УДК 004.056.55

Кравченко В.О.,
аспирант
Донской государственный технический университет
Россия, г. Ростов-на-Дону
Черкесова Л.В.,
доктор физико-математических наук, профессор
профессор кафедры «Кибербезопасность информационных систем»
Донской государственный технический университет
Россия, г. Ростов-на-Дону

ОБЗОР ПОСТКВАНТОВЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Аннотация: *После создания достаточно мощного квантового компьютера неизбежен пересмотр требований к алгоритмам информационной безопасности. В данной статье сравниваются алгоритмы, способные не утратить актуальность при появлении мощных квантовых компьютеров. Проанализированы сорок два источника, из которых четырнадцать опубликованы в последние пять лет.*

Ключевые слова: *криптография, постквантовая криптография, асимметричная криптография, протоколы обмена ключами, электронная цифровая подпись.*

Annotation: *The revision of the requirements for information security algorithms will be inevitable after the creation of a sufficiently powerful quantum computer. This article compares the algorithms that can not lose relevance when powerful quantum computers appear. Forty-two sources are analyzed, of which fourteen have been published in the last five years.*

Key words: *cryptography, postquantum cryptography/quantum-safe cryptography, public-key cryptography, key exchange, digital signature.*

В современном мире информация играет особенно важную роль, поэтому передача и хранение данных должны быть максимально безопасными. На успехи физиков и инженеров, постепенно приближающих момент создания квантового компьютера, специалисты по информационной безопасности смотрят настороженно. Такая полезная в некоторых областях применения инновация, как квантовый компьютер в криптографическом сообществе, будет встречена не только без энтузиазма, но и с сожалением об обесценивании огромного пласта нашей науки. Скоропостижно уйдут в историю широко используемые алгоритмы, чья стойкость основывалась на сложности факторизации целых чисел или дискретного логарифмирования, ведь они станут бесполезны благодаря алгоритму Шора[1].

Одним своим существованием квантовый компьютер обрушит мир асимметричной криптографии [2], например, существующие в нынешнем виде банковские системы. И пока мир к этому не готов, но и физики работают медленно. С момента первых удачных экспериментов в 1998 г с 3-х кубитным компьютером на ядерно-магнитном резонансе [3] до современного 72-кубитного варианта [4] прошло целых 20 лет.

Для практической реализации этих угроз необходим достаточно производительный квантовый компьютер, а оценить его «эффективность» мы попробуем количеством кубитов. На самом деле, это не совсем верно: как число битов для классического компьютера, так и количество кубитов для квантового – в первую очередь, объем памяти. Однако, благодаря принципу квантовой суперпозиции и свойству запутанности, появилась возможность создать компьютер, способный к параллельным вычислениям на уровне своего физического устройства. Все оценки производительности квантового компьютера, которые будут приведены ниже, будут действительны только при условии стопроцентной надежности системы, в реальности из-за необходимости исправления ошибок, кубитов потребуется больше.

Существует такое понятие, как «квантовое превосходство» – это потенциальная способность квантовых вычислительных устройств решать

проблемы, которые классические компьютеры практически не могут, или им потребуется для этого слишком много времени [5]. В статье [6] был дан критерий наступления квантового превосходства, по мнению авторов, это – порог вычислительной мощности в 50 кубитов. Таким образом, квантовое превосходство достигнуто, а недавно созданная 72-кубитный квантовая машина Google Bristlecone [4] уже превосходит классический суперкомпьютер по четко определенной вычислительной задаче. Впрочем, каких-либо экспериментальных данных Google пока не обнародовала, ограничившись лишь небольшой заметкой об оптимистичных прогнозах тестирования своей новинки.

В статье [7] определено конкретное число $2n + 3$ кубитов, необходимых квантовому компьютеру для факторизации числа размером n бит, а следовательно и взлома алгоритма RSA с такой же длиной ключа. Это значит, что для дискредитации современного стандарта RSA с ключом в 2048 бит потребуется минимум 4099 кубитов.

