УДК 638.235.231

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ. АЛГОРИТМЫ ЭФФЕКТИВНОГО РЕШЕНИЯ NP-ПОЛНЫХ ЗАДАЧ

Сергей Манойло, Руслан Оскома
Харьковский национальный университет радиоэлектроники

Аннотация: **Проведен анализ одного из наиболее известных алгоритмов квантовых вычислений – алгоритм факторизации Шора. Приведены результаты моделирования алгоритма а также оценки количества ресурсов, необходимых для проведения вычислений.**
Summary: **There was provided of the most popular quantum calculations algorithm (Shor factorization algorithm) analysis in that paper. There were presented of computer simulations results. Resources quality, which is necessary for calculations, was presented too.**
Ключевые слова: **Информация, теория алгоритмов, квантовые вычисления.**

Последние десятилетия современная микропроцессорная техника развивалось по пути повышения рабочих тактовых частот, что требовало уменьшения размеров pn-переходов базовых элементов полупроводников. Это в свою очередь приводит к уменьшению количества электронов, необходимых для хранения одного бита информации. Согласно прогнозам специалистов уже в ближайшее время будут достигнуты критические точки размеров pn-переходов, в которых начнут проявляться квантово-механические свойства элементарных частиц. Это в свою очередь потребует разработки как новых технологических решений, позволяющих реализовывать устойчивые к внешним воздействиям аппаратные решения, так и новой теоретико-алгоритмической базы, позволяющей решать как стандартные задачи, так и задачи, эффективного решения которых на данном этапе не существует. Квантово-механические свойства поведения элементарных частиц позволяют заложить в алгоритмическую теорию новую базу, которая отличается от традиционной теории машины Тьюринга. Впервые об этом написали Ю. И. Манин в 1980 [1] и Ричард Фейнман в 1982 году [2]. Затем в 1994 году был предложен полиномиальный алгоритм факторизации П. Шора [3 – 5], практическая реализация которого делает использование базовых алгоритмов несимметричной криптографии неэффективным. Алгоритм основан на эффективном использовании квантового параллелизма, который позволяет, переведя квантовые регистры аргументов в суперпозицию аргументов, получить за одну алгоритмическую итерацию суперпозицию результатов вычислений реализованной схемы вычислений. Также существует возможность экспоненциального увеличения объемов хранимой информации в регистрах квантовых вычислительных систем. Данные свойства позволяют эффективно решать некоторые NP-полные задачи, которые лежат в основе несимметричной криптографии.

Данная работа посвящена исследованию алгоритма факторизации Шора [5, 6]. Приведены результаты моделирования с использованием традиционных вычислительных средств.

II Алгоритм факторизации целых чисел

Для решения задачи факторизации используется алгоритм нахождения на квантовой вычислительной системе периода (порядка) r числа x в мультипликативной группе вычетов по модулю факторизуемого числа N [3, 5]. Такая группа является циклической.

Т. е., пусть необходимо факторизовать число *N*. При этом достаточно найти хотя бы один множитель факторизации. На первом этапе выбирается произвольное число x, которое является взаимно простым с числом *N*. Затем рассмотрим последовательность, образованную функцией:

$$f(a) = x^a \bmod N . \tag{1}$$

Последовательности $\{x^a\}$ и $\{x^a \bmod N\}$ выглядят следующим образом:

$$\{x^a\} = 1,\ x,\ \ldots,\ x^{r-1},\ x^r,\ x^{r+1},\ \ldots, \tag{2}$$

$$\{x^a \bmod N\} = 1,\ x,\ \ldots,\ x^r\ 1,\ x,\ \ldots,\ x^r,\ 1,\ x,\ \ldots,\ x^r . \tag{3}$$

Число r – минимальная степень, для которой

$$x^r = 1(\mathrm{mod}\, N). \tag{4}$$

Выражение следует из обобщения теоремы Эйлера, согласно которой для любых взаимно простых чисел a и n

$$a^{L(n)} = 1 \bmod n, \tag{5}$$

где $L(n)$ – обобщенная функция Эйлера.

В конечном итоге задача факторизации числа N заключается в сложности поиска периода r числа x (4). При больших N требуется перебор достаточно большого числа вариантов a. Эффективный алгоритм поиска периода r, в основе которого лежит модель квантового параллелизма, приведен ниже.

