'_{\text{lin}_i} = \text{lin}(f'_i)$, where lin denotes linearization operation.

Finally, it is easy to obtain the problem in the QUBO form as

$$(f'_{\text{lin}_0})^2 + \cdots + (f'_{\text{lin}_{n-1}})^2 + \text{Pen} - C.$$

It should be added that Pen denotes penalties obtained during linearization of equations, n is the number of equations and C is constant appearing in the polynomial

$$(f'_{\text{lin}_0})^2 + \cdots + (f'_{\text{lin}_{n-1}})^2 + \text{Pen}\,.$$

5. Solving ECDLP on twisted Edwards curves using quantum annealing - formulation of proper QUBO problem

The section below describes a method for solving ECDLP on twisted Edwards curves using quantum annealing.

5.1. Using symmetries to improve performance

An idea to improve solving ECDLP using the index calculus method was presented by Faugère et al. in 2012. In section 3.1, PDP was defined as finding such decomposition $R = P_1 \oplus \cdots \oplus P_n$ that all points P_i belong to the decomposition base $\mathcal{F}$. Suppose that a solution $P_1 \oplus \cdots \oplus P_n$ is known. Let T_2 be a 2-torsion point. That means, for all $k = 1, \ldots, \lfloor \frac{n}{2} \rfloor$ one has

$$P_1 \oplus \cdots \oplus P_n = P_1 \oplus \cdots \oplus P_n \oplus [2k]T_2 = R, \tag{24}$$

what gives 2^{n-1} decompositions of R obtained by adding an even number of times a 2-torsion point T_2. However, these decompositions do not always correspond to solutions of the PDP because point $P_i \oplus T_2$ does not have to belong to the factor base $\mathcal{F}$.

In our case, where we were looking for a PDP solution containing 2 elements, only 2 possibilities of using point T_2 existed - no using 2-torsion point or adding T_2 to both points from a solution

$$P_1 \oplus P_2 = (P_1 \oplus T_2) \oplus (P_2 \oplus T_2) = R. \tag{25}$$

That increases the number of solutions, thus, it can be solved faster with a hybrid solver.

As written in section 2.2, adding 2-torsion point T_2 to the point $P = (x, y)$ on the twisted Edwards curves gives $P + T_2 = (-x, -y)$. One should change the constraints to use this fact and maximize the probability of finding a relation of elements from a chosen range. The interval $\left[0, \lfloor \sqrt[r]{p} \rfloor\right]$ can be "pushed" backwards and changed into $\left[-\lfloor \sqrt[r]{p}/2 \rfloor, \lfloor \sqrt[r]{p}/2 \rfloor\right]$. Thanks to this, small negative numbers can also be considered as elements of the decomposition base.

5.2. Transformation of relation searching problem into the QUBO problem

Let us define the Semaev approach of relation searching for twisted Edwards curves.

Problem 1.

$$\begin{cases} f_{TE,m+1}(y_1,\ldots,y_m,y_R)=0, \\ 0\le y_1\le p^{\frac{1}{m}}, \\ \ldots \\ 0\le y_m\le p^{\frac{1}{m}}, \end{cases} \tag{26}$$

where $f_{TE,m+1}(y_1,\ldots,y_m,y_R)=0$ is $m+1$-th Semaev polynomial for twisted Edwards curves.

Now consider Semaev's approach to relation searching, given by Problem 1. Formulating the QUBO problem requires having some function to minimize and not having any constraints. That is why the conversion of inequalities is necessary. It may be done by following the steps below.

(1) First of all, variables must be converted to binary form. Based on the idea from [7] and [22], if variable z is from the set $U=\overline{a,b}$ and $\lfloor l=\log_2(b-a)\rfloor$, one can find a surjection $g:2^l\to U$, where $z=g(z_1,\ldots,z_l)=a+\sum_{i=0}^{l-1}(2^i z_i)+\mathrm{bl}((b-a)+1-2^l)z_l$. After transforming each variable, one has to make substitutions in polynomial $f_{TE,m+1}$.

(2) Secondly, a linearization of the equation $f_{TE,m+1}(y_1,\ldots,y_m,y_R)=0$ must be performed. That means that all monomials of a degree greater than 1 must be replaced using new variables, such as $y_iy_j=u_k$. Because of these substitutions, penalties need to be added to the QUBO problem. Each penalty monomial of the form $y_iy_jy_l$ will be constructed in the following way $y_iy_jy_l\to u_ky_l=y_lu_k+2(y_iy_j-2u_k(y_i+y_j)+3u_k)$, just like in [15].

