Постквантовая криптография: вызов брошен

Сергей Гребнев

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

06 июня 2019

Классическая криптография с открытым ключом

Диффи-Хеллман-Меркль, 1976

$$x, A = g^x \xrightarrow{A} \qquad y, B = g^y$$

$$\xleftarrow{B}$$

$$B^x = g^{xy} = A^y$$

RSA, 1978

$$N = pq;\ e, d:$$

$$ed \equiv 1 \pmod{\phi(N)} \qquad \overset{N,e}{\rightsquigarrow}$$

$$\xleftarrow{c} \qquad c = m^e \pmod{N}$$

$$m = c^d \pmod{N}.$$

Классический криптоанализ

Обоснование стойкости криптосхемы

- Решаем математическую задачу X $\Rightarrow$ взламываем схему Y
- Много ученых думали много лет, но не придумали эффективного (полиномиального) способа решения X
- Много ученых думали много лет, но не придумали иного способа взлома Y (в идеале - доказали эквивалентность)

Основные задачи классического криптоанализа:

- факторизация натуральных чисел (RSA)
- дискретное логарифмирование в конечных полях (DSA, DH, ГОСТ Р 34.10-94)
- дискретное логарифмирование в группе точек эллиптических кривых (ECDSA, ECDH, ГОСТ Р 34.10-2012).

Можно считать, что эти схемы обеспечивают защиту 99.9% трафика в Интернете.

Классический криптоанализ vs квантовый

Основные криптоаналитические задачи в классической модели

- Факторизация целого числа N (RSA): NFS, $\exp[(1.902 + o(1))(\ln N)^{1/3})(\ln \ln N)^{2/3}]$ битовых операций
- Дискретное логарифмирование в конечном поле GF(p) (DSA, DH, ГОСТ Р 34.10-94): NFS, $\exp[(1.902+o(1))(\ln p)^{1/3})(\ln \ln p)^{2/3}]$ битовых операций
- Дискретное логарифмирование на эллиптической кривой E(GF(p)) (ECDSA, ECDH, ГОСТ Р 34.10-2012): ρ-метод, $O(\sqrt{q})$ операций на кривой
- Поиск коллизии n-битовой хэш-функции: $O(2^{n/2})$ операций хэширования
- Поиск прообраза n-битовой хэш-функции/блочного шифра: $O(2^n)$ операций хэширования/зашифрования

