УДК 004.056.55

М.С. ЛУЦЕНКО, А.С. КИЯН, Т.Ю. КУЗНЕЦОВА, А.А. КУЗНЕЦОВ, д-р техн. наук

АНАЛИЗ И СРАВНИТЕЛЬНЫЕ ИССЛЕДОВАНИЯ КОДОВЫХ СХЕМ ИНКАПСУЛЯЦИИ КЛЮЧЕЙ, ПРЕДСТАВЛЕННЫХ НА КОНКУРС NIST PQC

Введение

В конце 2016 года Национальным институтом стандартов и технологий (National Institute of Standards and Technology, NIST) США объявлен конкурс постквантовой криптографии (Post-Quantum Cryptography, PQC) [1], в частности алгоритмов электронной цифровой подписи, направленного шифрования и схем инкапсуляции ключей. Среди перспективных направлений исследований особое место занимают кодовые криптосистемы (Code-Based Public-Key Cryptosystems), позволяющие эффективно реализовывать все три группы алгоритмов.

Цель работы – анализ и сравнительные исследования кодовых схем инкапсуляции ключей, представленных на конкурс NIST PQC. Рассмотрены все 12 алгоритмов инкапсуляции ключей, представленных на конкурс: BIKE [2], Classic McElice [3], DAGS [4], Edon-K [5], LAKE [6], LedaKem [7], Lepton [8], NTS-KEM [9], Ouroboros-R [10], QC –MDPC KEM [11], RLCE-KEM [12], RQC [13]. Для первичной оценки криптографической стойкости проведен анализ соответствия алгоритмов инкапсуляции ключей современным требованиям к криптосистемам с открытым ключом, а именно – обеспечению свойств неразличимости [14, 15]. Свойство неразличимости шифротекста определяет криптостойкость алгоритма к атаке на основе подобранного открытого текста. Обеспечение такого свойства неразличимости на основе открытого теста (IND-CPA) считается основным требованием для большинства доказуемо защищенных криптосистем с открытым ключом [14, 15], хотя некоторые схемы также обеспечивают криптографическую стойкость против атак на основе подобранного шифротекста и адаптивных атак на основе подобранного шифротекста. Такие свойства неразличимости обозначаются, как IND-CCA1 и IND-CCA2 соответственно [14, 15].

Для оценки уровня криптостойкости в классической и постквантовой криптографии для каждого алгоритма и его вариации используются обеспечиваемый уровень криптостойкости и соответствующие основные параметры преобразований. При описании требований к алгоритмам, подаваемым на конкурс, были определены уровни криптографической стойкости:

- Уровень 1: любая атака, которая взламывает IND-CCA-стойкий алгоритм, должна требовать вычислительных ресурсов, сравнимых или превышающих требуемые для поиска ключа на блочном шифре с 128-битным ключом (например, AES-128);
- Уровень 3: если существует атака на IND-CCA-криптостойкий алгоритм, то для проведения такой атаки должны обеспечиваться вычислительные ресурсы, соизмеримые или превышающие требуемые для поиска ключа на блочном шифре с 192-битным ключом (например, AES-192);
- Уровень 5: любая атака, которая нарушает криптостойкость IND-CCA-стойкой схемы, должна требовать вычислительных ресурсов, сравнимых или превышающих требуемые для поиска ключа на блочном шифре с 256-битным ключом (AES-256).

В работе также проведен сравнительный анализ показателей быстродействия неоптимизированных версий алгоритмов. Проводимый анализ носит первичный характер, все результаты оценки показателей стойкости и быстродействия основаны на экспериментах, проведенных авторами (разработчиками) алгоритмов.

Схемы инкапсуляции ключей: краткая характеристика

BIKE (BIt Flipping Key Encapsulation) – схема инкапсуляции ключей, представленная группой ученых – Николя Арагон, Пауло Баррето, Слим Беттайб, Лойк Биду, Оливье Блази, Жан-Кристоф Деневиль, Филлип Габорит, Шей Герон, Тим Ганейсу, Карлос Агилар Мелхор,

Рафаэль Мисоцки, Эдоардо Персикетти, Николя Сенриер, Жан-Пьер Тиллих, Жиль Земор – из университетов стран Франции, США, Израиля, Германии [2]. Квазициклические коды с проверкой на четность (QC-MDPC) с умеренной плотностью. Могут быть декодированы с использованием техники бит флиппинг. Алгоритм обладает IND-CPA криптостойкостью, из-за применения техники бит флиппинга ожидается и обеспечение IND-CCA стойкости. Авторами представлены три модификации алгоритма: BIKE-1, BIKE-2 и BIKE-3. Схема BIKE-1 основана на вариации алгоритма Мак-Элиса. В BIKE-1 обеспечивается ускоренная генерация ключей. Открытый ключ имеет удвоенную длину, по сравнению с BIKE-2. В основе алгоритма BIKE-2 лежит криптосистема Нидеррайтера с проверочной матрицей на четность. Вариация BIKE-3 по основным преобразованиям напоминает BIKE-1, но обладает значительно большим, по мнению авторов, запасом криптостойкости. Для каждой из вариации приведены входные параметры в зависимости от обеспечиваемого уровня криптостойкости (обеспечиваются 1, 3 и 5 уровни).

Classic McElice – схема предложенная, группой исследователей, в которую входят: Даниэль Дж. Бернстайн, Тун Чжоу, Таня Ланге, Инго фон Маурич, Рафаэль Мисоцки, Рубен Нидерхаген, Эдоардо Персикетти, Кристиан Петерс, Питер Швабе, Николя Сенриер, Якуб Сезер; из стран США, Япония, Нидерланды, Германия, Франция [3]. Вариация алгоритма Мак-Элиса, основанная на двоичных кодах Гоппы. Данный алгоритм инкапсуляции ключей разработан для обеспечения безопасности IND-CCA2 на очень высоком уровне криптостойкости. Авторы предполагают, что алгоритм может найти эффективное применение даже в системах с ограниченными вычислительными возможностями и ресурсами и при этом сохранить эффективную криптостойкость.

DAGS (Key Encapsulation from DyAdic GS Codes) – исследователи из университетов Нидерландов, США, Сенегала, Франции, Бразилии, предоставили на конкурс алгоритм инкапсуляции ключей. В группу разработчиков входят: Густаво Банегас, Паоло С. Л. М. Барретo, Брайс Одилон Бойддже, Пьер-Луис Кайрел, Гилберт Ндоллане Диона, Крис Гай, Шейх Тикумба Гуи, Ричард Хаусслер, Жан-Бело-Кламти, Усмане Ндиайе, Дюк Три Нгуен [4]. Алгоритм DAGS использует квазидвоичный (QD) подход с использованием обобщенных кодов Сривастава. Авторы утверждают, что это первый алгоритм, основанный на структурированных алгебраических кодах, обеспечивающих не только IND-CPA криптостойкость, но и IND-CCA. В целом, предложенная схема предлагает большую гибкость в обмене ключами. Предположительно алгоритм может найти применение в приложениях для Интернета.

