Тенденции развития постквантовой криптографии

Гребнев Сергей Владимирович

Технический комитет по стандартизации
«Криптографическая защита информации» (ТК 26)

21 марта 2019, РусКрипто

Постановка задачи

Основные криптоаналитические задачи в классической модели

- Факторизация целых чисел (RSA): $\exp[(1,923 + o(1))(\log N)^{1/3})(\log\log N)^{2/3}]$ битовых операций
- Дискретное логарифмирование в конечном поле (DSA, DH, ГОСТ Р 34.10-94): $\exp[(1,923 + o(1))(\log p)^{1/3})(\log\log p)^{2/3}]$
- Дискретное логарифмирование на эллиптических кривых (ECDSA, ECDH, ГОСТ Р 34.10-2012): $O(\sqrt{p})$ операций на кривой
- Поиск коллизий хэш-функции: $O(2^{n/2})$ операций хэширования
- Поиск прообраза: $O(2^n)$ операций хэширования/зашифрования

Постановка задачи

Основные криптоаналитические задачи в квантовой модели

- Факторизация целых чисел: метод Шора, $O(\log^2 N)$ операций, $O(\log N)$ кубитов
- Дискретное логарифмирование в конечном поле: метод Шора, $O(\log^2 p)$ операций, $O(\log p)$ кубитов
- Дискретное логарифмирование на эллиптических кривых: метод Шора, $O(\log^2 p)$ операций, $O(\log p)$ кубитов
- Поиск коллизий ($f : V^{2n} \mapsto V^n$): метод BHT $O(2^{n/3})$ операций, $O(2^{2n/3})$ кубитов; метод Амбайниса, $O(2^{n/3})$ операций, $O(2^{n/3})$ кубитов
- Поиск прообраза ($f : V^n \mapsto V^n$): метод Гровера, $O(2^{n/2})$ операций, $O(\log n)$ кубитов

Квантовое настоящее и будущее

Настоящее

- IBM: 20 кубитов (физический размер 9 м^3), облачный доступ
- D-Wave: 1152 “кубита”, GOOGLE, NASA

Будущее

- Оценка возможности появления квантовых компьютеров достаточной для задач криптоанализа производительности (≥ 2730) кубитов: $10 - 40 - \infty$ лет
- Необходимость создания постквантовых СКЗИ: **сейчас**

История постквантовой криптографии

- 2003 год: Д. Бернштейн предлагает термин “постквантовая криптография”
- 2006 год: первая конференция PQCrypto
- 2014 год: меморандум ЕС “Horizon 2020”
- 2015 год: меморандум АНБ о переходе на постквантовые алгоритмы
- 2017 год: объявлен конкурс NIST

“Конкурс” NIST-PQ

30 ноября 2017 г. – закончен прием заявок.
Апрель 2018 г. – рабочая встреча по презентации предложений и заявок.
30 января 2019 г. – результаты 1 этапа.
Результаты – 3-5 лет анализа, по опыту конкурсов AES, SHA-3; 2 года для подготовки стандартов.

Определения теоретической стойкости

Для классических асимметричных систем шифрования:

- Стойкость к угрозе различения шифртекстов относительно атаки на основе подобранного открытого текста (Indistinguishability against chosen plaintext attack, **IND-CPA**).
- Стойкость к угрозе различения шифртекстов относительно атаки на основе подобранного шифрованного текста (Indistinguishability against chosen ciphertext attack, **IND-CCA**).
- Стойкость к угрозе различения шифртекстов относительно атаки на основе (неадаптивно) подобранного открытого текста (Indistinguishability against (non-adaptive) chosen plaintext attack, **IND-CPA1**).

Определения теоретической стойкости

- Стойкость к угрозе различения шифртекстов относительно атаки на основе (неадаптивно) подобранного шифрованного текста (Indistinguishability against (non-adaptive) chosen ciphertext attack, **IND-CCA1**).
- Стойкость к угрозе различения шифртекстов относительно атаки на основе адаптивно подобранного открытого текста (Indistinguishability against adaptive chosen plaintext attack, **IND-CPA2**).
- Стойкость к угрозе различения шифртекстов относительно атаки на основе адаптивно подобранного шифрованного текста (Indistinguishability against adaptive chosen ciphertext attack, **IND-CCA2**).

Определения теоретической стойкости

Для схем подписи интерес представляют следующие понятия стойкости:

- Сильная стойкость к подделке относительно атак на основе подобранных сообщений (Strong Unforgeability under chosen message attacks, **SUF-CMA**).
- Стойкость к экзистенциальной подделке относительно атак на основе подобранных сообщений (Existentially Unforgeability under chosen message attacks, **EUF-CMA**).

