Лекция 12. Схемы разделения секрета

Косолапов Ю.В.

ЮФУ

25 ноября 2020 г.

Содержание

Постановка задачи

Постановка задачи

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

Постановка задачи

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $s \in \mathcal{S}$ — некоторый секрет, который известен *дилеру* D (в общем случае дилер может выступать в роли одного из участников).

Постановка задачи

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $s \in \mathcal{S}$ — некоторый секрет, который известен *дилеру* D (в общем случае дилер может выступать в роли одного из участников).
- **Требование**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации каждый участник не смог восстановить секрет, а, собравшись вместе, они смогли этот секрет восстановить.

Постановка задачи

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $s \in \mathcal{S}$ — некоторый секрет, который известен *дилеру* D (в общем случае дилер может выступать в роли одного из участников).
- **Требование**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации каждый участник не смог восстановить секрет, а, собравшись вместе, они смогли этот секрет восстановить.
- **Требование (обобщенное)**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации **любая коалиция мощности t и менее** не смогла восстановить секрет, а **любая коалиция мощности r и более** смогла этот секрет восстановить.

Постановка задачи

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $s \in \mathcal{S}$ — некоторый секрет, который известен *дилеру* D (в общем случае дилер может выступать в роли одного из участников).
- **Требование**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации каждый участник не смог восстановить секрет, а, собравшись вместе, они смогли этот секрет восстановить.
- **Требование (обобщенное)**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации **любая коалиция мощности t и менее** не смогла восстановить секрет, а **любая коалиция мощности r и более** смогла этот секрет восстановить.

Варианты

Постановка задачи

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $s \in \mathcal{S}$ — некоторый секрет, который известен *дилеру* D (в общем случае дилер может выступать в роли одного из участников).
- **Требование**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации каждый участник не смог восстановить секрет, а, собравшись вместе, они смогли этот секрет восстановить.
- **Требование (обобщенное)**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации **любая коалиция мощности t и менее** не смогла восстановить секрет, а **любая коалиция мощности r и более** смогла этот секрет восстановить.

Варианты

- Разрезать битовое представление секрета s на n частей и каждому участнику передать его долю.

Постановка задачи

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $s \in \mathcal{S}$ — некоторый секрет, который известен *дилеру* D (в общем случае дилер может выступать в роли одного из участников).
- **Требование**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации каждый участник не смог восстановить секрет, а, собравшись вместе, они смогли этот секрет восстановить.
- **Требование (обобщенное)**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации **любая коалиция мощности t и менее** не смогла восстановить секрет, а **любая коалиция мощности r и более** смогла этот секрет восстановить.

Варианты

- Разрезать битовое представление секрета s на n частей и каждому участнику передать его долю. Недостатки?

Постановка задачи

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $s \in \mathcal{S}$ — некоторый секрет, который известен *дилеру* D (в общем случае дилер может выступать в роли одного из участников).
- **Требование**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации каждый участник не смог восстановить секрет, а, собравшись вместе, они смогли этот секрет восстановить.
- **Требование (обобщенное)**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации **любая коалиция мощности t и менее** не смогла восстановить секрет, а **любая коалиция мощности r и более** смогла этот секрет восстановить.

Варианты

- Разрезать битовое представление секрета s на n частей и каждому участнику передать его долю. Недостатки?
- Зашифровать s с помощью блочного шифра, разрезать битовое представление шифрограммы на n частей и передать каждому участнику соответствующую долю и ключ шифрования.

Постановка задачи

- Пусть $\mathcal{P} = \{1, ..., n\}$ — множество участников.
- $s \in \mathcal{S}$ — некоторый секрет, который известен *дилеру* D (в общем случае дилер может выступать в роли одного из участников).
- **Требование**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации каждый участник не смог восстановить секрет, а, собравшись вместе, они смогли этот секрет восстановить.
- **Требование (обобщенное)**: дилер должен разделить секрет s среди участников $\mathcal{P}$ так, чтобы по полученной информации **любая коалиция мощности t и менее** не смогла восстановить секрет, а **любая коалиция мощности r и более** смогла этот секрет восстановить.

Варианты

- Разрезать битовое представление секрета s на n частей и каждому участнику передать его долю. Недостатки?
- Зашифровать s с помощью блочного шифра, разрезать битовое представление шифрограммы на n частей и передать каждому участнику соответствующую долю и ключ шифрования. Недостатки?

Определение схемы разделения секрета (СРС)

- **Схема разделения секрета** (СРС)

$$\Omega = (\mathcal{P}, \mathcal{S}, \textsc{Share}, \textsc{Recon}, \Gamma(\Omega), \mathcal{A}(\Omega))$$

состоит из следующих объектов:

Определение схемы разделения секрета (СРС)

- **Схема разделения секрета** (СРС)

$$\Omega = (\mathcal{P}, \mathcal{S}, \textsc{Share}, \textsc{Recon}, \Gamma(\Omega), \mathcal{A}(\Omega))$$

состоит из следующих объектов:

  - множество участников $\mathcal{P}$ мощности n;

Определение схемы разделения секрета (СРС)

- **Схема разделения секрета** (СРС)

$$\Omega = (\mathcal{P}, \mathcal{S}, \textsc{Share}, \textsc{Recon}, \Gamma(\Omega), \mathcal{A}(\Omega))$$

состоит из следующих объектов:

  - множество участников $\mathcal{P}$ мощности n;
  - множество возможных значений секретов $\mathcal{S}$;

Определение схемы разделения секрета (СРС)

- **Схема разделения секрета** (СРС)

$$\Omega = (\mathcal{P}, \mathcal{S}, \textsc{Share}, \textsc{Recon}, \Gamma(\Omega), \mathcal{A}(\Omega))$$

состоит из следующих объектов:

  - множество участников $\mathcal{P}$ мощности n;
  - множество возможных значений секретов $\mathcal{S}$;
  - протокола разделения секрета $\textsc{Share}$;

Определение схемы разделения секрета (СРС)

- **Схема разделения секрета** (СРС)

$$\Omega = (\mathcal{P}, \mathcal{S}, \textsc{Share}, \textsc{Recon}, \Gamma(\Omega), \mathcal{A}(\Omega))$$

состоит из следующих объектов:

  - множество участников $\mathcal{P}$ мощности n;
  - множество возможных значений секретов $\mathcal{S}$;
  - протокола разделения секрета $\textsc{Share}$;
  - протокола восстановления секрета $\textsc{Recon}$;

Определение схемы разделения секрета (СРС)