(3) Subsequently, modular equation $f_{TE,m+1}(y_1,\ldots,y_m,y_R)=0$ must be converted to an equation with Boolean variables and integer coefficients. To perform such operation, one should write $f_{TE,m+1}(y_1,\ldots,y_m,y_R)-vp=0$, where v is some positive integer, bounded with maximal value of $f_{TE,m+1}$ over $\mathbb{Z}$. If we assume that maximal value of $f_{TE,m+1}$ equals $f_{\max}$, then bit length of v is lesser or equal to $\log_2\lfloor\frac{f_{\max}}{p}\rfloor+1$. The variable v should be transformed into the binary form as well.

(4) Eventually, using constraints from the previous step in a minimization problem requires using this constraint as a penalty, which, while evaluating the equation with the correct values, gives 0 as a result and otherwise a value bigger than 0. That means QUBO problem should be constructed

as $(f_{TE,m+1}(y_1, \ldots, y_m, y_R) - vp)^2 + \text{Pen}$, where Pen denotes penalties obtained during linearization. Due to this linearization, in the obtained QUBO problem, only monomials of degree 2 may exist. Pen is the sum of all penalties from the previous step, where each of them is multiplied by a square of maximal coefficient appearing in $f_{TE,m+1}(y_1, \ldots, y_m, y_R)$ to be sure that minimal energy will be obtained for a correct solution.

6. Results and analysis

During the International Conference on Computational Science in 2021, Michał Wroński showed how to transform a relation searching problem into a QUBO problem and solve ECDLP on a short Weierstrass curve over an 8-bit prime field. We aimed to improve that achievement using a similar idea, which was described in detail in [22]. An example of the use of this method was described on the website [23].

Since solving the discrete logarithm problem on an elliptic curve over a prime field with a characteristic greater than 8 bits was not feasible with the method mentioned in the previous paragraph, we needed to develop it. We accomplished it with a conception described in section 5.1.

It would be logical to start with a short Weierstrass curve. However, the x--coordinate of the point $P + T_2$ (x-coordinate is used in summation polynomials for that model) does not depend only on x-coordinate of the point P, so it is not suitable to use it for our approach.

We decided to use another elliptic curve model known for its efficient arithmetic - Montgomery's model. To simplify our work and use built-in commands, for example, to find an elliptic curve's generator or order, we started with a short Weierstrass curve. We then transformed it via an isomorphism to the desired model.

An elliptic curve in short Weierstrass model is given by

$$E_{SW}/\mathbb{F}_{1021} : y^2 = x^3 + Ax + B.$$

We assumed that $A \equiv -3 \mod p$. Then, we had to choose such B that requirements for short Weierstrass→ Montgomery curve isomorphism were met. That means:

- order of E_{SW} is divisible by 4,
- $z^3 + Az + B$ has at least one root $r \in \mathbb{F}_p$,
- $3r^2 + A$ is a quadratic residue in $\mathbb{F}_p$.

One of the lowest numbers meeting the above conditions was 63, which gave $E_W : y^2 = x^3 + 1018x + 63$ with the generator $P_W = (568, 232)$.

Transformation into the Montgomery curve $E_M : by^2 = x^3 + ax^2 + x$ with generator $P_M = (x_M, y_M)$ could be performed with formulas:

$$\begin{cases} b &= \left(\sqrt{3r^2 + a}\right)^{-1}, \\ a &= 3rb\,, \\ x_M &= b(x_W - r)\,, \\ y_M &= y_W b\,. \end{cases}$$

That gave us $b = 848,\ a = 992$, therefore $E_M : 848y^2 = x^3 + 992x^2 + x$ with the generator $P_M = (102, 704)$. With knowledge about these parameters, one can perform the index calculus method using quantum annealing. Unfortunately, it did not succeed in our case - D-Wave did not solve the relation searching problem for the curve $E_M : 848y^2 = x^3 + 992x^2 + x$.

We decided to try a slightly different approach to make use of our previous work. Our idea was to apply an isomorphism again, but this time from the Montgomery curve into the twisted Edwards curve, as it has efficient arithmetic as well as the source curve. To obtain such curve $E_{TE} : a_{TE}x^2 + y^2 = 1 + d_{TE}x^2y^2$ with a generator $P_{TE} = (x_{TE}, y_{TE})$, one need to perform calculations:

$$\begin{cases} a_{TE} &= \frac{a+2}{b}, \\ d_{TE} &= \frac{a-2}{b}, \\ x_{TE} &= \frac{x_M}{y_M}, \\ y_{TE} &= \frac{x_{TE}-1}{x_{TE}+1}. \end{cases}$$

That gave us $a_{TE} = 490,\ d = 71$, therefore $E_{TE} : 490x^2 + y^2 = 1 + 71x^2y^2$ with $\mathrm{ord}(E_{TE}) = 4 \cdot 241$ and generator $P_E = (792, 566)$.

