Презентация к докладу

Варианты протокола вручения бита. Подбрасывание монеты по телефону

Исламова С.М.
2 декабря 2025
Российский университет дружбы народов, Москва, Россия

Вводная часть

Актуальность

- Фундаментальный примитив современной криптографии
- Основа электронного голосования, блокчейнов, онлайн-лотерей
- Задача сформулирована Мануэлем Блюмом в 1981–1982 гг.
- Активно развивается в постквантовую эпоху

Цели и задачи работы

Цель работы — изучить принципы работы **протоколов вручения бита**, их криптографические свойства, а также рассмотреть классический протокол Мануэля Блюма **«подбрасывание монеты по телефону»**, который позволяет двум удалённым участникам получить честный случайный результат.

Задачи работы:

- изучить теоретические основы протоколов фиксации значения (commitment);
- объяснить необходимость скрытности и необратимости выбора;
- рассмотреть несколько вариантов протоколов вручения бита;
- описать оригинальный протокол Блюма;
- выявить основные угрозы и методы атак;
- показать практическое значение таких протоколов в современных информационных системах.

Теоретическое введение

2.1 Протоколы вручения бита

Протокол вручения бита (Bit Commitment) — это механизм, позволяющий одной стороне (Алисе) зафиксировать некое значение (бит 0 или 1) таким образом, что:

1. **Скрытность (Hiding)** — другая сторона (Боб) не может узнать значение до раскрытия.
2. **Обязательность (Binding)** — Алиса не может изменить значение после фиксации [1;2]

Такие протоколы являются фундаментальными элементами криптографии и используются в:

- электронном голосовании,
- онлайн-аукционах,
- мультипартийных вычислениях,
- блокчейн-системах,
- честных лотереях и протоколах случайного выбора.

Суть протокола аналогична «запечатанному конверту»: Алиса кладёт в конверт число, запечатывает его и передаёт Бобу, а потом вскрывает его публично.

2.1.1 Математическая модель

Для надёжного выполнения требований скрытности и обязательности применяются криптографически стойкие функции:

- **хеш-функции** — SHA-256, SHA-3 (Рис. 1);
- **односторонние функции** — вычислить прямое значение легко, обратное — невозможно;
- **случайные строки (соли)** — обеспечивают непредсказуемость.

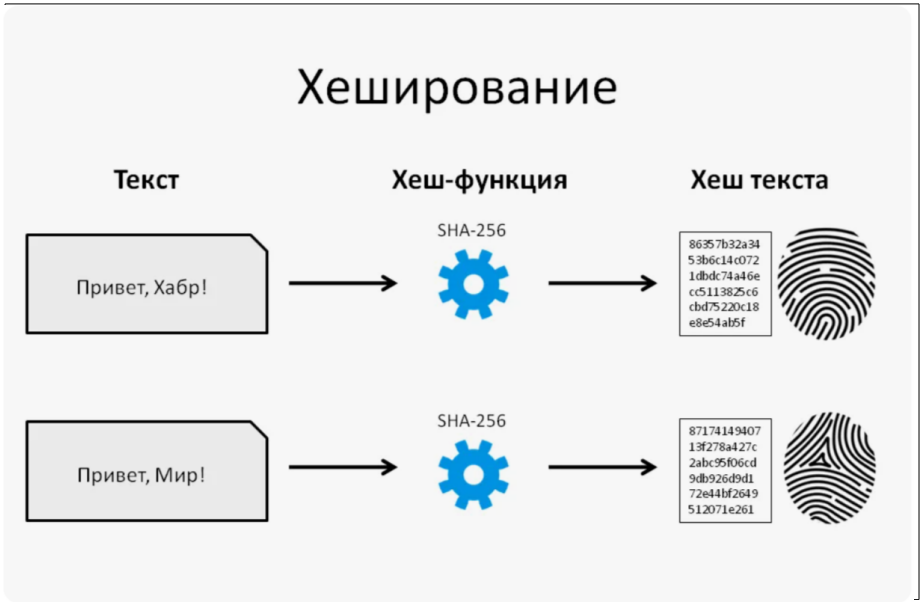

Рисунок 1 - Процесс хеширование (функция хеширования)

Пример простого коммитмента:

$C = H(b \parallel r)$

где
b — бит Алисы,
r — случайное число,
C — коммитмент.

