КриптоПро

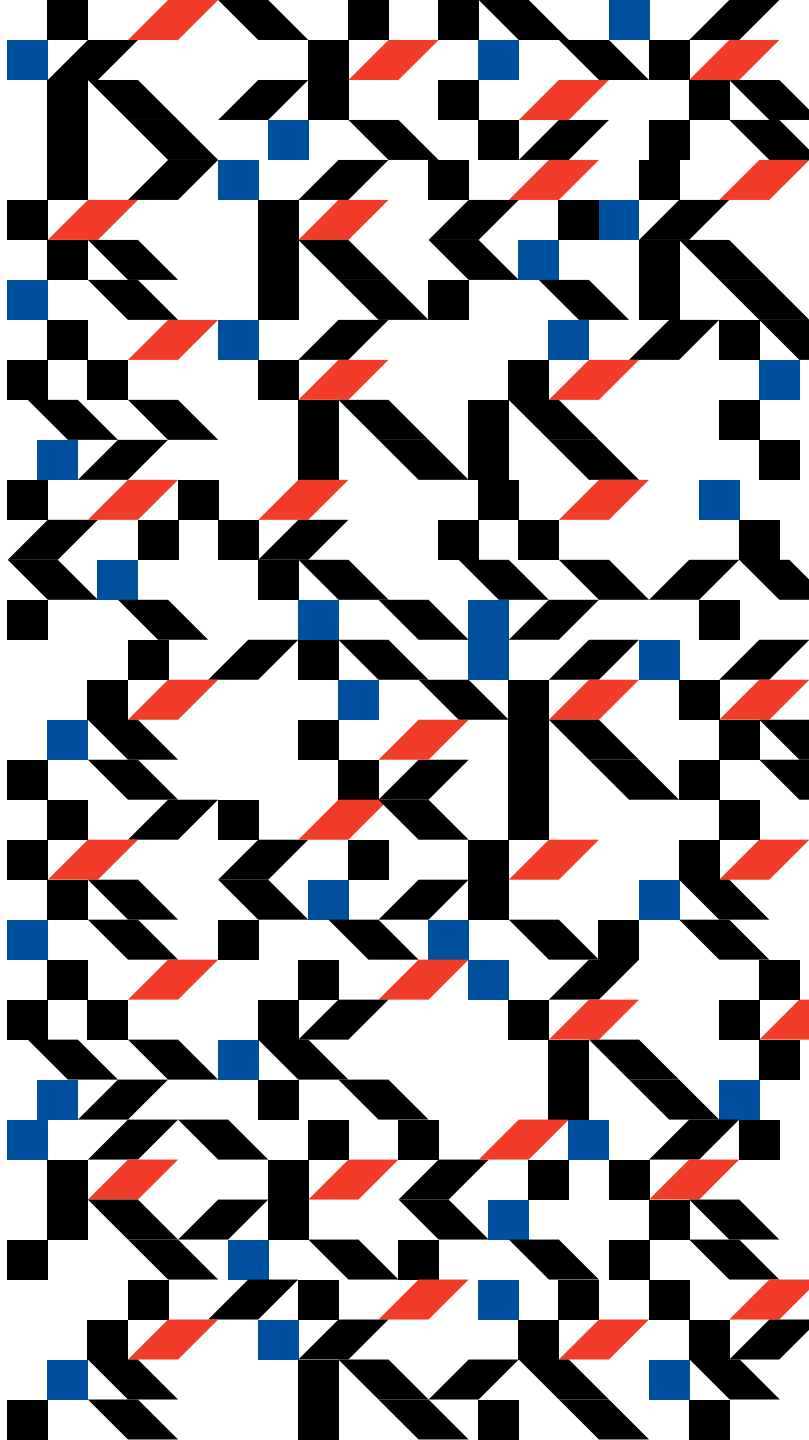
Конфиденциальное сложение данных: определение объекта и предмета исследования

Никифорова Лидия Олеговна, ведущий инженер-аналитик

Ахметзянова Лилия Руслановна, к.ф.-м.н., зам. начальника отдела криптографических исследований

Быстревский Сергей Андреевич, инженер-аналитик

Мухортова Алёна Андреевна, инженер-аналитик



ТК 26

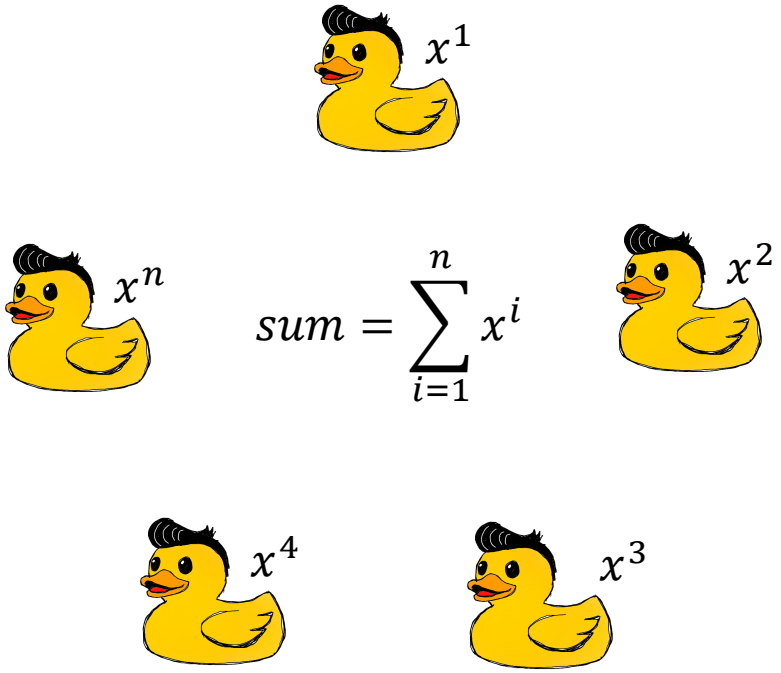
Рабочая группа, посвящённая использованию криптографии в финансовой сфере

Принципы построения для механизма конфиденциального сложения данных (проект MP компании Блумтех)

Объект:

схема конфиденциального сложения данных

Задача на интуитивном уровне



Условия:

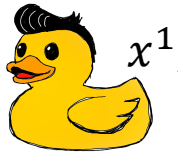
- n участников;
- каждый участник обладает данными $x^i, i \in \{1, \dots, n\}$.

Цель:

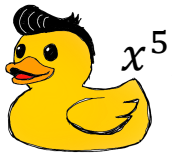
вычислить сумму данных $sum = \sum_{i=1}^{n} x^i$ с обеспечением конфиденциальности

- данных;
- суммы.

