МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«Южный федеральный университет»

Институт математики, механики
и компьютерных наук им. И. И. Воровича

Кафедра алгебры и дискретной математики

Денисов Илия Игоревич

МОДИФИКАЦИЯ ПРИМИТИВА СОВРЕМЕННОГО КРИПТОГРАФИЧЕСКОГО АГРЕГАТА

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по направлению подготовки
01.03.02— Прикладная математика и информатика

Научный руководитель –
доц., к. т. н. Мкртичян Вячеслав Виталиевич

Допущено к защите:
заведующий кафедрой _____ Штейнберг Б.Я.

Ростов-на-Дону – 2023

Задание на выпускную квалификационную работу

студента 4-го курса бакалавриата Денисова И.И.

Направление подготовки: 01.03.02 – Прикладная математика и информатика.

Студент: Денисов И.И.

Научный руководитель: Мкртичян В.В.

Год защиты: 2023.

Тема работы: Модификация примитива современного криптографического агрегата.

Цели работы: Целями работы являются построение модификации не интерактивного протокола доказательства знания с нулевым разглашением "ZK-SNARK" путём расширения полиномиальной базы его квадратичной арифметической программы и анализ параметров модифицированного протокола.

Задачи работы:

– Изучение и описание протокола ZK-SNARK.

– Модификация протокола ZK-SNARK.

– Построение модельного примера для изначальной и модифицированной версий ZK-SNARK.

– Анализ параметров модифицированного протокола.

Научный руководитель В.В. Мкртичян

Студент И.И. Денисов

21 сентября 2022 г

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

СПРАВКА

о результатах проверки текстового документа
на наличие заимствований

Южный Федеральный Университет

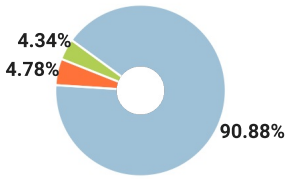
ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Денисов Илия Игоревич
Самоцитирование рассчитано для: Денисов Илия Игоревич
Название работы: ДЕНИСОВ_МОДИФИКАЦИЯ_ПРИМИТВА_СОВРЕМЕННОГО_КРИПТОГРАФИЧЕСКОГО_АГРЕГАТА
Тип работы: Не указано
Подразделение:

РЕЗУЛЬТАТЫ

СОВПАДЕНИЯ	4.78%
ОРИГИНАЛЬНОСТЬ	90.88%
ЦИТИРОВАНИЯ	4.34%
САМОЦИТИРОВАНИЯ	0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 15.06.2023



Структура документа: Проверенные разделы: титульный лист с.1, содержание с.2-3, основная часть с.4-50, библиография с.51
Модули поиска: ИПС Адилет; Библиография; Сводная коллекция ЭБС; Интернет Плюс*; Сводная коллекция РГБ; Цитирование; Переводные заимствования (RuEn); Переводные заимствования по eLIBRARY.RU (EnRu); Переводные заимствования по коллекции Гарант: аналитика; Переводные заимствования по коллекции Интернет в английском сегменте; Переводные заимствования по Интернету (EnRu); Переводные заимствования по коллекции Интернет в русском сегменте; Переводные заимствования издательства Wiley ; eLIBRARY.RU; СПС ГАРАНТ: аналитика; СПС ГАРАНТ: нормативно-правовая документация; Медицина; Диссертации НББ; Коллекция НБУ; Перефразирования по eLIBRARY.RU; Перефразирования по СПС ГАРАНТ: аналитика; Перефразирования по Интернету; Перефразирования по Интернету (EN); Перефразированные заимствования по коллекции Интернет в английском сегменте; Перефразированные заимствования по коллекции Интернет в русском сегменте; Перефразирования по коллекции

Работу проверил: Мкртичян Вячеслав Виталиевич

ФИО проверяющего

Дата подписи:

Подпись проверяющего

Чтобы убедиться
в подлинности справки, используйте QR-код,
который содержит ссылку на отчет.

Ответ на вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.

Оглавление

Введение 4

Постановка задачи 6

1. Предварительные сведения 7

1.1.1. Протокол Ethereum 7

1.1.2 ZK-Rollups 8

1.1.3 ZK-SNARK 9

1.2.1. Вычисление многочлена с помощью последовательности действий 11

1.2.2. Составление системы векторов ограничений 12

1.2.3 Переход от системы векторов ограничений к группам интерполяционных многочленов 14

1.2.4. Квадратичная арифметическая программа 16

1.2.5. Проверка правильности построения многочленов $A(x), B(x), C(x)$. 19

1.2.6. Следствие из леммы Шварца-Зиппеля 21

1.2.7. Полный гомоморфный шифр 22

1.3.2. Слепое вычисление многочленов с помощью гомоморфного шифрования 23

1.3.3. Случайный сдвиг многочленов 24

1.3.4. Общая ссылочная строка 25

1.4.2. Протокол Пиноккио 26

2. Модификация протокола ZK-SNARK 29

2.1. Модифицированная система векторов ограничений 30

2.2. Модифицированный переход от системы векторов ограничений к группам интерполяционных многочленов 32

2.3. Модификация квадратичной арифметической программы 35

2.4. Модификация в методе случайного сдвига многочленов. 38

2.5. Проверка правильности построения многочленов $A(x), B(x), Z(x), C(x)$ 39

2.6. Модификация протокола Пиноккио 41

3. Анализ параметров модифицированного протокола 44

3.1. Построение модельных примеров 44

3.1.1. Построение модельного примера для оригинального протокола . 44
3.1.2. Построение модельного примера модифицированного протокола 45
3.2. Анализ параметров модифицированного протокола 48
3.3. О неисследованных следствиях модификации протокола ZK-SNARK 51
3.4. Рассуждения о дальнейших возможных модификациях протокола ZK-SNARK 52
Заключение 53
Список литературы 54

Введение

В настоящее время область информационных технологий играет критическую роль в жизни каждого человека. Ярким примером выступает онлайн-банкинг, который стал неотъемлемой частью быта современного общества. Вместе с тем, все больше людей стали задумываться о проблемах безопасности подобных информационных систем. Важной проблемой является чрезмерная централизация. Так, например, на инфраструктуру банка могут совершить атаку и сделать изменения во внутренней базе данных, что повлечет за собой необратимые изменения текущего состояния счетов клиентов. Более того, банк может по субъективным причинам отклонять транзакции или блокировать счета некоторых клиентов. В ответ на эту проблему была создана технология блокчейн.

Блокчейн – это децентрализованная, распределенная и прозрачная система, которая дает возможность пользователям совершать транзакции и хранить записи о текущих состояниях системы в последовательности блоков, порядок которых обеспечивается криптографическими протоколами. Участники сети блокчейн хранят локальную копию его текущего состояния и участвуют в формировании новых блоков по заранее заданным правилам. Ввиду отсутствия централизации, участникам приходится определять между собой, какие транзакции нужно включать в очередной блок, а какие нет. А это в свою очередь влечет снижение скорости обработки транзакции.

Сегодня блокчейн представлен широким спектром протоколов. Наиболее популярными являются *Bitcoin* и *Ethereum*. В этой работе будет рассмотрен лишь последний. Как было сказано выше – скорость обработки транзакции является узким местом любого протокола блокчейн. В *Ethereum* существует технология *ZK-Rollups* [1], которая представляет собой инновационный метод для увеличения пропускной транзакционной способности в *Ethereum*.

Технология *ZK-Rollup* объединяет сотни транзакций вне основной цепочки блоков и генерирует криптографическое доказательство с нулевым разглашением, известное как *ZK-SNARK*, которое позволяет одной стороне доказать, что она обладает определенной информацией, не раскрывая эту информацию. Применение данной технология позволяет устранить необходимость в формировании консенсуса и взаимодействия с валидаторами.

В данной работе рассматривается и описывается протокол *ZK-SNARK* и предлагается вариант его модификации. Производится анализ новой версии протокола и делаются выводы о возможности применения данного протокола, его характеристиках и дальнейших областей исследования.

Постановка задачи

Целью данной работы является модификация протокола ZK-SNARK. Для достижения цели были поставлены следующие задачи:

1) Изучение и описание протокола ZK-SNARK.
2) Модификация протокола ZK-SNARK.
3) Построение модельного примера для изначальной и модифицированной версий ZK-SNARK.
4) Анализ параметров модифицированного протокола.

1. Предварительные сведения

1.1.1. Протокол Ethereum

Ethereum — это блокчейн, который предоставляет инфраструктуру для создания и запуска децентрализованных приложений и так называемых смарт-контрактов. Он использует свою нативную криптовалюту *Ether* (ETH) для оплаты транзакций и запуска смарт-контрактов в сети.

Концепт данного протокола был предложен Виталиком Бутериным в 2013 году и уже в июле 2015 года он был реализован и запущен. Он выделяется среди множества протоколов наличием смарт-контрактов – программ, которые могут быть опубликованы в сети *Ethereum* и использованы для автоматического выполнения заранее заданных действий по заранее заданным условиям.

1.1.2 ZK-Rollups

ZK-Rollups -это технология в *Ethereum,* которая позволяет объединять транзакции, которые выполняются вне цепочки. Автономные вычисления вне основной сети сокращают объем данных, которые необходимо разместить в блокчейн.

Так называемые операторы в протоколе *ZK-Rollup* отправляют сводку изменений, необходимых для представления всех транзакций в сжатом виде за определенный период, а не для отправки каждой транзакции по отдельности. Они также предоставляют доказательства, чтобы убедить основную сеть *Ethereum* в корректности своих изменений. Формируемое операторами доказательство с криптографической достоверностью демонстрирует, что предлагаемые изменения состояния сети второго уровня действительно являются конечным результатом выполнения всех транзакций.

1.1.3 ZK-SNARK

ZK-SNARK расшифровывается и переводится как – краткий не интерактивный аргумент знания с нулевым разглашением и относится к конструкции доказательства, при которой можно доказать владение определенной информацией, например секретным ключом, не раскрывая эту информацию.

Доказательства с “нулевым разглашением” позволяют одной стороне (доказывающему) доказать другой (проверяющему), что утверждение истинно, не раскрывая никакой информации, выходящей за рамки достоверности самого утверждения. Например, доказывающий мог бы убедить проверяющего в том, что действительно существует число с известным обоим сторонам хеш-значением, не раскрывая самого числа.

В *ZK-SNARK* доказывающий может убедить проверяющего не только в том, что число существует, но и в том, что он действительно знает такое число - опять же, не раскрывая никакой информации об этом числе.

