УДК 003.26 DOI 10.17223/20710410/69/5

ПРОТОКОЛ МЕНТАЛЬНОГО ПОКЕРА, ОСНОВАННЫЙ НА ЗАДАЧАХ ПОИСКА ИЗОГЕНИЙ МЕЖДУ ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ[1]

И. Д. Иогансон*,**,***, В. В. Давыдов*,**,***, Ж.-М. Н. Дакуо*,**,***, А. Ф. Хуцаева*,***

*Университет ИТМО, г. Санкт-Петербург, Россия
**QApp, г. Москва, Россия
***Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия

E-mail: ivan.ioganson@yandex.ru, vadimdavydov@outlook.com, jeandakuo@mail.ru, afkhutsaeva@itmo.ru

Представлен новейший квантово-устойчивый протокол ментального покера, основанный на задаче поиска изогений между эллиптическими кривыми. Данный протокол позволяет нескольким пользователям создавать и перемешивать колоду карт, а затем выдавать карту определённому пользователю. Разработаны две версии протокола: без валидации, которая позволяет защититься только от пассивного злоумышленника, и с валидацией, позволяющая обнаружить активное вмешательство в протокол с помощью протоколов доказательства с нулевым разглашением. Для валидации предложенного решения разработана программа на языке C, реализующая описанный протокол. Полученные результаты демонстрируют возможность практического применения предложенного решения, обеспечивая защиту от атак с использованием квантового компьютера.

Ключевые слова: *протокол ментального покера, эллиптические кривые, изогении, постквантовая криптография.*

MENTAL POKER PROTOCOL BASED ON THE PROBLEM OF FINDING ISOGENIES BETWEEN ELLIPTIC CURVES

I. D. Ioganson*,**,***, V. V. Davydov*,**,***, Zh.-M. N. Dakuo*,**,***, A. F. Khutsaeva*,***

*ITMO University, Saint Petersburg, Russia
**QApp, Moscow, Russia
***Saint-Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia

In the paper, a novel isogeny-based protocol for mental poker game is presented. This protocol allows multiple users to create and shuffle a deck of cards, and then issue a card to a specific user. Two versions of the protocol are developed: one without validation, which protects only against passive adversaries, and one with validation, which also allows detecting active interference with the protocol using zero-knowledge proof protocols. To validate the resulting solution, a C program was developed that implements the described protocol. This demonstrates the practical applicability of the proposed solution while ensuring protection against quantum attacks.

Keywords: *mental poker protocol, elliptic curves, isogenies, post-quantum cryptography.*

[1]Работа выполнена в рамках госзадания (проект FSER-2025-0003).

Введение

Протокол ментального покера — криптографический протокол, позволяющий нескольким игрокам играть в карточную игру на расстоянии с использованием средств связи. Основная цель таких протоколов — позволить игрокам играть в карточные игры, не раскрывая друг другу свои карты и не используя доверенную сторону, которая могла бы контролировать процесс игры. Все операции, включая генерацию и тасование колоды, должны быть распределены между игроками таким образом, чтобы гарантировать честность процесса.

Впервые протокол ментального покера был представлен в 1979 г. в работе [1], но впоследствии было показано, что предложенная схема небезопасна [2, 3]. В дальнейшем эта область получила некоторое развитие в работах [4, 5]. Протокол перемешивания карт в ментальном покере находит широкое применение в смешивающих сетях (Mix network) и протоколах электронного голосования [6, 7].

В связи с ростом интереса к децентрализованным технологиям протоколы ментальных карточных игр представляют важное направление развития криптографических методов, способных обеспечить честность даже в условиях полного недоверия между участниками. Упомянутые выше решения основаны на задачах, уязвимых к атакам на квантовом компьютере, в связи с чем появляется необходимость создания новых квантово-защищённых протоколов, в частности протоколов ментальных карточных игр.

Одной из актуальных постквантовых областей является криптография, основанная на изогениях между эллиптическими кривыми. Данная область динамично развивается; только за последний год был предложен ряд работ: новейшие схемы цифровой подписи [8–11], проверяемая случайная функция (VRF) [12], схема электронного голосования [13], механизм инкапсуляции ключа [14] и др. [15, 16]. Данные работы демонстрируют высокий потенциал математического аппарата изогений эллиптических кривых.

В данной работе предлагаются два варианта протокола, основанного на постквантовой задаче поиска изогений между суперсингулярными эллиптическими кривыми. Протокол состоит из четырёх фаз: подготовка колоды, тасование колоды, выдача карты пользователю и открытие карты. Рассматриваются два варианта протокола: *с валидацией*, который позволяет защищаться от активного злоумышленника, имеющего возможность манипулировать передаваемой информацией с целью получения преимущества, и *без валидации*, который является «облегчённой» версией протокола с валидацией и предназначен только для честных игроков (не нарушающих ход протокола); при этом скорость выполнения второго варианта протокола в разы выше первого.

Работа имеет следующую структуру. В п. 1 представлены предварительные сведения, необходимые для описания протокола. В п. 2 описаны существующие решения, а также прототип протокола, на основе которого строится разработанное решение. В п. 3 описываются два варианта разработанного протокола — без валидации и с валидацией. Пункт 4 содержит доказательства безопасности предложенных протоколов. В п. 5 описываются результаты вычислительных экспериментов, приводятся оценки быстродействия и затрачиваемой памяти. В заключении подводятся итоги работы, описываются достоинства и недостатки предложенного протокола.

1. Предварительные сведения

Введём базовые понятия, необходимые для описания протокола [17, 18].

Пусть $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ — стандартные обозначения числовых множеств. Эллиптическая кривая E — это неособая кубическая кривая, $\mathbb{K}$ — некоторое поле, ∞ — бесконечно удалён-

ная точка на эллиптической кривой. Для задач криптографии, как правило, используются кривые в форме Вейерштрасса:

$$E_W : y^2 = x^3 + Ax + B,$$

или в форме Монтгомери:

$$E_M : By^2 = x^3 + Ax^2 + x,$$

где $A, B \in \mathbb{K}$.

Пусть $n \in \mathbb{N}$. Группой точек кручения на кривой E, заданной над полем $\mathbb{K}$, называется группа точек

$$E[n] = \{P \in E(\overline{\mathbb{K}}) : nP = \infty\},$$

где $\overline{\mathbb{K}}$ — алгебраическое замыкание поля $\mathbb{K}$.

Кривая E, заданная над конечным полем $\mathbb{F}_p$, называется суперсингулярной, если $E[p] = \{\infty\}$. Кривая E называется обычной, если $E[p] \cong \mathbb{Z}/p\mathbb{Z}$.

Пусть E_1 и E_2 — эллиптические кривые, заданные над конечным полем $\mathbb{F}_q$, где $q = p^n$, p — некоторое простое число, $n \in \mathbb{N}$. Изогенией называется нетривиальный гомоморфизм

$$\varphi : E_1 \to E_2,\ \varphi(\infty_{E_1}) = \infty_{E_2}.$$

Две кривые называются изогенными, если существует изогения между ними. Любую изогению $\varphi : E_1 \to E_2$ можно задать в явном виде:

$$\forall P \in E_1(\mathbb{F}_q)\ \exists Q \in E_2(\mathbb{F}_q)\big(\varphi(P) = Q\big), \quad P = (x, y), \quad Q = \left(\frac{p(x)}{q(x)}, y \cdot r(x)\right).$$

Здесь $p(x), q(x), r(x) \in \mathbb{F}_q[x]$. Степень изогении может быть вычислена как

$$\deg \varphi = \max\{\deg p(x), \deg q(x)\}.$$

Изогения называется сепарабельной, если $\left(\frac{p(x)}{q(x)}\right)' \neq 0$. Для сепарабельных изогений верно, что $\deg \varphi = \# \ker \varphi$, где $\ker \varphi$ — ядро изогении. При построении криптографических схем работа ведётся только с сепарабельными изогениями.

Пусть необходимо вычислить изогению $\varphi : E_1 \to E_2$, $G = \ker \varphi$. Для её вычисления могут использоваться формулы Велу [19]:

— $\forall P \in G\ \big(\varphi(P) = \infty\big)$;

— $\forall P = (x_P, y_P) \notin G\ \left(\varphi(P) = \left(x_P + \sum\limits_{Q \in G \setminus \{\infty\}} (x_{P+Q} - x_Q),\ y_P + \sum\limits_{Q \in G \setminus \{\infty\}} (y_{P+Q} - y_Q)\right)\right)$.

Ядро G определяет отображение из кривой E_1 в кривую E_2 с точностью до изоморфизма:

$$E_1/G \stackrel{\text{def}}{=} E_2.$$

Если ядро изогении φ — циклическая подгруппа, то изогения называется циклической. Сложность подсчёта изогении растёт линейно в зависимости от количества точек в $\ker \varphi$, поэтому подсчёт не всегда эффективен. Пусть φ может быть представлена как композиция изогений

$$\varphi = \psi_1 \circ \psi_2 \circ \cdots \circ \psi_m,$$

где $\deg \psi_i = p_i$, $1 \leqslant i \leqslant m$. Тогда степень изогении φ можно представить как

$$\deg \varphi = \prod_{j=1}^{n} p_j^{\ell_j},$$

где ℓ_j — количество изогений степени p_j. В таком случае $\deg \varphi$ является гладким числом и изогению можно представить как композицию из ℓ_j изогений степени p_j для $1 \leqslant j \leqslant n$, тем самым сильно упростив вычисления.

Если $\varphi : E \to E'$ — изогения степени λ, то существует единственная изогения (называемая дуальной) $\hat{\varphi} : E' \to E$, такая, что

$$\hat{\varphi} \circ \varphi = [\lambda]_E, \quad \varphi \circ \hat{\varphi} = [\lambda]_{E'},$$

где $[\lambda]$ обозначает сложение точки самой с собой λ раз.

Пусть эллиптическая кривая E задана над конечным полем K. Эндоморфизмом кривой E называется её изогения, действующая в себя: $\varphi : E(\overline{K}) \to E(\overline{K})$. Множество всех таких изогений и нулевое отображение образуют кольцо эндоморфизмов $\mathrm{End}(E)$. Различают также кольцо эндоморфизмов, заданное над полем K: $\mathrm{End}_K(E)$, в котором содержатся все изогении $\varphi' : E(K) \to E(K)$.

Пусть X — некоторое коммутативное кольцо. X-модулем называется абелева группа M, на которой X действует линейно. X-модуль M называется конечно порождённым, если существует такое конечное множество элементов $\{m_1, \ldots, m_n\}$ в X-модуле, что верно следуюшее свойство:

$$\forall m \in M \left(m = x_1 m_1 + \ldots + x_n m_n\right), \quad x_i \in X,\ i \in \{1, \ldots, n\}.$$

Пусть $f : X \to Y$ — гомоморфизм колец, а произведение элементов $x \in X$, $y \in Y$ определяется формулой

$$xy = f(x)y.$$

Всякое кольцо Y, снабжённое структурой X-модуля, называется X-алгеброй, т. е. X-алгебра — пара, состоящая из кольца Y и гомоморфизма колец $f : X \to Y$; Y называется конечно порождённой X-алгеброй, если существует конечное число таких элементов $x_1, \ldots, x_n$ в X-алгебре, что каждый элемент Y можно записать в виде многочлена от $x_1, \ldots, x_n$ с коэффициентами из X [20].

Пусть K — конечно порождённая $\mathbb{Q}$-алгебра. Порядком $\mathcal{O} \subset K$ называется подкольцо K, которое является конечно порождённым $\mathbb{Z}$-модулем максимальной размерности.

Согласно соответствию Дойринга (Deuring) об изоморфизме кольца эндоморфизмов эллиптической кривой [21, 22], для кривой, заданной над конечным полем $\mathbb{K}$, кольцо эндоморфизмов изоморфно либо порядку в мнимом квадратичном поле, либо порядку в алгебре кватернионов, заданной над $\mathbb{Q}$.

