АНАЛИЗ ОСНОВНЫХ СУЩЕСТВУЮЩИХ ПОСТ-КВАНТОВЫХ ПОДХОДОВ И СХЕМ ЭЛЕКТРОННОЙ ПОДПИСИ[1]

Комарова А.В.[2], Коробейников А.Г.[3]

Цель статьи: *освещение последних тенденций развития пост-квантовой криптографии, в частности, схем электронной подписи, путем рассмотрения кандидатов, прошедших во второй тур конкурса стандартов Национального Института Стандартов и Технологий США (NIST).*

Метод: *анализ и синтез существующих пост-квантовых подходов, сравнительный анализ некоторых характеристик наиболее перспективных, по мнению авторов, схем электронной подписи.*

Полученный результат: *рассмотрены существующие пост-квантовые подходы и синтезированы наиболее перспективные из них. Проведено сравнение некоторых параметров схем электронной подписи, прошедших во второй тур конкурса пост-квантовых стандартов Национального Института Стандартов и Технологий США (NIST). Сделан вывод о том, что для построения схем электронной подписи наиболее перспективным подходом из всех предложенных является теория решеток, в частности схема FALCON. Данная схема обеспечивает наивысший уровень «компактности» по сумме длин открытого ключа и подписи среди всех представленных на конкурсе NIST пост-квантовых схем электронной подписи при сопоставимых уровнях безопасности и временных параметрах.*

Ключевые слова: *пост-квантовая криптография, квантовый компьютер, теория решеток, многомерные квадратичные системы, электронная подпись на хэш-функциях, теория алгебраического кодирования, изогении эллиптических кривых, теория кос, схема FALCON.*

DOI: *10.21681/2311-3456-2019-2-58-68*

1. Введение

В настоящее время в быстроразвивающемся технологическом мире появление квантового компьютера все больше становится реальностью [1]. Для некоторых областей знаний создание такого устройства позволит обрабатывать данные на порядок быстрее, чем это делают современные машины [2], что станет прорывом, но для современной криптографии - угрозой взлома всех существующих криптосистем.

Ведущими мировыми научными коллективами постоянно ведутся разработки по построению квантового вычислителя [3]. Некоторые учёные дают временную оценку в 20 лет для реализации полномасштабного квантового компьютера. Если вычислительные возможности нарушителя возрастут в десятки, сотни, тысячи раз, то это приведёт к резкой необходимости увеличения длины ключей до критического уровня, не пригодного для их успешной эксплуатации в реальных информационных системах. Также, необходимо отметить, что при появлении квантового противника с огромными вычислительными мощностями велика вероятность и тотального взлома существующих криптосистем путём полного перебора по всему пространству ключей [2].

Данную проблему можно решить путем использования примитивов пост-квантовой криптографии, сравнительно новой отрасли криптографии, призванной противостоять квантовым вычислениям.

Еще одним путем решения обозначенной выше проблемы, является использование квантовой криптографии. В отличие от асимметричной криптографии (и пост-квантовой, и классической), основанной на условно однонаправленных математических функциях, квантовая криптография основывается на принципах квантовой механики и квантовой теории информации, гарантирующих физическую однонаправленность. Однако существует ряд проблем, связанных со сложностью реализации и высокой стоимостью оборудования. При длине канала передачи данных более 100 км, скорость передачи значительно снижается (до нескольких битов в секунду) [4]. Данный факт пока не позволяет реализовать полноценный защищенный обмен критически важной информацией. В силу этого, авторам видится, что на данный момент пост-квантовая криптография является более реализуемой для использования в существующих системах.

С появлением реальных квантовых компьютеров переход на пост-квантовые протоколы может стать слишком резким, что повлечёт за собой большие финансовые потери. Поэтому рассматривать, анализировать и внедрять пост-квантовую криптографию в существующие системы нужно начинать в ближайшем будущем.

За последние пять лет количество публикуемых работ по данной тематике, как зарубежных, так и российских, значительно возросло [5-10]. Этот факт подчеркивает актуальность данной проблемы и вызывает интерес к дальнейшим исследованиям в этой области.

1 Работа выполнена при поддержке НИР Университета ИТМО №619296 «Разработка методов создания и внедрения киберфизических систем».

2 Комарова Антонина Владиславовна, аспирант, Университет ИТМО, Санкт-Петербург, Россия. E-mail: piter-ton@mail.ru

3 Коробейников Анатолий Григорьевич, доктор технических наук, профессор, институт земного магнетизма, ионосферы и распространения радиоволн имени Н. В. Пушкова РАН, Санкт-Петербург, Россия. E-mail: korobeynikov_a_g@mail.ru

Таблица 1.
Влияние квантового компьютера на существующие криптосистемы

Криптографический	Тип	Применение	Влияние полномасштабного квантового компьютера алгоритм
ГОСТ Р 34.12-2015, AES	Симметричный	Шифрование	Необходимы более длинные ключи
ГОСТ Р 34.11-2012, SHA-2, SHA-3	-	Хэш-функции	Необходимы более длинные выходные значения хэш-функции
RSA	Асимметричный	Электронная подпись, Генерация ключей	Становится небезопасным
DSA	Асимметричный	Электронная подпись, Обмен ключами	Становится небезопасным
ГОСТ Р 34.10-2012, ECDH, ECDSA	Асимметричный	Электронная подпись, Обмен ключами	Становится небезопасным

2. Постановка задачи

В 1994 году американский ученый П. Шор (P. W. Shor) предложил квантовый алгоритм, способный решать задачи факторизации и дискретного логарифмирования за полиномиальное время . Это означает, что криптографические механизмы, основанные на вышеперечисленных задачах, потеряют свою криптостойкость. К таким механизмам относятся и действующий стандарт Российской Федерации ГОСТ 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и действующий стандарт Соединенных Штатов Америки ECDSA, и многие другие протоколы.

Существует ещё один квантовый алгоритм - алгоритм Л. Гровера (L.Grover), сложность которого оценивается в , но он не дает столь большой выигрыш в скорости по сравнению с алгоритмом Шора и больше подходит для взлома симметричных криптосистем и хэш-функций. Как можно видеть, алгоритм Гровера квадратично повышает скорость вычислений по сравнению с классическими компьютерами.