- **Схема разделения секрета** (СРС)

$$\Omega = (\mathcal{P}, \mathcal{S}, \textsc{Share}, \textsc{Recon}, \Gamma(\Omega), \mathcal{A}(\Omega))$$

состоит из следующих объектов:

  - множество участников $\mathcal{P}$ мощности n;
  - множество возможных значений секретов $\mathcal{S}$;
  - протокола разделения секрета $\textsc{Share}$;
  - протокола восстановления секрета $\textsc{Recon}$;
  - структуры доступа $\Gamma(\Omega)$;

Определение схемы разделения секрета (СРС)

- **Схема разделения секрета** (СРС)

$$\Omega = (\mathcal{P}, \mathcal{S}, \textsc{Share}, \textsc{Recon}, \Gamma(\Omega), \mathcal{A}(\Omega))$$

состоит из следующих объектов:

  - множество участников $\mathcal{P}$ мощности n;
  - множество возможных значений секретов $\mathcal{S}$;
  - протокола разделения секрета $\textsc{Share}$;
  - протокола восстановления секрета $\textsc{Recon}$;
  - структуры доступа $\Gamma(\Omega)$;
  - структуры противника $\mathcal{A}(\Omega)$.

- **Участники** (пользователи, процессы и т. п.) из $\mathcal{P}$ обычно нумеруются натуральными числами от 1 до n: $\mathcal{P} = [n]$.

Протокол SHARE

Протокол SHARE

- Входом **протокола разделения секрета** SHARE является секрет s из $\mathcal{S}$, выбранный с вероятностью $p(s)$, а выходом – набор долей секрета $x(1),...,x(n)$, которые распределяются среди участников множества $\mathcal{P}$: i-ому участнику передается доля $x(i)$:

$$s \rightarrow \text{SHARE} \rightarrow (x(1), ..., x(n)).$$

Протокол SHARE

- Входом **протокола разделения секрета** SHARE является секрет s из $\mathcal{S}$, выбранный с вероятностью $p(s)$, а выходом – набор долей секрета $x(1),...,x(n)$, которые распределяются среди участников множества $\mathcal{P}$: i-ому участнику передается доля $x(i)$:

$$s \to \text{SHARE} \to (x(1), ..., x(n)).$$

- Множество возможных значений долей секрета для i-ого участника обозначим $\mathcal{X}(i)$.

Протокол SHARE

- Входом **протокола разделения секрета** SHARE является секрет s из $\mathcal{S}$, выбранный с вероятностью $p(s)$, а выходом – набор долей секрета $x(1),...,x(n)$, которые распределяются среди участников множества $\mathcal{P}$: i-ому участнику передается доля $x(i)$:

$$s \to \text{SHARE} \to (x(1), ..., x(n)).$$

- Множество возможных значений долей секрета для i-ого участника обозначим $\mathcal{X}(i)$.
- Протокол разделения секрета обычно выполняется специальным участником, который называется **дилером**.

Протокол RECON. Структура доступа.

Протокол Recon. Структура доступа.

- **Протокол восстановления секрета** Recon реализует алгоритм восстановления секрета по подмножеству долей секрета:

$$(x(i_1), ..., x(i_v)) \to \text{Recon} \to \{s, \text{error}\},$$

$\{i_1, ..., i_v\} (\subseteq \mathcal{P})$ – некоторая коалиция.

Протокол Recon. Структура доступа.

- **Протокол восстановления секрета** Recon реализует алгоритм восстановления секрета по подмножеству долей секрета:

$$(x(i_1), ..., x(i_v)) \to \text{Recon} \to \{s, \text{error}\},$$

$\{i_1, ..., i_v\} (\subseteq \mathcal{P})$ – некоторая коалиция.

- Всякое подмножество $B (\subset \mathcal{P})$ называется **правомочной коалицией**, если долей секрета участников из множества B достаточно для восстановления исходного секрета s.

Протокол Recon. Структура доступа.

- **Протокол восстановления секрета** Recon реализует алгоритм восстановления секрета по подмножеству долей секрета:

$$(x(i_1), ..., x(i_v)) \to \text{Recon} \to \{s, \text{error}\},$$

$\{i_1, ..., i_v\} (\subseteq \mathcal{P})$ – некоторая коалиция.

- Всякое подмножество $B (\subset \mathcal{P})$ называется **правомочной коалицией**, если долей секрета участников из множества B достаточно для восстановления исходного секрета s.
- Множество всех правомочных коалиций называется **структурой доступа** $\Gamma(\Omega)$.

Совершенная СРС

Определение

Схема разделения секрета Ω называется совершенной, если выполняются следующие свойства:

1. для каждого $B \in \Gamma(\Omega)$, для каждого $s \in \mathcal{S}$ и для каждого $\nu(i)$, где $i \in B$:
$$\Pr\{S = s | X(i) = \nu(i), i \in B\} \in \{0, 1\};$$
2. для каждого $A \in 2^{\mathcal{P}} \backslash \Gamma(\Omega)$, для каждого $s \in \mathcal{S}$ и для каждого $\nu(i)$, где $i \in A$:
$$\Pr\{S = s | X(i) = \nu(i), i \in A\} = \Pr\{S = s\},$$

где $X(i)$ — случайная величина, моделирующая появление значений доли секрета у i-ого участника.

Структура противника. Идеальная СРС

Структура противника. Идеальная СРС

- Если для множества $A(\subset \mathcal{P})$ протокол восстановления секрета $\textsc{Recon}$ не позволяет получить информацию о секрете, то A называется **неправомочной** коалицией.

Структура противника. Идеальная СРС

- Если для множества $A(\subset \mathcal{P})$ протокол восстановления секрета $\textsc{Recon}$ не позволяет получить информацию о секрете, то A называется **неправомочной** коалицией.
- Множество $\mathcal{A}(\Omega)$ всех неправомочных коалиций называется **структурой противника**.

Идеальная СРС

Схема разделения секрета называется идеальной, если число битов, содержащееся в каждой доле секрета, равно числу битов, содержащихся в самом секрете. В терминах теории информации:

$$\mathrm{H}(S) = \mathrm{H}(X(1)) = \ldots = \mathrm{H}(X(n)),$$

где $H(\cdot)$ — энтропия дискретной случайной величины.

Пример 1

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

Пример 1

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

- SHARE: заключается в генерации по секрету $s \in \mathcal{S}$ трех чисел: s_1, s_2, s_3, где $s_1, s_2 \in_R \mathbb{Z}_m$,

$$s_3 = s - (s_1 + s_2) \bmod m. \tag{1}$$

Доли секрета имеют вид $x(i) = s_i$, $i = 1, ..., 3$.

