«Пример применения квантового алгоритма Шора для решения задачи дискретного логарифмирования в группе точек эллиптической кривой над конечным простым полем»

РусКрипто 2025

НИЦ Академии криптографии РФ, МГТУ им. Н.Э. Баумана

Квантовый алгоритм Шора, 1994 г.

Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring, doi:10.1109/sfcs.1994.365700 – дискретное логарифмирование в $(\mathbb{Z}_p^*, \cdot) = \{1, \ldots, p-1\}$ (т.е. в мультипликативной группе поля $GF(p)$, p – простое число).

ГОСТ 34.10-2018 основан на сложности ECDLP

Требуется реализация групповой операции сложения точек эллиптической кривой P и Q в виде квантовой схемы с минимальным количеством необходимых квантовых ресурсов – кубитов и квантовых гейтов.

Для реализации $|P\rangle + Q \mapsto |P+Q\rangle$ требуются базовые операции с $x, y \in GF(p)$:

1) $|x\rangle \mapsto |(x + const) \mod p\rangle$,
2) $|x\rangle\,|y\rangle \mapsto |x\rangle\,|y + x \mod 2^n\rangle$
3) $|x\rangle|y\rangle \mapsto |x\rangle|(y + x) \mod p\rangle$,
4) $|x\rangle \mapsto |(2x) \mod p\rangle$,
5) $|x\rangle|y\rangle|0\rangle \mapsto |x\rangle|y\rangle|(x \cdot y) \mod p\rangle$,
6) $|x\rangle \mapsto |x^{-1} \mod p\rangle$.
7) $|x\rangle \mapsto |-x \mod p\rangle$.

В процессе вычислений указанных операций используемые дополнительные кубиты должны возвращаться в исходные состояния для возможности их дальнейшего повторного использования.

Каноническая форма ЭК (форма Вейерштрасса, см. ГОСТ 34.10-2018)

Эллиптической кривой (далее ЭК) E, определенной над $GF(p)$ ($p > 3$ – простое число), называется множество пар (x, y), $x, y \in GF(p)$ для которых

$$y^2 = x^3 + ax + b (\mathrm{mod}\ p),$$

где $a, b \in GF(p)$ и $4a^3 + 27b^2 \neq 0 \mod p$.

Для произвольных точек $Q_1(x_1, y_1)$ и $Q_2(x_2, y_2)$ кривой E вводится операция сложения:

1. Если $x_1 \neq x_2$, то $Q_1(x_1, y_1) + Q_2(x_2, y_2) = Q_3(x_3, y_3)$,

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 (\mathrm{mod}\ p), \\ y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p), \end{cases}$$

   где $\lambda = \frac{y_2 - y_1}{x_2 - x_1} (\mathrm{mod}\ p)$, а точнее $\lambda = (y_2 - y_1) \cdot (x_2 - x_1)^{-1} (\mathrm{mod}\ p)$.
2. Если $x_1 = x_2$ и $y_1 = y_2 \neq 0$, то координаты Q_3:

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 (\mathrm{mod}\ p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p), \end{cases}$$

   где $\lambda \equiv \frac{3x_1^2 + a}{2y_1} (\mathrm{mod}\ p)$.
3. Если $x_1 = x_2$ и $y_1 = -y_2 (\mathrm{mod}\ p)$, то сумма точек $Q_1 + Q_2 = O$ называется нулевой точкой O. В этом случае точка Q_2 называется отрицанием точки Q_1. Для нулевой точки O выполнены равенства

$$Q + O = O + Q = Q,$$

   где Q - произвольная точка ЭК E.

$(E, +)$ – это группа (мн-во элементов с бинарной операцией)

Относительно введенной операции сложения множество всех точек ЭК E, вместе с нулевой точкой, образуют конечную абелеву (коммутативную) группу порядка q:

$$p + 1 - 2\sqrt{p} \leq q \leq p + 1 + 2\sqrt{p}.$$

Точка Q называется «точкой кратности k» если для некоторой точки P выполнено равенство $Q = P + \ldots + P = kP$. В литературе вместо kP встречается обозначение $P + \ldots + P = [k]P$.

Задача дискретного логарифмирования в группе точек ЭК (ECDLP)

Для заданных точек P и Q требуется найти такое значение k, что $Q = [k]P$.

В схемах ЭЦП точка P – общий известный параметр, генератор всей группы ЭК, т.е. любой элемент $Z \in (E, +)$ представляется в виде $Z = [m]P$, $m \in \mathbb{N}$, k – секретный ключ, $Q = [k]P$ – открытый ключ (ключ проверки подписи). Например, см. параметры ЭК в рекомендациях Р 50.1.114-2016 «Параметры эллиптических кривых для криптографических алгоритмов и протоколов».

P.S. Существуют другие представления ЭК[1]. Считается, что минимальное кол-во кубит достигается при использовании канонической формы Вейерштрасса.

[1] См. 1) Василенко О.Н. Новые методы вычисления кратной точки эллиптической кривой над конечным полем, 2008. 2) Василенко О.Н. О вычислении кратных точек на эллиптических кривых над конечными полями с использованием нескольких оснований систем счисления и новых видов координат, 2011.

Известные публикации

1) *Proos J., Zalka C.* Shor's discrete logarithm quantum algorithm for elliptic curves, 2003;
2) *Roetteller M., Naehrig M., Svore K.M., Lauter K.* Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms, 2017;
3) *Häner T., Jaques S., Naehrig M., Roetteler M., Soeken M.* Improved Quantum Circuits for Elliptic Curve Discrete Logarithms, 2020; (далее [HanJNRS2020])
   - (Low Width) $\approx 8n + 10.2\lfloor \lg n \rfloor - 1$ логических кубит, $2800n^3 - 1.08 \cdot 2^{31}$ гейтов[2];
   - (Low T-gates) $\approx 10n + 7.4\lfloor \lg n \rfloor + 1.3$ кубит, $6262n^3 / \lg n - 1.72 \cdot 2^{24}$ гейтов;
   - (Low Depth) $\approx 11n + 3.9\lfloor \lg n \rfloor + 16.5$ кубит, $12478n^3 / \lg n - 1.25 \cdot 2^{29}$ гейтов.
4) *Litinski D., Alto P.* How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates, 2023;
5) *Gouzien E., Ruiz D., Regent F.M., Guillaud J., Sangouard, N.* Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126 133 Cat Qubits, 2023. (Требуется $\approx 9n + w_e + 4$ кубит, $448n^3/w_e$ CNOT и $348n^3/w_e$ гейтов Тоффоли, $w_e = 2\log_2 n$. При использовании полу-классического сумматора из [HanRS2017][3] можно получить схему на $8n + w_e + 6$ логических кубитах).

[2] При $n < \sqrt[3]{(1.08 \cdot 2^{31})/2800} = 93$ получается отрицательное количество гейтов!!!

[3] *Häner T., Roetteler M., Svore K.M.* Factoring using 2n+2 qubits with Toffoli based modular multiplication, Quantum Information & Computation 17, 673 (2017), 1611.07995

ECDLP сводится к задаче поиска периода некоторой $f(x_1, x_2)$

К ECDLP применим квантовый алгоритм Шора

Рассматривается функция $f(x_1, x_2) = [x_1]P + [x_2]Q$, у которой есть два периода:

1) $f(x_1 + q, x_2) = [x_1 + q]P + [x_2]Q = f(x_1, x_2)$ при $q = |(E, +)|$ и
2) $f(x_1 + k, x_2 - 1) = [x_1 + k]P + [x_2 - 1]Q = [x_1]P + Q + [x_2 - 1]Q = f(x_1, x_2)$.

Так как $Q = [k]P$ (k надо найти, точки P и Q знаем), $[x_1]P + [x_2]Q = [x_1]P + [x_2]([k]P)$.

В [GouRRGS2023] рассматривают $f(x_1, x_2) = [x_1]P - [x_2]Q$, для которой

$$\forall t f(x_1 + k \cdot t, x_2 + t) = [x_1 + kt]P - [x_2 + t]Q = [x_1]P + [t]Q - [x_2]Q + [-t]Q = f(x_1, x_2)$$

