конференция РусКрипто

QApp

Исследование специальных видов постквантовых электронных подписей и проблем их реализации

Сергей Гребнев
Руководитель направления
прикладных исследований

qapp.tech

Участник

Актуальность

В связи с текущим переходом
на постквантовые алгоритмы важно
исследовать постквантовые варианты
специальных видов подписей, которые имеют
широкое применение в большом количестве
практических приложений

Пороговые подписи

QApp

Пороговые подписи — электронные подписи, в которых участники могут создавать группы таким образом, что только определенные подмножества группы могут создавать подписи от имени группы

Пороговые подписи применяются:

- Для обеспечения безопасности цифровых кошельков
- В финансовой среде, где подписывающие лица должны нести ответственность за созданные ими пороговые подписи
- В схемах электронного голосования
- Для безопасности мобильных агентов
- ... и другое

Постквантовые пороговые подписи

- Большинство работ носят теоретический характер и не предлагают эффективных реализаций
- Основные примитивы: решётки, изогении, хэш-функции
- Основные проблемы: размеры общей коммуникации, многораундовость
- Пример: пороговая подпись Raccoon * (решётки). Для уровня безопасности NIST-1:
  - Количество раундов – 3
  - Открытый ключ — 3,9 Кбайт
  - Подпись – 12,7 Кбайт
  - Общая коммуникация на одного участника – 40,8 Кбайт

* Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions / R. del Pino [и др.]. — 2024. — URL: https://eprint.iacr.org/2024/184. Cryptology ePrint Archive, Paper 2024/184

Кольцевые подписи

QApp

Кольцевая подпись — тип электронной подписи, который позволяет некоторому участнику группы подписать сообщение от имени всей группы, сохраняя при этом собственную анонимность

Кольцевые подписи применяются:

- Для анонимного информирования общественности о нарушениях
- В криптовалютах для возможности делать транзакции неотслеживаемыми
- В схемах электронного голосования и электронных денег
- Для защиты авторских прав
- ... и другое

Постквантовые кольцевые подписи

QApp

- Наиболее изученное направление из рассматриваемых: представлены схемы и их эффективные реализации
- Основные примитивы: изогении, решётки
- Основные проблемы: размеры ключей и подписей

Постквантовые кольцевые подписи

Сравнительная таблица размеров кольцевых подписей и открытых ключей при различных размерах кольца

Название схемы кольцевой подписи	Размер подписи (Кб) при различных n (n – размер кольца)					Размер открытого ключа, Кб
	$n = 2$	$n = 2^3$	$n = 2^6$	$n = 2^{10}$	$n = 2^{12}$	
Calamari (изогении)	3.5	5.4	8.2	10.4	14	0.06
Falafl (решётки)	29	30	32	32.5	35	1.28
DualRing (решётки)	4.48	4.63	6.02	30.13	106.57	2.84
Smile (решётки)	$*$	$*$	> 16	18	$*$	2
Erebor (изогении)	0.35	1.34	10.64	170	680	0.06
Durian (изогении, не реализован)	4.08	$*$	$*$	9.87	$*$	0.06
Gandalf (решётки)	1.21	4.76	37.9	606.02	2424	0.89

Кольцевые пороговые подписи

QApp

Кольцевая пороговая подпись — расширение концепции кольцевых подписей, которое добавляет возможность создания подписи только при участии определённого числа участников группы (порога)

Кольцевые пороговые подписи применяются в тех же сферах, что и кольцевые подписи, с дополнительными требованиями к системам, где важна гибкость или необходимо собрать анонимный кворум

Постквантовые кольцевые пороговые подписи

- Схемы существуют почти во всех разделах постквантовой криптографии: коды, решётки, многомерные уравнения, изогении
- Основные проблемы: крайне неэффективны; в работе * было указано, что схемы, построенные на основе преобразования Фиата-Шамира, не всегда обеспечивают надёжность в модели QROM
- Работа * предлагает концепцию стойкой в модели QROM схемы, но не имеет какой-либо практической реализации

* Haque A., Scafuro A. Threshold ring signatures: new definitions and post-quantum security // Public-Key Cryptography-PKC 2020: 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4–7, 2020, Proceedings, Part II 23. — Springer. 2020. — с. 423—452

Постквантовые кольцевые пороговые подписи

Сравнительная таблица размеров кольцевых пороговых подписей

Алгоритм подписи	Уровень безопасности λ, бит	Размер подписи при $t = 50$, $N = 100$, Мб (N – число участников, t – порог схемы)	Размер открытого ключа, Кб
Работа [1]	$*$	2	34713.6
Работа [2]	80	1.25	0.008
Работа [3]	111	12.8	8.19
Работа [4]	80	0.62	3584
Работа [5]	128	0.069	0.06

[1] A new efficient threshold ring signature scheme based on coding theory / C. A. Melchor [и др.] // IEEE Transactions on Information Theory. — 2011. — т. 57, № 7. — с. 4833—4842

[2] Assidi H., Ayebie E. B., Souidi E. M. An efficient code-based threshold ring signature scheme // Journal of information security and applications. — 2019. — т. 45. — с. 52—60

[3] Bettaieb S., Schrek J. Improved lattice-based threshold ring signature scheme // Post-Quantum Cryptography: 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings 5. – Springer Berlin Heidelberg, 2013. – С. 34-51