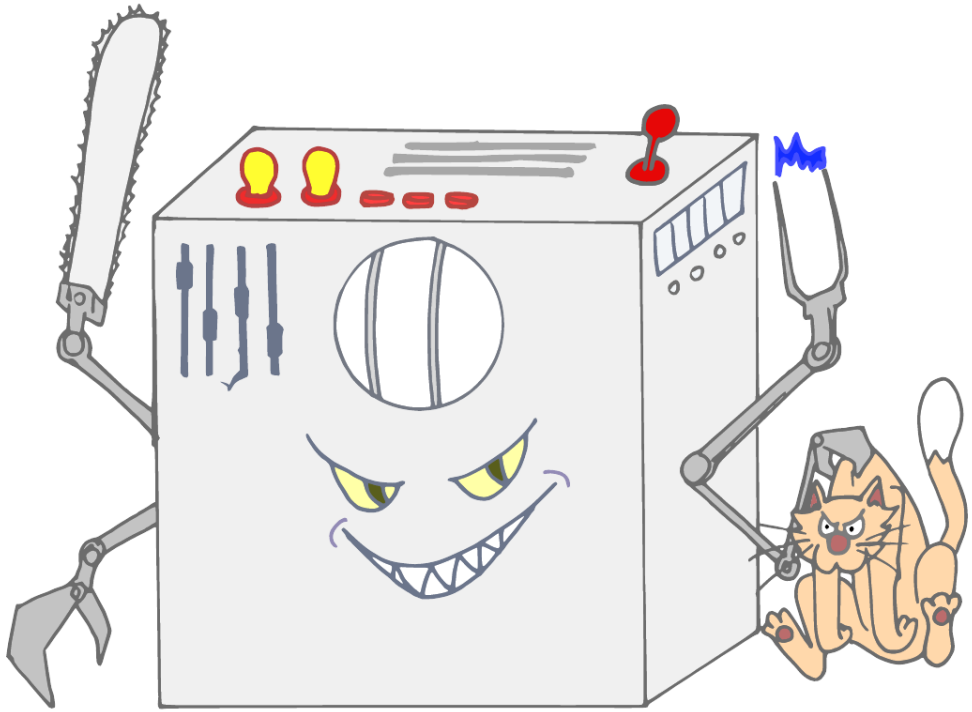
Классический криптоанализ

Практическая стойкость криптосхемы Y

Оценка стойкости – из вычислительной эквивалентности задачи взлома системы Y и блочного шифра с длиной ключа n.
Например:

Блочный шифр	RSA, FF-DLP	EC-DLP
128 (AES-128)	3072	256
256 (Кузнечик, AES-256)	15360	512

Те же, входит квантовый компьютер



Портрет злодея (Luca De Feo, 2018)

Классический криптоанализ vs квантовый

Основные криптоаналитические задачи в квантовой модели

- Факторизация целого числа N: метод Шора, $O(\ln^2 N)$ операций, $O(\ln N)$ кубитов
- Дискретное логарифмирование в конечном поле GF(p): метод Шора, $O(\ln^2 p)$ операций, $O(\ln p)$ кубитов
- Дискретное логарифмирование на эллиптических кривых E(GF(p)): метод Шора, $O(\ln^2 q)$ операций, $O(\ln q)$ кубитов
- Поиск коллизии n-битовой хэш-функции: метод BHT, $O(2^{n/3})$ операций, $O(2^{n/3})$ кубитов
- Поиск прообраза n-битовой хэш-функции/блочного шифра: метод Гровера, $O(2^{n/2})$ операций, $O(n)$ кубитов

Как противостоять квантовому криптоанализу?

Увеличение размеров параметров

- Факторизация целых чисел: экспоненциально
- Дискретное логарифмирование в конечном поле: экспоненциально
- Дискретное логарифмирование на эллиптических кривых: экспоненциально
- Поиск коллизий ($f : V_{2n} \mapsto V_n$): увеличение длины блока в 3 раза
- Поиск прообраза ($f : V_n \mapsto V_n$): увеличение длины ключа/блока в 2 раза

Квантовое настоящее и будущее

Настоящее

- IBM: 20-50 кубитов (9 м^3), облачный доступ
- Google: 72 кубита
- D-Wave: 1152 “кубита”, Google, NASA
- ЦКТ МГУ – анонсируют 50 кубитов к 2021 году

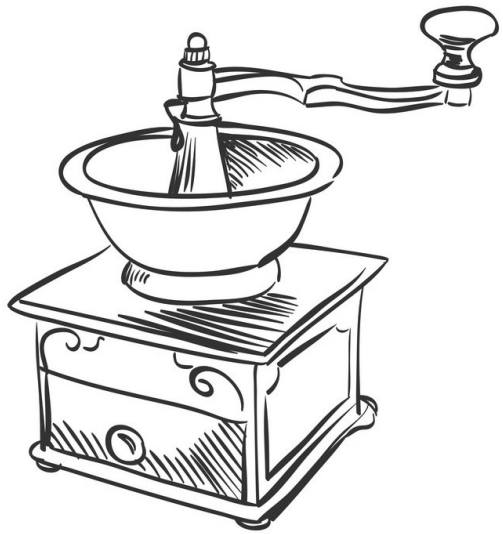
Будущее

- Оценка возможности появления квантовых компьютеров достаточной для задач криптоанализа производительности (RSA: $\geq$ 2730 логических, 20×10^6 физических кубитов): $10 - 40 - \infty$ лет
- Необходимость создания постквантовых криптосхем: сейчас

