

# Протоколы многосторонних вычислений, часть 2

Косолапов Ю.В.

ЮФУ

9 декабря 2020 г.

# Содержание

- 1 Протокол многосторонних вычислений арифметических выражений (ПМВАМ)

# Формулировка задачи

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

## Формулировка задачи

- Пусть  $\mathcal{P} = \{1, \dots, n\}$  — множество участников.
- $\mathcal{S} = \mathbb{F}_q$  — множество возможных значений секретов.

## Формулировка задачи

- Пусть  $\mathcal{P} = \{1, \dots, n\}$  — множество участников.
- $\mathcal{S} = \mathbb{F}_q$  — множество возможных значений секретов.
- Каждый участник  $i$  из  $\mathcal{P}$  обладает некоторым секретом  $s_i \in \mathcal{S}$ .

## Формулировка задачи

- Пусть  $\mathcal{P} = \{1, \dots, n\}$  — множество участников.
- $\mathcal{S} = \mathbb{F}_q$  — множество возможных значений секретов.
- Каждый участник  $i$  из  $\mathcal{P}$  обладает некоторым секретом  $s_i \in \mathcal{S}$ .
- Требуется защищенным образом вычислить функцию  $f(x_1, \dots, x_n) = (y_1, \dots, y_n)$ ,  $y_i \in \mathbb{F}_q$ .

## Формулировка задачи

- Пусть  $\mathcal{P} = \{1, \dots, n\}$  — множество участников.
- $\mathcal{S} = \mathbb{F}_q$  — множество возможных значений секретов.
- Каждый участник  $i$  из  $\mathcal{P}$  обладает некоторым секретом  $s_i \in \mathcal{S}$ .
- Требуется защищенным образом вычислить функцию  $f(x_1, \dots, x_n) = (y_1, \dots, y_n)$ ,  $y_i \in \mathbb{F}_q$ .
- Функция не  $f(x_1, \dots, x_n)$  не является секретной.

# Формулировка задачи



## Формулировка задачи

Будем предполагать, что  $f(x_1, \dots, x_n)$  реализуется *арифметической схемой*, которая представляет собой направленный граф без циклов.

## Формулировка задачи

Будем предполагать, что  $f(x_1, \dots, x_n)$  реализуется *арифметической схемой*, которая представляет собой направленный граф без циклов.

- 1 В таком графе каждая вершина (шлюз) имеет не более двух входящих ребер (соединительных линий).

## Формулировка задачи

Будем предполагать, что  $f(x_1, \dots, x_n)$  реализуется *арифметической схемой*, которая представляет собой направленный граф без циклов.

- 1 В таком графе каждая вершина (шлюз) имеет не более двух входящих ребер (соединительных линий).
- 2 Среди вершин имеется  $n$  *входных* вершин без входящих ребер и с одним исходящим ребром. Входные вершины помечаются номерами участников.

## Формулировка задачи

Будем предполагать, что  $f(x_1, \dots, x_n)$  реализуется *арифметической схемой*, которая представляет собой направленный граф без циклов.

- 1 В таком графе каждая вершина (шлюз) имеет не более двух входящих ребер (соединительных линий).
- 2 Среди вершин имеется  $n$  *входных* вершин без входящих ребер и с одним исходящим ребром. Входные вершины помечаются номерами участников.
- 3 Каждому участнику также соответствует одна *выходная* вершина.

# Формулировка задачи

## Формулировка задачи

- 4 Кроме входных и выходных вершин имеются вершины, которые соответствуют операциям сложения и умножения (эти шлюзы имеют соответственно метки «+» и «·»). Такие вершины имеют по два входящих ребра и по несколько исходящих ребер.

## Формулировка задачи

- 4 Кроме входных и выходных вершин имеются вершины, которые соответствуют операциям сложения и умножения (эти шлюзы имеют соответственно метки «+» и «·»). Такие вершины имеют по два входящих ребра и по несколько исходящих ребер.
- 5 В графе также могут быть шлюзы, в которых выполняется умножение входного значения на некоторую константу  $\alpha$ ; такие вершины имеют метку  $\alpha\cdot$ , содержат одно входящее ребро и несколько исходящих.