Краткие доказательства с нулевым разглашением могут быть проверены в течение нескольких миллисекунд, при этом длина доказательства составляет всего несколько сотен байт даже для утверждений об очень больших программах. В первых протоколах с нулевым разглашением проверяющий и верификатор должны были обмениваться данными в течение нескольких раундов, но в “неинтерактивных” конструкциях доказательство состоит из одного сообщения, отправляемого от проверяющего к верификатору. Наиболее эффективным известным способом получения доказательств с нулевым разглашением, которые неинтерактивны и достаточно коротки, является этап начальной настройки, который генерировал общую ссылочную строку, совместно используемую доказывающим и проверяющим.

ZK-SNARK сначала преобразует то, что необходимо доказать, в эквивалентную форму знания решения некоторых алгебраических уравнений.

Первым шагом в преобразовании функции в математическое представление является разбиение логических шагов на наименьшие возможные операции, создавая арифметическую схему. Подобно логической схеме, в которой программа компилируется до дискретных отдельных действий, таких как *AND, OR, NOT*, при преобразовании в арифметическую схему, программа разбивается на отдельные действия, состоящие из основных арифметических операций сложения и умножения в некотором конечном поле [4]. В этой работе представлена изменение в разбиении на действия, которое влечет за собой модификацию в протоколе *ZK-SNARK*.

1.2.1. Вычисление многочлена с помощью последовательности действий

Пусть задан многочлен $f(x_1, x_2, .., x_l),\ f: \mathbb{F}_p^l \to \mathbb{F}_p\ , l \in \mathbb{N}$ и определено уравнение:

$$f(x_1, x_2, .., x_l) = 0, \tag{1.1}$$

Пусть задан вектор значений $\vec{k}$ – входные значения для многочлена (1):

$$\vec{k} := \{k_1, k_2, \dots, k_l\} \in \mathbb{F}_p^l, l \in \mathbb{N}, \tag{1.2}$$

и определены $d \in \mathbb{N}$ действий вида для вычисления значения многочлена (1) в точке $\vec{k}$:

$$\begin{gathered} \mathrm{u}_i := o_1\ \cdot o_2\ \text{ или } \mathrm{u}_i := o_1 + o_2, \\ \text{где } i \in \{1, 2, \dots d\}, i \in \mathbb{N}, \end{gathered} \tag{2}$$

Для каждого u_i из (2) переменные o_1, o_2 являются элементами вектора $\vec{k}$ (1) или значениями предыдущих действий u_j, где $j\ \in \{1, 2, \dots i-1\}$. То есть $\mathrm{u}_i, o_1, o_2\ \in \mathbb{F}_p$.

Таким образом, с помощью действий u_i можно построить многочлен.

Составим вектор, содержащий все значения вектора $\vec{k}$ и все промежуточные переменные u_i из (2):

$$\vec{s} := (s_1, s_2, \dots, s_m) = (1, k_1, , .. k_l, \mathrm{u}_1, \dots, \mathrm{u}_d), m \in \mathbb{N}, \qquad m = d + l + 1 \tag{3}$$

Примечание 1. В дальнейшем мы будем называть вектор $\vec{s}$ – допустимым набором присваивания, если он составлен как в (3), а в противном случае - недопустимым набором присваивания.

1.2.2. Составление системы векторов ограничений

Для каждого u_i-го действия из (2) построим тройку векторов ограничений:

$$\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{c^i}\right) \in \mathbb{F}_p^m, i \in \{1, 2, \dots, d\}, \tag{4}$$

удовлетворяющую уравнению:

$$\begin{pmatrix} a_1^i \\ a_2^i \\ a_3^i \\ \dots \\ \dots \\ a_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \dots \\ \dots \\ s_m \end{pmatrix} \times \begin{pmatrix} b_1^i \\ b_2^i \\ b_3^i \\ \dots \\ \dots \\ b_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \dots \\ \dots \\ s_m \end{pmatrix} - \begin{pmatrix} c_1^i \\ c_2^i \\ c_3^i \\ \dots \\ \dots \\ c_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \dots \\ \dots \\ s_m \end{pmatrix} = 0, \tag{5}$$

Элементы векторов $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{c^i}\right)$ из (4) отвечают за коэффициенты при переменных, использованных в u_i-м действии.

Приведем простой пример:

Пусть задано уравнение $x^2 + 2 = 0$ набор значений из (2):

$$\vec{k} = \{1, x\} \in \mathbb{F}_p, \tag{6.1}$$

и пусть заданы два действия:

$$\begin{aligned} u_1 &:= x * x, \\ u_2 &:= u_1 + 2, \end{aligned} \tag{6.2}$$

Тогда мы можем построить тройки векторов ограничений из (4) для действий (6.2):

$$a^1 = (0, 1, 0, 0), a^2 = (2, 0, 1, 0)$$

$$b^1 = (0, 1, 0, 0), b^2 = (1, 0, 0, 0)$$

$$c^1 = (0, 0, 1, 0), c^2 = (0, 0, 0, 1)$$

Пусть существует некий допустимый набор присваиваний $\vec{s} = (1, x, u_1, u_2)$. Подставим построенные тройки $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{c^i}\right), i \in \{1, 2\}$ в уравнение (5) и убедимся, что оно обращается в ноль при подстановке $\vec{s}$:

Для тройки $\left(\overrightarrow{a^1}, \overrightarrow{b^1}, \overrightarrow{c^1}\right)$:

$$\begin{pmatrix}0\\1\\0\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\end{pmatrix} \times \begin{pmatrix}0\\1\\0\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\end{pmatrix} - \begin{pmatrix}0\\0\\1\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\end{pmatrix} =$$

$$= s_2 \cdot s_2 - s_3 = x \cdot x - u_1 = 0, \tag{6.3}$$

Для тройки $\left(\overrightarrow{a^2}, \overrightarrow{b^2}, \overrightarrow{c^2}\right)$:

$$\begin{pmatrix}2\\0\\1\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\end{pmatrix} \times \begin{pmatrix}1\\0\\0\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\end{pmatrix} - \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\end{pmatrix} =$$

$$= (2s_1 + s_3) \cdot s_1 \cdot -s_4 \; = \; u_1 + 2 - u_2 = 0, \tag{6.4}$$

Если же хотя бы одно из выражений (6.3), (6.4) не обращается в ноль при заданном $\vec{s}$, то это означает, что допустимый набор присваивания $\vec{s}$ составлен неверно – как мининмум для одного из действий не выполняется проверка.

1.2.3 Переход от системы векторов ограничений к группам интерполяционных многочленов

Как известно из теории численных методов с помощью метода интерполяции по d точкам можно построить многочлен степени $d-1$, который проходит через эти точки. Примером такого метода является метод интерполяции Лагранжа. Воспользуемся этим методом и построим многочлены с помощью элементов векторов ограничений $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{c^i}\right)$ из (4):

для векторов a^i:

$$A_1(x) \text{ для точек } (1, a_1^1), (2, a_1^2), \dots, \left(d, a_1^d\right)$$

$$A_2(x) \text{ для точек } (1, a_2^1), (2, a_2^2), \dots, \left(d, a_2^d\right)$$

...

$$A_m(x) \text{ для точек } (1, a_m^1), (2, a_m^2), \dots, (d, a_m^d)$$

Примечание 2. Таким образом, многочлен $A_1(x)$ проходит через первые координаты всех векторов ограничений $a^1, a^2, \dots, a^d$. Так что $A_i(x)$ проходит через i-е координаты всех векторов ограничений $a^1, a^2, \dots, a^d$. Аналогичные выводы справедливы для многочленов $B_i(x), C_i(x), i \in \{1, 2, \dots m\}, i \in \mathbb{N}$.

для векторов b^i:

$$B_1(x) \text{ для точек } (1, b_1^1), (2, b_1^2), \dots, \left(d, b_1^d\right)$$

$$B_2(x) \text{ для точек } (1, b_2^1), (2, b_2^2), \dots, \left(d, b_2^d\right)$$

...

$$B_m(x) \text{ для точек } (1, b_m^1), (2, b_m^2), \dots, (d, b_m^d)$$

для векторов c^i:

$$C_1(x) \text{ для точек } (1, c_1^1), (2, c_1^2), \ldots, \left(d, c_1^d\right)$$

$$C_2(x) \text{ для точек } (1, c_2^1), (2, c_2^2), \ldots, \left(d, c_2^d\right)$$

$$\ldots$$

$$C_m(x) \text{ для точек } (1, c_m^1), (2, c_m^2), \ldots, (d, c_m^d)$$

Таким образом, мы построили многочлены:

$$A_1(x), \ldots, A_m(x), B_1(x), \ldots, B_m(x), C_1(x), \ldots, C_m(x),$$
$$\deg\left(A_i(x)\right) = \deg\left(B_i(x)\right) = \deg\left(C_i(x)\right) \leq d - 1, \quad (7)$$

Составим векторы из этих многочленов следующим образом:

$$\overrightarrow{A(x)} = (A_1(x), A_2(x), \ldots, A_m(x))$$

$$\overrightarrow{B(x)} = (B_1(x), B_2(x), \ldots, B_m(x))$$

$$\overrightarrow{C(x)} = (C_1(x), C_2(x), \ldots, C_m(x))$$

Подставив номер i-го действия вместо x, мы получим тройку векторов ограничений $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{c^i}\right)$ для этого действия.

Например, пусть $x = 1$, тогда:

$$\overrightarrow{A(1)} = (A_1(1), A_2(1), \ldots, A_m(1)) = (a_1^1, a_2^1, \ldots, a_m^1) = \overrightarrow{a^1}$$

$$\overrightarrow{B(1)} = (B_1(1), B_2(1), \ldots, B_m(1)) = (b_1^1, b_2^1, \ldots, b_m^1) = \overrightarrow{b^1}$$

$$\overrightarrow{C(1)} = (C_1(1), C_2(1), \ldots, C_m(1)) = (c_1^1, c_2^1, \ldots, c_m^1) = \overrightarrow{c^1}$$

1.2.4. Квадратичная арифметическая программа

Определим *целевой многочлен* следующим образом:

$$T(x) := (x - 1) \cdot (x - 2) \cdot \ldots \cdot (x - d), \quad (8)$$

Пусть также заданы многочлены из (7): $A_1(x), \ldots, A_m(x), B_1(x), \ldots, B_m(x), C_1(x), \ldots, C_m(x)$.

