Квантовые устройства в криптографии

С.А. Букашкин, М.А. Черепнев,

Аннотация --- **В последнее время появилось много работ, где предлагается использовать квантово-механические свойства межатомного взаимодействия для решения криптографических задач. Фактически, речь идет о перенесении решения задачи стойкости схем защиты информации с математического аппарата на свойства квантово-механических объектов. В работе рассматриваются положительные и отрицательные стороны этого подхода в сравнении с математической криптографией. Представлены предложения по использованию криптографических устройств для построения и анализа криптопротоколов. Важное направление приложения квантовых механизмов – это построение на их основе вычислительного устройства. В статье дан обзор и рассматриваются проблемы и перспективы такого подхода. Рассматриваются преимущества полупроводниковых и фотонных реализаций. Предложена новая структура фотонного устройства для решения практических вычислительных задач с использованием новых принципов квантовой физики. Это предложение представляется более стойким относительно проблем с идеальными условиями работы и исправлением ошибок. Проведен анализ криптографических свойств используемых сегодня квантовых каналов на предмет новизны по сравнению с аналогичными решениями математической криптографии. Рассмотрены некоторые другие возможности применения квантовых устройств (квантовых сенсоров) в криптографии. В том числе предложены конструкции криптопротоколов на чисто физической основе.**

Ключевые слова: квантовый компьютер, квантовые алгоритмы, постквантовая криптография, фотоны.

I. ВВЕДЕНИЕ

В 1979-80 годах Манин Ю.И. [1] анонсировал необходимость создания математической теории квантовых автоматов, основой которых будет использование суперпозиции, отсутствие однозначного разделения квантовой системы на элементы, описание взаимодействия Эрмитовыми операторами и вероятностными терминами. Исследуя некоторые квантово-механические эффекты Р.Фейнман [2] в 1982г. пришел к аналогичным выводам. В дальнейшем вместо бит, как единиц хранения информации, стали рассматривать так называемые кубиты (или квантовые биты) способные принимать уже не два, а большее количество состояний, обычно представляемых на так называемой сфере Блоха. Физически это могут быть атомы, фотоны, находящиеся в возбужденном состоянии, или другие физические объекты, поглощающие и отдающие энергию фиксированными порциями, квантами. Реализовать работу кубитов на практике оказалось сложной задачей.

Введем несколько определений.

Квантовый процессор – вычислительное устройство, в основе которого лежат Эрмитовы унитарные операции с кубитами. Например, n-разрядный квантовый регистр может хранить 2^n значений в одном месте, а квантовый процессор может все эти значения одновременно обрабатывать [7,8].

Квантовый компьютер – вычислительное устройство на основе квантовых процессоров, способное работать по программе.

В отличие от квантового процессора, квантовый компьютер трудно реализовать. Существующие реализации, пока носят лабораторный характер. Камнем преткновения является проблема исправления ошибок, связанная с невозможностью копирования состояния, а также вытекающая из этого неустойчивость физических устройств и самих вычислений.

Важно отметить, что элементарные операции в квантовом компьютере (квантовая арифметика) связаны с тригонометрическими суммами, и поэтому принципиально отличаются от операций обычной арифметики.

Основы квантовых вычислений были заложены Дэвидом Дойчем в 1985 году в работе [3]. Однако за истекшие 40 лет квантовый компьютер построен не был. Есть рабочие модели квантовых процессоров [6], работающие с некоторыми ошибками, которые пока не удается исправить. Эти ошибки могут быть связаны с внешним шумом, работой соседних кубитов и попытками измерения состояния кубита или сравнения состояний разных кубитов. Из-за этого в квантовых вычислениях происходят ошибки, и дальше эволюция квантового процессора становится уже неконтролируемой. Применение известной технологии кодирования с последующим исправлением ошибок осложнено невозможностью копирования состояния кубита.

Проблемы, с которыми столкнулись технологи при построении квантового компьютера, имеют качественный, а не количественный характер. Поэтому в самое ближайшее время он, вероятно, не может быть построен. С другой стороны, открытые в последнее время квантово-механические эффекты в физике и теория тригонометрических сумм могут быть положены в основу новой теории квантовых

вычислений вне зависимости от вида и времени её реализации на практике. Эта теория может быть использована как для моделирования природных квантово-механических процессов, так и для решения с их помощью вычислительных задач, решение которых на обычном компьютере практически невозможно.