Квантовая схема алгоритма Шора для ECDLP

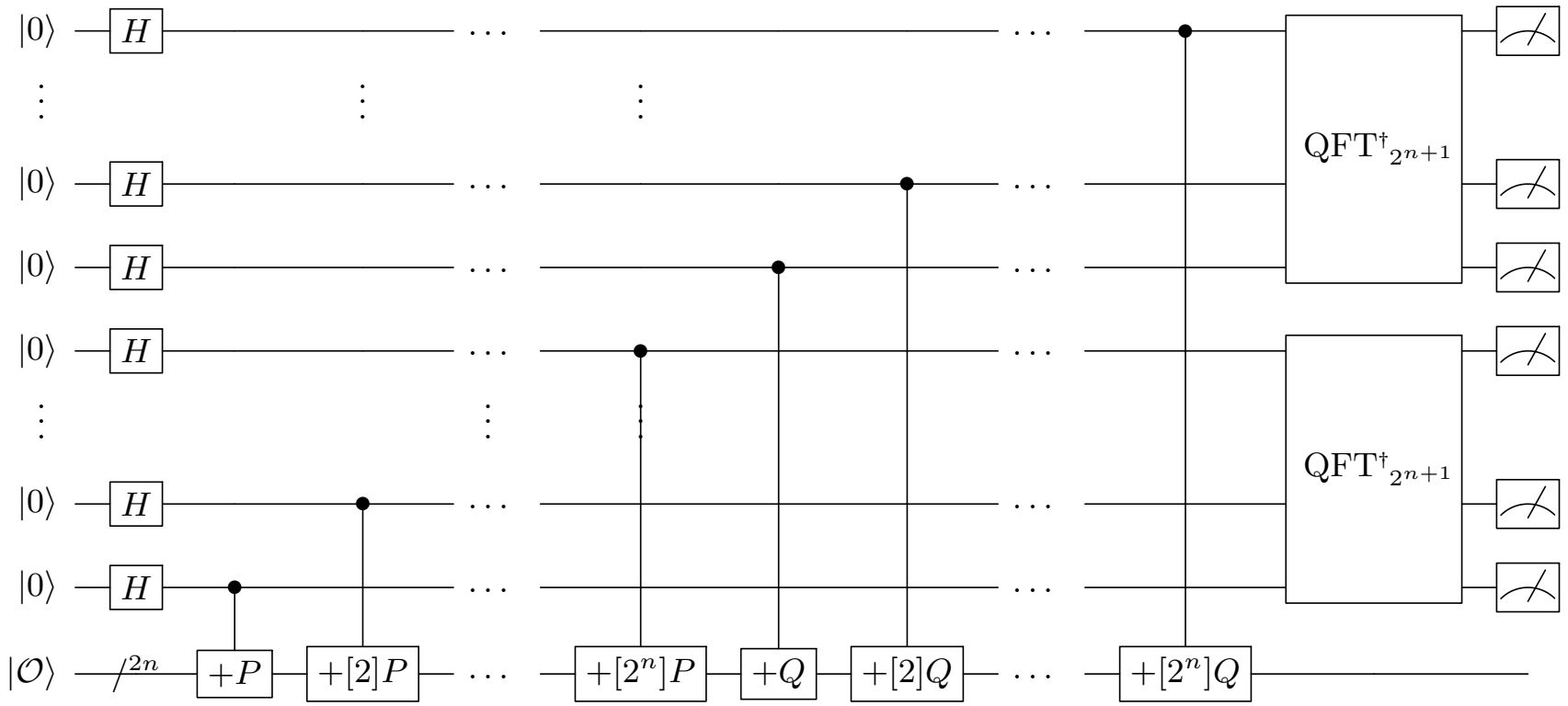

Рис. 1: Квантовая схема алгоритма Шора для решения задачи ECDLP. Элемент P – известный порождающий элемент циклической подгруппы группы точек ЭК, на «вход» алгоритма подается точка Q, требуется определить $k \in \{1, \ldots, ord(P)\}$, при котором $Q = [k]P$.

В регистр «аккумулятор» последовательно (в данном варианте $2n + 2$ раза) применяем контролируемые операторы, реализующие сложение «аккумулятора» с заранее вычисленны точками $P, [2]P, [4]P, \ldots [2^n]P$ и $Q, [2]Q, [4]Q, \ldots [2^n]Q$.

Рассмотрим пример

$p = 29$, $n = \lceil \log_2 p \rceil = 5$, $y^2 = x^3 + 4x + 20 \mod 29$

Выбранному уравнению соответствуют 36 пар (x, y), $x, y \in \overline{0, 28}$:

(0,7), (0,22), (1,5), (1,24), (2,6), (2,23), (3,1), (3,28), (4,10), (4,19), (5,7), (5,22), (6,12), (6,17), (8,10), (8,19), (10,4), (10,25), (13,6), (13,23), (14,6), (14,23), (15,2), (15,27), (16,2), (16,27), (17,10), (17,19), (19,13), (19,16), (20,3), (20,26), (24,7), (24,22), (27,2), (27,27) – точки ЭК, вместе с нейтральным элементом $O = (0, 0)$ и определенной выше операцией сложения, задают группу точек ЭК. В этой группе всего 37 элементов, т.е. у неё нет нетривиальных собственных подгрупп.

