УДК 004.056.55

Федоров С.К.,
Магистрант
2 курс, факультет «Космический»
МФ МГТУ им. Н. Э. Баумана
Россия, г. Москва
Научный руководитель: Афанасьев А.В.,
кандидат технических наук

АНАЛИЗ ПОСТКВАНТОВЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Аннотация: *В статье рассматриваются четыре криптографических схемы. Их алгоритмы являются участниками конкурса Национального Института Стандартизации и Технологий США в качестве кандидатов на стандарт постквантовой криптографии. В работе описываются основополагающие алгоритмы и принципы. Также кратко приводятся общие исторические сведения.*

Ключевые слова: *квантовый компьютер, шифрование, алгоритмы, коды исправления ошибок, криптография на решетках*

Annotation: *This article highlights four cryptographic schemes. Their algorithms are nominated for a post-quantum cryptography standard by the US National Institute for Standardization and Technology. The paper describes the underlying algorithms and principles. General historical information is also briefly provided.*

Keywords: *quantum computer, encryption, algorithms, error correction codes, lattice cryptography.*

McEliece это одна из первых криптосистем на основе исправляющих ошибки кодов, предложенная в 1978 году Робертом Мак-Элисом. Открытый ключ определяет случайный двоичный код Гоппы. Шифротекст это кодовое слово с примесью случайных ошибок. Закрытый ключ дает возможность эффективного декодирования: извлечения кодового слова из зашифрованного текста, а также определение и удаление ошибок.

Система McEliece была спроектирована таким образом, чтобы быть однонаправленной (OW-CPA), то есть атакующий не может эффективно найти кодовое слово для заданного зашифрованного текста и публичного ключа, когда кодовое слово выбрано случайно. Уровень безопасности McEliece оставался на удивление стабильным несмотря на большое количество попыток взлома за последние сорок лет. Оригинальные параметры McEliece был спроектированы для 2^{64} безопасности, но система легко масштабируется до «заоблачных» параметров, которые предоставляют достаточный запас против возможных прорывов в компьютерных технологиях. Что также включает квантовые компьютеры.

По системе McEliece было проделано колоссальное количество работы. Часть из проектов улучшают эффективность, не затрагивая уровень безопасности. Как, например «двойная» PKE, предложенная Нидеррайтером или аппаратное ускорение, описанное в источнике [1].

Более того, на данный момент хорошо известен эффективный способ для превращения OW-CPA PKE схемы в механизм инкапсуляции ключей, который IND-CCA2-безопасен против всех ROM атак. Это преобразование достаточно строгое. Оно сохраняет уровень безопасности при выполнении двух условий. Во-первых, PKE является детерминированной (то есть дешифрование устраняет всю использованную случайность). Во-вторых, PKE не имеет ошибок дешифрования для правильных зашифрованных текстов. Недавние работы достигают похожего уровня строгости против более широкого класса атак. В особенности QROM атак. Риск того, что зависимая от

хэш-функции атака окажется эффективнее чем ROM или QROM атаки, нивелируется стандартной практикой выбора хорошо изученной и хорошо защищенной «неструктурированной» хэш-функции.

Предложение Classic McEliece (Классическая схема Мак Элиса) собирает все эти наработки воедино. Оно представляет механизм инкапсуляции ключей, спроектированный с учетом IND-CCA2 безопасности на очень высоком уровне безопасности, даже против квантовых компьютеров. KEM консервативно выводится из схемы шифрования с открытым ключом, которая является OW-CPA безопасной. Конкретно говоря, это «двойная» версия Нидеррайтера схемы McEliece, основанной на двоичных кодах Гоппы. Каждая деталь схемы была разработана с учетом возможных будущих изменений в безопасности криптографических схем, таким образом, что аудиторы могут быть уверены долгосрочной защищенности схем шифрования с открытым ключом.

Kyber это IND-CCA2-безопасный механизм инкапсуляции ключей (KEM). Безопасность Kyber основывается на сложности решения проблемы обучения с ошибками в модульных решетках (MLWE). Kyber конструируется в два шага: сначала определяется IND-CPA-безопасная схема с открытым ключом, для шифрования сообщений с фиксированной длиной в 32 байта, называемая Kyber.CPAPKE. Затем используется слегка измененное преобразование Фуджисаки – Окамото для создания IND-CCA2-безопасной KEM. В дальнейшем, если имеется в виду IND-CCA2-безопасная KEM, используется термин Kyber.CCAKEM.

Saber это семейство криптографических примитивов, опирающихся на сложность решения задачи обучения с округлением по модулю (Mod-LWR или MLWR). Как и перечисленные выше схемы, Saber сначала определяет IND-CPA безопасную схему шифрования с открытым ключом Saber.PKE, а затем, при помощи одной из разновидностей преобразования Фуджисаки –

Окамото, трансформирует её в механизм инкапсуляции ключей Saber.KEM, которая является безопасной в контексте IND-CCA.

Схема Saber проектировалась с направлением на простоту, эффективность и гибкость в использовании. Это привело к ряду решений. Так, например, все модули целых чисел выбраны в степенях двойки, что позволяет полностью избежать взятий по модулю и процедуры взятия образца, в противовес схеме NTRU. Так же использование принципа LWR в два раза понижает необходимой случайности, по сравнению с основанными на LWE схемами, а также понижает требуемую пропускную способность канала. Модульная структура предоставляет гибкость в использовании благодаря тому, что для разных уровней безопасности используется один и тот же ключевой компонент (ядро).

