Index calculus method for solving elliptic curve discrete logarithm problem using quantum annealing - example

Michał Wroński[1][0000−0002−8679−9399]

Military University of Technology, Kaliskiego Str. 2, Warsaw, Poland
michal.wronski@wat.edu.pl

Abstract. This is example of application of method presented in the paper "Index calculus method for solving elliptic curve discrete logarithm problem using quantum annealing" accepted to International Conference on Computational Science 2021 (ICCS 2021).

1 Example

We will present an example of the application of the given method. At first, let us assume that $p = 13$ and an elliptic curve E is given by an equation $E/\mathbb{F}_p : y^2 = x^3 + 2x + 4$, where $\#E(\mathbb{F}_p) = 17$. Point R is equal to $(12, 12) = [\alpha]P + [\beta]Q$ for generator $P = (10, 6)$, resulting point $Q = [k]P = (5, 3)$ and random values $\alpha = 3, \beta = 10$. Moreover, $m = 2$, so we try to find the decomposition of R as a sum of two points from decomposition base $\mathcal{B}$, $R = P_1 + P_2$. We will use in this case 3-rd Semaev summation polynomial $f_3(x_1, x_2, x_R) = 0$.

Decomposition base $\mathcal{B}$ is then equal to

$$\mathcal{B} = \{0, 2\}, \tag{1}$$

which may be identified with points

$$\{\pm(0 : 2 : 1), \pm(2 : 4 : 1)\} = \{\pm P_1, \pm P_2\}. \tag{2}$$

From this moment, we operate on integers, not on elements from field $\mathbb{F}_p$.

Because points in decomposition base $\mathcal{B}$ have their x-coordinates limited by $\lfloor\sqrt{p}\rfloor = 3$, and one can estimate that $v \leq 9$ in this case. Then one can write for boolean variables $u_1, \ldots, u_8$ that

$$\begin{cases} x_1 = u_1 + 2u_2, \\ x_2 = u_3 + 2u_4, \\ v = u_5 + 2u_6 + 4u_7 + 2u_8. \end{cases} \tag{3}$$

Then, after making a substitution, one has to linearize $f_{m+1}(x_1, \ldots, x_m, x_R)$, which gives in result polynomial with 16 terms
$3u_1u_2u_3u_4 + 12u_1u_2u_3 + 6u_1u_2u_4 + 12u_1u_3u_4 + 6u_2u_3u_4 + 4u_1u_2 + 12u_1u_3 +$

$17u_1u_4 + 17u_2u_3 + 11u_2u_4 + 4u_3u_4 + 2u_1 + 6u_2 + 2u_3 + 6u_4 + 7.$

In the next step, one needs to transform this polynomial of degree 4 to the linear polynomial of degree 1. It is necessary to make 11 substitutions

$u_9 = u_1u_2, u_{10} = u_1u_3, u_{11} = u_1u_4, u_{12} = u_2u_3, u_{13} = u_2u_4, u_{14} = u_3u_4, u_{15} = u_3u_9, u_{16} = u_4u_9, u_{17} = u_4u_{10}, u_{18} = u_4u_{12}, u_{19} = u_9u_{14}.$

So after linearization, one obtains

$2u_1+6u_2+2u_3+6u_4+4u_9+12u_{10}+17u_{11}+17u_{12}+11u_{13}+4u_{14}+12u_{15}+6u_{16}+12u_{17}+6u_{18}+3u_{19}+7.$