Таблица Кэли выбранной группы $(E, +)$

"+"	{0,0}	{0,7}	{0,22}	{1,5}	{1,24}	{2,6}	{2,23}	{3,1}	{3,28}	{4,10}	{4,19}	{5,7}	{5,22}	{6,12}	{6,17}	{8,10}	{8,19}	{10,4}	{10,25}	{13,6}	{13,23}	{14,6}	{14,23}	{15,2}	{15,27}	{16,2}	{16,27}	{17,10}	{17,19}	{19,13}	{19,16}	{20,3}	{20,26}	{24,7}	{24,22}	{27,2}	{27,27}
{0,0}	{0,0}	{0,7}	{0,22}	{1,5}	{1,24}	{2,6}	{2,23}	{3,1}	{3,28}	{4,10}	{4,19}	{5,7}	{5,22}	{6,12}	{6,17}	{8,10}	{8,19}	{10,4}	{10,25}	{13,6}	{13,23}	{14,6}	{14,23}	{15,2}	{15,27}	{16,2}	{16,27}	{17,10}	{17,19}	{19,13}	{19,16}	{20,3}	{20,26}	{24,7}	{24,22}	{27,2}	{27,27}
{0,7}	–	{6,12}	{0,0}	{3,28}	{27,27}	{20,3}	{4,19}	{1,24}	{17,19}	{2,6}	{5,7}	{24,22}	{4,10}	{10,4}	{0,22}	{8,19}	{16,27}	{13,23}	{6,17}	{10,25}	{17,10}	{19,13}	{24,7}	{27,2}	{19,16}	{8,10}	{20,26}	{3,1}	{13,6}	{15,2}	{14,23}	{16,2}	{2,23}	{5,22}	{14,6}	{1,5}	{15,27}
{0,22}	–	–	{6,17}	{27,2}	{3,1}	{4,10}	{20,26}	{17,10}	{1,5}	{5,22}	{2,23}	{4,19}	{24,7}	{0,7}	{10,25}	{16,2}	{8,10}	{6,12}	{13,6}	{17,19}	{10,4}	{24,22}	{19,16}	{19,13}	{27,27}	{20,3}	{8,19}	{13,23}	{3,28}	{14,6}	{15,27}	{2,6}	{16,27}	{14,23}	{5,7}	{15,2}	{1,24}
{1,5}	–	–	–	{4,19}	{0,0}	{27,27}	{2,6}	{0,22}	{5,7}	{1,24}	{20,3}	{16,2}	{3,1}	{17,19}	{15,2}	{14,23}	{24,7}	{13,6}	{19,13}	{14,6}	{10,25}	{8,19}	{13,23}	{20,26}	{6,12}	{19,16}	{5,22}	{6,17}	{24,22}	{16,27}	{10,4}	{15,27}	{4,10}	{17,10}	{8,10}	{2,23}	{0,7}
{1,24}	–	–	–	–	{4,10}	{2,23}	{27,2}	{5,22}	{0,7}	{20,26}	{1,5}	{3,28}	{16,27}	{15,27}	{17,10}	{24,22}	{14,6}	{19,16}	{13,23}	{10,4}	{14,23}	{13,6}	{8,10}	{6,17}	{20,3}	{5,7}	{19,13}	{24,7}	{6,12}	{10,25}	{16,2}	{4,19}	{15,2}	{8,19}	{17,19}	{0,22}	{2,6}
{2,6}	–	–	–	–	–	{1,5}	{0,0}	{20,26}	{15,27}	{27,2}	{0,7}	{6,12}	{15,2}	{16,2}	{5,22}	{13,6}	{10,25}	{8,10}	{24,7}	{14,23}	{8,19}	{13,23}	{14,6}	{3,1}	{5,7}	{17,19}	{6,17}	{16,27}	{19,16}	{17,10}	{24,22}	{3,28}	{0,22}	{19,13}	{10,4}	{1,24}	{4,19}
{2,23}	–	–	–	–	–	–	{1,24}	{15,2}	{20,3}	{0,22}	{27,27}	{15,27}	{6,17}	{5,7}	{16,27}	{10,4}	{13,23}	{24,22}	{8,19}	{8,10}	{14,6}	{14,23}	{13,6}	{5,22}	{3,28}	{6,12}	{17,10}	{19,13}	{16,2}	{24,7}	{17,19}	{0,7}	{3,1}	{10,25}	{19,16}	{4,10}	{1,5}
{3,1}	–	–	–	–	–	–	–	{24,7}	{0,0}	{16,27}	{27,2}	{1,5}	{8,19}	{27,27}	{13,23}	{5,7}	{24,22}	{15,27}	{10,4}	{6,12}	{19,16}	{17,19}	{16,2}	{10,25}	{2,6}	{4,19}	{14,6}	{14,23}	{0,7}	{13,6}	{20,3}	{2,23}	{19,13}	{8,10}	{3,28}	{6,17}	{4,10}
{3,28}	–	–	–	–	–	–	–	–	{24,22}	{27,27}	{16,2}	{8,10}	{1,24}	{13,6}	{27,2}	{24,7}	{5,22}	{10,25}	{15,2}	{19,13}	{6,17}	{16,27}	{17,10}	{2,23}	{10,4}	{14,23}	{4,10}	{0,22}	{14,6}	{20,26}	{13,23}	{19,16}	{2,6}	{3,1}	{8,19}	{4,19}	{6,12}
{4,10}	–	–	–	–	–	–	–	–	–	{15,2}	{0,0}	{0,7}	{19,13}	{20,3}	{24,7}	{17,19}	{13,6}	{16,2}	{14,23}	{19,16}	{8,10}	{10,4}	{24,22}	{17,10}	{4,19}	{3,28}	{10,25}	{8,19}	{15,27}	{13,23}	{5,7}	{1,5}	{6,17}	{14,6}	{6,12}	{3,1}	{2,23}
{4,19}	–	–	–	–	–	–	–	–	–	–	{15,27}	{19,16}	{0,22}	{24,22}	{20,26}	{13,23}	{17,10}	{14,6}	{16,27}	{8,19}	{19,13}	{24,7}	{10,25}	{4,10}	{17,19}	{10,4}	{3,1}	{15,2}	{8,10}	{5,22}	{13,6}	{6,12}	{1,24}	{6,17}	{14,23}	{2,6}	{3,28}
{5,7}	–	–	–	–	–	–	–	–	–	–	–	{14,23}	{0,0}	{14,6}	{2,23}	{17,10}	{3,1}	{19,13}	{20,26}	{16,27}	{15,2}	{5,22}	{6,17}	{2,6}	{13,6}	{13,23}	{1,24}	{27,2}	{8,19}	{4,10}	{10,25}	{10,4}	{27,27}	{0,22}	{24,7}	{20,3}	{17,19}
{5,22}	–	–	–	–	–	–	–	–	–	–	–	–	{14,6}	{2,6}	{14,23}	{3,28}	{17,19}	{20,3}	{19,16}	{15,27}	{16,2}	{6,12}	{5,7}	{13,23}	{2,23}	{1,5}	{13,6}	{8,10}	{27,27}	{10,4}	{4,19}	{27,2}	{10,25}	{24,22}	{0,7}	{17,10}	{20,26}
{6,12}	–	–	–	–	–	–	–	–	–	–	–	–	–	{13,23}	{0,0}	{16,27}	{20,26}	{17,10}	{0,22}	{6,17}	{3,1}	{15,2}	{5,22}	{1,5}	{14,23}	{8,19}	{2,23}	{1,24}	{10,25}	{27,2}	{24,7}	{8,10}	{4,19}	{4,10}	{19,13}	{3,28}	{19,16}
{6,17}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{13,6}	{20,3}	{16,2}	{0,7}	{17,19}	{3,28}	{6,12}	{5,7}	{15,27}	{14,6}	{1,24}	{2,6}	{8,10}	{10,4}	{1,5}	{24,22}	{27,27}	{4,10}	{8,19}	{19,16}	{4,19}	{19,13}	{3,1}
{8,10}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{0,22}	{0,0}	{20,26}	{2,6}	{4,10}	{2,23}	{1,24}	{27,2}	{15,27}	{19,13}	{6,17}	{0,7}	{4,19}	{5,22}	{27,27}	{15,2}	{10,25}	{6,12}	{1,5}	{3,1}	{19,16}	{14,6}
{8,19}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{0,7}	{2,23}	{20,3}	{2,6}	{4,19}	{27,27}	{1,5}	{19,16}	{15,2}	{0,22}	{6,12}	{5,7}	{4,10}	{15,27}	{27,2}	{6,17}	{10,4}	{3,28}	{1,24}	{14,23}	{19,13}
{10,4}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{3,1}	{0,0}	{0,22}	{1,24}	{27,2}	{4,10}	{3,28}	{24,7}	{16,27}	{4,19}	{27,27}	{6,17}	{1,5}	{5,22}	{8,19}	{5,7}	{2,6}	{15,2}	{17,19}	{14,23}
{10,25}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{3,28}	{1,5}	{0,7}	{4,19}	{27,27}	{24,22}	{3,1}	{4,10}	{16,2}	{6,12}	{27,2}	{5,7}	{1,24}	{5,22}	{8,10}	{15,27}	{2,23}	{14,6}	{17,10}
{13,6}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{27,2}	{0,0}	{2,23}	{1,24}	{5,7}	{17,10}	{5,22}	{20,3}	{0,7}	{15,2}	{4,19}	{3,1}	{24,7}	{16,2}	{27,27}	{20,26}	{24,22}	{13,23}
{13,23}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{27,27}	{1,5}	{2,6}	{17,19}	{5,22}	{20,26}	{5,7}	{15,27}	{0,22}	{3,28}	{4,10}	{16,27}	{14,23}	{20,3}	{27,2}	{13,6}	{24,7}
{14,6}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{2,6}	{0,0}	{16,2}	{6,17}	{3,1}	{15,27}	{3,28}	{20,26}	{20,3}	{0,22}	{17,10}	{19,16}	{0,7}	{4,10}	{8,10}	{10,25}
{14,23}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{2,23}	{6,12}	{16,27}	{15,2}	{3,28}	{20,3}	{3,1}	{0,7}	{20,26}	{19,13}	{17,19}	{4,19}	{0,22}	{10,4}	{8,19}
{15,2}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{8,19}	{0,0}	{27,27}	{14,23}	{13,6}	{4,19}	{8,10}	{0,7}	{1,24}	{24,7}	{10,4}	{20,3}	{16,27}	{0,22}
{15,27}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{8,10}	{14,6}	{27,2}	{4,10}	{13,23}	{0,22}	{8,19}	{24,22}	{1,5}	{20,26}	{10,25}	{0,7}	{16,2}
{16,2}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{10,25}	{0,0}	{2,23}	{24,7}	{1,24}	{19,13}	{13,6}	{0,7}	{27,2}	{17,10}	{15,27}	{24,22}
{16,27}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{10,4}	{24,22}	{2,6}	{19,16}	{1,5}	{0,22}	{13,23}	{17,19}	{27,27}	{24,7}	{15,2}
{17,10}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{19,16}	{0,0}	{17,19}	{2,6}	{20,26}	{14,6}	{16,2}	{1,5}	{10,25}	{5,22}
{17,19}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{19,13}	{2,23}	{17,10}	{14,23}	{20,3}	{1,24}	{16,27}	{5,7}	{10,4}
{19,13}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{16,2}	{0,0}	{3,1}	{14,23}	{6,12}	{2,6}	{8,19}	{6,17}
{19,16}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{16,27}	{14,6}	{3,28}	{2,23}	{6,17}	{6,12}	{8,10}
{20,3}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{17,19}	{0,0}	{15,2}	{13,23}	{27,27}	{5,7}
{20,26}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{17,10}	{13,6}	{15,27}	{5,22}	{27,2}
{24,7}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{5,7}	{0,0}	{13,23}	{16,27}
{24,22}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{5,22}	{16,2}	{13,6}
{27,2}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{20,26}	{0,0}
{27,27}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	{20,3}

Рис. 2: Табличное представление операции сложения точек в выбранной группе точек ЭК (таблица симметрична относительно главной диагонали, для наглядности нижняя часть пропущена).

По известным P и Q требуется найти такое k, при котором $Q = [k]P$.

В качестве генератора группы выберем точку $P = (2, 6)$, в качестве «неизвестного» параметра выберем $k = 29$ и вычислим $Q = (15, 2)$. Регистр-«аккумулятор» инициализируем точкой $(17, 10)$, чтобы избежать реализации удвоения точек в виде квантовой схемы [a].

[a] Надеемся, что достаточно реализовать $A + B$ для случая $A \neq B$ и $A \neq -B$, $A \neq O$, $B \neq O$ – большая часть таблицы Кэли

Разработаны программные реализации функций, необходимых для применения алгоритма Шора к ECDLP

1) myShorECDLP
2) myRegInit
3) myECadd2020forShor
4) my_qftTrue
5) fromBinary
6) toBinary
7) myConstAddModIntP
8) myConstAddMicrosoft
9) myCompareWithConst2024
10) myIncrementTakahashi
11) mySubtract
12) mySum
13) computeCarry
14) computeCarryCascade
15) myAdd
16) mySubstraction
17) myCompare
18) myAddModPInt
19) myIntMultXYModP
20) myDblModIntP
21) myIntSquareModP
22) myInverseModP2024
23) myMontBitGCDRound2024
24) mySpecFunctionForFig15
25) mySpecFunction
26) mySWAP
27) myRightShift
28) myIntMultConstXModP
29) myMinusXModPInt