В отчете Национального Института Стандартов и Технологий США (The National Institute of Standards and Technology, NIST) [11] (апрель 2016 года) отмечается, что большинство асимметричных криптографических примитивов, широко используемых сегодня в разных сферах общественной жизни, и которые базируются на задачах факторизации и дискретного логарифмирования в разных группах, будут скомпрометированы, что показано в Таблице 1.

Не смотря на то, что уже происходит переход от хэш-алгоритмов MD5 и SHA-1 к SHA-2 и SHA-3 [12], как видно из Таблицы 1, то появление квантового компьютера повлечёт за собой необходимость многократного увеличения длины ключей для симметричного шифрования, а для хэш-функций - многократного увеличения длины хэша. Такие длины становятся неприемлемыми для практического использования симметричных алгоритмов и существующих хэш-функций в будущем.

Считается, что 2048-битовые ключи RSA будут обеспечивать достаточный уровень безопасности до 2030 года, а 3072 битовые ключи будут безоговорочно безопасными в обозримом будущем [12], однако, согласно отчету NIST [11], в случае реализации полномасштабного квантового компьютера, и RSA и ECDSA станут небезопасными. Некоторые учёные дают временную оценку в 20 лет для реализации такого полномасштабного устройства.

Для решения поднятой выше проблемы, в 2016 году NIST объявил о старте открытого конкурса на создание новых пост-квантовых алгоритмов и стандартов.

В силу всего выше сказанного, очевидной становится необходимость дальнейшего развития пост-квантовой криптографии. Так как схемы электронной подписи полностью потеряют свою криптостойкость в случае появления квантового компьютера, в отличие от шифрования и обмена ключами, то именно для этих криптографических функций первостепенной необходимостью является поиск новых пост-квантовых аналогов.

Таким образом, в рамках проводимого исследования была поставлена задача по анализу и синтезу существующих пост-квантовых подходов, а также кандидатов второго тура конкурса стандартов NIST среди схем электронной подписи для выявления наиболее перспективной, по мнению авторов, схемы.

3. Существующие пост-квантовые подходы

Пост-квантовая криптография на данный момент включает в себя следующие основные подходы:

- теория решеток;
- многомерные квадратичные системы;
- электронные подписи на хэш-функциях;
- теория алгебраического кодирования;
- изогении эллиптических кривых;
- теория кос.

Рассмотрим кратко преимущества и недостатки каждого подхода, приведем примеры конкретных реализаций.

Криптография на решётках. Данный раздел криптографии начал активно развиваться с 1990-х годов

и включает в себя большое количество трудно вычислительных задач, некоторые из которых считаются NP-полными [13]. Большинство схем просты в понимании, обеспечивают хорошее быстродействие и обладают свойством распараллеливания вычислений. Помимо шифрования и подписи, на решётках могут быть построены другие интересные приложения (полностью гомоморфное шифрование [14], шифрование и подпись с использованием атрибута [15], обфускация кодов и другие). Некоторые системы из этого раздела обладают сложностью в наихудшем случае, а не в среднем, как большинство криптосистем. К минусам можно отнести отсутствие точного метода оценки сложности алгоритмов на решетках к существующим видам атак [16]. Наиболее известной схемой является криптосистема NTRU (Nth-degree TRUncated polynomial ring), предложенная в 1998 году. На базе криптосистемы NTRU можно реализовать алгоритмы шифрования и электронной подписи. Модифицированная версия данного алгоритма была взята за основу стандарта для финансовых организаций ANSI X9.98-2010 «Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry». В 2008 году криптосистема NTRU была включена в стандарт IEEE 1363.1 «Lattice-based public-key cryptography».

Криптография, основанная на многомерных квадратичных системах. Стойкость этого раздела криптографии основывается на сложности решения системы многомерных квадратичных многочленов над конечным полем [17]. Данная задача считается NP-полной. Системы из этого раздела обладают хорошей скоростью и небольшими требованиями к вычислительным ресурсам, однако, длины открытых ключей довольно большие. Наиболее известным примером является криптосистема HFE (Hidden Fields Equations), основанная на скрытых уравнениях поля и предложенная Ж. Патариным (J.Patarin) в 1996 году.

Криптография, основанная на хэш-функциях. В данный раздел входят электронные подписи, построенные с помощью хэш-функций, в силу чего обеспечивается их стойкость к квантовым вычислениям [18]. С помощью этого подхода можно выработать лишь ограниченное количество подписей на одном ключе. Также, к недостаткам системы относится тот факт, что подписанту необходимо записывать точное количество уже подписанных сообщений. Ошибка в этой записи приведёт к уязвимостям системы. Классическим примером является подпись Р. Меркла (R. Merkle), предложенная в 1979 году.

Криптография на кодах, исправляющих ошибки (теория алгебраического кодирования [19]). К плюсам такого рода систем можно отнести скорость вычислений. К минусам - слишком большую длину ключей [20]. На теории алгебраического кодирования базируются классические криптосистемы McEliece и Niederreiter. McEliece была предложенная Р. Мак-Элисом (R. Mac-Eliece) в 1978 году. Niederreiter была разработана Х. Нидеррайтером (H. Niederreiter) в 1986 году.

Изогении суперсингулярной эллиптической кривой. Наиболее популярный протокол SIDH (Supersingular isogeny Diffie–Hellman, SIDH) позволяет произвести обмен ключами по незащищенному каналу связи. Этот факт и является его отличительной особенностью, гарантирующей совершенную секретность [21]. С учётом сжатия SIDH имеет наименьшую длину ключа из всех постквантовых протоколов обмена ключами. Однако полноценной криптосистемы на изогениях пока реализовано не было.

Криптосистемы, основанные на группах кос. Основы теории кос были введены в 20-х годах 19 века немецким математиком Э. Артином (E. Artin). Криптографические примитивы, основанные на группах кос, могут решать большой спектр задач информационной безопасности (обеспечение целостности, подлинности, неотказуемости, конфиденциальности передаваемой информации, осуществление протоколов обмена ключами, шифрования и электронной подписи) [22]. Также они обладают свойством быстрой генерации ключей, но время шифрования или подписания документа оставляет желать лучшего. В качестве примера, можно привести схему электронной подписи WalnutDSA.

Обобщение вышеупомянутых подходов приведено в Таблице 2.

Как и в классических асимметричных криптографических алгоритмах и схемах электронной подписи, трудность взлома которых основывается на сложности вычисления какой-либо «трудной» односторонней математической задачи (функции), в пост-квантовой криптографии стойкость основывается также на сложности вычисления некоторой трудно решаемой задачи.