Определение 1:

Квадратичная арифметическая программа Q (КАП) степени d и размера m состоит из многочленов:

$A_1(x), \ldots, A_m(x), B_1(x), \ldots, B_m(x), C_1(x), \ldots, C_m(x)$ и целевого многочлена $T(x)$. [3]

Определение 2:

Определим $A(x) := \sum_{i=1}^{m} s_i \cdot A_i(x)$, $B(x) := \sum_{i=1}^{m} s_i \cdot B_i(x)$, $C(x) := \sum_{i=1}^{m} s_i \cdot C_i(x)$, $E(x) := A(x) \cdot B(x) - C(x)$.

Набор допустимых значений $\vec{s} = (s_1, s_2, \ldots, s_m)$ *удовлетворяет* КАП Q, если, многочлен $E(x)$ делится без остатка на целевой многочлен $T(x)$.

Лемма 1. Пусть заданы набор значений $\vec{s} = (s_1, s_2, \ldots, s_m)$ *и многочлены* $A(x) := \sum_{i=1}^{m} s_i \cdot A_i(x)$, $B(x) := \sum_{i=1}^{m} s_i \cdot B_i(x)$, $C(x) := \sum_{i=1}^{m} s_i \cdot C_i(x)$, $E(x) := A(x) \cdot B(x) - C(x)$.

Если $\vec{s}$ *– допустимый набор значений, то* $E(x)$ *равен нулю в точках* $x \in \{1, 2, \ldots, d\}$. *Если же* $\vec{s}$ *не является допустимым набором значений, то E(x) не обращается в ноль для всех* $x \in \{1, 2, \ldots, d\}$.

Доказательство:

Представим $E(x)$ в скалярном виде:

$$\begin{pmatrix} A_1(x) \\ A_2(x) \\ A_3(x) \\ \cdots \\ \cdots \\ A_m(x) \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} \times \begin{pmatrix} B_1(x) \\ B_2(x) \\ B_3(x) \\ \cdots \\ \cdots \\ B_m(x) \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} - \begin{pmatrix} C_1(x) \\ C_2(x) \\ C_3(x) \\ \cdots \\ \cdots \\ C_m(x) \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} =$$
$$= A(x) \cdot B(x) - C(x) = E(x), \quad (8.1)$$

Подставив в $E(x)$ $x = i$ – номер действия, $i \in \{1, 2, \dots, \mathrm{d}\}$, получим уравнение вида (5):

$$E(i) = \begin{pmatrix} a_1^i \\ a_2^i \\ a_3^i \\ \cdots \\ \cdots \\ a_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} \times \begin{pmatrix} b_1^i \\ b_2^i \\ b_3^i \\ \cdots \\ \cdots \\ b_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} - \begin{pmatrix} c_1^i \\ c_2^i \\ c_3^i \\ \cdots \\ \cdots \\ c_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} = 0 \quad (8.2)$$

Вектора ограничений $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{c^i}\right)$ из (4) были построены таким образом, что для допустимого набора значений $\vec{s}$ уравнение (8.2) обращается в ноль для всех $i \in \{1, 2, \dots, d\}$, а значит и $E(x)$ обращается в ноль для всех $x = i \in \{1, 2, \dots, d\}$. Если же $\vec{s} = (s_1, s_2, \dots, s_m)$ – не является набором допустимых значений, то для некоторого i уравнение (8.2) не обращается в ноль, а так как уравнение (8.2) — это уравнение $E(i) = 0$, то $\exists x \in \{1, 2, \dots, d\}, E(x) \neq 0$. Лемма доказана.

Лемма 2. Пусть заданы набор значений $\vec{s} = \left(s_{1,}\, s_2, \dots, s_m\right)$ *и многочлены* $A(x) := \sum_{i=1}^{m} s_i \cdot A_i(x)$, $B(x) := \sum_{i=1}^{m} s_i \cdot B_i(x)$, $C(x) := \sum_{i=1}^{m} s_i \cdot C_i(x)$, $E(x) := A(x) \cdot B(x) - C(x)$.

Тогда степени $A(x), B(x), C(x)$ *не выше* $d - 1$. *Степень* $E(x)$ *не выше* $2(d - 1)$.

Доказательство:

$A(x), B(x), C(x)$ являются линейной комбинацией многочленов степени не

выше $d-1$, а значит их степени не выше $d-1$. Так как $E(x) := A(x) \cdot B(x) - C(x)$, то его степень не превосходит суммы степеней $A(x)$ и $B(x)$.

$$\begin{gathered} deg\big(A(x)\big) \leq d-1, \\ deg\big(B(x)\big) \leq d-1, \\ deg\big(C(x)\big) \leq d-1, \\ deg\big(E(x)\big) \leq deg\big(A(x)\big) + deg\big(B(x)\big) \leq 2(d-1), \end{gathered} \tag{8.3}$$

Лемма доказана.

Заметим также, что если $\vec{s}$ удовлетворяет *КАП* Q, то согласно определению 2 $E(x)$ делится нацело многочленом $T(x)$ и согласно *лемме* 1, лемме 2 и теории линейной алгебры, мы можем представить $E(x)$ в виде:

$$E(x) \equiv H(x) \cdot T(x), \qquad \forall x \in F_p \tag{9}$$

1.2.5. Проверка правильности построения многочленов $A(x), B(x), C(x)$.

Если Алиса не обладает допустимым набором присваиваний $\vec{s}$, то это не значит, что она не может построить многочлены $A(x), B(x), C(x), H(x)$ степени не выше d такие, что:

$$A(x) \cdot B(x) - C(x) = H(x) \cdot T(x)$$

Однако это означает, что она не может найти такие многочлены $A(x), B(x), C(x)$ степени не выше d, построенные как в определении 2:

$$A(x) := \sum_{i=1}^{m} s_i \cdot A_i(x), \qquad B(x) := \sum_{i=1}^{m} s_i \cdot B_i(x),$$
$$C(x) := \sum_{i=1}^{m} s_i \cdot C_i(x), \tag{10}$$

Объединим многочлены $A(x), B(x), C(x)$ в один многочлен $F(x)$ следующим образом:

$$F(x) = A(x) + B(x) \cdot x^{d+1} + C(x) \cdot x^{2(d+1)}, \tag{10.1}$$

Составим многочлены $F_i(x)$, используя многочлены из (7):

$$F_i(x) = A_i(x) + B_i(x) \cdot x^{d+1} + C_i(x) \cdot x^{2(d+1)}, \qquad i \in \{1, 2, \dots, m\}, \tag{10.2}$$

Лемма 3. Пусть заданы многочлены $F(x)$ (10.1) и $F_i(x)$ (10.2).

Если $F(x) = \sum_{i=1}^{m} s_i \cdot F_i(x)$ для некоторого набора значений $\vec{s} = (s_1, s_2, \dots, s_m)$, то и

$$A(x) = \sum_{i=1}^{m} s_i \cdot A_i(x), B(x) = \sum_{i=1}^{m} s_i \cdot B_i(x), C(x) = \sum_{i=1}^{m} s_i \cdot C_i(x), \tag{10.3}$$

Доказательство:

Заметим, что коэффициенты многочленов $A(x), B(x), C(x)$ не смешивались в $F(x)$. Коэффициенты при степенях $1, x, \dots, x^d$ в $F(x)$ соответствуют коэффициентам $A(x)$, следующие $d+1$ коэффициента в $F(x)$ при степенях $x^{d+1}, \dots, x^{2d+1}$ являются коэффициентами $B(x)$, коэффициенты в $F(x)$ при степенях $x^{2(d+1)}, \dots, x^{3d+2}$ являются коэффициентами $C(x)$.

Например, для $m = 2$*:*

$$F_1(x) + F_2(x) = (A_1(x) + A_2(x)) + (B_1(x) \cdot B_2(x)) \cdot x^{d+1} + (C_1(x) \cdot C_2(x)) \cdot x^{2(d+1)}, \quad (10.4)$$

Глядя на (10.4), можно сделать вывод, что если $F(x) = \sum_{i=1}^{m} s_i \cdot F_i(x)$ для некоторого допустимого набора присваиваний $\vec{s}$, то и

$$A(x) = \sum_{i=1}^{m} s_i \cdot A_i(x), B(x) = \sum_{i=1}^{m} s_i \cdot B_i(x), C(x) = \sum_{i=1}^{m} s_i \cdot C_i(x)$$

Лемма доказана.

Другими словами, с помощью *леммы 3* Боб может удостовериться в том, то $A(x), B(x), C(x)$ были составлены с помощью одно и того же набора присваиваний, если Алиса докажет, что $F(x)$ – линейная комбинация $F_i(x)$.

Доказать, что $F(x) = \sum_{i=1}^{m} s_i \cdot F_i(x)$ можно, воспользовшись методом слепого вычисления многочленов и методом предположения о знании коэффициента, описанный в работе [5].

1.2.6. Следствие из леммы Шварца-Зиппеля

Пусть дан набор значений $\vec{w}$, который не удовлетворяет Q из определения 2. Построим многочлены:

$$A(x) := \sum_{i=1}^{m} w_i \cdot A_i(x), \qquad B(x) := \sum_{i=1}^{m} w_i \cdot B_i(x), \qquad C(x) := \sum_{i=1}^{m} w_i \cdot C_i(x),$$

$$E(x) := A(x) \cdot B(x) - C(x).$$

Заметим, что мы использовали метод предположения о знании коэффициента для этих многочленов и точно знаем, что они построены с помощью одного и того же набора значений $\vec{w}$. Из примечания 3 следует, что:

$$E(x) \neq 0, \forall\, x \in \{1, 2, \dots, d\}$$

А значит $E(x)$ не может быть представим в виде $E(x) \equiv H(x) \cdot T(x)$:

$$E(x) \not\equiv H(x) \cdot T(x), \tag{11}$$

Из леммы Шварца-Зиппеля следует, что два различных многочлена степени не более $2(d-1)$ могут совпадать не более чем в $2(d-1)$ точках из $\mathbb{F}_p$. Таким образом, если количество элементов в поле p намного больше степени многочленов $2(d-1)$, то вероятность того, что эти многочлены будут равны в случайно выбранной точке $q \in F_p$, очень мала [2]. Также, с помощью этой леммы мы можем оценить вероятность совпадения $E(x)$ и $H(x) \cdot T(x)$ в точке $q \in F_p$:

$$\Pr[E(q) = H(q) \cdot T(q)] \leq \frac{2(d-1)}{p},$$
$$\text{где } q \in F_p - \text{случайно выбранное значение},$$
$$E(q) - \text{многочлен построенный с } \vec{w},$$
$$\text{которое не удовлетворяет } Q,$$
$$\deg\big(E(q)\big) \leq 2(d-1) \tag{12}$$

1.2.7. Полный гомоморфный шифр

Полный гомоморфный шифр – это криптографическая схема, которая позволяет выполнять вычисления над зашифрованными данными без их расшифровки. Он обладает двумя основными свойствами:

1. Гомоморфность сложения: Зная значения $Enc(x), Enc(y)$, а также коэффициенты $\alpha, \beta \in F_p$, можно вычислить зашифрованное значение $Enc(\alpha x + \beta y)$ по формуле:

$$Enc(\alpha x + \beta y) = \alpha Enc(x) + \beta Enc(y), \quad (13.1)$$

2. Гомоморфность умножения: Зная значения $Enc(x), Enc(y)$, можно вычислить зашифрованное значение $Enc(x \cdot y)$ по формуле:

$$Enc(a \cdot b) = Enc(a) \cdot Enc(b), \quad (13.2)$$

То есть, полный гомоморфный шифр позволяет выполнять операции сложения и умножения над зашифрованными данными, результаты которых также останутся зашифрованными. Это открывает возможности для обработки конфиденциальных данных, сохраняя их конфиденциальность на протяжении всего вычислительного процесса.

