



# Practical example from paper "Transformation of the discrete logarithm problem over $\mathbb{F}_{2^n}$ to the QUBO problem using normal bases"

Michał Wroński  and Mateusz Leśniak 

NASK - National Research Institute, Warsaw, Poland,  
[michal.wronski@nask.pl](mailto:michal.wronski@nask.pl), [mateusz.lesniak@nask.pl](mailto:mateusz.lesniak@nask.pl)

---

**Keywords:** Quantum annealing · Discrete Logarithm Problem · Binary fields · QUBO · normal bases

---

## Introduction

Below we present a working example of practical solving discrete logarithm problem over  $\mathbb{F}_{2^3}$  field. The example is part of the paper "Transformation of the discrete logarithm problem over  $\mathbb{F}_{2^n}$  to the QUBO problem using normal bases" submitted to the 24th edition of the Central European Cryptology Conference (CECC 2024).

## 1 Working example

Let's consider multiplicative subgroup of field  $\mathbb{F}_{2^3}$  generated by irreducible polynomial  $f(t) = t^3 + t^2 + 1$ . Let  $g = t$  be the generator of this subgroup. Let  $h = t^2 + 1$ . We will show how to transform this problem to the QUBO form.

### 1.1 Transformation of the example problem

At first let's look that the order of multiplicative subgroup  $\mathbb{F}_{2^3}^*$  is equal to 7, which is prime. Therefore we have to solve the following problem:

$$g^y \equiv h \pmod{f(t)}, \quad (1)$$

which is equivalent to the problem of solving

$$t^y \equiv t^4 + t^2 \pmod{t^3 + t^2 + 1}, \quad (2)$$

where  $y = 4u_2 + 2u_1 + u_0$ , for binary variables  $u_0, u_1, u_2$ .

Let's note, that it is equivalent to

$$t^{4u_2+2u_1+u_0} = t^{4u_2} t^{2u_1} t^{u_0} = t^{4u_2} t^{2u_1} t^{u_0} \equiv t^2 + 1 \pmod{t^3 + t^2 + 1}. \quad (3)$$

As we use normal basis system representation, in this system one can use vector notation, in which  $t = [0, 0, 1]$  and  $t^2$  and  $t^4$  are just simply rotations of  $t$ . In such a case  $t^2 = [0, 1, 0]$  and  $t^4 = [1, 0, 0]$ . Let's note that neutral element in normal basis is  $t^4 + t^2 + t = [1, 1, 1]$ . Let's take the multiplication matrix  $T$ , defined as (such matrix may be easily obtained using method for generation such a matrix for normal bases of  $\Pi$  type given in [1]):

$$T^{(0)} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}. \quad (4)$$

Now let  $A, B, C \in \mathbb{F}_{2^3}$ , where  $C = A \cdot B$ . Then product  $C$  is given by

$$\begin{aligned} c_0 &= a_2b_2 + a_1b_2 + a_2b_1 + a_0b_1 + a_1b_0, \\ c_1 &= a_0b_0 + a_2b_0 + a_0b_2 + a_1b_2 + a_2b_1, \\ c_2 &= a_1b_1 + a_0b_1 + a_1b_0 + a_2b_0 + a_0b_2. \end{aligned} \quad (5)$$

Now let's note that

$$t^{u_0} = \begin{cases} 1 = t + t^2 + t^4, u_0 = 0, \\ t, u_0 = 1. \end{cases} \quad (6)$$

So  $t^{u_0}$  may be presented as:

$$t^{u_0} = t + (1 - u_0)t^2 + (1 - u_0)t^4 = [1 - u_0, 1 - u_0, 1]. \quad (7)$$

Writing  $t^{u_0}$  in general form and using new variables, one obtains  $t^{u_0} = v_{0,0}t + v_{0,1}t^2 + v_{0,2}t^4$ , where  $v_{0,0} = 1, v_{0,1} = 1 - u_0, v_{0,2} = 1 - u_0$ .

Now let's perform the multiplication of  $t^{u_0}$  by  $t^{u_1}$ . Similarly as before, if  $u_1 = 0$ , then the result will be equal to  $t^{u_0} = [v_{0,2}, v_{0,1}, v_{0,0}]$ . If  $u_1 = 1$ , then one has to use Equation (5). In such a case the resulting vector  $[v_{1,2}, v_{1,1}, v_{1,0}]$  will be of the following form:

$$\begin{cases} v_{1,0} = v_{0,2}u_1 + v_{0,0}u_1 + (1 - u_1)v_{0,0}, \\ v_{1,1} = v_{0,2}u_1 + (1 - u_1)v_{0,1}, \\ v_{1,2} = v_{0,1}u_1 + v_{0,0}u_1 + (1 - u_1)v_{0,2}. \end{cases} \quad (8)$$

Now let's note that System of equations above will have to be taken into account while analyzing the transformation of the DLP over  $\mathbb{F}_{2^3}$  to the QUBO problem.

Finally, the last step is multiplication of  $[v_{1,2}, v_{1,1}, v_{1,0}]$  by  $t^4$ . This step goes as follows:

$$\begin{cases} v_{2,0} = v_{1,2}u_2 + v_{1,1}u_2 + (1 - u_2)v_{1,0} = 0, \\ v_{2,1} = v_{1,0}u_2 + v_{1,1}u_2 + (1 - u_2)v_{1,1} = 1, \\ v_{2,2} = v_{1,0}u_2 + (1 - u_2)v_{1,2} = 1. \end{cases} \quad (9)$$

But let's note that the vector  $[v_{2,2}, v_{2,1}, v_{2,0}]$  is equal to  $t^2 + 1$ , so in vector form it will be  $[1, 1, 0]$ .