# Формулировка задачи

Вычисление на арифметической схеме выполняется следующим образом:



## Формулировка задачи

Вычисление на арифметической схеме выполняется следующим образом:

- для каждого  $i \in [n]$  ребро, исходящее из входной вершины с меткой  $i$ , помечается значением секрета участника  $i$ ;

## Формулировка задачи

Вычисление на арифметической схеме выполняется следующим образом:

- для каждого  $i \in [n]$  ребро, исходящее из входной вершины с меткой  $i$ , помечается значением секрета участника  $i$ ;
- остальным ребрам присваиваются метки в соответствии с порядком вычисления арифметических выражений.

## Пример арифметической схемы

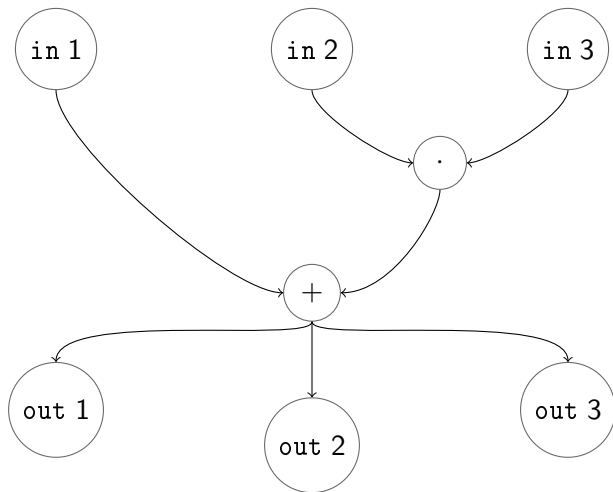


Рис.: Арифметическая схема, соответствующая отображению  $f(x_1, x_2, x_3) = (y_1, y_2, y_3)$ ,  $y_i = x_1 + x_2 \cdot x_3$  для  $i = 1, 2, 3$ .

## Пример арифметической схемы

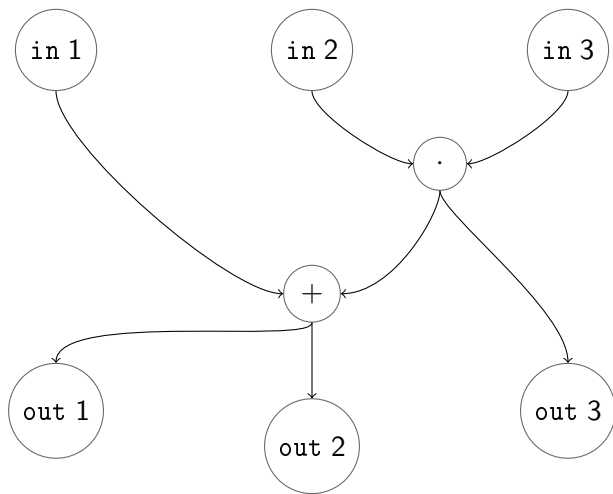


Рис.: Арифметическая схема, соответствующая отображению  $f(x_1, x_2, x_3) = (y_1, y_2, y_3)$ ,  $y_1 = y_2 = x_1 + x_2 \cdot x_3$ ,  $y_3 = x_2 \cdot x_3$ .

# Обозначения

## Обозначения

- Пусть  $SS$  —  $(n, t + 1)$ -схема Шамира над полем  $\mathbb{F}_q$ ,  $n/2 > t$ ;

## Обозначения

- Пусть  $SS$  —  $(n, t + 1)$ -схема Шамира над полем  $\mathbb{F}_q$ ,  $n/2 > t$ ;
- Через  $[a, f_a]_t$  обозначим набор долей, вычисленных по секрету  $a \in \mathbb{F}_q$  с помощью полинома  $f_a(x)$  степени не выше  $t$ :

$$[a; f_a]_t = (f_a(1), \dots, f_a(n)), \quad f_a(0) = a, \quad \deg(f_a(x)) \leq t.$$

# Обозначения

- Пусть  $SS$  —  $(n, t + 1)$ -схема Шамира над полем  $\mathbb{F}_q$ ,  $n/2 > t$ ;
- Через  $[a, f_a]_t$  обозначим набор долей, вычисленных по секрету  $a \in \mathbb{F}_q$  с помощью полинома  $f_a(x)$  степени не выше  $t$ :

$$[a; f_a]_t = (f_a(1), \dots, f_a(n)), \quad f_a(0) = a, \quad \deg(f_a(x)) \leq t.$$