Примером полного гомоморфного шифра является шифр BGV (Brakerski-Gentry-Vaikuntanathan), который был предложен в работе [7]. Этот шифр обладает полной гомоморфностью и может выполнять операции сложения и умножения над зашифрованными данными.

1.3.2. Слепое вычисление многочленов с помощью гомоморфного шифрования

Пусть существует полный гомоморфный шифр $Enc(x)$, обладающий свойством (12.1).

Предположим, что у Алисы есть многочлен $f(x)$ степени d, который она скрывает:

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0 x^0, x, a_i \in F_p, \qquad (14.1)$$

Боба выбрал случайным образом значение $q \in \mathbb{F}_p$ и хочет получить от Алисы $Enc\big(f(q)\big)$, причем Алиса не должна узнать точку q.

Боб может отправить Алисе значения гомоморфного шифра в точках $q^0, q^1, \dots, q^d$ – $Enc(q^0), Enc(q^1), \dots, Enc(q^d)$. Тогда она может воспользоваться свойством гомомофрного шифра (12.1) и вычислить $Enc\big(f(q)\big)$:

$$E\big(f(q)\big) = E(a_d q^d + a_{d-1}q^{d-1} + \cdots + a_0 q^0) = \\ = a_d E(q^d) + a_{d-1}E(q^{d-1}) + .. + a_0\, E(q^0), \qquad (14.2)$$

Получив значение $E\big(f(q)\big)$, Боб не сможет найти $f(x)$. Так же и Алиса, получив значения $E(q^0), E(q^1), \dots, E(q^d)$, не сможет восстановить по ним q. Будем называть такой способ вычисления значения гомоморфного шифра – *слепое вычисление многочленов.*

1.3.3. Случайный сдвиг многочленов

Пусть задан допустимый набор присваивания $\vec{s}$, удовлетворяющий КАП Q из определения 2 и пусть с помощью $\vec{s}$ построены $A(x), B(x), C(x), H(x), T(x)$. Из примечания 4 следует тождество (9):

$$A(x) \cdot B(x) - C(x) \equiv H(x) \cdot T(x), \qquad \forall x \in F_p, \tag{15.1}$$

Выберем случайным образом $\delta_1, \delta_2, \delta_3 \in \mathbb{F}_p^*$ и определим многочлены $\tilde{A}(x), \tilde{B}(x), \tilde{C}(x), \tilde{H}(x)$, отличные от $A(x), B(x), C(x), H(x)$:

$$\tilde{A}(x) := A(x) + \delta_1 T(x)$$

$$\tilde{B}(x) := B(x) + \delta_2 T(x)$$

$$\tilde{C}(x) := C(x) + \delta_3 T(x)$$

$$\tilde{H}(x) := H(x) + \delta_2 A(x) + \delta_1 B(x) + \delta_1 \delta_2 T(x) - \delta_3, \tag{15.2}$$

Тогда для них выполняется тождество:

$$\begin{gathered}\tilde{A}(x) \cdot \tilde{B}(x) - \tilde{C}(x) = \\ \big(A(x) + \delta_1 T(x)\big) \cdot \big(B(x) + \delta_2 T(x)\big) - C(x) - \delta_3 T(x) = \\ A(x) \cdot B(x) + A(x) \cdot \delta_2 T(x) + \delta_1 T(x) B(x) + \delta_1 \delta_2 T^2(x) - C(x) - \delta_3 T(x) = \\ T(x)(H(x) + \delta_2 A(x) + \delta_1 B(x) + \delta_1 \delta_2 T(x) - \delta_3) \equiv \\ \equiv \tilde{H}(x) \cdot T(x), \qquad \forall x \in F_p, \end{gathered} \tag{15.3}$$

Итак, замена многочленов $A(x), B(x), C(x), H(x)$ на $\tilde{A}(x), \tilde{B}(x), \tilde{C}(x), \tilde{H}(x)$ обеспечивает выполнение тождества (15.3), эквивалентного (15.1). В дальнейшем мы будем называть такую замену *случайным сдвигом многочленов*.

1.3.4. Общая ссылочная строка

Интуитивно понятное представление о неинтерактивном доказательстве, заключается в следующем – чтобы доказать определенное утверждение, проверяющий передает всем сторонам одно сообщение без какой-либо предварительной связи; и любой, кто прочтет это сообщение, будет убежден в утверждении проверяющего. Однако в большинстве случаев это невозможно.

Смягченное понятие неинтерактивного доказательства состоит в том, чтобы разрешить использование общедоступного набора данных – *общей ссылочной строки*. В модели *общей ссылочной строки*, прежде чем будут созданы какие-либо доказательства, существует фаза настройки, на которой строка создается в соответствии с определенным рандомизированным процессом и передается всем сторонам. Пример такой настройки можно найти в работе [8].

Общая ссылочная строка затем используется для построения и проверки доказательств. Предполагается, что случайность, использованная при создании *общей ссылочной строки*, неизвестна ни одной стороне, поскольку знание этой случайности может позволить построить доказательства ложных утверждений.

В данной работе общая ссылочная строка будет представлять собой последовательность значений полного гомоморфного шифра со свойствами (13.1) -(13.2) в случайно выбранной точке $q \in \mathbb{F}_p$:

$$Enc(q^0), Enc(q^1), \dots, Enc\left(q^{2(d-1)}\right), d \in \mathbb{N}, \qquad (16)$$

1.4.2. Протокол Пиноккио

Пусть есть две стороны, которые мы обозначим как Алиса и Боб. Алиса хочет доказать Бобу, что она обладает допустимым набором присваивания $\vec{s} = (s_1, s_2, \dots, s_m) \in \mathbb{F}_p$ (3), удовлетворяющим Q из определения 2, без раскрытия $\vec{s}$.

Пусть задан полный гомоморфный шифр $Enc(x)$ со свойствами (13.1) - (13.2).

Воспользуемся протоколом Пиноккио [5], который имеет вид:

1. Алиса строит многочлены $A(x), B(x), C(x), E(x)$ из определения 2:

$$A(x) := \sum_{i=1}^{m} s_i \cdot A_i(x), \qquad B(x) := \sum_{i=1}^{m} s_i \cdot B_i(x),$$
$$C(x) := \sum_{i=1}^{m} s_i \cdot C_i(x)$$
$$E(x) := A(x) \cdot B(x) - C(x), \tag{17.1}$$

Многочлены $A(x), B(x), C(x), H(x)$ построены с помощью допустимого набора присваивания $\vec{s}$, а потому эти многочлены раскрывают информацию об $\vec{s}$. Поэтому Алиса использует *случайный сдвиг многочленов* и составляет многочлены $\tilde{A}(x), \tilde{B}(x), \tilde{C}(x), \tilde{H}(x)$ как в (13.2). Из (13.3) имеет место тождество:

$$\tilde{E}(x) := \tilde{A}(x) \cdot \tilde{B}(x) - \tilde{C}(x) \equiv \tilde{H}(x) \cdot T(x)$$

2. Задана *общая ссылочная строка* (16):

$$Enc(q^0), Enc(q^1), \dots, Enc\left(q^{2(d-1)}\right), d \in \mathbb{N}, \tag{17.2}$$

3. Алиса формирует доказательство, которое состоит из значений $Enc\left(\tilde{A}(q)\right), Enc\left(\tilde{B}(q)\right), Enc\left(\tilde{C}(q)\right), Enc(\tilde{H}(q))$. Алиса может

вычислить эти значения, используя *метод слепого вычисления многочленов* (14.2). Сообщение отправляется Бобу.

4. Боб, используя свойства (13.1) -(13.2) шифра $Enc(x)$, проверяет, что:

$$Enc\left(\tilde{A}(q)\cdot\tilde{B}(q)-\tilde{C}(q)\right)=\ Enc\left(T(q)\cdot\widetilde{H}(q)\right), \qquad (18)$$

Заметим, что (16) эквивалентно:

$$Enc\big(A(q)\cdot B(q)-\ C(q)\big)=\ Enc\big(T(q)\cdot H(q)\big)$$

Если левая и правая части уравнения (18) равны, то Боб с уверенностью может полагать, что Алиса обладает допустимым набором значений $\vec{s}=(s_1,s_2,\dots,s_m)\in\mathbb{F}_p^m$. При этом Алиса не раскрывает Бобу $\vec{s},E(x),A(x),B(x),C(x),H(x)$.

Так как в качестве q была выбрана случайная точка из $\mathbb{F}_p$, то согласно (12) вероятность того, что многочлены $A(x),B(x),C(x)$, построенные без допустимого набора значений, будут удовлетворять равенству (18) мала. Следовательно, Алиса не сможет убедить Боба с высокой вероятностью в том, что она обладает $\vec{s}$, без его наличия.