Пример 1

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

- SHARE: заключается в генерации по секрету $s \in \mathcal{S}$ трех чисел: s_1, s_2, s_3, где $s_1, s_2 \in_R \mathbb{Z}_m$,

$$s_3 = s - (s_1 + s_2) \bmod m. \tag{1}$$

  Доли секрета имеют вид $x(i) = s_i$, $i = 1, ..., 3$.

- RECON: сложение всех долей секрета по модулю m.

Пример 1

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

- SHARE: заключается в генерации по секрету $s \in \mathcal{S}$ трех чисел: s_1, s_2, s_3, где $s_1, s_2 \in_R \mathbb{Z}_m$,

$$s_3 = s - (s_1 + s_2) \bmod m. \tag{1}$$

  Доли секрета имеют вид $x(i) = s_i$, $i = 1, ..., 3$.
- RECON: сложение всех долей секрета по модулю m.
- Структура доступа $\Gamma(\Omega) = \{1, 2, 3\}$.

Пример 1

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

- SHARE: заключается в генерации по секрету $s \in \mathcal{S}$ трех чисел: s_1, s_2, s_3, где $s_1, s_2 \in_R \mathbb{Z}_m$,

$$s_3 = s - (s_1 + s_2) \bmod m. \tag{1}$$

  Доли секрета имеют вид $x(i) = s_i$, $i = 1, ..., 3$.
- RECON: сложение всех долей секрета по модулю m.
- Структура доступа $\Gamma(\Omega) = \{1, 2, 3\}$.
- Структура противника

$$\mathcal{A}(\Omega) = \{\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{1, 3\},\ \{2, 3\}\ \}.$$

Пример 1

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

- SHARE: заключается в генерации по секрету $s \in \mathcal{S}$ трех чисел: s_1, s_2, s_3, где $s_1, s_2 \in_R \mathbb{Z}_m$,

$$s_3 = s - (s_1 + s_2) \bmod m. \tag{1}$$

  Доли секрета имеют вид $x(i) = s_i$, $i = 1, ..., 3$.
- RECON: сложение всех долей секрета по модулю m.
- Структура доступа $\Gamma(\Omega) = \{1, 2, 3\}$.
- Структура противника

$$\mathcal{A}(\Omega) = \{\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{1, 3\},\ \{2, 3\}\ \}.$$

- Эта схема разделения секрета является идеальной и совершенной.

Пример 2

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

Пример 2

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

- SHARE: заключается в генерации по секрету $s \in \mathcal{S}$ трех чисел: s_1, s_2, s_3, где $s_1, s_2 \in_R \mathbb{Z}_p$, а s_3 вычисляется в соответствии с правилом

$$s_3 = s - (s_1 + s_2) \bmod m. \tag{2}$$

Доли секрета имеют вид: $x(i) = (s_l, s_j)$, $i = 1, ..., 3$, $i \neq l$, $i \neq j$.

Пример 2

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

- SHARE: заключается в генерации по секрету $s \in \mathcal{S}$ трех чисел: s_1, s_2, s_3, где $s_1, s_2 \in_R \mathbb{Z}_p$, а s_3 вычисляется в соответствии с правилом

$$s_3 = s - (s_1 + s_2) \bmod m. \tag{2}$$

  Доли секрета имеют вид: $x(i) = (s_l, s_j)$, $i = 1, ..., 3$, $i \neq l$, $i \neq j$.
- RECON: аналогично (могут выполнить любые два участника).

Пример 2

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

- SHARE: заключается в генерации по секрету $s \in \mathcal{S}$ трех чисел: s_1, s_2, s_3, где $s_1, s_2 \in_R \mathbb{Z}_p$, а s_3 вычисляется в соответствии с правилом

$$s_3 = s - (s_1 + s_2) \bmod m. \tag{2}$$

  Доли секрета имеют вид: $x(i) = (s_l, s_j)$, $i = 1, ..., 3$, $i \neq l$, $i \neq j$.
- RECON: аналогично (могут выполнить любые два участника).
- Структура доступа $\Gamma(\Omega) = \{ \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} \}$.

Пример 2

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

- SHARE: заключается в генерации по секрету $s \in \mathcal{S}$ трех чисел: s_1, s_2, s_3, где $s_1, s_2 \in_R \mathbb{Z}_p$, а s_3 вычисляется в соответствии с правилом

$$s_3 = s - (s_1 + s_2) \bmod m. \tag{2}$$

  Доли секрета имеют вид: $x(i) = (s_l, s_j)$, $i = 1, ..., 3$, $i \neq l$, $i \neq j$.
- RECON: аналогично (могут выполнить любые два участника).
- Структура доступа $\Gamma(\Omega) = \{ \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} \}$.
- Структура противника $\mathcal{A}(\Omega) = \{ \{1\}, \{2\}, \{3\}, \}$.

Пример 2

Пусть $\mathcal{S} = \mathbb{Z}_m$, m – большое число, $m \geqslant 2$, $n = 3$, $\mathcal{P} = [3] = \{1, 2, 3\}$, секрет выбирается в соответствии с **равновероятным распределением**.

- SHARE: заключается в генерации по секрету $s \in \mathcal{S}$ трех чисел: s_1, s_2, s_3, где $s_1, s_2 \in_R \mathbb{Z}_p$, а s_3 вычисляется в соответствии с правилом

$$s_3 = s - (s_1 + s_2) \bmod m. \tag{2}$$

  Доли секрета имеют вид: $x(i) = (s_l, s_j)$, $i = 1, ..., 3$, $i \neq l$, $i \neq j$.
- RECON: аналогично (могут выполнить любые два участника).
- Структура доступа $\Gamma(\Omega) = \{ \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} \}$.
- Структура противника $\mathcal{A}(\Omega) = \{ \{1\}, \{2\}, \{3\}, \}$.
- Эта схема разделения секрета является совершенной, но не является идеальной (почему?).

