DOI: 10.55648/1998-6920-2025-19-1-45-53 УДК 519.7

Протокол безопасных вычислений для трех участников с пассивным противником

С. М. Рацеев[1], О. И. Череватенко[2]

[1]Ульяновский государственный университет
[2]Ульяновский государственный педагогический университет имени И. Н. Ульянова

Аннотация: В 2016 г. авторы Araki T., Furukawa J., Lindell Y., Nof A. и Ohara K. представили протокол AFLNO для трехстороннего вычисления любой функциональности с честным большинством и пассивным противником. Этот протокол имеет небольшую вычислительную и коммуникационную сложность. Указанные авторы не приводят полных протоколов как для вычисления логических схем, так и для вычисления арифметических схем, показывая лишь идеи для этих протоколов. В данной работе приводятся полные протоколы безопасных вычислений.

Ключевые слова: криптографический протокол, многосторонние вычисления, схема разделения секрета.

Для цитирования: Рацеев С. М., Череватенко О. И. Протокол безопасных вычислений для трех участников с пассивным противником // Вестник СибГУТИ. 2025. Т. 19, № 1. С. 45–53. https://doi.org/10.55648/1998-6920-2025-19-1-45-53.

Статья поступила в редакцию 06.06.2024;
переработанный вариант 16.07.2024;
принята к публикации 17.07.2024.

Введение

Существуют два основных подхода к построению протоколов многосторонних вычислений: протоколы на основе *схем разделения секрета*, которые работают за счет взаимодействия участников для каждого элемента схемы; протоколы на основе *искаженных схем*, которые работают за счет того, что участники создают искаженную версию схемы, которая может быть вычислена сразу. Оба подхода важны и имеют настройки, при которых один подход работает лучше, чем другой. С одной стороны, подход с искаженными схемами дает протоколы с постоянным числом раундов. Таким образом, в сетях с высокой задержкой они намного превосходят протоколы, основанные на схемах разделения секрета, у которых количество раундов линейно по глубине вычисляемой схемы. С другой стороны, протоколам, основанным на схемах разделения секрета, обычно достаточно низкой пропускной способности канала и они передают небольшие сообщения на каждый элемент схемы, в отличие от искаженных схем, которые передают большие объемы информации и требуют большой (и дорогостоящей) пропускной способности.

В работе приводится протокол AFLNO (Araki T., Furukawa J., Lindell Y., Nof A., Ohara K.) для безопасного трехстороннего вычисления любой функциональности с честным большинством и пассивным противником. Протокол AFLNO имеет небольшую вычислительную и коммуникационную сложность: для вычисления логической схемы

каждый участник отправляет только один бит для каждого элемента AND (и ничего не отправляется для элементов XOR и NOT). Этот протокол безопасен в присутствии пассивного противника и обеспечивает конфиденциальность в модели клиент-сервер в присутствии активного противника.

Рассматриваемый протокол подходит для арифметических схем над любым полем или над любым конечным коммутативным кольцом с единицей, в котором элемент 3=1+1+1 обратим, где 1 – единичный элемент кольца. Элементы сложения требуют только локального сложения, а элементы умножения требуют, чтобы каждый участник отправлял только один элемент поля/кольца другому участнику. Для случая логических схем это означает, что каждый участник передает только один бит для элемента AND. Кроме того, вычисления в этом протоколе очень просты: в случае логических схем каждый участник выполняет две операции $\oplus$ на элемент XOR, а на элемент AND выполняются две операции $\bullet$ и три операции $\oplus$. Все операции поддаются распараллеливанию на стандартных компьютерах.

В оригинальной работе авторы не приводят полных протоколов как для вычисления логических схем, так и для вычисления арифметических схем, показывая лишь идеи для этих протоколов. В данной работе приводятся полные протоколы безопасных вычислений, дополняющие работу , сопровождающие числовым примером применения таких протоколов.

Все необъясняемые ниже понятия можно найти в [1].

