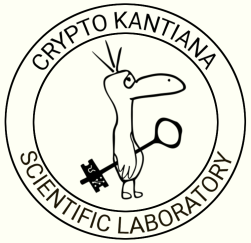
# Эллиптические кривые

## Лекция 11. Схема подписи SQISign

Семён Новосёлов

БФУ им. И. Канта

2026




IKBFU

# Введение

**SQISign** (Short Quaternion and Isogeny Signature) – схема подписи, построенная применением преобразования Фиата-Шамира к протоколу доказательства с нулевым разглашением (Σ-протоколу).

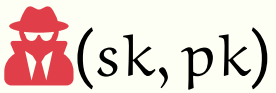
- De Feo L., Kohel D., Leroux A., Petit C., Wesolowski B.
  “SQISign: compact post-quantum signatures from quaternions and isogenies”.
  AsiaCrypt 2020. `https://eprint.iacr.org/2020/1240`

Последняя версия схемы:

- `https://sqisign.org`

# $\Sigma$-протокол

Позволяет доказать знание секрета без раскрытия самого секрета.







сген. обязательство $\mathrm{com}$ $\xrightarrow{\mathrm{com}}$ ...

... $\xleftarrow{\mathrm{chl}}$ сген. вызов $\mathrm{chl}$

сген. ответ $\mathrm{rsp}$ $\xrightarrow{\mathrm{rsp}}$ ...

вернуть “accept” или “reject”

# Преобразование Фиата-Шамира

Позволяет построить цифровую подпись из любого Σ-протокола.

- $\mathrm{m}$ – сообщение для подписи
- при генерации $\mathrm{chl}$ заменяем  на хэш-функцию:

$$\mathrm{chl} = \mathrm{hash}(\mathrm{m}||\mathrm{com})$$

- **подпись** $\mathrm{s} := (\mathrm{com}, \mathrm{rsp})$
- **проверка**: вычисляем $\mathrm{chl} = \mathrm{hash}(\mathrm{m}||\mathrm{com})$ и проверяем условие Σ-протокола

# Подпись SQISign. Параметры

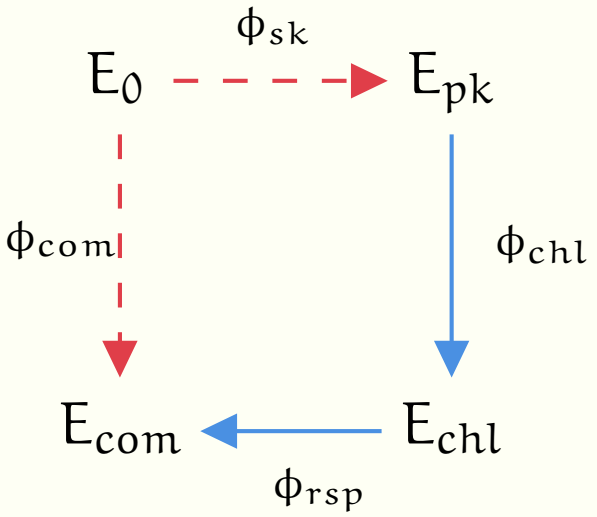
- $E_0$ – (открытая) кривая с известным $\mathrm{End}(E_0)$
- $\phi_{sk} : E_0 \to E_{pk}$ – случайная секретная изогения
- $E_{pk}$ – открытый ключ
- $\mathrm{End}(E_{pk})$ – секретный ключ

**Замечание:**

- зная $\phi : E_0 \to E$ можно вычислить $\mathrm{End}(E)$ за полиномиальное время
- зная $\mathrm{End}(E_1)$ и $\mathrm{End}(E_2)$ можно вычислить изогению $\phi : E_1 \to E_2$ за полиномиальное время

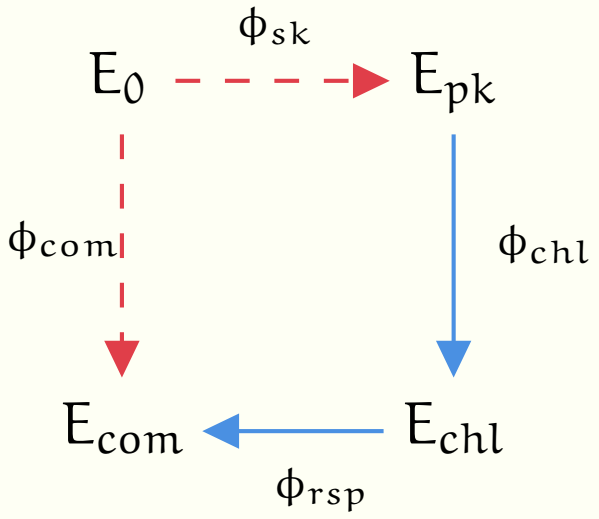
# Подпись SQISign. $\Sigma$-протокол

1. генерирует секретную $\phi_{com}$, отсылает $E_{com}$
2. генерирует случ. $\phi_{chl}$, отправляет $\phi_{chl}$
3. вычисляет и отправляет $\phi_{rsp}$
4. проверяет, что $\phi_{rsp}$ – изогения $E_{chl} \to E_{com}$