Проверка, $|P(2,6)\rangle + Q(15,2) \mapsto |P(2,6) + Q(15,2)\rangle = |(3,1)\rangle$

```
module Main where  --компилируемый файл main.hs, в терминале: "quipper main.hs", затем запуск "./main > out.txt"
import System.Random
import Data.Time
import Quipper
import Quipper.Internal.Printing
import Quipper.Libraries.Simulation
import Quipper.Internal.QData
import Quipper.Libraries.QFT
import Quipper.Libraries.QuantumIf
import Quipper.Libraries.Arith -- we make use of the QDInt data type for quantum integers
import Quipper.Utils.Auxiliary

import MyArithmetic --все доп. функции в отдельном файле, MyArithmetic.hs

-- Run the program
main :: IO ()
main = do
  myTestECpointAdd
--  myShorECDLPTest
-------------------------------------------------------------------------------------------------------------------
myTestECpointAdd:: IO()
myTestECpointAdd = do
--p=29
--кривая: y^2= x^3 + 4x + 20 mod 29
--P=(2,6)  = [False, False, False, True, False], [False, False, True, True, False]
--Q=(15,2) = [False, True, True, True,  True], [False, False, False, True, False]
  let xP = [False, False, False, True, False]
  let yP = [False, False, True, True, False]
  let xQ = reverse (toBinary(15, 5 ) )
  let yQ = reverse (toBinary(2, 5 ) )
  --myECadd2020 -- это myECadd2020forShor, в которой regLambda, regU, regR, regS, regM инициализируются внутри функции
  print_generic Preview          myECadd2020 (replicate 5 qubit, replicate 5 qubit, xQ, yQ)      --покажет схему в PDF
  print $ sim_generic undefined  myECadd2020 (xP, yP, xQ, yQ)          --выдаст вероятности перед процедурой измерения
  print_generic GateCount        myECadd2020 (replicate 5 qubit, replicate 5 qubit, xQ, yQ)  --посчитает гейты в схеме
--Проверил:
--(2,6)+(15,2) = (3,1)+
--(2,6)+(13,23) = (8,19)+
--(15,27)+(13,23) = (5,22)+
--(15,27)+(27,27) = (16,2)+
-------------------------------------------------------------------------------------------------------------------
myShorECDLPTest:: IO()
myShorECDLPTest = do
--  print_generic Preview          myShorECDLP (replicate 5 qubit, replicate 5 qubit, replicate 5 qubit, replicate 5 qubit)
  print $ sim_generic undefined  myShorECDLP (replicate 6 False, replicate 6 False, replicate 5 False, replicate 5 False)
  print_generic GateCount        myShorECDLP (replicate 6 qubit, replicate 6 qubit, replicate 5 qubit, replicate 5 qubit)
```

Рис. 3: Компилируемый файл. Вычисление $|P(2,6)\rangle + Q(15,2) \mapsto |P(2,6) + Q(15,2)\rangle$.

Проверка, $|P(2,6)\rangle + Q(15,2) \mapsto |P(2,6) + Q(15,2)\rangle = |(3,1)\rangle$

```
[(([False,False,False,True,True],[False,False,False,False,True],[0,1,1,1,1],[0,0,0,1,0]),1.0)]
   27: "Init0"
    6: "Init1"
  443: "X, arity 1"
    1: "X, arity 1" controls 0+1
 1806: "X, arity 1", controls 1
    7: "X, arity 1" controls 1+1
 2257: "X, arity 1", controls 2
    6: "X, arity 1" controls 2+1
 1498: "X, arity 1", controls 3
  315: "X, arity 1", controls 4
  474: "not, arity 1"
  129: "not, arity 1" controls 0+1
    2: "not, arity 1" controls 0+5
 4135: "not, arity 1", controls 1
   48: "not, arity 1" controls 1+1
   40: "not, arity 1" controls 1+2
   40: "not, arity 1" controls 1+5
 5294: "not, arity 1", controls 2
 1604: "not, arity 1" controls 2+1
 2321: "not, arity 1", controls 3
  720: "not, arity 1" controls 3+1
  280: "not, arity 1", controls 4
  420: "swap, arity 2"
  960: "swap, arity 2", controls 1
Total gates: 22833
Inputs: 10
Outputs: 43
Qubits in circuit: 43
```

Рис. 4: Вычислили $|P(2,6)\rangle + Q(15,2) \mapsto |P(2,6) + Q(15,2)\rangle$, получили точку $(3,1)$. Квантовая схема построена на 43 кубитах и содержит 22 833 квантовых гейта[4].

[4] Ограничимся подсчётом общего количества гейтов. Отметим, что обобщенные CNOT могут быть декомпозированы в комбинацию гейтов CNOT и Toffoli с использованием единственного дополнительного кубита в произвольном неизвестном состоянии, см. *Craig Gidney*. StackExchange: Creating bigger controlled nots from single qubit, Toffoli, and CNOT gates, without workspae. 2015. https://cs.stackexchange.com/questions/40933.

Выводы

Вывод №1.

Для сложения точки $P(x_1, y_1)$ ЭК, координаты которой записаны в квантовый регистр (т.е. $|x_1\rangle\,|y_1\rangle$), с другой известной точкой $Q(x_2, y_2)$ ЭК ($Q \neq -P, Q \neq O, P \neq O$) достаточно $8n + 3$ кубит.

Вывод №2.

Для применения алгоритма Шора к ECDLP может потребоваться ещё $2 \times (n + 1)$ кубит для $QFT^\dagger$, т.е. при использовании канонического представления ЭК (в форме Вейерштрасса) для решения ECDLP требуется $10n + 5$ кубит. В случае применения полуклассического[a] $QFT^\dagger$ для применения алгоритма Шора к ECDLP потребуется $8n + 4$ кубита.

[a] Chiaverini J., Britton J., Leibfried D. et al. Implementation of the Semiclassical Quantum Fourier Transform in a Scalable System, Science 308(5724):997-1000, 2005.

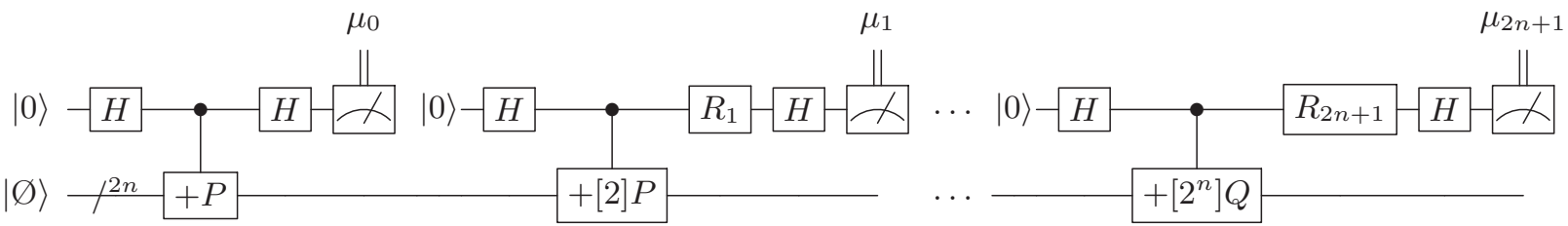

Рис. 5: Алгоритм Шора в задаче ECDLP с использованием полуклассического $QFT^\dagger$ из работы [RoeNSL2017]. Здесь $R_k = \mathrm{diag}(1, e^{i\theta_k})$, $\theta_k = -\pi \sum_{j=0}^{k-1} 2^{k-j} \mu_j$, т.е. в зависимости от результатов измерения верхнего кубита либо применяем гейты поворота из $QFT^\dagger$, либо нет – просто последовательное вычисление результатов измерений рис. 1 за $2n + 2$ запусков

Вернёмся к примеру

Выбрали $p = 29$, $n = \lceil \log_2 p \rceil = 5$, $y^2 = x^3 + 4x + 20 \mod 29$, в качестве генератора группы выберем точку $P = (2, 6)$, в качестве «неизвестного» параметра выбрали $k = 29$, вычислили $Q = (15, 2)$.
Регистр-«аккумулятор» инициализируем точкой $(17, 10)$, чтобы избежать реализации удвоен точек в виде квантовой схемы [5].

При $[x_1]P + [x_2]Q$	При $[x_1]P - [x_2]Q$
$[2^0]P = (2, 6)$	$[2^0]P = (2, 6)$
$[2^1]P = (1, 5)$	$[2^1]P = (1, 5)$
$[2^2]P = (4, 19)$	$[2^2]P = (4, 19)$
$[2^3]P = (15, 27)$	$[2^3]P = (15, 27)$
$[2^4]P = (8, 10)$	$[2^4]P = (8, 10)$
$[2^5]P = (0, 22)$	$[2^5]P = (0, 22)$
$[2^0]Q = (15, 2)$	$[2^0]Q = (15, 29 - 2)$
$[2^1]Q = (8, 19)$	$[2^1]Q = (8, 29 - 19)$
$[2^2]Q = (0, 7)$	$[2^2]Q = (0, 29 - 7)$
$[2^3]Q = (6, 12)$	$[2^3]Q = (6, 29 - 12)$
$[2^4]Q = (13, 23)$	$[2^4]Q = (13, 29 - 23)$
$[2^5]Q = (27, 27)$	$[2^5]Q = (27, 29 - 27)$

Таблица 1: Точки ЭК, которые добавляются в регистр-«аккумулятор» (2 варианта).

