Протоколы многосторонних вычислений, часть 1

Косолапов Ю.В.

ЮФУ

9 декабря 2020 г.

Содержание

Основные объекты

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.

Основные объекты

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $\mathcal{S}$ — множество возможных значений секретов, например, множество действительных чисел, или векторы фиксированной длины на каким-то полем или кольцом.

Основные объекты

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $\mathcal{S}$ — множество возможных значений секретов, например, множество действительных чисел, или векторы фиксированной длины на каким-то полем или кольцом.
- Каждый участник i из $\mathcal{P}$ обладает некоторым секретом $s_i \in \mathcal{S}$.

Основные объекты

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $\mathcal{S}$ — множество возможных значений секретов, например, множество действительных чисел, или векторы фиксированной длины на каким-то полем или кольцом.
- Каждый участник i из $\mathcal{P}$ обладает некоторым секретом $s_i \in \mathcal{S}$.
- $f(x_1, ..., x_n)$ — функция, значение которой участники из $\mathcal{P}$ намерены вычислить. Сама функция несекретная.

Пример 1

- $\mathcal{P} = \{1, ..., n\}$ — множество студентов группы №1.

Пример 1

- $\mathcal{P} = \{1, ..., n\}$ — множество студентов группы №1.
- $\mathcal{S}$ — множество действительных чисел в диапазоне от 36.6 до 41.

Пример 1

- $\mathcal{P} = \{1, ..., n\}$ — множество студентов группы №1.
- $\mathcal{S}$ — множество действительных чисел в диапазоне от 36.6 до 41.
- Каждый участник i из $\mathcal{P}$ обладает некоторым секретом $s_i \in \mathcal{S}$. Секрет – это температура тела.

Пример 1

- $\mathcal{P} = \{1, ..., n\}$ — множество студентов группы №1.
- $\mathcal{S}$ — множество действительных чисел в диапазоне от 36.6 до 41.
- Каждый участник i из $\mathcal{P}$ обладает некоторым секретом $s_i \in \mathcal{S}$. Секрет – это температура тела.
- $f(x_1, ..., x_n) = \frac{\sum_{i=1}^{n} s_i}{n}$ — средняя температура тела.

Пример 2

- $\mathcal{P} = \{1, 2\}$ — Алиса (1) и Боб (2).

Пример 2

- $\mathcal{P} = \{1, 2\}$ — Алиса (1) и Боб (2).
- $\mathcal{S} = \{0, 1\}$.

Пример 2

- $\mathcal{P} = \{1, 2\}$ — Алиса (1) и Боб (2).
- $\mathcal{S} = \{0, 1\}$.
- Каждый участник i из $\mathcal{P}$ обладает некоторым секретом $s_i \in \mathcal{S}$.

Пример 2

- $\mathcal{P} = \{1, 2\}$ — Алиса (1) и Боб (2).
- $\mathcal{S} = \{0, 1\}$.
- Каждый участник i из $\mathcal{P}$ обладает некоторым секретом $s_i \in \mathcal{S}$.
  - $s_i = 1$ означает, что участник i хотел бы пойти на свидание с участником $\{1, 2\} \backslash \{i\}$;

Пример 2

- $\mathcal{P} = \{1, 2\}$ — Алиса (1) и Боб (2).
- $\mathcal{S} = \{0, 1\}$.
- Каждый участник i из $\mathcal{P}$ обладает некоторым секретом $s_i \in \mathcal{S}$.
  - $s_i = 1$ означает, что участник i хотел бы пойти на свидание с участником $\{1, 2\} \backslash \{i\}$;
  - $s_i = 0$ — участник i не хотел бы этого делать.

Пример 2

- $\mathcal{P} = \{1, 2\}$ — Алиса (1) и Боб (2).
- $\mathcal{S} = \{0, 1\}$.
- Каждый участник i из $\mathcal{P}$ обладает некоторым секретом $s_i \in \mathcal{S}$.
  - $s_i = 1$ означает, что участник i хотел бы пойти на свидание с участником $\{1, 2\} \backslash \{i\}$;
  - $s_i = 0$ — участник i не хотел бы этого делать.
- $f(x_1, x_2) = s_1 \cdot s_2$:

Пример 2

- $\mathcal{P} = \{1, 2\}$ — Алиса (1) и Боб (2).
- $\mathcal{S} = \{0, 1\}$.
- Каждый участник i из $\mathcal{P}$ обладает некоторым секретом $s_i \in \mathcal{S}$.
  - $s_i = 1$ означает, что участник i хотел бы пойти на свидание с участником $\{1, 2\} \backslash \{i\}$;
  - $s_i = 0$ — участник i не хотел бы этого делать.
- $f(x_1, x_2) = s_1 \cdot s_2$:
  - $f(x_1, x_2) = 1$ — оба участника хотели бы пойти друг с другом на свидание;

Пример 2

- $\mathcal{P} = \{1, 2\}$ — Алиса (1) и Боб (2).
- $\mathcal{S} = \{0, 1\}$.
- Каждый участник i из $\mathcal{P}$ обладает некоторым секретом $s_i \in \mathcal{S}$.
  - $s_i = 1$ означает, что участник i хотел бы пойти на свидание с участником $\{1, 2\} \backslash \{i\}$;
  - $s_i = 0$ — участник i не хотел бы этого делать.
- $f(x_1, x_2) = s_1 \cdot s_2$:
  - $f(x_1, x_2) = 1$ — оба участника хотели бы пойти друг с другом на свидание;
  - $f(x_1, x_2) = 0$ — кто-то (или оба) не хотели бы пойти друг с другом на свидание.

Как можно вычислить функции из примеров 1 и 2?

Как можно вычислить функции из примеров 1 и 2?

Вариант №1:

Как можно вычислить функции из примеров 1 и 2?

Вариант №1:

- Каждый участник отправляет всем свой секрет (по открытым или защищенным каналам).

Как можно вычислить функции из примеров 1 и 2?

Вариант №1:

- Каждый участник отправляет всем свой секрет (по открытым или защищенным каналам).
- После обмена все располагают необходимыми для вычисления аргументами.

Как можно вычислить функции из примеров 1 и 2?