Примечание 3. Поясним важность случайного сдвига многочленов. Если бы у Боба был набор присваивания $\vec{h}$, удовлетворяющий Q и отличный от набора присваивания Алисы $\vec{s}$, то он бы мог построить многочлены $A_h(x),B_h(x),C_h(x),H_h(x)$ и вычислить $Enc(A_h(q)),Enc(B_h(q)),Enc(C_h(q)),Enc(H_h(q))$. Эти значения он бы мог сравнить с значениями $Enc(A_s(q)),Enc(B_s(q)),Enc(C_s(q)),Enc(H_s(q))$, полученными от Алисы, и сделать вывод о том, что они различны, а, следовательно, набор присваивания $\vec{h}$ Боба отличается от набора присваивания $\vec{s}$ Алисы. Это раскрывает некоторую информацию об $\vec{s}$. При

использовании же случайного сдвига многочленов Алиса не раскрывает ничего об $\vec{s}$.

2. Модификация протокола ZK-SNARK

В качестве модификации протокола ZK-SNARK предлагается изменить вид действий, для вычисления многочлена (1.1).

Пусть задан вектор значений $\vec{k}$ из (1.2):

$$\vec{k} := \{k_1, k_2, \dots, k_l\} \in \mathbb{F}_p^l, l \in \mathbb{N}$$

и определены $d \in \mathbb{N}$ действий вида:

$$\mathrm{u}_i := o_1 \cdot o_2 \cdot o_3 \text{ или } \mathrm{u}_i := o_1 + o_2, \quad \text{где } i \in \{1, 2, \dots d\}, i \in \mathbb{N}, \tag{19}$$

Для каждого u_i из (19) переменные o_1, o_2, o_3 являются элементами вектора $\vec{k}$ (1.2) или значениями предыдущих действий u_j, где $j \in \{1, 2, \dots i-1\}$. То есть $\mathrm{u}_i, o_1, o_2, o_3 \in \mathbb{F}_p$.

Допустимый набор присваивания задается как в (3):

$$\vec{s} := (s_1, s_2, \dots, s_m) = (1, k_1, ,.. k_l, \mathrm{u}_1, \dots, \mathrm{u}_d), m \in \mathbb{N}, \qquad m = d + l + 1$$

2.1. Модифицированная система векторов ограничений

Для каждого u_i-го действия из (2) построим четверку векторов ограничений:

$$\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{z^i}, \overrightarrow{c^i}\right) \in \mathbb{F}_p^m, i \in \{1, 2, \dots, d\}, \tag{20}$$

удовлетворяющую уравнению, аналогичному уравнению (5):

$$\begin{pmatrix} a_1^i \\ a_2^i \\ a_3^i \\ \cdots \\ \cdots \\ a_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} \times \begin{pmatrix} b_1^i \\ b_2^i \\ b_3^i \\ \cdots \\ \cdots \\ b_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} \times \begin{pmatrix} z_1^i \\ z_2^i \\ z_3^i \\ \cdots \\ \cdots \\ z_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} - \begin{pmatrix} c_1^i \\ c_2^i \\ c_3^i \\ \cdots \\ \cdots \\ c_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} = 0, \tag{21}$$

Элементы векторов $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{z^i}, \overrightarrow{c^i}\right)$ из (18) отвечают за коэффициенты при переменных, использованных в u_i-м действии.

Приведем пример:

Пусть задано уравнение $x^2 + 2 = 0$ набор значений из (2):

$$\vec{k} = \{1, x\} \in \mathbb{F}_p, \tag{21.1}$$

и пусть заданы два действия:

$$\begin{aligned} u_1 &:= x * x * 1, \\ u_2 &:= u_1 + 2, \end{aligned} \tag{21.2}$$

Тогда мы можем построить четверки векторов ограничений из (20) для действий (21.2):

$$a^1 = (0, 1, 0, 0, 0, 0), a^2 = (1, 0, 0, 0, 1, 0)$$

$$b^1 = (0, 0, 1, 0, 0, 0), b^2 = (1, 0, 0, 0, 0, 0)$$

$$z^1 = (0, 0, 0, 1, 0, 0), z^2 = (1, 0, 0, 0, 0, 0)$$

$$c^1 = (0,0,0,0,1,0), c^2 = (0,0,0,0,0,1)$$

Пусть существует некий допустимый набор присваиваний $\vec{s} = (1, x, y, z, u_1, u_2)$. Подставим построенные четверки $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{z^i}, \overrightarrow{c^i}\right), i \in \{1,2\}$ в уравнение (21) и убедимся, что оно обращается в ноль при подстановке $\vec{s}$:

Для четверки $\left(\overrightarrow{a^1}, \overrightarrow{b^1}, \overrightarrow{z^1}, \overrightarrow{c^1}\right)$:

$$\begin{pmatrix}0\\1\\0\\0\\0\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\\s_5\\s_6\end{pmatrix} \times \begin{pmatrix}0\\0\\1\\0\\0\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\\s_5\\s_6\end{pmatrix} \times \begin{pmatrix}0\\0\\0\\1\\0\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\\s_5\\s_6\end{pmatrix} - \begin{pmatrix}0\\0\\0\\0\\1\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\\s_5\\s_6\end{pmatrix} =$$

$$= s_2 \cdot s_3 \cdot s_4 - s_5 = x \cdot y \cdot z - u_1 = 0, \qquad (21.3)$$

Для четверки $\left(\overrightarrow{a^2}, \overrightarrow{b^2}, \overrightarrow{z^2}, \overrightarrow{c^2}\right)$:

$$\begin{pmatrix}1\\0\\0\\0\\1\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\\s_5\\s_6\end{pmatrix} \times \begin{pmatrix}1\\0\\0\\0\\0\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\\s_5\\s_6\end{pmatrix} \times \begin{pmatrix}1\\0\\0\\0\\0\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\\s_5\\s_6\end{pmatrix} - \begin{pmatrix}0\\0\\0\\1\\1\\0\end{pmatrix}\begin{pmatrix}s_1\\s_2\\s_3\\s_4\\s_5\\s_6\end{pmatrix} =$$

$$= (s_1 + s_5) \cdot s_1 \cdot s_1 - s_6 = u_1 + 1 - u_2 = 0, \qquad (21.4)$$

Мы составили систему ограничений из четверок векторов $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{z^i}, \overrightarrow{c^i}\right), i \in \{1,2\}$, аналогичную системе ограничений из троек векторов (4).

Если же хотя бы одно из выражений (21.3), (21.4) не обращается в ноль при заданном $\vec{s}$, то это означает, что допустимый набор присваивания $\vec{s}$ составлен некорректно.

2.2. Модифицированный переход от системы векторов ограничений к группам интерполяционных многочленов

Схожим образом с преобразованием троек векторов ограничений к группам полиномов, покажем преобразование четверок векторов ограничений к группам полиномов с использованием метода интерполяции Лагранжа. Построим многочлены с помощью элементов векторов ограничений $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{z^i}, \overrightarrow{c^i}\right)$ из (20):

для векторов a^i:

$$A_1(x) \text{ для точек } (1, a_1^1), (2, a_1^2), \dots, \left(d, a_1^d\right)$$

$$A_2(x) \text{ для точек } (1, a_2^1), (2, a_2^2), \dots, \left(d, a_2^d\right)$$

…

$$A_m(x) \text{ для точек } (1, a_m^1), (2, a_m^2), \dots, (d, a_m^d)$$

Примечание 4. Таким образом, многочлен $A_1(x)$ проходит через первые координаты всех векторов ограничений $a^1, a^2, \dots, a^d$. Так что $A_i(x)$ проходит через i-е координаты всех векторов ограничений $a^1, a^2, \dots, a^d$. Аналогичные выводы справедливы для многочленов $B_i(x), Z_i(x), C_i(x), i \in \{1, 2, \dots m\}, i \in \mathbb{N}$.

для векторов b^i:

$$B_1(x) \text{ для точек } (1, b_1^1), (2, b_1^2), \dots, \left(d, b_1^d\right)$$

$$B_2(x) \text{ для точек } (1, b_2^1), (2, b_2^2), \dots, \left(d, b_2^d\right)$$

…

$$B_m(x) \text{ для точек } (1, b_m^1), (2, b_m^2), \dots, (d, b_m^d)$$

для векторов z^i:

$$Z_1(x) \text{ для точек } (1, z_1^1), (2, z_1^2), \dots, \left(d, z_1^d\right)$$

$$Z_2(x) \text{ для точек } (1, z_2^1), (2, z_2^2), \dots, \left(d, z_2^d\right)$$

...

$$Z_m(x) \text{ для точек } (1, z_m^1), (2, z_m^2), \dots, (d, z_m^d)$$

для векторов c^i:

$$C_1(x) \text{ для точек } (1, c_1^1), (2, c_1^2), \dots, \left(d, c_1^d\right)$$

$$C_2(x) \text{ для точек } (1, c_2^1), (2, c_2^2), \dots, \left(d, c_2^d\right)$$

...

$$C_m(x) \text{ для точек } (1, c_m^1), (2, c_m^2), \dots, (d, c_m^d)$$

Таким образом, мы построили многочлены:

$$A_1(x), \dots, A_m(x), B_1(x), \dots, B_m(x), Z_1(x), \dots, Z_m(x), C_1(x), \dots, C_m(x),$$
$$\deg\left(A_i(x)\right) = \deg\left(B_i(x)\right) = \deg\left(Z_i(x)\right) = \deg\left(C_i(x)\right) \leq d - 1, \qquad (22)$$

Составим векторы из этих многочленов следующим образом:

$$\overrightarrow{A(x)} = (A_1(x), A_2(x), \dots, A_m(x))$$

$$\overrightarrow{B(x)} = (B_1(x), B_2(x), \dots, B_m(x))$$

$$\overrightarrow{Z(x)} = (Z_1(x), Z_2(x), \dots, Z_m(x))$$

$$\overrightarrow{C(x)} = (C_1(x), C_2(x), \dots, C_m(x))$$

Подставив номер i-го действия вместо x, мы получим четверку векторов ограничений $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{z^i}, \overrightarrow{c^i}\right)$ для этого действия.