[4] Petzoldt A., Bulygin S., Buchmann J. A multivariate based threshold ring signature scheme // Applicable Algebra in Engineering, Communication and Computing. — 2013. — т. 24. — с. 255—275

[5] Pham M. T. T. et al. Threshold Ring Signature Scheme from Cryptographic Group Action // International Conference on Provable Security. – Cham : Springer Nature Switzerland, 2023. – С. 207-227

Кольцевые связываемые подписи

QApp

Кольцевая связываемая подпись — расширение концепции кольцевых подписей, которое добавляет возможность проверки, были ли две подписи созданы одним и тем же участником группы, без раскрытия его личности

Кольцевые связываемые подписи имеют схожее применение, что и кольцевые подписи, в том числе они применяются:

- В схемах электронного голосования
- В криптовалютах для возможности отслеживания мошеннических действий
- В анонимных аукционах, где пользователи подписывают транзакции, впоследствии объединяя их и исследуя легитимность покупателя
- ... и другое

Постквантовые кольцевые связываемые подписи

- В настоящее время активно разрабатываются постквантовые кольцевые связываемые подписи
- Основные примитивы: изогении, решётки, коды
- Основные проблемы: размеры подписи

Постквантовые кольцевые связываемые подписи

QApp

Сравнительная таблица размеров кольцевых связываемых подписей, Кб

Название схемы	Количество пользователей в кольце					Размер открытого ключа, Кб
	$n = 2$	$n = 2^3$	$n = 2^6$	$n = 2^{10}$	$n = 2^{12}$	
Calamari	3.5	5.4	8.2	10.4	14	0.06
Falafl	29	30	32	32.5	35	1.28
L2RS	$*$	44.3	340.4	$*$	$*$	1.92
Работа [1]	$*$	82.5	> 305.7	> 1198	$*$	8
Работа [2]	5.38	14.38	98.4	1536	6144	8
Работа [3]	77.6	310.4	2483	39731	158925	98.2

[1] Baum C., Lin H., Oechsner S. Towards practical lattice-based one-time linkable ring signatures // International Conference on Information and Communications Security. – Cham : Springer International Publishing, 2018. – С. 303-322
[2] Ren Y., Guan H., Zhao Q. An efficient lattice-based linkable ring signature scheme with scalability to multiple layer // Journal of Ambient Intelligence and Humanized Computing. – 2022. – С. 1-10
[3] Branco P., Mateus P. A code-based linkable ring signature scheme // Provable Security: 12th International Conference, ProvSec 2018, Jeju, South Korea, October 25-28, 2018, Proceedings 12. – Springer International Publishing, 2018. – С. 203-219

Кольцевые прослеживаемые подписи

Кольцевая прослеживаемая подпись — расширение концепции кольцевых подписей, которое добавляет возможность сохранения анонимности подписанта до тех пор, пока он не подпишет определённое сообщение или не нарушит правила системы

Данный вид подписи достаточно специфичен и имеет в целом намного более узкую применимость, чем те же кольцевые или пороговые подписи. Некоторыми из сфер применения являются:

- Анонимное голосование в электронной доске объявлений
- Системы анонимной аутентификации
- Системы электронных денег

Постквантовые кольцевые прослеживаемые подписи

QApp

- Основные примитивы: коды, решётки, хэш-функции
- Основные проблемы: размеры ключей, подписей, поддерживаемый размер кольца
- Пример: подпись * (коды)
  - Уровень безопасности – $\lambda = 128$ бит
  - Число участников – $N = 3$
  - Открытый ключ – $3.75 \cdot 10^3$ Кб
  - Подпись – $9.87 \cdot 10^3$ Кб

* Qi Y., Wang L.-P. A New Code-Based Traceable Ring Signature Scheme // Security and Communication Networks. — 2022. — апр. — т. 2022. — с. 1—10. — DOI: 10.1155/2022/3938321

Протоколы с нулевым разглашением

Протокол с нулевым разглашением — криптографический протокол, позволяющей одной стороне доказать другой стороне знание секрета, не раскрывая никакой информации о самом секрете

Протоколы с нулевым разглашением применяются:

- При построении схем электронной подписи
- В приложениях, связанных с технологиями, обеспечивающими приватность (PET)
- В блокчейн-системах
- ... и другое

Постквантовые протоколы с нулевым разглашением

QApp

- Основные проблемы: большие размеры доказательств
- Специальные протоколы с нулевым разглашением для построения электронных подписей: схема Штерна, протокол идентификации CSI-FiSh и другие
- Протоколы zk-SNARK, zk-STARK, zk-BOO для использования в блокчейн
  Размеры доказательств для одной транзакции:
  - zk-SNARK — 200 байт
  - zk-STARK — 45 Кбайт
  - zk-BOO — от 224 до 836 Кбайт

Соавторы доклада

QApp

QApp

Сергей Гребнев

Руководитель направления прикладных исследований

Вадим Давыдов

Криптограф-исследователь, PhD

Ирина Полтавская

Коммерческий директор

СБЕР
Blockchain Lab

Алексей Курочкин

Руководитель направления

QApp

Сергей Гребнев
Руководитель направления
прикладных исследований

sg@qapp.tech
@pikkunorsu

qapp.tech

Участник