Для обычной кривой $E'/\mathbb{F}_p$ кольцо эндоморфизмов изоморфно порядку в мнимом квадратичном поле, а также $\mathrm{End}(E') = \mathrm{End}_{\mathbb{F}_p}(E')$. Для суперсингулярной кривой $E/\mathbb{F}_p$ $\mathrm{End}(E)$ изоморфно порядку в алгебре кватернионов, при этом $\mathrm{End}_{\mathbb{F}_p}(E)$ — это порядок в мнимом квадратичном поле, т. е.

$$\mathrm{End}_{\mathbb{F}_p}(E) \hookrightarrow \mathbb{Q}(\pi),$$

где π — эндоморфизм Фробениуса эллиптической кривой $E/\mathbb{F}_p$:

$$\pi : E \to E, \quad (x, y) \mapsto (x^p, y^p).$$

Обозначим такой порядок как $\mathcal{O}$. Тогда, так как $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathcal{O}$ (порядку в мнимом квадратичном поле), можно определить действие элемента $\alpha \in \mathcal{O}$ на точку кривой $P \in E$ как $\alpha(P) = \varphi_\alpha(P)$, где φ_α — это эндоморфизм кривой E, изоморфный α. Для любого ненулевого идеала $\mathfrak{a} \subset \mathcal{O}$ можно построить подгруппу

$$E[\mathfrak{a}] = \{P \in E : \forall \alpha \in \mathfrak{a}\,(\alpha(P) = 0)\}.$$

Изогения $\varphi_\mathfrak{a} : E \to E/E[\mathfrak{a}]$, соответствующая идеалу $\mathfrak{a}$, является изогенией с ядром $\ker(\varphi_\mathfrak{a}) = E[\mathfrak{a}]$. Норма идеала $\mathfrak{a} \subset \mathcal{O}$ задаётся как $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$, то есть как мощность фактор-кольца. Степень изогении $\varphi_\mathfrak{a}$ равна норме идеала: $\deg \varphi_\mathfrak{a} = \mathrm{N}(\mathfrak{a})$.

Пусть $I(\mathcal{O})$ — множество всех идеалов порядка $\mathcal{O}$. Идеалы $\mathfrak{a}, \mathfrak{b} \in I(\mathcal{O})$ называются эквивалентными, если существует $\alpha \in \mathcal{O}$, такой, что $\mathfrak{a} = \alpha \cdot \mathfrak{b} = \{\alpha \cdot \beta : \beta \in \mathfrak{b}\}$. Обозначим эквивалентность идеалов $\mathfrak{a}$ и $\mathfrak{b}$ как $\mathfrak{a} \sim \mathfrak{b}$. Классом эквивалентности идеала $\mathfrak{a}$ называется множество $[\mathfrak{a}] = \{\mathfrak{b} \in I(\mathcal{O}) : \mathfrak{a} \sim \mathfrak{b}\}$. Множество классов эквивалентности идеалов кольца $\mathcal{O}$ обозначим $Cl(\mathcal{O})$. Между классами эквивалентности можно определить операцию «$\cdot$» через соответствующую операцию кольца $\mathcal{O}$:

$$[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a} \cdot \mathfrak{b}].$$

Для простоты далее будем считать, что $[\mathfrak{a} \cdot \mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$. Тогда $Cl(\mathcal{O})$ образует конечную абелеву группу [23] относительно операции «$\cdot$» умножения идеалов с нейтральным элементом $[\mathcal{O}]$ — класс идеала, включающего всё кольцо. Одним из свойств группы является обратимость элементов: для любого $[\mathfrak{a}] \in Cl(\mathcal{O})$ существует $[\mathfrak{a}]^{-1} \in Cl(\mathcal{O})$, такой, что $[\mathfrak{a}] \cdot [\mathfrak{a}]^{-1} = [\mathcal{O}]$.

Если идеалы $\mathfrak{a}$ и $\mathfrak{b}$ лежат в одном и том же классе из группы классов идеалов $Cl(\mathcal{O})$, то $E/E[\mathfrak{a}] \cong E/E[\mathfrak{b}]$ над полем $\mathbb{F}_p$.

Дадим определение группового действия [24]. Группа G действует на множестве X, если существует отображение $\star : G \times X \to X$, для которого выполнены следующие свойства:

1) взаимодействие с нейтральным элементом: если e — нейтральный элемент группы G, то $e \star x = x$ для всех $x \in X$;
2) совместимость: $(gh) \star x = g \star (h \star x)$ для всех $g, h \in G$ и $x \in X$.

В такой нотации групповое действие обозначается как $(G, X, \star)$. Групповые действия могут обладать дополнительными свойствами:

1) транзитивностью: групповое действие $(G, X, \star)$ транзитивно, если

$$\forall x_1, x_2 \in X\, \exists g \in G\, (x_2 = g \star x_1);$$

2) свободой: групповое действие $(G, X, \star)$ свободно, если для всех $g \in G$ элемент g является нейтральным тогда и только тогда, когда существует $x \in X$, такой, что $x = g \star x$;
3) коммутативностью: групповое действие $(G, X, \star)$ коммутативно, если

$$\forall g_1, g_2 \in G \forall x \in X \left(g_1 \star (g_2 \star x) = g_2 \star (g_1 \star x)\right).$$

Групповое действие называется криптографическим, если оно удовлетворяет следующим свойствам [24]:

1) однонаправленностью: по заданной паре элементов $(x, g \star x)$, где $g \in G$ и $x \in X$ выбраны случайным образом, вычислительно сложно найти g;

2) непредсказуемостью: пусть дано полиномиально большое количество пар элементов $(x_i, g \star x_i)$, где $g \in G$ и $x_i \in X$ выбраны случайным образом. Тогда вычислительно сложно найти $g \star x^*$ для заданного $x^* \in X$;
3) псевдослучайностью: вычислительно сложно отличить множество пар элементов $(x_i, g \star x_i)$ от множества пар элементов (x_i, u_i), где $g \in G$ и $x_i, u_i \in X$ выбраны случайным образом.

Пусть $\mathscr{E}\ell\ell(\mathcal{O})$ — множество эллиптических кривых над конечным полем $\mathbb{F}_p$, кольца эндоморфизмов которых изоморфны порядку $\mathcal{O}$ в мнимом квадратичном поле. Зададим действие группы классов идеалов $Cl(\mathcal{O})$ на множестве кривых $\mathscr{E}\ell\ell(\mathcal{O})$:

$$\star : Cl(\mathcal{O}) \times \mathscr{E}\ell\ell(\mathcal{O}) \to \mathscr{E}\ell\ell(\mathcal{O}), \quad (\mathfrak{a}, E) \mapsto [\mathfrak{a}] \star E.$$

Указанное действие выполняется следующим образом. Для идеала $\mathfrak{a}$ вычисляется подгруппа точек кручения $E[\mathfrak{a}]$. Затем по алгоритму Велу вычисляется изогения $\varphi_{\mathfrak{a}} : E \to E_1$, такая, что $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}]$. Результатом выполнения группового действия является кривая $E_1 = [\mathfrak{a}] \star E$, лежащая в том же множестве [25].

Данное групповое действие является криптографическим, а также транзитивно, свободно и коммутативно. Задача обращения группового действия на множестве эллиптических кривых является вычислительно трудной [26].

Задача обратного группового действия (*Group Action Inverse Problem, GAIP*)

Пусть заданы эллиптические кривые E_0 и E над конечным полем $\mathbb{F}_p$, $\mathrm{End}_{\mathbb{F}_p}(E) = \mathcal{O}$. Вычислительно трудно найти идеал $\mathfrak{a} \subset \mathcal{O}$, такой, что $E = [\mathfrak{a}] \star E_0$. При этом идеал $\mathfrak{a}$ должен быть представлен таким образом, что групповое действие $\star$ может быть эффективно вычислено.

Данная задача лежит в основе известного протокола выработки общего ключа CSIDH [27, 28] и алгоритма цифровой подписи CSI-FiSh [26]. Её преимуществом является сложность решения не только на классических вычислительных машинах, но и на квантовых. Наиболее эффективный алгоритм в классической модели вычислений имеет экспоненциальную сложность, а в квантовой модели — субэкспоненциальную (алгоритм Куперберга [29]).

2. Существующие решения

Протоколы ментальных карточных игр можно разделить на две группы: с доверенной третьей стороной (Trusted Third Party, TTP) и без неё. Первая группа протоколов для генерации, тасования колоды и последующей раздачи карт использует TTP, а вторая группа производит все эти операции децентрализованно. В данной работе рассматриваются и строятся протоколы без участия TTP.

Протоколы ментальных карточных игр без TTP также можно разделить на две основные группы. Протоколы из первой группы называют протоколами «без перетасовок». К данному типу относится, например, протокол, описанный в [30]. К протоколам второй группы относятся протоколы «с перетасовкой» [31–33].

В протоколе «без перетасовок» выдача карты происходит путём совместной генерации зашифрованного случайного номера выдаваемой карты. Затем игроки должны проверить, что данная карта ещё ни разу не была выдана, и если это не так, то они вынуждены запускать протокол сначала. Таким образом, чем больше карт выдаётся, тем больше вероятность того, что новая карта совпадёт с одной из уже выданных, что увеличивает ожидаемое количество перезапусков протокола. Следовательно, в играх, где используется вся колода, данная группа протоколов может требовать большого

времени на генерацию карты. В данной работе рассматриваются протоколы «с перетасовкой».

Будем называть открытой колодой карт колоду до перетасовки, перетасованной (закрытой) колодой — колоду после перетасовки, открытой и закрытой картой — карту из открытой и перетасованной колод соответственно, маской карты — секретное значение, индивидуальное для каждого игрока и генерируемое при перетасовке.

В качестве прототипа предлагаемого протокола выбран протокол [33] ментального покера, состоящий из четырёх основных частей: 1) подготовка колоды (протокол 2.1); 2) тасование колоды (протокол 2.2); 3) выдача карты (протокол 2.3); 4) открытие карты.

Протокол 2.1. Подготовка колоды

Вход: M — количество карт.

Выход: открытая колода A.

1 Игроки генерируют случайное большое простое число n и группу $\langle G, \cdot \rangle$ порядка n.

2 Игроки сообща генерируют случайные значения $a_i \in G$ для $i = 0, \ldots, M$.

3 **Вернуть** $A = \{a_i : i \in \{0, \ldots, M\}\}$.

Значение a_0 не является картой, а используется в дальнейшем для верификации; общее количество игроков — N.

Протокол 2.2. Тасование колоды

Вход: A — открытая колода, n — порядок группы G, M — количество карт.

Выход: перетасованная колода B.

1 $B_0 := \{b_{0,i}\}$, где $b_{0,i} = a_i \in A$ для $i = 0, \ldots, M$.

2 **Для** $j \in \{1, \ldots, N\}$ *каждый игрок* P_j*:*

3 Выбирает случайное число $0 < x_j < n$ и запоминает его.

4 Выбирает случайную перестановку $S_j : \{0, \ldots, M\} \to \{0, \ldots, M\}$, такую, что $S_j(0) = 0$.

5 Публикует $B_j = \{b_{j,i}\}$, где $b_{j-1,i} = b_{j,S_j(i)}^{x_j} \in G$ для $i = 0, \ldots, M$.

6 Остальные игроки проверяют корректность перетасовки с помощью заранее выбранного протокола доказательства с нулевым разглашением

7 . **Вернуть** $B = B_N$ — *перетасованная колода.*

Во время выполнения протокола 2.2 на шаге 3 каждый игрок запоминает значение секретной маски x_j для последующего использования в протоколе 2.3 на шагах 5 и 8.

Для открытия карты игрок P_{j_0} публикует ранее выданную карту c, и с помощью сигма-протокола Чаума — Педерсена [34] остальные игроки проверяют, что полученное значение корректно.

Протокол 2.3. Выдача карты

Вход: c_0 — карта из перетасованной колоды, j_0 — номер игрока, получающего карту c_0, n — порядок группы G.

Выход: открытая карта c.