Вариант №1:

- Каждый участник отправляет всем свой секрет (по открытым или защищенным каналам).
- После обмена все располагают необходимыми для вычисления аргументами.
- Каждый участник вычисляет самостоятельно значение функции $f(x_1, ..., x_n)$.

Как можно вычислить функции из примеров 1 и 2?

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №1:

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №1:

- Простота реализации.

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №1:

- Простота реализации.

Недостатки Варианта №1:

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №1:

- Простота реализации.

Недостатки Варианта №1:

- Все участники узнают секреты других участников.

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №1:

- Простота реализации.

Недостатки Варианта №1:

- Все участники узнают секреты других участников.
  - В случае с вычислением средней температуры каждый узнает температуру другого участника, т.е. узнает персональные данные другого участника (здесь могут быть проблемы с соблюдением **ФЗ-152 «О персональных данных»**).

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №1:

- Простота реализации.

Недостатки Варианта №1:

- Все участники узнают секреты других участников.
  - В случае с вычислением средней температуры каждый узнает температуру другого участника, т.е. узнает персональные данные другого участника (здесь могут быть проблемы с соблюдением **ФЗ-152 «О персональных данных»**).
  - В примере со свиданием все еще хуже.

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №1:

- Простота реализации.

Недостатки Варианта №1:

- Все участники узнают секреты других участников.
  - В случае с вычислением средней температуры каждый узнает температуру другого участника, т.е. узнает персональные данные другого участника (здесь могут быть проблемы с соблюдением **ФЗ-152 «О персональных данных»**).
  - В примере со свиданием все еще хуже.
    - Когда оба значения s_1 и s_2 равны 1, то все довольны.

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №1:

- Простота реализации.

Недостатки Варианта №1:

- Все участники узнают секреты других участников.
  - В случае с вычислением средней температуры каждый узнает температуру другого участника, т.е. узнает персональные данные другого участника (здесь могут быть проблемы с соблюдением **ФЗ-152 «О персональных данных»**).
  - В примере со свиданием все еще хуже.
    - Когда оба значения s_1 и s_2 равны 1, то все довольны.
    - Когда оба значения s_1 и s_2 равны 0, то также все не очень плохо: никто не хочет идти на свидание.

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №1:

- Простота реализации.

Недостатки Варианта №1:

- Все участники узнают секреты других участников.
  - В случае с вычислением средней температуры каждый узнает температуру другого участника, т.е. узнает персональные данные другого участника (здесь могут быть проблемы с соблюдением **ФЗ-152 «О персональных данных»**).
  - В примере со свиданием все еще хуже.
    - Когда оба значения s_1 и s_2 равны 1, то все довольны.
    - Когда оба значения s_1 и s_2 равны 0, то также все не очень плохо: никто не хочет идти на свидание.
    - Если $s_1 != s_2$, то тому участнику, у которого значение равно 1, такой исход может не понравиться.

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №1:

- Простота реализации.

Недостатки Варианта №1:

- Все участники узнают секреты других участников.
  - В случае с вычислением средней температуры каждый узнает температуру другого участника, т.е. узнает персональные данные другого участника (здесь могут быть проблемы с соблюдением **ФЗ-152 «О персональных данных»**).
  - В примере со свиданием все еще хуже.
    - Когда оба значения s_1 и s_2 равны 1, то все довольны.
    - Когда оба значения s_1 и s_2 равны 0, то также все не очень плохо: никто не хочет идти на свидание.
    - Если $s_1 != s_2$, то тому участнику, у которого значение равно 1, такой исход может не понравиться.

Как можно вычислить функции из примеров 1 и 2?

Поэтому нужен протокол вычисления функции **без обмена самими секретами**.

Как можно вычислить функции из примеров 1 и 2?

Поэтому нужен протокол вычисления функции **без обмена самими секретами**.

Вариант №2:

Как можно вычислить функции из примеров 1 и 2?

Поэтому нужен протокол вычисления функции **без обмена самими секретами**.

Вариант №2:

- Предполагается наличие «суперзащищенного» сервера, с которым у каждого участника есть «суперзащищенный» канал. Такой сервер назовем Оракулом.

Как можно вычислить функции из примеров 1 и 2?

Поэтому нужен протокол вычисления функции **без обмена самими секретами**.

Вариант №2:

- Предполагается наличие «суперзащищенного» сервера, с которым у каждого участника есть «суперзащищенный» канал. Такой сервер назовем Оракулом.
- Каждый участник отправляет Оракулу свой секрет s_i по «суперзащищенному» каналу.

Как можно вычислить функции из примеров 1 и 2?

Поэтому нужен протокол вычисления функции **без обмена самими секретами**.

Вариант №2:

- Предполагается наличие «суперзащищенного» сервера, с которым у каждого участника есть «суперзащищенный» канал. Такой сервер назовем Оракулом.
- Каждый участник отправляет Оракулу свой секрет s_i по «суперзащищенному» каналу.
- Оракул вычисляет $f(x_1, ..., x_n)$ и по широковещательному каналу отправляет вычисленное значение всем участникам.

Как можно вычислить функции из примеров 1 и 2?

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №2:

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №2:

- Участники не обмениваются сообщениями друг с другом.

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №2:

- Участники не обмениваются сообщениями друг с другом.

Недостатки Варианта №2:

Как можно вычислить функции из примеров 1 и 2?

Достоинства Варианта №2:

- Участники не обмениваются сообщениями друг с другом.

Недостатки Варианта №2:

- Схема неосуществимая, так как не существует «суперзащищенных» серверов (и которым можно было бы безгранично доверять).

Одно замечание относительно Варианта 2

Одно замечание относительно Варианта 2

- Из того, что участники друг с другом не взаимодействуют, не следует, что они не получают какой-либо информации о значениях секрета других участников.

Одно замечание относительно Варианта 2

- Из того, что участники друг с другом не взаимодействуют, не следует, что они не получают какой-либо информации о значениях секрета других участников.
- Например, в примере со свиданиями, из значения $f(x_1, x_2) = 1$ каждый участник в точности узнает значение другого участника.

Одно замечание относительно Варианта 2

- Из того, что участники друг с другом не взаимодействуют, не следует, что они не получают какой-либо информации о значениях секрета других участников.
- Например, в примере со свиданиями, из значения $f(x_1, x_2) = 1$ каждый участник в точности узнает значение другого участника.
- В общем случае, построить такой протокол, чтобы после вычисления функции $f(x_1, ..., x_n)$ каждый участник не получал **никакой информации** о значениях секретов других участников, **невозможно**.

