Открытые вопросы в пост-квантовой криптографии

aka ToDo лист криптографа исследователя

Екатерина Малыгина, Семён Новоселов
Елена Киршанова, Никита Колесников

ИНФОБЕЗ - 2019: ПРОБЛЕМЫ, МЕТОДОЛОГИИ, ТЕХНОЛОГИИ
БФУ им. И. Канта, Калининград
22 октября 2019 г.

Балтийский федеральный университет имени Иммануила Канта

Что такое “пост-квантовая криптография”? –

– это классические крипто-протоколы стойкие к атакам на квантовом компьютере

Расшифруем

- классические = эффективны на современных устройствах
- крипто-протоколы = {шифрование, цифровая подпись}
- стойкие к атакам = мы не знаем эффективного алгоритма для задачи, лежащей в основе протокола
- на квантовом компьютере = злоумышленник имеет доступ к квантовому компьютеру с необходимым количеством кубит [1]

[1] Чтобы факторизовать n-бит RSA, нужно $(\frac{3}{2} + o(1))n$ логических кубит, [EH17]

Чем не устраивает RSA/ECDH/ГОСТ?

Чем не устраивает RSA/ECDH/ГОСТ?

- всем устраивает, но

Чем не устраивает RSA/ECDH/ГОСТ?

- всем устраивает, но
- задачи факторизации (RSA) и дискретного логарифма (ECDH/ГОСТ) решаются на квантовом за полиномиальное (!) от уровня безопасности время (алгоритм Шора); при этом квантовый компьютер не обязан быть “мощным”

Чем не устраивает RSA/ECDH/ГОСТ?

- всем устраивает, но
- задачи факторизации (RSA) и дискретного логарифма (ECDH/ГОСТ) решаются на квантовом за полиномиальное (!) от уровня безопасности время (алгоритм Шора); при этом квантовый компьютер не обязан быть “мощным”
- успехи в классических алгоритмах факторизации, dlog: от экспоненциальных до суб-экспоненциальных. Рекомендованный размер ключа сегодня RSA 4096 бит (в 90-е: 463 бит).

Чем не устраивает RSA/ECDH/ГОСТ?

- всем устраивает, но
- задачи факторизации (RSA) и дискретного логарифма (ECDH/ГОСТ) решаются на квантовом за полиномиальное (!) от уровня безопасности время (алгоритм Шора); при этом квантовый компьютер не обязан быть “мощным”
- успехи в классических алгоритмах факторизации, dlog: от экспоненциальных до суб-экспоненциальных. Рекомендованный размер ключа сегодня RSA 4096 бит (в 90-е: 463 бит).
- в ближайшее время – стандарт в США ($\Longrightarrow$ OpenSSL, TLS и т.д.)
- красивая математика в пост-квантовых протоколах ☺

Шо там у них

- Декабрь 2016: NIST (агентство стандартизации США) запускает конкурсный отбор пост-квантовых криптографических схем для стандартизации
- Июль 2017: Google анонсирует запуск тестовой версии пост-квантовой схемы передачи ключа New Hope в браузере Chrome Canary[2]
- Январь 2019: NIST выбрал 26 кандидатов для второго раунда конкурса
- Январь 2019: Cloudflare анонсировала две реализации пост-квантовых обменов ключами для TLS 1.3
- Июнь 2020: NIST планируем выбрать протоколы для стандартизации