Определения практической стойкости

- I уровень: эквивалентно определению ключа 128-битового БШ;
- II уровень: эквивалентно поиску коллизии 256-битовой хэш-функции;
- III уровень: эквивалентно определению ключа 192-битового БШ;
- IV уровень: эквивалентно поиску коллизии 384-битовой хэш-функции;
- V уровень: эквивалентно определению ключа 256-битового БШ.

Основные подходы к синтезу

- Использование теории целочисленных решеток.
- Использование кодов, исправляющих ошибки.
- Использование многочленов от многих переменных.
- Использование криптографических хэш-функций.
- Использование изогений на суперсингулярных эллиптических кривых.
- “Эзотерика” (проблемы сопряженного поиска (search problem) или операции в группах кос (braid groups), алгебра октонионов, многочлены Чебышёва и т.д)

“Конкурс” NIST-PQ, 1 этап

- Всего 69 заявок.
- 14 из них уже отозваны или взломаны.
- 1 “сатирическая” (RSA и DSS с экспоненциальными параметрами)
- Опубликованы атаки на 13 из предложенных.

Теория решеток

Сложные задачи

- Задача поиска кратчайшего вектора (*SVP*); $SVP \in NP$
- Задача поиска ближайшего вектора (*CVP*); $CVP \in NP$
- Обучение с ошибками (*LWE*; *RLWE*)
- Наименьшее целочисленное решение СЛАУ (*SIS*)

Теория решеток

Криптосхемы

- Схема Меркля-Хеллмана, 1978 (укладка рюкзака) – взломана (Шамир, 1984)
- Схема Аджатаи-Дворка, 1997 (вариант *SVP*) – взломана (Нгуен, 1998)
- Схема Голдрайха-Голдвассер-Халеви (GGH), 1997 (*CVP*) – взломана (Нгуен, 1999)
- NTRU (Хоффштейн, Пайфер, Силверман, 1996) (*CVP*, не доказано) – шифрование, подпись. Стандарт IEEE P1363.
- BLISS (Дукас и др., 2013) (*CVP*, не доказано)
- RLWE-KEX (Регев и др., 2005) (*RLWE*)
- NewHope (Алким и др., 2015) – реализован Google, Infineon (*RLWE*)

Теория решеток - пример

Общая схема (на примере *RLWE*)

- $R_q = \mathbb{Z}_q[x]/(X^n + 1)$.
- ξ – распределение ошибки (обычно гауссово).
- Секретный ключ – $s \in R_q$.
- Открытый ключ – $as + e$, $a \in_R R_q$, e – ошибка.
- Аналог схемы Диффи-Хеллмана: $as + e$, $bs' + e'$; общий ключ $v = ass' + e's \approx bss' + es'$; s, s', e, e' – малы относительно некоторой нормы.

Теория решеток в рамках NIST-PQ

Криптосхемы

~~Compact LWE~~, CRYSTALS-KYBER, Ding Key Exchange, EMBLEM and R.EMBLEM, FrodoKEM, ~~HILA5~~ (*), KCL (pka OKCN/AKCN/CNKE), KINDI, LAC, LIMA, Lizard, LOTUS, NewHope, NTRUEncrypt, NTRU-HRSS-KEM, NTRU Prime, Odd Manhattan, ~~Round2~~, Round5, SABER, Three Bears, Titanium, CRYSTALS-DILITHIUM, DRS (*), FALCON, pqNTRUSign, qTESLA.

Теория кодирования

Сложная задача – декодирование линейного кода.

Криптосхемы

- МакЭлис, 1978 – взломана для ряда вариантов (Сидельников, 1990-е), однако для кодов Гоппы считается стойкой. Рассматривается Еврокомиссией как перспективная.
- Нидеррайтер, 1986 – аналогично.

Теория кодирования – пример

Пример: криптосхема МакЭлиса

- G – порождающая матрица двоичного линейного (n, k)-кода, исправляющего k ошибок;
- $S \in_R GL(k, 2)$ – случайная матрица;
- P – подстановочная $n \times n$ матрица;
- $G' = SGP$; (G', t) – открытый ключ, (S, G, P) – секретный ключ.
- Зашифрование: $c = E(m) = mG' + e$, e – случайный вектор веса t.
- Расшифрование: $c' = c \cdot P^{-1}$; m' – результат декодирования кода G; $m = m' \cdot S^{-1}$.