Edon-K – схема инкапсуляции, представленная норвежскими учеными Данилой Глигороски, Кристианом Гьёстином [5]. Этот алгоритм основан на схеме Мак-Элиса, но использует другое семейство кодов. Эти коды определены над другим полем и не основываются на метрике Хэмминга. Такой подход позволяет значительно сокращать длину открытых ключей, по сравнению со схемой Мак-Элиса. Код, используемый в Edon-K, является суперкодом с ранговой проверкой на четность (LRPC) очень малого ранга (1 или 2). Соответствующая матрица проверки на четность для суперкода такого низкого ранга может быть легко получена для открытого ключа. Алгоритм Edon-K обеспечивает уровни криптостойкости 1 и 3. Edon-K предназначен для обеспечения безопасности CCA2 без необходимости дополнительного (потенциально дорогостоящего) преобразования CPA-CCA.

LAKE (Low rAnk parity check codes Key Exchange) – еще один алгоритм, представленный группой ученых из Франции. Авторами алгоритма выступили Николя Арагон, Оливье Блази, Жан-Кристоф Деневиль, Филипп Габорит, Адриен Хаутвиль, Оливье Руатта, Жан-Пьер Тиллих, Жиль Земор [6]. Алгоритм основан на кодах с проверкой на четность Ideal-LRPC и механизме инкапсуляции ключей IND-CPA (KEM). Схема имеет некоторую вероятность ошибки при деинкапсуляции, которая, по мнению авторов, может быть легко устранена. Существует три вариации схемы для обеспечения трех уровней криптостойкости 1, 3 и 5. Предложенная схема очень эффективна, как с точки зрения выбранных размеров основных параметров (ключей и шифротекста), так и вычислительной сложности.

LedaKem (Low dEnsity coDe-bAsed key encapsulation mechanism) – ученые Марко Балди, Алессандро Баренги, Франко Чиаралесе, Херардо Пелоси, Паоло Сантини из Италии представили алгоритм инкапсуляции ключей [7]. Схема основывается на криптосистеме Нидеррайтера с линейной коррекцией ошибок. LEDAkem использует преимущества использования квазициклических кодов четности с низкой плотностью (QC-LDPC), обеспечивающих высокие скорости декодирования и малые длины ключей. Следует отметить крайне малую длину получаемого шифротекста – 64 байта, даже при уровне криптостойкости 5. Схема обладает IND-CCA криптостойкостью. Представленные вариации алгоритма с различными входными параметрами обеспечивают необходимую криптостойкость для уровней 1, 3, 5. В свою очередь, для каждой вариации определены по три подварианта с разным количеством циркулянтных блоков (n_0).

Lepton (LEarning PariTy with Noise) – китайский алгоритм инкапсуляции, представленный авторами Ю Ю, Цзян Чжан [8]. Алгоритм Lepton основан на определении четности с помехами (Learning Parity with Noise). Авторы представили две версии алгоритма. В данной схеме присутствует вероятность ошибки, которая колеблется для разных вариаций алгоритма от 2^{-87} до 2^{-148}. Первый Lepton.CPA направлен на достижение CPA-безопасности и основан на Ring-CLPN (Compact Learning Parity with Noise). Второй вариант Lepton.CCA представляет собой схему KEM для достижения CCA-безопасности, которая получается путем применения преобразования Фудзисаки – Окамото над Lepton.CPA.

NTS-KEM – исследователи из Великобритании, подали на конкурс алгоритм инкапсуляции. Авторы – Мартин Альбрехт, Карлос Сид, Кеннет Г. Патерсон, Цзэн Юнг Тхай, Мартин Томлинсон [9]. NTS-KEM можно рассматривать как вариант схемы шифрования с открытым ключом Мак-Элиса – двоичные линейные коды Гоппы используются в криптосистеме Нидеррайтера. NTS-KEM обеспечивает безопасность IND-CCA (как KEM) в модели случайного предсказателя, используя преобразование, похожее на преобразования Фудзисаки-Окамото или Дента. Авторы представили три версии алгоритма для обеспечения трех уровней криптостойкости.

Ouroboros-R – алгоритм, представленный исследователями – Карлос Агилар Мелхор, Жан-Кристоф Деневиль, Николя Арагон, Филипп Габорит, Слим Беттейб, Адриен Хаутвиль, Лойк Биду, Жиль Земо; Франция [10]. Используемый квазициклический код позволяет ускорить процесс декодирования при увеличении длины шифротекста. Алгоритм имеет некоторые схожие черты с NTRU-подобными схемами. Ouroboros также имеет вероятность отказа (как и другие протоколы NTRU), в связи с используемым алгоритмом декодирования. Ouroboros-R обладает криптостойкостью IND-CPA в соответствии с предположениями 2-QCRSD и 3-QCRSD.

QC–MDPC KEM – алгоритм разработали Ацуши Ямада, Эдвард Итон, Кассем Калач, Филип Лафранс, Алекс Родитель; Канада [11]. Алгоритм основан на криптосистеме Мак-Элиса. В QC-MDPC KEM используется квазициклическая проверка на четность с умеренной плотностью. Авторами указано, что алгоритм может быть недостаточно быстрым, по сравнению с другими алгоритмами. Алгоритм обеспечивает IND-CPA криптостойкость.

RLCE-KEM – схема инкапсуляции ключей исследователя Юн Ван из США [12]. В алгоритме используется схема шифрования Мак-Элиса на основе случайного линейного кода (RLCE). Преимущество схемы RLCE заключается в том, что ее криптостойкость не зависит от какой-либо конкретной структуры базовых линейных кодов. Считается, что безопасность RLCE зависит от NP-сложности декодирования случайных линейных кодов. Автором представлено несколько вариаций алгоритма, которые обеспечивают три уровня криптостойкости.

RQC (Rank Quasi-Cyclic) – алгоритм сформирован группой французских ученых, в состав которой входят: Карлос Агилар Мелхор, Николя Арагон, Слим Беттейб, Лойк Биду, Оливье Блази, Жан-Кристоф Деневиль, Филипп Габорит, Жиль Земор [13]. Схема RQC основана на квазциклическом коде. Используемый подход для инкапсуляции ключей позволяет

гарантировать IND-CCA2 криптостойкость и обеспечивает высокие показатели эффективности. Предлагаются различные значения параметров для уровней безопасности 1, 3 и 5. Авторы указывают, что алгоритм имеет нулевую вероятность отказа декодирования.