Свойства структуры доступа и структуры противника

Для $\mathcal{A}(\Omega)$ и $\Gamma(\Omega)$ выполняются следующие свойства:

Свойства структуры доступа и структуры противника

Для $\mathcal{A}(\Omega)$ и $\Gamma(\Omega)$ выполняются следующие свойства:

1. $\varnothing \in \mathcal{A}(\sigma)$;

Свойства структуры доступа и структуры противника

Для $\mathcal{A}(\Omega)$ и $\Gamma(\Omega)$ выполняются следующие свойства:

1. $\varnothing \in \mathcal{A}(\sigma)$;
2. $\mathcal{P} \in \Gamma(\Omega)$;

Свойства структуры доступа и структуры противника

Для $\mathcal{A}(\Omega)$ и $\Gamma(\Omega)$ выполняются следующие свойства:

1. $\varnothing \in \mathcal{A}(\sigma)$;
2. $\mathcal{P} \in \Gamma(\Omega)$;
3. $A \in \mathcal{A}(\Omega),\ A' \subseteq A \Rightarrow A' \in \mathcal{A}(\Omega)$;

Свойства структуры доступа и структуры противника

Для $\mathcal{A}(\Omega)$ и $\Gamma(\Omega)$ выполняются следующие свойства:

1. $\varnothing \in \mathcal{A}(\sigma)$;
2. $\mathcal{P} \in \Gamma(\Omega)$;
3. $A \in \mathcal{A}(\Omega),\ A' \subseteq A \Rightarrow A' \in \mathcal{A}(\Omega)$;
4. $B \in \Gamma(\Omega),\ B' \supseteq B \Rightarrow B' \in \Gamma(\Omega)$ (свойство монотонности);

Свойства структуры доступа и структуры противника

Для $\mathcal{A}(\Omega)$ и $\Gamma(\Omega)$ выполняются следующие свойства:

1. $\varnothing \in \mathcal{A}(\sigma)$;
2. $\mathcal{P} \in \Gamma(\Omega)$;
3. $A \in \mathcal{A}(\Omega),\ A' \subseteq A \Rightarrow A' \in \mathcal{A}(\Omega)$;
4. $B \in \Gamma(\Omega),\ B' \supseteq B \Rightarrow B' \in \Gamma(\Omega)$ (свойство монотонности);
5. $\Gamma(\Omega) \cap \mathcal{A}(\Omega) = \varnothing$;

Свойства структуры доступа и структуры противника

Для $\mathcal{A}(\Omega)$ и $\Gamma(\Omega)$ выполняются следующие свойства:

1. $\varnothing \in \mathcal{A}(\sigma)$;
2. $\mathcal{P} \in \Gamma(\Omega)$;
3. $A \in \mathcal{A}(\Omega),\ A' \subseteq A \Rightarrow A' \in \mathcal{A}(\Omega)$;
4. $B \in \Gamma(\Omega),\ B' \supseteq B \Rightarrow B' \in \Gamma(\Omega)$ (свойство монотонности);
5. $\Gamma(\Omega) \cap \mathcal{A}(\Omega) = \varnothing$;
6. $\Gamma(\Omega) \cup \mathcal{A}(\Omega) \subseteq 2^{\mathcal{P}}$.

Замечание

Если $2^{\mathcal{P}} \backslash (\Gamma(\Omega) \cup \mathcal{A}(\Omega)) \neq \varnothing$, то элементы этого мультимножества не являются ни правомочными коалициями, ни неправомочными коалициями. Другими словами, если $A \in 2^{\mathcal{P}} \backslash (\Gamma(\Omega) \cup \mathcal{A}(\Omega))$, $A \neq \varnothing$, то коалиция A не может однозначно восстановить секрет, однако может получить ненулевую информацию о нем. В терминах теории информации:

$$0 < \frac{\mathrm{I}(S; (X(i))_{i \in A})}{\mathrm{H}(S)} < 1, \tag{3}$$

где $\mathrm{I}(X; Y)$ – взаимная информация для случайных величин X и Y.

Пороговая СРС

Пусть Ω — схема разделения секрета. Говорят, что схема Ω:

Пороговая СРС

Пусть Ω — схема разделения секрета. Говорят, что схема Ω:

1. обладает свойством t-секретности, если

$$\{A \subseteq \mathcal{P} : |A| = t\} \subseteq \mathcal{A}(\Omega);$$

Пороговая СРС

Пусть Ω — схема разделения секрета. Говорят, что схема Ω:

1. обладает свойством t-секретности, если

$$\{A \subseteq \mathcal{P} : |A| = t\} \subseteq \mathcal{A}(\Omega);$$

2. обладает свойством r-восстановления, если

$$\{B \subseteq \mathcal{P} : |B| = r\} \subseteq \Gamma(\Omega).$$

Пороговая СРС

Пусть Ω — схема разделения секрета. Говорят, что схема Ω:

1. обладает свойством t-секретности, если

$$\{A \subseteq \mathcal{P} : |A| = t\} \subseteq \mathcal{A}(\Omega);$$

2. обладает свойством r-восстановления, если

$$\{B \subseteq \mathcal{P} : |B| = r\} \subseteq \Gamma(\Omega).$$

Так как $\Gamma(\Omega) \cap \mathcal{A}(\Omega) = \varnothing$, то $t < r$.

Пороговая СРС

Пусть Ω — схема разделения секрета. Говорят, что схема Ω:

1. обладает свойством t-секретности, если

$$\{A \subseteq \mathcal{P} : |A| = t\} \subseteq \mathcal{A}(\Omega);$$

2. обладает свойством r-восстановления, если

$$\{B \subseteq \mathcal{P} : |B| = r\} \subseteq \Gamma(\Omega).$$

Так как $\Gamma(\Omega) \cap \mathcal{A}(\Omega) = \varnothing$, то $t < r$.

Определение

Если для некоторого t схема разделения секрета Ω обладает свойством $t-1$-секретности и t-восстановления, то такая схема называется **пороговой** (n, t)-схемой.

Схема Шамира. Протокол SHARE

Параметры схемы

Схема Шамира. Протокол SHARE

Параметры схемы

- $\mathcal{S} = \mathbb{F}_q$

Схема Шамира. Протокол SHARE

Параметры схемы

- $\mathcal{S} = \mathbb{F}_q$
- $\mathcal{P} = [n]$, $n < q$ (q задает максимальное число участников)

Схема Шамира. Протокол SHARE

Параметры схемы

- $\mathcal{S} = \mathbb{F}_q$
- $\mathcal{P} = [n]$, $n < q$ (q задает максимальное число участников)
- $t \in \mathbb{N}, t < n$ (t задает минимальную мощность для правомочной коалиции).

Протокол SHARE

Схема Шамира. Протокол SHARE

Параметры схемы

- $\mathcal{S} = \mathbb{F}_q$
- $\mathcal{P} = [n]$, $n < q$ (q задает максимальное число участников)
- $t \in \mathbb{N}, t < n$ (t задает минимальную мощность для правомочной коалиции).

