

Fiat-Shamir Code

Denis Fomin and Anton Guselev

Academy of Cryptography of the Russian Federation

Эволюция схем подписи на основе кодов

1994: Протоколы идентификации

Штерн предложил протокол идентификации, основанный на задаче синдромного декодирования. Это открыло путь к созданию схем подписи.

1

2001: Схема CFS

Появилась схема CFS, использующая идеи алгоритма асимметричного шифрования МакЭлиса. Несмотря на недостатки оригинальной схемы, она стала основой для многих последующих разработок (hash-and-sign).

3

1997: Схема KKS

Предложена неэффективная схема, допускающая только однократное использование ключа. Были найдены эффективные методы криптографического анализа.

2

2022: MPC-in-the-Head

Появилась новейшая концепция, основанная на идее использования протокола многосторонних вычислений, реализуемого на стороне пользователя, формирующего подпись. Ее безопасность ещё требует изучения.

4

Конкурс NIST и перспективы

NIST
2016

Конкурс NIST 2016

Схемы pqsigRM, RaCoSS, RankSign (на основе CFS) были сняты из-за уязвимостей или отзыва авторами.

NIST
2022

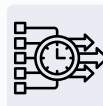
Конкурс NIST 2022

Из 40 представленных схем, 6 были на основе кодов. Три из них — это варианты CFS, три — на основе протокола идентификации (CROSS, LESS, MEDS).



Результаты первого конкурса

Только две схемы на основе кодов прошли во второй этап: CROSS и LESS. Обе используют протоколы идентификации.



Будущее

Схемы на основе протоколов идентификации зарекомендовали себя наиболее перспективными. Выбор базового кода критичен для безопасности и эффективности.

Выбор базового кода является ключевым аспектом, влияющим на безопасность и эффективность схем подписи.

Дальнейшие исследования будут сосредоточены на универсальных характеристиках, определяемых протоколом идентификации и преобразованием Фиата-Шамира.

Классификация протоколов идентификации

Группа 1: $p = \frac{2}{3}$

Включает протоколы Штерна и Верона.

Для их реализации требуется **3 пересылки**.

Группа 2: $p = \frac{1}{2}$

Яркий пример — протокол CVE (Cayrel, Véron, El Yousfi), а также CROSS, LESS и MEDS (NIST 2022).

Для реализации требуется **3 или 5 пересылок**.

Группа 3: $p = \frac{1}{n}$

Включает протоколы, основанные на Штерне и CVE.