1. Безопасное вычисление логических схем

Корреляционная случайность. Протокол AFLNO предполагает, что для каждого элемента умножения три участника P_1, P_2, P_3 обладают *корреляционной случайностью* (correlated randomness) в виде случайных элементов $x_1, x_2, x_3 \in \{0, 1\}$ с условием, что $x_1 \oplus x_2 \oplus x_3 = 0$. Протокол AFLNO обладает теоретико-информационной безопасностью с совершенной корреляционной случайностью, но фактическая реализация является вычислительно безопасной благодаря использованию симметричного блочного шифра для генерации корреляционной случайности.

Пока будем предполагать, что участники P_1, P_2, P_3 способны получить случайные $x_1, x_2, x_3 \in \{0, 1\}$ такие, что $x_1 \oplus x_2 \oplus x_3 = 0$.

Схема разделения секрета. Определим (3,2) пороговую (реплицированную) схему разделения секрета следующим образом. Пусть $s \in \{0, 1\}$ – секрет. Дилер выбирает три случайные бита $x_1, x_2, x_3 \in \{0, 1\}$ с условием $x_1 \oplus x_2 \oplus x_3 = 0$. Тогда долями секрета s будут следующие значения:

долей участника P_1 будет (x_1, a_1), где $a_1 = x_3 \oplus s$;

долей участника P_2 будет (x_2, a_2), где $a_2 = x_1 \oplus s$; ;

долей участника P_3 будет (x_3, a_3), где $a_3 = x_2 \oplus s$; .

Заметим, что $a_1 \oplus a_2 \oplus a_3 = s$. Обозначим процедуру разделения секрета s через share(s). Видно, что каждый участник в отдельности не имеет никакой информации о секрете. При этом любые два участника легко восстановят секрет:

$$P_1, P_2: \ s = a_2 \oplus x_1,$$
$$P_1, P_3: \ s = a_1 \oplus x_3,$$
$$P_2, P_2: \ s = a_3 \oplus x_2,$$

Данные соотношения означают следующее, что определяет процедуру восстановления секрета open([s]):

- P_1 передает P_2 значение x_1. После этого участник P_2 вычисляет $s = a_2 \oplus x_1$;
- P_3 передает P_1 значение x_3. После этого участник P_1 вычисляет $s = a_1 \oplus x_3$;
- P_2 передает P_3 значение x_2. После этого участник P_3 вычисляет $s = a_3 \oplus x_2$.

Операции над долями. Определим следующие (локальные) операции над долями. Пусть $[s_1] = ((x_1,a_1), (x_2,a_2), (x_3,a_3))$, $[s_2] = ((y_1,b_1), (y_2,b_2), (y_3,b_3))$ – векторы долей соответственно секретов s_1 и s_2. Тогда операции над долями определяются следующим образом.

- *Сложение*
  $[s_1] \oplus [s_2] = [s_1 \oplus s_2] = ((x_1 \oplus y_1, a_1 \oplus b_1), (x_2 \oplus y_2, a_2 \oplus b_2), (x_3 \oplus y_3, a_3 \oplus b_3))$.
- *Умножение на константу* $c \in \{0,1\}$.
  $c \cdot [s] = [c \cdot s] = ((c \cdot x_1, c \cdot a_1), (c \cdot x_2, c \cdot a_2), (c \cdot x_3, c \cdot a_3))$.
- *Сложение с константой* c.
  $[s] \oplus c = [s \oplus c] = ((x_1, a_1 \oplus c), (x_2, a_2 \oplus c), (x_3, a_3 \oplus c))$.
- *Операция* NOT.
  $\overline{[s]} = [\bar{s}] = ((x_1, \bar{a}_1), (x_2, \bar{a}_2), (x_3, \bar{a}_3))$, где $\bar{s} = 1 \oplus s$.
- *Умножение*.
  $[s_1] \cdot [s_2] = [s_1 \cdot s_2] = ((z_1, c_1), (z_2, c_2), (z_3, c_3))$,

где вычисление (z_i, c_i) проходит следующим образом. Пусть участники P_1, P_2, P_3 обладают корреляционной случайностью α_1, α_2, α_3 соответственно, причем $\alpha_1 \oplus \alpha_2 \oplus \alpha_3 = 0$. Участники вычисляют доли (3, 2) доли секрета $s_1 \cdot s_2$ следующим образом.

Этап 1 – вычисление долей (3, 3) аддитивной схемы.