2.1.2 Скрытность коммитмента

Хеш-функции обладают тем свойством, что по хешу невозможно определить исходные данные. Поэтому Боб не может узнать выбор Алисы до раскрытия.

2.1.3 Обязательность

Если хеш-функция устойчива к коллизиям (рис. 2), Алиса не сможет подобрать другое значение b', r' , дающее тот же хеш.

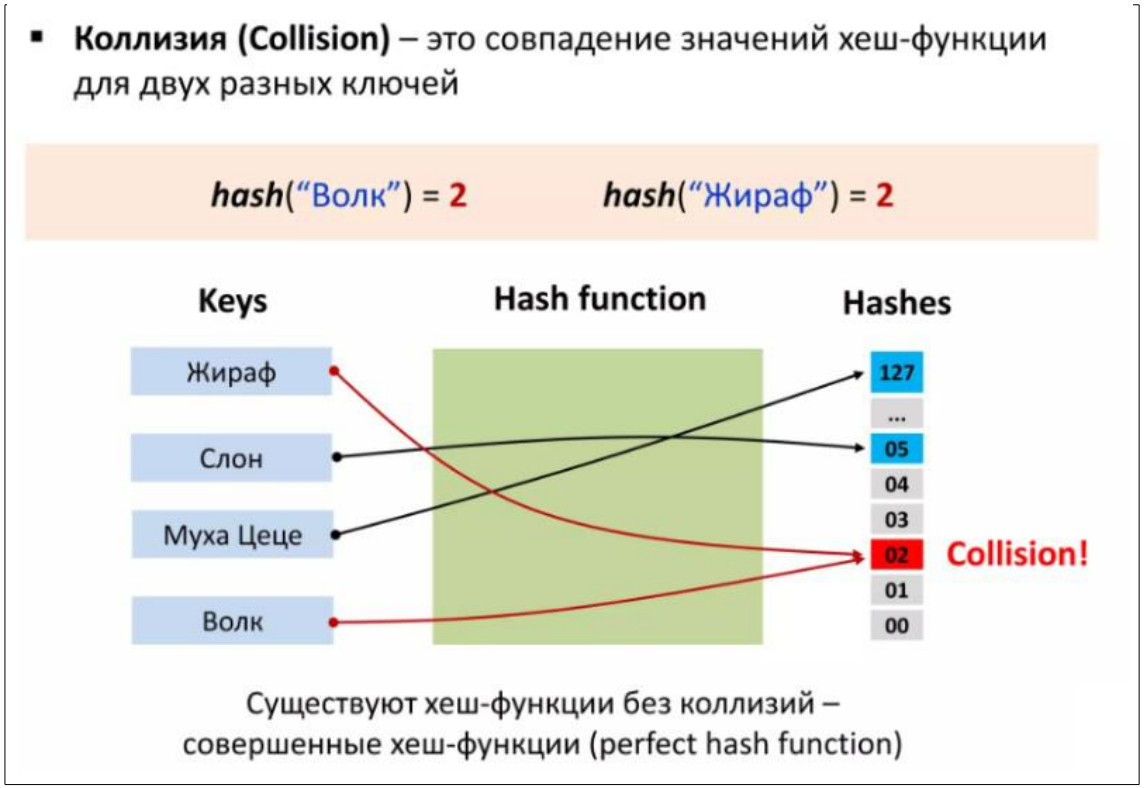

Рисунок 2 - Понятие коллизии

2.2 Мотивация: честный выбор между удалёнными участниками

Рассмотрим задачу:
две стороны хотят выбрать случайный результат (0 или 1), но не доверяют друг другу.