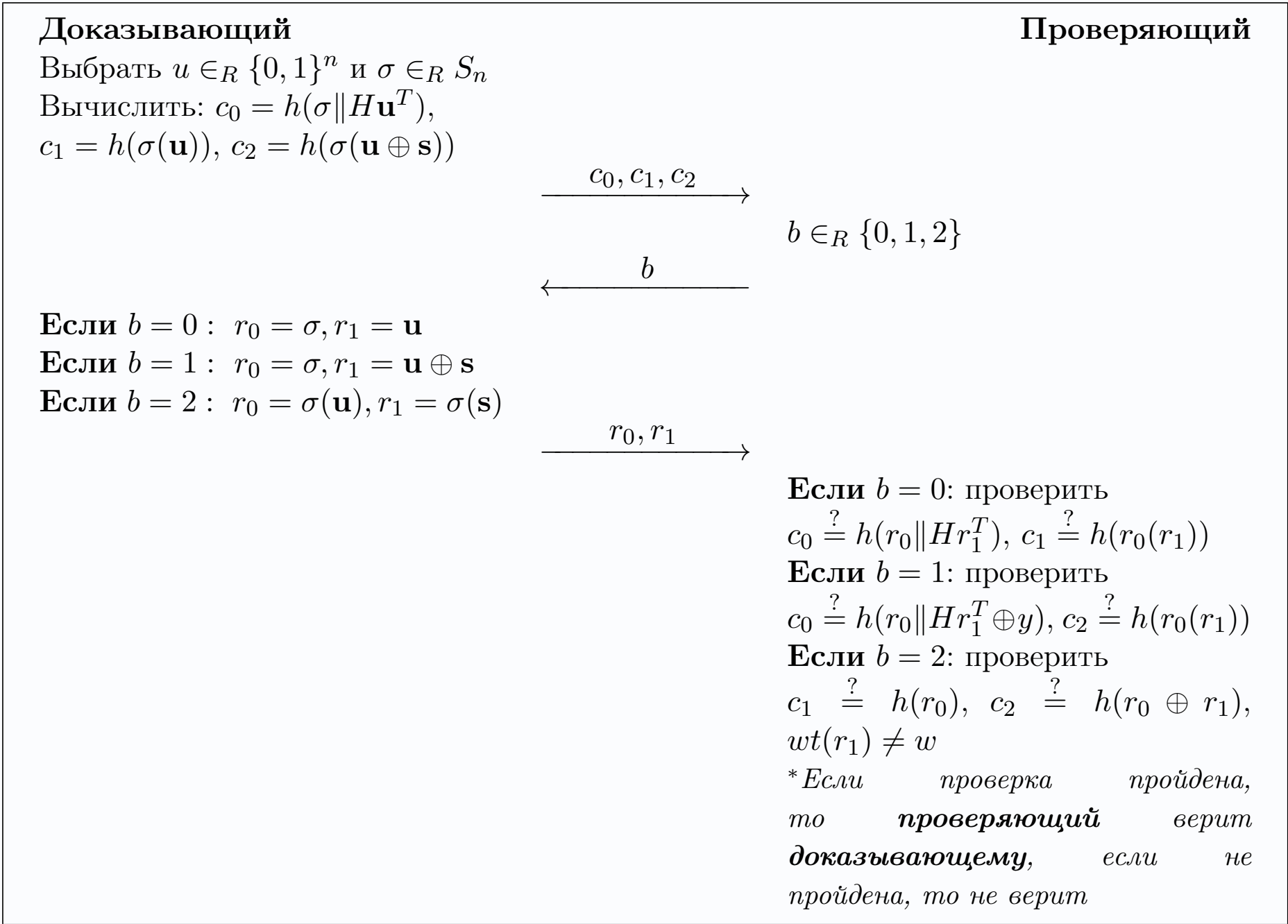
Для реализации требуется **3 или 5 пересылок**.

Группа 4: Принцип Шнорра

Наиболее яркий пример — протокол Durandal.

Для реализации требуется **3 пересылки** без вариативности последней.