- Введем обозначения:

$$[a; f_a]_t + [b; f_b]_t = (f_a(1) + f_b(1), \dots, f_a(n) + f_b(n)) = [a + b, f_a + f_b]_t,$$

$$\alpha[a; f_a]_t = (\alpha f_a(1), \dots, \alpha f_a(n)) = [\alpha a, \alpha f_a]_t,$$

$$[a; f_a]_t \star [b; f_b]_t = (f_a(1) \cdot f_b(1), \dots, f_a(n) \cdot f_b(n)) = [a \cdot b, f_a \cdot f_b]_{2t}.$$



# Обозначения

# Обозначения

- Вычисление отображения  $f$  производится с помощью арифметической схемы.

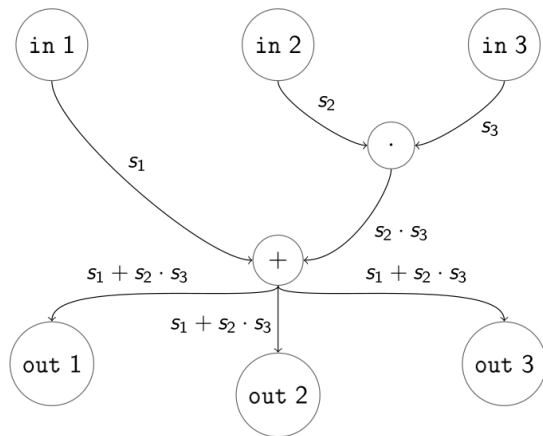
# Обозначения

- Вычисление отображения  $f$  производится с помощью арифметической схемы.
- В арифметической схеме, представленной графом, каждому ребру присваивается вычисленное значение.

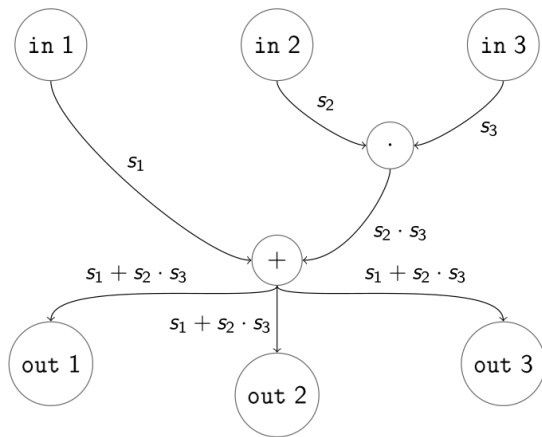
# Обозначения

- Вычисление отображения  $f$  производится с помощью арифметической схемы.
- В арифметической схеме, представленной графом, каждому ребру присваивается вычисленное значение.
- В рамках протокола, если  $a$  – присвоенное некоторому ребру значение, то считается, что все участники владеют набором  $[a, f_a]_t$ , где  $f_a(0) = a$ .