Без криптографии задача неразрешима:

- если выбор делает Алиса, она может подделать значение;
- если обе стороны говорят одновременно, всегда есть риск подстроить ответ.

Поэтому нужен протокол, при котором:

- Алиса фиксирует значение честно,
- Боб делает выбор независимо,
- итоговый результат не зависит от действий одной стороны.

2.3 Классическая задача: подбрасывание монеты по телефону

Проблему сформулировал М. Блюм в 1982 году [4].
Её смысл:
как двум людям на расстоянии честно симулировать подбрасывание монетки?

Пусть Алиса и Боб общаются по телефону.
Если Алиса говорит «выпал орёл», Боб ей не обязан верить.

Нужен формальный криптографический протокол.

Суть решения:

1. Алиса делает скрытый выбор (0 — орёл, 1 — решка).
2. Боб выбирает значение независимо.
3. Результат определяется XOR двух битов.

4. Никто не может обмануть, потому что коммитмент Алисы защищает от подмены.

3 Рассмотрение протоколов

3.1 Базовый протокол на основе хеш-коммитмента

1. Алиса выбирает бит *a*.
2. Генерирует случайную строку *r*.
3. Вычисляет коммитмент: **C = H(a || r)**.
4. Посылает коммитмент Бобу.
5. Боб выбирает бит *b* и отправляет его Алисе.
6. Алиса раскрывает *(a, r)*.
7. Боб проверяет корректность.
8. Итог: **a XOR b**.[5]

Достоинства:

- простота реализации;
- стойкость при правильном выборе хеша.

Недостатки:

- зависит от криптографических свойств хеша;
- требует аккуратной реализации.

3.2 Протокол с использованием симметричного шифрования

Здесь в качестве коммитмента используется шифрование.

1. Алиса выбирает бит и шифрует его ключом.
2. Передаёт шифртекст.

3. После ответа Боба раскрывает ключ.

3.3 Протокол Блюма на квадратичных вычетах

Наиболее строгий математически вариант.
Основан на сложности извлечения квадратного корня по модулю составного числа.

Используется:

- модуль $N = p \cdot q$ (секрет),
- квадратичные вычеты, обладающие необходимыми криптографическими свойствами.

Достоинства:

- строго доказанная безопасность;
- высокая стойкость к атакам.[6]

3.4 Физические протоколы случайного выбора

Используются источники энтропии:

- тепловой шум,
- радиоизлучение,
- атмосферный шум.

Эти методы иногда применяются в распределённых системах генерации ключей.[7]

3.5 Квантовые протоколы честного выбора

Современное направление:

- использование суперпозиции,
- защита на основе невозможности измерить квантовое состояние без его изменения.

Квантовый coin flipping обладает лучшими свойствами в плане честности.[8]

4. Выводы

В работе были рассмотрены:

- криптографические основы протоколов фиксации значения,
- механизмы скрытности и обязательности,
- классическая задача «подбрасывания монеты по телефону»,
- базовые и математически строгие протоколы честного выбора,
- типичные угрозы и атаки.

Изученные протоколы являются основой для:

- систем электронного голосования,
- блокчейна,
- распределённых вычислений,
- честных онлайн-лотерей,
- выбора лидера в распределённых сетях.

Протоколы честного выбора случайности остаются одной из ключевых тем криптографической теории и продолжают активно развиваться.

Список источников (литературы)

1. Отраслевой порта. Информационная безопасность бизнеса
2. Протоколы битовых обязательств.Криптографические методы защиты информации в компьютерных системах и сетях
3. Wikipedia.Криптографическая хеш-функция
4. Wikipedia.Подбрасывание монеты по телефону
5. Управление ключами шифрования и безопасность сети.Лекция 5.Управление ключами
6. Wikipedia.Алгоритм Блюма — Микали
7. Wikipedia.Источник энтропии
8. Dzen.Квантовые протоколы голосования: выборы без фальсификаций

Спасибо за внимание!