Для $j \in \{1, \dots, N\}$ *каждый игрок* P_j*:*
  Если $j = j_0$, **то:**
    $c_j := c_{j-1}$.
  Иначе:
    $y_j = x_j^{-1} \bmod n$, где x_j — секретная маска игрока j.
    Публикует $c_j := c_{j-1}^{y_j} \in G$.
    С помощью сигма-протокола Чаума — Педерсена [34] остальные игроки проверяют, что полученное значение корректно.
Игрок P_{j_0} вычисляет $y_{j_0} = x_{j_0}^{-1} \bmod n$, где x_{j_0} — секретная маска игрока j_0.
Игрок P_{j_0} вычисляет $c := c_N^{y_{j_0}} \in G$.
Карта c выдана игроку j_0.
Вернуть c — *открытая карта.*

3. Предлагаемое решение

3.1. Протокол без валидации

Данная версия протокола предназначена для защиты от модели злоумышленника «Honest-But-Curious». В этой модели злоумышленник не пытается активно вмешиваться в протокол, но может анализировать полученные в ходе протокола данные, чтобы получить преимущество.

Протоколы подготовки колоды, тасования колоды, выдачи карты и открытия карты описаны как протоколы 3.1, 3.2 и 3.3 соответственно. Здесь и далее операция $x \xleftarrow{\$} S$ — присвоение переменной x случайного значения, выбранного из равномерного распределения на множестве S; операция «$\star$» — действие группы классов идеалов $Cl(\mathcal{O})$ на множестве кривых $\mathscr{E}\ell\ell(\mathcal{O})$.

Протокол 3.1. Подготовка колоды

Вход: $p \in \mathbb{N}$ — простое число, $E_0/\mathbb{F}_p$ — начальная эллиптическая кривая с $\mathrm{End}_{\mathbb{F}_p}(E_0) \cong \mathcal{O}$, $Cl(\mathcal{O})$ — группа классов идеалов порядка $\mathcal{O}$, $M \in \mathbb{N}$ — количество карт, $N \in \mathbb{N}$ — количество игроков.

Выход: открытая колода $A \in \mathscr{E}\ell\ell(\mathcal{O})^M$.

Для $i = 1, \dots, M$*:*
  $a_i^{(0)} := E_0$.
  Для $j = 1, \dots, N$*:*
    Игрок P_j выбирает $[\mathfrak{x}_j] \xleftarrow{\$} Cl(\mathcal{O})$.
    Игрок P_j вычисляет $a_i^{(j)} := [\mathfrak{x}_j] \star a_i^{(j-1)}$.
    Игрок P_j передаёт $a_i^{(j)}$ игроку P_{j+1}.
$A := \{a_i^{(N)} : i = 1, \dots, M\}$
Вернуть A.

Протокол 3.2. Тасование колоды

Вход: $M \in \mathbb{N}$ — количество карт, $N \in \mathbb{N}$ — количество игроков, $A \in \mathscr{E}\ell\ell(\mathcal{O})^M$ — открытая колода, $Cl(\mathcal{O})$ — группа классов идеалов (см. протокол 3.1).

Выход: перетасованная колода $B \in \mathscr{E}\ell\ell(\mathcal{O})^M$.

1 $B^{(0)} := A$

2 **Для** $i = 1, \ldots, N$:

3 Игрок P_i выбирает случайную перестановку $S_i : \{1, \ldots, M\} \to \{1, \ldots, M\}$.

4 Игрок P_i выбирает $[\mathfrak{y}_i] \xleftarrow{\$} Cl(\mathcal{O})$ и запоминает его.

5 Игрок P_i вычисляет $B^{(i)} := \left([\mathfrak{y}_i] \star b^{(i-1)}_{S_i(1)}, [\mathfrak{y}_i] \star b^{(i-1)}_{S_i(2)}, \ldots, [\mathfrak{y}_i] \star b^{(i-1)}_{S_i(M)}\right)$, где $b^{(i-1)}_t \in B^{(i-1)}$ для $t \in \{1, \ldots, M\}$.

6 $B := B^{(N)}$.

7 **Вернуть** B.

Протокол 3.3. Выдача карты

Вход: $c^{(0)} \in \mathscr{E}\ell\ell(\mathcal{O})$ — карта из перетасованной колоды, $k \in \mathbb{N}$ — номер игрока, которому эта карта предназначена, $N \in \mathbb{N}$ — количество игроков.

Выход: открытая карта $c \in \mathscr{E}\ell\ell(\mathcal{O})$.

1 **Для** $j \in \{1, \ldots, N\} \setminus \{k\}$:

2 Игрок P_j вычисляет $c^{(j)} := [\mathfrak{y}_j]^{-1} \star c^{(j-1)}$, где $[\mathfrak{y}_j]$ — секретная маска игрока j.

3 Игрок P_k вычисляет $c := [\mathfrak{y}_k]^{-1} \star c^{(N-1)}$, где $[\mathfrak{y}_k]$ — секретная маска игрока k.

4 **Вернуть** c.

Во время выполнения протокола 3.2 на шаге 4 каждый игрок запоминает значение секретной маски $[\mathfrak{y}_i]$ для последующего использования в протоколе 3.3 на шагах 2 и 3.

Для открытия карты игрок P_j публикует ранее выданную карту c.

3.2. Протокол с валидацией

Данная версия протокола включает протоколы доказательства с нулевым разглашением (Zero-Knowledge Proof, ZKP) и предназначена для защиты от злоумышленника, который может активно подменять посылаемую информацию для получения выгоды. Если один из игроков нарушит ход протокола, то данный факт можно будет однозначно доказать. Для этого вся переданная в ходе работы протокола информация верифицируется с помощью протоколов доказательства с нулевым разглашением.

Описание работы протоколов 4.1, 4.2, 4.3 представлено в Приложении 1, протоколов доказательства с нулевым разглашением — в Приложении 2.

4. Стойкость протоколов

4.1. Стойкость протоколов без валидации

Стойкость предложенных протоколов основывается на предположении о сложности решения задачи обратного группового действия за полиномиальное время на классическом и квантовом компьютерах (см. п. 1).

Лучшим классическим алгоритмом для решения задачи обратного группового действия является атака «встреча посередине» [27], имеющая экспоненциальную сложность — $O(\sqrt{\#Cl(\mathcal{O})})$. Лучшим квантовым алгоритмом для решения GAIP является алгоритм Куперберга [29], обеспечивающий субэкспоненциальную временну́ю сложность — $2^{O(\sqrt{\log N})}$.

Свойства протокола

При разработке протокола ментального покера важными задачами являются формализация и реализация гарантий безопасности, характерных для классического оффлайн-покера, где физические ограничения и наблюдаемость процесса обеспечивают честность и справедливость. В цифровой среде отсутствие прямого контакта между участниками требует использования криптографических примитивов, которые позволяют гарантировать честность и прозрачность процесса игры. В связи с этим стойкий протокол ментального покера должен гарантировать следующие свойства:

1) при генерации колоды нельзя создать «краплёную» открытую колоду;
2) при перетасовке нельзя замешать колоду так, как это выгодно одному или нескольким игрокам;
3) при выдаче карты никто, кроме игрока, которому эта карта выдаётся, не может узнать содержимое карты;
4) для протокола с валидацией: если кто-то из игроков нарушает ход протокола, то существует доказательство этого.

Выбранные свойства напрямую отражают классические требования покера; при их выполнении протокол гарантирует честную игру или, в случае нарушений, идентификацию нечестных игроков.

Идеальная функциональность

Докажем выполнение перечисленных свойств через сведение протокола к идеальному путём использования UC-модели. В UC-модели для доказательства стойкости протокола сначала описывается идеальная функциональность протокола. Под идеальной функциональностью подразумевается версия протокола, которая получает тот же самый результат, но в которой все вычисления проводятся третьей доверенной стороной, которая работает как «чёрный ящик»: получает входные значения и выдаёт только результат работы протокола. Затем необходимо доказать, что работа настоящего протокола неотличима от его идеальной функциональности. Под неотличимостью понимается, что для стороннего наблюдателя, которому известен только вход и выход протокола, невозможно отличить, какой из протоколов использовался: настоящий или идеальный. Если настоящий протокол неотличим от идеального, то он считается стойким [35].

В протоколах 5.1–5.3 приведены три идеальные функциональности, которые полностью имитируют предлагаемый протокол ментального покера.

Протокол 5.1. Идеальный функционал протокола подготовки колоды

Вход: $\mathscr{E}\ell\ell(\mathcal{O})$ — множество эллиптических кривых, заданных над конечным полем $\mathbb{F}_p$ (p — простое число), кольца эндоморфизмов которых изоморфны порядку $\mathcal{O}$ в мнимом квадратичном поле, M — количество карт.

Выход: открытая колода A.

1 **Для** $i = 1, \ldots, M$:

2 ⌊ TTP генерирует случайное $a_i \xleftarrow{\$} \mathscr{E}\ell\ell(\mathcal{O})$.

3 $A := \{a_i\}$ для $i \in \{1 \ldots M\}$.

4 **Вернуть** A.

Протокол 5.2. Идеальный функционал протокола тасования колоды

Вход: $A = \{a_1, \ldots, a_M\}$ — открытая колода, M — количество карт, N — количество игроков, $Cl(\mathcal{O})$ — группа классов идеалов порядка $\mathcal{O}$ в мнимом квадратичном поле, $Y = \{[\mathfrak{y}_1], \ldots, [\mathfrak{y}_N]\} \subset Cl(\mathcal{O})$ — множество секретных ключей пользователей.

Выход: перетасованная колода B.

1 TTP выбирает случайную перестановку $S : \{1, \ldots, M\} \to \{1, \ldots, M\}$.

2 TTP вычисляет

$$B := \big([\mathfrak{y}_1] \star [\mathfrak{y}_2] \star \ldots [\mathfrak{y}_N] \star a_{S(1)},\ [\mathfrak{y}_1] \star [\mathfrak{y}_2] \star \ldots [\mathfrak{y}_N] \star a_{S(2)},\ \ldots,\ [\mathfrak{y}_1] \star [\mathfrak{y}_2] \star \ldots [\mathfrak{y}_N] \star a_{S(M)}\big).$$

3 **Вернуть** B.

Протокол 5.3. Идеальный функционал протокола выдачи карты

Вход: $c^{(0)}$ — карта из перетасованной колоды, N — количество игроков, $Cl(\mathcal{O})$ — группа классов идеалов порядка $\mathcal{O}$ в мнимом квадратичном поле, $Y = \{[\mathfrak{y}_1], \ldots, [\mathfrak{y}_N]\} \subset Cl(\mathcal{O})$ — множество секретных ключей пользователей.

Выход: открытая карта c.

1 TTP вычисляет $c := [\mathfrak{y}_1]^{-1} \star [\mathfrak{y}_2]^{-1} \star \cdots \star [\mathfrak{y}_N]^{-1} \star c^{(0)}$.

2 **Вернуть** c.

Модель злоумышленника

В контексте описанного протокола рассмотрим две модели злоумышленника: *Honest-But-Curious* и *Malicious* [36]. В обоих случаях злоумышленник является одним из игроков. В модели *Honest-But-Curious* злоумышленником является игрок, который честно следует протоколу, но обладает способностью анализировать полученную в ходе игры информацию для получения выгоды. В подобном случае достаточно быть уверенным, что такой игрок не сможет получить преимущество, анализируя полученную информацию. Вариант протокола без валидации направлен как раз на борьбу с подобным типом игроков. В модели *Malicious* злоумышленник может не только анализировать информацию, но и произвольно изменять отправляемые им данные. Для защиты от этого необходимо не только применять все те же методы, что и в модели *Honest-But-Curious*, но и проверять валидность полученной информации. Для этого в варианте протокола с валидацией используются протоколы доказательства с нулевым разглашением.