Требования к протоколу защищенных многосторонних вычислений

Требования к протоколу защищенных многосторонних вычислений

- Протокол должен вычислять функцию $f(x_1, ..., x_n)$;

Требования к протоколу защищенных многосторонних вычислений

- Протокол должен вычислять функцию $f(x_1, ..., x_n)$;
- Протокол должен быть реализуемым: на основе обмена сообщениями между участниками (без Оракула);

Требования к протоколу защищенных многосторонних вычислений

- Протокол должен вычислять функцию $f(x_1, ..., x_n)$;
- Протокол должен быть реализуемым: на основе обмена сообщениями между участниками (без Оракула);
- После вычисления $f(x_1, ..., x_n)$ участники не должны получать больше информации о секретах других участников, чем в случае вычислениея этой функции с помощью Оракула.

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Нам понадобится схема разделения секрета (СРС) Ω для трех участников;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Нам понадобится схема разделения секрета (СРС) Ω для трех участников;

- Пусть $\mathcal{P} = \{1, 2, 3\}$, $\mathcal{S} = \mathbb{Z}_m = \{0, ..., m-1\}$, $s \in \mathcal{S}$; m выбирается таким, чтобы сумма всегда была меньше m;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Нам понадобится схема разделения секрета (СРС) Ω для трех участников;

- Пусть $\mathcal{P} = \{1, 2, 3\}$, $\mathcal{S} = \mathbb{Z}_m = \{0, ..., m-1\}$, $s \in \mathcal{S}$; m выбирается таким, чтобы сумма всегда была меньше m;
  - $\textsc{Share}_\Omega$: $x_1, x_2 \in_R \mathbb{Z}_m$, $x_3 = s - (x_1 + x_2) (\mathrm{mod}\, m)$;
  - $\textsc{Recon}_\Omega$: $s = x_1 + x_2 + x_3 (\mathrm{mod}\, m)$.

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Нам понадобится схема разделения секрета (СРС) Ω для трех участников;

- Пусть $\mathcal{P} = \{1, 2, 3\}$, $\mathcal{S} = \mathbb{Z}_m = \{0, ..., m-1\}$, $s \in \mathcal{S}$; m выбирается таким, чтобы сумма всегда была меньше m;
  - $\textsc{Share}_\Omega$: $x_1, x_2 \in_R \mathbb{Z}_m$, $x_3 = s - (x_1 + x_2) (\mathrm{mod}\, m)$;
  - $\textsc{Recon}_\Omega$: $s = x_1 + x_2 + x_3 (\mathrm{mod}\, m)$.
- Будем писать для удобства так:
  - $\textsc{Share}_\Omega(s) = (x_1, x_2, x_2)$;
  - $\textsc{Recon}_\Omega(x_1, x_2, x_3) = s$.

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Сначала участники **независимо** друг от друга разделяют свои секреты на доли:

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Сначала участники **независимо** друг от друга разделяют свои секреты на доли:

Участник 1 (он владеет секретом s_1):

- $\textsc{Share}_\Omega(s_1) = (x_{11}, x_{12}, x_{13})$;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Сначала участники **независимо** друг от друга разделяют свои секреты на доли:

Участник 1 (он владеет секретом s_1):

- $\textsc{Share}_\Omega(s_1) = (x_{11}, x_{12}, x_{13})$;

Участник 2 (он владеет секретом s_2):

- $\textsc{Share}_\Omega(s_2) = (x_{21}, x_{22}, x_{23})$;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Сначала участники **независимо** друг от друга разделяют свои секреты на доли:

Участник 1 (он владеет секретом s_1):

- $\textsc{Share}_\Omega(s_1) = (x_{11}, x_{12}, x_{13})$;

Участник 2 (он владеет секретом s_2):

- $\textsc{Share}_\Omega(s_2) = (x_{21}, x_{22}, x_{23})$;

Участник 3 (он владеет секретом s_3):

- $\textsc{Share}_\Omega(s_3) = (x_{31}, x_{32}, x_{33})$;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Сначала участники **независимо** друг от друга разделяют свои секреты на доли:

Участник 1 (он владеет секретом s_1):

- $\textsc{Share}_\Omega(s_1) = (x_{11}, x_{12}, x_{13})$;

Участник 2 (он владеет секретом s_2):

- $\textsc{Share}_\Omega(s_2) = (x_{21}, x_{22}, x_{23})$;

Участник 3 (он владеет секретом s_3):

- $\textsc{Share}_\Omega(s_3) = (x_{31}, x_{32}, x_{33})$;

Не очень сложно заменить, что

$$\sum_{i}^{3} \sum_{j=1}^{3} x_{i,j} = \sum_{i}^{3} s_i = f(s_1, s_2, s_3).$$

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Сначала участники **независимо** друг от друга разделяют свои секреты на доли:

Участник 1 (он владеет секретом s_1):

- $\textsc{Share}_\Omega(s_1) = (x_{11}, x_{12}, x_{13})$;

Участник 2 (он владеет секретом s_2):

- $\textsc{Share}_\Omega(s_2) = (x_{21}, x_{22}, x_{23})$;

Участник 3 (он владеет секретом s_3):

- $\textsc{Share}_\Omega(s_3) = (x_{31}, x_{32}, x_{33})$;

Не очень сложно заменить, что

$$\sum_{i}^{3}\sum_{j=1}^{3} x_{i,j} = \sum_{i}^{3} s_i = f(s_1, s_2, s_3).$$

Остается **специальным** образом обменяться долями.