# Подпись SQISign. $\Sigma$-протокол

1. генерирует секретную $\phi_{com}$, отсылает $E_{com}$
2. генерирует случ. $\phi_{chl}$, отправляет $\phi_{chl}$
3. вычисляет и отправляет $\phi_{rsp}$
4. проверяет, что $\phi_{rsp}$ – изогения $E_{chl} \to E_{com}$




**Корректность:**

- знает $\mathrm{End}(E_0)$ и $\phi_{com}$ $\Longrightarrow$ вычисляет $\mathrm{End}(E_{com})$
- знает $\mathrm{End}(E_{pk})$ и $\phi_{chl}$ $\Longrightarrow$ находит $\mathrm{End}(E_{chl})$
- знает $\mathrm{End}(E_{chl}), \mathrm{End}(E_{com})$ $\Longrightarrow$ вычисляет $\phi_{rsp}$

# Подпись SQISign. Преобразование Фиата-Шамира

**Генерация** $\mathrm{chl}$:

$$\mathrm{chl} = \mathrm{hash}(\mathrm{j}(\mathrm{E}_{\mathrm{pk}})||\mathrm{j}(\mathrm{E}_{\mathrm{com}})||\mathrm{m}),$$

$\phi_{\mathrm{chl}}$ строится детерминировано по $\mathrm{chl}$.

**Подпись:** $\mathrm{s} := (\mathrm{E}_{\mathrm{com}}, \phi_{\mathrm{rsp}})$

**Проверка:** находим $\phi_{\mathrm{chl}}$ и проверяем, что $\phi_{\mathrm{rsp}}$ – изогения $\mathrm{E}_{\mathrm{chl}} \to \mathrm{E}_{\mathrm{com}}$.

# Представление изогений

- $\phi_{\mathrm{chl}}$, $\phi_{\mathrm{rsp}}$ – открыты
- от представления зависит размер подписи и скорость проверки
- представление изогений **не должно** давать возможность вычислять эндоморфизмы:
  - по одному эндоморфизму кривой $\mathrm{E}$ можно вычислить $\mathrm{End}(\mathrm{E})$ за полиномиальное время

# SQISign. Оригинальная схема

- изогении представляются в виде сжатых ядер цепочек изогений малой степени
- $\phi_{\mathrm{rsp}}$ вычисляется с помощью KLPT-алгоритма

# SQISignHD

- конструктивное применение атаки Кастрика-Декру
- изогении представляются в компактном виде $(d, E_{aux}, \phi(P), \phi(Q))$
- проверке подписи выполняется Кастрика-Декру

# SQIPrime

- вместо композиций изогений малых степеней используются изогении большой степени и новый алгоритм для их вычисления Clapoti

# Размеры ключей/скорость

| Схема | Уровень стойкости | Открытый ключ | Закрытый ключ | Подпись |
|---|---|---|---|---|
| SQISign | NIST-1 | 64 | 16 | 204 |
| SQISignHD | NIST-1 | 64 | 16 | 109 |
| SQISign2D-West | NIST-1 | 65 | 353 | 148 |
| SQIPrime | NIST-1 | 191 | ~ | 299 |

**Таблица 1:** Размеры ключей (в байтах) для схем подписи на изогениях.

# Скорость работы

| | Key gen. | Signing | Verif. |
|---|---|---|---|
| **Original SQIsign** | 2800 | 4600 | 93 |
| **Optimized SQIsign** | 400 | 1880 620ms | 29 10ms |
| **SQIsignHD** | 190 | 115 38ms | ? |
| **SQIsign2D-West** | 60 | 160 53ms | 9 3ms |
| **SQIsign2D-West + heuristics** | 58 | 100 33ms | 9 |

For NIST-V security level: cost x6

- Источник: Benjamin Wesolowski, ECC2024

# Литература


- Boneh D., Shoup V. “Graduate Course in Applied Cryptography” `https://toc.cryptobook.us`
- SQIsign: Algorithm specifications and supporting documentation. `https://sqisign.org/spec/sqisign-20250707.pdf`



Контакты

snovoselov@kantiana.ru