Квантовая криптография – не панацея

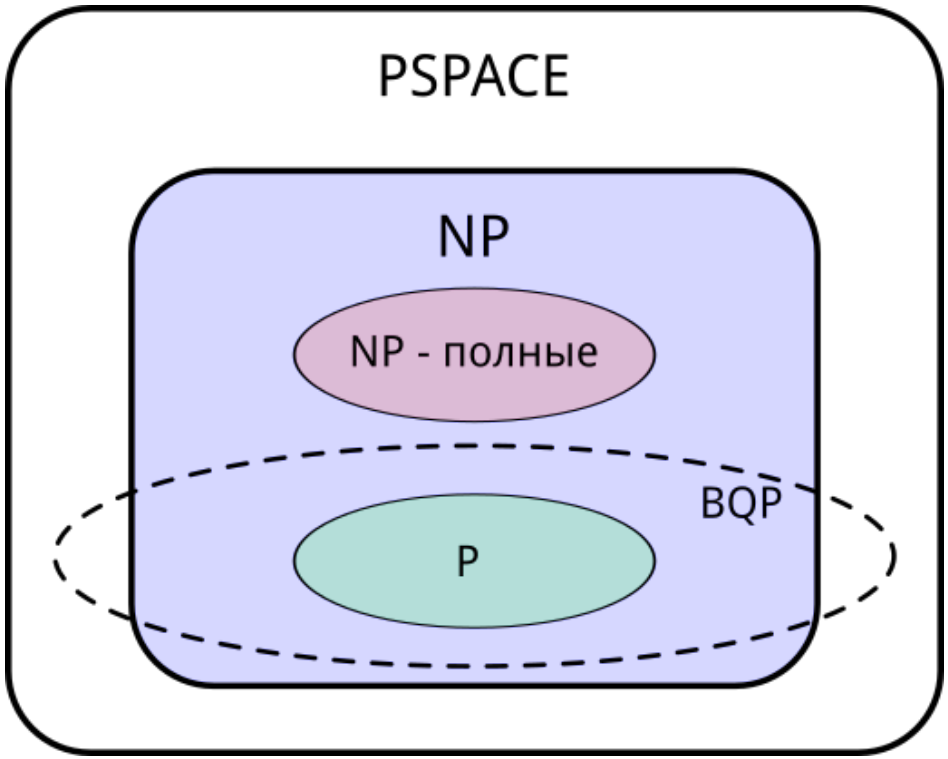
- Дороговизна оборудования.
- Ограниченная дальность связи – десятки километров.
- Малое быстродействие.

Только важнейшие направления связи. Невозможно снабдить оборудованием все устройства (особенно IoT).



Возможна ли постквантовая криптография?

Классы сложности



PSPACE – полиномиальная по памяти; P – полиномиальная по кол-ву операций; NP – неполиномиальная; BQP – квантовая полиномиальная с ошибкой не более 1/3

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. – опубликованы результаты I этапа.
30 марта 2019 г. – доработка схем, прошедших во II этап, с учетом поступивших замечаний.
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 (**IND-CPA**).
- К угрозе различения шифртекстов относительно атаки на основе подобранного шифртекста (**IND-CCA**).
- К угрозе различения шифртекстов относительно атаки на основе (неадаптивно) подобранного открытого текста (**IND-CPA1**).
- К угрозе различения шифртекстов относительно атаки на основе (неадаптивно) подобранного шифртекста (**IND-CCA1**).
- К угрозе различения шифртекстов относительно атаки на основе адаптивно подобранного открытого текста (**IND-CPA2**).
- К угрозе различения шифртекстов относительно атаки на основе адаптивно подобранного шифртекста (**IND-CCA2**).

Определения теоретической стойкости

Для схем подписи

- Сильная стойкость к подделке относительно атак на основе подобранных сообщений (**SUF-CMA**).
- Стойкость к экзистенциальной подделке относительно атак на основе подобранных сообщений (**EUF-CMA**).