Вышеуказанные системы, а точнее, некоторые их частные задачи, считаются стойкими как к классическим компьютерам, там и к квантовым в силу того, что на сегодняшний момент не было предложено эффективных полиномиальных квантовых алгоритмов решения этих задач, то есть криптоаналитики пока не нашли способа модификации алгоритма Шора для этих систем.

Согласно обобщенному сравнительному анализу, результаты которого можно видеть в Таблице 2, по мнению авторов, наиболее интересным подходом является криптография на решетках. Она обладает большим количеством сфер применения, хорошо реализуется на устройствах с ограниченными вычислительными ресурсами и обладает доказанной криптостойкостью в наихудшем случае.

В дальнейшем, при рассмотрении схем электронной подписи, также будет видно, что при сопоставимом уровне криптостойкости, схемы на основе теории решеток являются наиболее интересными и «компактными».

4. Кандидаты на новый пост-квантовый стандарт

Как уже было сказано ранее, в 2016 году Национальный Институт Стандартов и Технологий США объявил о тарте конкурса на создание новых пост-квантовых алгоритмов и стандартов взамен старых [11]. Всего было представлено 82 заявки. Подача заявок на участие в первом туре конкурса закончилась 30 декабря 2017 года. Всего было допущено 69 алгоритмов, из них 49 алгоритмов шифрования с открытым ключом и 20 схем электронной подписи. Результаты первого тура

Таблица 2.
Сравнение пост-квантовых подходов

	Вид	Обоснование сложности	Скорость	Преимущества	Недостатки
Теория решеток	Шифрование ЭП Хэш-функции Обмен ключами Полностью гомоморфное шифрование Протоколы «забывчивой передачи» Протоколы с использованием атрибута Шифрование, основанное на идентификации	Нахождение «хорошего» базиса решетки Решение задач теории решеток в особых решетках	Хорошо реализуется на специальном ПО	Обоснование сложности в наихудшем случае Множество сфер применения	Повышенная длина ключей по сравнению с ЭК Отсутствие точного метода оценки сложности
Многомерные квадратичные системы Многомерные квадратичные системы	Шифрование ЭП Обмен ключами	Решение систем многомерных квадратичных уравнений	Хорошо реализуется на аппаратных средствах	Быстрота Малая длина ключей даже в сравнении с ЭК	Несостоятельность обоснования безопасности Большое количество систем было взломано Повышенная длина открытого ключа
ЭП на хэш-функциях	ЭП	Сопротивление коллизиям	Зависит от используемой хэш-функции	Сравнительная быстрота	Возможность реализации только протоколов ЭП Ограниченное количество подписей на одном ключе Безопасность зависит от выбираемой хэш-функции Большая длина подписи
Теория алгебраического кодирования	Шифрование ЭП Хэш-функции Обмен ключами	Декодирование полных линейных кодов	Хорошо реализуется на аппаратных средствах	Хорошая скорость вычислений	Слишком большая длина ключей Большие требования к памяти устройства Большое количество систем было взломано
Изогении эллиптических кривых	Обмен ключами	Задача нахождения изогенных отображений между двумя суперсингуляр-ными эллиптическими кривыми	Хорошо реализуется на специальном ПО	Совершенно прямая секретность Наименьшая длина ключа	Отсутствие полноценной криптосистемы
Теория кос	Шифрование ЭП Обмен ключами	Решение проблемы поиска сопряжений	Хорошо реализуется на аппаратных средствах	Решают большой спектр задач Быстрая генерация ключей	Медленные процессы генерации и проверки ЭП

были объявлены 30 января 2019 года. Во второй тур прошли 26 кандидатов [23]: 17 алгоритмов шифрования и распределения ключей и 9 схем электронной подписи.

Среди схем электронной подписи во второй тур прошли:

- Схемы на решетках:
  - o CRYSTALS-DILITHIUM;
  - o FALCON;
  - o qTESLA;
- Многомерные квадратичные системы:
  - o GeMSS;
  - o LUOV;
  - o MQDSS;
  - o Rainbow;
- Электронные подписи на хэш-функциях:
  - o Picnic;
  - o SPHINCS+.

В сжатые сроки, до 15 марта 2019 года разработчики этих систем должны были внести требующиеся корректировки и обновить заявки. Организаторами планируется, что срок рассмотрения претендентов во втором туре продлится приблизительно год-полтора, после чего будут объявлены победителя конкурса, либо, по необходимости, будет назначен третий тур.

Конкурс является полностью открытым. Организаторы призывают все криптографическое научное сообщество, включая уже выбывших кандидатов принять участие в рассмотрении оставшихся заявок, для более скрупулезного выявления недостатков.

Три основных критерия, по которым производилась оценка кандидатов, были следующие: безопасность, быстродействие и использование ресурсов памяти, характеристики алгоритмов и нюансы реализаций.

• Безопасность является важнейшим требованием. NIST планирует использовать новый пост-квантовый стандарт для широкого ряда задач. Оценка кандидатов будет происходить именно по их способности обеспечения безопасности в этих криптографических задачах. Схемы электронной подписи должны быть стойкими к атакам при адаптивно выбираемом шифртексте (adaptive chosen cipher text attack), атакам на основе известных сообщений, к экзистенциальной подделке и другим видам атак. [11]

NIST определяет 5 уровней стойкости:

- o 1 уровень – «вероятно, безопасные алгоритмы в обозримом будущем (если не окажется, что КК будут работать быстрее, чем ожидается)»;
- o 2, 3 уровни – «вероятно, безопасные алгоритмы в обозримом будущем»;
- o 4, 5 уровни – «вероятно, чрезмерные по стойкости алгоритмы»;

Также одним из требований для кандидатов было предоставление информации для обобщения об известных криптоаналитических атаках на предлагаемые схемы, и оценка сложности этих атак.

• Второе по значимости требование - требование к эффективности выполнения и использованию ресурсов памяти. Сюда относятся: размеры ключей, размеры подписи; время, затраченное на генерацию ключей и подписи; время, требуемое на проверку подписи; а также доля возможных ошибок при работе алгоритмов. Требования по размеру памяти относятся как к программному, так и к аппаратному обеспечению.