[2] https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html

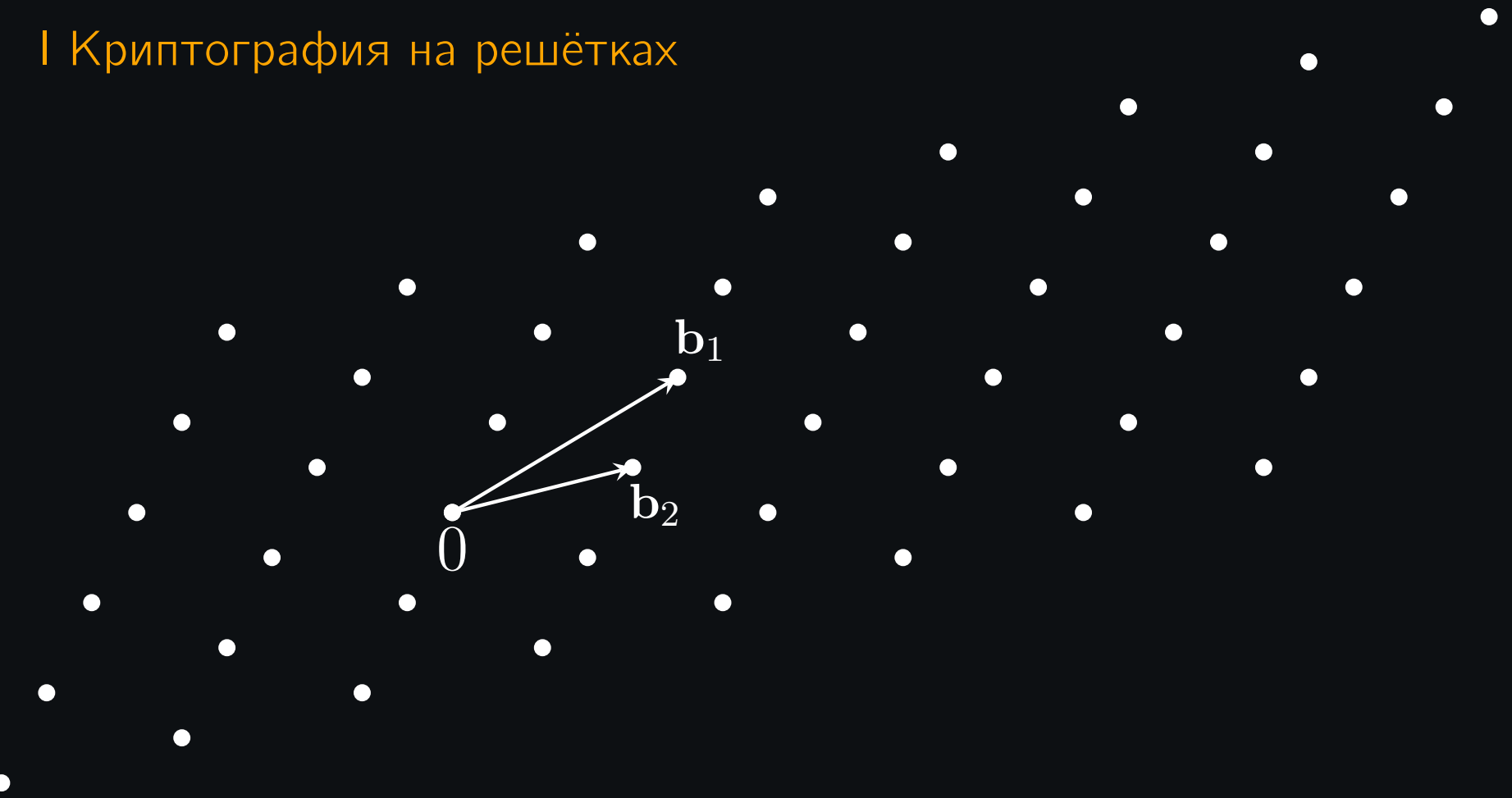
Основные направления пост-квантовой криптографии