Теория кодирования в “конкурсе” NIST-PQ

Криптосхемы

BIG QUAKE, BIKE, Classic McEliece, ~~DAGS~~ (*), ~~Edon-K~~ (*), HQC, LAKE, LEDAkem, LEDApkc, Lepton, LOCKER, McNie, NTS-KEM, Ouroboros-R, QC-MDPC KEM, Ramstake, RLCE-KEM (*), RQC, ~~pqsigRM~~, RaCoSS (*), ~~RankSign~~ (*).

Многочлены от многих переменных

Сложная задача – решение системы полиномиальных уравнений над конечным полем (*NP*-полная). XL, F4, F5 и т.д.

Криптосхемы

- Мацумото-Имаи (1988) – взломана (Патарин, 1995)
- HFE, Патарин (1996) – взломана (Шамир, Фужер, 2002)
- Rainbow (Петцольд, Булыгин, Бухманн, 2010) – подпись

Многочлены от многих переменных – пример

Общая схема

- В конечном поле K выбираются легкообратимое квадратичное отображение $F : K^n \to K^m$, $m \geq n$, и обратимые линейные отображения $S : K^m \to K^m$, $T : K^n \to K^n$.
- Секретный ключ – отображения S, F, T.
- Открытый ключ – отображение $P = S \circ F \circ T$.
- Зашифрование: $m \in K^n, c = E(m) = P(m)$.
- Расшифрование: $x = S^{-1}(c), y = F^{-1}(x), m = T^{-1}(y)$.

Многочлены в “конкурсе” NIST-PQ

Криптосхемы

~~CFPKM~~, ~~Giophantus~~ (*), DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow, ~~SRTPI~~ (*), ~~DME~~.

Основанные на хэшировании схемы подписи

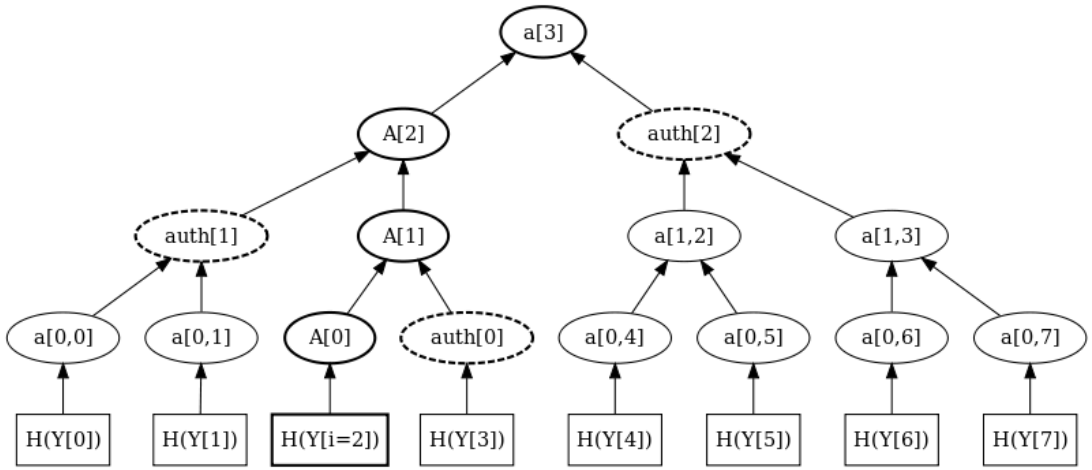
Стойкость схемы сводится к предположению о стойкости используемой хэш-функции.

Криптосхемы

- Древовидная подпись Меркля, 1979.
- XMSS (Бухманн, Дамен, Хюльзинг, 2001). Стандарт IEEE, 2015.
- SPHINCS (Бернштейн и др., 2015). Драфт IEEE, 2016.
- LMS

Основанные на хэшировании схемы подписи

Стойкость схемы сводится к предположению о стойкости используемой хэш-функции относительно задач поиска коллизий и/или прообразов.
Подпись строится на основе схем одноразовой подписи; может представлять собой путь в дереве специальным образом связанных хэш-значений.



Хэш в “конкурсе” NIST-PQ

Криптосхемы

SPHINCS+, GravitySPHINCS.

Изогении

Сложная задача – поиск пути в графе изогений между суперсингулярными эллиптическими кривыми над $GF(p^2)$. Классическая сложность – $O(p^{1/2})$; квантовая сложность – $O(p^{1/3})$.