Уровни практической стойкости

Уровни и эквивалентные задачи

I уровень	определение ключа 128-битового блочного шифра;
II уровень	поиск коллизии 256-битовой хэш-функции;
III уровень	определение ключа 192-битового блочного шифра;
IV уровень	поиск коллизии 384-битовой хэш-функции;
V уровень	определение ключа 256-битового блочного шифра.

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, I этап

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

Теория решеток

Трудные 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) – шифрование, подпись.
- BLISS (Дукас и др., 2013) (CVP, не доказано)
- RLWE-KEX (Регев и др., 2005) (RLWE – предположительно сводится к CVP)
- 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: $as + e$, $as' + e'$; общий ключ $v = ass' + e's \approx ass' + es'$; s, s', e, e' – малы относительно некоторой нормы.

Теория решеток - пример

Криптосхема GGH

- Секретный ключ – базис $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, унимодулярная матрица U
- Открытый ключ – базис $B = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = UR$
- Зашифрование: $c = E(m) = mB + e$
- Расшифрование: $D(c) = cB^{-1} = cUBB^{-1}$; ошибка eB^{-1} “мала” и удаляется округлением

Анализ: сводится к частному случаю задачи CVP.

Теория решеток в “конкурсе” 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.

(~~схема взломана~~; (*) – опубликована атака)

Теория кодирования

Трудная 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

Трудная 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: $x = S^{-1}(c), y = F^{-1}(x), m = T^{-1}(y)$.