# Пример арифметической схемы с метками

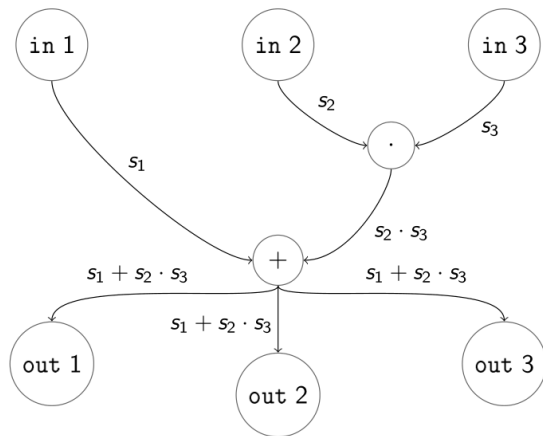


## После инициализации



$$\begin{bmatrix} s_1, f_{s_1} \\ s_2, f_{s_2} \\ s_3, f_{s_3} \end{bmatrix}_t$$

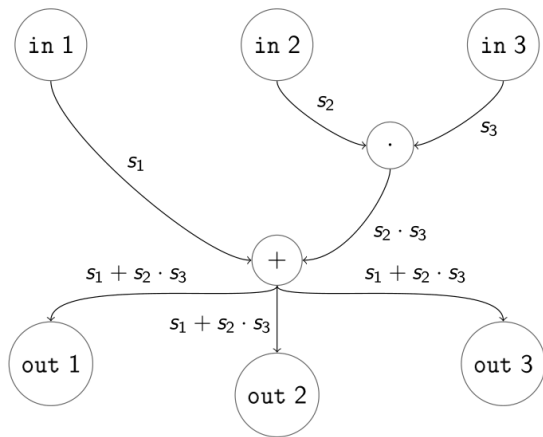
# После умножения



$[s_1, f_{s_1}]_t,$   
 $[s_2, f_{s_2}]_t,$   
 $[s_3, f_{s_3}]_t$

$[s_1, f_{s_1}]_t,$   
 $[s_2, f_{s_2}]_t,$   
 $[s_3, f_{s_3}]_t$   
 $[s_2 \cdot s_3, f_{s_2 \cdot s_3}]_t$

# После суммирования (в фазе завершения протокола)



$$\begin{aligned} & [s_1, f_{s_1}]_t, \\ & [s_2, f_{s_2}]_t, \\ & [s_3, f_{s_3}]_t \end{aligned}$$

$$\begin{aligned} & [s_1, f_{s_1}]_t, \\ & [s_2, f_{s_2}]_t, \\ & [s_3, f_{s_3}]_t \\ & [s_2 \cdot s_3, f_{s_2 \cdot s_3}]_t \end{aligned}$$

$$\begin{aligned} & [s_1, f_{s_1}]_t, \\ & [s_2, f_{s_2}]_t, \\ & [s_3, f_{s_3}]_t \\ & [s_2 \cdot s_3, f_{s_2 \cdot s_3}]_t \\ & [s_1 + s_2 \cdot s_3, f_{s_1 + s_1 \cdot s_2}]_t \end{aligned}$$



# Инициализация протокола

# Инициализация протокола

- Участник  $i (\in \{1, \dots, n\})$  вычисляет  $[s_i; f_{s_i}]_t$  и передает по защищенным каналам доли своего секрета остальным участникам, а  $i$ -ую долю оставляет себе и никому не передает;

# Инициализация протокола

- Участник  $i (\in \{1, \dots, n\})$  вычисляет  $[s_i; f_{s_i}]_t$  и передает по защищенным каналам доли своего секрета остальным участникам, а  $i$ -ую долю оставляет себе и никому не передает;
- После этого участник  $i$  кроме долей своего секрета  $s_i$  знает  $i$ -ую долю секретов других участников:

$$f_{s_1}(i), f_{s_2}(i), \dots, \underline{f_{s_i}(i)}, \dots, f_{s_n}(i).$$

# Инициализация протокола

- Участник  $i (\in \{1, \dots, n\})$  вычисляет  $[s_i; f_{s_i}]_t$  и передает по защищенным каналам доли своего секрета остальным участникам, а  $i$ -ую долю оставляет себе и никому не передает;
- После этого участник  $i$  кроме долей своего секрета  $s_i$  знает  $i$ -ую долю секретов других участников:

$$f_{s_1}(i), f_{s_2}(i), \dots, \underline{f_{s_i}(i)}, \dots, f_{s_n}(i).$$

- Таким образом, после инициализации все участники **владеют** наборами  $[s_1, f_{s_1}]_t, \dots, [s_n, f_{s_n}]_t$

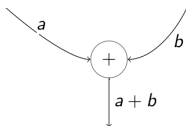
# Суммирование

## Суммирование

- Если входящие в вершину с меткой «+» ребра имеют метки  $a$  и  $b$ , то это означает, что все участники владеют наборами  $[a; f_a]_t$  и  $[b; f_b]_t$ .

# Суммирование

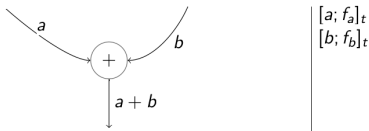
- Если входящие в вершину с меткой «+» ребра имеют метки  $a$  и  $b$ , то это означает, что все участники владеют наборами  $[a; f_a]_t$  и  $[b; f_b]_t$ .