Отметим, что ситуация с квантовым компьютером сейчас отличается от ситуации с обычным компьютером в середине 20 века и ранее. Первые компьютеры хоть и медленно, но работали (например, суммирующая машина Паскаля 1642г. осуществляла арифметические преобразования пятизначных десятичных чисел, разностная машина Беббиджа 1822г. вычисляла значения многочленов 7-й степени, ЭВМ “Bombe” Тьюринга 1940г. осуществляла взлом шифровальной машины Enigma), а первые квантовые - нет.

В условиях нарастающего глобального противостояния государств многократно возрастает ответственность за обеспечение безопасности киберпространства Российской Федерации. Киберзащищенность элементов критической инфраструктуры является вопросом национальной безопасности России.

В общем объеме вычислительных ресурсов, а также в доле суперкомпьютеров из списка TOP 500 Россия уступает США в 100 раз (аналогично и в отношении Китая). При существующем общемировом темпе роста вычислительных мощностей это отставание соответствует примерно 10 годам. В научно-технический оборот поступают вычислители на основе новых физических принципов (графические расширители, видеокарты и др.), существенно повышающие производительность обычных компьютеров. Еще более стремительно развиваются коммуникационные сети. Тем самым возрастают возможности утечки информации по неконтролируемым каналам связи.

Перспективы построения квантового компьютера и квантово-устойчивые алгоритмы рассмотрены авторами статьи в работе [11].

II. ОЦЕНКИ ДОСТОВЕРНОСТИ КВАНТОВОЙ ОПЕРАЦИИ

Если $1/k^s$ это вероятность успешного срабатывания одного кубита в s шагах программы для n кубитного процессора, вычисляющего функцию от n битного аргумента. Тогда для того, чтобы получить хотя бы один правильный результат нам понадобится в среднем произвести k^{sn} квантовых шагов. При $k^s>2$ это больше, чем количество всех возможных аргументов данной задачи (которое равно 2^n). Поэтому значительного выигрыша по сравнению с обычным компьютером, последовательно обрабатывающим эти аргументы, мы не получаем. По всей видимости, процедура исправления ошибок должна быть также квантовой. Отметим, что в данных рассуждениях мы рассматриваем вероятности успешного срабатывания кубитов как независимые случайные величины, что на практике совершенно не так. При работе кубит создает шум, который влияет на соседние кубиты. Как отмечалось в докладе директора совместного исследовательского центра «Функциональные Микро/Наносистемы» ФГБОУ ВО «МГТУ имеи Н.Э.Баумана (национальный исследовательский университет)» и ФГУП «ВНИИА имени Н.Л.Духова» И.А.Родионова на заседании, посвященном квантовым вычислениям, в марте 2022 года: реализация двухкубитной операции на 20-и кубитной системе обладала достоверностью примерно в 94%, в то время как изолированная работа двухкубитной системы показывала достоверность около 99,5%. Таким образом, оценка на число квантовых шагов, необходимых для достоверной реализации s шагов алгоритма на n-кубитной системе может оказаться больше приведенного выше значения.

Отметим, что для эффективного использования квантового компьютера при решении современных криптографических задач, достаточно 500-1000 кубит, по числу двоичных разрядов, используемых для записи параметров современных систем защиты информации. Например, если удастся записать преобразования секретного ключа в виде небольшой (полиномиальной длины) последовательности Эрмитовых унитарных преобразований, то при известном результате мы получим секретный ключ, поскольку все преобразования обратимы.