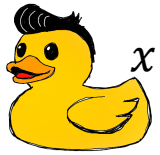
Пример



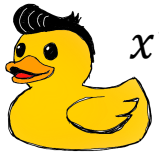
$x^1, k_{12}, k_{13}, k_{14}, k_{15}$



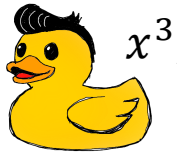
$x^5, k_{15}, k_{25}, k_{35}, k_{45}$



$x^2, k_{12}, k_{23}, k_{24}, k_{25}$



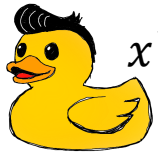
$x^4, k_{14}, k_{24}, k_{34}, k_{45}$



$x^3, k_{13}, k_{23}, k_{34}, k_{35}$

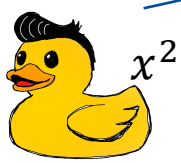
Пример

$c_1 = x^1 + k_{12} + k_{13} + k_{14} + k_{15}$



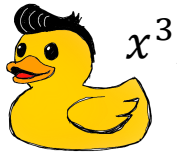
$x^1, k_{12}, k_{13}, k_{14}, k_{15}$

$c_2 = x^2 - k_{12} + k_{23} + k_{24} + k_{25}$



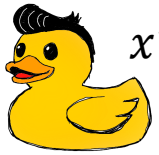
$x^2, k_{12}, k_{23}, k_{24}, k_{25}$

$c_3 = x^3 - k_{13} - k_{23} + k_{34} + k_{35}$



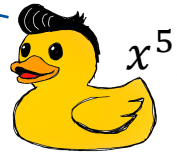
$x^3, k_{13}, k_{23}, k_{34}, k_{35}$

$c_4 = x^4 - k_{14} - k_{24} - k_{34} + k_{45}$



$x^4, k_{14}, k_{24}, k_{34}, k_{45}$

$c_4 = x^5 - k_{15} - k_{25} - k_{35} - k_{45}$



$x^5, k_{15}, k_{25}, k_{35}, k_{45}$

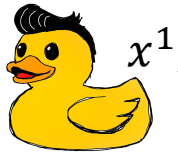
Общая формула $c_i = x^i + \sum_{j=1}^{n} (-1)^{i<j} k_{ij}$

$$sum = \sum_{i=1}^{n} c_i = \sum_{i=1}^{n} x^i$$

Пример

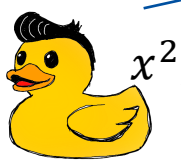
Честными должны быть
как минимум 2 участника

$c_1 = x^1 + k_{12} + k_{13} + k_{14} + k_{15}$



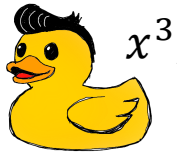
$x^1, k_{12}, k_{13}, k_{14}, k_{15}$

$c_2 = x^2 - k_{12} + k_{23} + k_{24} + k_{25}$



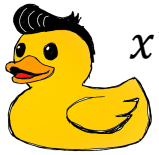
$x^2, k_{12}, k_{23}, k_{24}, k_{25}$

$c_3 = x^3 - k_{13} - k_{23} + k_{34} + k_{35}$



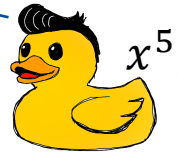
$x^3, k_{13}, k_{23}, k_{34}, k_{35}$

$c_4 = x^4 - k_{14} - k_{24} - k_{34} + k_{45}$



$x^4, k_{14}, k_{24}, k_{34}, k_{45}$

$c_4 = x^5 - k_{15} - k_{25} - k_{35} - k_{45}$



$x^5, k_{15}, k_{25}, k_{35}, k_{45}$

Общая формула $c_i = x^i + \sum_{j=1}^{n} (-1)^{i<j} k_{ij}$

$$sum = \sum_{i=1}^{n} c_i = \sum_{i=1}^{n} x^i$$

Схемы и протоколы

Криптографические механизмы для решения задачи

схемы	протоколы
PSA (Private Stream Aggregation)	SA (Secure Aggregation)
Фиксируют вычисления	Фиксируют архитектуру, вычисления, пересылки
Анализ не меняется, нужно сводить стойкость прикладной системы к стойкости схемы	Любое изменение на уровне прикладной системы требует проведения нового криптографического анализа

Схемы – более универсальный механизм для встраивания его в прикладные системы

Интерфейс

Схемой конфиденциального сложения PSA будем называть набор алгоритмов

KGen – генерации ключей

Enc – зашифрования данных

Agg – вычисления суммы

Интерфейс

$$\mathrm{KGen}(n) \rightarrow (sk_1, sk_2, \dots, sk_n)$$

$$\mathrm{Enc}(sk_i, x^i, l) \rightarrow ct_{i,l}$$

$$\mathrm{Agg}(ct_{1,l}, ct_{2,l}, \dots, ct_{n,l}) \rightarrow sum$$

l – метка сессии

Ограничения:

- статичный состав ключевой информации
- наличие сессий

Интерфейс

Без выделенного ключа агрегации

$$\mathrm{KGen}(n) \rightarrow (sk_1, sk_2, \dots, sk_n)$$

$$\mathrm{Enc}(sk_i, x^i, l) \rightarrow ct_{i,l}$$

$$\mathrm{Agg}(ct_{1,l}, ct_{2,l}, \dots, ct_{n,l}) \rightarrow sum$$

С выделенным ключом агрегации

$$\mathrm{KGen}(n) \rightarrow (\boldsymbol{sk_0}, sk_1, sk_2, \dots, sk_n)$$

$$\mathrm{Enc}(sk_i, x^i, l) \rightarrow ct_{i,l}$$

$$\mathrm{Agg}(\boldsymbol{sk_0}, ct_{1,l}, ct_{2,l}, \dots, ct_{n,l}, \boldsymbol{l}) \rightarrow sum$$

Интерфейс

Без выделенного ключа агрегации

$$\mathrm{KGen}(n) \to (sk_1, sk_2, \dots, sk_n)$$

$$\mathrm{Enc}(sk_i, x^i, l) \to ct_{i,l}$$

$$\mathrm{Agg}(ct_{1,l}, ct_{2,l}, \dots, ct_{n,l}) \to sum$$

Любой может узнавать сумму

С выделенным ключом агрегации

$$\mathrm{KGen}(n) \to (sk_0, sk_1, sk_2, \dots, sk_n)$$

$$\mathrm{Enc}(sk_i, x^i, l) \to ct_{i,l}$$

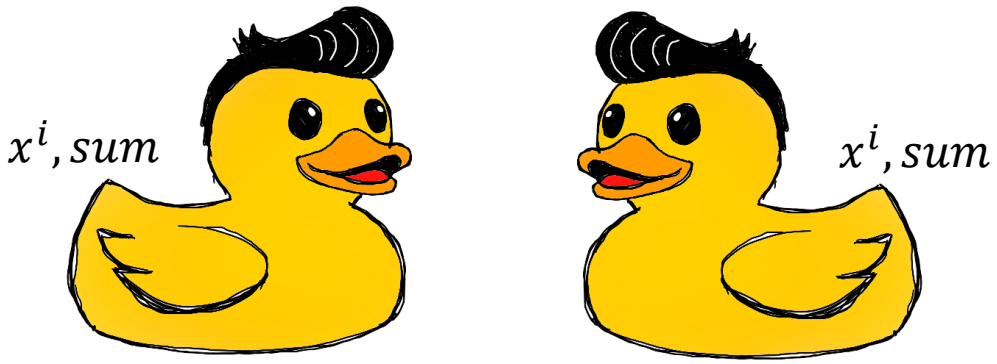
$$\mathrm{Agg}(sk_0, ct_{1,l}, ct_{2,l}, \dots, ct_{n,l}, l) \to sum$$