Таким образом, для того, чтобы представлять реальную опасность для современных криптографических алгоритмов, квантовом компьютеру пока недостает ресурсов, но авторитетные в вопросах защиты информации организации уже объявили о намерении перехода на постквантовые алгоритмы. В частности, подобное заявление сделало Агентство национальной безопасности Соединённых Штатов [8].

Рассмотрим некоторые криптографические примитивы, которые смогут остаться актуальными, даже когда появится полноценный квантовый компьютер.

1. Симметричные алгоритмы.

Некоторые исследователи видят будущее постквантовой криптографии в использовании симметричных алгоритмов шифрования [9]. К примеру, при достаточной длине ключа криптосистема AES, благодаря своей архитектуре, для квантового компьютера не намного уязвимей, чем для классического. Созданный в 1996 г. алгоритм Гровера доказывает, что квантовый компьютер ускоряет атаки настолько, что эффективная длина ключа уменьшается вдвое. То есть, 256-битный ключ так же сложен для квантового компьютера, как 128-битный ключ

для классического [10]. Удвоение длины ключа не очень высокая цена в отсутствии альтернатив, но эпоха исключительно симметричной криптографии закончилась еще в 70-х годах прошлого века, и было бы опрометчиво просто сделать такой шаг назад. Достоинства: малая длина ключа; это старые и проверенные временем алгоритмы, они досконально изучены и повсеместно распространены; быстрые и простые. Недостатки: невозможно использовать для электронной подписи; сложно управлять ключами; низкая устойчивость к атакам по сторонним каналам. Невозможно представить симметричные алгоритмы как полноценную замену криптографии с открытым ключом, но как часть замены – вполне.

2. Эллиптические кривые

Криптостойкость систем, в основе которых лежат операции над эллиптическими кривыми, опирается на сложность вычисления дискретного логарифма. В свое время такие криптосистемы получили признание в том числе и за меньшую, по сравнению с, например, RSA, длину ключа, необходимую для такого же уровня безопасности. Значит ли это, что квантовому компьютеру потребуется меньше кубитов для взлома? Нет однозначного соответствия между криптосистемами и нужными характеристиками ключей, но примерная оценка есть – критерий Ленстры, основанный на примерном времени, которое требуется для подбора ключа при атаке полным перебором. Считается, что это примерно характеризует пространство ключей в некой области. Также существуют рекомендации некоторых организаций, например, NIST: текущий стандарт ставит в соответствие 2048-битному ключу для RSA 224-битный ключ для криптосистем, основанных на эллиптических кривых[11]. Подсчитано [12], что для подбора такого ключа потребуется квантовая машина, располагающая 1600 кубитами. Однако, помимо задачи дискретного логарифмирования в группе точек (ECDLP), эллиптические кривые могут предложить еще одну проблему, которую квантовому компьютеру решить будет непросто, а значит, на ее основе можно строить криптосистему.

Допустимость применения изогений для разработки криптосистем была предложена относительно недавно. В 2003 году была опубликована статья [13], в которой была предложена схема депонирования ключей с использованием изогений. В 2006 году схема шифрования Эль-Гамаля была применена с помощью изогений эллиптических кривых [14]. Тогда же для реализации хэш-функций было предложено использовать графы изогенных суперсингулярных кривых [15]. Возникает парадокс: для привычной криптографии на эллиптических кривых суперсингулярные кривые не годятся: задача ECDLP решается относительно просто, но для задачи об изогениях доказано[16], что использование обычных кривых ненадежно с «квантовой» точки зрения, для криптосистем, использующих изогении стоит использовать только суперсингулярные кривые.

Саму задачу, на сложности которой можно выстраивать криптосистему, можно сформулировать так: имеются две кривые, о которых известно, что они изогенны (по теореме Тейта [17]), но неизвестно, при помощи какой подгруппы можно эту изогению получить. Число подгрупп должно быть настолько большим, чтобы невозможно было найти изогению простым перебором, подставляя подгруппы в алгоритм Велю (алгоритм поиска возможных изогений для каждой кривой [18]).