Протокол SHARE

1. Пусть $s \in \mathcal{S}$ – секрет, который требуется разделить среди участников.

Схема Шамира. Протокол SHARE

Параметры схемы

- $\mathcal{S} = \mathbb{F}_q$
- $\mathcal{P} = [n]$, $n < q$ (q задает максимальное число участников)
- $t \in \mathbb{N}, t < n$ (t задает минимальную мощность для правомочной коалиции).

Протокол SHARE

1. Пусть $s \in \mathcal{S}$ – секрет, который требуется разделить среди участников.
2. Дилер выбирает случайно вектор $\mathbf{p} = (p_1, ..., p_{t-1})$ $(\in \mathbb{F}_q^{t-1})$ и строит полином от переменной z:

$$b(z) = s + zp_1 + ... + z^{t-1}p_{t-1}. \tag{4}$$

Схема Шамира. Протокол SHARE

Параметры схемы

- $\mathcal{S} = \mathbb{F}_q$
- $\mathcal{P} = [n]$, $n < q$ (q задает максимальное число участников)
- $t \in \mathbb{N}, t < n$ (t задает минимальную мощность для правомочной коалиции).

Протокол SHARE

1. Пусть $s \in \mathcal{S}$ – секрет, который требуется разделить среди участников.
2. Дилер выбирает случайно вектор $\mathbf{p} = (p_1, ..., p_{t-1})$ $(\in \mathbb{F}_q^{t-1})$ и строит полином от переменной z:

$$b(z) = s + zp_1 + ... + z^{t-1}p_{t-1}. \tag{4}$$

Секрет здесь – это свободный коэффициент полинома: $b(0) = s$.

Схема Шамира. Протокол SHARE

Параметры схемы

- $\mathcal{S} = \mathbb{F}_q$
- $\mathcal{P} = [n]$, $n < q$ (q задает максимальное число участников)
- $t \in \mathbb{N}, t < n$ (t задает минимальную мощность для правомочной коалиции).

Протокол SHARE

1. Пусть $s \in \mathcal{S}$ – секрет, который требуется разделить среди участников.
2. Дилер выбирает случайно вектор $\mathbf{p} = (p_1, ..., p_{t-1})$ $(\in \mathbb{F}_q^{t-1})$ и строит полином от переменной z:

$$b(z) = s + zp_1 + ... + z^{t-1}p_{t-1}. \tag{4}$$

   Секрет здесь – это свободный коэффициент полинома: $b(0) = s$.
3. Доля участника с номером i имеет вид

$$x(i) = b(i).$$

Схема Шамира. Протокол SHARE

Параметры схемы

- $\mathcal{S} = \mathbb{F}_q$
- $\mathcal{P} = [n]$, $n < q$ (q задает максимальное число участников)
- $t \in \mathbb{N}, t < n$ (t задает минимальную мощность для правомочной коалиции).

Протокол SHARE

1. Пусть $s \in \mathcal{S}$ – секрет, который требуется разделить среди участников.
2. Дилер выбирает случайно вектор $\mathbf{p} = (p_1, ..., p_{t-1})$ $(\in \mathbb{F}_q^{t-1})$ и строит полином от переменной z:

$$b(z) = s + zp_1 + ... + z^{t-1}p_{t-1}. \tag{4}$$

   Секрет здесь – это свободный коэффициент полинома: $b(0) = s$.
3. Доля участника с номером i имеет вид

$$x(i) = b(i).$$

   Другими словами, доля — это значение полинома $b(z)$ в точке i.

Схема Шамира. Протокол Recon

Протокол Recon

Схема Шамира. Протокол RECON

Протокол RECON

1. Пусть $A \subseteq \mathcal{P}$, $|A| = t$.

Схема Шамира. Протокол Recon

Протокол Recon

1. Пусть $A \subseteq \mathcal{P}$, $|A| = t$.
2. Для восстановления A использует правило:

$$s = \sum_{i \in A} x(i)\lambda_{A,i}, \quad \lambda_{A,i} = \prod_{j \in A \setminus \{i\}} \frac{j}{j - i}. \tag{5}$$

Схема Шамира. Протокол Recon

Протокол Recon

1. Пусть $A \subseteq \mathcal{P}$, $|A| = t$.
2. Для восстановления A использует правило:

$$s = \sum_{i \in A} x(i)\lambda_{A,i}, \quad \lambda_{A,i} = \prod_{j \in A \setminus \{i\}} \frac{j}{j-i}. \tag{5}$$

Обоснование

Схема Шамира. Протокол Recon

Протокол Recon

1. Пусть $A \subseteq \mathcal{P}$, $|A| = t$.
2. Для восстановления A использует правило:

$$s = \sum_{i \in A} x(i)\lambda_{A,i}, \quad \lambda_{A,i} = \prod_{j \in A \setminus \{i\}} \frac{j}{j-i}. \tag{5}$$

Обоснование

- Полнота протокола Recon вытекает из того, что любой полином $b(z)$ степени не выше $t-1$ однозначно восстанавливается по t или более парам $(i, x(i))$, где $i \in A$, $|A| \geqslant t$, используя **интерполяционный многочлен Лагранжа**:

$$b(z) = \sum_{i \in A} x(i) \prod_{j \in A \setminus \{i\}} \frac{z-j}{i-j}.$$

Схема Шамира. Протокол RECON

Протокол RECON

1. Пусть $A \subseteq \mathcal{P}$, $|A| = t$.
2. Для восстановления A использует правило:

$$s = \sum_{i \in A} x(i)\lambda_{A,i}, \quad \lambda_{A,i} = \prod_{j \in A \setminus \{i\}} \frac{j}{j-i}. \tag{5}$$

Обоснование

- Полнота протокола RECON вытекает из того, что любой полином $b(z)$ степени не выше $t-1$ однозначно восстанавливается по t или более парам $(i, x(i))$, где $i \in A$, $|A| \geqslant t$, используя **интерполяционный многочлен Лагранжа**:

$$b(z) = \sum_{i \in A} x(i) \prod_{j \in A \setminus \{i\}} \frac{z-j}{i-j}.$$

- Так как секрет представляет собой свободный коэффициент, то есть $s = b(0)$, то правило восстановления секрета имеет вид (5).