Только тот, кто обладает ключом, может узнавать сумму

Интерфейс

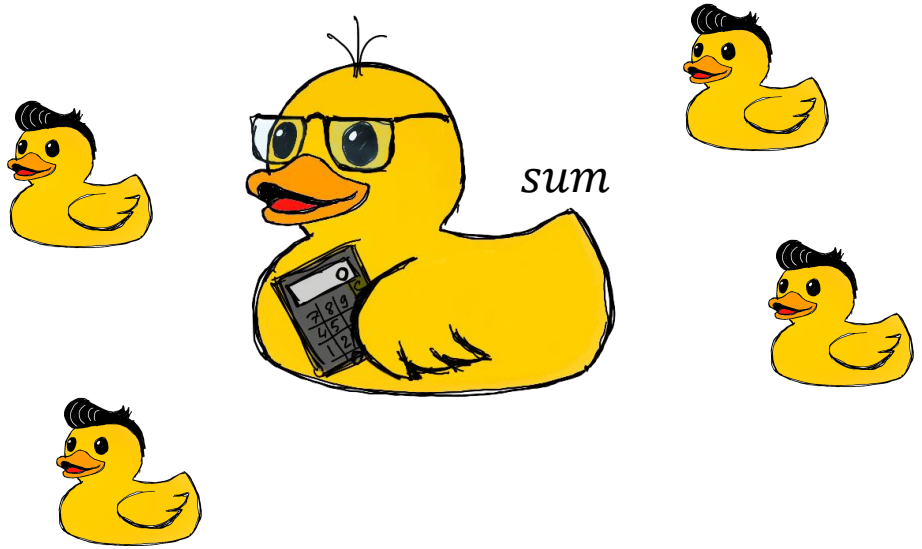
На практике

Без выделенного ключа агрегации



Участники равнозначны
Любой может инициировать вычисление
получить результат

С выделенным ключом агрегации



Есть выделенный участник – агрегатор
Только агрегатор инициирует
вычисление и получает результат

Интерфейс

Далее будем рассматривать схемы с выделенным ключом агрегации

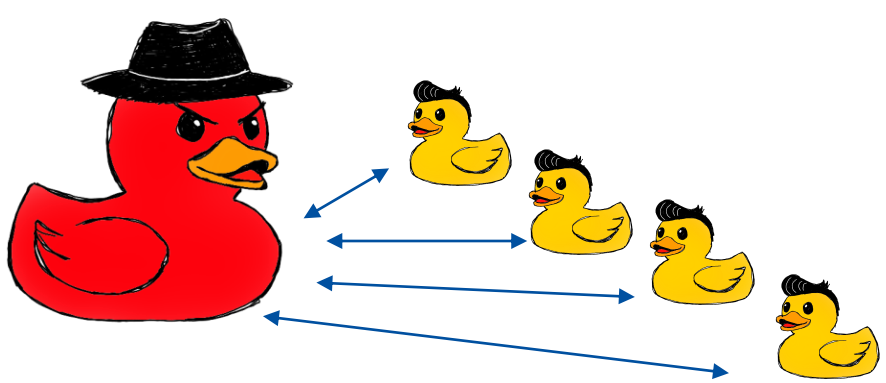
Предмет:

модели безопасности для схем, имеющих заданный интерфейс

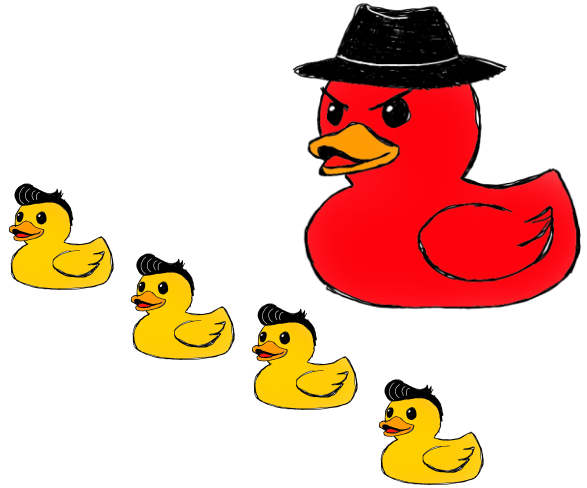
Модели безопасности

Возможности нарушителя

- ✓ Узнавать шифртексты для известных данных



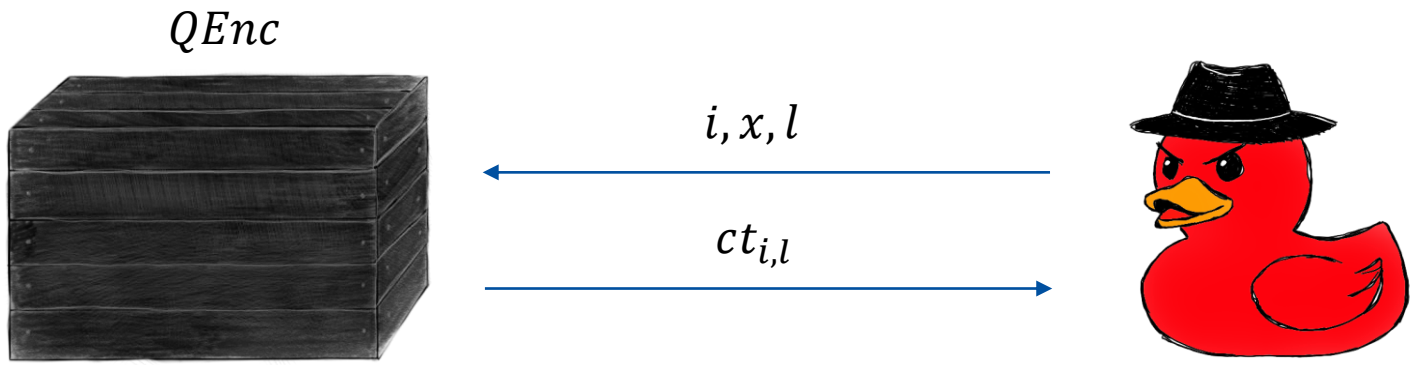
- ✓ Компрометировать участников



Возможность:

узнавать шифртексты для известных данных

Модели безопасности

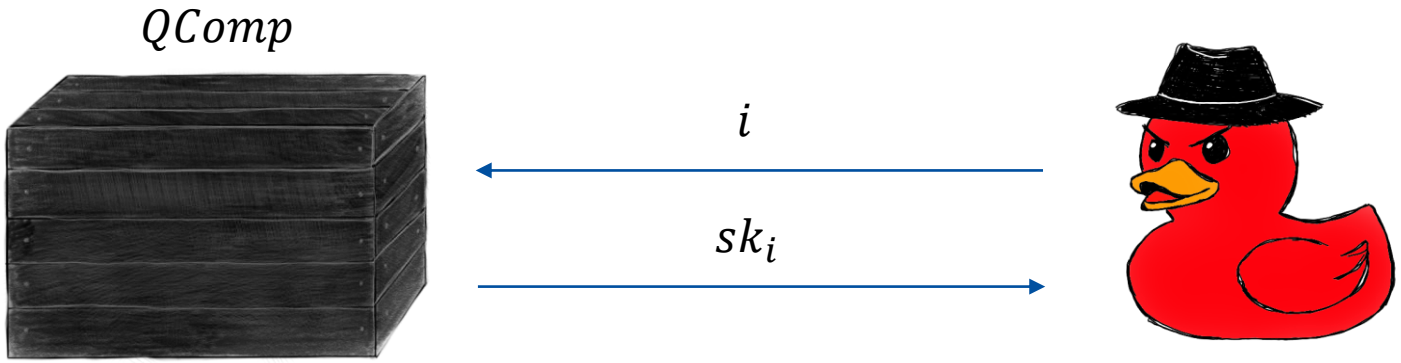


Возможность:

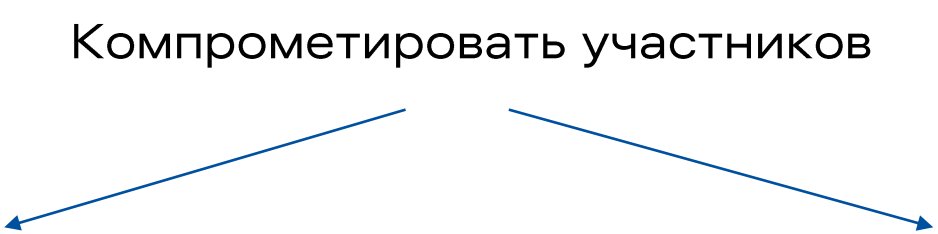
компрометировать участников

Модели безопасности

Компрометировать участников – узнавать ключи участников



Модели безопасности



Статически (S)

$$n, CS, state \leftarrow \mathcal{A}$$
$$\{sk_i\}_{i=0}^{n} \leftarrow \text{PSA. KGen(n)}$$
$$state \leftarrow \mathcal{A}^{QComp(CS)}(state)$$
$$res \leftarrow \mathcal{A}^{\cdots}(state)$$

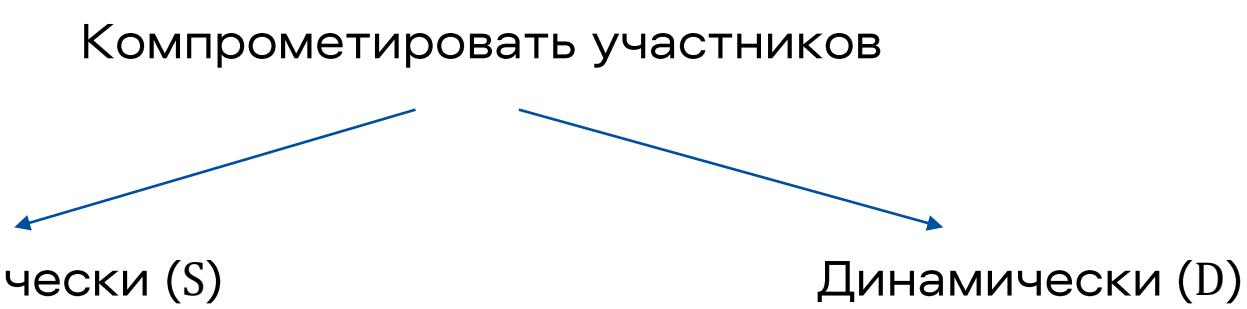
Заранее задаёт множество участников, которых может компрометировать

Динамически (D)

$$n, state \leftarrow \mathcal{A}$$
$$\{sk_i\}_{i=0}^{n} \leftarrow \text{PSA. KGen(n)}$$
$$res \leftarrow \mathcal{A}^{QComp,\cdots}(state)$$

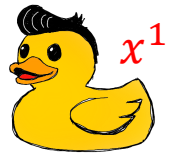
Может компрометировать участников в произвольные моменты времени

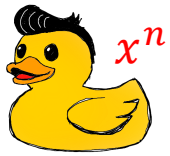
Модели безопасности

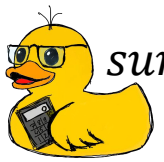


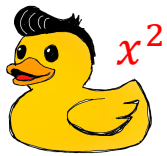
- когда участники преследуют разные (противоположные) цели
- когда есть некоторый орган, следящий за тем, чтобы стороны не объединялись
- когда участники взаимодействуют анонимно

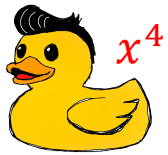
Модели безопасности

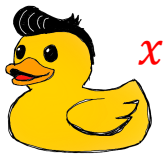








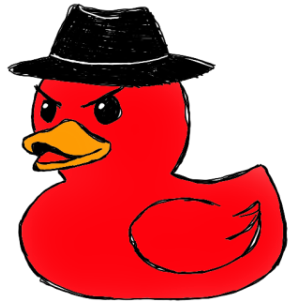




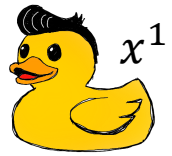
Угрозы

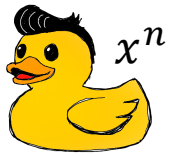
1) Нарушение конфиденциальности исходных данных

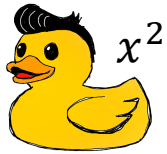
2) Нарушение конфиденциальности суммы

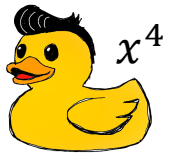


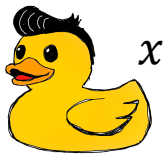
Модели безопасности







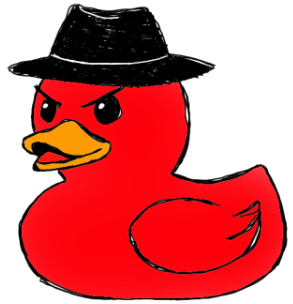




Угрозы

1) Нарушение конфиденциальности исходных данных

2) Нарушение конфиденциальности суммы



Модели безопасности

Моделирование угрозы (AO – aggregator oblivious)

- есть тестовая сессия – сессия, в которой нарушитель хочет получить какую-то информацию о данных или сумме

Выбор данных участниками в тестовой сессии

Неадаптивный (N)

данные заранее существуют

Адаптивный (A)

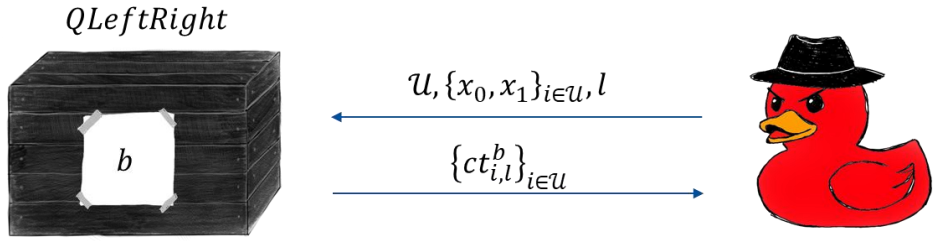
данные формируются в рамках работы

Модели безопасности

Выбор данных участниками в тестовой сессии

Неадаптивный выбор данных (N)

Адаптивный выбор данных (A)

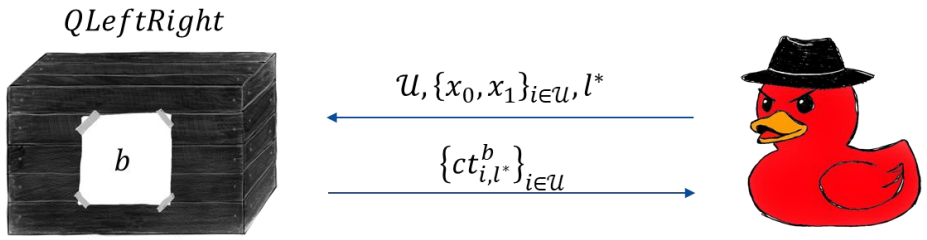


$\mathcal{U} \subseteq \{1, \ldots, n\}$

Модели безопасности

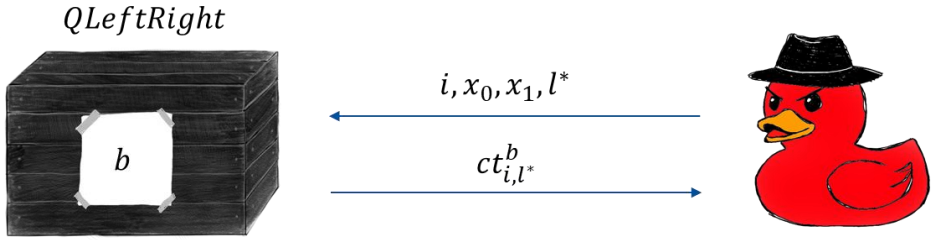
Выбор данных участниками в тестовой сессии