Например, пусть $x = 1$, тогда:

$$\overrightarrow{A(1)} = (A_1(1), A_2(1), \dots, A_m(1)) = (a_1^1, a_2^1, \dots, a_m^1) = \overrightarrow{a^1}$$

$$\overrightarrow{B(1)} = (B_1(1), B_2(1), \dots, B_m(1)) = (b_1^1, b_2^1, \dots, b_m^1) = \overrightarrow{b^1}$$

$$\overrightarrow{Z(1)} = (Z_1(1), Z_2(1), \dots, Z_m(1)) = (z_1^1, z_2^1, \dots, z_m^1) = \overrightarrow{z^1}$$

$$\overrightarrow{C(1)} = (C_1(1), C_2(1), \dots, C_m(1)) = (c_1^1, c_2^1, \dots, c_m^1) = \overrightarrow{c^1}$$

2.3. Модификация квадратичной арифметической программы

Пусть задан *целевой многочлен* из (8):

$$T(x) := (x - 1) \cdot (x - 2) \cdot \ldots \cdot (x - d)$$

Пусть также заданы многочлены из (22): $A_1(x), \ldots, A_m(x), B_1(x), \ldots, B_m(x), Z_1(x), \ldots, Z_m(x), C_1(x), \ldots, C_m(x)$.

Определение 3:

Квадратичная арифметическая программа Q (КАП) степени d и размера m состоит из многочленов:

$A_1(x), \ldots, A_m(x), B_1(x), \ldots, B_m(x), Z_1(x), \ldots, Z_m(x), C_1(x), \ldots, C_m(x)$ и целевого многочлена $T(x)$.

Определение 4:

Определим $A(x) := \sum_{i=1}^{m} s_i \cdot A_i(x)$, $B(x) := \sum_{i=1}^{m} s_i \cdot B_i(x)$, $Z(x) := \sum_{i=1}^{m} s_i \cdot Z_i(x)$, $C(x) := \sum_{i=1}^{m} s_i \cdot C_i(x)$, $E(x) := A(x) \cdot B(x) \cdot Z(x) - C(x)$.

Набор допустимых значений $\vec{s} = (s_1, s_2, \ldots, s_m)$ *удовлетворяет* КАП Q, если, многочлен $E(x)$ делится без остатка на целевой многочлен $T(x)$.

Лемма 4. Пусть заданы набор значений $\vec{s} = (s_1, s_2, \ldots, s_m)$ *и многочлены* $A(x) := \sum_{i=1}^{m} s_i \cdot A_i(x)$, $B(x) := \sum_{i=1}^{m} s_i \cdot B_i(x)$, $Z(x) := \sum_{i=1}^{m} s_i \cdot Z_i(x)$, $C(x) := \sum_{i=1}^{m} s_i \cdot C_i(x)$, $E(x) := A(x) \cdot B(x) \cdot Z(x) - C(x)$.

Если $\vec{s}$ *– допустимый набор значений, то* $E(x)$ *равен нулю в точках* $x \in \{1, 2, \ldots, d\}$. *Если же* $\vec{s}$ *не является допустимым набором значений, то E(x) не обращается в ноль для всех* $x \in \{1, 2, \ldots, d\}$.

Доказательство:

Представим $E(x)$ в скалярном виде:

$$\begin{pmatrix} A_1(x) \\ A_2(x) \\ A_3(x) \\ \cdots \\ \cdots \\ A_m(x) \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} \times \begin{pmatrix} B_1(x) \\ B_2(x) \\ B_3(x) \\ \cdots \\ \cdots \\ B_m(x) \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} \times \begin{pmatrix} Z_1(x) \\ Z_2(x) \\ Z_3(x) \\ \cdots \\ \cdots \\ Z_m(x) \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} - \begin{pmatrix} C_1(x) \\ C_2(x) \\ C_3(x) \\ \cdots \\ \cdots \\ C_m(x) \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} =$$
$$= A(x) \cdot B(x) \cdot Z(x) - C(x) = E(x), \quad (23.1)$$

Подставив в $E(x)$ $x = i$ – номер действия, $i \in \{1, 2, \dots, \mathrm{d}\}$, получим уравнение вида (21):

$$E(i) = \begin{pmatrix} a_1^i \\ a_2^i \\ a_3^i \\ \cdots \\ \cdots \\ a_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} \times \begin{pmatrix} b_1^i \\ b_2^i \\ b_3^i \\ \cdots \\ \cdots \\ b_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} \times \begin{pmatrix} z_1^i \\ z_2^i \\ z_3^i \\ \cdots \\ \cdots \\ z_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} - \begin{pmatrix} c_1^i \\ c_2^i \\ c_3^i \\ \cdots \\ \cdots \\ c_m^i \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ \cdots \\ s_m \end{pmatrix} = 0 \quad (23.2)$$

Вектора ограничений $\left(\overrightarrow{a^i}, \overrightarrow{b^i}, \overrightarrow{z^i}, \overrightarrow{c^i}\right)$ из (18) были построены таким образом, что для допустимого набора значений $\vec{s}$ уравнение (23.2) обращается в ноль для всех $i \in \{1, 2, \dots, d\}$, а значит и $E(x)$ обращается в ноль для всех $x = i \in \{1, 2, \dots, d\}$. Если же $\vec{s} = (s_1, s_2, \dots, s_m)$ – не является набором допустимых значений, то для некоторого i уравнение (23.2) не обращается в ноль, а так как уравнение (23.2) — это уравнение $E(i) = 0$, то $\exists x \in \{1, 2, \dots, d\}, E(x) \neq 0$. Лемма доказана.

Лемма 5. Пусть заданы набор значений $\vec{s} = \left(s_{1,} s_2, \dots, s_m\right)$ *и многочлены* $A(x) := \sum_{i=1}^{m} s_i \cdot A_i(x)$, $B(x) := \sum_{i=1}^{m} s_i \cdot B_i(x)$, $Z(x) := \sum_{i=1}^{m} s_i \cdot Z_i(x)$, $C(x) := \sum_{i=1}^{m} s_i \cdot C_i(x), E(x) := A(x) \cdot B(x) \cdot Z(x) - C(x)$.

Тогда степени $A(x), B(x), Z(x), C(x)$ *не выше* $d - 1$. *Степень* $E(x)$ *не выше* $3(d - 1)$.

Доказательство:

$A(x), B(x), Z(x), C(x)$ являются линейной комбинацией многочленов степени

не выше $d-1$, а значит их степени не выше $d-1$. Так как $E(x) := A(x) \cdot B(x) \cdot Z(x) - C(x)$, то его степень не превосходит суммы степеней $A(x)$, $B(x)$, $Z(x)$.

$$deg\big(A(x)\big) \leq d-1,$$
$$deg\big(B(x)\big) \leq d-1,$$
$$deg\big(Z(x)\big) \leq d-1,$$
$$deg\big(C(x)\big) \leq d-1,$$
$$deg\big(E(x)\big) \leq deg\big(A(x)\big) + deg\big(B(x)\big) + deg\big(Z(x)\big) \leq 3(d-1), \quad (23.3)$$

Лемма доказана.

Обратим внимание на то, что если $\vec{s}$ удовлетворяет *КАП* Q, то согласно определению 4 $E(x)$ делится нацело многочленом $T(x)$ и согласно *лемме* 4, лемме 5 и теории линейной алгебры, мы можем представить $E(x)$ в виде:

$$E(x) \equiv H(x) \cdot T(x), \qquad \forall x \in F_p \quad (24)$$

2.4. Модификация в методе случайного сдвига многочленов.

Пусть задан набор присваивания $\vec{s}$, удовлетворяющий КАП Q из определения 4 и пусть с помощью $\vec{s}$ построены $A(x), B(x), Z(x), C(x), H(x), T(x)$. Из примечания 8 следует тождество (24):

$$A(x) \cdot B(x) \cdot Z(x) - C(x) \equiv H(x) \cdot T(x), \qquad \forall x \in F_p, \tag{25.1}$$

Выберем случайным образом $\delta_1, \delta_2, \delta_3, \delta_4 \in \mathbb{F}_p^*$ и определим многочлены $\tilde{A}(x), \tilde{B}(x), \tilde{Z}(x), \tilde{C}(x), \tilde{H}(x)$, отличные от $A(x), B(x), C(x), H(x)$:

$$\tilde{A}(x) := A(x) + \delta_1 T(x)$$

$$\tilde{B}(x) := B(x) + \delta_2 T(x)$$

$$\tilde{Z}(x) := Z(x) + \delta_3 T(x)$$

$$\tilde{C}(x) := C(x) + \delta_4 T(x)$$

$$\begin{gathered}\tilde{H}(x) = H(x) + \delta_1 A(x)B(x) + \delta_2 A(x)Z(x) + \delta_2\delta_3 A(x)T(x) + \\ \delta_1 B(x)Z(x) + \delta_1\delta_3 B(x)T(x) + \delta_1\delta_2 T(x)Z(x) + \delta_1\delta_2\delta_3 T(x)^2 + \delta_4,\end{gathered} \tag{25.2}$$

Тогда для них выполняется тождество:

$$\begin{gathered}\tilde{A}(x) \cdot \tilde{B}(x) \cdot \tilde{Z}(x) - \tilde{C}(x) = \\ = \big(A(x) + \delta_1 T(x)\big) \cdot \big(B(x) + \delta_2 T(x)\big) \cdot \big(Z(x) + \delta_3 T(x)\big) - \\ -\big(C(x) + \delta_4 T(x)\big) = T(x)(H(x) + \delta_1 A(x)B(x) + \\ +\delta_2 A(x)Z(x) + \delta_2\delta_3 A(x)T(x) + \delta_1 B(x)Z(x) + \\ +\delta_1\delta_3 B(x)T(x) + \delta_1\delta_2 T(x)Z(x) + \delta_1\delta_2\delta_3 T(x)^2 + \delta_4) \equiv \\ \equiv \tilde{H}(x) \cdot T(x), \qquad \forall x \in F_p\end{gathered} \tag{25.3}$$

Итак, замена многочленов $A(x), B(x), Z(x), C(x), H(x)$ на $\tilde{A}(x), \tilde{B}(x), \tilde{Z}(x), \tilde{C}(x), \tilde{H}(x)$ обеспечивает выполнение тождества (25.3), эквивалентного (25.1).

2.5. Проверка правильности построения многочленов $A(x), B(x), Z(x), C(x)$.