I Криптография на решётках

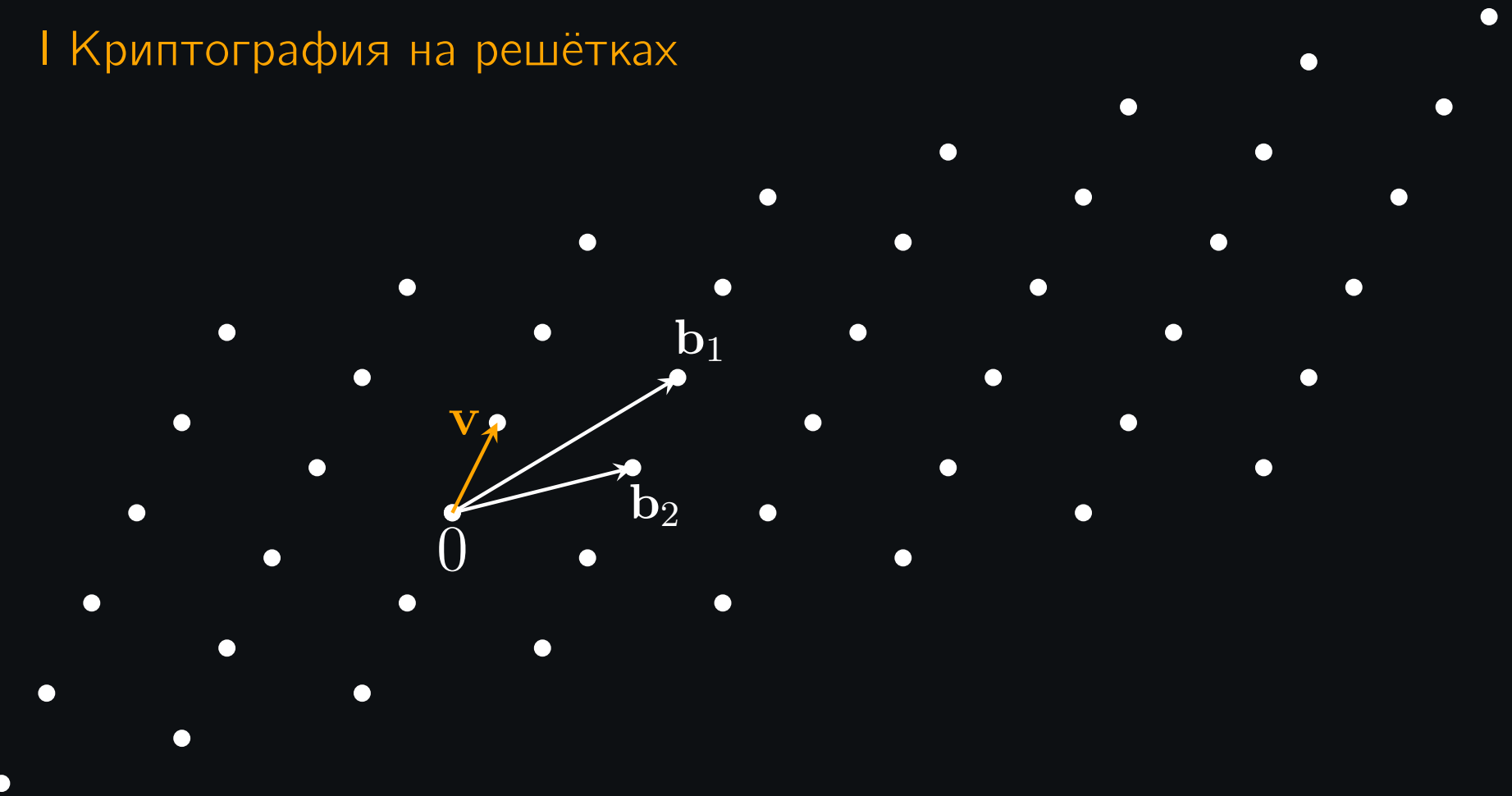
II Криптография на кодах

III Криптография на изогениях

Кроме этого: схемы подписи на системах полиномиальных уравнений и хэш-функциях (à la подпись Лэмпорта).



Решётка – это множество $\mathcal{L} = \{\sum_{i \le n} x_i \mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ для лин. независимых $\mathbf{b}_i \in \mathbb{R}^n$



Решётка – это множество $\mathcal{L} = \{\sum_{i \le n} x_i \mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ для лин. независимых $\mathbf{b}_i \in \mathbb{R}^n$

Задаче поиска кратчайшего вектора: найти $\mathbf{v} \in \mathcal{L}$:

$$\|\mathbf{v}\| = \min_{\mathbf{x} \neq 0 \in \mathcal{L}} \|\mathbf{x}\|$$

I Криптография на решётках

- эффективные конструкции
- широкий спектр примитивов (гомоморфное шифрование)
- большое внимание со стороны криптоанализа

- понимание сложности задачи короткого вектора для особых решёток
- реализация атак

По $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}, \mathbf{s} \in \mathbb{F}_2^{n-k}$, найти $\mathbf{e} \in \mathbb{F}_2^n$ малого веса Хэмминга такой, что $\mathbf{He} = \mathbf{s}$

II Криптография на кодах

- очень большое внимание со стороны криптоанализа за последние 50 лет
- “вера” в надежность конструкций