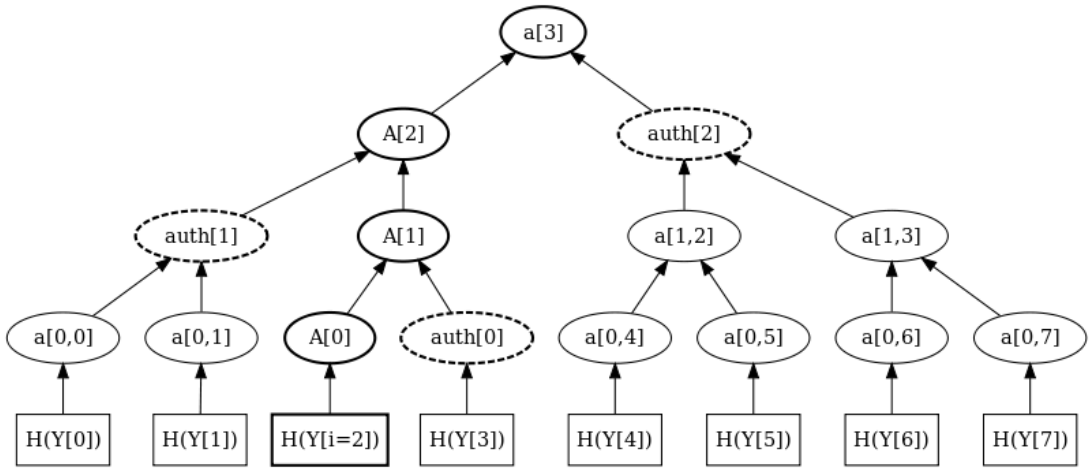
Многочлены в “конкурсе” NIST-PQ

Криптосхемы

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

Основанные на хэшировании схемы подписи

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



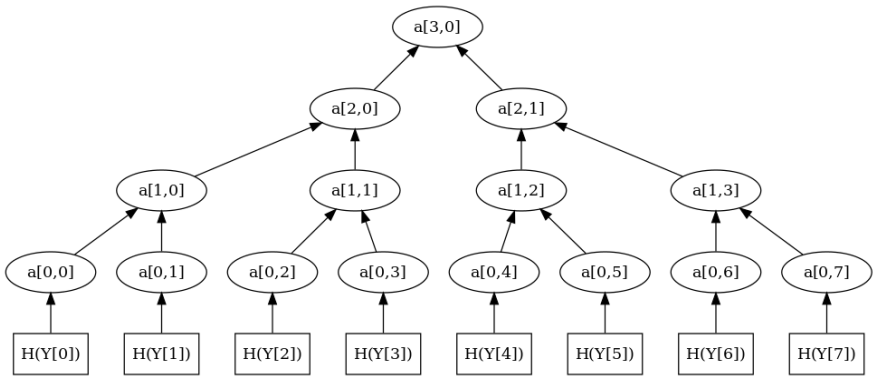
Основанные на хэшировании схемы подписи

Криптосхемы

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

Схема Меркля

- $N = 2^n$ – максимальное количество сообщений; одноразовая подпись (например, схема Лампорта); хэш-функция H.
- Построить N пар (X_i, Y_i) секретных/открытых ключей; вычислить $h_i = H(Y_i)$, построить дерево



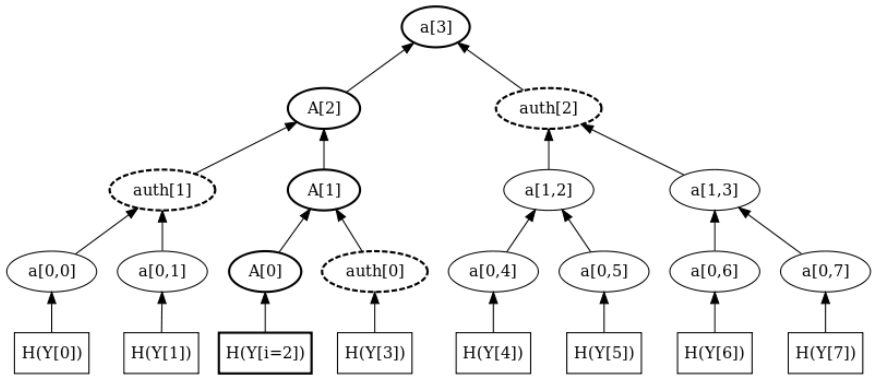
$(a[0, i] = h_i$ – листья; $a[1, 0] = H(a[0, 0] \parallel a[0, 1]))$

- Секретный ключ $\{X_i, Y_i\}$; открытый ключ $P = a[n, 0]$ (корень).

Схема Меркля

Выработка подписи:

Выбрать неиспользованную пару (X_i, Y_i), вычислить соответствующую одноразовую подпись S', построить путь от листа до корня $(A_0, \ldots, A_n)$, определить auth_i $(i = 0, \ldots, n-1)$ как другой лист соответствующей ветки, такой, что $A_{i+1} = H(A_i \parallel \text{auth}_i)$.
Подпись равна $S = (S' \parallel X_i \parallel Y_i \parallel \text{auth}_0 \parallel \cdots \parallel \text{auth}_{n-1})$.



Проверка подписи:

Подпись верна, если S' – верная одноразовая подпись, и при этом $A_n = P$, где $A_j = H(A_{j-1} \parallel \text{auth}_{j-1})$, $j = 1, \ldots, n$.

Хэш в “конкурсе” NIST-PQ

Криптосхемы

SPHINCS+, GravitySPHINCS.

Изогении

Трудная 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, 2011.
- CSIDH, 2017.

Изогении в “конкурсе” NIST-PQ

SIKE.