Введём понятие Knowledge для участника протокола. Knowledge участника протокола состоит из его секретных входных значений, случайных данных и всех сообщений, полученных в ходе выполнения протокола. Knowledge злоумышленника состоит из объединения Knowledge всех скомпрометированных сторон. Вся информация, которую злоумышленник может получить из протокола, должна быть вычисляемой за полиномиальное время из его Knowledge. Введём также понятие симулятора Sim. Под симулятором понимается некий оракул, который может вычислить Knowledge злоумышленника.

Более формально *Honest-But-Curious* злоумышленника можно описать следующим образом. Пусть есть протокол π и его идеальная функциональность $\mathcal{F}$;

$\mathcal{C} \subset \{P_1, P_2, \ldots, P_N\}$ — множество злоумышленников среди игроков; Sim — симулятор протокола. Определим следующие распределения случайных значений:

— $\mathsf{Real}_\pi(k, \mathcal{C}, x_1, \ldots, x_N)$: выполняет протокол с параметром стойкости k, где каждый участник P_i честно следует протоколу, используя входные секретные значения x_i. Пусть V_i обозначает $\mathsf{Knowledge}$ участника P_i, а y_i — его выходное значение. Выходом является $(V_1, \ldots, V_N)$, $(y_1, \ldots, y_N)$.

— $\mathsf{Ideal}_{\mathcal{F},\mathsf{Sim}}(k, \mathcal{C}, x_1, \ldots, x_N)$: вычисляет $(y_1, \ldots, y_N) = \mathcal{F}(x_1, \ldots, x_N)$. Выходом является $\mathsf{Sim}(\mathcal{C}, \{(x_i, y_i) : P_i \in \mathcal{C}\})$, $(y_1, \ldots, y_N)$.

Протокол считается стойким в *Honest-But-Curious*-модели злоумышленника, если злоумышленники в реальном протоколе имеют $\mathsf{Knowledge}$, неотличимое от их $\mathsf{Knowledge}$ в симуляторе.

Malicious злоумышленник, в отличие от *Honest-But-Curious*, может не только анализировать полученную в ходе протокола информацию, но и произвольно менять отправляемые данные. Это означает, что сообщения, посылаемые злоумышленником в данной модели, не могут быть заранее определены. Пусть $\mathcal{A}$ — алгоритм, которым руководствуется злоумышленник в реальном протоколе. Обозначим $\mathrm{corrupt}(\mathcal{A})$ множество участников, скомпрометированных злоумышленником, а $\mathrm{corrupt}(\mathsf{Sim})$ — множество участников, скомпрометированных злоумышленником в идеальной функциональности. Определим следующие распределения случайных значений:

— $\mathsf{Real}_{\pi,\mathcal{A}}(k, \{x_i : P_i \notin \mathrm{corrupt}(\mathcal{A})\})$: выполняет протокол с параметром стойкости k, где каждый участник $P_i \notin \mathrm{corrupt}(\mathcal{A})$ выполняет протокол честно, используя свои секретные входные значения x_i, а сообщения, отправляемые злоумышленниками, выбираются согласно алгоритму $\mathcal{A}$. Пусть y_i обозначает выходное значение каждого честного участника P_i, а V_i — $\mathsf{Knowledge}$ участника P_i. Выходом является $(\{V_i : P_i \in \mathrm{corrupt}(\mathcal{A})\}, \{y_i : P_i \notin \mathrm{corrupt}(\mathcal{A})\})$.

— $\mathsf{Ideal}_{\mathcal{F},\mathsf{Sim}}(k, \{x_i : P_i \notin \mathrm{corrupt}(\mathcal{A})\})$: вычисляет множество входных значений для злоумышленников $\{x_i : P_i \in \mathrm{corrupt}(\mathcal{A})\}$. Затем вычисляет $(y_1, \ldots, y_N) = = \mathcal{F}(x_1, \ldots, x_N)$, передаёт $\{y_i : P_i \in \mathrm{corrupt}(\mathcal{A})\}$ в Sim. Обозначим V^* выход Sim. Тогда выходом является $(V^*, \{y_i : P_i \notin \mathrm{corrupt}(\mathcal{A})\})$.

Протокол считается стойким в *Malicious*-модели злоумышленника, если для любого злоумышленника $\mathcal{A}$ существует симулятор Sim ($\mathrm{corrupt}(\mathcal{A}) = \mathrm{corrupt}(\mathsf{Sim})$), такой, что для любых входных значений честных участников распределения $\mathsf{Real}_{\pi,\mathcal{A}}(k, \{x_i : P_i \notin \notin \mathrm{corrupt}(\mathcal{A})\})$ и $\mathsf{Ideal}_{\mathcal{F},\mathsf{Sim}}(k, \{x_i : P_i \notin \mathrm{corrupt}(\mathcal{A})\})$ неотличимы друг от друга.

Доказательство стойкости в Honest-But-Curious-модели злоумышленника

Теорема 1. Протокол 3.1 неотличим от протокола 5.1 для модели злоумышленника *Honest-But-Curious*.

Доказательство. Протокол 5.1 генерирует набор из M случайных кривых. Докажем, что результаты протокола 3.1 неотличимы от случайных, если хотя бы один из игроков действовал честно.

Пусть существует вероятностный алгоритм $\mathcal{A}$, который для входных открытых колод A_1 и A_2 пытается угадать, какая из колод была сгенерирована с помощью протокола 3.1, и выдаёт в качестве результата значение $r \in \{1, 2\}$ — номер открытой колоды. Если для любого вероятностного алгоритма $\mathcal{A}$ при любых действиях злоумышленников вероятность успешно угадать, какая колода была сгенерирована протоколом 3.1, не превышает $1/2 + negl$, где $negl$ — пренебрежимо малая величина, то можно считать, что протоколы 3.1 и 5.1 неотличимы.

Проведём следующий эксперимент. Пусть задан порядок $\mathcal{O}$ в мнимом квадратичном поле, $Cl(\mathcal{O})$ — группа классов идеалов, $\mathscr{E}\ell\ell(\mathcal{O})$ — множество изогенных эллиптических кривых, $\star : Cl(\mathcal{O}) \times \mathscr{E}\ell\ell(\mathcal{O}) \to \mathscr{E}\ell\ell(\mathcal{O})$ — групповое действие и $b \in \{0, 1\}$. Тогда эксперимент $\mathsf{Exp}_1(b)$ с входным значением b выполняется следующим образом. Злоумышленник $\mathcal{A}$ сгенерировал колоду $X = \{x_1, x_2, \dots x_M\}$ и у него есть доступ к оракулу Oracle_b^1, который получает на вход колоду X и в зависимости от значения b вычисляет результат Y следующим образом:

1) если $b = 0$, то $Y := \{[\mathfrak{x}_i] \star x_i : x_i \in X\}$ для $i \in \{1, \dots, M\}$, где $[\mathfrak{x}_i] \xleftarrow{\$} Cl(\mathcal{O})$;
2) если $b = 1$, то $Y := \{y_1, y_2, \dots, y_M\}$, где $y_i \xleftarrow{\$} \mathscr{E}\ell\ell(\mathcal{O})$.

Злоумышленник $\mathcal{A}$ получает Y и выдаёт $b' \in \{0, 1\}$.

Преимущество злоумышленника $\mathcal{A}$ в Exp^1 определяется как

$$\mathsf{Adv}^1(\mathcal{A}) = \left|\Pr\left[\mathcal{A}(\mathsf{Exp}^1(b = 1)) \to 1\right] - \Pr\left[\mathcal{A}(\mathsf{Exp}^1(b = 0)) \to 1\right]\right|.$$

Так как в случае $b = 0$ оракул генерирует случайные значения $[\mathfrak{x}_i]$, взятые из равномерного распределения над $Cl(\mathcal{O})$, то кривая, вычисленная таким образом, также получена из равномерного распределения над $\mathscr{E}\ell\ell(\mathcal{O})$. Это ничем не отличается от результата в случае $b = 1$. Таким образом, отличить эти два случая для злоумышленника $\mathcal{A}$ наверняка невозможно. Тогда найдётся такая пренебрежимо малая функция $negl$, что $\mathsf{Adv}^1(\mathcal{A}) \leqslant negl(\lambda)$, где λ — параметр стойкости.

Очевидно, что в Exp^1 случай Oracle_0^1 соответствует протоколу 3.1 в худшем случае, где все пользователи, кроме одного, являются злоумышленниками в модели *Honest-But-Curious*, а Oracle_1^1 соответствует протоколу 5.1. ■

Следствие 1. Свойство 1 выполняется, пока есть хотя бы один честный игрок, не участвующий в сговоре.

Теорема 2. Если верно предположение о сложности задачи обратного группового действия, то протокол 3.2 неотличим от протокола 5.2 для *Honest-But-Curious*-модели злоумышленника.

Доказательство. Докажем, что перемешивание колоды протоколом 3.2 неотличимо от случайного, если хотя бы один из игроков действует честно.

Пусть существует вероятностный алгоритм $\mathcal{A}$, который для входных закрытых колод B_1 и B_2, которые получены из одной открытой колоды A, пытается угадать, какая из колод была перемешана с помощью протокола 3.2, и выдаёт значение $r \in \{1, 2\}$ — номер закрытой колоды, перемешанной протоколом 3.2. Если для любого алгоритма $\mathcal{A}$ при любых действиях злоумышленников вероятность успешно угадать, какая колода была перемешана протоколом 3.2, не превышает $1/2 + negl$, то можно считать, что протоколы 3.2 и 5.2 неотличимы.

Пусть только игрок P_j действует честно, а за всех остальных игроков действует злоумышленник. Пусть игрок P_j получает от игрока P_{j-1} (злоумышленника) частично перемешанную колоду $B^{(j-1)}$. Далее в протоколе 3.2 пользователь P_j выбирает случайную перестановку $S_i : \{1, \dots, M\} \to \{1, \dots, M\}$ и с помощью неё и своего секретного ключа $[\mathfrak{y}_j]$ получает новую колоду $B^{(j)}$:

$$B^{(j)} := ([\mathfrak{y}_j] \star b^{(j-1)}_{S_j(1)}, [\mathfrak{y}_j] \star b^{(j-1)}_{S_j(2)}, \dots, [\mathfrak{y}_j] \star b^{(j-1)}_{S_j(M)}).$$

Далее колода передаётся злоумышленнику. Единственным способом для злоумышленника найти соответствие между картами колод $B^{(j)}$ и $B^{(j-1)}$ является решение задачи GAIP. Тогда преимущество Adv^2 злоумышленника $\mathcal{A}$ равно вероятности того, что

$\mathcal{A}$ решит задачу GAIP за разумное время (время проведения игры). Так как GAIP считается сложной задачей, найдётся пренебрежимо малая функция $negl$, такая, что $\mathsf{Adv}^2 \leqslant negl(\lambda)$. Таким образом, перемешанная колода в итоге будет неотличима от случайной. ■

Следствие 2. Свойство 2 выполняется, пока есть хотя бы один честный игрок, не участвующий в сговоре, так как для того, чтобы замешать карты в нужном порядке, злоумышленнику необходимо решить задачу GAIP.

Теорема 3. Если верно предположение о сложности задачи обратного группового действия, то в протоколе 3.3 никто, кроме игрока, которому выдаётся карта, не сможет узнать содержимое карты для *Honest-But-Curious*-модели злоумышленника.

Доказательство. Пусть есть закрытая карта b и соответствующая ей открытая карта a. Тогда между ними есть зависимость

$$b = [\mathfrak{y}_1] \star [\mathfrak{y}_2] \star \cdots \star [\mathfrak{y}_N] \star a,$$

где $[\mathfrak{y}_1], [\mathfrak{y}_2], \ldots, [\mathfrak{y}_N]$ — маски игроков.