Пусть период r найден. Если период нечетный, выбирается новое число x и алгоритм поиска r повторяется. Если алгоритм четный, приступаем к выполнению факторизации. Выражение (4) может быть записано в следующем виде:

$$x^r - 1 = 0(\mathrm{mod}\, N). \tag{6}$$

Отсюда следует:

$$(x^{r/2})^2 - 1 = 0(\mathrm{mod}\, N). \tag{7}$$

Далее:

$$((x^{r/2}) - 1)((x^{r/2}) + 1) = 0(\mathrm{mod}\, N). \tag{8}$$

Из выражения (8) следует, что произведение двух сомножителей кратно числу *N*. Таким образом, один из сомножителей должен иметь с N общий множитель. Окончательный этап факторизации заключается в поиске наибольшего общего делителя сомножителей:

$$\gcd(((x^{r/2}) - 1), N), \tag{9}$$

$$\gcd(((x^{r/2}) + 1), N). \tag{10}$$

Найденное значение $\gcd$ является искомым числом.

Ниже представлен пример факторизации. Пусть необходимо факторизовать число *N* = 91. Выберем *x* = 3. Вычислим последовательности

a: 0, 1, 2, 3, 4, 5, 6, 7, …

3^a: 1, 3, 9, 27, 81, 243, 729, 2187, …

$3^a \bmod 91$: 1, 3, 9, 27, 81, 61, 1, 3, …

Таким образом, искомое значение *r* = 6.

Далее получаем:

$$((x^{r/2}) - 1) = 3^3 - 1 = 26, \tag{11}$$

$$((x^{r/2}) + 1) = 3^3 + 1 = 28. \tag{12}$$

Находим с помощью алгоритма Евклида (алгоритм Евклида имеет полиномиальную сложность):

$$\gcd(((x^{r/2}) - 1), N) = \gcd(26,91) = 13, \tag{13}$$

$$\gcd(((x^{r/2}) + 1), N) = \gcd(28,91) = 7. \tag{14}$$

Полученные значения 7 и 13 являются результатом факторизации числа *N* = 91.

III Алгоритм поиска периода *r* Шора

Для поиска периода r реализуется квантовая система, состоящая из двух регистров [3 – 7]:

$$\varphi(a, f(a)) = | 0, 0, 0...; 0, 0, 0, \ ... > . \tag{15}$$

Длина регистров выбирается таким образом, чтобы первый регистр мог вместить максимально-допустимое значение a (длины m) выражения (1), а второй регистр мог вместить число N (длины *l*).

1. Для каждого кубита регистра 1 выполняется преобразование Адамара-Уолша, которое может быть представлено следующей матрицей:

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{16}$$

т. е. квантовые состояние преобразуются следующим образом: $|0> \rightarrow |0> + |1>$, $|1> \rightarrow |0> - |1>$.

При этом первый регистр переводится в суперпозицию состояний всех допустимых аргументов:

$$\varphi(a, f(a)) = \frac{1}{2^m} \sum_{a=0}^{2^m-1} |a, 0>. \tag{17}$$

2. Используя квантовый параллелизм вычисляется значение функции (1) для каждого возможного a. Результат (суперпозиция результатов) помещается во второй регистр. При этом квантовая система переводится в состояние:

$$\varphi(a, f(a)) = \frac{1}{2^m} \sum_{a=0}^{2^m-1} |a, f(a)>. \tag{18}$$

При этом функция $f(a)$ имеет вид, представленный на рис. 1.

3. Производится измерение f_c одного полученного результата функции $f(a)$. При этом волновая функция проецируется в суперпозицию состояний:

$$\varphi(a, f(a)) = \frac{1}{2^m} \sum_{x=0}^{2^m-1} g(a) |a, f(a)>, \tag{19}$$

где

$$g(a) = \begin{cases} 1, f(a) = f_c \\ 0, f(a) \neq f_c \end{cases}. \tag{20}$$

Т. е., квантовая система содержит только состояния аргумента a, для которых значения функции $f(a)$ равно измеренному f_c; волновая функция в данном случае является периодической с периодом r.

4. Для извлечения периода необходимо выполнить преобразование Фурье волновой функции (19). При этом используется реализация квантового преобразования Фурье, имеющего следующий вид:

$$U_{qft} : |c, f_c> \rightarrow \frac{1}{\sqrt{2^m}} \sum_a e^{\frac{2\pi i a c}{2^m}} |a, f_c>. \tag{21}$$

В случае преобразования Фурье дискретной периодической функции получаем спектр, содержащий спектральные «всплески», связанные с периодом исходной периодической функции. Для квантовой системы получаем следующую волновую функцию:

$$\varphi(c) = \sum_j^{2^m-1} c_j \left| j \frac{2^m}{r}, f_c \right>. \tag{22}$$

Квантовая система переводится в суперпозицию состояний. При этом первый регистр содержат значения, обратно пропорциональные r. Спектр имеет вид, представленный на рис. 2.