Достоинства: система подходит для шифрования с открытым ключом[19], доказательства с нулевым разглашением[19], схемы неоспоримой подписи [20], подписи вслепую[21] и обмена ключами[22]; небольшой размер ключа. Недостатки: относительно медленный алгоритм, малопригодный для использования на небольших, ограниченных в ресурсах устройствах; это относительно новая и неизученная область.

Компания Microsoft в 2016 году выпустила библиотеку SIDH (Supersingular Isogeny Key Exchange) с открытым исходным кодом. SIDH реализована на языке Си. В библиотеке представлена реализация базовых арифметических функций и оптимизированная реализация операций на эллиптических кривых. В библиотеке

уже реализован протокол разделения ключа Диффи-Хеллмана на изогениях суперсингулярных кривых[23].

3. Коды исправления ошибок

Такие криптосистемы основаны на теории алгебраического кодирования, а сами алгоритмы базируются на сложности декодирования полных линейных кодов.

Достоинства: некоторые модификации, вроде системы Нидеррайтера могут быть использованы для ЭЦП [24]; по сравнению с RSA, скорость шифрования выше приблизительно в 50 раз, а дешифрования — в 100 раз, и с ростом длины ключа степень защиты данных растет гораздо быстрее [25];

Недостатки: размер ключа, так, к примеру, для устойчивости против квантового компьютера размер публичного ключа следует увеличить до 8,373,911 бит [26]; большой размер шифротекста, обусловленный использованием кодов с исправлением ошибок.

4. Группы кос

Первоначально косы были предложены Эмилем Артином в качестве математической модели для текстильной промышленности, но приложения этой теории оказались весьма разнообразными. Группы кос крайне эффективны при обеспечении трудоёмких вычислительных процессов.

Стойкость криптографических преобразований, основанных на группе кос, заключается в сложности решения проблемы поиска сопряжений и проблемы одновременного поиска множества сопряжений [27]. Эта задача была решена Ф.А. Гарсидом в 1969 г. Е.А. Элрифай и Г.Р. Мортон представили алгоритм, вычисляющий секретную косу за, где n — количество нитей в косе. Системы, основанные на группах кос, неоднократно подвергались криптоанализу [28], и совершенствовались в соответствии с полученными результатами атак. Также подвергался модернизации и алгоритм поиска сопряжений [28]. Однако в том, что касается существующей технологии и теории, проблема сопряженности в группе кос по-прежнему остается сложной [29], т.е. способа решения за

полиномиальное время пока не существует. Следовательно, n играет надежную роль параметра безопасности.

Достоинства: при более высокой вычислительной сложности алгоритма (по сравнению с RSA-1024) время шифрования больше, но дешифрования - меньше [30]. При этом генерация ключа происходит более чем в 100 раз быстрее, а общее время шифрования и дешифрования сообщений с использованием криптосистемы на группе кос меньше [30]. Современные варианты схем ЭЦП [31], высоко оцениваются с практической точки зрения[28]. Из недостатков можно отметить только высокую вычислительную сложность операции шифрования, а также новизну и «необкатанность» технологии.

5. Криптография на решётках

Криптостойкость этих алгоритмов базируется на сложности задач теории решёток, самой основной из которых является задача поиска кратчайшего вектора (SVP). Здесь в качестве входных данных мы задаем решетку, представленную произвольным базисом, и наша цель состоит в том, чтобы вывести в ней кратчайший ненулевой вектор [32]. На этом примитиве построены несколько протоколов шифрования[33][34], реализована ЭЦП [35], но отдельно необходимо отметить протокол обмена ключами с прекрасным названием «New Hope» [36], выбранным в 2015 году компанией Google для первого массового эксперимента по испытанию и внедрению постквантовой криптографии [37]. В рамках этого исследования новый протокол применялся в браузере «поверх» прежнего, что не позволяло снизиться уровню безопасности. Получившаяся комбинация получила название «CECPQ1», что в переводе на русский означает «Комбинированная эллиптическая кривая + постквантовый № 1». В ноябре 2016 года Адам Лэнгли, инженер Google поделился обновленной информацией о ходе эксперимента в заметке [38], признав его успешным: исследователей полностью удовлетворила работа постквантового алгоритма, а сопутствующее снижение производительности было признано умеренным и приемлемым [38].