[5] Надеемся, что достаточно реализовать $A + B$ для случая $A \neq B$ и $A \neq -B$, $A \neq O$, $B \neq O$ – большая часть таблицы Кэли

Реализация алгоритма Шора (вариант $[x_1]P - [x_2]Q$)

24: "H, arity 1"
32: "Init0"
1: "Init1"
6: "Rot(R(2pi/%)*,16.0), arity 1 controls 1
4: "Rot(R(2pi/%)*,32.0), arity 1 controls 1
10: "Rot(R(2pi/%)*,4.0), arity 1 controls 1
2: "Rot(R(2pi/%)*,64.0), arity 1 controls 1
8: "Rot(R(2pi/%)*,8.0), arity 1 controls 1
9: "X, arity 1"
5292: "X, arity 1 controls 1
12: "X, arity 1"controls 1+1
21643: "X, arity 1 controls 2
84: "X, arity 1"controls 2+1
27078: "X, arity 1 controls 3
72: "X, arity 1"controls 3+1
17976: "X, arity 1 controls 4
3780: "X, arity 1 controls 5
5556: "not, arity 1 controls 1
1548: "not, arity 1"controls 1+1
24: "not, arity 1"controls 1+5
49452: "not, arity 1 controls 2
576: "not, arity 1"controls 2+1
480: "not, arity 1"controls 2+2
480: "not, arity 1"controls 2+5
63504: "not, arity 1 controls 3
19248: "not, arity 1"controls 3+1
27852: "not, arity 1 controls 4
8640: "not, arity 1"controls 4+1
3360: "not, arity 1 controls 5
6: "swap, arity 2"
5040: "swap, arity 2 controls 1
11520: "swap, arity 2 controls 2
Total gates: 273 319
Qubits in circuit: 55

Результаты измерения отсортированы по убыванию вероятности их измерения. В таблице представлены 450 из 4096 строк, в остальных случаях вероятность получить пару (x_1, x_2) меньше 0.000244141, т.е. меньше $1/4096$.

Номер	Измерение (x_1, x_2) при $[x_1]P + [x_2]Q$	Вероятность получить (x_1, x_2) при $[x_1]P + [x_2]Q$	Измерение (x_1, x_2) при $[x_1]P - [x_2]Q$	Вероятность получить (x_1, x_2) при $[x_1]P - [x_2]Q$
1	(0,0)	0.0167992	(0,0)	0.0157592
2	(12,31)	0.014953	(52,31)	0.0141224
3	(52,33)	0.014953	(12,33)	0.0141224
4	(31,7)	0.0144761	(33,7)	0.0138431
5	(33,57)	0.0144761	(31,57)	0.0138431
6	(43,38)	0.0133896	(45,40)	0.0126863
7	(21,26)	0.0133896	(19,24)	0.0126863
8	(19,40)	0.0131357	(21,38)	0.0126167
9	(45,24)	0.0131357	(43,26)	0.0126167
10	(14,17)	0.0112015	(14,47)	0.010645
11	(50,47)	0.0112015	(50,17)	0.010645
12	(62,14)	0.0110812	(62,50)	0.0106219
13	(2,50)	0.0110812	(2,14)	0.0106219
14	(24,62)	0.0107141	(40,62)	0.0102384
15	(40,2)	0.0107141	(24,2)	0.0102384
16	(57,55)	0.0102401	(7,55)	0.00986642
17	(7,9)	0.0102401	(57,9)	0.00986642
18	(55,5)	0.00994958	(55,59)	0.00927115
19	(9,59)	0.00994958	(9,5)	0.00927115
20	(10,45)	0.00920053	(10,19)	0.00882583
21	(54,19)	0.00920053	(54,45)	0.00882583
22	(38,16)	0.0091139	(26,16)	0.00861448
23	(26,48)	0.0091139	(38,48)	0.00861448
24	(29,21)	0.00795587	(47,54)	0.00744145
25	(35,43)	0.00795587	(17,10)	0.00744145
26	(17,54)	0.0079172	(29,43)	0.00739821

27	(47,10)	0.0079172	(35,21)	0.00739821
28	(5,22)	0.00667653	(59,22)	0.00637551
29	(59,42)	0.00667653	(5,42)	0.00637551
30	(42,52)	0.00647803	(22,52)	0.00612532
31	(22,12)	0.00647803	(42,12)	0.00612532
32	(36,29)	0.00632996	(36,35)	0.006087
33	(28,35)	0.00632996	(28,29)	0.006087
34	(5,23)	0.00608415	(59,23)	0.00581915
35	(59,41)	0.00608415	(5,41)	0.00581915
36	(41,52)	0.00607969	(23,52)	0.00563961
37	(23,12)	0.00607969	(41,12)	0.00563961
38	(26,49)	0.00572251	(26,15)	0.00546725
39	(38,15)	0.00572251	(38,49)	0.00546725
40	(3,36)	0.00571487	(61,36)	0.0053112
41	(61,28)	0.00571487	(3,28)	0.0053112
42	(48,61)	0.00405432	(48,3)	0.00387912
43	(16,3)	0.00405432	(16,61)	0.00387912
44	(4,36)	0.00398816	(60,36)	0.0037388
45	(60,28)	0.00398816	(4,28)	0.0037388
46	(7,8)	0.00373887	(57,8)	0.00362661
47	(57,56)	0.00373887	(7,56)	0.00362661
48	(30,21)	0.0037044	(30,43)	0.00340546
49	(34,43)	0.0037044	(34,21)	0.00340546
50	(11,45)	0.00352001	(47,53)	0.00327708
51	(53,19)	0.00352001	(17,11)	0.00327708
52	(17,53)	0.00343128	(11,19)	0.00325936
53	(47,11)	0.00343128	(53,45)	0.00325936
54	(36,30)	0.00335664	(28,30)	0.00322449
55	(28,34)	0.00335664	(36,34)	0.00322449
56	(16,4)	0.00309033	(48,4)	0.00295952
57	(48,60)	0.00309033	(16,60)	0.00295952
58	(56,5)	0.00304455	(56,59)	0.00275126
59	(8,59)	0.00304455	(8,5)	0.00275126
60	(50,46)	0.00277305	(14,46)	0.00272117

61	(14,18)	0.00277305	(50,18)	0.00272117
62	(49,61)	0.00246622	(49,3)	0.00230689
63	(15,3)	0.00246622	(15,61)	0.00230689
64	(24,63)	0.00226247	(40,63)	0.00217827
65	(40,1)	0.00226247	(24,1)	0.00217827
66	(19,39)	0.00193878	(45,39)	0.00189289
67	(45,25)	0.00193878	(19,25)	0.00189289
68	(15,4)	0.00188004	(49,4)	0.00175911
69	(49,60)	0.00188004	(15,60)	0.00175911
70	(3,37)	0.00171817	(3,27)	0.00163241
71	(61,27)	0.00171817	(61,37)	0.00163241
72	(44,38)	0.00165248	(38,47)	0.00158163
73	(20,26)	0.00165248	(26,17)	0.00158163
74	(18,54)	0.00157975	(26,14)	0.00153021
75	(46,10)	0.00157975	(38,50)	0.00153021
76	(38,17)	0.00151249	(5,40)	0.00149711
77	(26,47)	0.00151249	(59,24)	0.00149711
78	(63,14)	0.0015	(7,54)	0.00148836
79	(1,50)	0.0015	(57,10)	0.00148836
80	(38,14)	0.00148268	(57,7)	0.00146688
81	(26,50)	0.00148268	(7,57)	0.00146688
82	(37,29)	0.00147017	(20,38)	0.00140577
83	(27,35)	0.00147017	(44,26)	0.00140577
84	(57,54)	0.00145466	(46,54)	0.00139678
85	(7,10)	0.00145466	(18,10)	0.00139678
86	(59,40)	0.00144901	(63,50)	0.00138213
87	(5,24)	0.00144901	(1,14)	0.00138213
88	(7,7)	0.00141292	(37,35)	0.00136834
89	(57,57)	0.00141292	(27,29)	0.00136834
90	(29,20)	0.00134027	(5,43)	0.00135178
91	(35,44)	0.00134027	(59,21)	0.00135178
92	(5,21)	0.00131173	(50,16)	0.00133274
93	(59,43)	0.00131173	(14,48)	0.00133274
94	(52,32)	0.00128526	(35,20)	0.0013254

95	(12,32)	0.00128526	(29,44)	0.0013254
96	(45,23)	0.00128454	(19,23)	0.00130104
97	(19,41)	0.00128454	(45,41)	0.00130104
98	(14,16)	0.00127802	(52,32)	0.00128715
99	(50,48)	0.00127802	(12,32)	0.00128715
100	(24,61)	0.00124045	(24,3)	0.0012426
101	(40,3)	0.00124045	(40,61)	0.0012426
102	(50,45)	0.00122548	(50,19)	0.00122993
103	(14,19)	0.00122548	(14,45)	0.00122993
104	(4,37)	0.00120208	(47,55)	0.00121806
105	(60,27)	0.00120208	(17,9)	0.00121806
106	(55,6)	0.00116769	(62,51)	0.00115831
107	(9,58)	0.00116769	(2,13)	0.00115831
108	(17,55)	0.0011645	(9,6)	0.00115598
109	(47,9)	0.0011645	(55,58)	0.00115598
110	(62,13)	0.00115109	(45,38)	0.001155
111	(2,51)	0.00115109	(19,26)	0.001155
112	(28,36)	0.00113032	(4,27)	0.00114321
113	(36,28)	0.00113032	(60,37)	0.00114321
114	(19,38)	0.00106243	(28,31)	0.00112297
115	(45,26)	0.00106243	(36,33)	0.00112297
116	(12,30)	0.00104009	(36,36)	0.00110903
117	(52,34)	0.00104009	(28,28)	0.00110903
118	(36,31)	0.0010045	(52,30)	0.00109136
119	(28,33)	0.0010045	(12,34)	0.00109136
120	(31,6)	0.000996127	(40,0)	0.00107668
121	(33,58)	0.000996127	(24,0)	0.00107668
122	(17,52)	0.000971371	(47,52)	0.00100072
123	(47,12)	0.000971371	(17,12)	0.00100072
124	(31,8)	0.000936437	(33,6)	0.000991863
125	(33,56)	0.000936437	(31,58)	0.000991863
126	(40,0)	0.000923659	(33,8)	0.000959148
127	(24,0)	0.000923659	(31,56)	0.000959148
128	(2,49)	0.000894744	(0,63)	0.000955721