Неадаптивный выбор данных (N)



$\mathcal{U} \subseteq \{1, \dots, n\}$

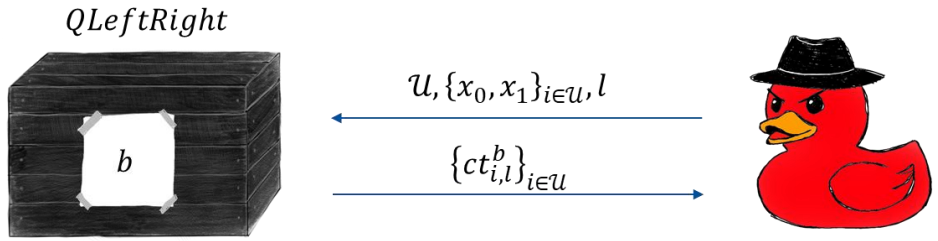
Адаптивный выбор данных (A)



Модели безопасности

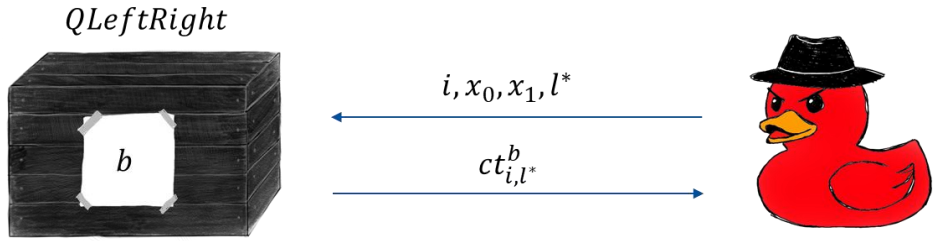
Выбор данных участниками в тестовой сессии

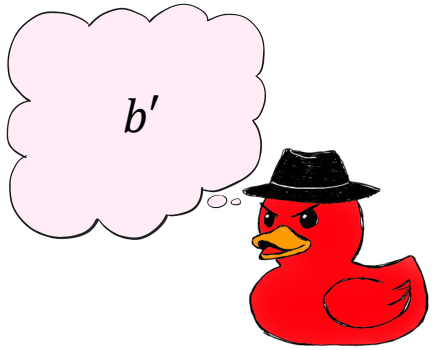
Неадаптивный выбор данных (N)



$\mathcal{U} \subseteq \{1, \dots, n\}$

Адаптивный выбор данных (A)





Если $b' = b$, нарушитель реализует угрозу

Модели безопасности

Соответствуют всем возможным комбинациям описанных возможностей нарушителя

Модели безопасности

AO-DA

Waldner H. et al. Private stream aggregation from labeled secret sharing schemes //Cryptology ePrint Archive. – 2021.

AO-DH

Ernst J., Koch A. Private stream aggregation with labels in the standard model //Proceedings on Privacy Enhancing Technologies. – 2021.

AO-DN

AO-SA

AO-SH

Brorsson J., Gunnarsson M. Dipsauce: efficient private stream aggregation without trusted parties //Nordic Conference on Secure IT Systems. – Cham : Springer Nature Switzerland, 2023. – С. 204-222.

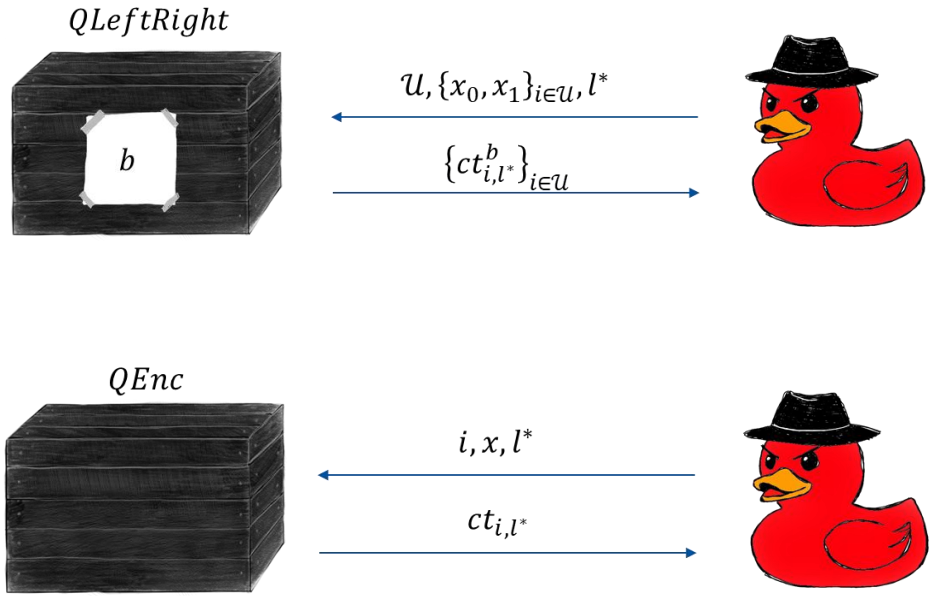
AO-SN

Встречаются в литературе под названием модель AO

Модели безопасности

Выбор данных участниками в тестовой сессии

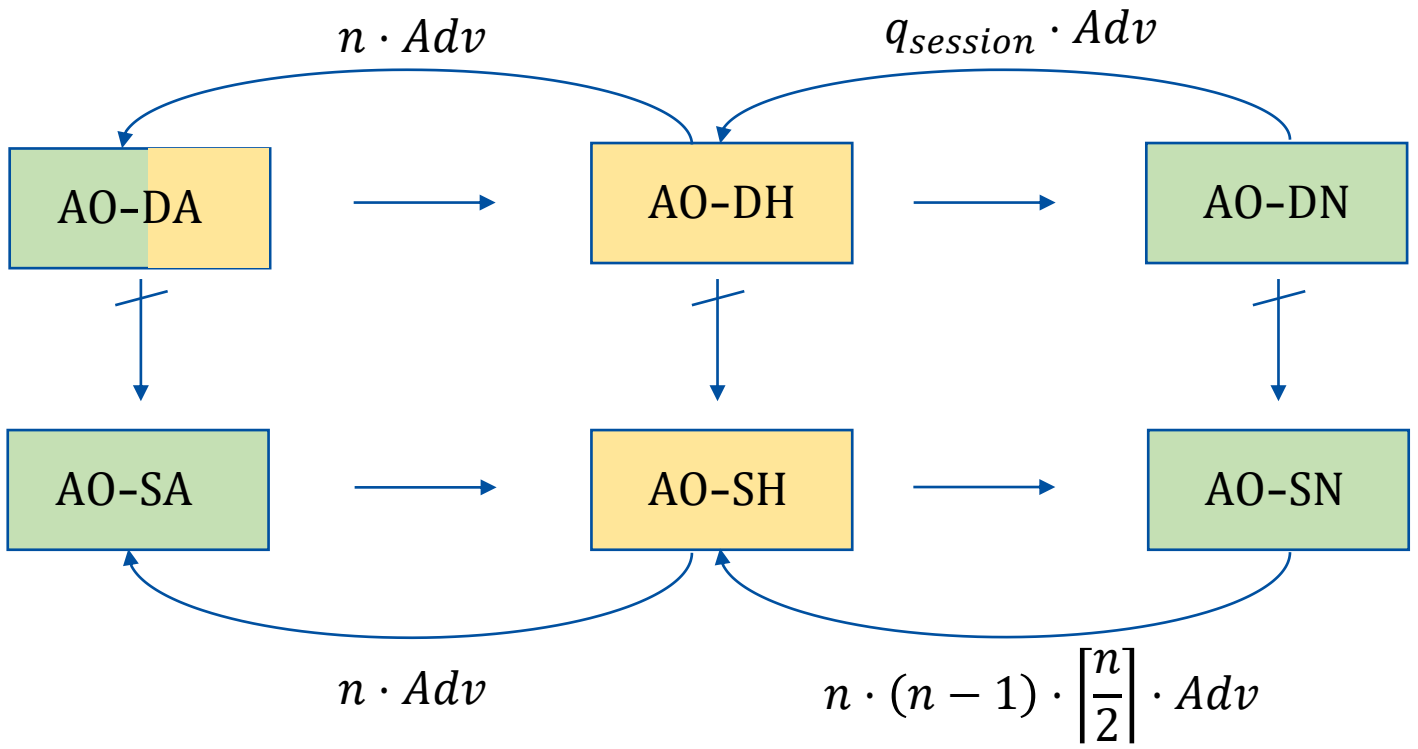
Гибридный выбор данных (H)