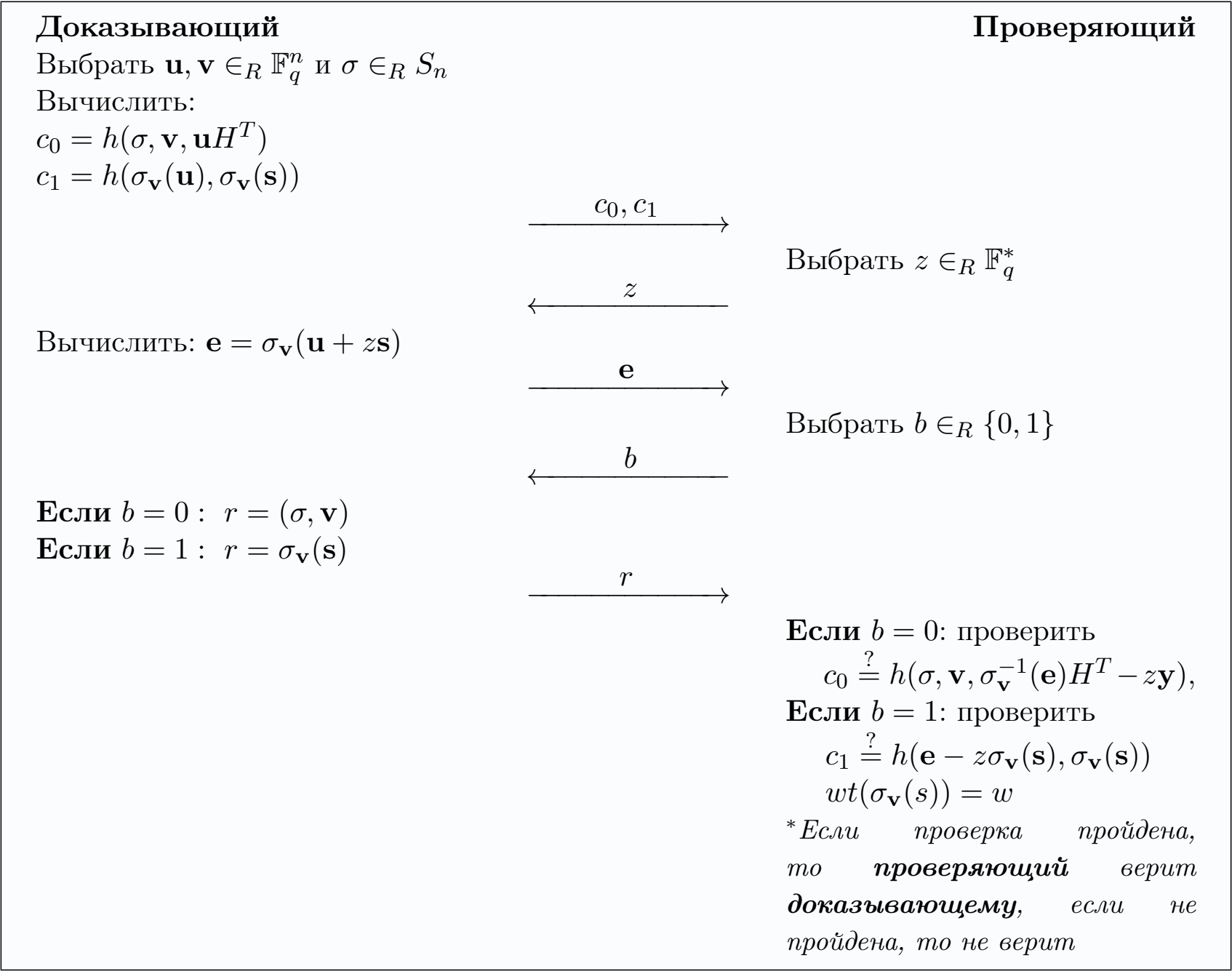
Протокол Штерна $p = 2/3$



Цель:
Доказательство знания
секретного вектора $\mathbf{s} \in \mathbb{F}_2^n$,
такого, что $wt(\mathbf{s}) = t$

Таблица 1 – Протокол идентификации Я. Штерна.