• Критерий «характеристики алгоритмов и нюансы реализаций» заключаются в каких-либо специфических возможностях каждого алгоритма, например, в хорошей способности эффективно работать на различных платформах, или в возможности распараллеливания вычислений для достижения большего быстродействия.

Рассмотрим кандидатов второго тура среди схем электронной подписи более подробно (Таблица 3). Параметры, по которым производится сравнительный анализ следующие: длина закрытого ключа, длина открытого ключа, длина подписи.

Таблица 3.

Схемы электронной подписи, прошедшие во второй тур конкурса пост-квантовых стандартов NIST

Алгоритм	Конкретная реализация	Пост-квант. подход	Закрытый ключ, байт	Открытый ключ, байт	Длина подписи, байт	Категория безопасности
CRYSTALS-Dilithium	Dilithium_medium	Теория решеток (Lattices)	2 800	1 184	2 044	1
	Dilithium_recommended		3 504	1 472	2 701	2
	Dilithium_very_high		3 856	1 760	3 366	3
Falcon	falcon1024		8 193	1 793	1 330	5
	falcon512		4 097	897	690	1
	falcon768		6 145	1 441	1 077	3
qTESLA	qTesla_128		2 112	4 128	3 104	1
	qTesla_192		8 256	8 224	6 176	3
	qTesla_256		8 256	8 224	6 176	5

GeMSS	GeMSS128	Многомерные квадратичные системы (Multivariate)	14 208	417 408	48	1
	GeMSS192		39 440	1 304 192	88	3
	GeMSS256		82 056	3 603 792	104	5
LUOV	luov-48-49-242		32	7 536	1 746	2
	luov-64-68-330		32	19 973	3 184	4
	luov-80-86-399		32	40 248	4 850	5
	luov-8-117-404		32	100 989	521	5
	luov-8-63-256		32	15 908	319	2
	luov-8-90-351		32	46 101	441	4
MQDSS	mqdss-48		32	62	32 882	2
	mqdss-64		48	88	67 800	4
Rainbow	Ia		100 209	152 097	64	1
	Ib		114 308	163 185	78	1
	Ic		143 385	192 241	104	1
	IIIb		409 463	564 535	112	3
	IIIc		537 781	720 793	156	3
	IVa		376 141	565 489	92	4
	Vc		1 274 317	1 723 681	204	5
	VIa		892 079	1 351 361	118	5
	VIb		1 016 868	1 456 225	147	5
Picnic	picnicl1fs	Подписи на основе хэш-функций (Hash)	49	33	34 004	1
	picnicl1ur		49	33	53 933	1
	picnicl3fs		73	49	76 744	3
	picnicl3ur		73	49	121 817	3
	picnicl5fs		97	65	132 828	5
	picnicl5ur		97	65	209 478	5
Sphincs+	sphincs-sha256-128f		64	32	16 976	1
	128s		64	32	8 080	1
	192f		96	48	35 664	3
	192s		96	48	17 064	3
	256f		128	64	49 216	5
	256s		128	64	29792	5

Различные криптографические схемы, помимо обеспечения должного уровня безопасности, могут оцениваться по другим разным параметрам, например, по быстродействию (то есть по скорости выполнения процедур, как на стороне отправителя, так и на стороне получателя), по требуемой памяти обрабатывающего устройства (как отправителя, так и получателя), по длинам закрытых ключей, которые необходимо хранить, и по некоторым другим параметрам.

Для схем подписи, по понятным причинам, определяющим параметром является длина подписи, а также длина открытого ключа подписывающего, поэтому при дальнейшем анализе будем особое внимание уделять следующему параметру: |pk| + |Sign|, где |pk| - длина открытого ключа, |Sign| - длина подписи.

Из основных классов пост-квантовой криптографии, наиболее перспективными являются схемы на основе решеток, многомерных квадратичных многочленов и схемы на основе хэш-функций. Каждая из схем имеет различные реализации в зависимости от обеспечиваемого уровня безопасности согласно требованиям конкурса.

Для схем электронной подписи определяющими параметрами являются длины ключей (особенно открытого ключа) и подписи. В меньшей степени – время генерации, подписания и проверки. Поэтому, предлагается «от-

Таблица 4.
Первый уровень безопасности

Алгоритм	Конкретная реализация	Подход	Закрытый ключ, байт	Открытый ключ, байт	Длина подписи, байт
CRYSTALS-Dilithium	Dilithium_ medium	Подписи на основе теории решеток (Lattices)	2 800	1 184	2 044
Falcon	falcon512		4 097	897	690
qTesla	qTesla_128		2 112	4 128	3 104

бросить» схемы GeMSS и Rainbow, так как длины ключей в этих схемах достигают нескольких сотен Кбайт. Также, предлагается исключить подписи, основанные на хэш-функциях – Picnic и Sphincs+ - в силу их ограниченности по количеству генерируемых подписей на одной паре ключей.

Для дальнейшей выборки рассмотрим параметры оставшихся схем (CRYSTALS-DILITHIUM, FALCON, qTESLA, LUOV, MQDSS) для разных уровней безопасности: первого уровня (Таблица 4), второго-третьего уровней (Таблица 5) и четвертого-пятого уровней (Таблица 6).

но слишком большую длину подписи, что совершенно неприемлемо для гибридных систем.

По параметру снова явное преимущество имеют схемы на решетках, в частности, схема Falcon768 (Рис. 2).

На четвертом – пятом уровнях безопасности многомерные квадратичные схемы luov-80-86-399, luov-8-117-404 и luov-8-90-351 обладают слишком большими длинами открытых ключей. Схема mqdss-64 – большой длиной подписи. Среди остальных схем наибольшее быстродействие обеспечивает qTesla_256, относящаяся к криптографии на решетках. По сумме длин открыто-