P_1 вычисляет $r_1 = x_1y_1 \oplus a_1b_1 \oplus \alpha_1$ и значение r_1 передает P_2.

P_2 вычисляет $r_2 = x_2y_2 \oplus a_2b_2 \oplus \alpha_2$ и значение r_2 передает P_3.

P_3 вычисляет $r_3 = x_3y_3 \oplus a_3b_3 \oplus \alpha_3$ и значение r_3 передает P_1.

Эти значения вычисляются и передаются параллельно.

Этап 2 – вычисление долей (3, 2) схемы. На этом этапе участники вычисляют доли (3, 2) схемы на основе долей (3, 3) схемы. Все вычисления производятся локально без взаимодействия участников.

P_1 определяет $(z_1, c_1) = (r_1 \oplus r_3, r_1)$.

P_2 определяет $(z_2, c_2) = (r_2 \oplus r_1, r_2)$.

P_3 определяет $(z_3, c_3) = (r_3 \oplus r_2, r_3)$.

Нетрудно видеть, что приведенные выше операции над долями определяют доли соответственно секретов $s_1 \oplus s_2$, $c \cdot s$, $s \oplus c$, $\bar{s}$, $s_1 \cdot s_2$.

Генерирование корреляционной случайности. Протокол AFLNO основан на том факте, что участники имеют случайные биты с α_1, α_2, α_3 условием $\alpha_1 \oplus \alpha_2 \oplus \alpha_3 = 0$, причем каждый участник обладает только своим битом. Такая тройка битов нужна для каждого элемента AND. Покажем, как можно эффективно генерировать такие тройки битов с тем условием, что у каждого участника свой бит.

Теоретико-информационная корреляционная случайность. Можно надежно генерировать корреляционную случайность с теоретико-информационной безопасностью. Для этого каждый участник P_i должен выбрать $\rho_i \in_R \{0,1\}$ и передать это значение участнику P_{i+1} (при этом P_3 передает ρ_3 участнику P_1). Затем каждый участник складывает свой бит с тем битом, который он получил:

$$P_1: \ \alpha_1 = \rho_1 \oplus \rho_3,$$
$$P_2: \ \alpha_2 = \rho_2 \oplus \rho_1,$$
$$P_3: \ \alpha_3 = \rho_3 \oplus \rho_2,$$

При этом $\alpha_1 \oplus \alpha_2 \oplus \alpha_3 = 0$. Заметим, что если P_1 нечестный, то он не имеет никакой информации (в теоретико-информационном смысле) о α_2 и, кроме того, что $\alpha_2 \oplus \alpha_3 = \alpha_1$. Это потому, что $\alpha 2$ и $\alpha 3$ скрыты битом ρ_2, который неизвестен участнику P_1. Аналогичный аргумент справедлив для нечестных P_2 или P_3. Несмотря на элегантность и простоту этого решения, приведем еще один метод. Это связано с тем фактом, что приведенный выше подход удваивает коммуникационную сложность передачи данных для элемента AND.

Вычислительная корреляционная случайность. Теперь покажем, как можно (вычислительно) безопасно вычислять корреляционную случайность без какого-либо взаимодействия, кроме короткой начальной настройки. Это позволяет поддерживать

ситуацию, когда участникам требуется передавать только один бит на элемент AND. Пусть k – параметр безопасности и пусть $F:\{0,1\}^k\times\{0,1\}^k\to\{0,1\}$ – псевдослучайная функция (pseudorandom function), которая возвращает один бит.

1. **Инициализация.**
   a. Каждый участник P_i выбирает $k_i \in_R \{0,1\}^k$.
   b. P_1 передает участнику P_3 значение k_1, P_2 передает участнику P_1 значение k_2, P_3 передает участнику P_2 значение k_3.

   P_1 обладает k_1, k_2; P_2 обладает k_2, k_3; P_3 обладает k_3, k_1.
2. **GetNextBit** вычисления. Для заданного уникального идентификатора $id \in_R \{0,1\}^k$ участники делают следующее.
   a. P_1 вычисляет $\alpha_1 = F_{k1}(id) \oplus F_{k2}(id)$.
   b. P_2 вычисляет $\alpha_2 = F_{k2}(id) \oplus F_{k3}(id)$.
   c. P_3 вычисляет $\alpha_3 = F_{k3}(id) \oplus F_{k1}(id)$.