Протокол CVE $p = 1/2$

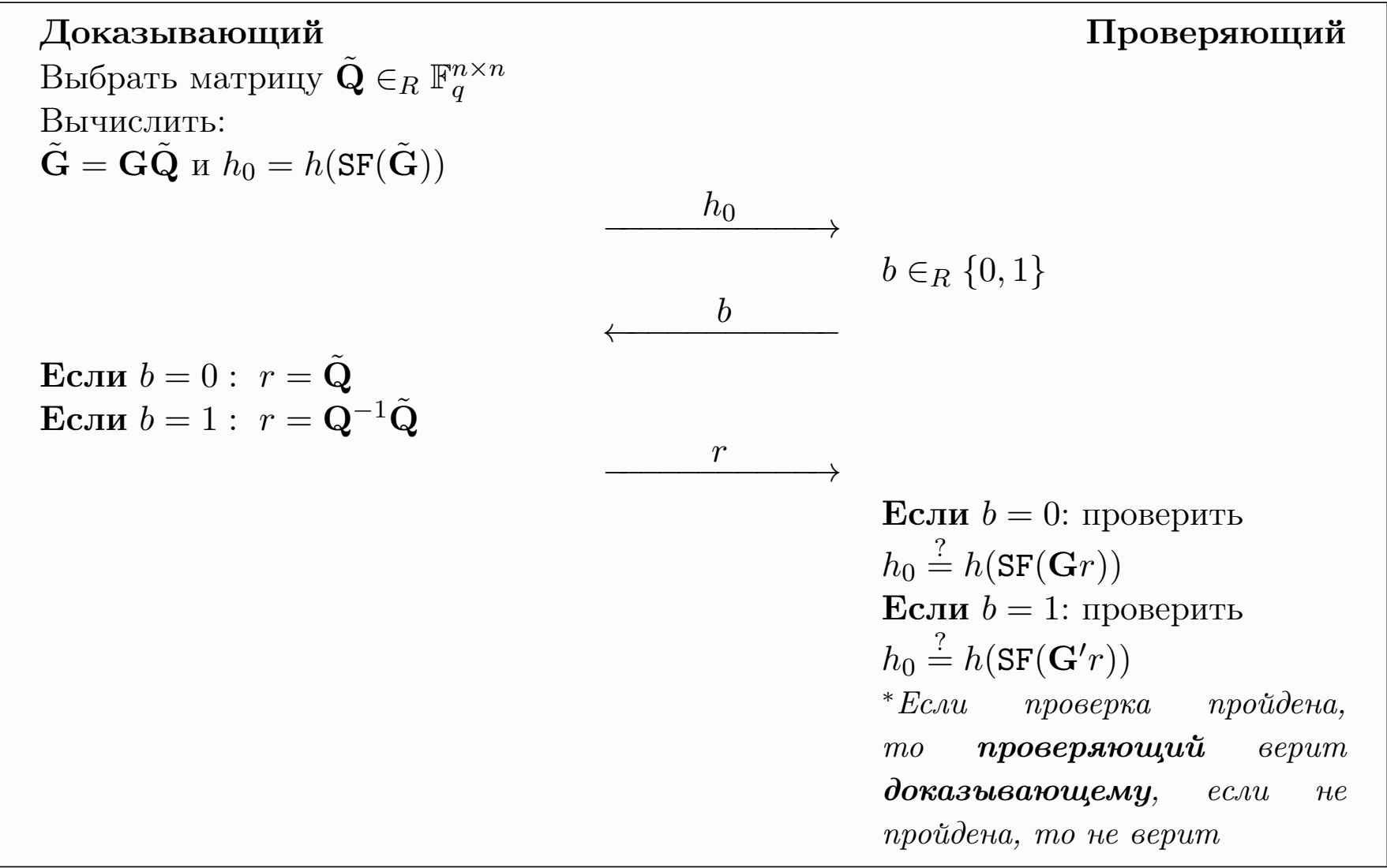


Цель:

Доказательство знания
секретного вектора $\mathbf{s} \in \mathbb{F}_2^n$,
такого, что $wt(\mathbf{s}) = t$

Таблица 2 – Протокол идентификации CVE.

Протокол J.-F. Biasse et al., 2020 $p = 1/2$



Цель:
Доказательство знания
двух матриц $\mathbf{S}$ и $\mathbf{Q}$, где $\mathbf{S}$ —
обратимая $k \times k$ матрица,
составленная из элементов
 $\mathbb{F}_q$, а $\mathbf{Q}$ — мономиальная
 $n \times n$ матрица,
составленная из элементов
 $\mathbb{F}_q$.

Таблица 3 – Протокол идентификации из [13].

Преобразование Фиата-Шамира

Алгоритм 1 формирования подписи в схеме подписи из (V. Vysotskaya and I. Chizhov, 2021).

Вход: ключ подписи s , сообщение $m \in \{0, 1\}^*$.

- 1: **Для каждого** $1 \leq i \leq \delta$ **выполнить**
 - 2: выбрать $\mathbf{u}_i \in \mathbb{F}_2^n$ и $\sigma_i \in S_n$
 - 3: вычислить $c_{i,0} = h(\sigma_i \| H\mathbf{u}_i^T)$
 - 4: вычислить $c_{i,1} = h(\sigma_i(\mathbf{u}_i))$
 - 5: вычислить $c_{i,2} = h(\sigma_i(\mathbf{u}_i \oplus \mathbf{s}))$
 - 6: вычислить $\mathbf{c}_i = (c_{i,0} \| c_{i,1} \| c_{i,2})$
 - 7: Вычислить $b = f(m \| \mathbf{c}_1 \| \dots \| \mathbf{c}_\delta)$
 - 8: **Для каждого** $1 \leq i \leq \delta$ **выполнить**
 - 9: вычислить $r_i = \begin{cases} \sigma_i \| \mathbf{u}_i, & \text{если } b_i = 0; \\ \sigma_i \| (\mathbf{u}_i \oplus \mathbf{s}), & \text{если } b_i = 1; \\ \sigma_i(\mathbf{u}_i) \| \sigma_i(\mathbf{s}), & \text{если } b_i = 2; \end{cases}$
 - 10: Положить **подпись**: $\zeta = (\mathbf{c}_1 \| \dots \| \mathbf{c}_\delta \| r_1 \| \dots \| r_\delta)$
-

+

Преимущества:

Возможность создания цифровой подписи.
Безопасность на уровне исходного протокола.

—

Недостаток:

Большой размер подписи (ранние реализации)

Основная идея: Перевод интерактивного протокола в неинтерактивную схему.

Запрос формируется с помощью хэша сообщения и данных доказывающего.