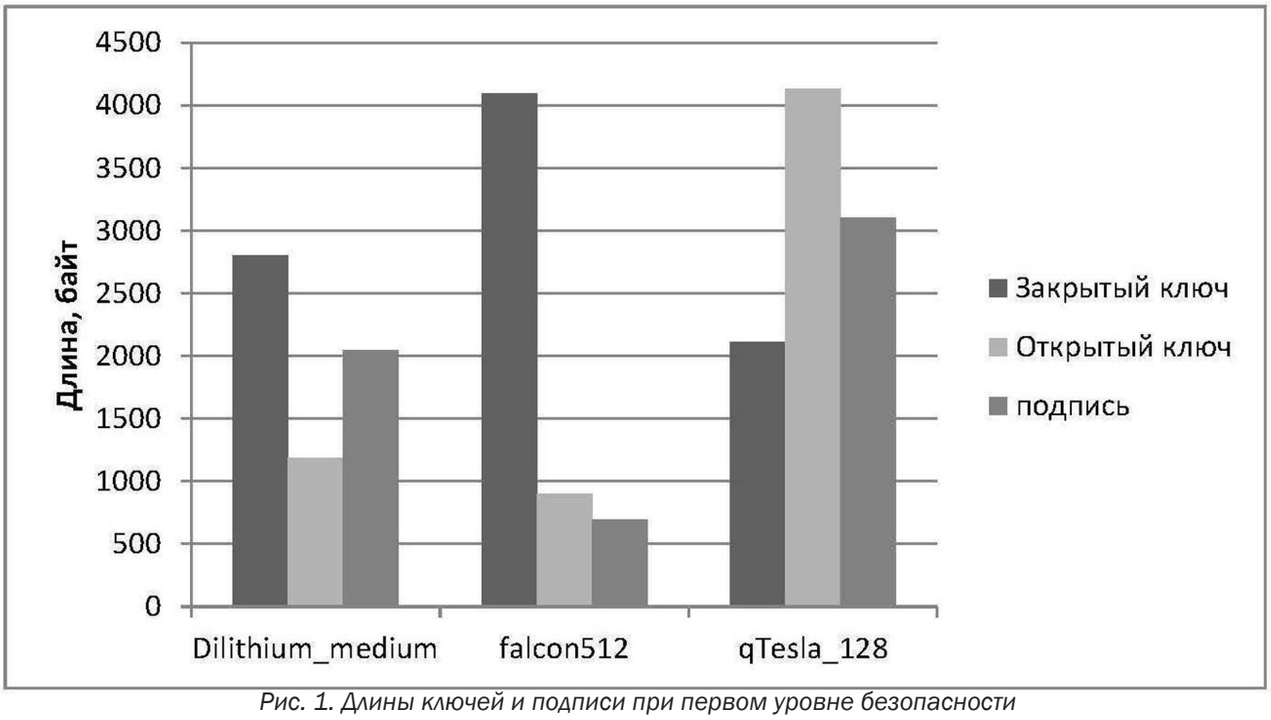

Рис. 1. Длины ключей и подписи при первом уровне безопасности

Первый уровень безопасности из оставшихся кандидатов обеспечивают только схемы на решетках. Многомерные квадратичные схемы обладают более высокими уровнями безопасности, но конкретных реализаций для первого уровня не имеют. По тактовым затратам наиболее интересным является схема qTesla_128. Что касается параметра , то явно выигрывает Falcon512 (Рис. 1).

Среди схем второго-третьего уровней наибольшим быстродействием обладает CRYSTALS-Dilithium. Наименьшим – MQDSS. MQDSS-48 имеет короткие ключи, го ключа и подписи снова побеждает схема falcon1024 (Рис. 3), также относящаяся к криптографии на решетках.

Проведенный сравнительный анализ пост-квантовых схем электронной подписи выявил наиболее перспективного кандидата – схему FALCON, которая при всех уровнях безопасности обеспечивала наименьшую длину ключей и подписи. При первом уровне значение |pk|+|Sign| равно 1587 байт, на третьем – 2518 байт, на пятом – 3123 байт. Эти цифры сопоставимы с аналогичными параметрами схемы RSA.

Таблица 5.
Второй-третий уровни безопасности

Алгоритм	Конкретная реализация	Пост-квантовый класс	Закрытый ключ, байт	Открытый ключ, байт	Длина подписи, байт
CRYSTALS-Dilithium	Dilithium_ recommended	Подписи на основе теории решеток	3 504	1 472	2 701
	Dilithium_ very_ high		3 856	1 760	3 366
Falcon	falcon768		6 145	1 441	1 077
qTesla	qTesla_192		8 256	8 224	6 176
LUOV	luov-48-49-242	Многомерные квадратичные системы	32	7 536	1 746
	luov-8-63-256		32	15 908	319
MQDSS	mqdss-48		32	62	32 882