Заметим, что $\alpha_1 \oplus \alpha_2 \oplus \alpha_3 = 0$. Более того, P_1 не знает k_3, которое используется для получения α_2 и α_3. Поэтому k_3 является псевдослучайным для P_1 при ограничении, что $\alpha_2 \oplus \alpha_3 = \alpha_1$. На практике идентификатор id может быть счетчиком, который все участники локально увеличивают при каждом вызове GetNextBit.

Протокол вычисления логических схем. Полный трехсторонний протокол работает естественным образом. Участники сначала обмениваются своими входными данными, используя схему разделения секрета. Затем они вычисляют каждый элемент XOR, NOT и AND в схеме в соответствии с заданным топологическим порядком для схемы. Наконец, участники восстанавливают свои выходные данные на выходных проводах схемы.

Протокол 1 (вычисление логической схемы).

Вход. Каждый участник P_i, $i = 1, 2, 3$, обладает входным значением $x_i \in_R \{0,1\}^l$. Участники обладают описанием логической схемы C , которая вычисляет функциональность f, с входными данными (общей) длины $M = 3 \cdot l$. Пусть N – число элементов AND в схеме C.

Предварительный этап. Участники вычисляют N корреляционных случайностей для применения их в элементах AND. Это можно сделать до начала протокола.

Протокол.

1. *Получение долей входных данных на основе схемы разделения секрета*.
   a. Для каждого значения s_i участника P_i этот участник с помощью процедуры share(s_i) разделяет секрет s_i среди всех участников.
   b. Каждый участник P_i сохраняет вектор долей $(s^j_1, \ldots, s^j_M)$ всех входных значений, полученных с помощью процедуры share.
2. *Вычисление логической схемы*. Пусть $G_1,\ldots,G_T$ – топологический порядок следования элементов схемы. Для k=1,...T участники делают следующее.
   - Пусть G_k является элементом XOR. Пусть $[s_1]$ и $[s_2]$ – векторы долей участников на входных проводах элемента G_k. Тогда на выходном проводе элемента G_k будет вектор долей $[s_1] \oplus [s_2] = [s_1 \oplus s_2]$, который вычисляется участниками локально.
   - Пусть G_k является элементом NOT. Пусть $[s]$ – вектор долей участников на входном проводе элемента G_k. Тогда на выходном проводе элемента G_k будет вектор долей $\overline{[s]} = [\bar{s}]$, который вычисляется участниками локально.
   - Пусть G_k является элементом AND. Пусть $[s_1]$ и $[s_2]$ – векторы долей участников на входных проводах элемента G_k. Тогда на выходном проводе элемента G_k будет вектор долей $[s_1] \cdot [s_2] = [s_1 \cdot s_2]$, который вычисляется описанным выше способом, расходуя при этом очередную корреляционную случайность.
3. *Восстановление выходных значений*. Для каждого выходного провода схемы C участники передают свои доли участнику P_i для получения им $[s]$, где $[s]$ – вектор долей значения на выходном проводе, соответствующее участнику P_i. На основе $[s]$ участник P_i получает выходное значение.

2. Протокол AFLNO над кольцами

Протокол, описанный выше, работает для логических схем. Однако в некоторых случаях арифметические схемы гораздо эффективнее. Пусть R – коммутативное кольцо с единицей 1. Будем считать, что элемент 3=1+1+1 обратим в R. В данном параграфе покажем, как обобщить описанный выше протокол на общий случай кольца R (в частности, кольца вычетов по модулю 2^n) и случай произвольного конечного поля. Заметим, что при $R = GF(2^n)$ получаем, что сложение (и вычитание) совпадает с операцией $\oplus$.

(3,2) схема разделения секрета. Для того, чтобы разделить секрет $s \in R$, дилер выбирает три случайных элемента $x_1, x_2, x_3 \in {}_R R$, при условии, что $x_1 + x_2 + x_3 = 0$. Тогда долями секрета s будут следующие значения.

