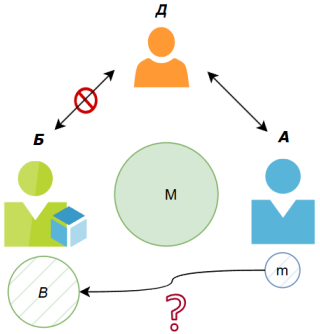
РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Протокол анонимного подтверждения наличия элемента в рассматриваемом множестве

Хуцаева Алтана, Беззатеев Сергей

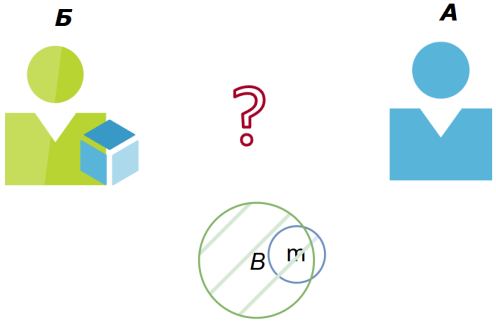
ИТМО, ГУАП

При поддержке государственного задания FSER-2025-0003

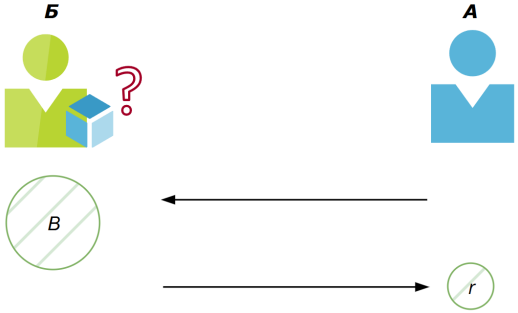


- Сторона ***А*** хочет проверить **принадлежность** элемента m множеству стороны ***Б***, не раскрывая сам элемент m
- Стороне ***А*** требуется **криптографически проверяемый ответ**, который можно предъявить третьей стороне

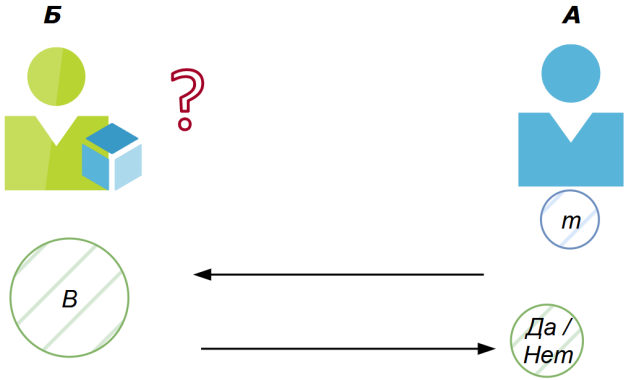
Протокол пересечения закрытых множеств (Private Set Intersection, PSI) – криптографический протокол, позволяющий участникам по их секретным множествам найти пересечение без раскрытия дополнительной информации



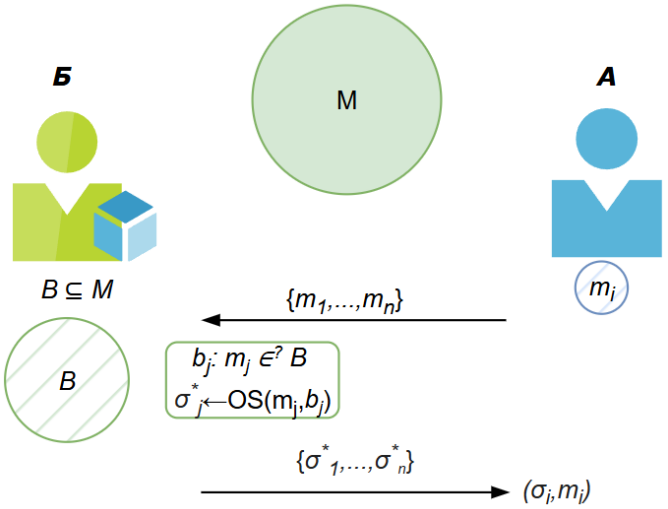
Протокол получения скрытой информации (Private Information Retrieval, PIR) – криптографический протокол приватного запроса к базе данных,позволяющий пользователю получить нужную запись, не раскрывая серверу, какой именно элемент запрашивается



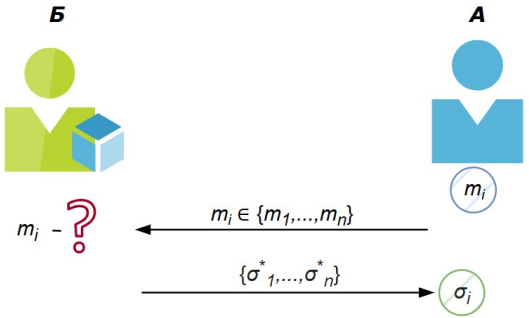
Протокол скрытой проверки принадлежности (Private Membership Test, PMT) – криптографический протокол, позволяющий клиенту скрыть свой запрос при проверке наличия соответствующих данных в базе сервера



Протокол	Решаемая задача	Гарантия принадлежности
PSI	Поиск общих элементов множеств	Нет
PIR	Скрытое извлечение записи по индексу	Нет
PMT	Скрытая проверка наличия элемента в базе сервера	Нет


Б
M
A
$B \subseteq M$
$\{m_1,\ldots,m_n\}$
m_i
B
b_j: $m_j \in^? B$
$\sigma^*_j \leftarrow OS(m_j,b_j)$
$\{\sigma^*_1,\ldots,\sigma^*_n\}$
(σ_i,m_i)