В работе проанализированы основные параметры преобразования для всех приведенных выше алгоритмов на основе характеристик, указанных авторами. В табл. 1 приведены значения основных параметров для различных версий алгоритмов и их вариации, в соответствии с обеспечиваемым уровнем криптостойкости. Для алгоритма BIKE длины личного и открытого ключей шифротекста авторы привели в битах. Для наглядности эти параметры нормированы в байты.

Таблица 1

Характеристика основных криптографических параметров

№	Название	Версия	Уровень безопасности	Личный ключ, байт	Открытый ключ, байт	Шифротекст, байт
1	BIKE	BIKE-1	1	266,25	2540,75	2540,75
			3	287	5473,25	5473,25
			5	548	8187,25	8187,25
		BIKE-2	1	266,25	1270,375	1270,375
			3	412	2736,625	2736,625
			5	548	4093,625	4093,625
		BIKE-3	1	251,25	2756,75	2756,75
			3	396	5420,75	5420,75
			5	565,25	9032,75	9032,75
2	Classic McElice	mceliece8192128	1	14080	1357824	240
		mceliece6960119	3	13908	1047319	226
3	DAGS	DAGS_1	1	432640	6760	552
		DAGS_3	3	1284096	8448	944
		DAGS_5	5	2230272	11616	1616
4	Edon-K	EDON-K128 ref	1	32	2576	2336
		EDON-K192 ref	3	32	2192	2736
5	LAKE	LAKE I	1	-	3149	-
		LAKE II	3	-	4717	-
		LAKE III	5	-	6313	-
6	LedaKem		1, $n_0 = 2$	668	3480	32
			1, $n_0 = 3$	844	4688	32
			1, $n_0 = 4$	1036	6408	32
			2-3, $n_0 = 2$	972	7200	48
			2-3, $n_0 = 3$	1196	10384	48
			2-3, $n_0 = 4$	1364	13152	48
			4-5, $n_0 = 2$	1244	12384	64
			4-5, $n_0 = 3$	1548	18016	64
			4-5, $n_0 = 4$	1772	22704	64
7	Lepton. CPA	Light I	1	1045	32	1585
		Light II	1	1045	40	1966
		Moderate I	1	2052	38	2465
		Moderate II	1	2052	48	2765
		Moderate III	3	2052	56	2973
		Moderate IV	5	2052	74	3989
		Paranoid I	5	4128	70	5303
		Paranoid II	5	4128	80	5557
	Lepton.	Light I	1	1045	1077	1617

№	Название	Версия	Уровень безопас-ности	Личный ключ, байт	Открытый ключ, байт	Шифро-текст, байт
	CCA	Light II	1	1045	1085	1998
		Moderate I	1	2052	2090	2497
		Moderate II	1	2052	2100	2751
		Moderate III	3	2052	2018	3005
		Moderate IV	5	2052	2126	4021
		Paranoid I	5	4128	4198	5335
		Paranoid II	5	4128	4208	5589
8	NTS-KEM	NTS-KEM(12,64)	1	9216	319488	128
		NTS-KEM(13,80)	3	17524	929760	162
		NTS-KEM(13,136)	5	19890	1419704	253
9	Ouroboros-R	Ouroboros-R I	1	1180	1180	1180
		Ouroboros-R II	3	1490	1490	1490
		Ouroboros-R III	5	2128	2128	2128
10	QC –MDPC KEM	QC –MDPC KEM 58	58	-	4801	-
		QC –MDPC KEM 86	86	-	9857	-
		QC –MDPC KEM 154	154	-	32771	-
11	RLCE-KEM	ID = 0	1	310116	188001	988
		ID = 1	1	179946	118441	785
		ID = 2	3	747393	450761	1545
		ID = 3	3	440008	287371	138
		ID = 4	5	1773271	1232001	2640
		ID = 5	5	1049176	742089	2023
		ID = 6		1059	626	57
12	RQC(Rank Quasi-Cyclic)	RQC-I	1	1491	1491	1055
		RQC-II	3	2741	2741	2805
		RQC-III	5	3510	3510	3574

Так как значения параметров разнятся на несколько порядков, для наглядного представления на рис. 1 – 3 данные длины личных и открытых ключей, а также длины соответствующих шифротекстов представлены в логарифмическом масштабе. Суть использования такого масштабирования заключается в преобразовании длин данных следующим образом: $x = \log_{10} X$, где X – параметр, такой как длина открытого или личного ключа, длина шифротекста, который подлежит масштабированию; x – результат вычисления десятичного логарифма над масштабируемым значением.

Данные на гистограммах приведены для всех вариаций алгоритмов и отсортированы по уменьшению длины. Следует отметить, что в зависимости от предполагаемой сферы применения алгоритма при одном и том же обеспечиваемом уровне криптостойкости будут предпочтительны разные длины ключей. Например, для использования схемы инкапсуляции ключей в системах с ограниченными ресурсами предпочтительнее использовать алгоритмы с более короткими длинами параметров.

Согласно данным, приведенным на рис. 1, можно заключить, что наименьшей длиной личного ключа обладает схема Edon-K, для обеих вариаций – 32 байта. Более длинные ключи имеет схема BIKE, причем закономерно, что вариация BIKE-3, обеспечивающая уровень криптостойкости 5, имеет больший личный ключ, в отличие от BIKE-1 и BIKE-2. Далее следуют примерно сравнимые по длине личных ключей вариации алгоритмов LedaKem, Lepton.CPA и Lepton.CCA, Ouroboros-R. Наибольшие личные ключи у алгоритмов DAGS-5 и RLCE-KEM – 2230272 и 1049176 байт соответственно.