- Долей участника P_1 будет (x_1, a_1), где $a_1 = x_3 - s$.
- Долей участника P_2 будет (x_2, a_2), где $a_2 = x_1 - s$.
- Долей участника P_3 будет (x_3, a_3), где $a_3 = x_2 - s$.

Как и для случая логических схем, видно, что каждая доля не несет никакой информации о секрете s и что любых двух долей достаточно для восстановления s:

$$P_1, P_2: \quad s = x_1 - a_2,$$
$$P_1, P_3: \quad s = x_3 - a_1,$$
$$P_2, P_3: \quad s = x_2 - a_3.$$

Операции над долями. Определим следующие (локальные) операции над долями. Пусть

$$[s_1] = ((x_1, a_1), (x_2, a_2), (x_3, a_3)), \quad [s_2] = ((y_1, b_1), (y_2, b_2), (y_3, b_3))$$

– векторы долей соответственно секретов s_1 и s_2. Тогда операции над долями определяются следующим образом.

- *Сложение*.
$$[s_1] + [s_2] = [s_1 + s_2] = ((x_1 + y_1, a_1 + b_1), (x_2 + y_2, a_2 + b_2), (x_3 + y_3, a_3 + b_3)).$$
- *Умножение на константу* $c \in R$.
$$c \cdot [s] = [c \cdot s] = ((c \cdot x_1, c \cdot a_1), (c \cdot x_2, c \cdot a_2), (c \cdot x_3, c \cdot a_3)).$$
- *Сложение с константой* c.
$$[s] + c = [s + c] = ((x_1, a_1 + c), (x_2, a_2 + c), (x_3, a_3 + c)).$$
- *Умножение*.
$$[s_1] \cdot [s_2] = [s_1 \cdot s_2] = ((z_1, c_1), (z_2, c_2), (z_3, c_3)),$$
где вычисление (z_i, c_i)проходит следующим образом. Пусть участники P_1, P_2, P_3 обладают корреляционной случайностью α_1, α_2, α_3 соответственно, причем $\alpha 1+\alpha 2+\alpha 3=0$. Участники вычисляют доли (3,2) доли секрета $s_1 \cdot s_2$ следующим образом.
    - **Этап 1 – вычисление долей (3,3) аддитивной схемы.**
        - P_1 вычисляет $r_1 = 3^{-1}(a_1b_1 - x_1y_1 + \alpha_1)$ и передает r_1 участнику P_2.
        - P_2 вычисляет $r_2 = 3^{-1}(a_2b_2 - x_2y_2 + \alpha_2)$ и передает r_2 участнику P_3.
        - P_3 вычисляет $r_3 = 3^{-1}(a_3b_3 - x_3y_3 + \alpha_3)$ и передает r_3 участнику P_1.

      Эти значения вычисляются и передаются параллельно.
    2. **Этап 2 – вычисление долей (3,2) схемы.** На этом этапе участники вычисляют доли (3,2) схемы на основе долей (3,3) схемы. Все вычисления производятся локально без взаимодействия участников.
        - P_1 определяет долю $(z_1, c_1) = (r_3 - r_1, -2r_3 - r_1)$.
        - P_2 определяет долю $(z_2, c_2) = (r_1 - r_2, -2r_1 - r_2)$.
        - P_3 определяет долю $(z_3, c_3) = (r_2 - r_3, -2r_2 - r_3)$.

Безопасность умножения следует из того, что секрет надежно скрыт в результате схемы разделения секрета. Это следует из того, что в вычислениях применяется корреляционная случайность.

Генерация корреляционной случайности. Участники применяют тот же (вычислительно) безопасный метод на основе псевдослучайной функции, описанный выше.

Разница состоит в следующем. Во-первых, псевдослучайная функция имеет вид $F:\{0,1\}^k\times\{0,1\}^k\to\{0,1\}^n$, где $R = \{0,1\}^n$, т. е. с точностью до изоморфизма будем считать, что каждый элемент кольца R представим в виде битовой строки длины n (если $|R| \neq 2^n$, то можно генерировать теоретико-информационная корреляционную случайность, описанную выше). Во-вторых, участники проделывают следующие действия.

