Successful Shor's Factorization of N=1031167 using the IBM Quantum Systems

Jiří Tomčala

IT4Innovations, VŠB – Technical University of Ostrava

Short introduction

So far, the highest number factorized on a quantum computer using Shor's algorithm was 35. This poster shows that much larger numbers can be factorized using this algorithm on current quantum computers. The factorization of number 1031167, along with results from the IBM quantum systems, is shown.

Shor's algorithm [1] was proposed in 1994, but only now has quantum technology evolved to such a level that its realization has become possible. The bottleneck of this algorithm is the implementation of the modular exponentiation function (MEF), which is the subject of this poster and also my paper [2].

The task of the quantum part of this algorithm is to find the period r of the MEF $f(x) = a^x \bmod N$ (a is a appropriately chosen integer and N is a number being factorized) and for this purpose it is necessary to construct and run a so-called period-finder quantum circuit. Once the period r is found, the factors can then be calculated by using this formula: $\gcd(a^{r/2} \pm 1, N)$.

The MEF can be decomposed in this way:

$$a^x \bmod N = (...((a^{x_0 2^0} \bmod N) \times a^{x_1 2^1} \bmod N) \times ...) \times a^{x_{n-1} 2^{n-1}} \bmod N$$

where $(x_{n-1}x_{n-2}\ ...\ x_2x_1x_0)_2$ is the binary representation of the variable x. This decomposition makes it possible to construct the period-finder circuit (Figure 1). For the factorization of $N = 1031167$, it is appropriate to choose $a = 6882$.

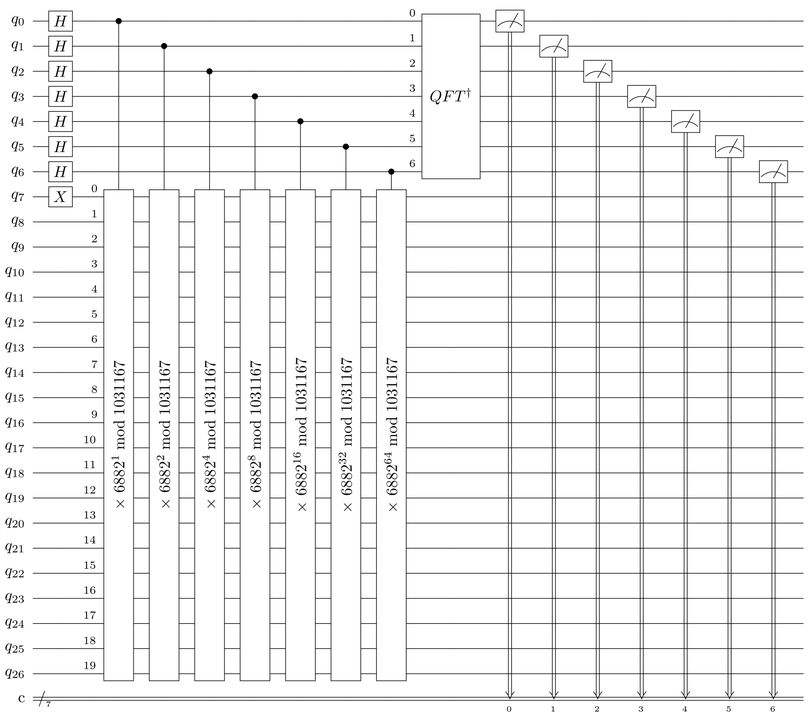

Figure 1: Period-finder circuit for function $f(x) = 6882^x \bmod 1031167$.

Modular Exponentiation Functions

Implementations of MEFs: $g_i(y) = (y \times 6882^{2^i}) \bmod 1031167$ in Figure 1 should respond to inputs in the manner expressed in Table 1. No other values will appear on their inputs, so there is no need to take them into account when designing each individual MEF implementation. This made the quantum circuits implementing these MEFs quite simple. They are shown in Figure 2.

i	Input = y		Output = (y $\times 6882^{2^i}$) mod 1031167
0	0000 0000 0000 0000 0001 (1)	→	0000 0001 1010 1110 0010 (6882)
1	0000 0000 0000 0000 0001 (1)	→	1110 1010 0011 1011 0001 (959409)
	0000 0001 1010 1110 0010 (6882)	→	0001 0110 0001 0100 0101 (90437)
2	0000 0000 0000 0000 0001 (1)	→	1001 0000 1111 0100 0101 (593733)
	0000 0001 1010 1110 0010 (6882)	→	1000 1111 0100 0110 0100 (586852)
	0001 0110 0001 0100 0101 (90437)	→	0111 1010 1110 0000 0001 (503297)
	1110 1010 0011 1011 0001 (959409)	→	1010 0010 0111 1001 0100 (665492)

Table 1: Truth tables of the functions $g_i(y) = (y \times 6882^{2^i}) \bmod 1031167$.