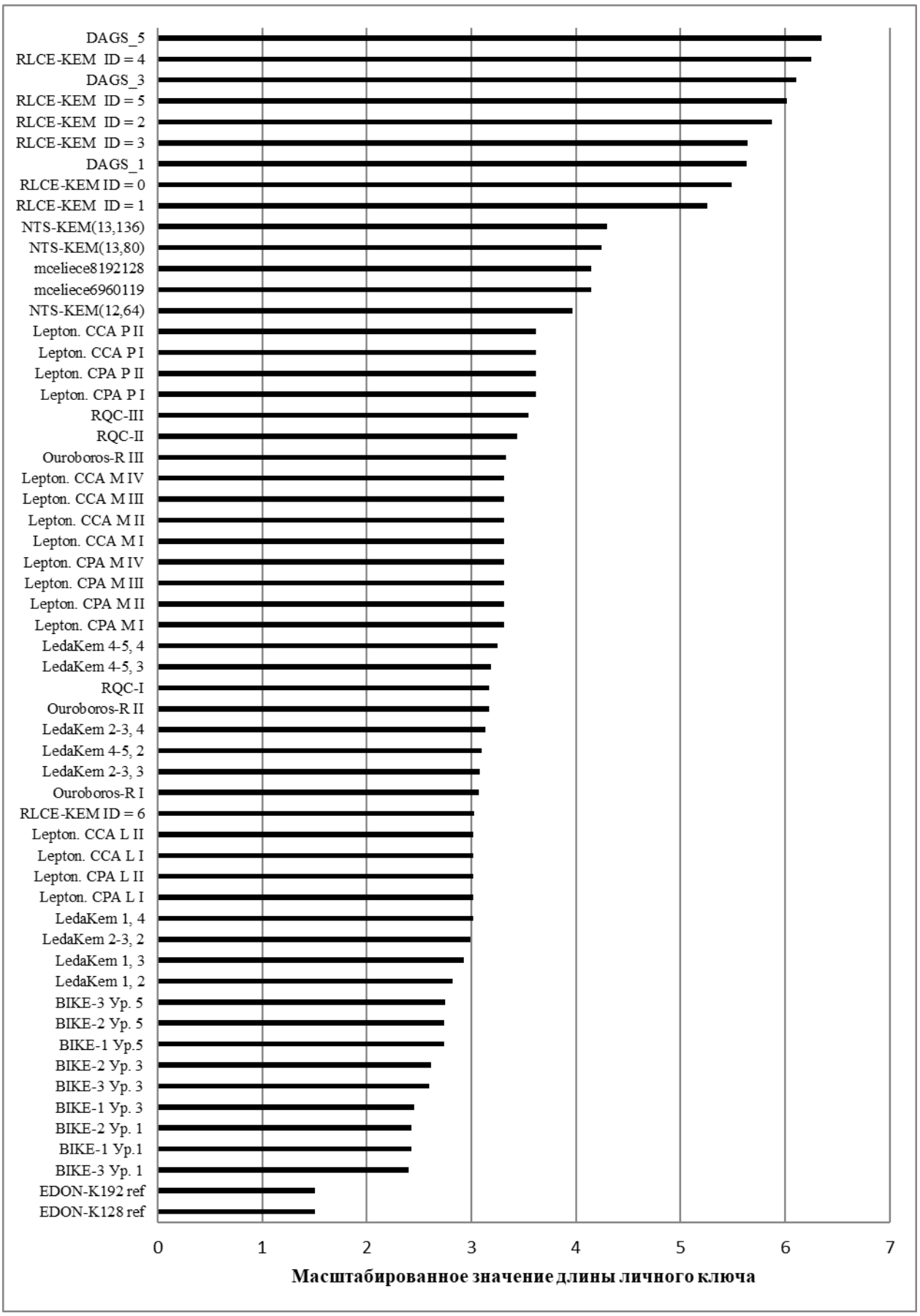

Рис. 1. Гистограмма сравнительного анализа длин личного ключа
(в байтах, логарифмический масштаб) для алгоритмов инкапсуляции ключей

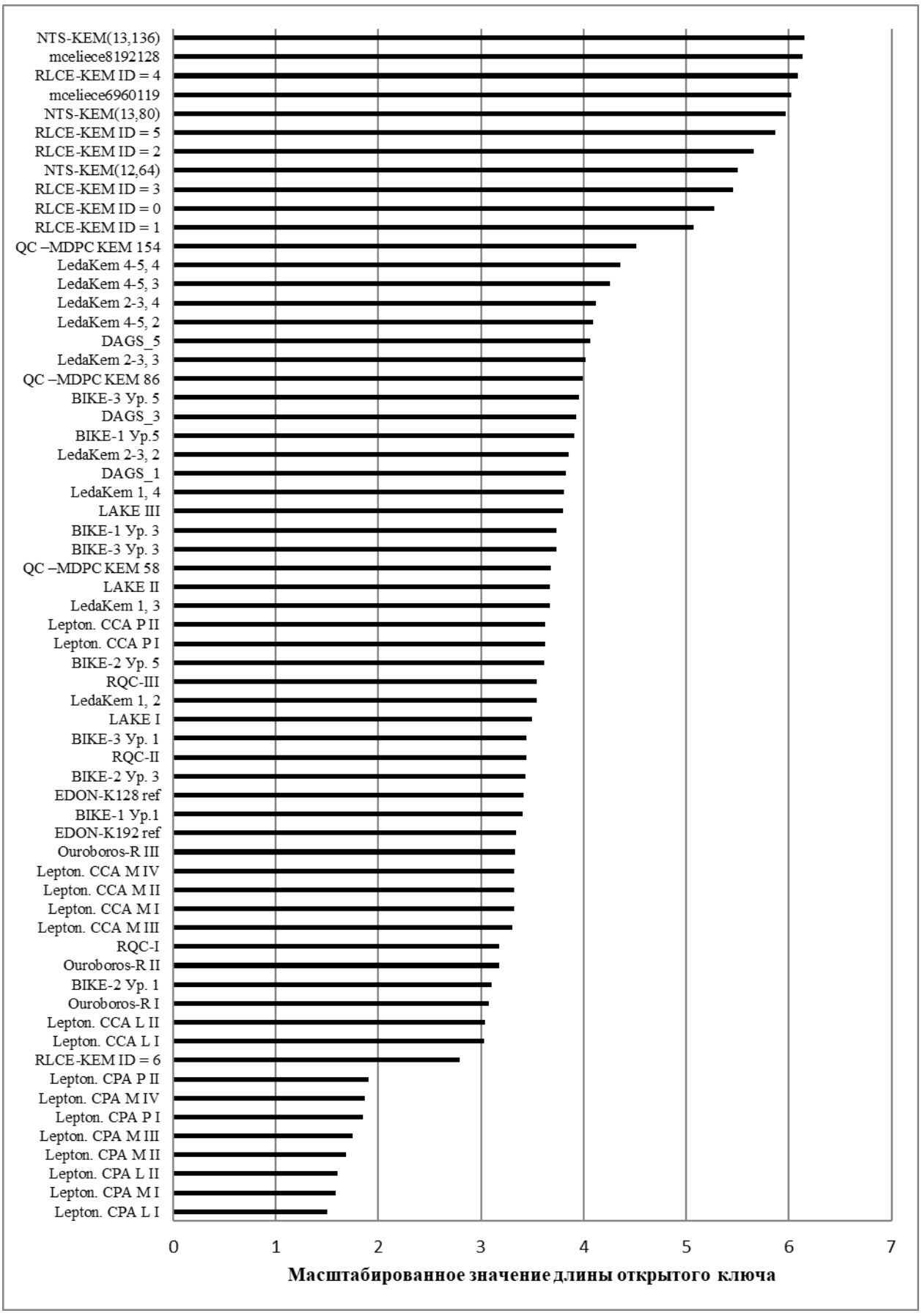

Рис. 2. Гистограмма сравнительного анализа длин открытого ключа
(в байтах, логарифмический масштаб) для алгоритмов инкапсуляции ключей