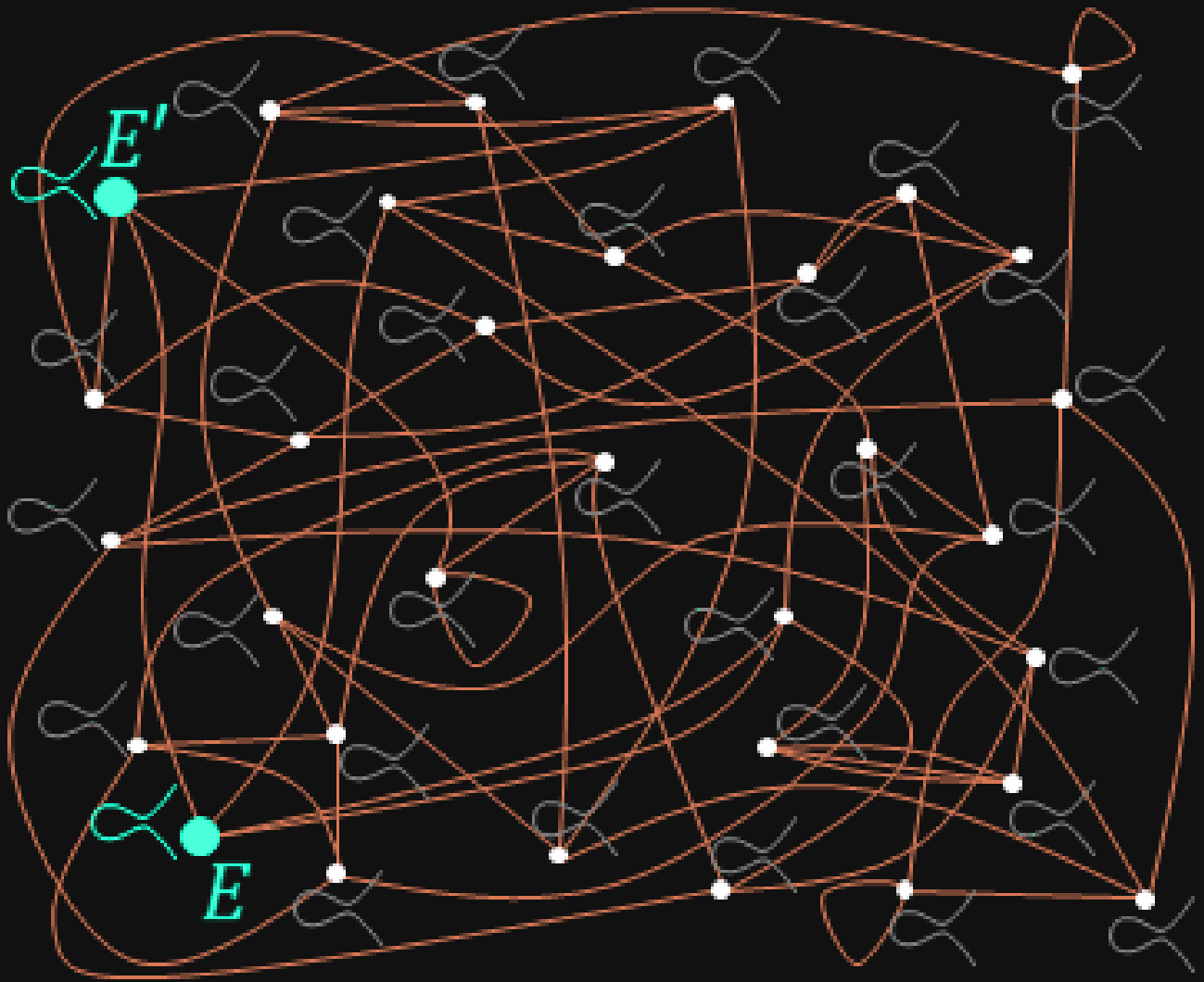
- большие размеры ключей
- реализация атак

Изогения - неконстантное рациональное отображение ϕ между двумя эллиптическими кривыми как алг. многообразиями

$$\phi : E \to E'$$

$$\phi(x, y) = \left(\frac{f_1(x)}{f_2(x)}, \frac{g_1(x)}{g_2(x)} \right)$$

Задача: по данным E, E' найти $\phi : E \to E'$



W. Castryck (GIF): https://www.esat.kuleuven.be/cosic/?p=7404

III Криптография на изогениях

- малый размер ключей
- красивая математика

- неэффективные алгоритмы генерации ключей
- слабо исследовано исследована сложность задачи

Наши исследования в этих областях

1. Криптоанализ систем на решётках: теоретический (асимптотика) и практический (реализация атак)
   Коллаборации: ENS Lyon, CWI, Royal Holloway, Lund University

2. Криптоанализ систем на кодах, построение эффективных кодов
   Коллаборации: Ruhr Universität Bochum

3. Квантовый криптоанализ
   Коллаборации: Ruhr Universität Bochum, University of Oxford

4. Эффективные алгоритмы вычисления изогений

Наша команда

Екатерина Малылина, к.ф-м.н.
Фокус: Алгебраическая геометрия, АГ коды

Семен Новоселов, ассистент
Фокус: Эффективные алгоритмы подсчёта точек

Никита Колесников, аспирант
Фокус: Коды, алг. кривые

Елена Киршанова, PhD
Фокус: Решётки, криптоанализ

Текущая научная работа

1. Построение / обобщение криптографических схем на изогениях алгебраических кривых

2. Криптоанализ алгебраических решёток (NTRU, RingLWE)

3. Криптоанализ кандидатов NIST, построенных на кодах (McEliece)

Текущая научная работа

1. Построение / обобщение криптографических схем на изогениях алгебраических кривых

2. Криптоанализ алгебраических решёток (NTRU, RingLWE)

3. Криптоанализ кандидатов NIST, построенных на кодах (McEliece)

Спасибо за внимание!

crypto-kantiana.com