$[a; f_a]_t$   
 $[b; f_b]_t$

# Суммирование

- Если входящие в вершину с меткой «+» ребра имеют метки  $a$  и  $b$ , то это означает, что все участники владеют наборами  $[a; f_a]_t$  и  $[b; f_b]_t$ .

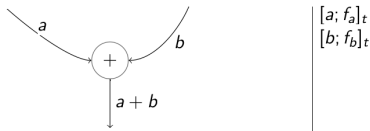


- Участник с номером  $i (\in [n])$  вычисляет  $f_a(i) + f_b(i)$ .



# Суммирование

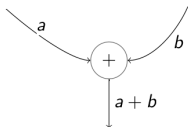
- Если входящие в вершину с меткой «+» ребра имеют метки  $a$  и  $b$ , то это означает, что все участники владеют наборами  $[a; f_a]_t$  и  $[b; f_b]_t$ .



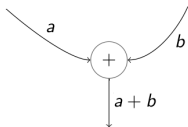
- Участник с номером  $i (\in [n])$  вычисляет  $f_a(i) + f_b(i)$ .
- Таким образом, участники вычисляют  $[a; f_a]_t + [b; f_b]_t = [a + b; f_{a+b}]_t$ ,  $f_{a+b} = f_a + f_b$

# Суммирование

- Если входящие в вершину с меткой «+» ребра имеют метки  $a$  и  $b$ , то это означает, что все участники владеют наборами  $[a; f_a]_t$  и  $[b; f_b]_t$ .


$$\begin{array}{|l} [a; f_a]_t \\ [b; f_b]_t \end{array}$$

- Участник с номером  $i (\in [n])$  вычисляет  $f_a(i) + f_b(i)$ .
- Таким образом, участники вычисляют  $[a; f_a]_t + [b; f_b]_t = [a + b; f_{a+b}]_t$ ,  $f_{a+b} = f_a + f_b$


$$\begin{array}{|l} [a; f_a]_t \\ [b; f_b]_t \\ [a; f_a]_t \\ [b; f_b]_t \\ [a + b; f_{a+b}]_t \end{array}$$

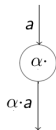
# Умножение на скаляр

## Умножение на скаляр

- Если входящее в вершину с меткой « $\alpha$ » ребро имеет метку  $a$ , то это означает, что все участники владеют набором  $[a; f_a]_t$ .

# Умножение на скаляр

- Если входящее в вершину с меткой « $\alpha \cdot$ » ребро имеет метку  $a$ , то это означает, что все участники владеют набором  $[a; f_a]_t$ .



$[a; f_a]_t$

## Умножение на скаляр

- Если входящее в вершину с меткой « $\alpha \cdot$ » ребро имеет метку  $a$ , то это означает, что все участники владеют набором  $[a; f_a]_t$ .



- Участник с номером  $i (\in [n])$  вычисляет  $\alpha f_a(i)$ .

## Умножение на скаляр

- Если входящее в вершину с меткой « $\alpha$ » ребро имеет метку  $a$ , то это означает, что все участники владеют набором  $[a; f_a]_t$ .



- Участник с номером  $i (\in [n])$  вычисляет  $\alpha f_a(i)$ .
- Таким образом, участники вычисляют  $\alpha[a; f_a]_t = [\alpha \cdot a; f_{\alpha \cdot a}]_t$ ,  
 $f_{\alpha \cdot a} = \alpha \cdot f_a$ .

# Умножение на скаляр

- Если входящее в вершину с меткой « $\alpha \cdot$ » ребро имеет метку  $a$ , то это означает, что все участники владеют набором  $[a; f_a]_t$ .



- Участник с номером  $i (\in [n])$  вычисляет  $\alpha f_a(i)$ .
- Таким образом, участники вычисляют  $\alpha[a; f_a]_t = [\alpha \cdot a; f_{\alpha \cdot a}]_t$ ,  $f_{\alpha \cdot a} = \alpha \cdot f_a$ .





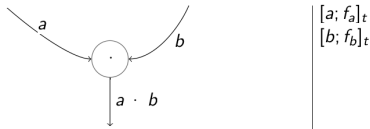
# Умножение

## Умножение

- Если входящие в вершину с меткой « $\cdot$ » ребра имеют метки  $a$  и  $b$ , то это означает, что все участники владеют наборами  $[a; f_a]_t$  и  $[b; f_b]_t$ .