1. P_1 вычисляет $\alpha_1 = F_{k1}(id) - F_{k2}(id)$.
2. P_2 вычисляет $\alpha_2 = F_{k2}(id) - F_{k3}(id)$.
3. P_3 вычисляет $\alpha_3 = F_{k3}(id) - F_{k1}(id)$..

Протокол вычисления арифметической схемы. Теперь приведем протокол вычисления арифметической схемы над кольцом R.

Протокол 2 (вычисление арифметической схемы).

Вход. Каждый участник P_i, i = 1, 2, 3 обладает входным значением $x_i \in R^l$. Участники обладают описанием арифметической схемы C, которая вычисляет функциональность f с входными данными (общей) длины $M = 3 \cdot l$. Пусть N – число элементов умножения в схеме C.

Предварительный этап. Участники вычисляют N корреляционных случайностей для применения их в элементах умножения.

Протокол.

1. *Получение долей входных данных на основе схемы разделения секрета*.
   a. Для каждого значения s_i участника P_i этот участник с помощью процедуры share(s_i) над R разделяет секрет s_i среди всех участников.
   b. Каждый участник P_i сохраняет вектор долей (s^j_1, …, s^j_M) всех входных значений, полученных с помощью процедуры share.
2. *Вычисление арифметической схемы*. Пусть G_1, …, G_T – топологический порядок следования элементов схемы. Для k = 1, …, T участники делают следующее:
   - Пусть G_k является элементом сложения. Пусть $[s_1]$ и $[s_2]$ – векторы долей участников на входных проводах элемента G_k. Тогда на выходном проводе элемента G_k будет вектор долей $[s_1] + [s_2] = [s_1 + s_2]$, который вычисляется участниками локально.
   - Пусть G_k является элементом умножения на константу $c \in R$. Пусть [s] – вектор долей участников на входном проводе элемента G_k. Тогда на выходном проводе элемента G_k будет вектор долей $c \cdot [s] = [c \cdot s]$, который вычисляется участниками локально.
   - Пусть G_k является элементом умножения. Пусть $[s_1]$ и $[s_2]$ – векторы долей участников на входных проводах элемента G_k. Тогда на выходном проводе элемента G_k будет вектор долей $[s_1] \cdot [s_2] = [s_1 \cdot s_2]$, который вычисляется описанным выше способом, расходуя при этом очередную корреляционную случайность.
3. *Восстановление выходных значений*. Для каждого выходного провода схемы C участники передают свои доли вектора [s] участнику P_i для получения им [s], где [s] – вектор долей значения на выходном проводе, соответствующее участнику P_i. На основе [s] участник P_i получает выходное значение.

Представленный протокол является безопасным для случая одного нечестного участника, которого контролирует пассивный противник. Пусть F_{mult} – идеальная функциональность для вычисления долей произведения секретов s_1 и s_2, которая получает на вход доли этих секретов.

Теорема 1 [3]. *Пусть* $f:(R^*)^3\to(R^*)^3$ *– тернарная функциональность. Тогда протокол 2 вычисляет f с совершенной безопасностью в* F_{mult} *– гибридной модели для случая пассивного противника, контролирующего одного участника.*

3. Численный пример протокола AFLNO

Покажем, как можно безопасно вычислить значение функции $y = f(x_1, x_2, x_3) = x_1x_2 + 5x_3$ над полем $F = GF(11)$ с помощью протокола AFLNO для участников P_1, P_2, P_3, обладающих соответственно значениями $x_1 = 5$, $x_2 = 2$, $x_3 = 4$. Все участники должны получить одно и то же значение $y = y_1 = y_2 = y_3 = f(x_1, x_2, x_3)$. Предполагается, что противник пассивный. Далее под x_1, x_2, x_3 будем обозначать доли секретов, чтобы не менять обозначения из протокола AFLNO.