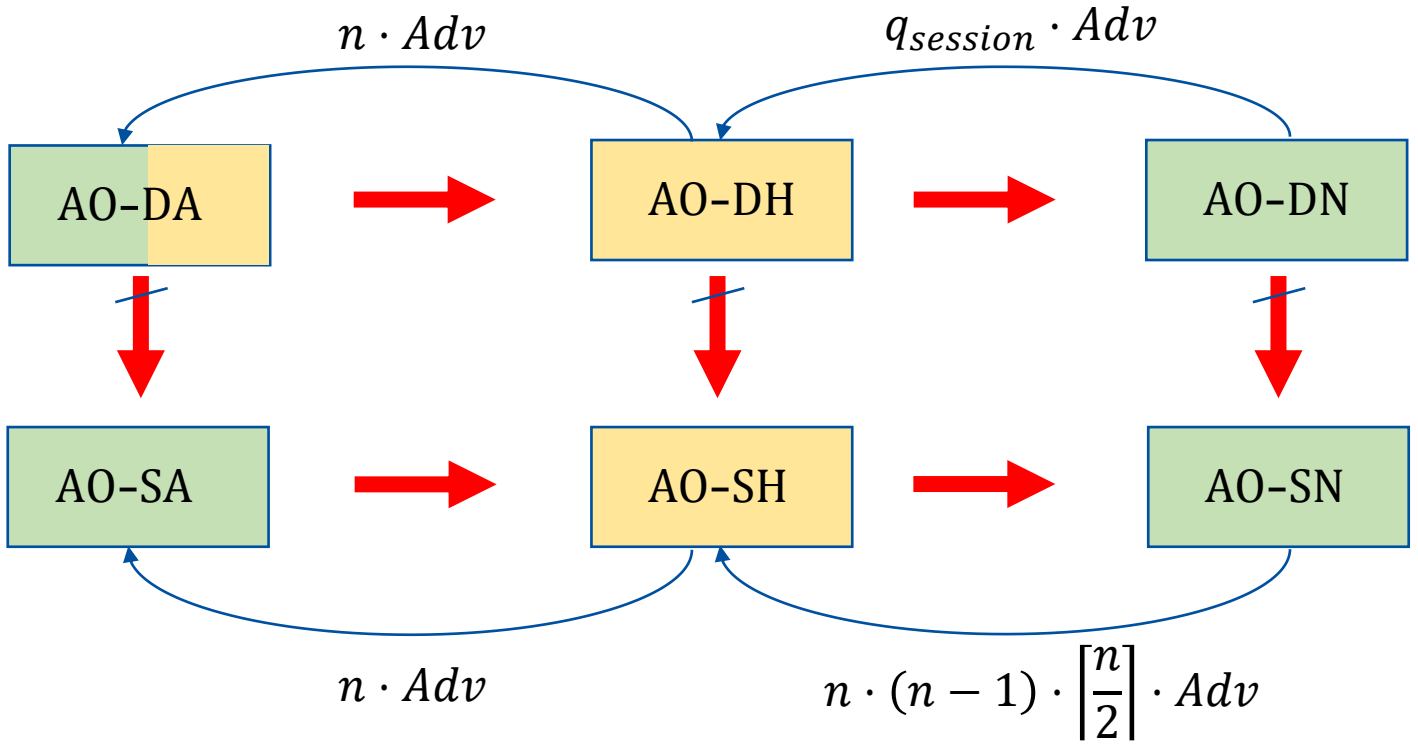
$\mathcal{U} \subseteq \{1, \dots, n\}$

$i \in \{1, \dots, n\} \backslash \mathcal{U}$

Соотношения

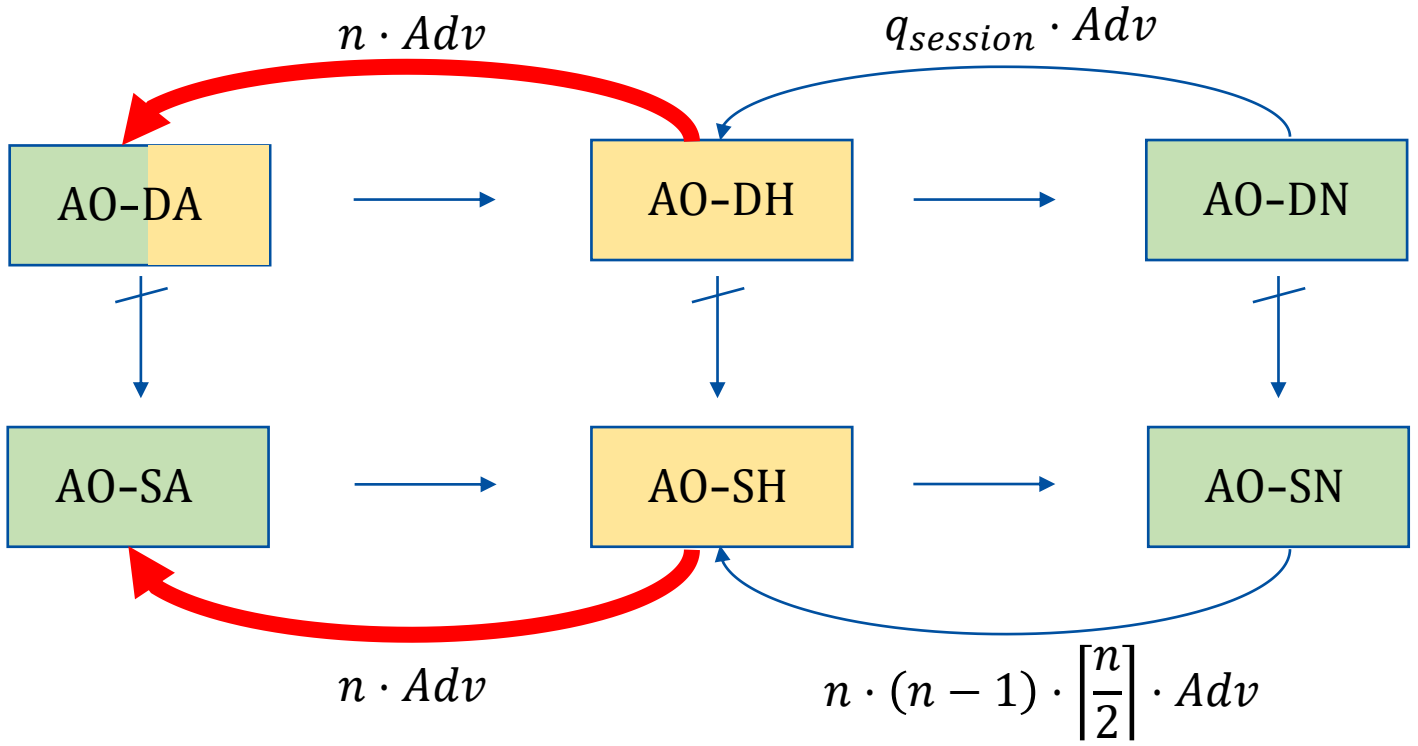


Соотношения



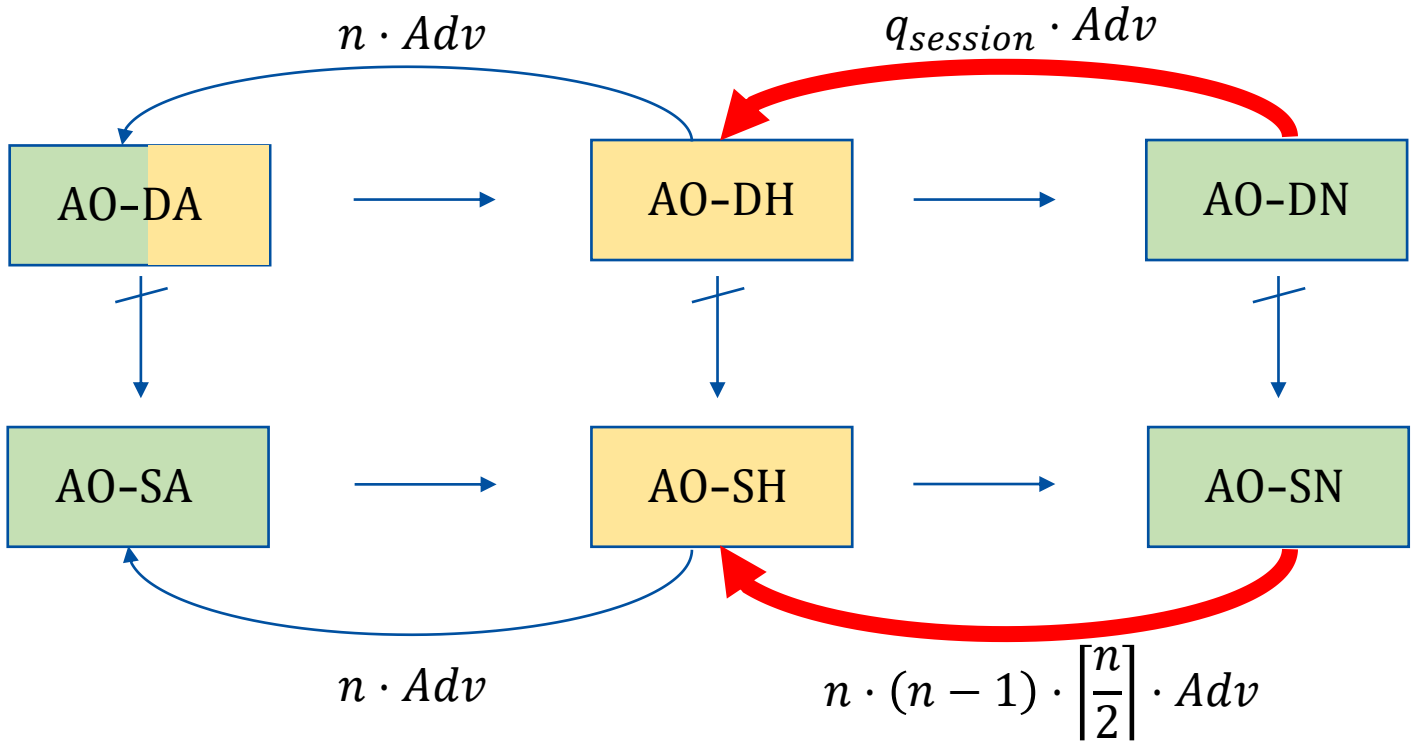
Возможности нарушителя в модели у начала вектора включают в себя возможности нарушителя в модели у конца вектора

Соотношения



Доказательство использует технику гибридного аргумента

Соотношения

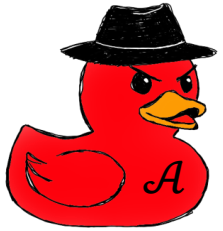


Есть отличия в случае динамической и в случае статической компрометации

Соотношения

AO-DH

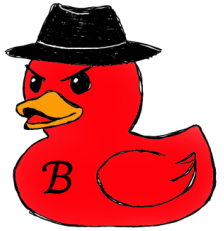
AO-DN