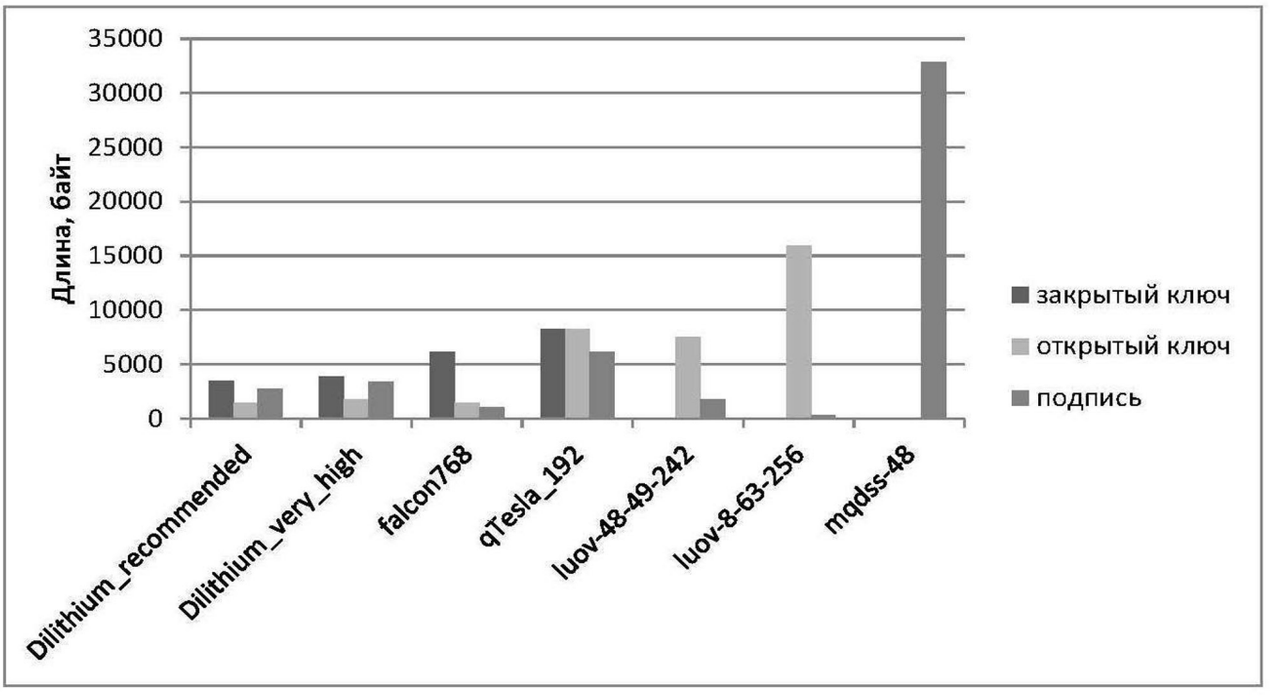

Рис. 2. Длины ключей и подписи при втором и третьем уровнях безопасности

Таблица 6.
Четвертый-пятый уровни безопасности

Алгоритм	Конкретная реализация	Пост-квантовый класс	Закрытый ключ, байт	Открытый ключ, байт	Длина подписи, байт
Falcon	falcon1024	Подписи на основе теории решеток	8 193	1 793	1 330
qTesla	qTesla_256		8 256	8 224	6 176
LUOV	luov-64-68-330	Многомерные квадратичные системы	32	19 973	3 184
	luov-80-86-399		32	40 248	4 850
	luov-8-117-404		32	100 989	521
	luov-8-90-351		32	46 101	441
MQDSS	mqdss-64		48	88	67 800

Таким образом, по мнению авторов, дальнейшие исследования и разработки с целью криптографической защиты от квантового компьютера, необходимо продолжать в области криптографии на решетках, ее теоретической и практической базах, преимуществах и недостатках, трудных задачах, лежащих в основе.

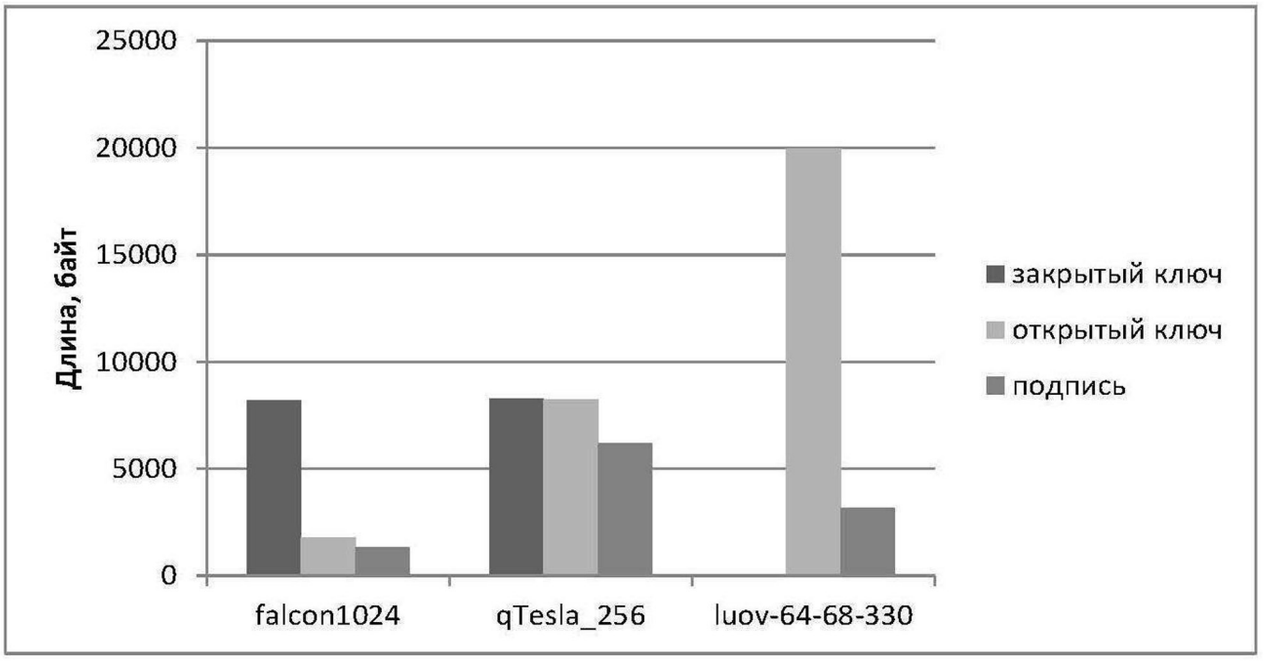

Рис. 3. Длины ключей и подписи при четвертом и пятом уровнях безопасности

5. Выводы

В данной работе был проведен анализ и синтез существующих пост-квантовых подходов, отмечены преимущества и недостатки данных подходов. Также были рассмотрены пост-квантовые схемы электронной подписи, прошедшие во второй тур конкурса NIST на создание новых пост-квантовых стандартов. Проведен сравнительный анализ данных кандидатов. Выявлено, что некоторые многомерные квадратичные схемы обладают неприемлемо большими размерами закрытого, и особенно, открытого ключей, а схемы с использованием хэш-функций обладают ограничениями по использованию, что позволяет убрать данные подходы из дальнейшего рассмотрения.

Показано, что по требованию компактности, то есть по сумме длин подписи и открытого ключа схема на основе теории решеток FALCON (во всех трех конкретных реализациях) имеет наименьшую длину из всех представленных выше алгоритмов при сопоставимом времени работы и уровне безопасности.

Полученные результаты могут быть использованы другими авторами для дальнейшего исследования передовых пост-квантовых технологий, а также студентами аспирантами технических специальностей в целях ознакомления и обучения.

В дальнейшем предполагается подробнее изучить схему электронной подписи FALCON: процедуры генерации ключей, генерации подписи, проверки подписи, рекомендуемые разработчиками параметры, положительные и отрицательные стороны.