Схема Шамира. Протокол RECON (продолжение)

Схема Шамира. Протокол RECON (продолжение)

- Участники правомочной коалиции A могут восстановить не только секрет, но и весь полином $b(z)$

Схема Шамира. Протокол RECON (продолжение)

- Участники правомочной коалиции A могут восстановить не только секрет, но и весь полином $b(z)$
- Пусть $|A| = t$ (случай для $|A| > t$ сводится к случаю $|A| = t$)

Схема Шамира. Протокол RECON (продолжение)

- Участники правомочной коалиции A могут восстановить не только секрет, но и весь полином $b(z)$
- Пусть $|A| = t$ (случай для $|A| > t$ сводится к случаю $|A| = t$)
- Рассмотрим полиномы

$$\lambda_{A,i}(z) = \prod_{j \in A \setminus \{i\}} \frac{z-j}{i-j}, \quad \deg(\lambda_{A,i}(z)) \leqslant t-1.$$

Схема Шамира. Протокол RECON (продолжение)

- Участники правомочной коалиции A могут восстановить не только секрет, но и весь полином $b(z)$
- Пусть $|A| = t$ (случай для $|A| > t$ сводится к случаю $|A| = t$)
- Рассмотрим полиномы

$$\lambda_{A,i}(z) = \prod_{j \in A \setminus \{i\}} \frac{z-j}{i-j}, \quad \deg(\lambda_{A,i}(z)) \leqslant t-1.$$

- Следовательно,

$$b(z) = \sum_{i \in A} x(i)\lambda_{A,i}(z) = s + zp_1 + \ldots + z^{t-1}p_t,$$

откуда приравниванием коэффициентов при соответствующих степенях переменной z находятся коэффициенты полинома $b(z)$.

Схема Шамира. Стойкость схемы

Утверждение

Схема разделения секрета Шамира является совершенной пороговой (n, t)-схемой.

Доказательство:

Схема Шамира. Стойкость схемы

Утверждение

Схема разделения секрета Шамира является совершенной пороговой (n, t)-схемой.

Доказательство:

- Достаточно показать, что любая коалиция A мощности $t-1$ не получает информации о секрете.

Схема Шамира. Стойкость схемы

Утверждение

Схема разделения секрета Шамира является совершенной пороговой (n, t)-схемой.

Доказательство:

- Достаточно показать, что любая коалиция A мощности $t-1$ не получает информации о секрете.
- Пусть $(x(i))_{i \in A}$ — вектор долей этой коалиции. Зафиксируем произвольное значение $\hat{s}$ (возможное значение секрета).

Схема Шамира. Стойкость схемы

Утверждение

Схема разделения секрета Шамира является совершенной пороговой (n, t)-схемой.

Доказательство:

- Достаточно показать, что любая коалиция A мощности $t-1$ не получает информации о секрете.
- Пусть $(x(i))_{i \in A}$ — вектор долей этой коалиции. Зафиксируем произвольное значение $\hat{s}$ (возможное значение секрета).
- Тогда, набор из t пар

$$(0, \hat{s}), (i, x(i)), i \in A$$

уникальным образом определяет полином $\hat{b}(z)$.

Схема Шамира. Стойкость схемы

Утверждение

Схема разделения секрета Шамира является совершенной пороговой (n, t)-схемой.

Доказательство:

- Достаточно показать, что любая коалиция A мощности $t-1$ не получает информации о секрете.
- Пусть $(x(i))_{i \in A}$ — вектор долей этой коалиции. Зафиксируем произвольное значение $\hat{s}$ (возможное значение секрета).
- Тогда, набор из t пар

$$(0, \hat{s}), (i, x(i)), i \in A$$

уникальным образом определяет полином $\hat{b}(z)$.

- Таким образом, по долям коалиции A можно построить q **уникальных** полиномов, каждый из которых соответствует одному из возможных значений секрета.

Схема Шамира. Стойкость схемы

Утверждение

Схема разделения секрета Шамира является совершенной пороговой (n, t)-схемой.

Доказательство:

- Достаточно показать, что любая коалиция A мощности $t-1$ не получает информации о секрете.
- Пусть $(x(i))_{i \in A}$ — вектор долей этой коалиции. Зафиксируем произвольное значение $\hat{s}$ (возможное значение секрета).
- Тогда, набор из t пар

$$(0, \hat{s}), (i, x(i)), i \in A$$

уникальным образом определяет полином $\hat{b}(z)$.

- Таким образом, по долям коалиции A можно построить q **уникальных** полиномов, каждый из которых соответствует одному из возможных значений секрета.
- Следовательно, все возможные значения секрета равновероятны и коалиция A не получает информации о секрете.

Схема Шамира. Коэффициенты рекомбинации

Схема Шамира. Коэффициенты рекомбинации

- Выше было показано, что секрет s для правомочной коалиции A может быть представлен в виде

$$s = b(0) = \sum_{i \in A} b(i)\lambda_{A,i},$$

$$\lambda_{A,i} = \lambda_{A,i}(0) = \prod_{j \in A \setminus \{i\}} \frac{j}{j-i}, \quad i \in A. \tag{6}$$

Схема Шамира. Коэффициенты рекомбинации

- Выше было показано, что секрет s для правомочной коалиции A может быть представлен в виде

$$s = b(0) = \sum_{i \in A} b(i)\lambda_{A,i},$$

$$\lambda_{A,i} = \lambda_{A,i}(0) = \prod_{j \in A \setminus \{i\}} \frac{j}{j-i}, \quad i \in A. \tag{6}$$

- При этом коэффициенты (6) не зависят от значения секрета s и вообще от полинома $b(z)$. Эти коэффициенты зависят только от состава коалиции A.

Схема Шамира. Коэффициенты рекомбинации

- Выше было показано, что секрет s для правомочной коалиции A может быть представлен в виде

$$s = b(0) = \sum_{i \in A} b(i)\lambda_{A,i},$$

$$\lambda_{A,i} = \lambda_{A,i}(0) = \prod_{j \in A \setminus \{i\}} \frac{j}{j-i}, \quad i \in A. \tag{6}$$

- При этом коэффициенты (6) не зависят от значения секрета s и вообще от полинома $b(z)$. Эти коэффициенты зависят только от состава коалиции A.

Определение

Для (n, t)-схемы разделения секрета Шамира и правомочной коалиции A чи́сла вида (6) называются **коэффициентами рекомбинации**.

Схема Шамира. Коэффициенты рекомбинации

- Выше было показано, что секрет s для правомочной коалиции A может быть представлен в виде

$$s = b(0) = \sum_{i \in A} b(i)\lambda_{A,i},$$

$$\lambda_{A,i} = \lambda_{A,i}(0) = \prod_{j \in A \setminus \{i\}} \frac{j}{j-i}, \quad i \in A. \tag{6}$$

- При этом коэффициенты (6) не зависят от значения секрета s и вообще от полинома $b(z)$. Эти коэффициенты зависят только от состава коалиции A.