При выдаче карты игроку P_k остальные игроки последовательно снимают маски:

$$\begin{aligned}
c^{(1)} &= [\mathfrak{y}_2] \star \cdots \star [\mathfrak{y}_N] \star a,\\
c^{(2)} &= [\mathfrak{y}_3] \star \cdots \star [\mathfrak{y}_N] \star a,\\
&\cdots\\
c^{(k-1)} &= [\mathfrak{y}_k] \star \cdots \star [\mathfrak{y}_N] \star a,\\
c^{(k+1)} &= [\mathfrak{y}_k] \star [\mathfrak{y}_{k+2}] \star \cdots \star [\mathfrak{y}_N] \star a,\\
&\cdots\\
c^{(N)} &= [\mathfrak{y}_k] \star a.
\end{aligned}$$

В конце игрок P_k снимает свою маску $[\mathfrak{y}_k]$ и узнаёт открытую карту a.

В худшем случае, если все остальные игроки объединят полученную в ходе протокола информацию, а именно $b, c^{(1)}, c^{(2)}, \ldots, c^{(N)}$, они всё равно не смогут узнать открытую карту a за время игры, так как для этого необходимо решить задачу обратного группового действия. ■

Необходимо отметить, что протоколы 3.3 и 5.3 неотличимы друг от друга для злоумышленника $\mathcal{A}$, так как при одинаковых входных параметрах они выдают одну и ту же открытую карту.

4.2. Стойкость протоколов с валидацией

Протоколы 4.1, 4.2 и 4.3 (см. Приложение 1) отличаются от протоколов 5.1, 5.2 и 5.3 соответственно наличием верификации полученных пользователями значений с помощью протоколов доказательства с нулевым разглашением. Докажем, что протоколы ZKP_1, ZKP_2 и ZKP_3 (см. Приложение 2) являются протоколами с нулевым разглашением. Для доказательства воспользуемся понятием Σ-протокола.

Σ-протокол [37] — вид интерактивного доказательства с нулевым разглашением, в котором участвуют две стороны (доказывающий и проверяющий) и который состоит из трёх раундов:

1) Свидетельство: доказывающий вычисляет некоторое свидетельство на основе сгенерированного случайного значения и отправляет его проверяющему.

2) Запрос: проверяющий генерирует случайный запрос из допустимого набора и отправляет его доказывающему.
3) Ответ: доказывающий вычисляет ответ на основе секрета, свидетельства и запроса и отправляет ответ проверяющему.

Проверяющий либо принимает ответ, либо не принимает.

Σ-протокол должен удовлетворять трём свойствам:

1) Полнота. Если доказывающий и проверяющий запускают протокол и честно следуют ему, а доказывающий действительно знает секрет, то проверяющий всегда примет доказательство.
2) Корректность. Если доказывающий действительно знает секрет, то он всегда сможет убедить в этом проверяющего. Чтобы доказать это свойство, необходимо показать, что, зная передаваемую информацию для разных запросов и одного и того же свидетельства, можно найти секрет. Таким образом, свойство корректности гарантирует, что доказывающий знает секрет, а не угадывает его.
3) Нулевое разглашение для честного проверяющего (Honest Verifier Zero-Knowledge, HVZK). Проверяющий, честно следующий протоколу, не может узнать ничего о секрете доказывающего.

Доказав, что представленные в работе протоколы удовлетворяют свойствам Σ-протоколов, мы установим, что они удовлетворяют свойствам протоколов с нулевым разглашением.

Теорема 4. Протокол ZKP_1 является Σ-протоколом и обладает свойствами полноты, корректности и HVZK.

Доказательство.

1) Полнота. Предположим, что протокол выполняется честно. Пусть доказывающий выбрал $[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$ и вычислил кривую E.

Если проверяющий отправляет $c = 0$, то получает в ответ $[\mathfrak{r}] = [\mathfrak{b}]$ и вычисляет $E' = [\mathfrak{b}] \star E_1 = E$.

Если проверяющий отправляет $c = 1$, то получает в ответ $[\mathfrak{r}] = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$ и вычисляет

$$E' = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \star E_2 = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \cdot [\mathfrak{x}] \star E_1 = [\mathfrak{b}] \star E_1 = E.$$

В обоих случаях проверяющий получает корректный результат и протокол возвращает значение ИСТИНА. Таким образом, свойство полноты выполняется.

2) Корректность. Пусть даны два набора $(E, 0, [\mathfrak{r}_1])$ и $(E, 1, [\mathfrak{r}_2])$, которые были приняты проверяющим. Тогда $E = [\mathfrak{r}_1] \star E_1 = [\mathfrak{r}_2] \star E_2$. Отсюда следует, что $E = [\mathfrak{r}_1] \star E_1 = = [\mathfrak{r}_2] \cdot [\mathfrak{x}] \star E_1$. Следовательно, секрет может быть извлечён как $[\mathfrak{x}] = [\mathfrak{r}_1] \cdot [\mathfrak{r}_2]^{-1}$. Таким образом, свойство корректности выполняется.

3) Нулевое разглашение для честного проверяющего. Пусть проверяющий честно следует протоколу; $\mathcal{S}$ — симулятор, получающий на вход (E_1, E_2, c) и возвращающий $(E, c, [\mathfrak{r}])$ (при этом $\mathcal{S}$ не знает секрет $[\mathfrak{x}]$). Итоговая E вычисляется как

$$E = [\mathfrak{r}] \star E_{c+1}.$$

Можно заметить, что и в случае проведения самого протокола, и в случае работы симулятора $\mathcal{S}$ значение $[\mathfrak{r}]$ имеет равномерное распределение, поэтому наборы передаваемых данных в обоих случаях будут неотличимы. Таким образом, свойство нулевого разглашения для честного проверяющего выполняется.

Итак, протокол ZKP_1 является Σ-протоколом и, следовательно, протоколом с нулевым разглашением. ■

Теорема 5. Протокол ZKP_2 является Σ-протоколом и обладает свойствами полноты, корректности и HVZK.

Доказательство.

1) Полнота. Предположим, что протокол выполняется честно. На вход поступают два набора кривых $B^{(1)} = \{B_1^{(1)}, B_2^{(1)}, \ldots, B_M^{(1)}\}$ и $B^{(2)} = \{B_1^{(2)}, B_2^{(2)}, \ldots, B_M^{(2)}\}$, где $B_j^{(i)} \in \in \mathscr{E}\ell\ell(\mathcal{O})$ для $i \in \{1,2\}$ и $j \in \{1,\ldots,M\}$. Пусть доказывающий выбрал $[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$ и случайную перестановку S_b и с их помощью вычислил кривую b_0^b и набор кривых B^b. Если проверяющий отправляет $c = 0$, то получает в ответ $S_r = S_b$, $[\mathfrak{r}] = [\mathfrak{b}]$ и вычисляет

$$B' = \{[\mathfrak{r}] \star B_{S_r(i)}^{(c+1)} : i \in \{1,\ldots,M\}\} = \{[\mathfrak{b}] \star B_{S_b(i)}^{(1)} : i \in \{1,\ldots,M\}\} = B^b,$$
$$b_0' = [\mathfrak{r}] \star b_0^{(c+1)} = [\mathfrak{b}] \star b_0^{(1)} = b_0^b.$$

Если проверяющий отправляет $c = 1$, то получает в ответ $S_r = S^{-1}(S_b)$, $[\mathfrak{r}] = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$ и вычисляет

$$B' = \{[\mathfrak{r}] \star B_{S_r(i)}^{(c+1)} : i \in \{1,\ldots,M\}\} = \{([\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}) \star B_{S^{-1}(S_b(i))}^{(2)} : i \in \{1,\ldots,M\}\} =$$
$$= \{([\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \cdot [\mathfrak{x}]) \star B_{S(S^{-1}(S_b(i)))}^{(1)} : i \in \{1,\ldots,M\}\} = \{[\mathfrak{b}] \star B_{S_b(i)}^{(1)} : i \in \{1,\ldots,M\}\} = B^b,$$
$$b_0' = [\mathfrak{r}] \star b_0^{(c+1)} = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \star b_0^{(2)} = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \cdot [\mathfrak{x}] \star b_0^{(1)} = b_0^b.$$

В обоих случаях проверяющий получает корректный результат и протокол возвращает значение ИСТИНА. Таким образом, свойство полноты выполняется.

2) Корректность. Пусть даны два набора $(B^b, b_0^b, 0, [\mathfrak{r}_1], S_{r_1})$ и $(B^b, b_0^b, 1, [\mathfrak{r}_2], S_{r_2})$, которые были приняты проверяющим. Тогда

$$b_0^b = [\mathfrak{r}_1] \star b_0^{(1)} = [\mathfrak{r}_2] \star b_0^{(2)},$$
$$B^b = \{[\mathfrak{r}_1] \star B_{S_{r_1}(i)}^{(1)} : i \in \{1,\ldots,M\}\} = \{[\mathfrak{r}_2] \star B_{S_{r_2}(i)}^{(2)} : i \in \{1,\ldots,M\}\}.$$

Отсюда следует, что

$$b_0^b = [\mathfrak{r}_1] \star b_0^{(1)} = [\mathfrak{r}_2] \cdot [\mathfrak{x}] \star b_0^{(1)},$$
$$B^b = \{[\mathfrak{r}_1] \star B_{S_{r_1}(i)}^{(1)} : i \in \{1,\ldots,M\}\} = \{[\mathfrak{r}_2] \cdot [\mathfrak{x}] \star B_{S(S_{r_2}(i))}^{(1)} : i \in \{1,\ldots,M\}\}.$$

Следовательно, секреты могут быть извлечены как $[\mathfrak{x}] = [\mathfrak{r}_1] \cdot [\mathfrak{r}_2]^{-1}$, $S = S_{r_1}(S_{r_2}^{-1})$.

3) Нулевое разглашение для честного проверяющего. Пусть проверяющий честно следует протоколу; $\mathcal{S}$ — симулятор, получающий на вход $(B^{(1)}, B^{(2)}, b_0^{(1)}, b_0^{(2)}, c)$ и возвращающий $(B^b, b_0^b, c, [\mathfrak{r}], S_r)$ (при этом $\mathcal{S}$ не знает секрет $[\mathfrak{x}], S$). Итоговые значения B^b и b_0^b вычисляются как

$$B^b = \{[\mathfrak{r}] \star B_{S_r(i)}^{(c+1)} : i \in \{1,\ldots,M\}\}, \quad b_0^b = [\mathfrak{r}] \star b_0^{(c+1)}.$$

Можно заметить, что и в случае проведения самого протокола, и в случае работы симулятора $\mathcal{S}$ значения $[\mathfrak{r}]$ и S_r имеют равномерное распределение, поэтому наборы передаваемых данных в обоих случаях будут неотличимы. Таким образом, свойство нулевого разглашения для честного проверяющего выполняется.

Необходимые свойства выполняются, поэтому протокол ZKP_2 является Σ-протоколом и, следовательно, протоколом с нулевым разглашением. ■

Теорема 6. Протокол ZKP_3 является Σ-протоколом и обладает свойствами полноты, корректности и HVZK.

Доказательство.

1) Полнота. Предположим, что протокол выполняется честно. Пусть доказывающий выбрал $[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$ и вычислил кривые E_1 и E_2.

Если проверяющий отправляет $c = 0$, то получает в ответ $[\mathfrak{r}] = [\mathfrak{b}]$ и вычисляет $E'_1 = [\mathfrak{b}] \star E_{11} = E_1$ и $E'_2 = [\mathfrak{b}] \star E_{21} = E_2$.

Если проверяющий отправляет $c = 1$, то получает в ответ $[\mathfrak{r}] = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$ и вычисляет

$$E'_1 = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \star E_{12} = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \cdot [\mathfrak{x}] \star E_{11} = [\mathfrak{b}] \star E_{11} = E_1,$$
$$E'_2 = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \star E_{22} = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \cdot [\mathfrak{x}] \star E_{21} = [\mathfrak{b}] \star E_{21} = E_2.$$

В обоих случаях проверяющий получает корректный результат и протокол возвращает значение ИСТИНА. Таким образом, свойство полноты выполняется.