Рецензент: *Исмагилов Валерий Сарварович, кандидат физико-математических наук, ученый секретарь Санкт-Петербургского филиала Федерального государственного бюджетного учреждения науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н.В. Пушкова РАН, Санкт-Петербург, Россия.*
E-mail: ivs@izmiran.spb.ru

Литература

1. Ллойд С. Программируя вселенную. Квантовый компьютер и будущее науки. – М. : Альпина нон-фикшн, 2014. - 256 с.
2. Душкин Р.В. Обзор текущего состояния квантовых технологий // Компьютерные исследования и моделирование. 2018. Т. 10. № 2. С. 165-179.
3. Соловьев В. М. Квантовые компьютеры и квантовые алгоритмы. Часть 1. Квантовые компьютеры // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2015. Т. 15, вып. 4. С. 462-477.
4. Филиппов М.А., Кротова Е.Л. Квантовая криптография. Преимущества и недостатки // Вестник УрФО. Безопасность в информационной сфере. 2017. № 4 (26). С. 25-27.
5. Bernstein DJ, Lange T. Post-quantum cryptography: dealing with the fallout of physics success, IACR, 2017. 20 p.
6. Кравченко В.О., Черкесова Л.В. Обзор постквантовых криптографических алгоритмов // Аллея науки. 2019. Т. 3. № 1 (28). С. 966-974.
7. Михайличенко Д.А., Егорова А.А. Основные направления развития постквантовой криптографии // Труды Ростовского государственного университета путей сообщения. 2016. № 2. С. 41-45.
8. Березовский Г.Ю., Гущина О.М. Исследование постквантовой криптографии // Прикладная математика и информатика: современные исследования в области естественных и технических наук: материалы III научно-практической

всероссийской конференции (школы-семинара) молодых ученых 24-25 апреля 2017 г. - Тольятти: Издатель Качалин Александр Васильевич, 2017. 2017. С. 71 - 73.
9. Рябый М.А. Обзор современных методов квантовой и пост-квантовой криптографии // Безпека інформації. 2014. Т. 20. № 3. С. 236-241.
10. Горбенко И. Пономарь В. Исследование возможности использования и преимуществ постквантовых алгоритмов в зависимости от условий применения // Восточно-Европейский журнал передовых технологий. 2017. Т. 2. № 9 (86). С. 21-32.
11. Chen L., Jordan S., Liu Y.K., Moody D., Peralta R., Perlner R., Smith-tone D. Report on Post-Quantum Cryptography, NISTIR 8105, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2016, 10pp. https://doi.org/10.6028/NIST.IR.8105.
12. Семенов Ю.А. Квантовая криптография [Электронный ресурс]. - Режим доступа: http://book.itep.ru/6/q_crypt.htm, свободный. - Заголовок с экрана (дата обращения: 28.04.2019).
13. Пискова А.В., Коробейников А.Г. Теория решеток в постквантовой криптографии // Сборник трудов V Всероссийского конгресса молодых ученых материалы конгресса : в 2 т. Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. 2016. С. 91-93.
14. Александрова Е.Б., Шенец Н.Н. Применение постквантовой и гомоморфной криптографии в задачах кибербезопасности // Неделя науки СПбПУ. Материалы научного форума с международным участием. Междисциплинарные секции и пленарные заседания институтов. 2015. С. 9-17.
15. Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan. Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption, IEEE transactions on information forensics and security, 2010, P. 190-199.
16. Кузнецов А.А., Горбенко Ю.И. Исследование криптографических атак на схемы электронной цифровой подписи в фактор-кольце усеченных полиномов // Захист інформації. 2016. Т. 18. № 4. С. 293-300.
17. Жаткин А.В. Применение систем квадратных уравнений многих переменных в асимметричной криптографии // Безопасность информационных технологий. 2013. Т. 20. № 1. С. 98-99.
18. Батенко К.Е., Прокудин А.Н. Пост-квантовый алгоритм электронно-цифровой подписи на основе дерева Меркла и ГОСТ РФ 34.11–12 «СТРИБОГ» // Молодой ученый. 2017. № 23 (157). С. 100-103.
19. Завгородний С.Д. Криптография на основе кодов исправления ошибок // Научные исследования и разработки студентов Сборник материалов VI Международной студенческой научно-практической конференции. Редколлегия: О.Н. Широков [и др.]. 2018. С. 96-98.
20. Кузнецов А.А., Киян А.С., Деменко Е.Е. Схемы электронной цифровой подписи на основе алгебраического кодирования // Актуальные научные исследования в современном мире. 2017. № 11-9 (31). С. 57-60.
21. Александрова Е.Б., Пендрикова О.Н. Применение графов изогений для проверки суперсингулярности эллиптических кривых // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 63-69.
22. Shpilrain V., Zapata G. Combinatorial group theory and public key cryptography, Appl. Algebra Eng. Commun. Comput, 17 (2006), no. 3-4, 291–302.
23. Alagic J., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Yi-Kai Liu., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8240, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2019, 27 pp. http://dx.doi.org/10.6028/NIST.IR.8240.

THE ANALYSIS OF EXISTING POST-QUANTUM APPROACHES AND ELECTRONIC SIGNATURE SCHEMES

Komarova A.V.[4], Korobeynikov A.G.[5]

The purpose *of the article is to highlight the latest trends in the post-quantum cryptography development, in particular, in electronic signature schemes. The goal is achieved by considering the second round candidates of the National Institute of Standards and Technology (NIST) competition.*

Method: *analysis and synthesis of existing post-quantum approaches, comparative analysis of the most promising electronic signature schemes, according to the authors point of view, and its characteristics.*

The result: *the existing post-quantum approaches are considered and the most promising of them are synthesized. The comparison of some second round electronic signature scheme parameters is held. It is concluded that for the construction of electronic signature schemes the most promising approach of all proposed is the lattice theory, in particular the FALCON scheme. This scheme provides the highest level of «compactness» in the sum of the public key and signature lengths among all the post-quantum electronic signature schemes presented at the NIST competition with comparable levels of security and time parameters.*

4 Antonina Komarova, postgraduate student, St. Petersburg National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, piter-ton@mail.ru

5 Anatoly Korobeynikov, Dr.Sc., Professor, Pushkov institute of terrestrial magnetism, ionosphere and radio wave propagation of the Russian Academy of Sciences St.-Petersburg Filial, St. Petersburg, korobeynikov_a_g@mail.ru

Keywords: *post-quantum cryptography, quantum computer, lattice theory, multivariate quadratic equations, hash-based signatures, code-based signatures, isogenies of elliptic curves, braid theory.*