According to section 5.1, elements of the decomposition base $\mathcal{F}$ had to be in the range $\left[-\lfloor \sqrt[v]{p}/2 \rfloor, \lfloor \sqrt[v]{p}/2 \rfloor\right]$, what in our case gave us an interval $\left[-\lfloor \sqrt{1021}/2 \rfloor, \lfloor \sqrt{1021}/2 \rfloor\right] = [-16, 16]$. Numbers from that range can be represented as 6 bits (5 bits for a number and 1 for a sign). To improve efficiency at the cost of only a slight reduction of the number of possible points in the decomposition base $\mathcal{F}$, we decided to cut 1 number bit and focus on coordinates with a maximum of 5 bits (4 bits for number and 1 for a sign).

Let us present the results of our application of the described method. We tried to solve ECDLP $log_P Q$ for twisted Edwards elliptic curve $E_{TE} : 490x^2 + y^2 = 1 + 71x^2y^2$, where $P = (792, 566)$ was a generator of a group of points of order 241 and $Q = [m]P = (542, 258)$ was a m^{th} multiplicity of P. We obtained a decomposition base with 5 elements, which were

$$\mathcal{F} = \{-7, -4, -2, 5, 6\}, \tag{27}$$

which may be identified with points

$$\{\pm P_1, \pm P_2, \pm P_3, \pm P_4, \pm P_5\} = \\ \{\pm(513 : -7 : 1), \pm(279 : -4 : 1), \pm(165 : -2 : 1), \pm(482 : 5 : 1), \pm(394 : 6 : 1)\}. \tag{28}$$

In the next step, converting into binary form and linearization of the 3rd Semaev's summation polynomial is necessary. It was performed as described in section 5.2.

After finishing operations mentioned in the previous paragraph, we could have started searching for such relations that $[\alpha]\,P + [\beta]\,Q = R = \pm P_i \pm P_j$, where:

- P was a generator,
- Q was a resulting point,
- α and β were random values,
- P_i and P_j were points from decomposition base $\mathcal{F}$.

To find a solution of ECDLP for a decomposition base with 5 elements, we needed to find 6 relations. To obtain each of them, we had to choose random α and β, calculate $R = [\alpha]\,P + [\beta]\,Q$, and then find such combination of two points P_i, P_j from the decomposition base that $R = \pm P_i \pm P_j$. This part was performed by looking for solutions y_1, y_2 of Semaev's summation polynomial $f_{TE,3}(y_1, y_2, y_R) = 0$ by the D-Wave computer's hybrid solver, which was searching for values satisfying the linearized equation. Each searching has lasted 30 seconds of the hybrid solver time.

The first pair of α and β was $\alpha = 3, \beta = 13$. That gave us $R_1 = [3]\,P + [13]\,Q = (331, 877)$. The D-wave computer found that $R_1 = (331, 877) = P_1 + P_3$, so we added a vector $[1, 0, 1, 0, 0]$ to the relations matrix M.

The second pair of the random values was $\alpha = 11, \beta = 10$, what meant that $R_2 = [11]\,P + [10]\,Q = (587, 443)$. The relation from the hybrid solver was $R_2 = (587, 443) = P_4 + P_5$. We extended the matrix M by a vector $[0, 0, 0, 1, 1]$.

The third pair was $\alpha = 10, \beta = 15$. That gave us $R_3 = [10]\,P + [15]\,Q = (900, 808)$. The D-wave computer found that such $R_3 = P_5 + P_5 = [2]P_5$, so we added a vector $[0, 0, 0, 0, 2]$ to the relations matrix M.

The fourth pair of α and β was $\alpha = 19, \beta = 6$, what meant that $R_4 = [19]\,P + [6]\,Q = (433, 25)$. The relation from the hybrid solver was $R = P_1 + P_2$. We extended the matrix M by a vector $[1, 1, 0, 0, 0]$.

The fifth pair of the random values was $\alpha = 10, \beta = 6$. That gave us $R_5 = [10]\,P + [6]\,Q = (619, 98)$. The D-wave computer found that $R_5 = P_4 - P_5$, so we added a vector $[0, 0, 0, 1, -1]$ to the relations matrix M.