Now one computes $(f_{m+1}(x_1,\ldots,x_m,x_R)-vp)^2$, which gives in result
$4u_1^2+24u_1u_2+8u_1u_3+24u_1u_4-52u_1u_5-104u_1u_6-208u_1u_7-104u_1u_8+16u_1u_9+48u_1u_{10}+68u_1u_{11}+68u_1u_{12}+44u_1u_{13}+16u_1u_{14}+48u_1u_{15}+24u_1u_{16}+48u_1u_{17}+24u_1u_{18}+12u_1u_{19}+36u_2^2+24u_2u_3+72u_2u_4-156u_2u_5-312u_2u_6-624u_2u_7-312u_2u_8+48u_2u_9+144u_2u_{10}+204u_2u_{11}+204u_2u_{12}+132u_2u_{13}+48u_2u_{14}+144u_2u_{15}+72u_2u_{16}+144u_2u_{17}+72u_2u_{18}+36u_2u_{19}+4u_3^2+24u_3u_4-52u_3u_5-104u_3u_6-208u_3u_7-104u_3u_8+16u_3u_9+48u_3u_{10}+68u_3u_{11}+68u_3u_{12}+44u_3u_{13}+16u_3u_{14}+48u_3u_{15}+24u_3u_{16}+48u_3u_{17}+24u_3u_{18}+12u_3u_{19}+36u_4^2-156u_4u_5-312u_4u_6-624u_4u_7-312u_4u_8+48u_4u_9+144u_4u_{10}+204u_4u_{11}+204u_4u_{12}+132u_4u_{13}+48u_4u_{14}+144u_4u_{15}+72u_4u_{16}+144u_4u_{17}+72u_4u_{18}+36u_4u_{19}+169u_5^2+676u_5u_6+1352u_5u_7+676u_5u_8-104u_5u_9-312u_5u_{10}-442u_5u_{11}-442u_5u_{12}-286u_5u_{13}-104u_5u_{14}-312u_5u_{15}-156u_5u_{16}-312u_5u_{17}-156u_5u_{18}-78u_5u_{19}+676u_6^2+2704u_6u_7+1352u_6u_8-208u_6u_9-624u_6u_{10}-884u_6u_{11}-884u_6u_{12}-572u_6u_{13}-208u_6u_{14}-624u_6u_{15}-312u_6u_{16}-624u_6u_{17}-312u_6u_{18}-156u_6u_{19}+2704u_7^2+2704u_7u_8-416u_7u_9-1248u_7u_{10}-1768u_7u_{11}-1768u_7u_{12}-1144u_7u_{13}-416u_7u_{14}-1248u_7u_{15}-624u_7u_{16}-1248u_7u_{17}-624u_7u_{18}-312u_7u_{19}+676u_8^2-208u_8u_9-624u_8u_{10}-884u_8u_{11}-884u_8u_{12}-572u_8u_{13}-208u_8u_{14}-624u_8u_{15}-312u_8u_{16}-624u_8u_{17}-312u_8u_{18}-156u_8u_{19}+16u_9^2+96u_9u_{10}+136u_9u_{11}+136u_9u_{12}+88u_9u_{13}+32u_9u_{14}+96u_9u_{15}+48u_9u_{16}+96u_9u_{17}+48u_9u_{18}+24u_9u_{19}+144u_{10}^2+408u_{10}u_{11}+408u_{10}u_{12}+264u_{10}u_{13}+96u_{10}u_{14}+288u_{10}u_{15}+144u_{10}u_{16}+288u_{10}u_{17}+144u_{10}u_{18}+72u_{10}u_{19}+289u_{11}^2+578u_{11}u_{12}+374u_{11}u_{13}+136u_{11}u_{14}+408u_{11}u_{15}+204u_{11}u_{16}+408u_{11}u_{17}+204u_{11}u_{18}+102u_{11}u_{19}+289u_{12}^2+374u_{12}u_{13}+136u_{12}u_{14}+408u_{12}u_{15}+204u_{12}u_{16}+408u_{12}u_{17}+204u_{12}u_{18}+102u_{12}u_{19}+121u_{13}^2+88u_{13}u_{14}+264u_{13}u_{15}+132u_{13}u_{16}+264u_{13}u_{17}+132u_{13}u_{18}+66u_{13}u_{19}+16u_{14}^2+96u_{14}u_{15}+48u_{14}u_{16}+96u_{14}u_{17}+48u_{14}u_{18}+24u_{14}u_{19}+144u_{15}^2+144u_{15}u_{16}+288u_{15}u_{17}+144u_{15}u_{18}+72u_{15}u_{19}+36u_{16}^2+144u_{16}u_{17}+72u_{16}u_{18}+36u_{16}u_{19}+144u_{17}^2+144u_{17}u_{18}+72u_{17}u_{19}+36u_{18}^2+36u_{18}u_{19}+9u_{19}^2+28u_1+84u_2+28u_3+84u_4-182u_5-364u_6-728u_7-364u_8+56u_9+168u_{10}+238u_{11}+238u_{12}+154u_{13}+56u_{14}+168u_{15}+84u_{16}+168u_{17}+84u_{18}+42u_{19}+49.$