129	(62,15)	0.000894744	(0,1)	0.000955721
130	(0,63)	0.000892298	(16,62)	0.000916273
131	(0,1)	0.000892298	(48,2)	0.000916273
132	(48,62)	0.000863701	(2,15)	0.000913805
133	(16,2)	0.000863701	(62,49)	0.000913805
134	(2,52)	0.000846111	(12,31)	0.000897506
135	(62,12)	0.000846111	(52,33)	0.000897506
136	(43,52)	0.000806203	(21,39)	0.000839616
137	(21,12)	0.000806203	(43,25)	0.000839616
138	(43,39)	0.000803636	(62,52)	0.00082359
139	(21,25)	0.000803636	(2,12)	0.00082359
140	(9,45)	0.000801972	(9,4)	0.000812451
141	(55,19)	0.000801972	(55,60)	0.000812451
142	(25,62)	0.000801911	(9,19)	0.000807866
143	(39,2)	0.000801911	(55,45)	0.000807866
144	(55,4)	0.000782058	(35,22)	0.000788923
145	(9,60)	0.000782058	(29,42)	0.000788923
146	(37,30)	0.000777508	(21,52)	0.000786397
147	(27,34)	0.000777508	(43,12)	0.000786397
148	(16,5)	0.000759818	(31,55)	0.000782872
149	(48,59)	0.000759818	(33,9)	0.000782872
150	(61,29)	0.000750973	(31,59)	0.000780398
151	(3,35)	0.000750973	(33,5)	0.000780398
152	(29,22)	0.000744305	(0,62)	0.000773404
153	(35,42)	0.000744305	(0,2)	0.000773404
154	(52,31)	0.000743389	(43,27)	0.000772645
155	(12,33)	0.000743389	(21,37)	0.000772645
156	(43,37)	0.000739729	(21,40)	0.000769475
157	(21,27)	0.000739729	(43,24)	0.000769475
158	(33,55)	0.00073848	(16,59)	0.000748667
159	(31,9)	0.00073848	(48,5)	0.000748667
160	(45,22)	0.000708581	(61,35)	0.000743655
161	(19,42)	0.000708581	(3,29)	0.000743655
162	(31,5)	0.000693821	(27,30)	0.000736358

163	(33,59)	0.000693821	(37,34)	0.000736358
164	(12,29)	0.000688229	(19,22)	0.000734532
165	(52,35)	0.000688229	(45,42)	0.000734532
166	(18,53)	0.000685355	(39,62)	0.000734361
167	(46,11)	0.000685355	(25,2)	0.000734361
168	(0,62)	0.00067897	(9,7)	0.000726221
169	(0,2)	0.00067897	(55,57)	0.000726221
170	(43,40)	0.000678623	(12,35)	0.000709761
171	(21,24)	0.000678623	(52,29)	0.000709761
172	(26,46)	0.000657588	(38,46)	0.0006651
173	(38,18)	0.000657588	(26,18)	0.0006651
174	(35,45)	0.00065155	(61,38)	0.000661231
175	(29,19)	0.00065155	(3,26)	0.000661231
176	(57,53)	0.000643766	(50,15)	0.000651937
177	(7,11)	0.000643766	(14,49)	0.000651937
178	(30,20)	0.000629518	(57,11)	0.000647307
179	(34,44)	0.000629518	(7,53)	0.000647307
180	(40,4)	0.000617937	(35,19)	0.000636823
181	(24,60)	0.000617937	(29,45)	0.000636823
182	(38,13)	0.000611368	(18,11)	0.000623985
183	(26,51)	0.000611368	(46,53)	0.000623985
184	(55,7)	0.000605582	(2,16)	0.000611391
185	(9,57)	0.000605582	(62,48)	0.000611391
186	(50,49)	0.000596986	(34,20)	0.000604373
187	(14,15)	0.000596986	(30,44)	0.000604373
188	(10,46)	0.000585499	(24,4)	0.000602196
189	(54,18)	0.000585499	(40,60)	0.000602196
190	(59,39)	0.000579601	(54,59)	0.000589777
191	(5,25)	0.000579601	(10,5)	0.000589777
192	(54,20)	0.00056047	(38,51)	0.000580798
193	(10,44)	0.00056047	(26,13)	0.000580798
194	(26,52)	0.000560255	(24,52)	0.000580126
195	(38,12)	0.000560255	(40,12)	0.000580126
196	(5,20)	0.000558242	(54,47)	0.000579468

197	(59,44)	0.000558242	(10,17)	0.000579468
198	(5,36)	0.000556632	(54,46)	0.000578403
199	(59,28)	0.000556632	(10,18)	0.000578403
200	(49,62)	0.000550899	(10,20)	0.000568471
201	(15,2)	0.000550899	(54,44)	0.000568471
202	(26,45)	0.000550434	(60,35)	0.000566249
203	(38,19)	0.000550434	(4,29)	0.000566249
204	(60,29)	0.000547426	(5,39)	0.000562927
205	(4,35)	0.000547426	(59,25)	0.000562927
206	(54,5)	0.000538336	(3,14)	0.000555153
207	(10,59)	0.000538336	(61,50)	0.000555153
208	(3,38)	0.00053832	(28,43)	0.00055443
209	(61,26)	0.00053832	(36,21)	0.00055443
210	(32,7)	0.000537241	(59,36)	0.000550543
211	(32,57)	0.000537241	(5,28)	0.000550543
212	(7,6)	0.0005341	(21,36)	0.000545812
213	(57,58)	0.0005341	(43,28)	0.000545812
214	(59,38)	0.000531837	(17,8)	0.000543103
215	(5,26)	0.000531837	(47,56)	0.000543103
216	(62,16)	0.000523761	(22,38)	0.000538471
217	(2,48)	0.000523761	(42,26)	0.000538471
218	(47,8)	0.000522121	(59,20)	0.000536272
219	(17,56)	0.000522121	(5,44)	0.000536272
220	(42,38)	0.000521356	(15,59)	0.000518407
221	(22,26)	0.000521356	(49,5)	0.000518407
222	(40,52)	0.000519825	(31,43)	0.000517372
223	(24,12)	0.000519825	(33,21)	0.000517372
224	(61,14)	0.000512585	(42,14)	0.000507809
225	(3,50)	0.000512585	(22,50)	0.000507809
226	(22,13)	0.000511842	(15,62)	0.000502764
227	(42,51)	0.000511842	(49,2)	0.000502764
228	(31,21)	0.00050611	(12,19)	0.000501959
229	(33,43)	0.00050611	(52,45)	0.000501959
230	(28,21)	0.000502514	(22,51)	0.000499457

231	(36,43)	0.000502514	(42,13)	0.000499457
232	(43,36)	0.000497407	(57,6)	0.000498121
233	(21,28)	0.000497407	(7,58)	0.000498121
234	(52,36)	0.000495215	(26,19)	0.000496262
235	(12,28)	0.000495215	(38,45)	0.000496262
236	(54,17)	0.000486163	(23,51)	0.000490353
237	(10,47)	0.000486163	(41,13)	0.000490353
238	(6,22)	0.00048528	(5,38)	0.000479726
239	(58,42)	0.00048528	(59,26)	0.000479726
240	(47,7)	0.000476554	(62,36)	0.000477273
241	(17,57)	0.000476554	(2,28)	0.000477273
242	(54,21)	0.000476152	(47,3)	0.000471107
243	(10,43)	0.000476152	(17,61)	0.000471107
244	(12,45)	0.000473787	(54,43)	0.000468388
245	(52,19)	0.000473787	(10,21)	0.000468388
246	(45,21)	0.000470511	(38,52)	0.000463544
247	(19,43)	0.000470511	(26,12)	0.000463544
248	(47,61)	0.000470305	(35,35)	0.000459463
249	(17,3)	0.000470305	(29,29)	0.000459463
250	(14,20)	0.000468551	(17,7)	0.000446507
251	(50,44)	0.000468551	(47,57)	0.000446507
252	(28,37)	0.000461126	(35,23)	0.000440277
253	(36,27)	0.000461126	(29,41)	0.000440277
254	(57,52)	0.000456939	(36,37)	0.000439312
255	(7,12)	0.000456939	(28,27)	0.000439312
256	(7,5)	0.000454159	(14,50)	0.000436246
257	(57,59)	0.000454159	(50,14)	0.000436246
258	(40,5)	0.000453574	(9,3)	0.000435785
259	(24,59)	0.000453574	(55,61)	0.000435785
260	(14,14)	0.000451979	(50,20)	0.000426217
261	(50,50)	0.000451979	(14,44)	0.000426217
262	(35,29)	0.000451565	(41,11)	0.000423839
263	(29,35)	0.000451565	(23,53)	0.000423839
264	(23,13)	0.000445945	(57,59)	0.000423696