The sixth and the last pair of the random values was $\alpha = 10, \beta = 12$, which meant that $R_6 = [10]\,P + [12]\,Q = (620, 650)$. The relation from the hybrid solver was $R_6 = -P_2 + P_3$. We extended the matrix M by a vector $[0, -1, 1, 0, 0]$.

After finding $\#\mathcal{F}+1$ relations, we were able to construct matrixes as in [23]

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & -1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \end{bmatrix} = \begin{bmatrix} [3]P & + & [13]Q \\ [11]P & + & [10]Q \\ [10]P & + & [15]Q \\ [19]P & + & [6]Q \\ [10]P & + & [6]Q \\ [10]P & + & [12]Q \end{bmatrix}.$$

Then a non-zero element of the kernel of matrix M should be found, so such vector $[k_1, k_2, k_3, k_4, k_5, k_6]$ is needed that

$$\begin{bmatrix} k_1 & k_2 & k_3 & k_4 & k_5 & k_6 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & -1 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

One of the solutions is $[-1, -1, 1, 1, 1, 1]$.

That was time for a final step. We needed to multiply matrixes

$$\begin{bmatrix} -1 & -1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} [3]P & + & [13]Q \\ [11]P & + & [10]Q \\ [10]P & + & [15]Q \\ [19]P & + & [6]Q \\ [10]P & + & [6]Q \\ [10]P & + & [12]Q \end{bmatrix} =$$

$$\begin{aligned} &(-1)([3]P + [13]Q) + (-1)([11]P + [10]Q) + \\ &\quad ([10]P + [15]Q) + ([19]P + [6]Q) + ([10]P + [6]Q) + ([10]P + [12]Q) = \\ &\qquad - [3]P - [13]Q - [11]P - [10]Q + [10]P + [15]Q + [19]P + [6]Q + \\ &\qquad\qquad [10]P + [6]Q + [10]P + [12]Q = [35]P + [16]Q = 0. \end{aligned} \quad (29)$$

Finally, $[35]P = [225]Q \Leftrightarrow Q = [43]P$ and ECDLP has been solved.

7. Conclusion and further works

This paper discusses the application of symmetries to speed up the relations searching step using quantum annealing for the index calculus method for elliptic curves over prime fields. We applied the index calculus method using quantum annealing for twisted Edwards curves, where at the relations searching step, one can use, in this case, symmetries and, therefore, faster find necessary relations. The idea of the application of symmetries of twisted Edwards curves to the index calculus method was first shown by Faugère et al. [13]. However, the main

difference is that in [13], authors searched for relations using the Groebner basis. In this paper, we aimed to apply some quantum methods for the relations searching step, and therefore we used quantum annealing, especially nowadays promising quantum method, as one of them.

Our main result was finding a discrete logarithm on the elliptic curve E_{TE} : $490x^2 + y + 2 = 1 + 71x^2y^2$ defined over a prime field $\mathbb{F}_{1021}$. The group size generated by the generator $P_{TE} = (792, 566)$ was equal to 241. It is up now the biggest ECDLP problem which has been broken using the hybrid quantum-classical method.

The further works should focus on searching for optimal QUBO problem shape equivalent to the relations searching step, which may allow solving bigger problems.

REFERENCES

[1] AMADORI, A.—PINTORE, F.—SALA, M.: *On the discrete logarithm problem for prime-field elliptic curves*, Finite Fields and Their Applications **51** (2018), 168–182.

[2] BERNSTEIN, D. J.—BIRKNER, P.—JOYE, M.—LANGE, T.—PETERS, C.: *Twisted Edwards Curves*. In: *Progress in Cryptology — AFRICACRYPT 2008* (S. Vaudenay, ed.), Springer-Verlag, Berlin 2008, pp. 389–405.

[3] BERNSTEIN, D. J.—LANGE, T.: *Faster Addition and Doubling on Elliptic Curves*. In: *Advances in Cryptology — ASIACRYPT 2007* (K. Kurosawa, ed.), Springer-Verlag, Berlin, 2007.

[4] BETTALE, L.—FAUGERE, J.-C.—PERRET, L.: *Hybrid approach for solving multivariate systems over finite fields*, J. Math. Cryptol. **3** (2009), 177–197.

[5] BUREK, E.—WROŃSKI, M.—MAŃK, K.—MISZTAL, M.: *Algebraic attacks on block ciphers using quantum annealing*, IEEE Transactions on Emerging Topics in Computing **10** (2022), 678–689.