2) Корректность. Пусть даны два набора $(E_1, E_2, 0, [\mathfrak{r}_1])$ и $(E_1, E_2, 1, [\mathfrak{r}_2])$, которые были приняты проверяющим. Тогда

$$E_1 = [\mathfrak{r}_1] \star E_{11} = [\mathfrak{r}_2] \star E_{12}, \quad E_2 = [\mathfrak{r}_1] \star E_{21} = [\mathfrak{r}_2] \star E_{22}.$$

Отсюда следует, что $E_1 = [\mathfrak{r}_1] \star E_{11} = [\mathfrak{r}_2] \cdot [\mathfrak{x}] \star E_{11}$, $E_2 = [\mathfrak{r}_1] \star E_{21} = [\mathfrak{r}_2] \cdot [\mathfrak{x}] \star E_{21}$. Следовательно, секрет может быть извлечён как $[\mathfrak{x}] = [\mathfrak{r}_1] \cdot [\mathfrak{r}_2]^{-1}$. Таким образом, свойство корректности выполняется.

3) Нулевое разглашение для честного проверяющего. Пусть проверяющий честно следует протоколу; $\mathcal{S}$ — симулятор, получающий $(E_{11}, E_{12}, E_{21}, E_{22}, c)$ и возвращающий $(E_1, E_2, c, [\mathfrak{r}])$ (при этом $\mathcal{S}$ не знает секрет $[\mathfrak{x}]$). Итоговые E_1, E_2 вычисляются как $E_1 = [\mathfrak{r}] \star E_{1(c+1)}$, $E_2 = [\mathfrak{r}] \star E_{2(c+1)}$. Можно заметить, что и в случае проведения самого протокола, и в случае работы симулятора $\mathcal{S}$ значение $[\mathfrak{r}]$ имеет равномерное распределение, поэтому наборы передаваемых данных в обоих случаях будут неотличимы. Таким образом, свойство нулевого разглашения для честного проверяющего выполняется.

Необходимые свойства выполняются, поэтому протокол ZKP_3 является Σ-протоколом и, следовательно, протоколом с нулевым разглашением. ■

Теорема 7. Если верно предположение о сложности задачи обратного группового действия, то протоколы 4.1, 4.2 и 4.3 неотличимы от протоколов 5.1, 5.2 и 5.3 соответственно для *Malicious*-модели злоумышленника.

Доказательство. Протоколы 4.1–4.3 отличаются от протоколов 5.1–5.3 наличием верификации полученных пользователями значений с помощью протоколов доказательства с нулевым разглашением. В теоремах 4–6 доказано, что протоколы ZKP_1, ZKP_2 и ZKP_3 являются Σ-протоколами, то есть они не разглашают никакой информации о секрете. Если при проверке доказательства будет выявлено нарушение, то протокол будет остановлен. Таким образом, злоумышленник не сможет действовать никак иначе, кроме как следовать протоколу, а значит, он будет действовать как *Honest-But-Curious* злоумышленник, поэтому все доводы, приведённые в теоремах 1–3, остаются достоверными и для протоколов 4.1, 4.2 и 4.3. Вследствие этого работа данных протоколов неотличима от работы протоколов 5.1, 5.2 и 5.3 соответственно. ■

5. Быстродействие протокола

Описанный протокол реализован на языке программирования C [38] с использованием сторонней библиотеки faster-csidh [39]. Для оценки быстродействия замерено

время подготовки колоды, тасования колоды и выдачи карты с валидацией и без. Все замеры производились на персональном компьютере с процессором AMD Ryzen 7 5800H.

На рис. 1 показана зависимость от количества игроков времени работы протоколов без валидации для колоды из 52 карт.

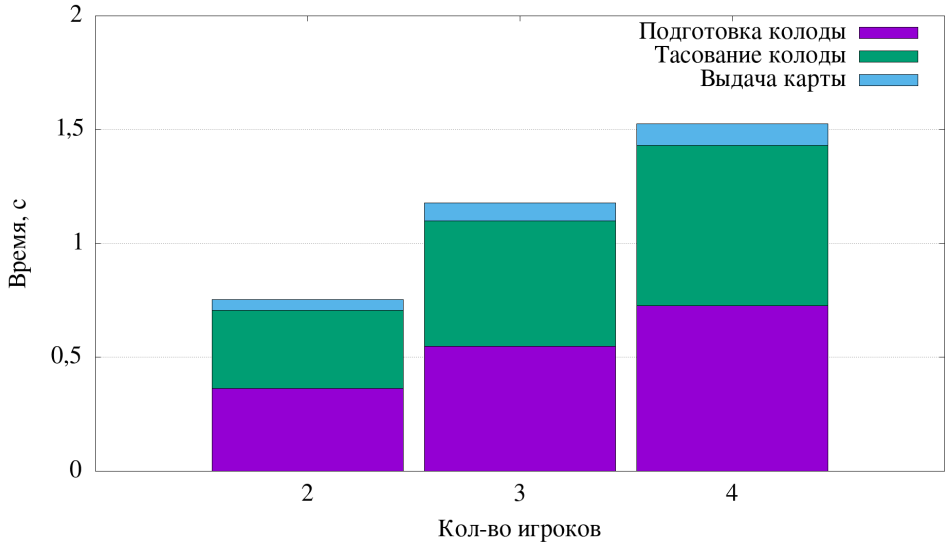

Рис. 1. Зависимость времени работы протоколов без валидации от количества игроков

На рис. 2 показана зависимость от количества игроков времени работы протоколов с валидацией для колоды из 52 карт и параметром стойкости 20 (под параметром стойкости понимается количество итераций ZKP_1, ZKP_2, ZKP_3). Так как шанс успешного обмана для каждой итерации протокола доказательства с нулевым разглашением равен $1/2$, параметр стойкости 20 обеспечивает общий шанс обмана 2^{-20}. Выбор такого уровня стойкости обусловлен его оптимальностью: при параметре стойкости 20 протокол работает за приемлемое время и за время проведения игры пользователи не смогут нарушить стойкость протокола.

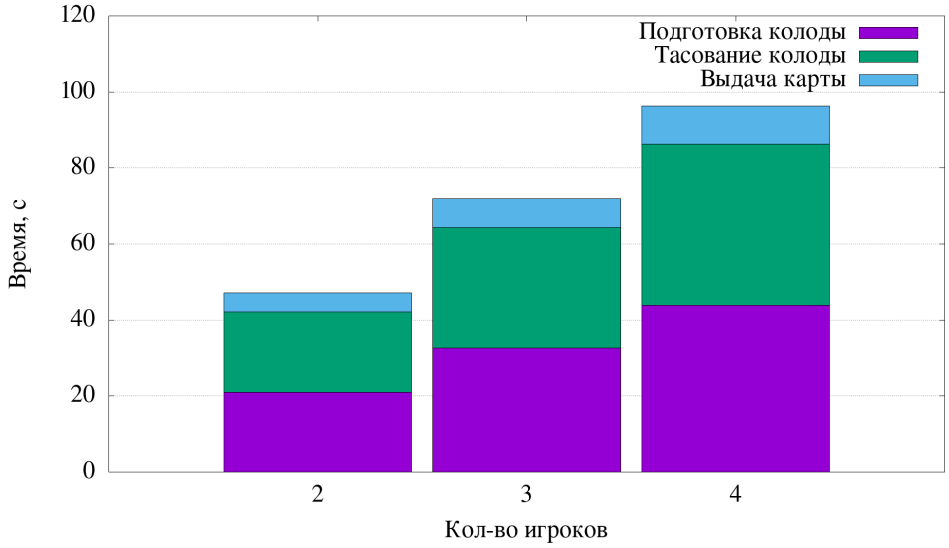

Рис. 2. Зависимость времени работы протоколов с валидацией от количества игроков

Можно заметить, что при добавлении валидации время выполнения протоколов возрастает в несколько раз, поскольку групповое действие является затратной операцией.

На рис. 3 показана зависимость от параметра стойкости времени работы протоколов с валидацией для колоды из 52 карт и для трёх игроков.

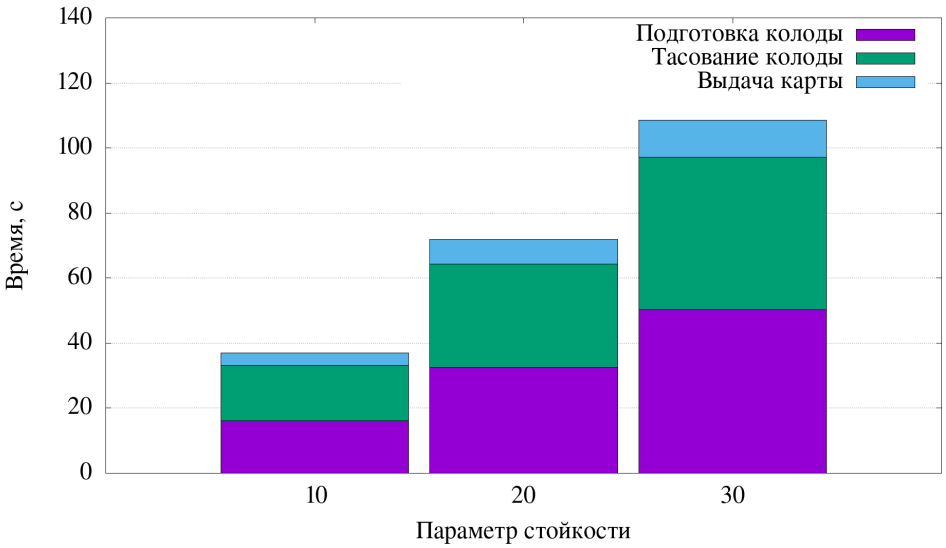

Рис. 3. Зависимость времени работы протоколов от параметра стойкости с валидацией

Замеры времени выполнения протокола с валидацией показывают, что в среднем при параметре стойкости 20 для создания перетасованной колоды требуется 21,42 с на одного игрока, что позволяет применять данное решение на практике. Решение, представленное в [33], при таком же параметре стойкости требовало 28,78 с на игрока для создания открытой колоды. Конечно, следует учитывать, что работа [33] написана в 2012 г., а с тех пор мощность среднего персонального компьютера заметно возросла.

Затраты по памяти представлены в таблице, где N — количество игроков, а λ — параметр стойкости.

Затраты памяти

Объект	Размер хранимых данных, байт
Карта	64
Колода карт	$64\,N$
Секретная маска карты	74
Протокол	**Размер передаваемых данных, байт**
ZKP_1 Commit	$(64+74)(N+1)\,\lambda$
ZKP_1 Responce	$74(N+1)\,\lambda$
ZKP_2 Commit	$(64+74)(N+1)\,\lambda$
ZKP_2 Responce	$(74+(4+64)N)\,\lambda$
ZKP_3 Commit	$(2\cdot 64+74)\,\lambda$
ZKP_3 Responce	$74\,\lambda$

Заключение

В работе представлен постквантовый протокол ментального покера, основанный на задаче поиска изогений между суперсингулярными эллиптическими кривыми. Предложено два варианта протокола: без валидации (где подразумевается, что игроки будут строго следовать протоколу, но могут «подглядывать», если у них будет такая

возможность) и с валидацией (где любое нарушение протокола может быть обнаружено). Для каждого из представленных вариантов доказана безопасность в *Honest-But-Curious*- и *Malicious*-моделях злоумышленника для классического и квантового вычислителей, получены экспериментальные оценки по времени и по памяти.

Экспериментальные результаты показали, что время выполнения протокола, особенно без валидации, позволяет применять его на практике. Создание перетасованной колоды из 52 карт занимает около 21,42 с на игрока. Тем не менее для широкого применения потребуется оптимизация протокола с целью сокращения времени выполнения, особенно в режиме с валидацией, так как сложные криптографические вычисления требуют значительных ресурсов.

Основным преимуществом представленного протокола является устойчивость перед атаками на квантовом компьютере. В качестве дальнейших исследований стоит задача по оптимизации протокола по времени.

Помимо времени выполнения, стоит отметить требования протокола к памяти, которые подробно исследованы в ходе работы. Для каждого игрока объём данных включает 64 байта на карту и 74 байта на секретную маску карты. Для протоколов доказательства с нулевым разглашением требуются дополнительные ресурсы памяти.