Аналогично пункту 1.2.5. представим проверку правильности построение многочленов $A(x), B(x), C(x), Z(x)$. Они должны быть построены следующим образом:

$$A(x) := \sum_{i=1}^{m} s_i \cdot A_i(x), \qquad B(x) := \sum_{i=1}^{m} s_i \cdot B_i(x),$$
$$Z(x) := \sum_{i=1}^{m} s_i \cdot Z_i(x), \quad C(x) := \sum_{i=1}^{m} s_i \cdot C_i(x), \tag{26.1}$$

Схожим образом с (10.1) объединим $A(x), B(x), Z(x), C(x)$ в один многочлен $F(x)$ следующим образом:

$$F(x) = A(x) + B(x) \cdot x^{d+1} + Z(x) \cdot x^{2(d+1)} + C(x) \cdot x^{3(d+1)}, \tag{26.2}$$

Многочлены $F_i(x)$ составим, используя многочлены из (20):

$$F_i(x) = A_i(x) + B_i(x) \cdot x^{d+1} + Z_i(x) \cdot x^{2(d+1)} + C_i(x) \cdot x^{3(d+1)},$$
$$i \in \{1, 2, \dots, m\}, \tag{26.3}$$

Обратим внимание на то, что при суммировании $F_i(x)$, суммируются коэффициенты при соответствующих многочленых. Например:

$$F_1(x) + F_2(x) = (A_1(x) + A_2(x)) +$$
$$(B_1(x) \cdot B_2(x)) \cdot x^{d+1} +$$
$$(Z_1(x) \cdot Z_2(x)) \cdot x^{2(d+1)} +$$
$$(C_1(x) \cdot C_2(x)) \cdot x^{3(d+1)}, \tag{26.4}$$

Боб будет использовать *лемму 3*, чтобы удостовериться в том, то $A(x), B(x), Z(x), C(x)$ были составлены с помощью одно и того же набора присваиваний, если Алиса докажет, что $F(x)$ – линейная комбинация $F_i(x)$.

Доказать, что $F(x) = \sum_{i=1}^{m} s_i \cdot F_i(x)$ можно, применив метод *слепого вычисления многочленов* и метод *предположения о знании коэффициента*, описанный в работе [5].

2.6. Модификация протокола Пиноккио

Пусть есть две стороны, которые мы обозначим как Алиса и Боб. Алиса хочет доказать Бобу, что она обладает допустимым набором присваивания $\vec{s} = (s_1, s_2, \dots, s_m) \in \mathbb{F}_p$ (3), удовлетворяющим Q из определения 4, без раскрытия $\vec{s}$.

Пусть задан полный гомоморфный шифр $Enc(x)$ со свойствами (13.1)-(13.2).

Модифицируем протокол Пиноккио [5]:

5. Алиса строит многочлены $A(x), B(x), Z(x), C(x), E(x)$ из определения 2:

$$A(x) := \sum_{i=1}^{m} s_i \cdot A_i(x), \qquad B(x) := \sum_{i=1}^{m} s_i \cdot B_i(x),$$
$$Z(x) := \sum_{i=1}^{m} s_i \cdot Z_i(x), \qquad C(x) := \sum_{i=1}^{m} s_i \cdot C_i(x)$$
$$E(x) := A(x) \cdot B(x) \cdot Z(x) - C(x), \tag{27.1}$$

Многочлены $A(x), B(x), Z(x), C(x), H(x)$ построены с помощью допустимого набора присваивания $\vec{s}$, а потому эти многочлены раскрывают информацию об $\vec{s}$. Поэтому Алиса использует *случайный сдвиг многочленов* и составляет многочлены $\tilde{A}(x), \tilde{B}(x), \tilde{Z}(x), \tilde{C}(x), \tilde{H}(x)$ как в (25.2). Из (25.3) имеет место тождество:

$$\tilde{E}(x) := \tilde{A}(x) \cdot \tilde{B}(x) \cdot \tilde{Z}(x) - \tilde{C}(x) \equiv \tilde{H}(x) \cdot T(x)$$

6. Задана *общая ссылочная строка*:

$$Enc(q^0), Enc(q^1), \dots, Enc\left(q^{3(d-1)}\right), d \in \mathbb{N}, \tag{27.2}$$

7. Алиса формирует доказательство, которое состоит из значений $Enc\left(\tilde{A}(q)\right), Enc\left(\tilde{B}(q)\right), Enc(\tilde{Z}(q)), Enc\left(\tilde{C}(q)\right), Enc(\tilde{H}(q))$. Алиса может вычислить эти значения, используя *метод слепого вычисления многочленов* (14.2). Сообщение отправляется Бобу.

8. Боб, используя свойства (13.1)-(13.2) шифра $Enc(x)$, проверяет, что:

$$Enc\left(\tilde{A}(q)\cdot\tilde{B}(q)\cdot\tilde{Z}(q)-\tilde{C}(q)\right)=\ Enc\left(T(q)\cdot\tilde{H}(q)\right), \qquad (28)$$

Заметим, что (28) эквивалентно:

$$Enc\left(A(q)\cdot B(q)\cdot Z(q)-\ C(q)\right)=\ Enc\left(T(q)\cdot H(q)\right)$$

Если левая и правая части уравнения (28) равны, то Боб с уверенностью может полагать, что Алиса обладает допустимым набором значений $\vec{s}=(s_1,s_2,\dots,s_m)\in\mathbb{F}_p^m$. При этом Алиса не раскрывает Бобу $\vec{s}, E(x), A(x), B(x), C(x), H(x)$.

Так как в качестве q была выбрана случайная точка из $\mathbb{F}_p$, то согласно (12) вероятность того, что многочлены $A(x), B(x), Z(x), C(x), H(x)$, построенные без допустимого набора значений, будут удовлетворять равенству (28) мала. Следовательно, Алиса не сможет убедить Боба с высокой вероятностью в том, что она обладает $\vec{s}$, без его наличия.

Примечание 5. *Поясним важность случайного сдвига многочленов. Если бы у Боба был набор присваивания $\vec{h}$, удовлетворяющий Q и отличный от набора присваивания Алисы $\vec{s}$, то он бы мог построить многочлены $A_h(x), B_h(x), Z_h(x), C_h(x), H_h(x)$ и вычислить $Enc(A_h(q)), Enc(B_h(q)), Enc(Z_h(q)), Enc(C_h(q)), Enc(H_h(q))$. Эти значения он бы мог сравнить с значениями $Enc(A_s(q)), Enc(B_s(q)), Enc(Z_s(q)), Enc(C_s(q)), Enc(H_s(q))$, полученными от Алисы, и сделать вывод о том, что они различны, а, следовательно, набор*

присваивания $\vec{h}$ *Боба отличается от набора присваивания* $\vec{s}$ *Алисы. Это раскрывает некоторую информацию об* $\vec{s}$*. При использовании же случайного сдвига многочленов Алиса не раскрывает ничего об* $\vec{s}$*.*

3. Анализ параметров модифицированного протокола

3.1. Построение модельных примеров

Пусть задан многочлен над полем $\mathbb{F}_{13}$:

$$f(x) = x^3 + 3x + 8, \quad (29)$$

Покажем работу изначальной и модифицированной версии протокола ZK-SNARK для $f(x)$.

3.1.1. Построение модельного примера для оригинального протокола

Пусть задан многочлен $f(x)$ из (29):

$$x^3 + 3x + 8 = 0$$

В первую очередь воспользуемся старым способом разбиения многочлена на действия (2):

1) $u_1 = x \cdot x$
2) $u_2 = u_1 \cdot x$
3) $u_3 = u_2 + 3x$
4) $u_4 = u_3 + 8$

Определим допустимый набор присваиваний:

$$\vec{s} = (1, x, u_1, u_2, u_3, u_4) \in \mathbb{F}_p^m, p = 13, m = 6$$

Выпишем тройки векторов ограничений (4) для каждого действия:

1) $\overrightarrow{a^1} = (0,1,0,0,0,0), \overrightarrow{b^1} = (0,1,0,0,1,0),\ \overrightarrow{c^1} = (0,0,1,0,0,0)$

2) $\overrightarrow{a^2} = (0,0,1,0,0,0), \overrightarrow{b^2} = (0,1,0,0,0,0),\ \overrightarrow{c^2} = (0,0,0,1,0,0)$

3) $\overrightarrow{a^3} = (0,3,0,1,0,0), \overrightarrow{b^3} = (1,0,0,0,0,0),\ \overrightarrow{c^3} = (0,0,0,0,1,0)$

4) $\overrightarrow{a^4} = (8,0,0,0,1,0), \overrightarrow{b^4} = (1,0,0,0,0,0),\ \overrightarrow{c^4} = (0,0,0,0,0,1)$

Построим интерполяционные многочлены степени как в (7):

$$A_1(x), A_2(x), \dots, A_6(x)$$

$$B_1(x), B_2(x), \dots, B_6(x)$$

$$C_1(x), C_2(x), \dots, C_6(x)$$

Итак, мы построили группы многочленов степени не выше 3. Составим многочлены $A(x), B(x), C(x), T(x)$ степени не выше 3 из определения 2:

$$A(x) := \sum_{i=1}^{6} s_i \cdot A_i(x),$$
$$B(x) := \sum_{i=1}^{6} s_i \cdot B_i(x),$$
$$C(x) := \sum_{i=1}^{6} s_i \cdot C_i(x),$$
$$T(x) := (x - 1) \cdot (x - 2) \cdot \dots \cdot (x - 4), \quad (30)$$

Общая ссылочная строка для протокола Пиноккио будет иметь вид:

$$Enc(q^0), Enc(q^1), \dots, Enc(q^6),$$
$$d \in \mathbb{N}, q - \text{случайно выбранная точка из } \mathbb{F}_{13}, \quad (31)$$

Алиса должна будет построить доказательство с помощью значений гомоморфного шифра $Enc\left(\tilde{A}(q)\right), Enc\left(\tilde{B}(q)\right), Enc(\tilde{C}(q)), Enc(\tilde{H}(q))$ и отправить его Бобу.