Криптосхемы

- Ростовцев, Столбунов, 2006 – несуперсингулярные кривые, продемонстрирована эффективная квантовая атака.
- SIDH (Supersingular Isogeny Diffie-Hellman), де Фео, Плут, Яо, 2010.
- CSIDH, 2017.

Изогении в “конкурсе” NIST-PQ

SIKE.

Прочее в “конкурсе” NIST-PQ

Криптосхемы

~~WalnutDSA~~ (*) (группы кос);
pqRSA (юмор),
~~Guess Again~~ (*), ~~HK17~~ (*), Mersenne-756839, ~~RVB~~ (*) (октонионы),
Picnic.

Эффективность

Ориентировочные размеры параметров в байтах (V уровень стойкости)

Название	Тип	Длина с.к.	Длина о.к.	Длина ш.т. (подписи)
Lepton	Ш	80	4128	5557
Three Bears	Ш, ВОК	40	1584	1697
qTESLA	П	4128	6432	5920
Classic McEliece	Ш	13908	1047319	22
LEDAcrypt	ВОК/Ш	40	18016	9008
DILITHIUM	П	3856	760	3366
FrodoKEM	ВОК	31272	15632	15768
RQC	ВОК	3510	3510	3574
NTRU	Ш	6130	6734	140
SIKE	ВОК	826	726	766
Rainbow	П	1319000	871000	118
LUOV	П	32	39300	4700
SPHINCS	П	1024	1024	41800
Picnic	П	256	512	209474
RVB	ВОК	334	332	
WalnutDSA	П	1040	634	7704
pqRSA	Ш, П	25769803776	8589934592 (8 ТБ!)	8589934592
RSA, FF-DLP	П, Ш, ВОК	3 / 384	384	384
EC-DLP	П, Ш, ВОК	64	128	128

Коды — решетки — изогении — многочлены — хэш — прочее

“Конкурс” NIST-PQ, 2 этап

30 января 2019 года NIST опубликовал перечень кандидатов, прошедших на 2 этап конкурса.

- Для шифрования с открытым ключом и инкапсуляции ключа: BIKE, Classic McEliece, CRYSTALS-KYBER, FrodoKEM, HQC, LAC, LEDAcrypt (производная схема от LEDAkem/LEDApkc), NewHope, NTRU (производная схема от NTRUEncrypt/NTRU-HRSS-KEM), NTRU Prime, NTS-KEM, ROLLO (производная схема от LAKE/LOCKER/Ouroboros-R), Round5 (производная схема от Hila5/Round2), RQC, SABER, SIKE, Three Bears.
- Для схем цифровой подписи: CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow, SPHINCS+.

Коды — решетки — изогении — многочлены — хэш — прочее

PQCRYPTO

Программа ЕС “Horizon 2020”: предварительные рекомендации

- Блочный шифр: AES256, Salsa-20. Рассматривается: Serpent-256.
- Аутентификация: 128-бит GCM, Poly1305.
- Шифрование с открытым ключом: схема МакЭлиса на двоичных кодах Гоппы. Рассматриваются: QC-MDPC, NTRU.
- Подпись: XMSS, Sphincs+. Рассматривается: HFEv-.

IETF, IEEE

IETF

- RFC 8391: XMSS
- draft: LMS

IEEE

- NTRU: P1363/1

ISARA

ISARA – канадский производитель СКЗИ. Предлагаемые решения:

- QC-MDPC – схема инкапсуляции ключа
- qTESLA – схема подписи (2 этап конкурса NIST)

Выводы

- Имеется долгосрочная перспектива появления квантовых компьютеров достаточной производительности, что повлечет отказ от классических криптосхем с открытым ключом.
- Национальные и международные организации разворачивают работы по созданию постквантовых стандартизированных криптосхем.
- Появляются постквантовые криптосхемы, пригодные к практическому использованию.
- При этом есть проблемы, связанные с их “криптографической зрелостью”.
- Есть проблемы доверия, связанные с желанием внедрить ослабленные криптомеханизмы (Dual_EC_DRBG).

Выводы II

- Фундаментальные исследования в новых математических областях.
- Анализ деятельности международных и национальных организаций по стандартизации.
- Выбор наиболее перспективных синтезных решений.
- Разработка предложений по составу перспективного семейства национальных стандартов в области криптографии с открытым ключом.

Вопросы

- Нужен ли нам аналог конкурса NIST?
- Кто мог бы принять участие в этом конкурсе?
- Критерии оценки, эксперты?

Спасибо за внимание.

grebnev_sv@tc26.ru