Таким образом, представленный протокол ментального покера является квантово-устойчивым, гибким, эффективным. Перспективы дальнейшего развития включают оптимизацию вычислительных затрат и исследование возможностей применения подобных подходов в прикладных задачах.

ЛИТЕРАТУРА

1. *Shamir A., Rivest R. L., and Adleman L. M.* Mental Poker / D. A. Klarner (eds). The Mathematical Gardner. Boston: Springer, 1981. P. 37–43.
2. *Lipton R.* How to cheat at mental poker // Proc. AMS Short Course on Cryptography. 1981. `https://cir.nii.ac.jp/crid/1570854175390364160`.
3. *Coppersmith D.* Cheating at mental poker // LNCS. 1986. V. 218. P. 104–107.
4. *Barany I. and Furedi Z.* Mental poker with three or more players // Inf. Control. 1984. V. 59. No. 1–3. P. 84–93.
5. *Jabbar Z. S. and Aboud S. J.* An efficient poker protocol for shuffling and dealing cards // Intern. J. Innovative Technol. Exploring Engin. 2019. V. 8. No. 12. P. 2175–2179.
6. *Aranha D. F., Baum C., Gjøsteen K., and Silde T.* Verifiable Mix-Nets and Distributed Decryption for Voting from Lattice-Based Assumptions. Cryptology ePrint Archive. 2022. Paper 2022/422. `https://eprint.iacr.org/2022/422`.
7. *Haines T., Goré R., and Sharma B.* Did you mix me? Formally verifying verifiable mix nets in electronic voting // Proc. SP'2021. San Francisco, CA, USA, 2021. P. 1748–1765.
8. *Lin K., Wang W., Zhao C.-A., and Zhao Y.* π-signHD: A New Structure for the SQIsign Family with Flexible Applicability. Cryptology ePrint Archive. 2024. Paper 2024/1404. `https://eprint.iacr.org/2024/1404`.
9. *Nakagawa K. and Onuki H.* SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies. Cryptology ePrint Archive. 2024. Paper 2024/771. `https://eprint.iacr.org/2024/771`.
10. *Borin G., Lai Y.-F., and Leroux A.* Erebor and Durian: Full Anonymous Ring Signatures from Quaternions and Isogenies. Cryptology ePrint Archive. 2024. Paper 2024/1185. `https://eprint.iacr.org/2024/1185`.

11. *Duparc M. and Fouotsa T. B.* SQIPrime: A Dimension 2 Variant of SQISignHD with Non-Smooth Challenge Isogenies. Cryptology ePrint Archive. 2024. Paper 2024/773. https://eprint.iacr.org/2024/773.
12. *Levin S. and Pedersen R.* Faster Proofs and VRFs from Isogenies. Cryptology ePrint Archive. 2024. Paper 2024/1626. https://eprint.iacr.org/2024/1626.
13. *El Baraka M. and Ezzouak S.* Isogeny-Based Secure Voting Systems for Large-Scale Elections. Cryptology ePrint Archive. 2024. Paper 2024/1472. https://eprint.iacr.org/2024/1472.
14. *Moriya T.* IS-CUBE: An Isogeny-Based Compact KEM Using a Boxed SIDH Diagram. Cryptology ePrint Archive. 2023. Paper 2023/1506. https://eprint.iacr.org/2023/1506.
15. *De Feo L., Fouotsa T. B., Kutas P., et al.* SCALLOP: Scaling the CSI-FiSh. Cryptology ePrint Archive. 2023. Paper 2023/058. https://eprint.iacr.org/2023/058.
16. *Chen M., Leroux A., and Panny L.* SCALLOP-HD: Group Action from 2-dimensional Isogenies. Cryptology ePrint Archive. 2023. Paper 2023/1488. https://eprint.iacr.org/2023/1488.
17. *Stolbunov A.* Cryptographic Schemes Based on Isogenies. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/262577/529395_FULLTEXT01.pdf. 2012.
18. *Sotakova J.* Elliptic Curves, Isogenies, and Endomorphism Rings. https://janasotakova.eu/writings/ANTS_school_exposition.pdf. 2020.
19. *Velu J.* Isogenies entre courbes elliptiques // Comptes-Rendus de l'Academie des Sciences. 1971. V. 273. P. 238–241.
20. *Атья М., Макдональд И.* Введение в коммутативную алгебру. М.: Мир, 1972.
21. *Deuring M.* Die Typen der Multiplikatorenringe elliptischer Funktionenkörper // Ach. Math. Sem. Hab. 1941. P. 197–272.
22. *Eriksen J. K., Panny L., Sotáková J., and Veroni M.* Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic. Cryptology ePrint Archive. 2023. Paper 2023/106. https://eprint.iacr.org/2023/106.
23. *Conrad K.* Ideal Classes and the Kronecker Bound. https://kconrad.math.uconn.edu/blurbs/gradnumthy/classgroupKronecker.pdf.
24. *Alamati N., De Feo L., Montgomery H., and Patranabis S.* Cryptographic Group Actions and Applications. Cryptology ePrint Archive. 2020. Paper 2020/1188. https://eprint.iacr.org/2020/1188.
25. *Ростовцев А. Г., Маховенко Е. Б.* Теоретическая криптография. СПб.: АНО НПО «Профессионал», 2005.
26. *Beullens W., Kleinjung T., and Vercauteren F.* CSI-FiSh: efficient isogeny based signatures through class group computations. Cryptology ePrint Archive. 2019. Paper 2019/498. https://eprint.iacr.org/2019/498.
27. *Castryck W., Lange T., Martindale C., et al.* CSIDH: an efficient post-quantum commutative group action. Cryptology ePrint Archive. 2018. Paper 2018/383. https://eprint.iacr.org/2018/383.
28. *Campos F., Chavez-Saab J., Chi-Dominguez J.-J., et al.* Optimizations and Practicality of High-Security CSIDH. Cryptology ePrint Archive. 2023. Paper 2023/793. https://eprint.iacr.org/2023/793.
29. *Kuperberg G.* A subexponential-time quantum algorithm for the dihedral hidden subgroup problem // SIAM J. Computing. 2005. V. 35. No. 1. P. 170–188.
30. *Golle P.* Dealing cards in poker games // Proc. ITCC'05. Las Vegas, NV, USA, 2005. V. 1. P. 506–511.
31. *Castella-Roca J.* Contributions to Mental Poker. https://ddd.uab.cat/pub/tesis/2005/tdx-0131106-193157/jcr1de1.pdf. 2006.

32. *Barnett A. and Smart N. P.* Mental poker revisited // LNCS. 2003. V. 2898. P. 370–383.
33. *Wei T.-J. and Wang L.-C.* A fast mental poker protocol // J. Math. Cryptology. 2012. V. 6. No. 1. P. 39–68.
34. *Chaum D. and Pedersen T. P.* Wallet databases with observers // LNCS. 1993. V. 740. P. 89–105.
35. *Canetti R.* Universally Composable Security: A New Paradigm for Cryptographic Protocols. Cryptology ePrint Archive. 2000. Paper 2000/067. https://eprint.iacr.org/2000/067.
36. Secure Computation. https://www.cs.jhu.edu/~abhishek/classes/CS600-642-442-Fall2018/L12.pdf. 2018.
37. *Damgård I.* On Σ-protocols. https://www.cs.au.dk/~ivan/Sigma.pdf. 2010.
38. Isogeny Mental Card Game. https://github.com/IvanIoganson/isogeny_mental_card_game.git. 2024.
39. Faster-csidh. https://github.com/herumi/faster-csidh.git. 2023.

REFERENCES

1. *Shamir A., Rivest R. L., and Adleman L. M.* Mental Poker. D. A. Klarner (eds). The Mathematical Gardner. Boston, MA, Springer, 1981, pp. 37–43.
2. *Lipton R.* How to cheat at mental poker. Proc. AMS Short Course on Cryptography, 1981, https://cir.nii.ac.jp/crid/1570854175390364160.
3. *Coppersmith D.* Cheating at mental poker. LNCS, 1986, vol. 218, pp. 104–107.
4. *Barany I. and Furedi Z.* Mental poker with three or more players. Inf. Control, 1984, vol. 59, no. 1–3, pp. 84–93.
5. *Jabbar Z. S. and Aboud S. J.* An efficient poker protocol for shuffling and dealing cards. Intern. J. Innovative Technol. Exploring Engin., 2019, vol. 8, no. 12, pp. 2175–2179.
6. *Aranha D. F., Baum C., Gjøsteen K., and Silde T.* Verifiable Mix-Nets and Distributed Decryption for Voting from Lattice-Based Assumptions. Cryptology ePrint Archive, 2022, Paper 2022/422, https://eprint.iacr.org/2022/422.
7. *Haines T., Goré R., and Sharma B.* Did you mix me? Formally verifying verifiable mix nets in electronic voting. Proc. SP'2021, San Francisco, CA, USA, 2021, pp. 1748–1765.
8. *Lin K., Wang W., Zhao C.-A., and Zhao Y.* π-signHD: A New Structure for the SQIsign Family with Flexible Applicability. Cryptology ePrint Archive, 2024, Paper 2024/1404, https://eprint.iacr.org/2024/1404.
9. *Nakagawa K. and Onuki H.* SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies. Cryptology ePrint Archive, 2024, Paper 2024/771, https://eprint.iacr.org/2024/771.
10. *Borin G., Lai Y.-F., and Leroux A.* Erebor and Durian: Full Anonymous Ring Signatures from Quaternions and Isogenies. Cryptology ePrint Archive, 2024, Paper 2024/1185, https://eprint.iacr.org/2024/1185.
11. *Duparc M. and Fouotsa T. B.* SQIPrime: A Dimension 2 Variant of SQISignHD with Non-Smooth Challenge Isogenies. Cryptology ePrint Archive, 2024, Paper 2024/773, https://eprint.iacr.org/2024/773.
12. *Levin S. and Pedersen R.* Faster Proofs and VRFs from Isogenies. Cryptology ePrint Archive, 2024, Paper 2024/1626, https://eprint.iacr.org/2024/1626.
13. *El Baraka M. and Ezzouak S.* Isogeny-Based Secure Voting Systems for Large-Scale Elections. Cryptology ePrint Archive, 2024, Paper 2024/1472, https://eprint.iacr.org/2024/1472.
14. *Moriya T.* IS-CUBE: An Isogeny-Based Compact KEM Using a Boxed SIDH Diagram. Cryptology ePrint Archive. 2023. Paper 2023/1506. https://eprint.iacr.org/2023/1506.