Боб проверяет, что:

$$Enc\left(\tilde{A}(q) \cdot \tilde{B}(q) - \tilde{C}(q)\right) = Enc\left(T(q) \cdot \tilde{H}(q)\right), \quad (32)$$

3.1.2. Построение модельного примера модифицированного протокола

Пусть также определен многочлен $f(x)$ из (29):

$$x^3 + 3x + 8 = 0$$

Применим новый способ разбиения многочлена на действия (19):

1) $u_1 = x \cdot x \cdot x$

2) $u_2 = u_1 + 3x$

3) $u_3 = u_2 + 8$

Определим допустимый набор присваиваний:

$$\vec{s} = (1, x, u_1, u_2, u_3) \in \mathbb{F}_p^m, p = 13, m = 5$$

Построим четверки векторов ограничений (18) для каждого действия:

1) $\overrightarrow{a^1} = (0,1,0,0,0), \overrightarrow{b^1} = (0,1,0,0,0), \overrightarrow{z^1} = (0,1,0,0,0)\ \overrightarrow{c^1} = (0,0,1,0,0)$

2) $\overrightarrow{a^2} = (0,3,1,0,0), \overrightarrow{b^2} = (1,0,0,0,0),\ \overrightarrow{z^2} = (1,0,0,0,0)\ \overrightarrow{c^2} = (0,0,0,1,0)$

3) $\overrightarrow{a^3} = (8,0,0,1,0), \overrightarrow{b^3} = (1,0,0,0,0), \overrightarrow{z^3} = (1,0,0,0,0)\ \overrightarrow{c^3} = (0,0,0,0,1)$

Построим интерполяционные многочлены степени как в (22):

$$A_1(x), A_2(x), \dots, A_5(x)$$

$$B_1(x), B_2(x), \dots, B_5(x)$$

$$Z_1(x), Z_2(x), \dots, Z_5(x)$$

$$C_1(x), C_2(x), \dots, C_5(x)$$

Итак, мы построили группы многочленов степени не выше 2. Составим многочлены $A(x), B(x), Z(x), C(x), T(x)$ степени не выше 2 из определения 4:

$$A(x) := \sum_{i=1}^{5} s_i \cdot A_i(x),$$

$$B(x) := \sum_{i=1}^{5} s_i \cdot B_i(x),$$

$$Z(x) := \sum_{i=1}^{5} s_i \cdot Z_i(x)$$

$$C(x) := \sum_{i=1}^{5} s_i \cdot C_i(x),$$

$$T(x) := (x - 1) \cdot (x - 2) \cdot \dots \cdot (x - 3), \qquad (33)$$

Общая ссылочная строка для протокола Пиноккио будет иметь вид:

$$Enc(q^0), Enc(q^1), \dots, Enc(q^4),$$
$$d \in \mathbb{N}, q - \text{случайно выбранная точка из } \mathbb{F}_{13}, \quad (34)$$

Алиса должна будет построить доказательство с помощью значений гомоморфного шифра $Enc(\tilde{A}(q)), Enc(\tilde{B}(q)), Enc(\tilde{Z}(q)), Enc(\tilde{C}(q)), Enc(\tilde{H}(q))$ и отправить его Бобу.

Боб проверяет, что:

$$Enc\left(\tilde{A}(q) \cdot \tilde{B}(q) \cdot \tilde{Z}(q) - \tilde{C}(q)\right) = Enc\left(T(q) \cdot \tilde{H}(q)\right), \quad (35)$$

3.2. Анализ параметров модифицированного протокола

В рамках исследования было выявлено:

1. Размер общей ссылочной строки (27.2) увеличился относительно количества действий d для вычисления многочлена на 50 процентов в сравнение с изначальным вариантом (16.2).

   Размер действий d для вычисления многочлена сократился. Если ранее количество действий для достаточно большой степени многочлена можно было оценить как $d \approx \log_2 x$, где $x -$ максимальная степень многочлена то для модифицированной версии протокола $\tilde{d} \approx \log_3 x$ (см. лемма 6). Можно оценить отношение количества действий в оригинальном протоколе к новому значению $\tilde{d}$ как:

$$\frac{d-\tilde{d}}{d} = \frac{\log_2 x - \log_3 x}{\log_2 x} = 1 - \frac{\log_3 x}{\log_2 x} \approx 0.37,$$
$$\tilde{d} = \frac{\log_3 x}{\log_2 x} \cdot d \qquad (36)$$

   Таким образом, учитывая соотношение (36), подсчитываем изменение в размере общей ссылочной строки $|\widetilde{CRS}|$ к изначальному размеру $|CRS|$:

$$\frac{|\widetilde{CRS}|}{|CRS|} = \frac{3(\tilde{d}-1)}{2(d-1)} = \frac{3 \cdot \frac{\log_3 x}{\log_2 x} d - 3}{2d-2},$$
$$0.88 \leq \frac{3 \cdot \frac{\log_3 x}{\log_2 x} 10 - 3}{20-2} \leq \frac{|\widetilde{CRS}|}{|CRS|} \leq \lim_{d\to\infty} \frac{3 \cdot \frac{\log_3 x}{\log_2 x} d - 3}{2d-2} =$$
$$\lim_{d\to\infty} \frac{d\left(3 \cdot \frac{\log_3 x}{\log_2 x} - \frac{3}{d}\right)}{d\left(2 - \frac{2}{d}\right)} = \lim_{d\to\infty} \frac{3 \cdot \frac{\log_3 x}{\log_2 x}}{2} \approx 0.945,$$
$$d \in [10, \infty), \qquad (37)$$

Из (37) можно сделать вывод, что сокращение в размере $\widetilde{CRS}$ варьируется от 5.5 до 11 процентов. При достаточно больших d (>1000) сокращение размера не достигает 5.5 процентов.

2. Отметим также, что при проверке доказательства Бобу будет необходимо проверить на одно значения больше, вычислив произведение гомоморфных шифров. Заметим, что время выполнения данной операции может быть значительным в зависимости от выбранной реализации шифра [7].

Лемма 6. Пусть задано значение x и необходимо вычислить x^m с помощью действий вида (2) и (19).

Тогда можно вычислить x^m с помощью действий вида (2) за $log_2 m$ шагов, а с помощью действий вида (19) за $log_3 m$ шагов.

Доказательство:

Для вычисления x^m при заданном значении x и действиях вида *(2)*, необходимо будет формировать действия следующим образом*:*

$$u_1 = x \cdot x = x^2$$

$$u_2 = u_1 \cdot u_1 = x^4$$

....

$$u_i = u_{i-1} \cdot u_{i-1} = x^{2^i}$$

Таким образом, на i -м шаге, x будет возведен в степень 2^i. Значит, чтобы вычислить, сколько шагов потребуется для вычисления степени d необходимо решить уравнение*:*

$$2^d = m$$

Решением данного уравнение будет $d = log_2 m$ – количество действий для вычисления x^mс помощью действий вида *(2).*

Аналогичные рассуждения следуют для вычисления x^m с помощью действий вида *(19):*

$$u_1 = x \cdot x \cdot x = x^3$$

$$u_2 = u_1 \cdot u_1 \cdot u_1 = x^9$$

....

$$u_i = u_i \cdot u_i \cdot u_i = x^{3^i}$$

Решением данного уравнение будет $d = log_3 m$ – количество действий для вычисления x^mс помощью действий вида *(19).*

3.3. О неисследованных следствиях модификации протокола ZK-SNARK

При построении протокола ZK-SNARK важную роль играет доказательство правильности построения многочленов $A(x), B(x), C(x), Z(x)$ согласно определению 4. В данной работе не было изучено, каким образом изменится размер доказательства правильности построения вышеуказанных многочленов.

Также следует отметить, что не были рассмотрены спаривания эллиптических кривых[6], использованные в качестве гомоморфного шифра в оригинальном протоколе [5].

Данная работа также не исследует одновременное использование метода проверки правильности построения многочленов (пункт 2.5.) и протокола Пиноккио (пункт 2.6.).

3.4. Рассуждения о дальнейших возможных модификациях протокола ZK-SNARK

По аналогии с осуществленной модификацией действий (19) можно увеличить количество множителей в каждом действии с 2 до $n + 2$, что приведет к снижению количества действий до $\log_{n+2} d$, где d – степень многочлена (1.1). Следовательно, будет иметь место рост числа векторов ограничений и интерполяционных многочленов с 3 до $n + 3$, так как каждому дополнительному сомножителю будет соответствовать дополнительный вектор ограничений, а следовательно, дополнительный интерполяционный многочлен. Это увеличит время проверки в протоколе Пиноккио на стороне Боба, так как ему будет необходимо найти произведение $n + 3$ шифров от значений многочленов в случайно выбранной точке вместо 3 значений в изначальном протоколе.

Общая ссылочная строка в случае с введением n дополнительных множителей в действия увеличится относительно d со значения $2(d - 1)$ до значения $(2 + n)(d - 1)$. Оценить длину общей ссылочной строки $|CRS|$ в абсолютном выражении можно с помощью формулы:

$$|CRS| = \frac{(\log_{n+2} d) \cdot (2 + n) \cdot (d - 1)}{\log_2 d},$$

где $n -$ количество добавленных множителей в действии,
$d -$ степень многочлена из (1.1), (38)

Заключение

В рамках работы был изучен протокол *Ethereum*, протоколы слепого вычисления многочленов, протокол *Пиноккио*, полные гомоморфные шифры.

Также была представлена модификация примитива современного криптографического агрегата – протокола *ZK-SNARK*.

В результате выполнения работы была проанализирована возможность использования модифицированного протокола и выявлено, что изменение протокола позволяет сократить количество действий, которые должны отвечать за формирование многочлена, примерно на 37 процентов. Размер данных для коммуникаций в канале рамках данного протокола сократился на 5.5–11 процентов. Стоит подчеркнуть, что требуются дополнительные исследования размера доказательства правильности построения вышеуказанных многочленов. Также в работе не были рассмотрены спаривания эллиптических кривых, использованные в качестве гомоморфного шифра в оригинальном протоколе [5].

Список литературы

1. Ethereum Whitepaper – URL: https://ethereum.org/en/whitepaper/#ethereum (дата обращения 02.06.2023)

2. Schwartz J. T. Fast probabilistic algorithms for verification of polynomial identities //Journal of the ACM (JACM). – 1980. – Т. 27. – №. 4. – С. 701-717.

3. Gennaro R. et al. Quadratic span programs and succinct NIZKs without PCPs //Advances in Cryptology–EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings 32. – Springer Berlin Heidelberg, 2013. – С. 626-645.

4. Gabizon A. Explaining SNARKs – URL: https://electriccoin.co/blog/snark-explain/ (дата обращения 02.06.2023)

5. Parno B. et al. Pinocchio: Nearly practical verifiable computation //Communications of the ACM. – 2016. – Т. 59. – №. 2. – С. 103-112.

6. Groth J. Short Pairing-Based Non-interactive Zero-Knowledge Arguments //Asiacrypt. – 2010. – Т. 6477. – С. 321-340.

7. Brakerski Z., Gentry C., Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping //ACM Transactions on Computation Theory (TOCT). – 2014. – Т. 6. – №. 3. – С. 1-36.

8. Bünz B., Fisch B., Szepieniec A. Transparent SNARKs from DARK compilers //Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part I 39. – Springer International Publishing, 2020. – С. 677-706.