Забывчивая подпись 1-из-n (*Oblivious Signature, OS*) – интерактивный протокол подписи, позволяющий получить подпись на одно из n сообщений без раскрытия подписанту выбранного сообщения



	Сторона *А*		**Сторона *Б***
2 :	$m \in M, pp_B$		$B \subseteq M, sk_B$
3 :	$\mathbf{y} \leftarrow F(m)$		
4 :	$\mathbf{y} = (y_1, \ldots, y_n)$		
5 :	$(\mathsf{req}, \mathsf{st}) \leftarrow \mathsf{OS.Sign}(pp_B, \mathbf{y})$		
6 :		$\xrightarrow{\mathbf{y}, \mathsf{req}}$	
7 :			$\forall i \in \{1, \ldots, n\}:$
8 :			$b_i \leftarrow (y_i \in B \ ? \ 1 : 0)$
9 :			$t_i \leftarrow \mathsf{timestamp}()$
10 :			$y_i^* \leftarrow (y_i \parallel b_i \parallel t_i)$
11 :			$\sigma_i' \leftarrow \mathsf{OS.Sign}(sk_B, y_i^*, \mathsf{req})$

12: $\boldsymbol{\sigma}' \leftarrow \{\sigma'_1, \ldots, \sigma'_n\}$

13: $\xleftarrow{\boldsymbol{\sigma}', \mathbf{y}^*}$

14: $(b, t) \leftarrow \mathsf{Parse}(\mathbf{y}^*, j), m = y_j$

15: $m^* \leftarrow (m \parallel b \parallel t)$

16: $(m^*, \sigma) \leftarrow \mathsf{OS.Sign}(\mathsf{st}, \boldsymbol{\sigma}')$

17: $\mathsf{Token} \leftarrow (m^*, \sigma)$

$$F\colon M \to M^n$$
$$F(m) = (f_1(m), \ldots, f_n(m)),$$
$$\text{где } f_i\colon M \to M$$

- **Попарная различность элементов**: $\forall m \in M, \forall i \neq j\colon f_i(m) \neq f_j(m)$
  Пример: $F(m_1) = (m_1, m_2, m_3), \quad F(m_4) = (m_4, m_5, m_6)$
- **Инвариантность на элементах образа**:
  $\forall m \in M, \forall i \in \{1, \ldots, n\}\colon F(f_i(m)) = F(m)$
  Пример: $F(m_1) = F(m_2) = F(m_3) = (m_1, m_2, m_3)$
- **Наличие самого элемента в векторе**: $\forall m \in M\ \exists! i \in \{1, \ldots, n\}\colon f_i(m) = m$

Функция F разбивает множество M на непересекающиеся подмножества мощности n
$|M| = N,\ N = n \cdot L$

Вариант 1: разбиение M

- выбирается разбиение M на подмножества фиксированного размера
- каждому элементу соответствует определенное подмножество

Преимущество

Гибкая настройка подмножеств

Недостаток

Требуется хранить подмножества

Вариант 2: модульная арифметика

Для $m \in M$:

$$f_i(m) = (m \bmod L) + (i-1)L$$

$$F(m) = \{\, m \bmod L,\ (m \bmod L) + L,\ \dots \}$$

Преимущество

Простое и быстрое вычисление

Недостаток

Нет гибкой настройки подмножеств

Анонимность

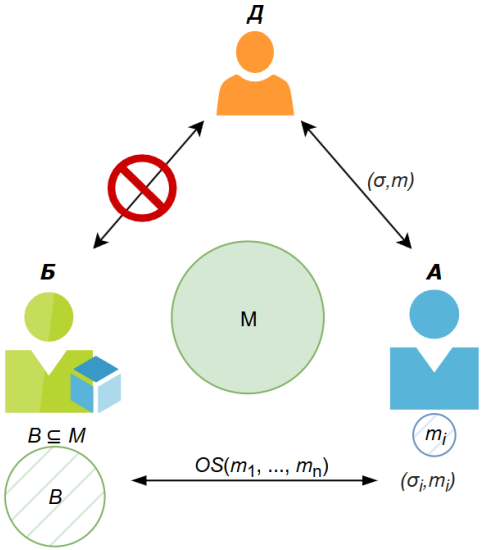
Сторона **Б** не узнает, какой именно элемент m_i запрашивала сторона **А**:

- неоднозначность (*ambiguity*) забывчивой подписи
- инвариантность на элементах образа и попарная различность элементов $F(m)$

Неподделываемость

Сторона ***A*** не сможет подтвердить принадлежность элементов вектора $\mathbf{y}^*$, кроме запрашиваемого элемента m_i:

- выполняется свойство неподделываемости забывчивой подписи


Д
(σ,m)
Б
А
M
B ⊆ M
B
OS(m1, ..., mn)
mi
(σi,mi)

- Предложен протокол анонимного подтверждения принадлежности элемента заданному множеству, основанный на **схеме забывчивой подписи** и **функции** F
- Протокол обеспечивает **анонимность** запроса стороны $\boldsymbol{A}$, **однозначность** ответа стороны $\boldsymbol{Б}$ и **криптографически проверяемый** результат для третьей стороны
- Разработанный протокол может применяться в задачах анонимной проверки принадлежности элемента заданному множеству в различных прикладных сценариях

РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Протокол анонимного подтверждения наличия элемента в рассматриваемом множестве

Хуцаева Алтана, Беззатеев Сергей

ИТМО, ГУАП

akhutsaeva@yandex.ru, bsv@guap.ru