Пример выполнения индивидуального задания №3

Пусть $\mathbb{F}_7$ – поле, Ω – $(3,2)$-схема Шамира, $\mathcal{P} = \{1,2,3,4,5\}$, $n = 5$, $t = 2$. Требуется трем участникам защищенным образом вычислить значение функции $f(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 \cdot x_3$. Секреты участников показаны в таблице 1.

Таблица 1: Секреты участников перед выполненем протокола

Секреты участников		
s_1	s_2	s_3
1	5	2

1 Фаза распределения долей

В соответствии с протоколом Шамира, участник i независимо от других участников выбирает полином $b_i(z)$ степени не выше $t-1$, так, чтобы свободный коэффициент равнялся значению его секрета. Выбранные полиномы указаны в таблице 2.

Таблица 2: Полиномы $b_i(z)$ участников, $\deg(b_i(z)) \leqslant t-1 = 1$

Полиномы участников		
$b_1(z)$	$b_2(z)$	$b_3(z)$
$1+z$	$5+2z$	$2+6z$

Каждый участник выполняе протокол распределения своего секрта с помощью схемы Шамира и передает полученные доли соответствующим участникам по **защищенным** каналам (см. таблицу 3).

Таблица 3: Распределение долей секретов s_i среди участников

		Доля i-ого участника				
		$i=1$	$i=2$	$i=3$	$i=4$	$i=5$
Секреты	$s_1 = 1$	$b_1(1) = 2$	$b_1(2) = 3$	$b_1(3) = 4$	$b_1(4) = 5$	$b_1(5) = 6$
	$s_2 = 5$	$b_2(1) = 0$	$b_2(2) = 2$	$b_2(3) = 4$	$b_2(4) = 6$	$b_2(5) = 1$
	$s_3 = 2$	$b_3(1) = 1$	$b_3(2) = 0$	$b_3(3) = 6$	$b_3(4) = 5$	$b_3(5) = 4$

2 Фаза арифметических вычислений

1. **Вычисление $s_2 \cdot s_3$.**

   - Каждый из участников должен перемножить доли, соответствующие второму и третьему секрету. Результат показан ниже в таблице 4.

Таблица 4: Доли участников, вычисленные по полиному $h(z) = b_2(z) \cdot b_3(z)$

Доли участников				
$h(1)$	$h(2)$	$h(3)$	$h(4)$	$h(5)$
$b_2(1) \cdot b_3(1) = 0$	$b_2(2) \cdot b_3(2) = 0$	$b_2(3) \cdot b_3(3) = 3$	$b_2(4) \cdot b_3(4) = 2$	$b_2(5) \cdot b_3(5) = 4$

- Каждый из участников, снова используя схему Шамира, распределяет свои значения $h(i)$ среди остальных участников.

Таблица 5: Полиномы $f_i(z)$ участников, $\deg(f_i(z)) \leqslant t - 1 = 1$

Полиномы участников				
$f_1(z)$	$f_2(z)$	$f_3(z)$	$f_4(z)$	$f_5(z)$
$2z$	z	3	$2 + 4z$	4

Таблица 6: Распределение долей секретов $h(i)$ среди участников

		Доля i-ого участника				
		$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$
Секреты	$h(1) = 0$	$f_1(1) = 2$	$f_1(2) = 4$	$f_1(3) = 6$	$f_1(4) = 1$	$f_1(5) = 3$
	$h(2) = 0$	$f_2(1) = 1$	$f_2(2) = 2$	$f_2(3) = 3$	$f_2(4) = 4$	$f_2(5) = 5$
	$h(3) = 3$	$f_3(1) = 3$	$f_3(2) = 3$	$f_3(3) = 3$	$f_3(4) = 3$	$f_3(5) = 3$
	$h(4) = 2$	$f_4(1) = 6$	$f_4(2) = 3$	$f_4(3) = 0$	$f_4(4) = 4$	$f_4(5) = 1$
	$h(5) = 4$	$f_5(1) = 4$	$f_5(2) = 4$	$f_5(3) = 4$	$f_5(4) = 4$	$f_5(5) = 4$

- Все участники находят вектор реконструкции $\mathbf{r} = (r_1, ..., r_5)$ для коалиции $\mathcal{P} = \{1, ..., 5\}$:

$$r_i = \prod_{j \in \{1,...,5\} \setminus \{i\}} \frac{j}{j - i}.$$

Получаем

$$\mathbf{r} = (5, 4, 3, 2, 1).$$

- Участник i вычисляет (в поле) настоящие доли, соответствующие произведению $s_2 \cdot s_3$,

$$v_i = \sum_{l=1}^{5} r_l f_l(i).$$

Получаем:

$$v_1 = 2 \cdot 5 + 1 \cdot 4 + 3 \cdot 3 + 6 \cdot 2 + 4 \cdot 1 = 4,$$
$$v_2 = 4 \cdot 5 + 2 \cdot 4 + 3 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 = 5,$$
$$v_3 = 6 \cdot 5 + 3 \cdot 4 + 3 \cdot 3 + 0 \cdot 2 + 4 \cdot 1 = 6,$$
$$v_4 = 1 \cdot 5 + 4 \cdot 4 + 3 \cdot 3 + 4 \cdot 2 + 4 \cdot 1 = 0,$$
$$v_5 = 3 \cdot 5 + 5 \cdot 4 + 3 \cdot 3 + 1 \cdot 2 + 4 \cdot 1 = 1.$$

- Таким образом, получаем распределение долей секрета $s_2 \cdot s_3$ среди участников (см. таблицу ниже)

Таблица 7: Распределение долей секрета $s_2 \cdot s_3$ среди участников

		Доля i-ого участника				
		$i=1$	$i=2$	$i=3$	$i=4$	$i=5$
Секрет	$s_2 \cdot s_3$	$v_1 = 4$	$v_2 = 5$	$v_3 = 6$	$v_4 = 0$	$v_5 = 1$

2. **Вычисление** $s_1 + s_2 \cdot s_3$**.**

   - Каждый участник i вычисляет $b_1(i) + v_i$. Результат см. в таблице

Таблица 8: Распределение долей секрета $s_1 + s_2 \cdot s_3$ среди участников

		Доля i-ого участника				
		$i=1$	$i=2$	$i=3$	$i=4$	$i=5$
Секрет	$s_1 + s_2 \cdot s_3$	$b_1(1) + v_1 = 6$	$b_1(2) + v_2 = 1$	$b_1(3) + v_3 = 3$	$b_1(4) + v_4 = 5$	$b_1(5) + v_5 = 0$

3 Фаза восстановления выходных значений

Каждый участник i по защищенным каналам передает значение $w_i = b_1(i) + v_i$ другим участнкам. В итоге каждый будет иметь набор w_1,...,w_5. Используя вектор рекомбинации $\mathbf{r}$ каждый вычисляет (в поле)

$$\sum_{l=1}^{5} r_l w_l = 6 \cdot 5 + 1 \cdot 4 + 3 \cdot 3 + 5 \cdot 2 + 1 \cdot 0 = 4 = s_1 + s_2 \cdot s_3 = 1 + 5 \cdot 2.$$