6. Хэш-функции

Самостоятельная их область применения ограничена лишь ЭЦП, но хэш-функции являются важным компонентом многих криптосистем. Алгоритм Гровера можно использовать для нахождения коллизии в хэш-функции с шагом в квадратный корень ее первоначальной длины. Кроме того, было доказано, что можно сочетать алгоритм Гровера с атакой «дней рождения» [39]. Поэтому эффективная длина ключа уменьшается в три раза, что скомпрометирует некоторые из использующихся сегодня функций.

Алгоритмы, зачастую созданные давно и не получившие широкого признания из-за каких-либо недостатков, благодаря квантовой угрозе переживают второе рождение, над ними снова кипит работа: к системе McEliece примеряют другие группы кодов [40], а признанные ранее бесперспективными для использования в криптографии суперсингулярные кривые снова выходят на первый план [16]. И эти недостатки не помешали всем вышеописанным примитивам в том или ином виде поучаствовать в конкурсе Национального института стандартов и технологий США, целью которого является поиск, испытания и стандартизация оптимального постквантового асимметричного алгоритма [41].

В условиях достигнутого квантового превосходства [6] и недвусмысленных заявлений уполномоченных лиц о необходимости безотлагательных мер [8], уже невозможно считать квантовые компьютеры страшилкой из далекого будущего. Компания IBM, например, позволяет каждому на своем сайте поэкспериментировать с эмулятором квантового компьютера на 5 кубит [42], - это будущее уже наступило. И несмотря на то, что у квантового компьютера еще много конструктивных проблем, и никто не знает точно даже абстрактную модель, в соответствии с которой удастся создать достаточно мощный квантовый компьютер (работы ведутся во множестве возможных направлений), специалисты по информационной безопасности неустанно ищут новые пути развития асимметричной криптографии. Это работа наперегонки, в которой криптографы пока отстают из-за недостатка сведений о «враге». В эпоху информационных войн даже гонка вооружений, и та электронная.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science: Conference Publications. — 1997. — P. 1484–1509.

2. Валиев, К.А. Квантовая информатика: компьютеры, связь и криптография // Вестник российской академии наук. — 2000. — Том 70. — № 8. — С. 688—695

3. Chuang, I. L. Experimental Implementation of Fast Quantum Searching/ I.L Chuang, N. Gershenfeld, M. Kubinec// Physical Review Letters.- 1998. - № 80 (15). – С. 3408–3411.

4. A Preview of Bristlecone, Google’s New Quantum Processor [Электронный ресурс] // Блог компании Google. – Режим доступа URL: // https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html (дата обращения 05.12.2018)

5. Preskill J. Quantum computing and the entanglement frontier [Электронный ресурс]/ arXiv.org – e-print service. 2018. – Режим доступа URL:// https://arxiv.org/abs/1203.5813 (дата обращения 07.12.2018)

6. Boixo S. Characterizing quantum supremacy in near-term devices/S. Boixo, S.V. Isakov, V. N. Smelyanskiy// Nature Physics. – 2018. - № 14. - С. 595–600

7. Beauregard S. Circuit for Shor's algorithm using 2n+3 qubits/ S.Beauregard// Quantum Information and Computation. – 2003. - № 3(2). – С. 175-185

8. Commercial National Security Algorithm Suite [Электронный ресурс] // Сайт Агентства национальной безопасности США – Режим доступа URL: // https://apps.nsa.gov/iad/programs/iad-initiatives/cnsa-suite.cfm (дата обращения 05.12.2018)