NTRU это механизм инкапсуляции ключей (KEM) основанный на схеме NTRUEncrypt за авторством Хоффшейна, Пайпфера и Сильвермана [1]. Алгоритм строится с использованием обобщенных трансформаций из корректной детерминированной схемы шифрования с публичным ключом (корректная DPKE, Deterministic Public Key Encryption). NTRU изначально описывался как частично-корректная вероятностная система шифрования с открытым ключом (частично корректная PPKE, Probabilistic Public Key Encryption). И большинство упоминаний в литературе основано на этой PPKE. Тем не менее, препринт документа NTRU, упоминаемого на CRYPTO'96 [2] описывает как NTRU может быть сделана детерминированной, а также полностью корректной, благодаря ряду небольших изменений, внесенных Хюлсингом, Рейнвельдом, Шанком и Швабе, авторами «Cryptographic Hardware and Embedded Systems». Корректная DPKE, описываемая здесь, получается при применении описанных в препринте трансформаций для детерминизма и корректности по отношению к PPKE из ANTS'98.

DPKE параметризирована взаимно простыми целыми числами (n, p, q), пространствами элементарных событий $(\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_r, \mathcal{L}_m)$, и инъекцией $Lift$:

$\mathcal{L}_m \to Z[x]$. Рекомендуется к реализации два узко определенных набора параметров называемых NTRU-HPS и NTRU-HRSS. NTRU-HPS использует определенные Хоффштейном, Пайпером и Сильверманом пространства элементарных событий с фиксированными весами. Он предоставляет несколько выборов q для каждого n. NTRU-HRSS использует определенные Хюлсингом, Рейнвельдом, Шанком и Швабе пространства элементарных событий со стандартными показателями весов и фиксированную q как функцию от n.

Предложенная на конкурс схема является слиянием предложений NTRUEncrypt и NTRU-HRSS-KEM. В ней объединены все аспекты их дизайнов, за исключением использования пробирования с фиксированными весами. В этом плане набор параметров NTRU-HPS следует по пути предложения NTRUEncrypt, а набор параметров NTRU-HRSS соответственно, предложения NTRU-HRSS-KEM. Авторами крайне рекомендуется набор параметров ntruhrss701 (то есть NTRU-HRSS с n = 701), который был единственным рекомендованным набором параметров в предложении NTRU-HRSS-KEM. Цель достижения максимальной корректности заставила авторов объявить устаревшим набор параметров, рекомендованных в предложении NTRUEncrypt. Чтобы заменить наборы параметров ntru-pke-443 и ntru-pke-743 предложения NTRUEncrypt, были выбраны ntruhps2048509 (NTRU-HPS с n = 509 и q = 2048) и ntruhps4096821 (NTRU-HPS с n = 821 и q = 4096). Так же в качестве альтернативы ntruhrss701 был выбран ntruhps2048677 (NTRU-HPS с n = 677 и q = 2048) как альтернативу ntruhrss701.

Получившийся механизм инкапсуляции ключей имеет убедительное доказательство неразличимости зашифрованного текста по IND-CCA2 в модели случайного оракула (ROM) с предположением, что используемая схема является OW-CPA безопасной. Так же существует убедительное доказательство неразличимости по IND-CCA2 в модели квантового оракула (QROM) под нестандартными предположениями Сайто, Хагавы и Ямикавы

[2]. KEM взаимозаменяема с KEM, созданной Сайто, Хагавой и Ямикавой, но так же может быть рассмотрена как приложение $U_m^{\perp}$ трансформации за авторством Хофхайнца, Хевельманнса и Кильца, или SimpleKEM трансформации Бернштейна и Персичетти. Причина этого в том, что описываемая DPKE немного отличается от NTRU DPKE Сайто, Хагавы и Ямикавы. Эта DPKE достигает нотации гибкости Бернштейна и Персичетти без применения «ре-шифрования». Это изменение влияет на внутреннее поведение KEM и результат остается взаимозаменяем с NTRU KEM Сайто-Хагавы-Ямикавы.

Заключение

В статье были разобраны четыре финалиста второго раунда конкурса Национального Института Стандартов и Технологий США по постквантовой криптографии. Три схемы (NTRU, Kyber и Saber) опираются на принципы криптографии на решетках и обучения с ошибками, тогда как четвертая (Classic McEliece) использует в своей основе коды, исправляющие ошибки.

Результаты конкурса будут объявлены в 2022 году, однако уже сейчас возможно использовать приведенные схемы для усиления безопасности существующих систем, опирающихся на принципы классической криптографии.

Использованные источники:

1. Eric R. Verheul, Jeroen M. Doumen, and Henk C. A. van Tilborg. Sloppy Al-ice attacks! Adaptive chosen ciphertext attacks on the McEliece public-key cryp-tosystem. In Mario Blaum, Patrick G. Farrell, and Henk C. A. van Tilborg, editors, Information, coding and mathematics, volume 687 of Kluwer International Series in Engineering and Computer Science, pages 99–119. Kluwer, 2002.
2. Tsunekazu Saito, Keita Xagawa, Takashi Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In Annual

International Conference on the Theory and Applications of Cryptographic Techniques, P. 520-551. Springer, 2018.