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:
  - $1 \to 2 : x_{1,1}, x_{1,3}$;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:
  - $1 \to 2 : x_{1,1}, x_{1,3}$;
  - $1 \to 3 :$

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:
  - $1 \to 2 : x_{1,1}, x_{1,3}$;
  - $1 \to 3 : x_{1,1}, x_{1,2}$;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:
  - $1 \to 2 : x_{1,1}, x_{1,3}$;
  - $1 \to 3 : x_{1,1}, x_{1,2}$;
- Передачи участника 2:

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:
  - $1 \to 2 : x_{1,1}, x_{1,3}$;
  - $1 \to 3 : x_{1,1}, x_{1,2}$;
- Передачи участника 2:
  - $2 \to 1 : x_{2,2}, x_{2,3}$;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:
  - $1 \to 2 : x_{1,1}, x_{1,3}$;
  - $1 \to 3 : x_{1,1}, x_{1,2}$;
- Передачи участника 2:
  - $2 \to 1 : x_{2,2}, x_{2,3}$;
  - $2 \to 3 : x_{2,1}, x_{2,2}$;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:
  - $1 \to 2 : x_{1,1}, x_{1,3}$;
  - $1 \to 3 : x_{1,1}, x_{1,2}$;
- Передачи участника 2:
  - $2 \to 1 : x_{2,2}, x_{2,3}$;
  - $2 \to 3 : x_{2,1}, x_{2,2}$;
- Передачи участника 3:

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:
  - $1 \to 2 : x_{1,1}, x_{1,3}$;
  - $1 \to 3 : x_{1,1}, x_{1,2}$;
- Передачи участника 2:
  - $2 \to 1 : x_{2,2}, x_{2,3}$;
  - $2 \to 3 : x_{2,1}, x_{2,2}$;
- Передачи участника 3:
  - $3 \to 1 : x_{3,2}, x_{3,3}$;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:
  - $1 \to 2 : x_{1,1}, x_{1,3}$;
  - $1 \to 3 : x_{1,1}, x_{1,2}$;
- Передачи участника 2:
  - $2 \to 1 : x_{2,2}, x_{2,3}$;
  - $2 \to 3 : x_{2,1}, x_{2,2}$;
- Передачи участника 3:
  - $3 \to 1 : x_{3,2}, x_{3,3}$;
  - $3 \to 2 : x_{3,1}, x_{3,3}$;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Правило обмена

Участник i передает **по защищенному каналу** участнику j доли $x_{i,l}$, где $l \neq j$.

- Передачи участника 1:
  - $1 \to 2 : x_{1,1}, x_{1,3}$;
  - $1 \to 3 : x_{1,1}, x_{1,2}$;
- Передачи участника 2:
  - $2 \to 1 : x_{2,2}, x_{2,3}$;
  - $2 \to 3 : x_{2,1}, x_{2,2}$;
- Передачи участника 3:
  - $3 \to 1 : x_{3,2}, x_{3,3}$;
  - $3 \to 2 : x_{3,1}, x_{3,3}$;

	Доли s_1	Доли s_2	Доли s_3
1	$x_{1,1}$ $x_{1,2}$ $x_{1,3}$	? $x_{2,2}$ $x_{2,3}$	? $x_{3,2}$ $x_{3,3}$
2	$x_{1,1}$? $x_{1,3}$	$x_{2,1}$ $x_{2,2}$ $x_{2,3}$	$x_{3,1}$? $x_{3,3}$
3	$x_{1,1}$ $x_{1,2}$?	$x_{2,1}$ $x_{2,2}$?	$x_{3,1}$ $x_{3,2}$ $x_{3,3}$

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

	Доли s_1	Доли s_2	Доли s_3
1	$x_{1,1}$	?	?
	$x_{1,2}$	$x_{2,2}$	$x_{3,2}$
	$x_{1,3}$	$x_{2,3}$	$x_{3,3}$
2	$x_{1,1}$	$x_{2,1}$	$x_{3,1}$
	?	$x_{2,2}$	?
	$x_{1,3}$	$x_{2,3}$	$x_{3,3}$
3	$x_{1,1}$	$x_{2,1}$	$x_{3,1}$
	$x_{1,2}$	$x_{2,2}$	$x_{3,2}$
	?	?	$x_{3,3}$

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

	Доли s_1	Доли s_2	Доли s_3
1	$x_{1,1}$ $x_{1,2}$ $x_{1,3}$	? $x_{2,2}$ $x_{2,3}$	? $x_{3,2}$ $x_{3,3}$
2	$x_{1,1}$? $x_{1,3}$	$x_{2,1}$ $x_{2,2}$ $x_{2,3}$	$x_{3,1}$? $x_{3,3}$
3	$x_{1,1}$ $x_{1,2}$?	$x_{2,1}$ $x_{2,2}$?	$x_{3,1}$ $x_{3,2}$ $x_{3,3}$

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

	Доли s_1	Доли s_2	Доли s_3
1	$x_{1,1}$ $x_{1,2}$ $x_{1,3}$	? $x_{2,2}$ $x_{2,3}$	? $x_{3,2}$ $x_{3,3}$
2	$x_{1,1}$? $x_{1,3}$	$x_{2,1}$ $x_{2,2}$ $x_{2,3}$	$x_{3,1}$? $x_{3,3}$
3	$x_{1,1}$ $x_{1,2}$?	$x_{2,1}$ $x_{2,2}$?	$x_{3,1}$ $x_{3,2}$ $x_{3,3}$

Участник 1:

$$S_2 = x_{1,2} + x_{2,2} + x_{3,2},$$

$$S_3 = x_{1,3} + x_{2,3} + x_{3,3}$$

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

	Доли s_1	Доли s_2	Доли s_3
1	$x_{1,1}$ $x_{1,2}$ $x_{1,3}$	? $x_{2,2}$ $x_{2,3}$	? $x_{3,2}$ $x_{3,3}$
2	$x_{1,1}$? $x_{1,3}$	$x_{2,1}$ $x_{2,2}$ $x_{2,3}$	$x_{3,1}$? $x_{3,3}$
3	$x_{1,1}$ $x_{1,2}$?	$x_{2,1}$ $x_{2,2}$?	$x_{3,1}$ $x_{3,2}$ $x_{3,3}$