Сокращение размера подписи на примере схемы MEDS

Описание

Функция ParseHash

$\text{ParseHash}_{s,t,w}: \{0,1\}^n \rightarrow \{0,1,\dots,s-1\}^t$

преобразующее хэш-значение

длины n в вектор

$v = (v_0, v_1, \dots, v_{t-1})$,

удовлетворяющий следующим

свойствам:

- ровно $t - w$ компонент вектора равны нулю
- оставшиеся w компонент вектора принимают значения из множества $\{1, 2, \dots, s - 1\}$

Преимущество

Уменьшение размера подписи за счет увеличения числа нулевых значений.

Безопасность

Вероятность угадывания:

$$\tilde{p} = \frac{1}{\binom{t}{w}(s-1)^w}.$$

Оценка безопасности схем подписи

- Принято считать, что для получения численных оценок безопасности **достаточно** использовать характеристики известных методов решения трудноразрешимых **задач теории кодирования** (в большинстве случаев задачи синдромного декодирования), а также поиска **коллизии** или (второго) **прообраза** для используемой функции хэширования.
- **Классическая модель:** сложность оценивается $\widetilde{O}(2^{0.0885n})$.
- **Квантовая модель:** сложность оценивается $\widetilde{O}(2^{0.05869n})$.

Метод анализа для трёхпроходных протоколов

Хэш-функция h

Отображает битовые строки произвольной длины в строки фиксированной длины n .

- Классические требования к криптографической хэш-функции

Функция g

Преобразует выход хэш-функции в последовательность из δ элементов множества R .

- Детерминированность
- Эффективность вычислений
- Равномерное распределение

Метод анализа для трёхпроходных протоколов

Случай классического нарушителя

Вероятность успешного нарушения доказательства в рамках одного раунда интерактивного протокола доказательства с нулевым разглашением:

$$p = \frac{|S|}{|R|},$$

где

$|S|$ — мощность множества допустимых ответов, которые может использовать нарушитель,
 $|R|$ — мощность множества всех возможных вызовов.

Для неинтерактивной схемы с δ раундами:

$$p^\delta = \left(\frac{|S|}{|R|} \right)^\delta = \frac{|S|^\delta}{|R|^\delta}.$$

Пример (схема Штерна): $|S| = 2$, $|R| = 3$.

Метод анализа для трёхпроходных протоколов

Квантовая модель

Трудоёмкость подделки с использованием алгоритма Гровера:

$$T = \left\lceil \frac{\pi}{4} \sqrt{\frac{N}{t}} \right\rceil,$$

где $N = |R|^\delta$, $t = |S|^\delta$.

Аналогично для преобразования типа **ParseHash** _{s,t,w} :

$$T = \left\lceil \frac{\pi}{4} \sqrt{\binom{t}{w} (s-1)^w} \right\rceil.$$

Оценки безопасности схем подписи по протоколу Я. Штерна

Значение δ	Безопасность в классической модели (бит)	Безопасность в квантовой модели (бит)
137	80	39.7
219	128	63.7

Для расчета оценки безопасности схем подписи на основе протокола идентификации Я. Штерна достаточно использовать значение δ .

Оценки безопасности схем подписи MEDS и LESS

Заявляемая оценка безопасности	Схема подписи	t	w	s	Полученная оценка безопасности
128	LESS	247	30	2	63.7
	MEDS	1152	14	4	63.7
192	LESS	759	33	2	95.7
	MEDS	608	26	4	95.9
256	LESS	1352	40	2	127.7
258	MEDS	112	66	6	129.1

Оценки безопасности схемы подписи CROSS

Заявляемая оценка безопасности	t	w	s	Полученная оценка безопасности
128	256	216	2	77.8
192	256	160	2	119.7
256	512	432	2	157.5

Заключение

Рассмотрены современные схемы подписи, основанные на сложных задачах теории кодирования.

Особое внимание – протоколы идентификации с преобразованием Фиата-Шамира.

Предложена классификация и универсальный метод оценки безопасности цифровых подписей.

Оценка безопасности универсальна и не зависит от конкретного кода.

Оценки применимы к схемам, участвующим в конкурсе НИСТ 2022.