В 1997 году Питером Шором [12] были предложены эффективные алгоритмы дискретного логарифмирования в простом поле и целой факторизации. Эти алгоритмы построены на основе реализации квантовой операции общего вида, представленной унимодулярным преобразованием экспоненциального размера, с помощью двухкубитных преобразований, выполняющихся последовательно. Например, для применения алгоритма Шора к решению задачи факторизации числа n (см. [4] стр.15) необходимо сделать $O((\log n)^2 (\log\log n) (\log\log\log n))$ квантовых шагов. То есть, для адекватных сегодняшним криптосхемам параметров, придется предусмотреть последовательное выполнение не менее 10^7 достоверных двухкубитных операций на системе из около 1000 кубитов. Для получения результата с некоторой реальной вероятностью, необходимо обеспечить вероятность ошибки при одной такой операции не выше 10^{-7} . В то же время, как мы видели выше, в современных реализациях систем из нескольких десятков кубитов, вероятность ошибки не опускается ниже 1/20. При этом зависимость вероятности ошибки в квантовой операции от числа предшествующих ей квантовых операций при последовательном их применении и от текущего состояния квантовой системы не исследовано. Сколько должно пройти времени, чтобы уменьшить вероятность ошибки при производстве квантовой операции в миллион раз? Ясно, что это задача не ближайшего будущего.

Ввиду полиномиального, но большого числа необходимых последовательных квантовых операций с большим числом кубитов, квантовые алгоритмы решения криптографически значимых задач, такие как алгоритмы факторизации и дискретного логарифмирования Шора и переборный алгоритм Гровера [5] , представляются на данный момент непрактичными. В тоже время, такие алгоритмы как алгоритм Дойча-Йожи [9] с одной квантовой операцией и алгоритм Бернштейна-Вазерани [10] с ограниченным, не зависящим от длины входа,

количеством квантовых операций, представляются более реалистичными с практической точки зрения.

Общий вывод можно сделать такой: Дальнейшее развитие теории и практики квантовых вычислений, скорее всего, пойдет по пути реализации алгоритмов с ограниченным числом квантовых операций. Именно об одной квантовой операции говорилось при постановке экспериментов с первыми квантовыми вычислителями Sicamore в США [6] , Jiuzhang в Китае [13] . Для эффективного решения задач дискретного логарифмирования и факторизации на квантовых вычислителях, работающих с ошибками, нужны алгоритмы, отличные от алгоритмов Шора и Гровера, использующие существенно меньшее, ограниченное число квантовых операций.

III. ТЕХНОЛОГИЯ «ВЫСТРЕЛ»

В последнее время появилась масса пропагандистских статей, предрекающих скорое построение квантового компьютера. Довольно часто авторами этих статей являются не физики и математики, а журналисты. В 2019 году появилась научная статья [6], где описаны эксперименты с 53 кубитным процессором. Он работает в гильбертовом пространстве размерности 2^{53} с двоичными переменными. Однако избавиться от ошибок в этих вычислениях авторы не смогли.

Более интересен китайский бозонный сэмплер «Jiuzhang 2020» [13]. Дело в том, что фотоны более стабильны, не требуют охлаждения, лучше масштабируются и обладают большим числом характеристик, которыми можно управлять, выше частота, скорость распространения сигнала, емкость канала передачи, возможны манипуляции. С другой стороны аналоговые устройства трудно сопрягать с существующими цифровыми устройствами.

Нам представляется, что для реализации конкретных практических задач не нужен полноценный квантовый компьютер. Предлагается технология «Выстрел»: Одна полномасштабная квантовая операция с последующим анализом результатов на обычном компьютере. В этом случае уменьшаются проблемы с нагревом, количеством ошибок, проще создать идеальные условия. Практическая реализация одной операции на квантовой системе, принимающей 2^{500} состояний, была бы принципиальным прорывом для решения прикладных задач. Это позволило бы реализовать квантовые алгоритмы с ограниченным количеством квантовых операций, такие как алгоритмы Дойча-Йожи [9] и Бернштейна-Вазерани [10]. Правда, при таком подходе известные квантовые алгоритмы Шора, Гровера остаются непрактичными. Нужны будут другие алгоритмы.

Принципиально китайский эксперимент с бозонным сэмплером Jiuzhang 2020 можно считать реализацией технологии «Выстрел» для решения чисто физических задач физическими же средствами. Этот эксперимент предсказывает, что эта технология может быть применена и для решения других задач. При этом представляется разумным подготовка начальных условий в такой задаче на физическом носителе, то есть в виде некоторой решетки или матрицы, через которую в дальнейшем пропустить фотоны и получить результат также на физическом, возможно другом, носителе.