Схема деФео-Яо-Плута

$p = l_A^{e_A} l_B^{e_B} \cdot f \pm 1, (l_A, f) = (l_B, f) = 1$, суперсингулярная э.к. $E_0(GF(p^2))$ и базисы $\{P_A, Q_A\}$ и $\{P_B, Q_B\}$, которые порождают, соответственно, $E_0[l_A^{e_A}]$ и $E_0[l_B^{e_B}]$.
Абонент A выбирает $m_A, n_A \in_R \mathbb{Z}/l_A^{e_A}\mathbb{Z}$, и строит изогению $\varphi_A : E_0 \to E_A$ с ядром $K_A := \langle [m_A]P_A + [n_A]Q_A \rangle$. Абонент A также вычисляет образ $\{\varphi_A(P_B), \varphi_A(Q_B)\}$ и посылает их B вместе с э.к. E_A. Абонент B выбирает $m_B, n_B \in_R \mathbb{Z}/l_B^{e_B}\mathbb{Z}$, и строит изогению $\varphi_B : E_0 \to E_B$ с ядром $K_B := \langle [m_B]P_B + [n_B]Q_B \rangle$. Абонент B также вычисляет образ $\{\varphi_B(P_B), \varphi_B(Q_B)\}$ и посылает их и E_B абоненту A.
Абонент A строит изогению $\varphi'_A : E_B \to E_{AB}$ с ядром $\langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle$.Общий ключ – j-инвариант кривой

$$E_{AB} = \varphi' B(\varphi_A(E_0)) = \varphi'_A(\varphi_B(E_0)) = \\ = E_0 / \langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle .$$

Эзотерика в “конкурсе” NIST-PQ

Криптосхемы

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

Эффективность I

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, Ш	3510	3510	3574
NTRU	Ш	6130	6734	140
NewHope	ВОК	3680	1824	2208
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
WalnutDSA	П	1040	634	7704
pqRSA	Ш, П	25769803776	8589934592 (8 Тб!)	8589934592
RSA, FF-DLP	П, Ш, ВОК	3 / 1920	1920	1920
EC-DLP	П, Ш, ВОК	64	128	128

Коды — решетки — изогении — многочлены — хэш — прочее

Эффективность II

Производительность (тыс. циклов на сообщение)

Название	Тип	Прямая операция	Обратная операция
Lepton	Ш	244	282
Three Bears	Ш, ВОК	145	213
qTESLA	П	26063	1310
Classic McEliece	Ш	3000	450
DILITHIUM	П	711	288
FrodoKEM	ВОК	3577	3580
RQC	ВОК, Ш	6460	18000
NTRU	Ш	59	97
NewHope	ВОК	210	220
SIKE	ВОК	14995	17957
Rainbow	П	8688	6174
LUOV	П	216000	124000
SPHINCS	П	164592	3975
pqRSA	Ш, П	22×10^9	$1,8 \times 10^9$
RSA	П, Ш, ВОК	75000	5000
EC-DLP	П, Ш, ВОК	400	600

Коды — решетки — изогении — многочлены — хэш — прочее

“Конкурс” NIST-PQ, II этап

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

- Для шифрования с открытым ключом и инкапсуляции ключа – 16 схем: 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 цифровой подписи – 9 схем: 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 etc

IETF

- RFC 8391: XMSS
- RFC 8554: LMS

IEEE

- NTRU: P1363/1

ISARA

Канадский производитель СКЗИ. Предлагаемые решения:

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

OQS

OpenQuantumSafe (University of Waterloo).
liboqs: BCNS15; NewHope; Frodo; NTRU; McBits.

Основные проблемы

Научно-методические

- Недостаток “криптографической зрелости”.
- Возрастающая сложность понятийного аппарата.
- Усложнение методов синтеза и анализа, в том числе квантового.

Политические

- Априори подозрительное отношение к новым решениям в пост-сноуденовскую эру.
- Инертность регуляторов, производителей и пользователей.
- Неясная степень угрозы.

Основные проблемы

Практические

- Сложность реализации.
- Низкая эффективность – большие размеры параметров, низкое быстродействие.