265	(41,51)	0.000445945	(7,5)	0.000423696
266	(6,23)	0.000445368	(45,43)	0.000421441
267	(58,41)	0.000445368	(19,21)	0.000421441
268	(0,61)	0.000445269	(42,11)	0.000419228
269	(0,3)	0.000445269	(22,53)	0.000419228
270	(33,54)	0.000444791	(24,63)	0.000417279
271	(31,10)	0.000444791	(40,1)	0.000417279
272	(19,37)	0.000439741	(7,52)	0.000414183
273	(45,27)	0.000439741	(57,12)	0.000414183
274	(13,17)	0.000438187	(32,7)	0.000414179
275	(51,47)	0.000438187	(32,57)	0.000414179
276	(22,14)	0.000435045	(48,54)	0.000413696
277	(42,50)	0.000435045	(16,10)	0.000413696
278	(2,36)	0.000434658	(36,32)	0.000412748
279	(62,28)	0.000434658	(28,32)	0.000412748
280	(15,5)	0.000432988	(7,59)	0.000408528
281	(49,59)	0.000432988	(57,5)	0.000408528
282	(9,61)	0.000425498	(58,22)	0.000406666
283	(55,3)	0.000425498	(6,42)	0.000406666
284	(40,63)	0.000422271	(19,27)	0.000401735
285	(24,1)	0.000422271	(45,37)	0.000401735
286	(47,13)	0.000419443	(12,36)	0.000396844
287	(17,51)	0.000419443	(52,28)	0.000396844
288	(59,45)	0.000417651	(31,54)	0.000395051
289	(5,19)	0.000417651	(33,10)	0.000395051
290	(14,21)	0.000414555	(47,51)	0.00039318
291	(50,43)	0.000414555	(17,13)	0.00039318
292	(42,53)	0.000414448	(12,30)	0.000392059
293	(22,11)	0.000414448	(52,34)	0.000392059
294	(52,30)	0.000413755	(60,38)	0.000389796
295	(12,34)	0.000413755	(4,26)	0.000389796
296	(36,32)	0.000410935	(13,47)	0.000387005
297	(28,32)	0.000410935	(51,17)	0.000387005
298	(23,14)	0.00040969	(0,3)	0.00038534

299	(41,50)	0.00040969	(0,61)	0.00038534
300	(41,53)	0.000407037	(34,19)	0.000378131
301	(23,11)	0.000407037	(30,45)	0.000378131
302	(4,38)	0.000403081	(58,23)	0.000375287
303	(60,26)	0.000403081	(6,41)	0.000375287
304	(57,5)	0.000393025	(47,4)	0.000374621
305	(7,59)	0.000393025	(17,60)	0.000374621
306	(16,54)	0.000392143	(40,59)	0.000372368
307	(48,10)	0.000392143	(24,5)	0.000372368
308	(17,4)	0.000382404	(59,19)	0.000370657
309	(47,60)	0.000382404	(5,45)	0.000370657
310	(21,23)	0.000378138	(41,62)	0.00037022
311	(43,41)	0.000378138	(23,2)	0.00037022
312	(29,23)	0.000370463	(16,63)	0.000363373
313	(35,41)	0.000370463	(48,1)	0.000363373
314	(31,4)	0.000364345	(41,14)	0.000360974
315	(33,60)	0.000364345	(23,50)	0.000360974
316	(39,52)	0.000356348	(8,6)	0.000357285
317	(25,12)	0.000356348	(56,58)	0.000357285
318	(48,63)	0.000356181	(25,52)	0.000355822
319	(16,1)	0.000356181	(39,12)	0.000355822
320	(56,6)	0.000355019	(43,23)	0.000351412
321	(8,58)	0.000355019	(21,41)	0.000351412
322	(0,14)	0.000344266	(62,47)	0.000350266
323	(0,50)	0.000344266	(2,17)	0.000350266
324	(30,22)	0.000343736	(14,43)	0.000345136
325	(34,42)	0.000343736	(50,21)	0.000345136
326	(61,30)	0.000342399	(34,22)	0.000343331
327	(3,34)	0.000342399	(30,42)	0.000343331
328	(2,47)	0.000340041	(0,14)	0.000341807
329	(62,17)	0.000340041	(0,50)	0.000341807
330	(28,38)	0.000334903	(36,31)	0.000337888
331	(36,26)	0.000334903	(28,33)	0.000337888
332	(19,36)	0.000334697	(23,54)	0.000331784

333	(45,28)	0.000334697	(41,10)	0.000331784
334	(23,62)	0.000334136	(29,40)	0.000328228
335	(41,2)	0.000334136	(35,24)	0.000328228
336	(47,14)	0.000332333	(3,30)	0.000328052
337	(17,50)	0.000332333	(61,34)	0.000328052
338	(21,29)	0.000331955	(24,62)	0.000326362
339	(43,35)	0.000331955	(40,2)	0.000326362
340	(9,62)	0.000329425	(16,0)	0.00032568
341	(55,2)	0.000329425	(48,0)	0.00032568
342	(2,53)	0.000324284	(9,8)	0.000321712
343	(62,11)	0.000324284	(55,56)	0.000321712
344	(40,62)	0.000324185	(33,4)	0.000321504
345	(24,2)	0.000324185	(31,60)	0.000321504
346	(55,8)	0.000320599	(50,3)	0.000321125
347	(9,56)	0.000320599	(14,61)	0.000321125
348	(34,45)	0.000317601	(27,43)	0.000315901
349	(30,19)	0.000317601	(37,21)	0.000315901
350	(28,31)	0.000314185	(37,36)	0.000305679
351	(36,33)	0.000314185	(27,28)	0.000305679
352	(50,61)	0.000311132	(62,19)	0.000304385
353	(14,3)	0.000311132	(2,45)	0.000304385
354	(35,40)	0.00030987	(34,7)	0.000303667
355	(29,24)	0.00030987	(30,57)	0.000303667
356	(52,29)	0.000308775	(52,35)	0.000303637
357	(12,35)	0.000308775	(12,29)	0.000303637
358	(38,20)	0.000304473	(45,36)	0.000303084
359	(26,44)	0.000304473	(19,28)	0.000303084
360	(16,0)	0.000304222	(38,35)	0.000301324
361	(48,0)	0.000304222	(26,29)	0.000301324
362	(16,6)	0.000299713	(53,59)	0.000300554
363	(48,58)	0.000299713	(11,5)	0.000300554
364	(27,21)	0.000299154	(8,19)	0.00030044
365	(37,43)	0.000299154	(56,45)	0.00030044
366	(30,7)	0.000299128	(36,38)	0.000295405

367	(34,57)	0.000299128	(28,26)	0.000295405
368	(38,29)	0.00029576	(26,20)	0.000293829
369	(26,35)	0.00029576	(38,44)	0.000293829
370	(38,21)	0.00029095	(61,39)	0.000291109
371	(26,43)	0.00029095	(3,25)	0.000291109
372	(37,31)	0.000290075	(55,55)	0.000290782
373	(27,33)	0.000290075	(9,9)	0.000290782
374	(8,45)	0.000287337	(47,50)	0.000288659
375	(56,19)	0.000287337	(17,14)	0.000288659
376	(13,45)	0.000285207	(2,11)	0.000283904
377	(51,19)	0.000285207	(62,53)	0.000283904
378	(61,31)	0.000280616	(63,36)	0.000282819
379	(3,33)	0.000280616	(1,28)	0.000282819
380	(14,13)	0.00028056	(21,35)	0.000282389
381	(50,51)	0.00028056	(43,29)	0.000282389
382	(0,4)	0.000280073	(48,6)	0.000281554
383	(0,60)	0.000280073	(16,58)	0.000281554
384	(35,46)	0.000279755	(4,14)	0.000281057
385	(29,18)	0.000279755	(60,50)	0.000281057
386	(9,55)	0.000277151	(4,30)	0.00028105
387	(55,9)	0.000277151	(60,34)	0.00028105
388	(1,36)	0.000277027	(29,30)	0.000276798
389	(63,28)	0.000277027	(35,34)	0.000276798
390	(27,36)	0.000276475	(10,16)	0.000275834
391	(37,28)	0.000276475	(54,48)	0.000275834
392	(26,53)	0.000276444	(43,22)	0.000274125
393	(38,11)	0.000276444	(21,42)	0.000274125
394	(50,52)	0.000276255	(26,11)	0.000272812
395	(14,12)	0.000276255	(38,53)	0.000272812
396	(21,22)	0.000275873	(14,14)	0.000272223
397	(43,42)	0.000275873	(50,50)	0.000272223
398	(53,5)	0.000275381	(0,4)	0.000271684
399	(11,59)	0.000275381	(0,60)	0.000271684
400	(13,31)	0.000275294	(13,19)	0.000268992