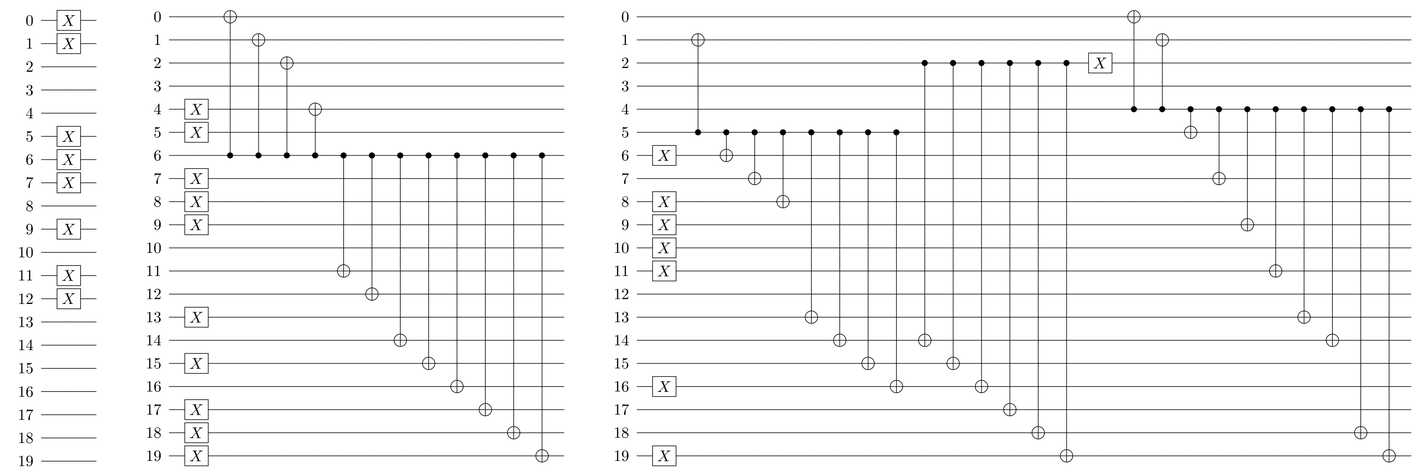

Figure 2: Quantum circuits implementing the functions $g_i(y) = (y \times 6882^{2^i}) \bmod 1031167$, from left to right $i = 0, 1, 2$.

Results

The quantum circuits shown above were programmed using Qiskit framework [3] and the results (Figures 3 and 4) were measured on the IBM quantum systems *ibm_brisbane* and *ibm_kyoto*.

As can be seen from the resulting quasi-probability distributions, the period $r = 8$ can be determined from their number of peaks. The factors then can be simply calculated as $\gcd(a^{r/2} \pm 1, N) = \gcd(6882^4 \pm 1, 1031167)$, which are the numbers 1049 and 983.

Since 1049 × 983 = 1031167, it can be stated that the highest number successfully factorized on a real quantum computer using Shor's algorithm is now 1031167.

Acknowledgement

This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic through the e-INFRA CZ (ID:90254).