Moreover, we have to add penalties to the function o, according to Equation (**??**). So finally, the objective function o is a quadratic function of 19 variables and 191 terms and is in the QUBO form
$2336u_1u_2+1164u_1u_3+602u_1u_4-52u_1u_5-104u_1u_6-208u_1u_7-104u_1u_8-4608u_1u_9-2264u_1u_{10}-1088u_1u_{11}+68u_1u_{12}+44u_1u_{13}+16u_1u_{14}+48u_1u_{15}+24u_1u_{16}+48u_1u_{17}+24u_1u_{18}+12u_1u_{19}+1180u_2u_3+650u_2u_4-156u_2u_5-$

$312u_2u_6 - 624u_2u_7 - 312u_2u_8 - 4576u_2u_9 + 144u_2u_{10} + 204u_2u_{11} - 2108u_2u_{12} - 1024u_2u_{13} + 48u_2u_{14} + 144u_2u_{15} + 72u_2u_{16} + 144u_2u_{17} + 72u_2u_{18} + 36u_2u_{19} + 1180u_3u_4 - 52u_3u_5 - 104u_3u_6 - 208u_3u_7 - 104u_3u_8 + 594u_3u_9 - 2264u_3u_{10} + 68u_3u_{11} - 2244u_3u_{12} + 44u_3u_{13} - 2296u_3u_{14} - 1108u_3u_{15} + 24u_3u_{16} + 48u_3u_{17} + 24u_3u_{18} + 12u_3u_{19} - 156u_4u_5 - 312u_4u_6 - 624u_4u_7 - 312u_4u_8 + 626u_4u_9 + 722u_4u_{10} - 952u_4u_{11} + 782u_4u_{12} - 1024u_4u_{13} - 2264u_4u_{14} + 144u_4u_{15} - 1084u_4u_{16} - 1012u_4u_{17} - 1084u_4u_{18} + 36u_4u_{19} + 676u_5u_6 + 1352u_5u_7 + 676u_5u_8 - 104u_5u_9 - 312u_5u_{10} - 442u_5u_{11} - 442u_5u_{12} - 286u_5u_{13} - 104u_5u_{14} - 312u_5u_{15} - 156u_5u_{16} - 312u_5u_{17} - 156u_5u_{18} - 78u_5u_{19} + 2704u_6u_7 + 1352u_6u_8 - 208u_6u_9 - 624u_6u_{10} - 884u_6u_{11} - 884u_6u_{12} - 572u_6u_{13} - 208u_6u_{14} - 624u_6u_{15} - 312u_6u_{16} - 624u_6u_{17} - 312u_6u_{18} - 156u_6u_{19} + 2704u_7u_8 - 416u_7u_9 - 1248u_7u_{10} - 1768u_7u_{11} - 1768u_7u_{12} - 1144u_7u_{13} - 416u_7u_{14} - 1248u_7u_{15} - 624u_7u_{16} - 1248u_7u_{17} - 624u_7u_{18} - 312u_7u_{19} - 208u_8u_9 - 624u_8u_{10} - 884u_8u_{11} - 884u_8u_{12} - 572u_8u_{13} - 208u_8u_{14} - 624u_8u_{15} - 312u_8u_{16} - 624u_8u_{17} - 312u_8u_{18} - 156u_8u_{19} + 96u_9u_{10} + 136u_9u_{11} + 136u_9u_{12} + 88u_9u_{13} + 610u_9u_{14} - 1060u_9u_{15} - 1108u_9u_{16} + 96u_9u_{17} + 48u_9u_{18} - 1132u_9u_{19} + 408u_{10}u_{11} + 408u_{10}u_{12} + 264u_{10}u_{13} + 96u_{10}u_{14} + 288u_{10}u_{15} + 144u_{10}u_{16} - 868u_{10}u_{17} + 144u_{10}u_{18} + 72u_{10}u_{19} + 578u_{11}u_{12} + 374u_{11}u_{13} + 136u_{11}u_{14} + 408u_{11}u_{15} + 204u_{11}u_{16} + 408u_{11}u_{17} + 204u_{11}u_{18} + 102u_{11}u_{19} + 374u_{12}u_{13} + 136u_{12}u_{14} + 408u_{12}u_{15} + 204u_{12}u_{16} + 408u_{12}u_{17} - 952u_{12}u_{18} + 102u_{12}u_{19} + 88u_{13}u_{14} + 264u_{13}u_{15} + 132u_{13}u_{16} + 264u_{13}u_{17} + 132u_{13}u_{18} + 66u_{13}u_{19} + 96u_{14}u_{15} + 48u_{14}u_{16} + 96u_{14}u_{17} + 48u_{14}u_{18} - 1132u_{14}u_{19} + 144u_{15}u_{16} + 288u_{15}u_{17} + 144u_{15}u_{18} + 72u_{15}u_{19} + 144u_{16}u_{17} + 72u_{16}u_{18} + 36u_{16}u_{19} + 144u_{17}u_{18} + 72u_{17}u_{19} + 36u_{18}u_{19} + 32u_1 + 120u_2 + 32u_3 + 120u_4 - 13u_5 + 312u_6 + 1976u_7 + 312u_8 + 7008u_9 + 3780u_{10} + 2261u_{11} + 3995u_{12} + 2009u_{13} + 3540u_{14} + 2046u_{15} + 1854u_{16} + 2046u_{17} + 1854u_{18} + 1785u_{19} + 49.$