9. Perlner R. A., David A. C. Quantum Resistant Public Key Cryptography: A Survey/ R. A. Perlner, A. C. David// 8th Symposium on Identity and Trust on the Internet (IDtrust 2009) сборник статей. – Gaithersburg, 2009. – С. 85-93

10. Grover L.K.: A fast quantum mechanical algorithm for database search/ L.K. Grover// 28th Annual ACM Symposium on the Theory of Computing сборник статей. – Philadelphia, 1996. - С. 212-219

11. Recommendation for Key Management, Part 1: General [Электронный ресурс]// The National Institute of Standards and Technology (NIST). – режим доступа URL: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final (дата обращения 05.12.2018)

12. Proos J. Shor's discrete logarithm quantum algorithm for elliptic curves / J. Proos, C. Zalka//QIC. – 2003. - № 3(4). – С.317-344

13. Teske E. An Elliptic Curve Trapdoor System/ E. Teske // Journal of Cryptology. – 2006. - №19(1). – С.115-133.

14. Rostovtsev A. Public-Key Cryptosystem Based on Isogenies [Электронный ресурс]/ A. Rostovtsev, A. Stolbunov// ResearchGate. – режим доступа URL:https://www.researchgate.net/publication/220336062_Public-Key_Cryptosystem_Based_on_Isogenies (дата обращения 06.12.2018)

15. Charles D. Cryptographic Hash Functions from Expander Graphs/ D. Charles, K. Lauter// Journal of Cryptology. – 2009. - № 22. – С. 93-113

16. Childs A. Constructing elliptic curve isogenies in quantum subexponential time/ A. M. Childs, D. Jao, V. Soukharev// J. Math. Cryptol. – 2014. - № 8(1). – С. 1-29

17. Tate J. Endomorphisms of abelian varieties over finite fields/ J. Tate// Invent. Math. – 1966. - №2. – С.134–144.

18. Moody D. Analogues of Velu's formulas for Isogenies on Alternate Models of Elliptic Curves/ D. Moody, D. Shumow// Mathematics of Computation. – 2011. - № 300.

19. Jao D. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies / D.Jao, L. De Feo// Post-quantum cryptography. 4th International Workshop, PQCrypto: сборник статей – Taiwan, 2011. - С. 19-34

20. Jao D. Isogeny-Based Quantum-Resistant Undeniable Signatures/ D.Jao, V.Soukharev// Post-quantum cryptography. 6th international workshop, PQCrypto: сборник статей. –Canada, 2014. - С.160-179

21. Srinath M. S. Isogeny-based Quantum-resistant Undeniable Blind Signature Scheme/ M.S Srinath, Venkatachalam Chandrasekaran// International Journal of Network Security. – 2018. - №20 (1). – С. 9-18

22. Costello C. Efficient algorithms for supersingular isogeny Diffie-Hellman/ C. Costello, P. Longa, M. Naehrig// Advances in Cryptology – CRYPTO 2016: 36th Annual International Cryptology: сборник статей. – Santa Barbara, USA, 2016.

23. SIDH Library [Электронный ресурс]// Библиотека SIDH. – режим доступа URL: https://www.microsoft.com/en-us/research/project/sidh-library/ (дата обращения 07.12.2018)

24. Courtois N. How to Achieve a McEliece-Based Digital Signature Scheme // Advances in Cryptology/ N.Courtois , M.Finiasz, N.Sendrier.// ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security: сборник статей. - Gold Coast, Australia, 2001. — С. 157–174

25. Canteaut A. Cryptanalysis of the Original McEliece Cryptosystem / A.Canteaut , N.Sendrier .// Advances in Cryptology — ASIACRYPT 1998: International Conference on the Theory and Applications of Cryptology and Information Security: сборник статей. - Beijing, China, 1998. — С.187–199.

26. Bernstein D. J. Attacking and Defending the McEliece Cryptosystem / D.J.Bernstein, T.Lange, C. Peters// Post-Quantum Cryptography: Second International Workshop, PQCrypto: сборник статей. - Cincinnati, USA, 2008. — С.31–46.