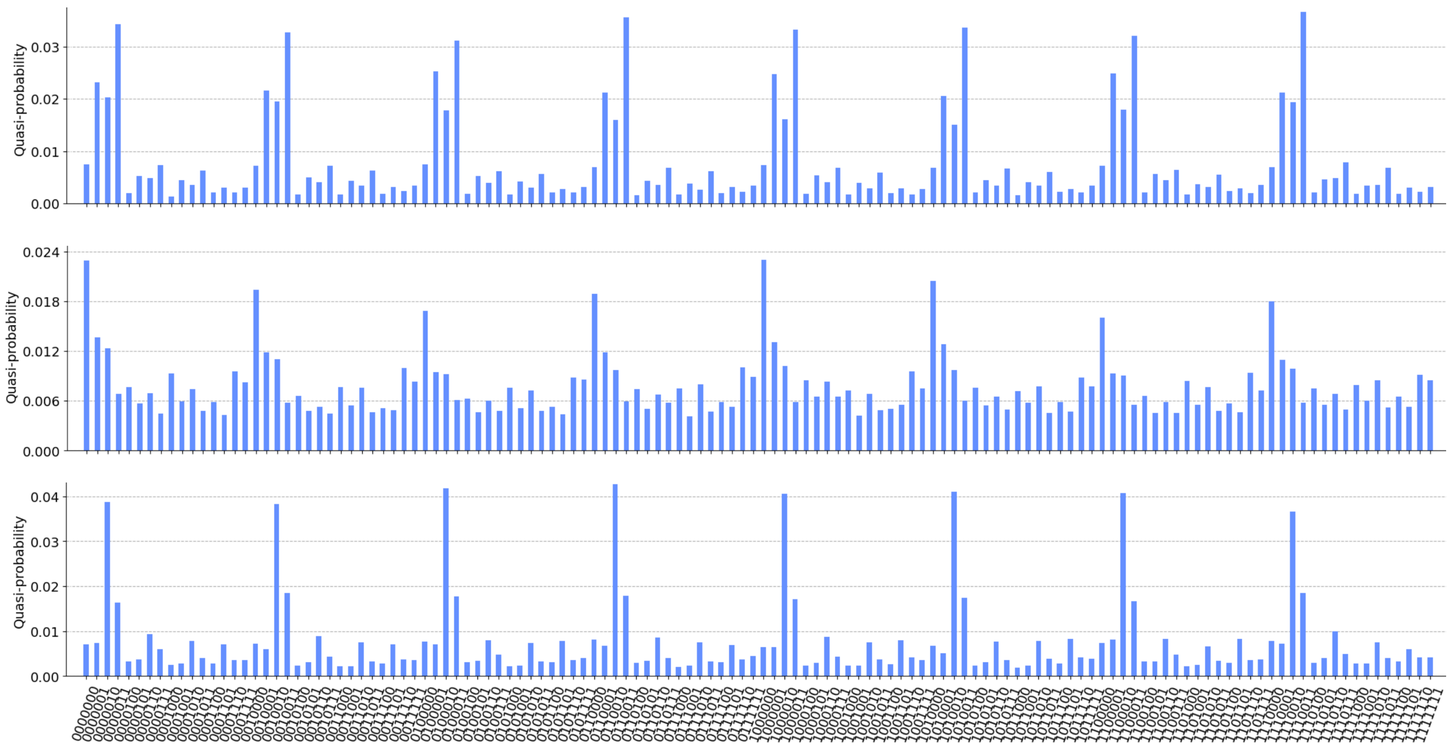

Figure 3: The resulting histograms obtained using the Qiskit framework [3] and the IBM Quantum systems *ibm_brisbane* (upper and middle) and *ibm_kyoto* (bottom) with Eagle R3 quantum processors. All using 100000 shots.

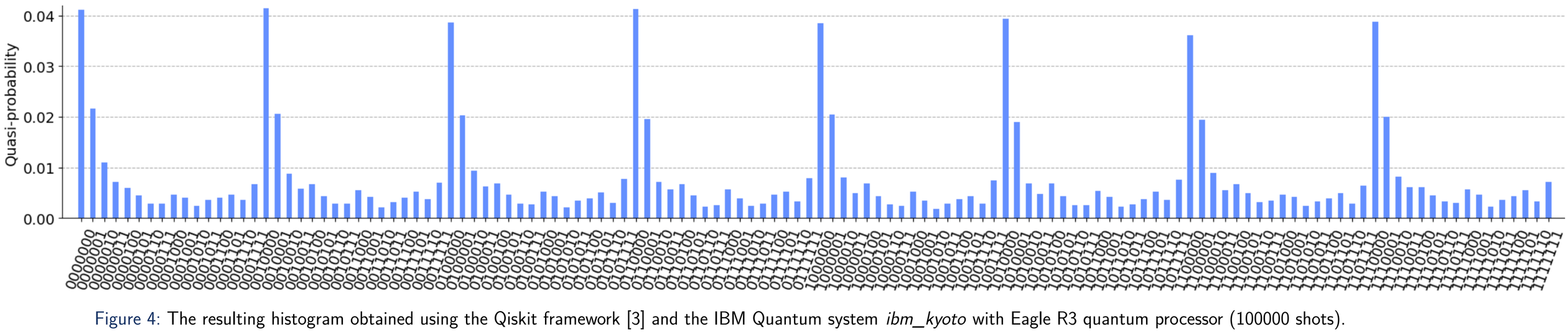

Figure 4: The resulting histogram obtained using the Qiskit framework [3] and the IBM Quantum system *ibm_kyoto* with Eagle R3 quantum processor (100000 shots).

References

[1] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994.

[2] Jiří Tomčala. On the various ways of quantum implementation of the modular exponentiation function for Shor's factorization. *International Journal of Theoretical Physics*, 63(14), 2024.

[3] Qiskit contributors. Qiskit: An open-source framework for quantum computing, 2023.

Contact Information

E-mail: jiri.tomcala@vsb.cz
Web: https://www.it4i.cz/en

VSB TECHNICAL UNIVERSITY OF OSTRAVA | IT4INNOVATIONS NATIONAL SUPERCOMPUTING CENTER