Целью рассматриваемых исследований является построение квантового спец-вычислителя для решения конкретных практических задач при помощи алгоритмов с небольшим количеством квантовых операций. В случае исключения получения практического результата как цели исследований, разрозненные усилия физиков и математиков будут наполнять знаниями международную базу знаний, увеличивая риски ее использования в деструктивных целях. Кроме указанных выше, хотелось бы отдельно упомянуть разработки ускорителей для обычных компьютеров и суперкомпьютеров на новых физических принципах.

IV. КВАНТОВАЯ КРИПТОГРАФИЯ

Необходимо принимать во внимание, что в отличие от традиционной криптографии, которая использует математические методы для обеспечения секретности информации, квантовая криптография сосредоточена, прежде всего, на физике и физических явлениях, при которых информация переносится и защищается с помощью объектов квантовой механики и их свойств. Подобные подходы были популярны в самом начале развития асимметричной криптографии (Bell Labs 1943, GCHQ (штаб правительственной связи) 1970 [14]). Технология квантовой криптографии опирается на принципиальную неопределенность поведения квантовой системы, выраженную в принципе неопределенности Гейзенберга - невозможно одновременно получить координаты и импульс частицы, невозможно измерить один параметр фотона, не исказив другой. В этой связи следует отметить риски применения квантово-механических криптосистем, связанные с неадекватным знанием их свойств по сравнению с уровнем знаний об этом в других государствах.

Наибольшее продвижение в современной квантовой криптографии получено в вопросе построения квантового канала передачи информации. При использовании одиночных фотонов в таком канале, невозможно измерить их характеристики не изменив их. То есть канал нельзя прослушать, не нарушив целостность передаваемой по нему информации. Это неизвестное математической криптографии свойство является следствием именно квантовых технологий, однако атаки типа «человека посередине» все равно остаются действенными. Другой пример квантового канала – это разделенные расстоянием частицы, находящиеся в запутанном состоянии. При изменении состояния одной из них, автоматически меняется состояние другой. Получается закрытый от постороннего доступа канал связи. Пара используемых при этом частиц является общим секретным ключом, распределение которого даже более трудоемко, чем в случае использования обычных цифровых ключей и не может быть сделано удаленно, как при использовании асимметричной криптографии.

Еще одно направление применения квантовых эффектов в криптографии - это квантовые сенсоры.

V. ОБ ИСПОЛЬЗОВАНИИ КВАНТОВЫХ СЕНСОРОВ В КРИПТОГРАФИИ

В последнее время очень много физических исследований нашли свое воплощение на практике в виде сенсоров, работающих на квантовом уровне. Граница между обычными и квантовыми сенсорами размыта. По большому счету речь идет о сенсорах с большой разрешающей способностью. С их помощью можно пробовать решать следующие криптографические задачи:

1. Построение псевдослучайных последовательностей. Эта задача решена до аппаратного завершения.
2. Всевозможные биосенсоры уже используются для локальной аутентификации клиентов.
3. Построение высокоточных атомных часов. Такие часы могли бы быть использованы вместо серверов времени на некоторых временных интервалах. В децентрализованных схемах это позволило бы избежать опасности перехвата управления сервером времени, который по своей природе является центральным устройством в системе (то есть слабым звеном). Конечно, данную уязвимость можно избежать и по-другому, дублированием сервера времени с последующей регулярной синхронизацией с консенсусом. Но и в этом случае использование высокоточных атомных часов разными «зеркалами» сервера времени позволило бы значительно увеличить время между синхронизациями, а значит повысить надежность всей системы.
4. Сенсоры электрического и магнитного полей могут быть использованы для прослушивания шифровального оборудования, работающего в той-же электрической сети, или при изучении генерируемого или рассеиваемого ими электрического или магнитного поля.
5. Эти же сенсоры могут быть использованы для создания электрических и магнитных ключей наряду с распространенными графическими (которые легко копировать) и биометрическими (которые привязаны к телу).
6. Поскольку при последовательном наложении электрических и магнитных полей результирующее поле не зависит от порядка их наложения, то, передавая возбуждение с помощью пар частиц в спутанном состоянии, можно реализовать схему открытого распределения ключа на чисто физических эффектах. Таким образом, мы можем получить в квантовой криптографии протоколы ОРК и ЦП.
7. Локальный сенсор химических событий может быть использован для существенного увеличения длины общего секретного ключа уже не аналитическими, а чисто физическими средствами. Совмещение этих способов могло бы кратно увеличить эту длину.