## Умножение

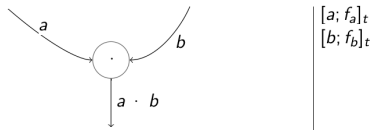
- Если входящие в вершину с меткой « $\cdot$ » ребра имеют метки  $a$  и  $b$ , то это означает, что все участники владеют наборами  $[a; f_a]_t$  и  $[b; f_b]_t$ .



- Участник с номером  $i (\in [n])$  вычисляет  $f_a(i) \cdot f_b(i)$ .

## Умножение

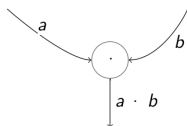
- Если входящие в вершину с меткой « $\cdot$ » ребра имеют метки  $a$  и  $b$ , то это означает, что все участники владеют наборами  $[a; f_a]_t$  и  $[b; f_b]_t$ .



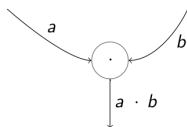
- Участник с номером  $i (\in [n])$  вычисляет  $f_a(i) \cdot f_b(i)$ .
- Таким образом, участники вычисляют  $[a; f_a]_t \star [b; f_b]_t = [a \cdot b; \hat{f}_{a \cdot b}]_{2t}$ ,  $\hat{f}_{a \cdot b} = f_a \cdot f_b$

# Умножение

- Если входящие в вершину с меткой « $\cdot$ » ребра имеют метки  $a$  и  $b$ , то это означает, что все участники владеют наборами  $[a; f_a]_t$  и  $[b; f_b]_t$ .

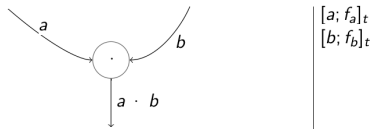

$$\begin{array}{|l} [a; f_a]_t \\ [b; f_b]_t \end{array}$$

- Участник с номером  $i \in [n]$  вычисляет  $f_a(i) \cdot f_b(i)$ .
- Таким образом, участники вычисляют  $[a; f_a]_t \star [b; f_b]_t = [a \cdot b; \hat{f}_{a \cdot b}]_{2t}$ ,  $\hat{f}_{a \cdot b} = f_a \cdot f_b$

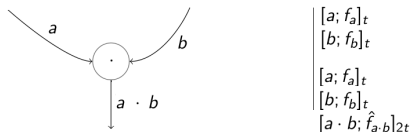

$$\begin{array}{|l} [a; f_a]_t \\ [b; f_b]_t \\ [a; f_a]_t \\ [b; f_b]_t \\ [a \cdot b; \hat{f}_{a \cdot b}]_{2t} \end{array}$$

## Умножение

- Если входящие в вершину с меткой « $\cdot$ » ребра имеют метки  $a$  и  $b$ , то это означает, что все участники владеют наборами  $[a; f_a]_t$  и  $[b; f_b]_t$ .


$$\begin{array}{l} [a; f_a]_t \\ [b; f_b]_t \end{array}$$

- Участник с номером  $i \in [n]$  вычисляет  $f_a(i) \cdot f_b(i)$ .
- Таким образом, участники вычисляют  $[a; f_a]_t \star [b; f_b]_t = [a \cdot b; \hat{f}_{a \cdot b}]_{2t}$ ,  $\hat{f}_{a \cdot b} = f_a \cdot f_b$


$$\begin{array}{l} [a; f_a]_t \\ [b; f_b]_t \\ [a; f_a]_t \\ [b; f_b]_t \\ [a \cdot b; \hat{f}_{a \cdot b}]_{2t} \end{array}$$

**Проблема:** полином степени не выше  $2t$ , а нужен не выше  $t$ .

# Умножение. Понижение степени полинома

## Умножение. Понижение степени полинома

- Пусть  $h(x) = f_a(x) \cdot f_b(x)$ . Тогда  $h(0) = f_a(0) \cdot f_b(0) = ab$  и все участники владеют набором  $[a \cdot b; h]_{2t}$ .