Участник 1:

$$S_2 = x_{1,2} + x_{2,2} + x_{3,2},$$

$$S_3 = x_{1,3} + x_{2,3} + x_{3,3}$$

Участник 2:

$$S_1 = x_{1,1} + x_{2,1} + x_{3,1},$$

$$S_3 = x_{1,3} + x_{2,3} + x_{3,3}$$

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

	Доли s_1	Доли s_2	Доли s_3
1	$x_{1,1}$ $x_{1,2}$ $x_{1,3}$	? $x_{2,2}$ $x_{2,3}$	? $x_{3,2}$ $x_{3,3}$
2	$x_{1,1}$? $x_{1,3}$	$x_{2,1}$ $x_{2,2}$ $x_{2,3}$	$x_{3,1}$? $x_{3,3}$
3	$x_{1,1}$ $x_{1,2}$?	$x_{2,1}$ $x_{2,2}$?	$x_{3,1}$ $x_{3,2}$ $x_{3,3}$

Участник 1:

$$S_2 = x_{1,2} + x_{2,2} + x_{3,2},$$

$$S_3 = x_{1,3} + x_{2,3} + x_{3,3}$$

Участник 2:

$$S_1 = x_{1,1} + x_{2,1} + x_{3,1},$$

$$S_3 = x_{1,3} + x_{2,3} + x_{3,3}$$

Участник 3:

$$S_1 = x_{1,1} + x_{2,1} + x_{3,1},$$

$$S_2 = x_{1,2} + x_{2,2} + x_{3,2}$$

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

- Все участник и публикуют вычисленные значения S_i.

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

- Все участник и публикуют вычисленные значения S_i.
- Для вычисления $f(s_1, s_2, s_3)$ каждый участник вычисляет $S_1 + S_2 + S_3$.

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

- Все участник и публикуют вычисленные значения S_i.
- Для вычисления $f(s_1, s_2, s_3)$ каждый участник вычисляет $S_1 + S_2 + S_3$.

Итоговый протокол (схема):

1. Выполнение протокола SHARE_Ω каждым участником;
2. Обмен долями $x_{i,l}$ по **защищенным каналам**;
3. Обмен значениями S_i по **открытым каналам**.

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Обоснование «защищенности» (схема):

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Обоснование «защищенности» (схема):

- После второго шага ни один участник не получает новой информации о секретах других участников;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Обоснование «защищенности» (схема):

- После второго шага ни один участник не получает новой информации о секретах других участников;
- После шага 3, например, первый участник узнает S_1;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Обоснование «защищенности» (схема):

- После второго шага ни один участник не получает новой информации о секретах других участников;
- После шага 3, например, первый участник узнает S_1;
- Но это значение первый участник может найти, зная значение $f(y_1, y_2, y_3)$ и два своих значения S_2 и S_3;

Протокол многостороннего суммирования для **трех участников**: $f(y_1, y_2, y_3) = \sum_{i=1}^{3} y_i$.

Обоснование «защищенности» (схема):

- После второго шага ни один участник не получает новой информации о секретах других участников;
- После шага 3, например, первый участник узнает S_1;
- Но это значение первый участник может найти, зная значение $f(y_1, y_2, y_3)$ и два своих значения S_2 и S_3;
- Поэтому «лишней» информации первый участник не узнает на третьем шаге.

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Для построения такого протокола воспользуемся примитивным криптографическим протоколом забывчивой передачи (oblivious transfer).

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Для построения такого протокола воспользуемся примитивным криптографическим протоколом забывчивой передачи (oblivious transfer).
  - Отправитель S имеет два секрета: $x_0, x_1 \in \{0, 1\}$;

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Для построения такого протокола воспользуемся примитивным криптографическим протоколом забывчивой передачи (oblivious transfer).
  - Отправитель S имеет два секрета: $x_0, x_1 \in \{0, 1\}$;
  - Получатель R желает получить секрет с номером $s \in \{0, 1\}$, т.е. секрет x_s (само значение секрета получателю априори неизвестно);

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Для построения такого протокола воспользуемся примитивным криптографическим протоколом забывчивой передачи (oblivious transfer).
  - Отправитель S имеет два секрета: $x_0, x_1 \in \{0, 1\}$;
  - Получатель R желает получить секрет с номером $s \in \{0, 1\}$, т.е. секрет x_s (само значение секрета получателю априори неизвестно);
  - Отправитель не должен знать, секрет с каким номером был запрошен;

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Для построения такого протокола воспользуемся примитивным криптографическим протоколом забывчивой передачи (oblivious transfer).
  - Отправитель S имеет два секрета: $x_0, x_1 \in \{0, 1\}$;
  - Получатель R желает получить секрет с номером $s \in \{0, 1\}$, т.е. секрет x_s (само значение секрета получателю априори неизвестно);
  - Отправитель не должен знать, секрет с каким номером был запрошен;
  - Получатель должен узнать значение секрета x_s, но не должен узнать значение секрета x_{1-s}.

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Для построения такого протокола воспользуемся примитивным криптографическим протоколом забывчивой передачи (oblivious transfer).
  - Отправитель S имеет два секрета: $x_0, x_1 \in \{0, 1\}$;
  - Получатель R желает получить секрет с номером $s \in \{0, 1\}$, т.е. секрет x_s (само значение секрета получателю априори неизвестно);
  - Отправитель не должен знать, секрет с каким номером был запрошен;
  - Получатель должен узнать значение секрета x_s, но не должен узнать значение секрета x_{1-s}.
  - Такой протокол обозначим $\mathrm{OT} - \binom{2}{1}$.

Реализация протокола OT $-\binom{2}{1}$

Реализация протокола OT_1^2

- Пусть $\langle g \rangle$ — циклическая группа, порождаемая g,

Реализация протокола OT_1^2

- Пусть $\langle g \rangle$ — циклическая группа, порождаемая g,
- h – общеизвестный элемент группы $\langle g \rangle$, однако значение $\log_g h$ ни одному из участников не известно,

Реализация протокола OT_1^2

- Пусть $\langle g \rangle$ — циклическая группа, порождаемая g,
- h – общеизвестный элемент группы $\langle g \rangle$, однако значение $\log_g h$ ни одному из участников не известно,
- $|\langle g \rangle| = n$ — простое число.