5. Производится измерение первого регистра. Получается значение:

$$v = j \frac{2^m}{r}, \tag{23}$$

где r – искомый период, j – неизвестный индекс спектрального всплеска.

Выражение (19) может быть представлено в следующем виде:

$$rv - j2^m = 0. \tag{24}$$

В данном выражении v – измеренное значение первого регистра, r – искомый период, j – неизвестный индекс измеренного регистра. В данном уравнении необходимо найти r и j. Данное уравнение является диафантовым. Существует эффективный (полиномиальный) алгоритм решения уравнения вида (24) с использованием цепных дробей. Если найденное значение r является четным, оно используется для факторизации числа N (8) – (10). В противном случае алгоритм повторяется с другим выбранным значением x (выражение (1)).

Данный алгоритм обладает полиномиальной сложностью, т. к. основан на эффекте квантового параллелизма и не требует перебора вариантов аргументов функции (1).

IV Моделирование алгоритма квантовых вычислений Шора

Приведенный выше алгоритм был промоделирован с использованием традиционных алгоритмических и вычислительных механизмов.

На рис. 1 представлено распределение значения функции $f(a) = x^a \bmod N$ (dependence of result on argument), а ее спектра $F(c) = \sum_{a=0}^{q-1} e^{2\pi i c a} f(a)$ (dependence of amplitude module on argument) – на рис. 2.

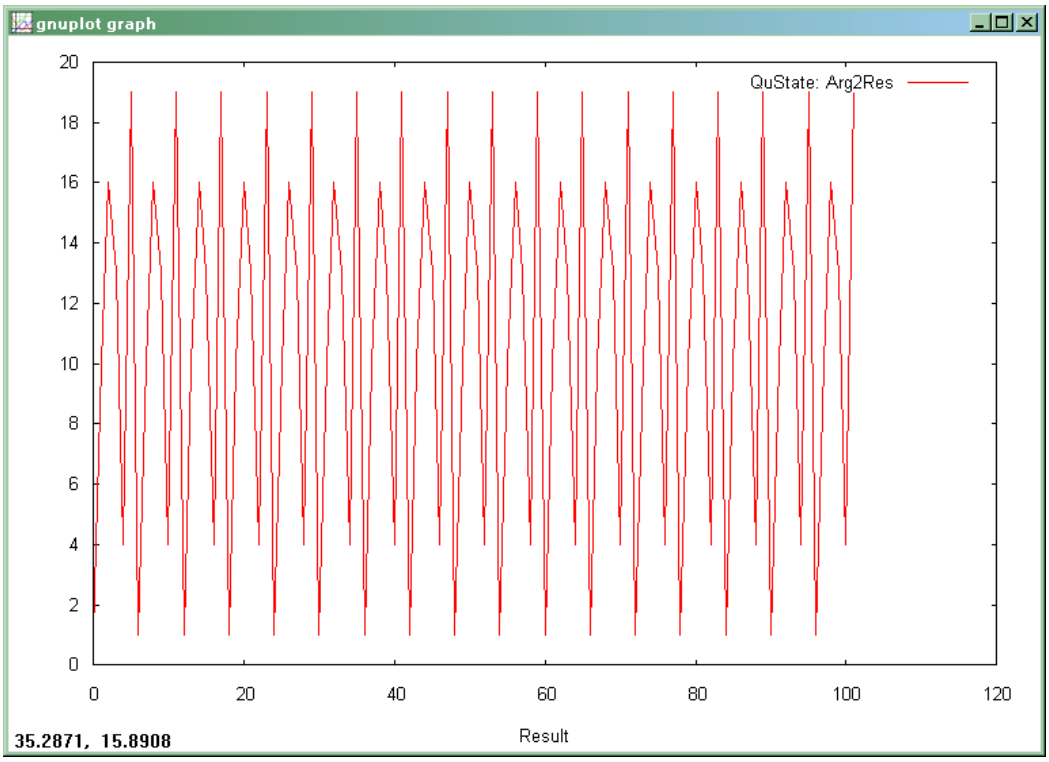

Рисунок 1

В связи с тем, что вычисления проводятся в Гильбертовом пространстве, система моделирования является достаточно требовательной к ресурсам (к памяти и производительности процессора).

При факторизации чисел необходимо учитывать, что потребная память для хранения отображения системы рассчитывается следующим образом:

$$mem(N) = 2^{3len(N)}[3len(N) + 2len(double)], \qquad (25)$$

где len – функция, возвращающая длину аргумента в битах.

Например, при факторизации числа $N = 21, len(21) = 5$ система моделирования использует не менее $2528 \cdot 1024$ бит. Для факторизации числа $len(N) = 16$ потребуется не менее 30064771072 Mb.