## Умножение. Понижение степени полинома

- Пусть  $h(x) = f_a(x) \cdot f_b(x)$ . Тогда  $h(0) = f_a(0) \cdot f_b(0) = ab$  и все участники владеют набором  $[a \cdot b; h]_{2t}$ .
- Таким образом, участник с номером  $i$  владеет значением  $h(i)$ ,  $i \in [n]$ .

## Умножение. Понижение степени полинома

- Пусть  $h(x) = f_a(x) \cdot f_b(x)$ . Тогда  $h(0) = f_a(0) \cdot f_b(0) = ab$  и все участники владеют набором  $[a \cdot b; h]_{2t}$ .
- Таким образом, участник с номером  $i$  владеет значением  $h(i)$ ,  $i \in [n]$ .
- Каждый участник  $i (\in [n])$ , используя  $(n, t + 1)$ -схему Шамира, распределяет набор  $[h(i), f_i]_t$  (полином  $f_i(z)$  выбирается  $i$ -ым участником случайно так, чтобы  $f_i(0) = h(i)$ ).

## Умножение. Понижение степени полинома

- Пусть  $h(x) = f_a(x) \cdot f_b(x)$ . Тогда  $h(0) = f_a(0) \cdot f_b(0) = ab$  и все участники владеют набором  $[a \cdot b; h]_{2t}$ .
- Таким образом, участник с номером  $i$  владеет значением  $h(i)$ ,  $i \in [n]$ .
- Каждый участник  $i (\in [n])$ , используя  $(n, t + 1)$ -схему Шамира, распределяет набор  $[h(i), f_i]_t$  (полином  $f_i(z)$  выбирается  $i$ -ым участником случайно так, чтобы  $f_i(0) = h(i)$ ).
- Пусть  $\mathbf{r} = (r_1, \dots, r_n)$  – вектор рекомбинации для коалиции  $\mathcal{P} = [n]$ . Тогда равенство

$$h(0) = \sum_{i=1}^n h(i)r_i$$

выполняется для любого полинома степени не выше  $n - 1$ . А по условию  $t < n/2$ , поэтому  $\deg(h(z)) \leq n - 1$ .

## Умножение. Понижение степени полинома

- Пусть  $h(x) = f_a(x) \cdot f_b(x)$ . Тогда  $h(0) = f_a(0) \cdot f_b(0) = ab$  и все участники владеют набором  $[a \cdot b; h]_{2t}$ .
- Таким образом, участник с номером  $i$  владеет значением  $h(i)$ ,  $i \in [n]$ .
- Каждый участник  $i (i \in [n])$ , используя  $(n, t + 1)$ -схему Шамира, распределяет набор  $[h(i), f_i]_t$  (полином  $f_i(z)$  выбирается  $i$ -ым участником случайно так, чтобы  $f_i(0) = h(i)$ ).
- Пусть  $\mathbf{r} = (r_1, \dots, r_n)$  – вектор рекомбинации для коалиции  $\mathcal{P} = [n]$ . Тогда равенство

$$h(0) = \sum_{i=1}^n h(i)r_i$$

выполняется для любого полинома степени не выше  $n - 1$ . А по условию  $t < n/2$ , поэтому  $\deg(h(z)) \leq n - 1$ .

- Так как  $\mathbf{r}$  известен всем, а также к этому моменту все участники владеют наборами  $[h(i), f_i]_t$ , то все участники могут вычислить  $\sum_{i=1}^n r_i [h(i); f_i]_t$ :

$$\sum_{i=1}^n r_i [h(i); f_i]_t = \left[ \sum_{i=1}^n r_i h(i); \sum_{i=1}^n r_i f_i \right]_t = [h(0); \sum_{i=1}^n r_i f_i]_t = [a \cdot b; \sum_{i=1}^n r_i f_i]_t.$$

# Умножение. Понижение степени полинома

# Умножение. Понижение степени полинома

- Таким образом, участник  $i$  вычисляет

$$\sum_{l=1}^n r_l \cdot f_l(i).$$

## Умножение. Понижение степени полинома

- Таким образом, участник  $i$  вычисляет

$$\sum_{l=1}^n r_l \cdot f_l(i).$$

- В итоге все участники владеют значением

$$[a \cdot b; \sum_{i=1}^n r_i f_i]_t.$$