Реализация протокола OT $-\binom{2}{1}$

Реализация протокола OT_1^2

- Получатель R выбирает $s \in \{0, 1\}$ (номер секрета, который он желает получить от S) и случайно выбирает число $u (\in \mathbb{Z}_n)$;

Реализация протокола OT_1^2

- Получатель R выбирает $s \in \{0, 1\}$ (номер секрета, который он желает получить от S) и случайно выбирает число $u (\in \mathbb{Z}_n)$;
- Получатель R вычисляет два числа: $h_s = g^u, \quad h_{1-s} = \frac{h}{g^u}$

Реализация протокола OT_1^2

- Получатель R выбирает $s \in \{0, 1\}$ (номер секрета, который он желает получить от S) и случайно выбирает число $u (\in \mathbb{Z}_n)$;
- Получатель R вычисляет два числа: $h_s = g^u, \quad h_{1-s} = \frac{h}{g^u}$
- $R \to S : h_0, h_1$ (если $s = 0$, то $h_0 = g^u, h_1 = \frac{h}{g^u}$; если $s = 1$, то $h_0 = \frac{h}{g^u}, h_1 = g^u$;)

Реализация протокола OT_1^2

- Получатель R выбирает $s \in \{0,1\}$ (номер секрета, который он желает получить от S) и случайно выбирает число $u (\in \mathbb{Z}_n)$;
- Получатель R вычисляет два числа: $h_s = g^u, \quad h_{1-s} = \frac{h}{g^u}$
- $R \to S : h_0, h_1$ (если $s = 0$, то $h_0 = g^u, h_1 = \frac{h}{g^u}$; если $s = 1$, то $h_0 = \frac{h}{g^u}, h_1 = g^u$;)
- Отправитель передает R две пары чисел:

$$(A_0, B_0) = (g^{u_0}, h_0^{u_0} g^{x_0}), u_0 \in_R \mathbb{Z}_n$$
$$(A_1, B_1) = (g^{u_1}, h_1^{u_1} g^{x_1}), u_1 \in_R \mathbb{Z}_n.$$

Реализация протокола OT_1^2

- Получатель R выбирает $s \in \{0, 1\}$ (номер секрета, который он желает получить от S) и случайно выбирает число $u (\in \mathbb{Z}_n)$;
- Получатель R вычисляет два числа: $h_s = g^u, \quad h_{1-s} = \frac{h}{g^u}$
- $R \to S : h_0, h_1$ (если $s = 0$, то $h_0 = g^u, h_1 = \frac{h}{g^u}$; если $s = 1$, то $h_0 = \frac{h}{g^u}, h_1 = g^u$;)
- Отправитель передает R две пары чисел:

$$(A_0, B_0) = (g^{u_0}, h_0^{u_0} g^{x_0}), u_0 \in_R \mathbb{Z}_n$$
$$(A_1, B_1) = (g^{u_1}, h_1^{u_1} g^{x_1}), u_1 \in_R \mathbb{Z}_n.$$

- Получатель выбирает пару, соответствующую номеру s, и вычисляет

$$x_s = \log_g \left(B_s A_s^{-u} \right).$$

Реализация протокола OT_1^2

- Получатель R выбирает $s \in \{0,1\}$ (номер секрета, который он желает получить от S) и случайно выбирает число $u (\in \mathbb{Z}_n)$;
- Получатель R вычисляет два числа: $h_s = g^u, \quad h_{1-s} = \frac{h}{g^u}$
- $R \to S : h_0, h_1$ (если $s = 0$, то $h_0 = g^u, h_1 = \frac{h}{g^u}$; если $s = 1$, то $h_0 = \frac{h}{g^u}, h_1 = g^u$;)
- Отправитель передает R две пары чисел:

$$(A_0, B_0) = (g^{u_0}, h_0^{u_0} g^{x_0}), u_0 \in_R \mathbb{Z}_n$$
$$(A_1, B_1) = (g^{u_1}, h_1^{u_1} g^{x_1}), u_1 \in_R \mathbb{Z}_n.$$

- Получатель выбирает пару, соответствующую номеру s, и вычисляет

$$x_s = \log_g \left(B_s A_s^{-u} \right).$$

- Введем обозначение: $\mathrm{OT}(x_0, x_1; s) = x_s$.

Реализация протокола OT_1^2

- Получатель R выбирает $s \in \{0,1\}$ (номер секрета, который он желает получить от S) и случайно выбирает число $u (\in \mathbb{Z}_n)$;
- Получатель R вычисляет два числа: $h_s = g^u, \quad h_{1-s} = \frac{h}{g^u}$
- $R \to S$: h_0, h_1 (если $s = 0$, то $h_0 = g^u, h_1 = \frac{h}{g^u}$; если $s = 1$, то $h_0 = \frac{h}{g^u}, h_1 = g^u$;)
- Отправитель передает R две пары чисел:

$$(A_0, B_0) = (g^{u_0}, h_0^{u_0} g^{x_0}), u_0 \in_R \mathbb{Z}_n$$
$$(A_1, B_1) = (g^{u_1}, h_1^{u_1} g^{x_1}), u_1 \in_R \mathbb{Z}_n.$$

- Получатель выбирает пару, соответствующую номеру s, и вычисляет

$$x_s = \log_g \left(B_s A_s^{-u} \right).$$

- Введем обозначение: $\mathrm{OT}(x_0, x_1; s) = x_s$.
- Заметим, что $\mathrm{OT}(x_0, x_1; s) = x_s = x_0(1-s) \oplus x_1 s$.