Определение

Для (n, t)-схемы разделения секрета Шамира и правомочной коалиции A чи́сла вида (6) называются **коэффициентами рекомбинации**.

Коэффициенты рекомбинации каждый участник конкретной коалиции A может вычислить самостоятельно (они не секретные).

Схема Шамира. Пример

Схема Шамира. Пример

- Пусть $n = 5$, $t = 3$, $q = 11$, $s = 7$.

Схема Шамира. Пример

- Пусть $n = 5$, $t = 3$, $q = 11$, $s = 7$.
- Построим полином $b(z)$ степени не выше $t - 1 = 2$:

$$b(x) = s + p_1 z + p_2 z^2 = 7 + 4z + z^2.$$

Схема Шамира. Пример

- Пусть $n = 5$, $t = 3$, $q = 11$, $s = 7$.
- Построим полином $b(z)$ степени не выше $t - 1 = 2$:

$$b(x) = s + p_1 z + p_2 z^2 = 7 + 4z + z^2.$$

- Вектор долей секрета имеет вид

$$(x(1), ..., x(5)) = (b(1), ..., b(5)) = (1, 8, 6, 6, 8).$$

Схема Шамира. Пример

- Пусть $n = 5$, $t = 3$, $q = 11$, $s = 7$.
- Построим полином $b(z)$ степени не выше $t - 1 = 2$:

$$b(x) = s + p_1 z + p_2 z^2 = 7 + 4z + z^2.$$

- Вектор долей секрета имеет вид

$$(x(1), ..., x(5)) = (b(1), ..., b(5)) = (1, 8, 6, 6, 8).$$

- Пусть коалиция $A = \{3, 4, 5\}$ намерена восстановить секрет. Тогда

$$\lambda_{A,3} = \prod_{j \in \{4,5\}} \frac{j}{j - i} = \left(\frac{4}{4-3}\right)\left(\frac{5}{5-3}\right) = 10 (\text{mod } 11) = 10,$$

$$\lambda_{A,4} = \prod_{j \in \{3,5\}} \frac{j}{j - i} = \left(\frac{3}{3-4}\right)\left(\frac{5}{5-4}\right) = -4 (\text{mod } 11) = 7,$$

$$\lambda_{A,5} = \prod_{j \in \{3,4\}} \frac{j}{j - i} = \left(\frac{3}{3-5}\right)\left(\frac{4}{4-5}\right) = 6 (\text{mod } 11) = 6.$$

Схема Шамира. Пример

- Пусть $n = 5$, $t = 3$, $q = 11$, $s = 7$.
- Построим полином $b(z)$ степени не выше $t - 1 = 2$:

$$b(x) = s + p_1 z + p_2 z^2 = 7 + 4z + z^2.$$

- Вектор долей секрета имеет вид

$$(x(1), ..., x(5)) = (b(1), ..., b(5)) = (1, 8, 6, 6, 8).$$

- Пусть коалиция $A = \{3, 4, 5\}$ намерена восстановить секрет. Тогда

$$\lambda_{A,3} = \prod_{j \in \{4,5\}} \frac{j}{j - i} = \left(\frac{4}{4-3}\right)\left(\frac{5}{5-3}\right) = 10 (\text{mod } 11) = 10,$$

$$\lambda_{A,4} = \prod_{j \in \{3,5\}} \frac{j}{j - i} = \left(\frac{3}{3-4}\right)\left(\frac{5}{5-4}\right) = -4 (\text{mod } 11) = 7,$$

$$\lambda_{A,5} = \prod_{j \in \{3,4\}} \frac{j}{j - i} = \left(\frac{3}{3-5}\right)\left(\frac{4}{4-5}\right) = 6 (\text{mod } 11) = 6.$$

- Восстановление секрета (по правилу (5)):

$$s = x(3)\lambda_{A,3} + x(4)\lambda_{A,4} + x(5)\lambda_{A,5} = 6 \cdot 10 + 6 \cdot 7 + 8 \cdot 6$$
$$= (60 + 42 + 48) \text{ mod } 11 = (13 \cdot 11 + 7) \text{ mod } 11 = 7.$$

Реплицированная СРС. Постановка задачи. Протокол SHARE

Постановка задачи

Реплицированная СРС. Постановка задачи. Протокол Share

Постановка задачи

- Пусть $\mathcal{P} = [n]$ – набор участников схемы, $\mathcal{S} = \mathbb{F}_q$, $\mathcal{A}(\subset 2^{\mathcal{P}})$ – **заданная** структура противника.

Реплицированная СРС. Постановка задачи. Протокол Share

Постановка задачи

- Пусть $\mathcal{P} = [n]$ – набор участников схемы, $\mathcal{S} = \mathbb{F}_q$, $\mathcal{A}(\subset 2^{\mathcal{P}})$ – **заданная** структура противника.
- Требуется построить такую СРС Ω, чтобы $\mathcal{A}(\Omega) = \mathcal{A}$.

Реплицированная СРС. Постановка задачи. Протокол Share

Постановка задачи

- Пусть $\mathcal{P} = [n]$ – набор участников схемы, $\mathcal{S} = \mathbb{F}_q$, $\mathcal{A}(\subset 2^{\mathcal{P}})$ – **заданная** структура противника.
- Требуется построить такую СРС Ω, чтобы $\mathcal{A}(\Omega) = \mathcal{A}$.

Протокол Share:

Реплицированная СРС. Постановка задачи. Протокол Share

Постановка задачи

- Пусть $\mathcal{P} = [n]$ – набор участников схемы, $\mathcal{S} = \mathbb{F}_q$, $\mathcal{A}(\subset 2^{\mathcal{P}})$ – **заданная** структура противника.
- Требуется построить такую СРС Ω, чтобы $\mathcal{A}(\Omega) = \mathcal{A}$.

Протокол Share:

1. Для каждого A из $\mathcal{A}$ дилер выбирает случайно и равновероятно число r_A из поля $\mathbb{F}_q$ так, чтобы выполнялось равенство

$$\sum_{A \in \mathcal{A}} r_A = s.$$

Реплицированная СРС. Постановка задачи. Протокол Share

Постановка задачи

- Пусть $\mathcal{P} = [n]$ – набор участников схемы, $\mathcal{S} = \mathbb{F}_q$, $\mathcal{A}(\subset 2^{\mathcal{P}})$ – **заданная** структура противника.
- Требуется построить такую СРС Ω, чтобы $\mathcal{A}(\Omega) = \mathcal{A}$.