$$QLeftRight(\mathcal{U}, \{x_0^i, x_1^i\}_{i \in \mathcal{U}}, l^*)$$

$$QEnc(j, x, l^*)$$

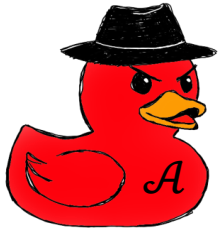
~~$QEnc(j, x, l^*)$~~



Соотношения

AO-DH

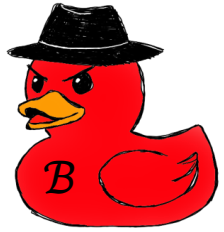
AO-DN



$QLeftRight(\mathcal{U}, \{x_0^i, x_1^i\}_{i \in \mathcal{U}}, l^*)$

$QEnc(j, x, l^*)$

~~$QEnc(j, x, l^*)$~~



Нарушитель $\mathcal{B}$ реализует эксперимент для нарушителя $\mathcal{A}$

Угадывает тестовую сессию l'

$QEnc(j, x, l')$ →

Компрометирует участника j

← $\text{PSA.Enc}(sk_j, x, l')$

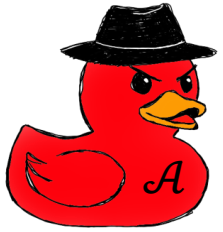
$QLeftRight(\mathcal{U}, \{x_0^i, x_1^i\}_{i \in \mathcal{U}}, l^*)$ →