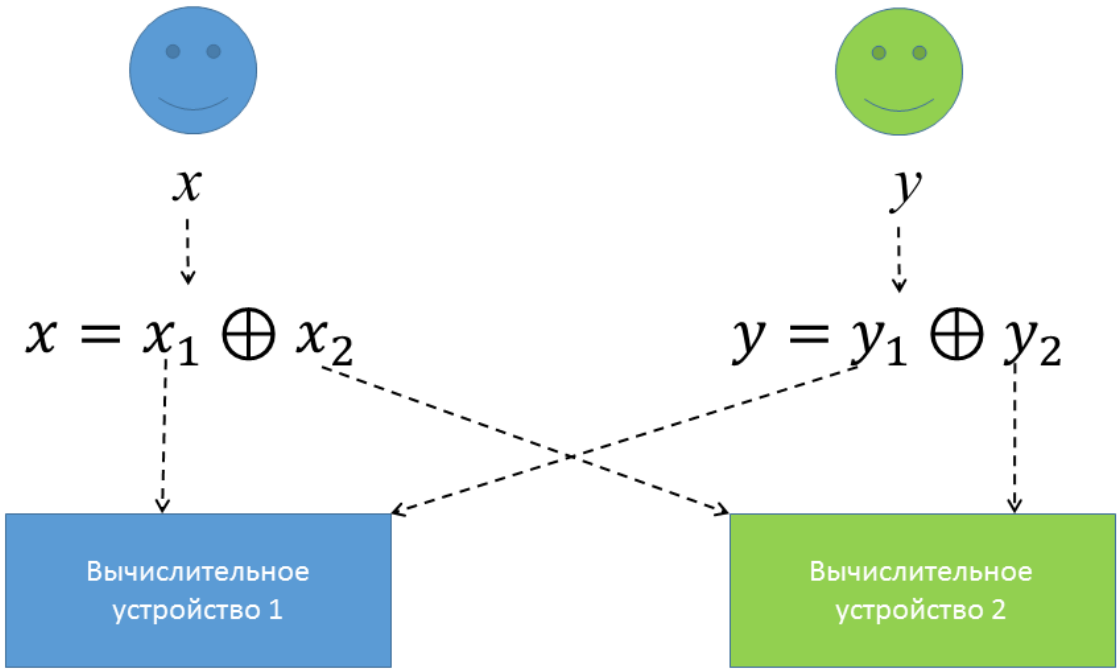
Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

x

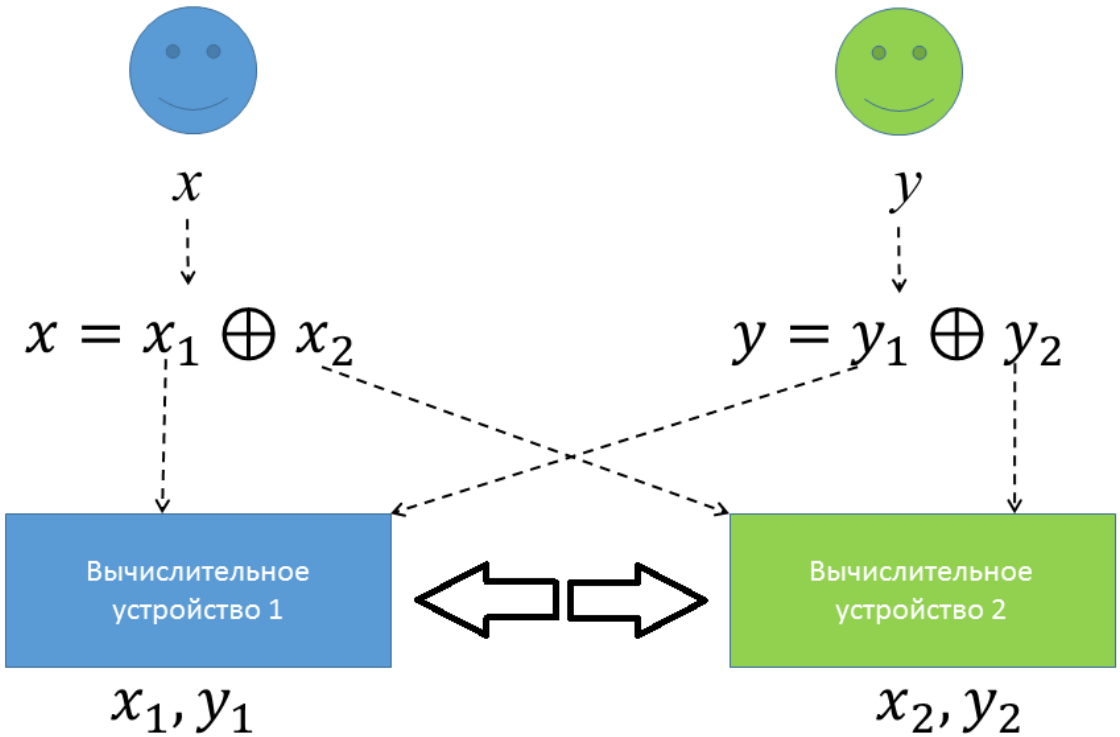
y

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.



Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.



Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участник 1 выбирает случайно число $u_1 (\in \{0, 1\})$; участник 2 выбирает случайно число $u_2 (\in \{0, 1\})$;

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участник 1 выбирает случайно число $u_1 (\in \{0, 1\})$; участник 2 выбирает случайно число $u_2 (\in \{0, 1\})$;
- Участники 1 и 2 выполняют протокол $\mathrm{OT} - \binom{2}{1}$:

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участник 1 выбирает случайно число $u_1 (\in \{0, 1\})$; участник 2 выбирает случайно число $u_2 (\in \{0, 1\})$;
- Участники 1 и 2 выполняют протокол $\mathrm{OT} - \binom{2}{1}$:
  - Участник 2 выполняет роль отправителя (S) и он обладает двумя секретами: u_2 и $x_2 \oplus u_2$;

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участник 1 выбирает случайно число $u_1 (\in \{0, 1\})$; участник 2 выбирает случайно число $u_2 (\in \{0, 1\})$;
- Участники 1 и 2 выполняют протокол $\mathrm{OT} - \binom{2}{1}$:
  - Участник 2 выполняет роль отправителя (S) и он обладает двумя секретами: u_2 и $x_2 \oplus u_2$;
  - Участник 1 выполняет роль получателя (R) и он желает получить секрет с номером y_1;

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участник 1 выбирает случайно число $u_1 (\in \{0, 1\})$; участник 2 выбирает случайно число $u_2 (\in \{0, 1\})$;
- Участники 1 и 2 выполняют протокол $\mathrm{OT} - \binom{2}{1}$:
  - Участник 2 выполняет роль отправителя (S) и он обладает двумя секретами: u_2 и $x_2 \oplus u_2$;
  - Участник 1 выполняет роль получателя (R) и он желает получить секрет с номером y_1;
  - В результате Участник 1 получает $OT(u_2, x_2 \oplus u_2; y_1) = u_2(1 - y_1) \oplus (x_2 \oplus u_2)y_1 = u_2 \oplus x_2 y_1$.