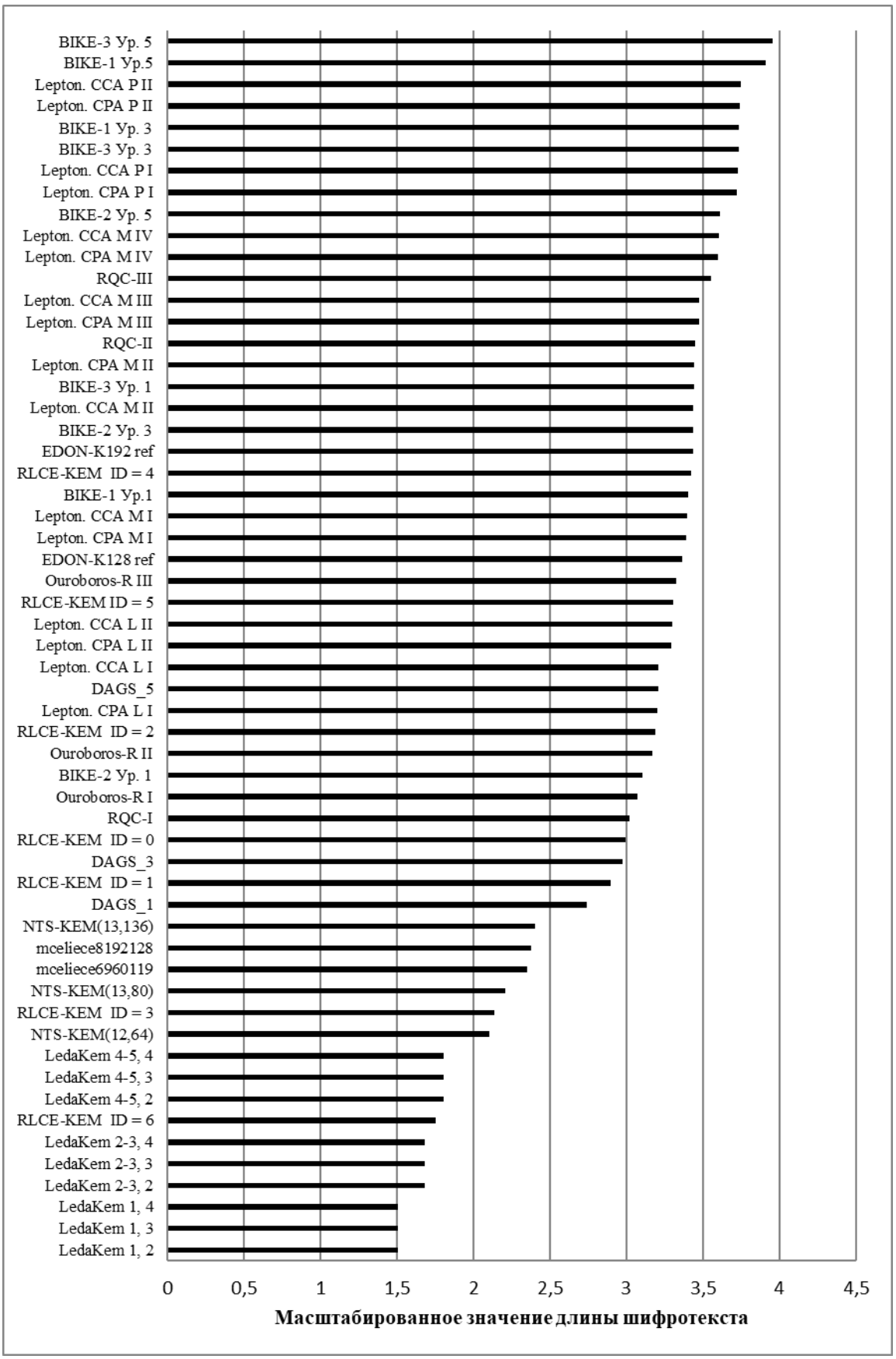

Рис. 3. Гистограмма сравнительного анализа длин шифротекста
(в байтах, логарифмический масштаб) для алгоритмов инкапсуляции ключей

Сравнительный анализ объема памяти, занимаемого открытым ключом в представленных схемах инкапсуляции ключей, дал несколько другой результат. Наименьшая длина открытого ключа у всех вариаций алгоритма Lepton.CPA – от 32 до 80 байт. Затем следуют алгоритмы RLCE-KEM ID = 6, Lepton.CCA, Ouroboros-R I, BIKE-2. Наиболее длинные открытые ключи имеют алгоритмы NTS-KEM (13, 136), Classic McElice 128 и RLCE-KEM ID = 4 – 1419704, 1357824 и 1232001 соответственно.

Для всех алгоритмов длина шифротекста сравнительно невелика и составляет от 32 до 9032,75 байт. По длине получаемого шифротекста алгоритмы инкапсуляции ключей расположились в следующем порядке. Сначала с наименьшей длиной следуют вариации схемы LedaKem и RLCE-KEM ID = 6. Некоторые авторы намеренно старались минимизировать длину шифротекста и при этом сохранить достаточную криптостойкость, чтобы такие алгоритмы инкапсуляции нашли свое применение в системах с ограниченными ресурсами. Логично, что наибольшую длину шифротекста имеют алгоритмы, обеспечивающие, по заявлению их авторов, наивысший уровень криптостойкости. Такими алгоритмами оказались вариации схем BIKE-1 и BIKE-3, Lepton.CPA и Lepton.CCA.

Сравнительный анализ показателей быстродействия

В табл. 2 приведены показатели быстродействия для алгоритмов инкапсуляции ключей. Оценка быстродействия проведена самими авторами на разных вычислительных платформах и представлена в формате количества циклов процессора, затраченных на выполнение операции формирования ключей, инкапсуляции и деинкапсуляции ключей. Все измерения происходили без применения каких-либо технологий оптимизации производительности. Разработчики алгоритма LedaKem эти показателя указали в миллисекундах, затраченных на выполнение операции на конкретной вычислительной платформе. Ввиду того, что все остальные разработчики для измерения быстродействия использовали другую метрику, а именно – циклы процессора, для алгоритма LedaKem эти оценки конвертированы в примерное количество затраченных циклов, определенное из характеристик вычислительной платформы.

Приведенные оценки быстродействия сравнимы при условии игнорирования остальных (помимо приведенных показателей используемого центрального процессора) характеристик используемых вычислительных систем. Такая оценка носит исключительно первичный ознакомительный анализ возможностей производительности перечисленных выше алгоритмов.