1. **Входной этап.** Так как в вычисляемой схеме только один элемент умножения, то необходима одна корреляционная тройка. Пусть $\alpha_1 = 4$, $\alpha_2 = 5$, $\alpha_3 = 2$ – корреляционная тройка, причем каждый участник знает только свою компоненту.
   Участник P_1 выбирает три случайных элемента $x_1, x_2, x_3 \in GF(11)$ при условии, что $x_1 + x_2 + x_3 = 0$. Пусть $x_1 = 4$, $x_2 = 8$, $x_3 = 10$. Тогда долями участников P_1, P_2, P_3 секретного значения 5 будут следующие значения.
   $$P_1\text{: } (4,5), \quad P_2\text{: } (8,10), \quad P_3\text{: } (10,3).$$
   Участник P_2 проделывает аналогичные действия. Пусть (7,3,1) – сгенерированная им корреляционная тройка. Тогда долями участников P_1, P_2, P_3 секретного значения 2 будут следующие значения.
   $$P_1\text{: } (7,10), \quad P_2\text{: } (3,5), \quad P_3\text{: } (1,1).$$
   Участник P_3 тоже проделывает аналогичные действия. Пусть (6,2,3) – сгенерированная им корреляционная тройка. Тогда долями участников P_1, P_2, P_3 секретного значения 4 будут следующие значения.
   $$P_1\text{: } (6,10), \quad P_2\text{: } (2,2), \quad P_3\text{: } (3,9).$$
2. **Этап вычислений.**
   a. *Элемент умножения*. По входным проводам элемента умножения проходят доли
   $$[5] = ((x_1, a_1), (x_2, a_2), (x_3, a_3)) = ((4,5), (8,10), (10,3))$$
   и
   $$[2] = ((y_1, b_1), (y_2, b_2), (y_3, b_3)) = ((7,10), (3,5), (1,1))$$
   Доли произведения вычисляются в два этапа.
   Этап 1 – вычисление долей (3,3) аддитивной схемы. Участники проделывают следующие действия.
   - P_1 вычисляет
     $$r_1 = 3^{-1}(a_1b_1 - x_1y_1 + \alpha) \equiv 3^{-1}(5 \cdot 10 - 4 \cdot 7 + 4) \equiv 5 \pmod{11}$$
     и передает $r_1 = 5$ участнику P_2.
   - P_2 вычисляет
     $$r_2 = 3^{-1}(a_2b_2 - x_2y_2 + \beta) \equiv 3^{-1}(10 \cdot 5 - 8 \cdot 3 + 5) \equiv 3 \pmod{11}$$
     и передает $r_2 = 3$ участнику P_3.
   - P_3 вычисляет
     $$r_3 = 3^{-1}(a_3b_3 - x_3y_3 + \gamma) \equiv 3^{-1}(3 \cdot 1 - 10 \cdot 1 + 2) \equiv 2 \pmod{11}$$
     и передает $r_3 = 2$ участнику P_1.

   Этап 2 – вычисление долей (3,2) схемы. На этом этапе участники вычисляют доли (3,2) схемы на основе долей (3,3) схемы. Все вычисления производятся локально без взаимодействия участников.
   - P_1 определяет долю $(z_1, c_1) = (r_3 - r_1, -2r_3 - r_1) = (8,2)$.
   - P_2 определяет долю $(z_2, c_2) = (r_1 - r_2, -2r_1 - r_2) = (2,9)$.
   - P_3 определяет долю $(z_3, c_3) = (r_2 - r_3, -2r_2 - r_3) = (1,3)$.

   b. *Элемент умножения на константу* 5. Каждый участник умножает свою долю вектора долей на 5, т. е.
   $$5 \cdot [4] = 5 \cdot ((6,10), (2,2), (3,9)) = ((8,6), (10,10), (4,1)).$$
   c. *Элемент сложения*. По входным проводам этого элемента проходят доли

((8,2), (2,9), (1,3)) и ((8,6), (10,10), (4,1)). Тогда на выходном проводе этого элемента будет следующий вектор долей:

((8,2), (2,9), (1,3)) + ((8,6), (10,10), (4,1)) = ((5,8), (1,8), (5,4)).

a. Напомним, что вычисления проходят по модулю 11.