Выводы

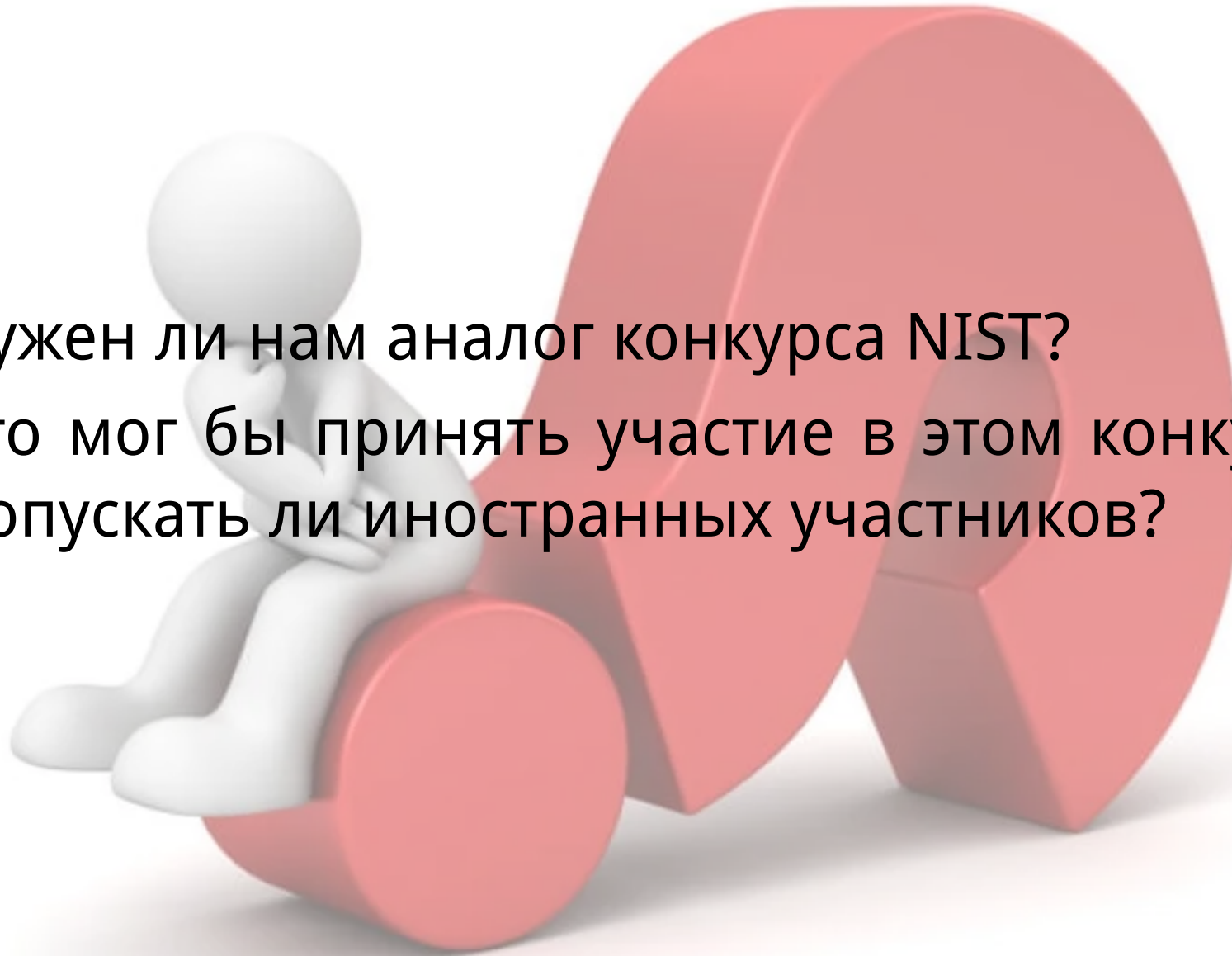
- Имеется долгосрочная перспектива появления квантовых компьютеров достаточной производительности, что повлечет отказ от классических криптосхем с открытым ключом.
- Национальные и международные организации разворачивают работы по созданию постквантовых стандартизированных криптосхем.
- Появляются постквантовые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

Выводы II

Необходимые направления исследований

- 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? Допускать ли иностранных участников?

Спасибо за внимание.

grebnev_sv@tc26.ru