Таблица 2

Показатели производительности для алгоритмов инкапсуляции ключей (данные приведены в циклах процессора, которые требуется выполнить для проведения каждой операции)

№	Название	Вычислительная платформа	Версия	Формирование ключевых данных, циклы	Инкапсуляция, циклы	Деинкапсуляция, циклы
1	BIKE	Intel Core i5-6260U, 1.80 ГГц	BIKE-1	730025	689138	2901203
				1709921	1850425	7666855
				2986647	3023816	17483906
			BIKE-2	6383408	281755	2674115
				22205901	710970	7114241
				58806046	1201161	16385956
			BIKE-3	433258	575237	3437956
				1100372	1460866	7732167
				2300332	3257675	18047493
2	Classic McElice	Intel Xeon E3-1220 v3 (Haswell), 3.10 ГГц	mceliece8192128	2000000000	300000	450000
			mceliece6960119	966400	-	17055

№	Название	Вычислительная платформа	Версия	Формирование ключевых данных, циклы	Инкапсуляция, циклы	Деинкапсуляция, циклы
3	DAGS	Intel Core i5-5300U, 2.30 ГГц	DAGS_1	49394032811	20109354	23639371
			DAGS_3	106876216775	26109354	24639371
			DAGS_5	136497712522	49029613	260829051
4	Edon-K	Intel Corei7-7600U, 2.90 Гц	EDON-K128 ref	2500000	576000	28700000
			EDON-K192 ref	2000000	496000	54600000
5	LAKE	Intel Core i7-4700hq, 3.4 ГГц	LAKE I	1580000	300000	1270000
			LAKE II	1740000	310000	2090000
			LAKE III	1790000	350000	2890000
6	Leda Kem	AMD Ryzen 5 1600, 3.2 ГГц,	1, $n_0 = 2$	34,11 мс ≈ 109152000	2,11 мс ≈ 6752000	16,78 мс ≈ 53696000
			1, $n_0 = 3$	16,02 мс ≈ 51264000	2,15 мс ≈ 6880000	21,65 мс ≈ 69280000
			1, $n_0 = 4$	13,41 мс ≈ 42912000	2,42 мс ≈ 7744000	24,31 мс ≈ 77792000
			2-3, $n_0 = 2$	142,71 мс ≈ 456672000	8,11 мс ≈ 25952000	48,23 мс ≈ 154336000
			2-3, $n_0 = 3$	76,74 мс ≈ 245568000	8,79 мс ≈ 28128000	49,15 мс ≈ 157280000
			2-3, $n_0 = 4$	51,93 мс ≈ 166176000	9,46 мс ≈ 30272000	46,16 мс ≈ 147712000
			4-5, $n_0 = 2$	427,38 мс ≈ 1367616000	23,00 мс ≈ 73600000	91,78 мс ≈ 293696000
			4-5, $n_0 = 3$	227,71 мс ≈ 728672000	24,85 мс ≈ 79520000	92,42 мс ≈ 295744000
			4-5, $n_0 = 4$	162,34 мс ≈ 519488000	26,30 мс ≈ 84160000	127,16 мс ≈ 406912000
7	Lepton. CPA	Intel Core-i7 4790, 3.6 ГГц	Light I	33625	78808	33400
			Light II	34912	85347	42462
			Moderate I	48932	117275	45519
			Moderate II	51519	125178	51353
			Moderate III	51508	130057	60289
			Moderate IV	57861	152431	72564
			Paranoid I	96602	237722	97757
			Paranoid II	97884	247932	105200
	Lepton. CCA		Light I	34308	79152	87043
			Light II	34536	86584	100141
			Moderate I	49943	121564	132708
			Moderate II	51658	124426	141988
			Moderate III	52699	130631	151185
			Moderate IV	59450	154473	179520
			Paranoid I	94454	234441	264881
			Paranoid II	94569	244706	282199
8	NTS-KEM	Intel Xeon E5-2667 v2, 3.3 ГГц	NTS-KEM(12,64)	41746373	172463	686087
			NTS-KEM(13,80)	135813837	429301	1300102
			NTS-KEM(13,136)	249939545	574406	2911120
9	Ouroboros-R	Intel Core i7-4770, 3.4 ГГц	Ouroboros-R I	600000	980000	1780000
			Ouroboros-R II	650000	1120000	3260000
			Ouroboros-R III	820000	1390000	4730000

№	Название	Вычислительная платформа	Версия	Формирование ключевых данных, циклы	Инкапсуляция, циклы	Деинкапсуляция, циклы
10	QC –MDPC KEM	Intel Core i7-7500U, 2.7 ГГц	QC –MDPC KEM 154	131038872	20263392	229002269
11	RLCE-KEM	Intel Core i7, 2.9 ГГц	ID = 0	1011071617	1805010	4646941
			ID = 1	465481183	1040629	3589491
			ID = 2	3829675407	3331234	8668186
			ID = 3	1962533052	2361787	7160709
			ID = 4	9612380645	8184051	36705481
			ID = 5	5057459034	5362174	24174369
12	RQC	Intel Core i7-4770, 3.4 ГГц	RQC-I	790000	1970000	5300000
			RQC-II	1760000	5600000	14460000
			RQC-III	2820000	5460000	18000000

Для наглядности на рис. 4 – 7 приведены гистограммы параметров быстродействия для вариаций алгоритмов, обеспечивающих наибольший уровень криптостойкости, а именно: Lepton.CCA P II, Lepton.CPA P II, Ouroboros-R III, LAKE III, EDON-K192, BIKE-3, RQC III, QC –MDPC KEM, NTS-KEM (13, 136), LedaKem 4-5, 4, Classic McElice 128, RLCE-KEM, ID = 5, DAGS_5. Для того чтобы адекватно продемонстрировать эти показатели, все данные на гистограммах приведены с использованием логарифмического масштаба, так как параметры разнятся на несколько порядков.

Следует отметить, что меньшие значения циклов, затрачиваемых на выполнение одной операции, являются предпочтительными. В то же время, бо́льшие значения количества затрачиваемых циклов указывают на низкую скорость выполнения операции.

На рис. 4 приведена сводная гистограмма всех показателей быстродействия, показывающая общее соотношение скорости выполнения трех операций (формирование ключей, инкапсуляция и деинкапсуляция ключей) для каждого из алгоритмов. Все данные указаны в затраченных на выполнение операции циклах.