3. **Выходной этап.** P_1 передает участнику P_2 значение $x_1 = 5$, P_2 передает участнику P_3 значение $x_2 = 1$, P_3 передает участнику P_1 значение $x_3 = 5$. Каждый участник теперь владеет следующими долями:

$$P_1: (x_1, a_1) = (5,8), x_3 = 5,$$
$$P_2: (x_2, a_2) = (1,8), x_1 = 5,$$
$$P_3: (x_3, a_3) = (5,4), x_2 = 1.$$

Участники вычисляют:

$$P_1: x_3 - a_1 = 5 - 8 \equiv 8 \pmod{11},$$
$$P_2: x_1 - a_2 = 5 - 8 \equiv 8 \pmod{11},$$
$$P_3: x_2 - a_3 = 1 - 4 \equiv 8 \pmod{11}.$$

Литература

1. *Рацеев С. М.* Криптография. Безопасные многосторонние вычисления : учеб. пособие для вузов. СПб. : Лань, 2025. 468 с.
2. *Feng D., Yang K.* Concretely efficient secure multi-party computation protocols: survey and more // Security and Safety. 2022. Vol. 1. P. 1–43. DOI: 10.1051/sands/2021001
3. *Araki T., Furukawa J., Lindell Y., Nof A., Ohara K.* High throughput semi-honest secure three-party computation with an honest majority // 2016. ACM. P. 805–817. DOI: 10.1145/2976749.2978331
4. *Рацеев С. М.* Криптографические протоколы. Схемы разделения секрета : учебное пособие для вузов. СПб. : Лань, 2024. 336 с.

Рацеев Сергей Михайлович

д.ф.-м.н., профессор кафедры информационной безопасности и теории управления Ульяновского государственного университета (432017, г. Ульяновск, ул. Льва Толстого, 42) e-mail: ratseevsm@mail.ru.

Череватенко Ольга Ивановна

к.ф.-м.н., доцент кафедры высшей математики Ульяновского государственного педагогического университета имени И.Н.Ульянова (432071, г. Ульяновск, площадь Ленина, д.4/5).

Авторы прочитали и одобрили окончательный вариант рукописи.

Авторы заявляют об отсутствии конфликта интересов.

Вклад соавторов: Каждый автор внёс равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.

Passive secure three-party computation with an honest majority

Sergey M. Ratseev[1], Olga I. Cherevatenko[2]

[1] Ulyanovsk State University
[2] Ulyanovsk State University of Education

Abstract: In 2016, the authors Araki T., Furukawa J., Lindell Y., Of A. and Ohara K. introduced a new information-theoretic protocol (and a computationally-secure variant) for secure three-party computation with an honest majority. The protocol has very minimal computation and communication. The authors did not provide a complete protocols. This paper provides complete protocols for secure multiparty computation.

Keywords: cryptographic protocol, multiparty computation, secret sharing.

For citation: Ratseev S. M., Cherevatenko O. I. Passive secure three-party computation with an honest majority Vestnik SibGUTI, 2025, vol. 19, no. 1, pp. 45–53. https://doi.org/10.55648/1998-6920-2025-19-1-45-53.

The article was submitted: 06.06.2024;
revised version: 16.06.2024;
accepted for publication 17.06.2024.

References

1. *Ratseev S. M.* Kriptografiya. Bezopasnye mnogostoronnie vychisleniya [Cryptography. Secure multiparty computation]. St. Petersburg: Lan Publishing House, 2024. 468 p.
2. *Feng D., Yang K.* Concretely efficient secure multi-party computation protocols: survey and more // Security and Safety. 2022. Vol. 1. P. 1–43. DOI: 10.1051/sands/2021001
3. *Araki T., Furukawa J., Lindell Y., Nof A., Ohara K.* High throughput semi-honest secure three-party computation with an honest majority // 2016. ACM. P. 805–817. DOI: 10.1145/2976749.2978331
4. *Ratseev S. M.* Kriptograficheskie protokoly. Skhemy razdeleniya sekreta [Cryptographic protocols. Secret sharing schemes]. St. Petersburg: Lan Publishing House, 2024. 336 p.

Sergey M. Ratseev
Doctor of Science (Physics and Mathematics), associate professor, professor of Department of Information Security and Control Theory, Ulyanovsk State University, (432017, Ulyanovsk, Lev Tolstoy str., 42) e-mail: ratseevsm@mail.ru.

Olga I. Cherevatenko
Candidate of Science (Physics and Mathematics), associate professor; Department of Higher Mathematics; Ulyanovsk State Pedagogical University named after I.N. Ulyanov. (432071, Ulyanovsk, Lenin sq., 4/5).