[6] CHEN, Y.-A.—GAO, X.-S.: *Quantum algorithm for Boolean equation solving and quantum algebraic attack on cryptosystems*, J. Syst. Sci. Complex. **35** (2022), 373–412.

[7] CHEN, Y.-A.—GAO, X.-S.—YUAN, C.-M.: *Quantum algorithm for optimization and polynomial system solving over finite field and application to cryptanalysis*, arXiv preprint arXiv:1802.03856, 2018.

[8] DIEM, C.: *The GHS attack in odd characteristic*, J. Ramanujan Math. Soc. **18** (2003), 1–32.

[9] DIEM, C.: *On the discrete logarithm problem in elliptic curves*, Compos. Math.**147** (2011), 75–104.

[10] DRIDI, R.—ALGHASSI, H.: *Prime factorization using quantum annealing and computational algebraic geometry*, Scientific Reports **7**, Article no. 43048 (2017), 1–10; https://doi.org/10.1038/srep43048

[11] DRYŁO, R.—KIJKO, T.—WROŃSKI, M.: *Determining formulas related to point compression on alternative models of elliptic curves*, Fundamenta Informaticae **169** (2019), 285–294.

[12] EDWARDS, H. M.: *A normal form for elliptic curves*, Bull. Amer. Math. Soc. **44** (2007), 393–422.

[13] FAUGÈRE, J.-C.—GAUDRY, P.—HUOT, L.—RENAULT, G.: *Using symmetries in the index calculus for elliptic curves discrete logarithm*, J. Cryptology **27** (2014), 595–635.

[14] GAUDRY, P.: *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, Journal of Symbolic Computation **44** (2009), 1690–1702.
[15] JIANG, S.—BRITT, K. A.—MCCASKEY, A. J.—HUMBLE, T. S.—KAIS, S.: *Quantum annealing for prime factorization*, Scientific Reports **8** (2018), 1–9; https://doi.org/10.1038/s41598-018-36058-z
[16] KUDO, M.—YOKOTA, Y.—TAKAHASHI, Y.—YASUDA, M.: *Acceleration of index calculus for solving ECDLP over prime fields and its limitation*. In: *Cryptology and Network Security* (J. Camenisch, P. Papadimitratos, eds.), Springer International Publishing. Cham, 2018. pp. 377–393.
[17] LENSTRA JR, H. W.: *Factoring integers with elliptic curves*, Ann. Math. (1987), 649–673.
[18] MONTGOMERY, P. L.: *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comput. **48** (1987), 243–264.
[19] PETIT, C.—KOSTERS, M.—MESSENG, A.: *Algebraic approaches for the elliptic curve discrete logarithm problem over prime fields*, In: *Public-Key Cryptography — PKC 2016* (C.-M. Cheng, K.-M. Chung, G. Persiano, B.-Y. Yang, eds.), Springer-Verlag, Berlin, 2016, pp. 3–18.
[20] SEMAEV, I.: *Summation polynomials and the discrete logarithm problem on elliptic curves*, Cryptology ePrint Archive, Paper 2004/031, (2004); https://ia.cr/2004/031
[21] WANG, B.—HU, F.—YAO, H.—WANG, C.: *Prime factorization algorithm based on parameter optimization of Ising model*, Scientific Reports **10** (2020), 1–10; https://doi.org/10.1038/s41598-020-62802-5
[22] WROŃSKI, M.: *Index calculus method for solving elliptic curve discrete logarithm problem using quantum annealing*. In: *International Conference on Computational Science*, Springer-Verlag, 2021. pp. 149–155.
[23] WROŃSKI, M.: *Index calculus method for solving elliptic curve discrete logarithm problem using quantum annealing - example* 2021; https://github.com/Michal-Wronski/ECDLP-index-calculus-using-QUBO
[24] WROŃSKI, M.: *Practical solving of discrete logarithm problem over prime fields using quantum annealing*. In: *International Conference on Computational Science*, Springer-Verlag, 2022, pp. 93–106.

Received October 5, 2022
Revised August 7, 2024
Accepted August 19, 2024
Publ. online November 10, 2024

Łukasz Dzierzkowski
Faculty of Cybernetics
Military University of Technology
Kaliskiego Str. 2
00-908–Warsaw
POLAND
E-mail: lukasz.dzierzkowski@wat.edu.pl

Michał Wroński
Department of Cryptology,
NASK National Research Institute
Kolska Str. 12
01-045–Warsaw
POLAND
E-mail: michal.wronski@nask.pl