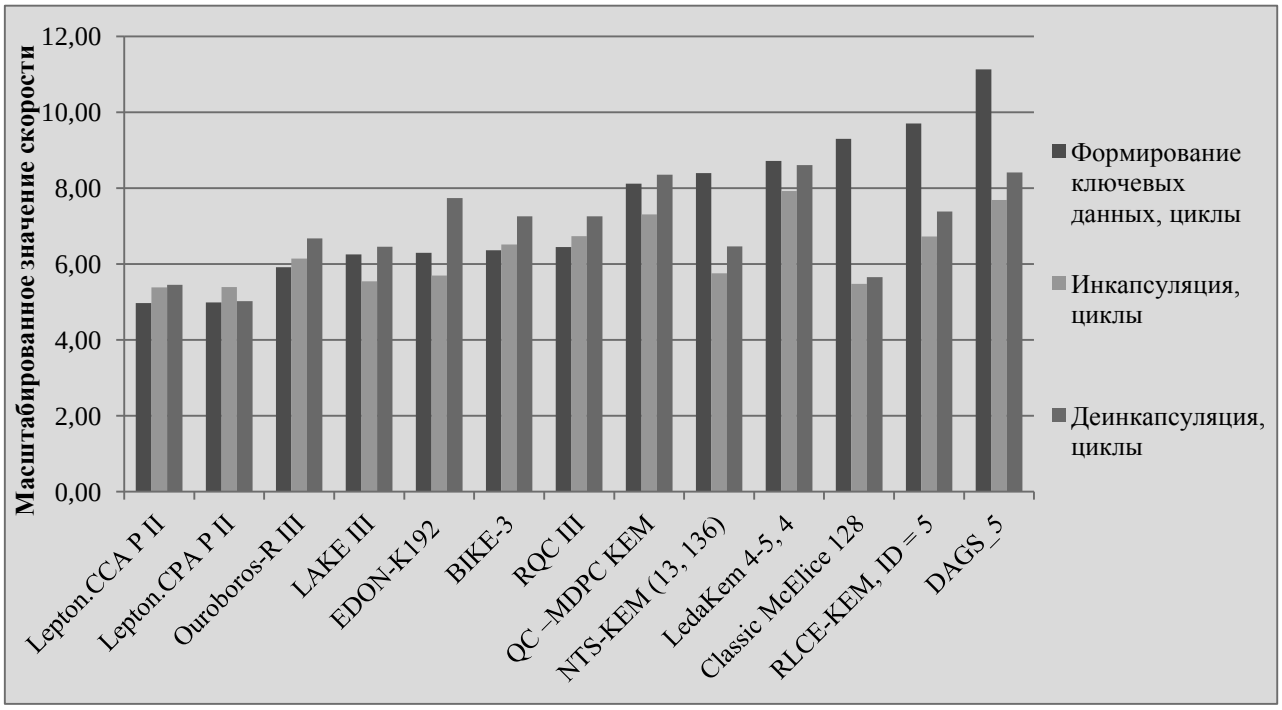

Рис. 4. Гистограмма показателей быстродействия (в логарифмическом масштабе)

Примерно сравнимую скорость выполнения всех операций имеют алгоритмы Lepton.CCA и Lepton.CPA, Ouroboros-R, LAKE, LedaKem. Достаточно большой разрыв в производительности между формированием ключей и инкапсуляцией (деинкапсуляцией) имеют схемы EDON-K, Classic McElic, RLCE-KEM, DAGS_5.

На рис. 5 приведена гистограмма оценки скорости формирования ключевых данных. Как показано выше, алгоритм Lepton имеет достаточно небольшие длины как открытого, так и личного ключей, и благодаря используемому алгоритму скорость формирования ключевых данных для данной схемы наибольшая. Наименьшая скорость формирования у алгоритма DAGS_5.

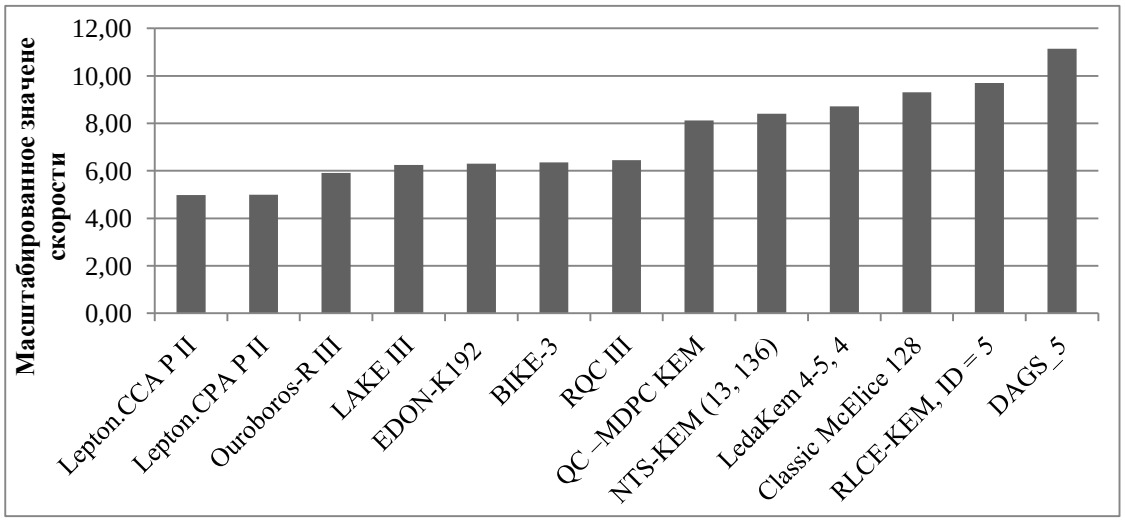

Рис. 5. Гистограмма показателя быстродействия: скорость формирования ключевых данных, в циклах (в логарифмическом масштабе)

Оценка скорости инкапсуляции приведена на рис. 6. Опять наибольшей скоростью обладает алгоритм Lepton. Наименьшая скорость у схемы LedaKem.

Показатель быстродействия – скорость деинкапсуляции напрямую зависит от выбранного метода для деинкапсуляции. Некоторые авторы указывают, что для выполнения этой операции в алгоритме может использоваться несколько различных методик, от выбора которых будет зависеть производительность операции. Так или иначе, согласно результатам оценки наибольшая скорость деинкапсуляции у алгоритма Lepton, наименьшая – у LedaKem.

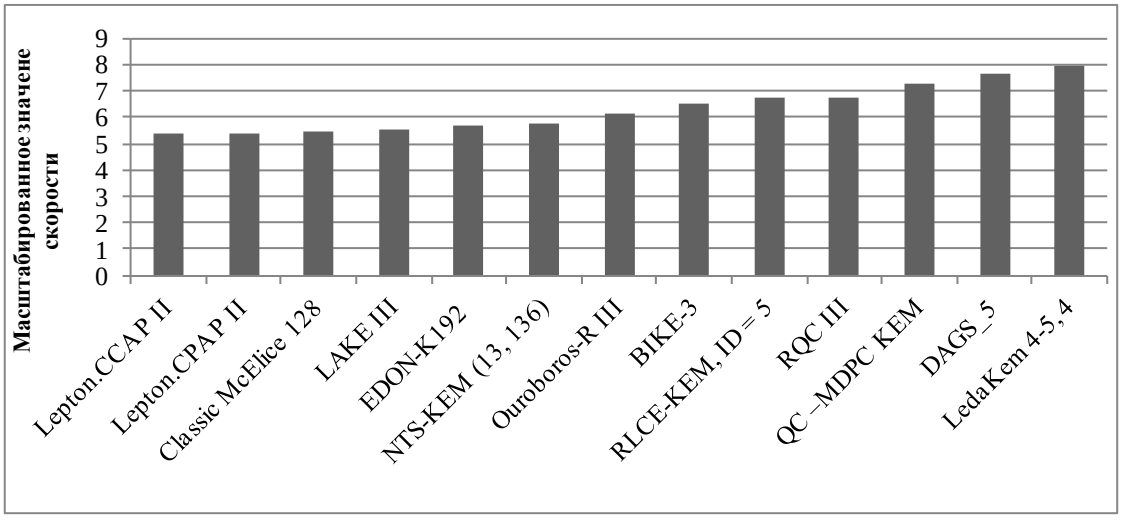

Рис. 6. Гистограмма показателя быстродействия: скорость инкапсуляции, в циклах (в логарифмическом масштабе)