Now we transform and simplify the system of equations given above.

Let us note that at first:

$$\begin{cases} u_3 = 1, \\ u_4 = 1 - u_0, \\ u_5 = 1 - u_0 = u_4. \end{cases} \quad (10)$$

Then

$$\begin{cases} u_6 = u_5u_1 + u_3u_1 + (1 - u_1)1 = u_4u_1 + u_3u_1 + 1 - u_1 = u_4u_1 + 1, \\ u_7 = u_4u_1 + (1 - u_1)u_4 = u_4, \\ u_8 = u_4u_1 + u_1 + (1 - u_1)u_4 = u_1 + u_4. \end{cases} \quad (11)$$

And then

$$\begin{cases} 0 = u_2u_8 + u_2u_7 + (1 - u_2)u_6 = u_2u_8 + u_2u_4 + (1 - u_2)u_6, \\ 1 = u_2u_6 + u_2u_7 + (1 - u_2)u_7 = u_2u_6 + u_7 = u_2u_6 + u_4, \\ 1 = u_2u_6 + (1 - u_2)u_8 = u_2u_6 + u_8 - u_2u_8, \end{cases} \quad (12)$$

Taking into account the whole equations, making at first linearization, removing all terms on the left side and making squaring, and, finally adding at the end penalty, one can obtain final QUBO form of our problem of solving DLP over binary fields. This method is presented

in details for example in [2] and [3]. The necessary equations to prepare the final QUBO problems are given below:

$$\begin{cases} F_1 = (1 - u_0 - u_4)^2, \\ F_2 = (1 - u_6 - u_{10})^2, \\ F_3 = (u_8 + u_1 + u_4 - 2 * u_{14})^2, \\ F_4 = (-u_{11} + u_{12} + u_6 - u_{13})^2, \\ F_5 = (1 - u_{13} - u_4)^2, \\ F_6 = (1 - u_{13} - u_8 + u_{11})^2, \\ Pen = 0, \\ Pen = Penalty(u_1, u_4, u_{10}), \\ Pen = Pen + Penalty(u_2, u_8, u_{11}), \\ Pen = Pen + Penalty(u_2, u_4, u_{12}), \\ Pen = Pen + Penalty(u_2, u_6, u_{13}), \end{cases} \quad (13)$$

where  $Pen$  is standard penalty in Rosenberg form and final QUBO problem is given by  $F = F_1 + F_2 + F_3 + F_4 + F_5 + F_6 + Pen$ .

We transformed the problem above into the QUBO problem using 11 logical variables. We obtained the correct solution of  $y = 5$  using quantum annealing.

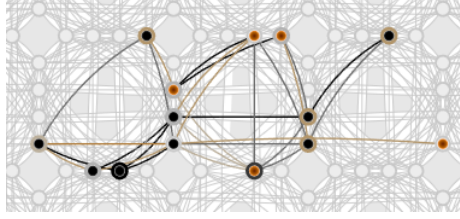


Figure 1: Embedding of DLP for  $\mathbb{F}_{2^3}$  in the D-Wave Advantage 2 QPU

Parameter	Value	Number of source variables	11
Name (chip ID)	Advantage2_prototype2.3	Number of target variables	14
Available qubits	1,248	Max chain length	2
Topology	Zephyr	Chain strength	1.8827
Number of reads	10,000	QPU access time ( $\mu s$ )	804,627.61
Annealing time ( $\mu s$ )	20	QPU programming time ( $\mu s$ )	19,227.61
Anneal schedule	[[0,0],[20,1]]	QPU sampling time ( $\mu s$ )	785,400
H gain schedule	[[0,0],[20,1]]	Total post processing time ( $\mu s$ )	1
Programming thermalization ( $\mu s$ )	1000	Post processing overhead time ( $\mu s$ )	1

Table 1: D-Wave Advantage solver parameters used in solving QUBO problem equivalent to the problem of finding elliptic curve discrete logarithm over  $\mathbb{F}_7$  on Edwards curve in the subgroup of size 8.

We run quantum annealing for the problem above 10 000 times. 7 415 trials gave proper minimal energy, what means that for the given example, the probability of obtaining proper result is equal to 74.15%.

**In the presentation during the conference and in the full paper in the post-conference proceedings, we will detail how the practical example for the  $\mathbb{F}_{2^3}$  field can be solved using quantum annealing.**

## References

- [1] Alaaeldin Amin and Turki Faisal Al-Somani. Hardware implementations of gf ( $2^m$ ) arithmetic using normal basis. *Journal of Applied Sciences*, 6(6):1362–1372, 2006.

- [2] Michał Wroński. Practical solving of discrete logarithm problem over prime fields using quantum annealing. In *Computational Science – ICCS 2022*, pages 93–106, Cham, 2022. Springer International Publishing.
- [3] Michał Wroński, Elżbieta Burek, Łukasz Dzierzkowski, and Olgierd Żołnierczyk. Transformation of elliptic curve discrete logarithm problem to qubo using direct method in quantum annealing applications. *Journal of Telecommunications and Information Technology*, (1):75–82, 2024.