Протокол Share:

1. Для каждого A из $\mathcal{A}$ дилер выбирает случайно и равновероятно число r_A из поля $\mathbb{F}_q$ так, чтобы выполнялось равенство

$$\sum_{A \in \mathcal{A}} r_A = s.$$

2. Для каждого A из $\mathcal{A}$ дилер передает значение r_A участникам из множества $\mathcal{P} \backslash A$. При этом участникам коалиции A значение r_A не сообщается.

Реплицированная СРС. Постановка задачи. Протокол Share

Постановка задачи

- Пусть $\mathcal{P} = [n]$ – набор участников схемы, $\mathcal{S} = \mathbb{F}_q$, $\mathcal{A}(\subset 2^{\mathcal{P}})$ – **заданная** структура противника.
- Требуется построить такую СРС Ω, чтобы $\mathcal{A}(\Omega) = \mathcal{A}$.

Протокол Share:

1. Для каждого A из $\mathcal{A}$ дилер выбирает случайно и равновероятно число r_A из поля $\mathbb{F}_q$ так, чтобы выполнялось равенство
$$\sum_{A \in \mathcal{A}} r_A = s.$$
2. Для каждого A из $\mathcal{A}$ дилер передает значение r_A участникам из множества $\mathcal{P} \backslash A$. При этом участникам коалиции A значение r_A не сообщается.
3. В результате выполнения этого протокола участник i получит долю $x(i)$ вида
$$x(i) = \{r_A | i \notin A, A \in \mathcal{A}\}.$$

Реплицированная СРС. Протокол RECON

Замечание

Реплицированная СРС. Протокол Recon

Замечание

- Протокол Share строит доли так, чтобы любое множество из $\mathcal{A}$ было неправомочной коалицией.

Реплицированная СРС. Протокол Recon

Замечание

- Протокол Share строит доли так, чтобы любое множество из $\mathcal{A}$ было неправомочной коалицией.
- Если $\mathcal{A}$ – произвольный набор подмножеств множества $\mathcal{P}$ ($\mathcal{P} \notin \mathcal{A}$), то в реплицированной СРС Ω структура противника имеет вид

$$\mathcal{A}(\Omega) = \mathcal{A} \cup \{A' \colon A' \subset A, A \in \mathcal{A}\}. \tag{7}$$

Реплицированная СРС. Протокол Recon

Замечание

- Протокол Share строит доли так, чтобы любое множество из $\mathcal{A}$ было неправомочной коалицией.
- Если $\mathcal{A}$ – произвольный набор подмножеств множества $\mathcal{P}$ ($\mathcal{P} \notin \mathcal{A}$), то в реплицированной СРС Ω структура противника имеет вид

$$\mathcal{A}(\Omega) = \mathcal{A} \cup \{A' \colon A' \subset A, A \in \mathcal{A}\}. \tag{7}$$

- Это следует из того, что если A – неправомочная коалиция, то и любое его подмножество A' также является неправомочной коалицией.

Реплицированная СРС. Протокол RECON

Замечание

- Протокол SHARE строит доли так, чтобы любое множество из $\mathcal{A}$ было неправомочной коалицией.
- Если $\mathcal{A}$ – произвольный набор подмножеств множества $\mathcal{P}$ ($\mathcal{P} \notin \mathcal{A}$), то в реплицированной СРС Ω структура противника имеет вид

$$\mathcal{A}(\Omega) = \mathcal{A} \cup \{A' \colon A' \subset A, A \in \mathcal{A}\}. \tag{7}$$

- Это следует из того, что если A – неправомочная коалиция, то и любое его подмножество A' также является неправомочной коалицией.
- Поэтому далее предполагается, что для реплицированной СРС во множестве $\mathcal{A}$ нет элементов $A(\subset \mathcal{P})$ и $B(\subset \mathcal{P})$, для которых либо $A \subset B$, либо $B \subset A$.

Реплицированная СРС. Протокол Recon

Замечание

- Протокол Share строит доли так, чтобы любое множество из $\mathcal{A}$ было неправомочной коалицией.
- Если $\mathcal{A}$ – произвольный набор подмножеств множества $\mathcal{P}$ ($\mathcal{P} \notin \mathcal{A}$), то в реплицированной СРС Ω структура противника имеет вид

$$\mathcal{A}(\Omega) = \mathcal{A} \cup \{A' \colon A' \subset A, A \in \mathcal{A}\}. \tag{7}$$

- Это следует из того, что если A – неправомочная коалиция, то и любое его подмножество A' также является неправомочной коалицией.
- Поэтому далее предполагается, что для реплицированной СРС во множестве $\mathcal{A}$ нет элементов $A(\subset \mathcal{P})$ и $B(\subset \mathcal{P})$, для которых либо $A \subset B$, либо $B \subset A$.

Протокол Recon:

- Состоит в вычислении коалицией $B \subseteq \mathcal{P}$ суммы вида

$$\sum_{A:\exists i \in B \setminus A} r_A.$$

Пример

Example

Пример

Пример

Example

Пример

- $\mathcal{P} = [4]$, $s(\in \mathbb{F}_q)$.

Пример

Example

Пример

- $\mathcal{P} = [4]$, $s (\in \mathbb{F}_q)$.
- $\mathcal{A} = \{A_1 = \{1, 3\}, A_2 = \{2\}, A_3 = \{3, 4\}\}$.

Пример

Example

Пример

- $\mathcal{P} = [4]$, $s (\in \mathbb{F}_q)$.
- $\mathcal{A} = \{A_1 = \{1, 3\}, A_2 = \{2\}, A_3 = \{3, 4\}\}$.
- Пусть r_{A_1}, r_{A_2} и r_{A_3} – такие числа, что

$$r_{A_1} + r_{A_2} + r_{A_3} = s. \tag{8}$$

Пример

Example

Пример

- $\mathcal{P} = [4]$, $s(\in \mathbb{F}_q)$.
- $\mathcal{A} = \{A_1 = \{1,3\}, A_2 = \{2\}, A_3 = \{3,4\}\}$.
- Пусть r_{A_1}, r_{A_2} и r_{A_3} – такие числа, что

$$r_{A_1} + r_{A_2} + r_{A_3} = s. \tag{8}$$

- Распределение долей секретов:

Участник	Доля
1	r_{A_2}, r_{A_3}
2	r_{A_1}, r_{A_3}
3	r_{A_2}
4	r_{A_1}, r_{A_2}

Заключение

Спасибо за внимание!