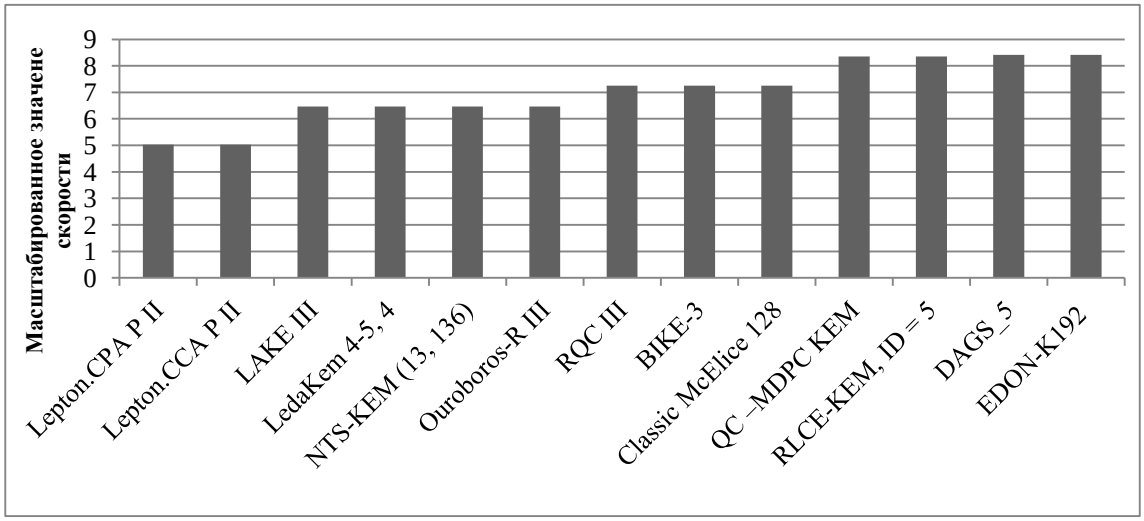

Рис. 7. Гистограмма показателя быстродействия: скорость деинкапсуляции, в циклах (в логарифмическом масштабе)

Выводы

Проведен первичный анализ схем-конкурсантов, представленных на конкурс постквантовой криптографии NIST PQC. Рассмотрены все 12 схем инкапсуляции ключей, проведены сравнения по показателям (указанными разработчиками) входных и выходных параметров, а также по показателям криптографической стойкости и быстродействия. На данный момент оценка криптостойкости и быстродействия взята из данных, указанных разработчиками.

В ходе исследований установлено, что практически все схемы удовлетворяют формальным требованиям к кандидатам на постквантовые схемы инкапсуляции ключей, т.е. имеют различные варианты алгоритмов, которые обеспечивают все три уровня криптостойкости (1-й, 3-й и 5-й). Исключение составляет алгоритм Edon-K (он обеспечивает только 1-й и 3-й уровни стойкости).

Наилучшие показатели быстродействия показал алгоритм Lepton. Однако следует отметить, что оценки быстродействия приводятся авторами для эталонных реализаций алгоритмов. В дальнейшем будут представлены оптимизированные реализации данных схем инкапсуляции ключей, их исследование является перспективным направлением.

Список литературы:

1. Post-Quantum Cryptography, Round 1 Submissions, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

2. Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zemor. BIKE – Bit Flipping Key Encapsulation, NIST Submission, 2017. [On-line]. Internet: http://bikesuite.org/#spec.

3. Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer. Classic McEliece, NIST Submission, 2017. [On-line]. Internet: https://classic.mceliece.org/index.html.

4. Gustavo Banegas, Paolo S.L M. Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndollane Dione, Kris Gaj, Cheikh Thiecoumba Gueye, Richard Haeussler, Jean Belo Klamti, Ousmane N'diaye, Duc Tri Nguyen. DAGS: Key Encapsulation using Dyadic GS Codes. NIST Submission, 2017. [On-line]. Internet: https://www.dags-project.org/#files.

5. Danilo Gligoroski, Kristian Gjøsteen. Post-quantum Key Encapsulation Mechanism EDON-K, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

6. Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zémor. LAKE – Low rAnk parity check codes Key Exchange, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

7. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, Paolo Santini. LEDAkem (Low dEnsity coDe-bAsed key encapsulation mechanism), NIST Submission, 2017. [On-line]. Internet: https://www.ledacrypt.org/LEDAkem/.

8. Yu Yu, Jiang Zhang. Lepton: Key Encapsulation Mechanisms from a variant of Learning Parity with Noise, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

9. Martin Albrecht, Carlos Cid, Kenneth G. Paterson, Cen Jung Tjhai, Martin Tomlinson. NTS-KEM, NIST Submission, 2017. [On-line]. Internet: https://nts-kem.io/.

10. Carlos Aguilar Melchor, Jean-Christophe Deneuville, Nicolas Aragon, Philippe Gaborit, Slim Bettaieb, Adrien Hauteville, Loïc Bidoux, Gilles Zémor . Ouroboros-R, NIST Submission, 2017. [On-line]. Internet: http://pqc-ouroborosr.org/.

11. Atsushi Yamada, Edward Eaton, Kassem Kalach, Philip Lafrance, Alex Parent. QC-MDPC KEM: A Key Encapsulation Mechanism Based on the QC-MDPC McEliece Encryption Scheme, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

12. Yongge Wang. RLCEKeyEncapsulation Mechanism (RLCE-KEM) Specifcation, NIST Submission, 2017. [On-line]. Internet: http://quantumca.org/.

13. Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillippe Gaborit, Gilles Zemor. Rank Quasi-Cyclic (RQC) , NIST Submission, 2017. [On-line]. Internet: http://pqc-rqc.org/.

14. Katz, Jonathan; Lindell, Yehuda. Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall / CRC Press, 2007. 553 p.

15. Bellare, Mihir; Rogaway, Phillip. "Introduction to Modern Cryptography. [On-line]. Internet: http://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf, September 21, 2005.

Харківський національний
університет імені В.Н.Каразіна

Надійшла до редколегії 00.00.2018