401	(51,33)	0.000275294	(51,45)	0.000268992
402	(60,14)	0.000274438	(38,43)	0.000268811
403	(4,50)	0.000274438	(26,21)	0.000268811
404	(47,5)	0.000273942	(8,4)	0.000268255
405	(17,59)	0.000273942	(56,60)	0.000268255
406	(7,13)	0.000271586	(50,4)	0.000267939
407	(57,51)	0.000271586	(14,60)	0.000267939
408	(35,30)	0.000271264	(14,51)	0.000264879
409	(29,34)	0.000271264	(50,13)	0.000264879
410	(3,39)	0.000267547	(14,52)	0.000263211
411	(61,25)	0.000267547	(50,12)	0.000263211
412	(12,36)	0.000263166	(47,59)	0.000262813
413	(52,28)	0.000263166	(17,5)	0.000262813
414	(42,54)	0.000263046	(55,62)	0.000262607
415	(22,10)	0.000263046	(9,2)	0.000262607
416	(45,20)	0.000261261	(4,31)	0.000261131
417	(19,44)	0.000261261	(60,33)	0.000261131
418	(60,30)	0.000260226	(59,27)	0.000259435
419	(4,34)	0.000260226	(5,37)	0.000259435
420	(59,37)	0.000260098	(22,54)	0.000258935
421	(5,27)	0.000260098	(42,10)	0.000258935
422	(14,4)	0.00026005	(53,43)	0.000258856
423	(50,60)	0.00026005	(11,21)	0.000258856
424	(54,16)	0.000259802	(20,52)	0.000257032
425	(10,48)	0.000259802	(44,12)	0.000257032
426	(59,46)	0.000255995	(61,40)	0.000256674
427	(5,18)	0.000255995	(3,24)	0.000256674
428	(7,4)	0.000255635	(10,52)	0.000254601
429	(57,60)	0.000255635	(54,12)	0.000254601
430	(33,53)	0.00025535	(45,7)	0.000251679
431	(31,11)	0.00025535	(19,57)	0.000251679
432	(56,4)	0.000254804	(23,19)	0.000250705
433	(8,60)	0.000254804	(41,45)	0.000250705
434	(40,61)	0.000250403	(29,46)	0.000249545

435	(24,3)	0.000250403	(35,18)	0.000249545
436	(18,55)	0.000249371	(38,62)	0.000247918
437	(46,9)	0.000249371	(26,2)	0.000247918
438	(62,45)	0.000249222	(52,36)	0.000247148
439	(2,19)	0.000249222	(12,28)	0.000247148
440	(53,20)	0.000246151	(35,52)	0.000247129
441	(11,44)	0.000246151	(29,12)	0.000247129
442	(0,5)	0.000245632	(7,51)	0.000245576
443	(0,59)	0.000245632	(57,13)	0.000245576
444	(33,61)	0.000244776	(17,6)	0.000245455
445	(31,3)	0.000244776	(47,58)	0.000245455
446	(2,54)	0.000243757	(33,11)	0.000244333
447	(62,10)	0.000243757	(31,53)	0.000244333
448	(52,37)	0.000242314	(57,4)	0.000242494
449	(12,27)	0.000242314	(7,60)	0.000242494
450	(47,6)	0.000241207	(29,38)	0.000242207
⋮	⋮	⋮	⋮	⋮
4092	(13,35)	0.0000319147	(1,2)	0.0000328012
4093	(13,13)	0.0000318704	(39,46)	0.0000325831
4094	(51,51)	0.0000318704	(25,18)	0.0000325831
4095	(39,20)	0.0000318562	(63,63)	0.0000306627
4096	(25,44)	0.0000318562	(1,1)	0.0000306627

Смоделируем запуски квантовой схемы и вычислим логарифм

в Wolftam:

1) myDistr = EmpiricalDistribution[probsArr -> valueArr];
2) RandomVariate[myDistr] – реализация сл. в., имеющей заданное распределение.

DLP в $\mathbb{Z}_p$: известны a и b, хотим найти такое k, при котором $b = a^k \mod p$ (положим ord a $= p-1$, a - генератор мультипликативной группы в $\mathbb{Z}_p$).

Рассматривается периодическая функция $f(x_1, x_2) = a^{x_1} \cdot b^{x_2} = a^{x_1} \cdot a^{k \cdot x_2} = a^{x_1 + k \cdot x_2}$

Выбираем, на какой период «смотреть»:
1) при $x_1 + k \cdot x_2 \equiv 0$ (попадём в нейтральный элемент, $f(x_1, x_2) = 1$) найдём $k = (-x_1)/x_2$.
2) при $x_1 - k \cdot x_2 \equiv 0$ (попадём в нейтральный элемент, $f(x_1, x_2) = 1$) найдём $k = (x_1)/x_2$.

сравнение – по модулю, равному порядку рассматриваемой группы?

и т.д. и т.п.

Для ECDLP рассуждаем по аналогии, просто группа $(E, +)$.

Что делать после измерения регистров $|x_1\rangle$ и $|x_2\rangle$?

Ожидаем получить в результатах измерения $x_1 - x_2 k \equiv 0 \mod q$ (k – искомый период). Проверяем, выполнено ли $Q = [k]P$ для $k = x_1 \cdot x_2^{-1} \mod q$ [a] ($x_2^{-1} \mod q$ вычисляем с помощью расширенного алгоритма Евклида на классическом ЭВМ с полиномиальной трудоемкостью).

---

[a] другие варианты постобработки см. в Ekera M. On the Success Probability of Quantum Order Finding, ACM Transactions on Quantum Computing 5 (130), 2024, doi:10.1145/3655026

/*
P.S. Реализован пример дискретного логарифмирования в $\mathbb{Z}_{29}$: $2^d = 5 \mod 29$.
Вероятность успеха при решении $2^d = 5 \mod 29$, $|x_1\rangle$ и $|x_2\rangle$ в 5-кубитовых регистрах, составляет 0.284137 (сумма вероятностей подходящих исходов:
$k = (x_1) \cdot (x_2)^{-1} - 0 \mod q$, либо $k = (x_1) \cdot (x_2)^{-1} - 1 \mod q$, либо
$k = (x_2) \cdot (x_1)^{-1} - 0 \mod q$, либо $k = (x_2) \cdot (x_1)^{-1} - 1 \mod q$, либо
$k = (-x_1) \cdot (x_2)^{-1} - 0 \mod q$, либо $k = (-x_1) \cdot (x_2)^{-1} - 1 \mod q$, либо
$k = (-x_2) \cdot (x_1)^{-1} - 0 \mod q$, либо $k = (-x_2) \cdot (x_1)^{-1} - 1 \mod q$
перед процедурой измерения кубит, получено экспериментально с помощью Quipper), т.е. при таком подходе до получения искомого ответа $d = 22$ в среднем потребуется 3 запуска квантовой схемы.
*/

В примере $x = x_1$, $y = x_2$, myN $= 37$

Вычислял «кандидатов» на значение логарифма (у нас $Q = [29]P$)

```
maybeD1 = Mod[x*ModularInverse[ y, myN] - 0, myN];
maybeD2 = Mod[x*ModularInverse[-y, myN] - 0, myN];
maybeD3 = Mod[y*ModularInverse[ x, myN] - 0, myN];
maybeD4 = Mod[y*ModularInverse[-x, myN] - 0, myN];
maybeD5 = Mod[x*ModularInverse[ y, myN] - 1, myN];
maybeD6 = Mod[x*ModularInverse[-y, myN] - 1, myN];
maybeD7 = Mod[y*ModularInverse[ x, myN] - 1, myN];
maybeD8 = Mod[y*ModularInverse[-x, myN] - 1, myN];
```

Просуммируем вероятности результатов измерений в тех случаях, когда удается вычислить дискретный логарифм maybeDn $= 29$, при котором $Q = [29]P$.

При $[x_1]P + [x_2]Q$:

{0.0318972,0.0241742,0.022834,0.0201105,0.0181438,0.0243215,0.0115765,0.0171809}
Суммарная вероятность успеха $= 0.170238$

При $[x_1]P - [x_2]Q$::

{0.0191498,0.0165527,0.0355646,0.0298046,0.0166805,0.015273,0.0399978,0.0668492}
Суммарная вероятность успеха $= 0.239872$

Интересные вопросы и задачи:

При увеличении количества кубитов в регистрах для $QFT^\dagger$ возрастёт точность алгоритма QPE (Quantum Phase Estimation algorithm). Количество «периодов» при вычислении $[x_1]P + [x_2]Q$ увеличится, начнёт ли доминировать период $|(E, +)|$?

Вместо применения двух $QFT^\dagger$ к регистрам $|x_1\rangle$ и $|x_2\rangle$ (каждый по 6 кубит) можно применять одно преобразование $QFT^\dagger$ к регистру из 12 кубит, далее для поиска периода использовать приближения цепными дробями как в задаче факторизации?

Проверить Ekera M. On the Success Probability of Quantum Order Finding, ACM Transactions on Quantum Computing 5 (130), 2024, doi:10.1145/3655026.

Добавление точки $|A\rangle + B$ реализовано не полностью, а только для случая $A \neq B$ и $A \neq -B$, $A \neq O$, $B \neq O$. Повторить всё с точной реализацией сложения?

Ложка дёгтя

Рассмотренный пример не сильно информативен

При использовании равномерного распределения (1/4096) результатов измерения на 12 кубитах вместо того, что было получено с помощью Quipper:

При myN = 37:
{0.026123,0.026123,0.026123,0.026123,0.026123,0.0258789,0.026123,0.0258789}
Суммарная вероятность успеха = 0.208496

При myN = 30:
{0.0249023,0.0256348,0.0249023,0.0256348,0.101318,0.101318,0.101318,0.101318}
Суммарная вероятность успеха = 0.506348

Спасибо за внимание.