Алгоритм 2 подделки подписи под случайным сообщением с использованием алгоритма Гровера

Require: Проверочная матрица кода H , ключ проверки подписи y

- 1: $\mathbf{N} \leftarrow \{0, 1, 2\}^\delta$, $\mathbf{M} \leftarrow \{0, 1\}^\delta$, $\mathbf{X} \leftarrow \mathbb{Z}_2^{512}$
- 2: **repeat**
- 3: **for all** $i = 1, 2, \dots, \delta$ **выполнить**
- 4: сформировать $\mathbf{c}_i$ так, чтобы в схеме идентификации Я. Штерна можно было корректно сформировать ответ в случае $b_i \in \{0, 1\}$
- 5: $\hat{f}_\delta(msg) := f(msg \parallel \mathbf{c}_1 \parallel \mathbf{c}_2 \parallel \dots \parallel \mathbf{c}_\delta)$ $\triangleright \hat{f}_\delta: \mathbf{X} \rightarrow \{0, 1, 2\}^\delta$
- 6: $msg \leftarrow Grvr(\mathbf{X}, \mathbf{M}, \mathbf{N}; \hat{f}_\delta)$
- 7: **until** $msg = \perp$
- 8: $(b_1, b_2, \dots, b_\delta) \leftarrow f(msg \parallel \mathbf{c}_1 \parallel \mathbf{c}_2 \parallel \dots \parallel \mathbf{c}_\delta)$
- 9: **for all** $i = 1, 2, \dots, \delta$ **выполнить**
- 10: сформировать r_i в зависимости от значения b_i

Ensure: Сообщение msg , подпись $\zeta = \mathbf{c}_1 \parallel \mathbf{c}_2 \parallel \dots \parallel \mathbf{c}_\delta \parallel r_1 \parallel r_2 \parallel \dots \parallel r_\delta$

Алгоритм 3 подделки подписи под выбранным сообщением msg с использованием алгоритма Гровера

Require: Проверочная матрица кода H , ключ проверки подписи $\mathbf{y}$, msg — сообщение, под которым необходимо сформировать подпись

- 1: $\mathbf{N} \leftarrow \{0, 1, 2\}^\delta$, $u \xleftarrow{\mathcal{U}} \mathbb{Z}_2^{2896}$, $\mathbf{M} \leftarrow \{0, 1\}^\delta$
- 2: $c_{\delta,1} \leftarrow h(0)$, $c_{\delta,2} \leftarrow h(1)$ $\triangleright 0,1$ – произвольные входы функции
- 3: **repeat**
- 4: **for all** $i = 1, 2, \dots, \delta - 1$ **выполнить**
- 5: сформировать $\mathbf{c}_i$ так, чтобы в схеме идентификации Я. Штерна можно было корректно сформировать ответ в случае $b_i \in \{0, 1\}$
- 6: Сформировать $\mathbf{t}$: $H\mathbf{t}^T = \mathbf{y}$, $\mathbf{u} \neq \mathbf{t}$
- 7: $\mathbf{X} \leftarrow \{\sigma \mid \sigma \in S(2896), \sigma(\mathbf{u} + \mathbf{t}) = 0, \sigma(\mathbf{u}) = 1\}$
- 8: $\widehat{f}_\delta(\sigma) := f(msg \parallel \mathbf{c}_1 \parallel \mathbf{c}_2 \parallel \dots \parallel \mathbf{c}_{\delta-1} \parallel (h(\sigma \parallel H(\mathbf{u} + \mathbf{t})) \parallel c_{\delta,1} \parallel c_{\delta,2}))$ $\triangleright \widehat{f}_\delta: \mathbf{X} \rightarrow \{0, 1, 2\}^\delta$
- 9: $\sigma \leftarrow Grvr(\mathbf{X}, \mathbf{M}, \mathbf{N}; \widehat{f}_\delta)$
- 10: **until** $\sigma = \perp$
- 11: $\mathbf{c}_\delta = (h(\sigma \parallel H(\mathbf{u} + \mathbf{t})) \parallel c_{\delta,1} \parallel c_{\delta,2})$
- 12: $(b_1, b_2, \dots, b_\delta) \leftarrow f(msg \parallel \mathbf{c}_1 \parallel \mathbf{c}_2 \parallel \dots \parallel \mathbf{c}_\delta)$
- 13: **for all** $i = 1, 2, \dots, \delta$ **выполнить**
- 14: сформировать r_i в зависимости от значения b_i

Ensure: Подпись $\zeta = \mathbf{c}_1 \parallel \mathbf{c}_2 \parallel \dots \parallel \mathbf{c}_\delta \parallel r_1 \parallel r_2 \parallel \dots \parallel r_\delta$ для сообщения msg