БИБЛИОГРАФИЯ

[1] Манин Ю.И. Вычислимое и невычислимое.// Советское радио, 1980, 130с.

[2] Feynman R. International Journal of Theoretical Physics 21 (1982) 467.

[3] Deutsch David Quantum theory, the Church-Turing principle and the universal quantum computer // Proceedings of the Royal Society of London; Series A, Mathematical and Physical Sciences : journal. — 1985. — July (vol. 400, no. 1818). — P. 97—117. — doi:10.1098/rspa.1985.0070.

[4] Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM J. Comput. 1997. Vol. 26, № 5. P. 1484–1509

[5] Grover L.K. A fast quantum mechanical algorithm for database search // Proceedings 28th Annual ACM Symposium on the Theory of Computing, (May 1996), p. 212

[6] Фрэнк Аруте , Кунал Арья , […] Джон М. Мартини Квантовое превосходство с использованием программируемого сверхпроводящего процессора // Nature v.574(2019), p.505-510 https://www.nature.com/articles/s41586-019-1666-5

[7] Andrew M. Steane, Eleanor G. Rieffel Beyond Bits: The Future of Quantum // Information Processing. Computer 33 (1): 38-45 DOI: 10.1109/2.816267

[8] Eleanor Rieffel An Introduction to Quantum Computing for Non-Physicists // ACM Computing Surveys 32 (3) 48p. DOI: 10.1145/367701.367709

[9] David Deutsch and Richard Jozsa // Rapid solution of problems by quantum computation. Proceedings of the royal society A math., phyz., eng. sci., 1992, v.439, iss. 1907 https://royalsocietypublishing.org/doi/10.1098/rspa.1992.0167

[10] Ethan Bernstein, Umesh Vazirani. Quantum Complexity Theory // Proceedings of the Twenty-fifth Annual ACM Symposium on Theory of Computing. — New York, NY, USA: ACM, 1993. — С. 11–20. — ISBN 978-0-89791-591-5. — doi:10.1145/167088.167097

[11] Букашкин С. А., Черепнёв М. А. Квантовый компьютер и постквантовая криптография. Программная инженерия, т.12 (2021), №4 (июль), с. 171–178, DOI: 10.17587/prin.12.171-178

[12] Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on IEEE, 1994., P. 124–134., ISBN 0-8186-6580-7, doi:10.1109/SFCS.1994.365700

[13] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, Peng Hu, Xiao-Yan Yang, Wei-Jun Zhang, Hao Li, Yuxuan Li, Xiao Jiang, Lin Gan, Guangwen Yang, Lixing You, Zhen Wang, Li Li, Nai-Le Liu, Chao-Yang Lu, Jian-Wei Pan Quantum computational advantage using photons.// Science, 3 Dec 2020, Vol 370, Issue 6523, pp. 1460-1463 DOI: 10.1126/science.abe8770

[14] James Ellis https://en.wikipedia.org/wiki/James_H._Ellis

* Статья опубликована при финансовой поддержке Минобрнауки России в рамках реализации программы Московского центра фундаментальной и прикладной математики по соглашению № 075-15-2022-284

Букашкин С.А. д.т.н., профессор, генеральный конструктор АО «Концерн «Автоматика» (e-mail: sergey.bukashkin@gmail.com,)

Черепнев М.А. д.ф.-м.н., профессор, факультет ВМК МГУ имени М.В.Ломоносова, кафедра информационной безопасности (e-mail: cherepniov@gmail.com).