27. Shpilrain V. Combinatorial group theory and public key cryptography/ V. Shpilrain, G. Zapata// Applicable Algebra in Engineering Communication and Computing. – 2004. - № 17(3-4). – С.291–302.

28. Chen X. Provably Secure Integration Cryptosystem on Non-Commutative Group/ X. Chen, W. You// [Электронный ресурс] arXiv.org – e-print service. 2018. – Режим доступа URL: // https://arxiv.org/pdf/1806.03075.pdf (дата обращения 10.12.2018)

29. Ko K.H. Towards generating secure keys for braid cryptography/ K.H. Ko, J. Lee, T. Thomas// Designs Codes and Cryptography. – 2007. - №45 (3).- C. 317-333

30. Cha J.C An efficient implementation of braid groups/ J.C. Cha, K.H. Ko, S.J. Lee, J.W. Han, J.H. Cheon// ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security : сборник статей. - Gold Coast, Australia. - 2001. – C.144–156.

31. Hart D. A Practical Cryptanalysis of WalnutDSATM/ D. Hart, D. Kim, G. Micheli, G. Pascual-Perez, C. Petit, Y. Quek // [Электронный ресурс] eprint.iacr.org - e-print service. 2018. – режим доступа URL:// eprint.iacr.org/2017/1160 (дата обращения 09.12.2018)

32. Bernstein D. J. Post-Quantum Cryptography / D. J. Bernstein, J. Buchmann, E. Dahmen. – Berlin: Springer, 2009. - pp. 147–192.

33. Hoffstein, J. NTRU: a ring-based public key cryptosystem/ J. Hoffstein , J. Pipher , J. H. Silverman// Lecture Notes in Computer Science: сборник статей. – 1998. - C. 267–288.

34. Lyubashevsky V. On ideal lattices and learning with errors over rings/ V. Lyubashevsky, C. Peikert, O. Regev// Advances in Cryptology – EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques: сборник статей. - French Riviera. - 2010. - C.1-23

35. Hoffstein J. Practical signatures from the partial Fourier recovery problem/ J. Hoffstein, J. Pipher, J. M. Schanck, W. Whyte// Applied cryptography and network security. 12th international conference, ACNS: сборник статей. - Lausanne, Switzerland. - 2014. - C. 476–493

36. Alkim E. Post-quantum key exchange - a new hope/ E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe//[Электронный ресурс] eprint.iacr.org - e-print service. 2018. – режим доступа URL: // https://eprint.iacr.org/2015/1092 (дата обращения 10.12.2018)

37. Experimenting with Post-Quantum Cryptography [Электронный ресурс] // Блог компании Google. – Режим доступа URL:

https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html, дата обращения 05.12.2018)

38. CECPQ1 results [Электронный ресурс] // Блог Адама Лэнгли. – Режим доступа URL: https://www.imperialviolet.org/2016/11/28/cecpq1.html, дата обращения 05.12.2018)

39. Brassard G. Quantum Cryptanalysis of Hash and Claw-Free Functions/ G. Brassard, P. Høyer, A. Tapp// LATIN'98: Theoretical Informatics. Third Latin American Symposium Campinas: сборник статей. - Brazil. - 1998. - С.163–169.

40. Bhatia A.S. McEliece Cryptosystem Based On Extended Golay Code/ A.S.Bhatia, A.Kumar// [Электронный ресурс] arXiv.org – e-print service. 2018. – Режим доступа URL:// https://arxiv.org/pdf/1811.06246.pdf (дата обращения 10.12.2018)

41. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [Электронный ресурс]// The National Institute of Standards and Technology (NIST). – режим доступа URL: https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms (дата обращения 05.12.2018)

42. IBM Q Experience [Электронный ресурс] // Блог компании IBM. – Режим доступа URL: // https://quantumexperience.ng.bluemix.net/qx/editor (дата обращения 05.12.2018)