15. *De Feo L., Fouotsa T. B., Kutas P., et al.* SCALLOP: Scaling the CSI-FiSh. Cryptology ePrint Archive, 2023, Paper 2023/058, https://eprint.iacr.org/2023/058.
16. *Chen M., Leroux A., and Panny L.* SCALLOP-HD: Group Action from 2-dimensional Isogenies. Cryptology ePrint Archive, 2023, Paper 2023/1488, https://eprint.iacr.org/2023/1488.
17. *Stolbunov A.* Cryptographic Schemes Based on Isogenies. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/262577/529395_FULLTEXT01.pdf, 2012.
18. *Sotakova J.* Elliptic Curves, Isogenies, and Endomorphism Rings. https://janasotakova.eu/writings/ANTS_school_exposition.pdf, 2020.
19. *Velu J.* Isogenies entre courbes elliptiques. Comptes-Rendus de l'Academie des Sciences, 1971, vol. 273, pp. 238–241.
20. *Atiyah M. F. and MacDonald I. G.* Introduction To Commutative Algebra. Addison-Wesley Publishing Company, Inc., 1969.
21. *Deuring M.* Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Ach. Math. Sem. Hab., 1941, pp. 197–272.
22. *Eriksen J. K., Panny L., Sotáková J., and Veroni M.* Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic. Cryptology ePrint Archive, 2023, Paper 2023/106, https://eprint.iacr.org/2023/106.
23. *Conrad K.* Ideal Classes and the Kronecker Bound. https://kconrad.math.uconn.edu/blurbs/gradnumthy/classgroupKronecker.pdf.
24. *Alamati N., De Feo L., Montgomery H., and Patranabis S.* Cryptographic Group Actions and Applications. Cryptology ePrint Archive, 2020, Paper 2020/1188, https://eprint.iacr.org/2020/1188.
25. *Rostovtsev A. G. and Makhovenko E. B.* Teoreticheskaya kriptografiya [Theoretical Cryptography]. Saint Petersburg, Professional Publ., 2005. (in Russian)
26. *Beullens W., Kleinjung T., and Vercauteren F.* CSI-FiSh: efficient isogeny based signatures through class group computations. Cryptology ePrint Archive, 2019, Paper 2019/498, https://eprint.iacr.org/2019/498.
27. *Castryck W., Lange T., Martindale C., et al.* CSIDH: an efficient post-quantum commutative group action. Cryptology ePrint Archive, 2018, Paper 2018/383, https://eprint.iacr.org/2018/383.
28. *Campos F., Chavez-Saab J., Chi-Dominguez J.-J., et al.* Optimizations and Practicality of High-Security CSIDH. Cryptology ePrint Archive, 2023, Paper 2023/793, https://eprint.iacr.org/2023/793.
29. *Kuperberg G.* A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM J. Computing, 2005, vol. 35, no. 1, pp. 170–188.
30. *Golle P.* Dealing cards in poker games. Proc. ITCC'05, Las Vegas, NV, USA, 2005, vol. 1, pp. 506–511.
31. *Castella-Roca J.* Contributions to Mental Poker. https://ddd.uab.cat/pub/tesis/2005/tdx-0131106-193157/jcr1de1.pdf, 2006.
32. *Barnett A. and Smart N. P.* Mental poker revisited. LNCS, 2003, vol. 2898, pp. 370–383.
33. *Wei T.-J. and Wang L.-C.* A fast mental poker protocol. J. Math. Cryptology, 2012, vol. 6, no. 1, pp. 39–68.
34. *Chaum D. and Pedersen T. P.* Wallet databases with observers. LNCS, 1993, vol. 740, pp. 89–105.
35. *Canetti R.* Universally Composable Security: A New Paradigm for Cryptographic Protocols. Cryptology ePrint Archive, 2000, Paper 2000/067, https://eprint.iacr.org/2000/067.

36. Secure Computation. `https://www.cs.jhu.edu/~abhishek/classes/CS600-642-442-Fall2018/L12.pdf`, 2018.
37. *Damgård I.* On Σ-protocols. `https://www.cs.au.dk/~ivan/Sigma.pdf`, 2010.
38. Isogeny Mental Card Game. `https://github.com/IvanIoganson/isogeny_mental_card_game.git`, 2024.
39. Faster-csidh. `https://github.com/herumi/faster-csidh.git`, 2023.

Приложение 1. Протокол с валидацией

Данная версия протокола включает в себя протоколы с нулевым разглашением и предназначена для защиты от злоумышленника, который может активно подменять посылаемую информацию для получения выгоды. Если один из игроков нарушит ход протокола, то данный факт можно будет однозначно доказать.

Протоколы подготовки и тасования колоды и выдачи карты описаны ниже как протоколы 4.1, 4.2 и 4.3 соответственно.

Протокол 4.1. Подготовка колоды

Вход: p — простое число, $E_0/\mathbb{F}_p$ — начальная эллиптическая кривая с $\mathrm{End}_{\mathbb{F}_p}(E_0) \cong \mathcal{O}$, $Cl(\mathcal{O})$ — группа классов идеалов порядка $\mathcal{O}$, M — количество карт, N — количество игроков.

Выход: открытая колода A, контрольное значение a_0.

Для $i = 1, \ldots, M$:
- $a_i^{(0)} := E_0$.
- **Для** $j = 1, \ldots, N$:
  - Игрок P_j выбирает $[\mathfrak{x}_j] \xleftarrow{\$} Cl(\mathcal{O})$.
  - Игрок P_j вычисляет $a_i^{(j)} := [\mathfrak{x}_j] \star a_i^{(j-1)}$.
  - Игрок P_j выполняет протокол ZKP_1 (см. Приложение 2) с остальными пользователями. В качестве открытых значений выступают $a_i^{(j-1)}$ и $a_i^{(j)}$, а в качестве секретного — $[\mathfrak{x}_j]$.

$A := \{a_i^{(N)}\}$ для $i \in \{1, \ldots, M\}$, $a_0 := a_0^{(N)}$.

Вернуть A, a_0.

Протокол 4.2. Тасование колоды

Вход: A — открытая колода, a_0 — контрольное значение, M — количество карт, N — количество игроков, $Cl(\mathcal{O})$ — группа классов идеалов (см. протокол 4.1).

Выход: перетасованная колода B, набор контрольных значений B_0.

$B^{(0)} := A$, $b_0^{(0)} := a_0$.

Для $i = 1, \ldots, N$:

- Игрок P_i выбирает случайную перестановку $S_i : \{1, \ldots, M\} \to \{1, \ldots, M\}$.
- Игрок P_i выбирает $[\mathfrak{y}_i] \xleftarrow{\$} Cl(\mathcal{O})$ и запоминает его.
- Игрок P_i вычисляет $B^{(i)} := ([\mathfrak{y}_i] \star b_{S_i(1)}^{(i-1)}, [\mathfrak{y}_i] \star b_{S_i(2)}^{(i-1)}, \ldots, [\mathfrak{y}_i] \star b_{S_i(M)}^{(i-1)})$, где $b_t^{(i-1)} \in B^{(i-1)}$, $t \in \{1, \ldots, M\}$.
- Игрок P_i вычисляет $b_0^{(i)} := [\mathfrak{y}_i] \star b_0^{(i-1)}$.
- Игрок P_i, выступая в роли доказывающего, выполняет протокол ZKP_2 (см. Приложение 2) со всеми остальными пользователями. В качестве открытыхП значений выступают $b_0^{(i-1)}$, $b_0^{(i)}$, $B^{(i-1)}$, $B^{(i)}$, а в качестве секретных — $[\mathfrak{y}_i]$ и S_i.

$B_0 := \{b_0^{(0)}, b_0^{(1)}, \ldots, b_0^{(N)}\}$, $B := B^{(N)}$.

Вернуть B, B_0.

Протокол 4.3. Выдача карты

Вход: $c^{(0)}$ — закрытая карта, $B_0 = \{b_0^{(0)}, b_0^{(1)}, \ldots, b_0^{(N)}\}$ — набор контрольных значений, k — номер игрока, которому эта карта предназначена, N — количество игроков.

Выход: карта c.

Для $j \in \{1, \ldots, N\} \setminus \{k\}$:

- Игрок P_j вычисляет $c^{(j)} := [\mathfrak{y}_j]^{-1} \star c^{(j-1)}$, где $[\mathfrak{y}_j]$ — секретная маска игрока j.
- Игрок P_j, выступая в роли доказывающего, выполняет протокол ZKP_3 (см. Приложение 2) со всеми остальными пользователями. В качестве открытых значений выступают $c^{(j-1)}, b_0^{(j)}, c^{(j)}$, $b_0^{(j-1)}$, а в качестве секретного — $[\mathfrak{y}_j]^{-1}$.

Игрок P_k вычисляет $c := [\mathfrak{y}_k]^{-1} \star c^{(N-1)}$, где $[\mathfrak{y}_k]$ — секретная маска игрока k.

Вернуть c.

Для открытия карты игрок P_j публикует ранее выданную карту c, а затем игрок P_j, выступая в роли доказывающего, выполняет протокол ZKP_3 (см. Приложение 2) со всеми остальными пользователями. В качестве открытых значений выступают $c^{(N)}, b_0^{(j)}, c, b_0^{(j-1)}$, а в качестве секретного — $[\mathfrak{y}_k]^{-1}$.

Приложение 2. Протоколы доказательства с нулевым разглашением

ZKP_1 (CSI-FiSh)
Доказать, что $E_2 = [\mathfrak{x}] \star E_1$.
Открытые значения: E_1, E_2.
Секрет: $[\mathfrak{x}] \in Cl(\mathcal{O})$.

	Доказывающий		**Проверяющий**
1 :	$[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$		
2 :	$E := [\mathfrak{b}] \star E_1$		
		$\xrightarrow{\quad E \quad}$	
3 :			$c \xleftarrow{\$} \{0,1\}$
		$\xleftarrow{\quad c \quad}$	
4 :	Если $c = 0$, то $[\mathfrak{r}] := [\mathfrak{b}]$ Иначе $[\mathfrak{r}] := [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$		
		$\xrightarrow{\quad [\mathfrak{r}] \quad}$	
5 :			$E' := [\mathfrak{r}] \star E_{c+1}$
6 :			Если $E' = E$, то ИСТИНА, иначе ЛОЖЬ.

ZKP_2 (Перетасовка)
Доказать, что $B^{(2)}$ получен из $B^{(1)}$ с помощью перестановки S и маски $[\mathfrak{x}]$ и что $b_0^{(2)} = [\mathfrak{x}] \star b_0^{(1)}$.
Открытые значения: $B^{(1)}, B^{(2)}, b_0^{(1)}, b_0^{(2)}$.
Секрет: $[\mathfrak{x}] \in Cl(\mathcal{O}), S : \{1, \ldots, M\} \to \{1, \ldots, M\}$.

	Доказывающий		**Проверяющий**
1 :	$[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$		
2 :	Случайная перестановка $S_b : \{1, \ldots, M\} \to \{1, \ldots, M\}$		
3 :	$B^b := ([\mathfrak{b}] \star B^{(1)}_{S_b(i)} \mid i \in \{1...M\})$ $b_0^b := [\mathfrak{b}] \star b_0^{(1)}$		
		$\xrightarrow{\quad B^b, b_0^b \quad}$	
4 :			$c \xleftarrow{\$} \{0,1\}$
		$\xleftarrow{\quad c \quad}$	
5 :	Если $c = 0$: $[\mathfrak{r}] := [\mathfrak{b}]$ $S_r := S_b$ Если $c = 1$: $[\mathfrak{r}] := [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$ $S_r := S^{-1}(S_b)$		
		$\xrightarrow{\quad [\mathfrak{r}], S_r \quad}$	
6 :			$B' := ([\mathfrak{r}] \star B^{(c+1)}_{S_r(i)} \mid i \in \{1...M\})$
7 :			$b'_0 := [\mathfrak{r}] \star b_0^{(c+1)}$
8 :			Если $B' = B^b$ и $b'_0 = b_0^b$, то ИСТИНА, иначе ЛОЖЬ.

ZKP_3 (Раскрытие)
Доказать, что $E_{12} = [\mathfrak{x}] \star E_{11}$ и $E_{22} = [\mathfrak{x}] \star E_{21}$.
Открытые значения: $E_{11}, E_{12}, E_{21}, E_{22}$.
Секрет: $[\mathfrak{x}] \in Cl(\mathcal{O})$.

	Доказывающий		**Проверяющий**
1 :	$[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$		
2 :	$E_1 := [\mathfrak{b}] \star E_{11}$		
3 :	$E_2 := [\mathfrak{b}] \star E_{21}$	$\xrightarrow{\quad E_1, E_2 \quad}$	
4 :			$c \xleftarrow{\$} \{0,1\}$
		$\xleftarrow{\quad c \quad}$	
5 :	Если $c = 0$, то $[\mathfrak{r}] := [\mathfrak{b}]$ Иначе $[\mathfrak{r}] := [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$		
		$\xrightarrow{\quad [\mathfrak{r}] \quad}$	
6 :			$E'_1 := [\mathfrak{r}] \star E_{1(c+1)}$
7 :			$E'_2 := [\mathfrak{r}] \star E_{2(c+1)}$
8 :			Если $E'_1 = E_1$ и $E'_2 = E_2$, то ИСТИНА, иначе ЛОЖЬ.