Reference

1. Lloid S. Programmiruia vselennuiu Kvantovyi kompiuter i budushchee nauki. – M.: Alpina non-fikshn, 2014. - 256 p.
2. Dushkin R. V. Obzor tekushchego sostoianiia kvantovykh tekhnologii // Kompiuternye issledovaniia i modelirovanie [Computer research and modeling]. 2018. V. 10. № 2. P. 165-179.
3. Solovev V. M. Kvantovye kompiutery i kvantovye algoritmy. Chast 1. Kvantovye kompiutery // Izv. Sarat un-ta Nov. ser. Ser. Matematika Mekhanika Informatika. [News Sarat. Un. New ser. Ser. Mathematics. Mechanics. Informatics]. 2015. V. 15. № 4. P. 462-477.
4. Filippov M.A., Krotova E.L. Kvantovaya kriptografiya. Preimushchestva i nedostatki // Vestnik UrFO. Bezopasnost' v informacionnoj sfere [Herald UrFO. Information security]. 2017. № 4 (26). P. 25-27.
5. Bernstein DJ, Lange T. Post-quantum cryptography: dealing with the fallout of physics success, IACR, 2017. 20 p.
6. Kravchenko V.O., Cherkesova L.V. Obzor postkvantovyh kriptograficheskih algoritmov // Alleya nauki [Alley of science]. 2019. V. 3. № 1 (28). P. 966-974.
7. Mihajlichenko D.A., Egorova A.A. Osnovnye napravleniya razvitiya postkvantovoj kriptografii // Trudy Rostovskogo gosudarstvennogo universiteta putej soobshcheniya [Proceedings of Rostov state University of railway engineering]. 2016. № 2. P. 41-45.
8. Berezovskij G.Yu., Gushchina O.M. Issledovanie postkvantovoj kriptografii // Prikladnaya matematika i informatika: sovremennye issledovaniya v oblasti estestvennyh i tekhnicheskih nauk: materialy III nauchno-prakticheskoj vserossijskoj konferencii (shkoly-seminara) molodyh uchenyh 24-25 aprelya 2017 g. [Applied mathematics and Informatics: modern research in the field of natural and technical Sciences: materials of the III scientific-practical all-Russian conference (school-seminar) of young scientists 24-25 April 2017] - Tol'yatti: Izdatel' Kachalin Aleksandr Vasil'evich, 2017. 2017. P. 71 - 73.
9. Ryabyj M.A. Obzor sovremennyh metodov kvantovoj i post-kvantovoj kriptografii // Bezpeka informacii [Information security]. 2014. V. 20. № 3. P. 236-241.
10. Gorbenko I. Ponomar' V. Issledovanie vozmozhnosti ispol'zovaniya i preimushchestv postkvantovyh algoritmov v zavisimosti ot uslovij primeneniya // Vostochno-Evropejskij zhurnal peredovyh tekhnologij. 2017. V. 2. № 9 (86). P. 21-32.
11. Chen L., Jordan S., Liu Y.K., Moody D., Peralta R., Perlner R., Smith-tone D. Report on Post-Quantum Cryptography, NISTIR 8105, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2016, 10pp. https://doi.org/10.6028/NIST.IR.8105.
12. Semenov Yu.A. Kvantovaya kriptografiya [electronic resource]. – Mode of access: http://book.itep.ru/6/q_crypt.htm, free. - The title screen (accessed date: 28.04.2019).
13. Piskova A.V., Korobejnikov A.G. Teoriya reshetok v postkvantovoj kriptografii // Sbornik trudov V Vserossijskogo kongressa molodyh uchenyh materialy kongressa: v 2 t. [Proceedings of the V all-Russian Congress of young scientists materials of the Congress: in 2 v]. Sankt-Peterburgskij nacional'nyj issledovatel'skij universitet informacionnyh tekhnologij, mekhaniki i optiki. 2016. P. 91-93.
14. Aleksandrova E.B., Shenec N.N. Primenenie postkvantovoj i gomomorfnoj kriptografii v zadachah kiberbezopasnosti // Nedelya nauki SPbPU. Materialy nauchnogo foruma s mezhdunarodnym uchastiem. Mezhdisciplinarnye sekcii i plenarnye zasedaniya institutov [The week of science of SPbSPU. Materials of the scientific forum with international participation. Interdisciplinary sections and plenary sessions of the institutes.]. 2015. P. 9-17.
15. Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan. Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption, IEEE transactions on information forensics and security, 2010, P. 190-199.
16. Kuznecov A.A., Gorbenko Yu.I. Issledovanie kriptograficheskih atak na skhemy elektronnoj cifrovoj podpisi v faktor-kol'ce usechennyh polinomov // Zahist informacii [Information protection]. 2016. V. 18. № 4. P. 293-300.
17. Zhatkin A.V. Primenenie sistem kvadratnyh uravnenij mnogih peremennyh v asimmetrichnoj kriptografii // Bezopasnost' informacionnyh tekhnologi [Information technology security]. 2013. V. 20. № 1. P. 98-99.
18. Batenko K.E., Prokudin A.N. Post-kvantovyj algoritm elektronno-cifrovoj podpisi na osnove dereva Merkla i GOST RF 34.11–12 «STRIBOG» // Molodoj uchenyj [Young scientist]. 2017. № 23 (157). P. 100-103.
19. Zavgorodnij S.D. Kriptografiya na osnove kodov ispravleniya oshibok // Nauchnye issledovaniya i razrabotki studentov Sbornik materialov VI Mezhdunarodnoj studencheskoj nauchno-prakticheskoj konferencii [Research and development of students Collection of materials VI International student scientific-practical conference]. Redkollegiya: O.N. Shirokov [i dr.]. 2018. P. 96-98.
20. Kuznecov A.A., Kiyan A.S., Demenko E.E. Ckhemy elektronnoj cifrovoj podpisi na osnove algebraicheskogo kodirovaniya // Aktual'nye nauchnye issledovaniya v sovremennom mire [Actual research in the modern world]. 2017. № 11-9 (31). P. 57-60.
21. Aleksandrova E.B., Pendrikova O.N. Primenenie grafov izogenij dlya proverki supersingulyarnosti ellipticheskih krivyh // Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy [Problems of information security. Computer systems]. 2018. № 3. P. 63-69.
22. Shpilrain V., Zapata G. Combinatorial group theory and public key cryptography, Appl. Algebra Eng. Commun. Comput, 17 (2006), no. 3-4, 291–302.
23. Alagic J., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Yi-Kai Liu., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8240, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2019, 27 pp. http://dx.doi.org/10.6028/NIST.IR.8240.