


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, 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 us consider the 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 $h = t^4 + t^2$. We will show how to transform this problem to the QUBO form.

1.1 Transformation of the example problem

First, let us look at 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 . We use normal bases now instead of polynomial bases.

Let us note that it is equivalent to

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

As we use normal basis system representation, one can use vector notation in which $t = [0, 0, 1]$ and t^2 and t^4 are simply rotations of t . In such a case $t^2 = [0, 1, 0]$ and $t^4 = [1, 0, 0]$. Let us note that the neutral element in normal basis is $t^4 + t^2 + t = [1, 1, 1]$.

Let us take the multiplication matrix T , defined as (such matrix may be easily obtained using method for generation such a matrix for normal bases of II 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 us 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^{2u_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 $u_1 = 1$, one must 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 the system of equations above must be considered 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^{4u_2} . 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 $t^4 + t^2$, so in vector form it will be $[1, 1, 0]$.

Now, we transform and simplify the system of equations given above. We set $u_3 = v_{0,0}, u_4 = v_{0,1}, u_5 = v_{0,2}, u_6 = v_{1,0}, u_7 = v_{1,1}, u_8 = v_{1,2}, v_{2,0} = 0, v_{2,1} = 1, v_{2,2} = 1$.

Let us note that 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 the final QUBO form of our problem of solving DLP over binary fields. This method is presented in detail, for example, in [2] and [3]. The necessary equations to prepare the final QUBO problems are given below. Let us note that in the system below-using arithmetic tricks, the

number of additional variables necessary to represent the multiplicities of 2 after transforming the equation from the boolean function to the pseudo boolean function is lowered.

$$\begin{cases} F_1 = (1 - u_0 - u_4)^2, \\ F_2 = (1 - u_6 - u_{10})^2, \\ F_3 = (u_8 + u_1 + u_4 - 2 * u_{14})^2, \\ F_4 = (-u_{11} + u_{12} + u_6 - u_{13})^2, \\ F_5 = (1 - u_{13} - u_4)^2, \\ F_6 = (1 - u_{13} - u_8 + u_{11})^2, \\ Pen_1 = Penalty(u_1, u_4, u_{10}), \\ Pen_2 = Penalty(u_2, u_8, u_{11}), \\ Pen_3 = Penalty(u_2, u_4, u_{12}), \\ Pen_4 = Penalty(u_2, u_6, u_{13}), \end{cases} \quad (13)$$

where Pen is a standard penalty in Rosenberg form: when is made substitution $z = xy$, the resulting penalty is of the form $(xy - 2(x + y)z + 3z)$ and is obtained by invoking function $Penalty(x, y, z)$. Then, the final QUBO problem is given by $F = F_1 + F_2 + F_3 + F_4 + F_5 + F_6 + Pen_1 + Pen_2 + Pen_3 + Pen_4$.

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

The scheme presenting embedding of our problem into the D-Wave Advantage 2 prototype 2.3 system having 1248 qubits is presented in Figure 1.

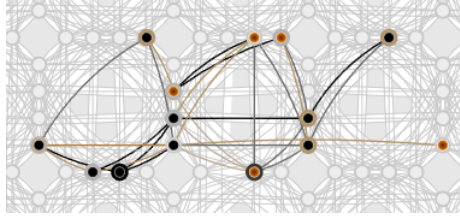


Figure 1: Embedding of DLP for \mathbb{F}_{2^3} in the D-Wave Advantage 2 QPU

The problem and used solver parameters are presented in Table 1.

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 (μs)	804,627.61
Annealing time (μs)	20	QPU programming time (μs)	19,227.61
Anneal schedule	[[0,0],[20,1]]	QPU sampling time (μs)	785,400
H gain schedule	[[0,0],[20,1]]	Total post-processing time (μs)	1
Programming thermalization (μs)	1000	Post processing overhead time (μs)	1

Table 1: D-Wave Advantage solver parameters used in solving QUBO problem equivalent to the problem of finding discrete logarithm over \mathbb{F}_{2^3} in the subgroup of size 7.

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

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.