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участники 1 и 2 меняются ролями и снова выполняют протокол OT_1^2:

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участники 1 и 2 меняются ролями и снова выполняют протокол OT_1^2:
  - Участник 1 выполняет роль отправителя (S) и он обладает двумя секретами: u_1 и $x_1 \oplus u_1$;

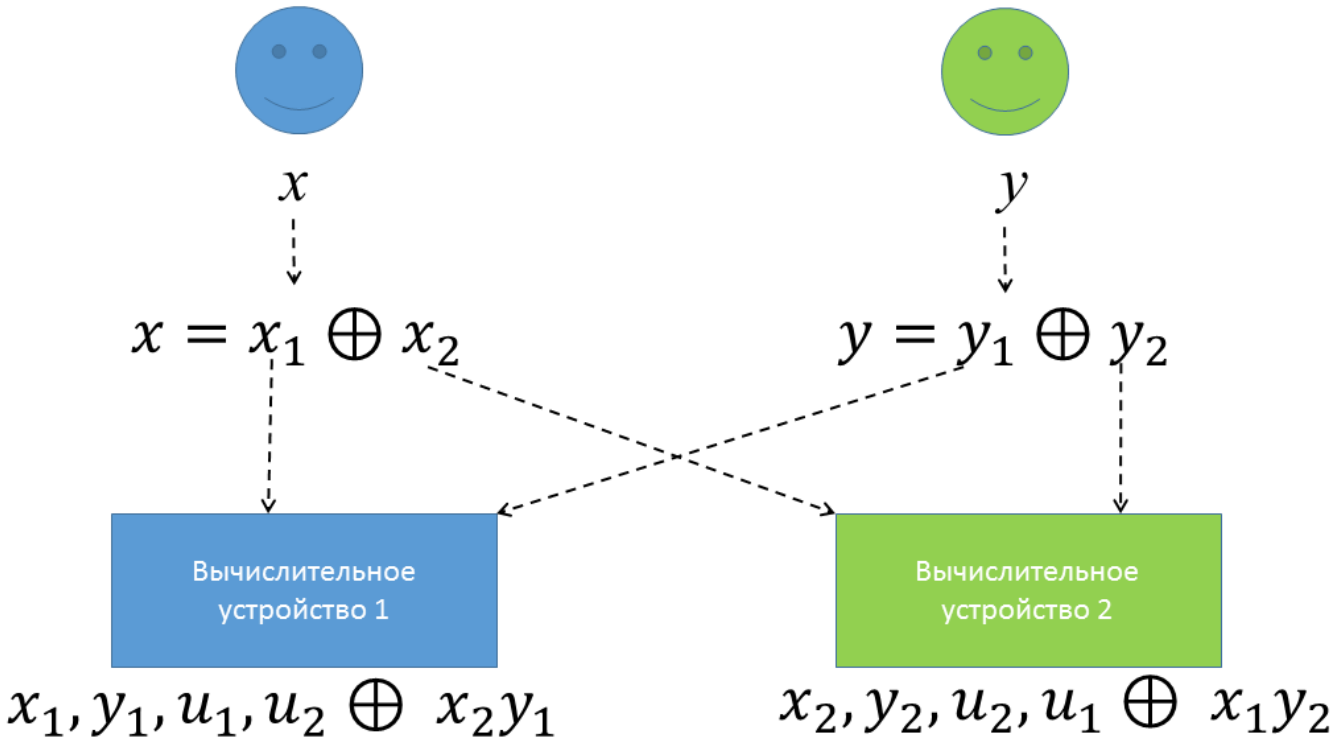
Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участники 1 и 2 меняются ролями и снова выполняют протокол OT_1^2:
  - Участник 1 выполняет роль отправителя (S) и он обладает двумя секретами: u_1 и $x_1 \oplus u_1$;
  - Участник 2 выполняет роль получателя (R) и он желает получить секрет с номером y_2;

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участники 1 и 2 меняются ролями и снова выполняют протокол $\mathrm{OT} - \binom{2}{1}$:
  - Участник 1 выполняет роль отправителя (S) и он обладает двумя секретами: u_1 и $x_1 \oplus u_1$;
  - Участник 2 выполняет роль получателя (R) и он желает получить секрет с номером y_2;
  - В результате Участник 2 получает $OT(u_1, x_1 \oplus u_1; y_2) = u_1(1 - y_2) \oplus (x_1 \oplus u_1)y_2 = u_1 \oplus x_1 y_2$.

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.



Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участник 1 вычисляет
  $z_1 = x_1 y_1 \oplus u_1 \oplus OT(u_2, x_2 \oplus u_2; y_1) = x_1 y_1 \oplus u_1 \oplus u_2 \oplus x_2 y_1$
  и отправляет z_1 Участнику 2 (по открытому каналу);

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участник 1 вычисляет
  $z_1 = x_1 y_1 \oplus u_1 \oplus OT(u_2, x_2 \oplus u_2; y_1) = x_1 y_1 \oplus u_1 \oplus u_2 \oplus x_2 y_1$
  и отправляет z_1 Участнику 2 (по открытому каналу);
- Участник 2 вычисляет
  $z_2 = x_2 y_2 \oplus u_2 \oplus OT(u_1, x_1 \oplus u_1; y_2) = x_2 y_2 \oplus u_2 \oplus u_1 \oplus x_1 y_2$
  и отправляет z_2 Участнику 1 (по открытому каналу).

Протокол **двустороннего** вычисления: $f(x, y) = x \cdot y$, $x, y \in \{0, 1\}$.

- Участник 1 вычисляет
  $z_1 = x_1 y_1 \oplus u_1 \oplus OT(u_2, x_2 \oplus u_2; y_1) = x_1 y_1 \oplus u_1 \oplus u_2 \oplus x_2 y_1$
  и отправляет z_1 Участнику 2 (по открытому каналу);
- Участник 2 вычисляет
  $z_2 = x_2 y_2 \oplus u_2 \oplus OT(u_1, x_1 \oplus u_1; y_2) = x_2 y_2 \oplus u_2 \oplus u_1 \oplus x_1 y_2$
  и отправляет z_2 Участнику 1 (по открытому каналу).
- Каждый из участников вычисляет
  $z_1 \oplus z_2 = x_1 y_1 \oplus x_1 y_2 \oplus x_2 y_1 \oplus x_2 y_2 = (x_1 \oplus x_2) \cdot (y_1 \oplus y_2) = x \cdot y$.

Заключение

Спасибо за внимание!