Quantum Devices in Cryptography

S.A. Bukashkin, M.A. Cherepnev,

Abstract - Recently, many papers have appeared where it is proposed to use the quantum mechanical properties of interatomic interaction to solve cryptographic problems. In fact, we are talking about transferring the solution of the problem of the stability of information protection schemes from the mathematical apparatus to the properties of quantum mechanical objects. The paper discusses the positive and negative aspects of this approach in comparison with mathematical cryptography. The proposals on the use of cryptographic devices for the construction and analysis of cryptographic protocols are presented. An important area of application of quantum mechanisms is the construction of a computing device based on them. The article provides an overview and discusses the problems and prospects of such an approach. The advantages of semiconductor and photonic realizations are considered. A new structure of a photonic device is proposed for solving practical computational problems using new principles of quantum physics. This proposal seems to be more resistant to problems with ideal working conditions and error correction. The cryptographic properties of the quantum channels used today are analyzed for novelty in comparison with similar solutions of mathematical cryptography. Some other possibilities of using quantum devices (quantum sensors) in cryptography are considered. In particular, the designs of cryptoprotocols on a purely physical basis are proposed.

Keywords: quantum computer, quantum algorithms, post-quantum cryptography, photons.

REFERENCES

[1] Manin Ju.I. Vychislimoe i nevychislimoe.// Sovetskoe radio, 1980, 130s.

[2] Feynman R. International Journal of Theoretical Physics 21 (1982) 467.

[3] Deutsch David Quantum theory, the Church-Turing principle and the universal quantum computer // Proceedings of the Royal Society of London; Series A, Mathematical and Physical Sciences : journal. — 1985. — July (vol. 400, no. 1818). — P. 97—117. — doi:10.1098/rspa.1985.0070.

[4] Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM J. Comput. 1997. Vol. 26, # 5. P. 1484–1509

[5] Grover L.K. A fast quantum mechanical algorithm for database search // Proceedings 28th Annual ACM Symposium on the Theory of Computing, (May 1996), p. 212

[6] Frjenk Arute , Kunal Ar'ja , […] Dzhon M. Martini Kvantovoe prevoshodstvo s ispol'zovaniem programmiruemogo sverhprovodjashhego processora // Nature v.574(2019), p.505-510 https://www.nature.com/articles/s41586-019-1666-5

[7] Andrew M. Steane, Eleanor G. Rieffel Beyond Bits: The Future of Quantum // Information Processing. Computer 33 (1): 38-45 DOI: 10.1109/2.816267

[8] Eleanor Rieffel An Introduction to Quantum Computing for Non-Physicists // ACM Computing Surveys 32 (3) 48p. DOI: 10.1145/367701.367709

[9] David Deutsch and Richard Jozsa // Rapid solution of problems by quantum computation. Proceedings of the royal society A math., phyz., eng. sci., 1992, v.439, iss. 1907 https://royalsocietypublishing.org/doi/10.1098/rspa.1992.0167

[10] Ethan Bernstein, Umesh Vazirani. Quantum Complexity Theory // Proceedings of the Twenty-fifth Annual ACM Symposium on Theory of Computing. — New York, NY, USA: ACM, 1993. — S. 11–20. — ISBN 978-0-89791-591-5. — doi:10.1145/167088.167097

[11] Bukashkin S. A., Cherepnjov M. A. Kvantovyj komp'juter i postkvantovaja kriptografija. Programmnaja inzhenerija, t.12 (2021), #4 (ijul'), c. 171–178, DOI: 10.17587/prin.12.171-178

[12] Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on IEEE, 1994., P. 124–134., ISBN 0-8186-6580-7, doi:10.1109/SFCS.1994.365700

[13] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, Peng Hu, Xiao-Yan Yang, Wei-Jun Zhang, Hao Li, Yuxuan Li, Xiao Jiang, Lin Gan, Guangwen Yang, Lixing You, Zhen Wang, Li Li, Nai-Le Liu, Chao-Yang Lu, Jian-Wei Pan Quantum computational advantage using photons.// Science, 3 Dec 2020, Vol 370, Issue 6523, pp. 1460-1463 DOI: 10.1126/science.abe8770

[14] James Ellis https://en.wikipedia.org/wiki/James_H._Ellis