Finally, one can solve this problem using, for example, a quantum annealing computer, which gives in result
$u_1 = 0, u_2 = 1, u_3 = 0, u_4 = 0, u_5 = 1, u_6 = 0, u_7 = 0, u_8 = 0, u_9 = 0, u_{10} = 0, u_{11} = 0, u_{12} = 0, u_{13} = 0, u_{14} = 0, u_{15} = 0, u_{16} = 0, u_{17} = 0, u_{18} = 0, u_{19} = 0,$
which has minimal energy equal to 0 (our QUBO problem is constructed in such a way that minimal energy, with high probability, is equal to 0 because in our QUBO problem appears constant energy offset).

We know that point R is the sum of two points, whose x-coordinates are equal to $u_1+2u_2 = 2$ and $u_3+2u_4 = 0$. We check that $R = (2,4)+(0,2) = P_2+P_1$, and we add vector $[1,1]$ to our relation matrix M, which, after collecting of $\#\mathcal{B}+1$ relations, we will be able to solve and find the discrete logarithm $\log_P Q$.

In the next step we choose $R = [6]P + [7]Q = (2,9)$. It is obvious, that $R = -P_2$ and we add vector $[0,-1]$ to matrix M. We need to find one more relation. We find the point $R = [11]P + [5]Q = (8,5)$. We formulate the QUBO problem, and finally one finds the solution
$u_1 = 0, u_2 = 1, u_3 = 0, u_4 = 1, u_5 = 0, u_6 = 0, u_7 = 1, u_8 = 0, u_9 = 0, u_{10} = 0, u_{11} = 0, u_{12} = 0, u_{13} = 1, u_{14} = 0, u_{15} = 0, u_{16} = 0, u_{17} = 0, u_{18} = 0, u_{19} = 0.$

We know that point R is a sum of two points, whose x-coordinates are equal to 2. We check that $R = [2](2,4) = [2]P_2$ and we add vector $[0,2]$ to our relation matrix M.

Finally, one obtains matrix equation

$$\begin{bmatrix} 1 & 1 \\ 0 & -1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} [3]P + [10]Q \\ [6]P + [7]Q \\ [11]P + [5]Q \end{bmatrix}.$$

Now, let us compute any nonzero element $[k_1, k_2, k_3]$ of the kernel K of matrix $\begin{bmatrix} 1 & 1 \\ 0 & -1 \\ 0 & 2 \end{bmatrix}$. It follows, that $[k_1, k_2, k_3] \begin{bmatrix} 1 & 1 \\ 0 & -1 \\ 0 & 2 \end{bmatrix} = [0,0]$ and of the kernel's element is $[k_1, k_2, k_3] = [0,2,1]$. What's more, now we can compute $[0,2,1] \begin{bmatrix} [3]P + [10]Q \\ [6]P + [7]Q \\ [11]P + [5]Q \end{bmatrix} = 0\,([3]P + [10]Q) + 2\,([6]P + [7]Q) + ([11]P + [5]Q) = [6]P + [19]Q = 0$. So $[6]P = [15]Q$ and finally $Q = [14]P$.