Проведен анализ алгоритма факторизации Шора, который позволяет решать задачи факторизации целых чисел с полиномиальной сложностью.

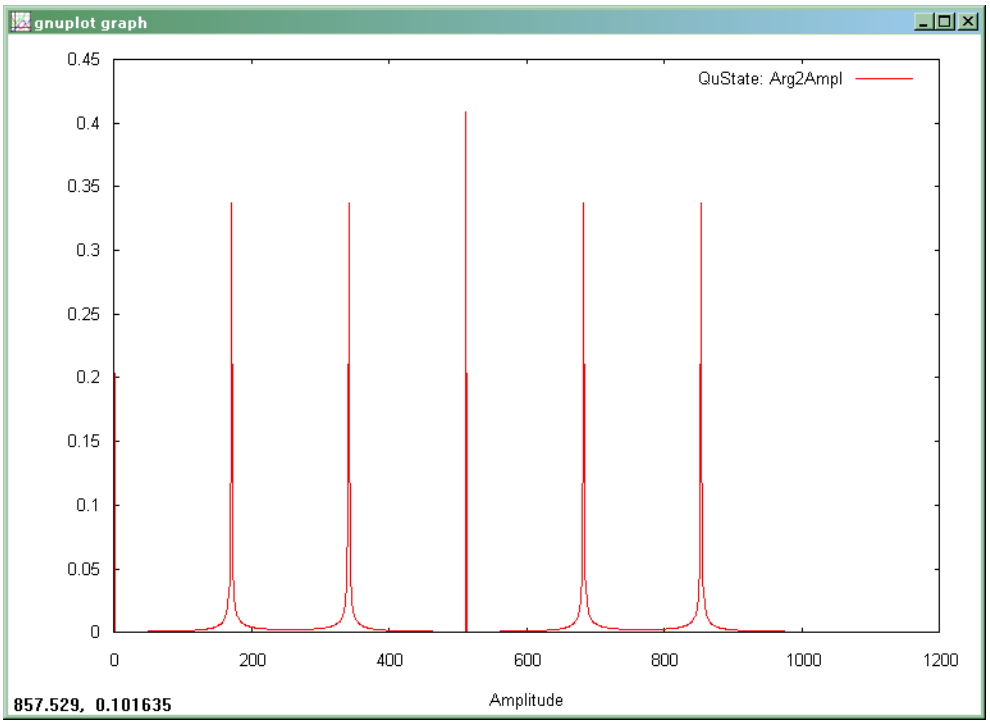

Рисунок 2

V Заключение

Следует отметить, что в настоящее время существует всего лишь несколько алгоритмов в основном для NP-полных задач: алгоритм факторизации целых чисел, алгоритм решения задачи дискретного логарифмирования, и алгоритм поиска элемента в несортированной базе. По-прежнему на данном этапе является открытой проблема возможности создания универсального решения, позволяющего решать широкий круг NP-полных задач с полиномиальной сложностью. Решение данной проблемы может расширить круг возможностей вычислительной техники в областях, связанных как с моделированием квантово-механических физических процессов, эффективным решением задач искусственного интеллекта, так и эффективным решением криптоаналитических задач несимметричной криптографии.

Литература: ***1.*** *Yu. Manin. Computable and uncomputable (in Russian). - Moscow, Sovetskoye Radio, - 1980. – 34-38pp.* ***2.*** *R. Feynman. Simulating physics with computers. - International Journal of Theoretical Physics 21, 6&7, – 1982. - 467-488pp.* ***3.*** *E. Reiffel, W. Polak. Fundamentals of quantum calculations. - ACM Computing Surveys, V. 32, №3, - September 2000. – 5-62pp.* ***4.*** *Брауншгейн С. Л. Квантовые вычисления: учебное руководство. - Encyclopedia of Applied Physics, Update, WILEY-VCH, - 1999, – 35.* ***5.*** *P. W. Shor. Algorithm for quantum computation: Discrete log and factoring. - In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, - November 1994. - 124-134 pp.* ***6.*** *Стин. Квантовые вычисления. - Ижевск: Регулярная и хаотическая динамика, - 2000. – 100 с. 7. B. Omer. Simualtion of Quantum Computers. – Vienna: Technical University of Vienna. - 1996. – 23.*

УДК 621.391.15

МЕТОД ФОРМИРОВАНИЯ СЕКРЕТНОГО КЛЮЧА В КВАНТОВО-КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ КОРРЕКТИРУЮЩЕГО КОДА

Дмитрий Алексеев
Специальный факультет СБ Украины ВИТИ НТУУ «КПИ»

Аннотация: **Предложен метод формирования секретного ключа с использованием корректирующих**