Если $l^* \neq l'$, то завершается с ошибкой

Соотношения

AO-SH

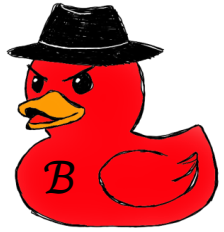
AO-SN



$QLeftRight(\mathcal{U}, \{x_0^i, x_1^i\}_{i \in \mathcal{U}}, l^*)$

$QEnc(j, x, l^*)$

~~$QEnc(j, x, l^*)$~~



Нарушитель $\mathcal{B}$ реализует эксперимент для нарушителя $\mathcal{A}$

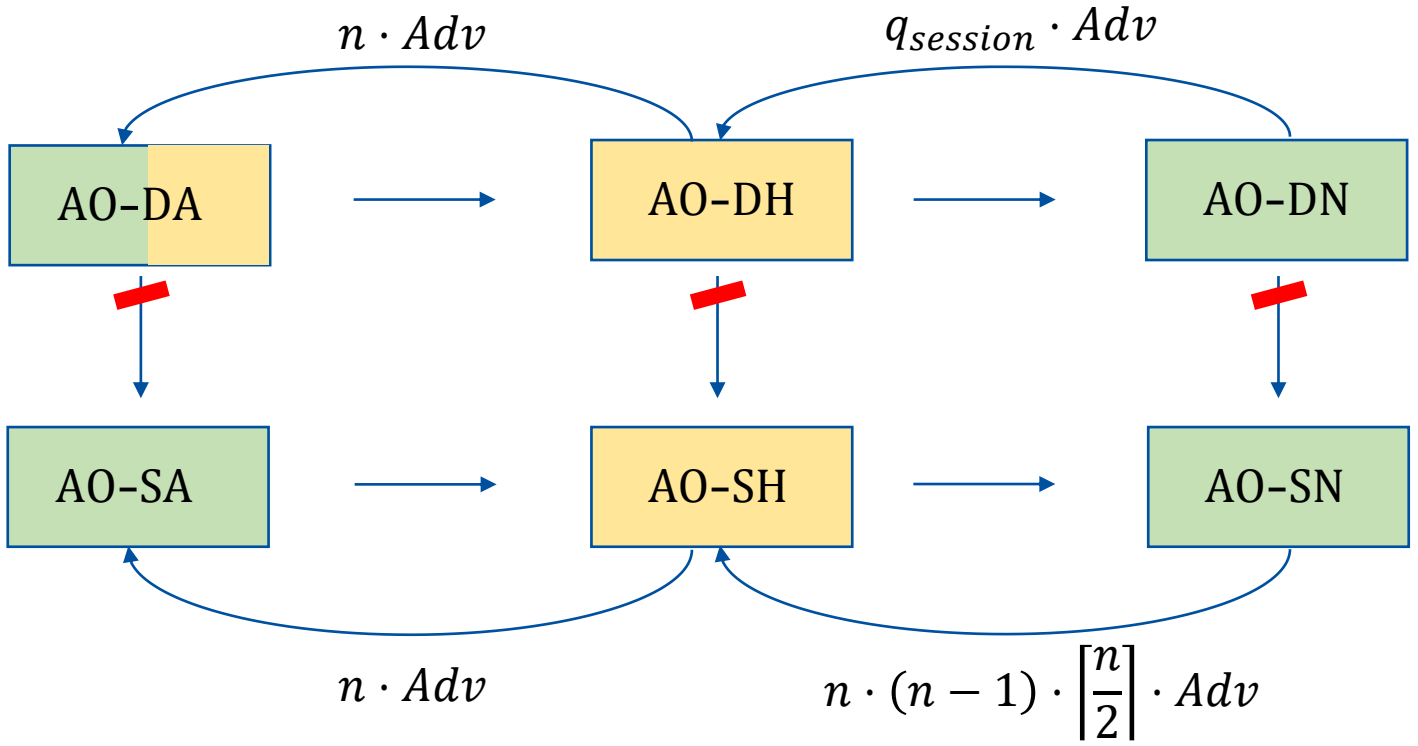
$QEnc(j, x, l')$ →

Угадывает тестовую сессию l'

~~Компрометирует участника j~~

Не может выполнить компрометацию участника j

Соотношения



Существует схема PSA, которая является стойкой в модели AO-S $*$ и нестойкой в модели AO-D $*$

Соотношения

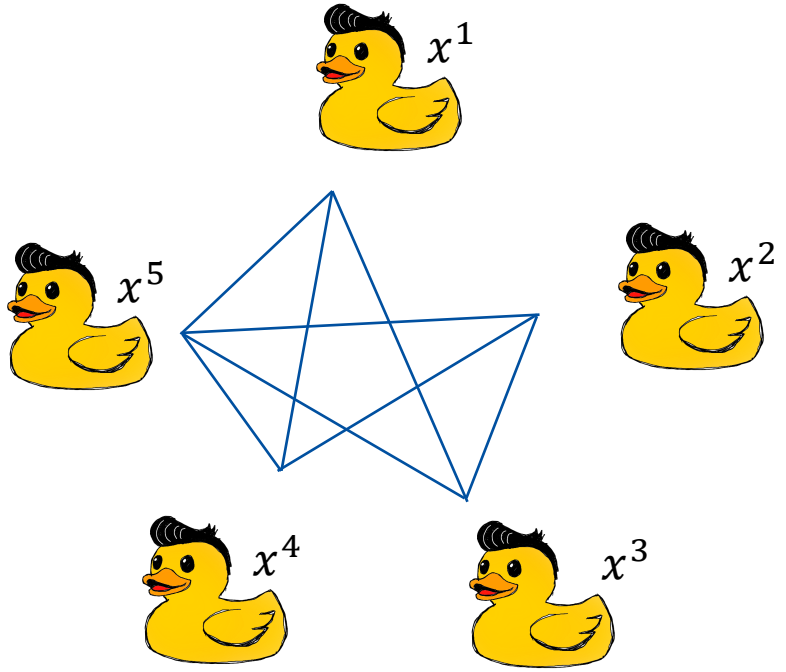
Идея: маска каких-то участников может зависеть не от всех оставшихся участников

Brorsson J., Gunnarsson M. Dipsauce: efficient private stream aggregation without trusted parties //Nordic Conference on Secure IT Systems. – Cham : Springer Nature Switzerland, 2023. – С. 204-222.

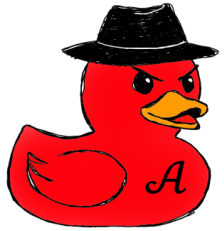
Соотношения

Идея: маска каких-то участников может зависеть не от всех оставшихся участников

Brorsson J., Gunnarsson M. Dipsauce: efficient private stream aggregation without trusted parties //Nordic Conference on Secure IT Systems. – Cham : Springer Nature Switzerland, 2023. – С. 204-222.

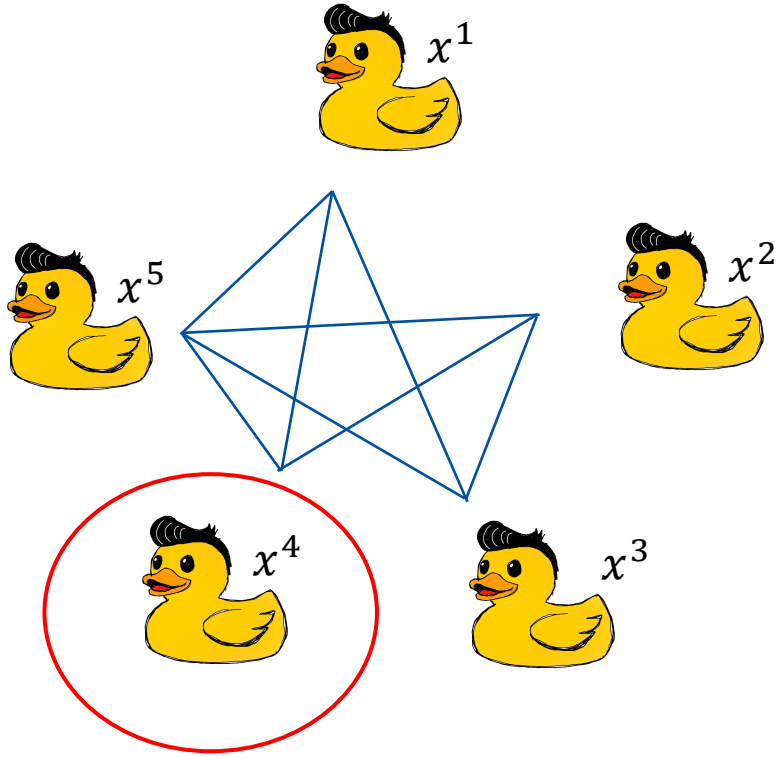


Соотношения

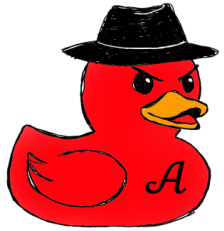


$AO\text{-}D *$

$\mathcal{A}$ компрометирует любого и узнаёт граф



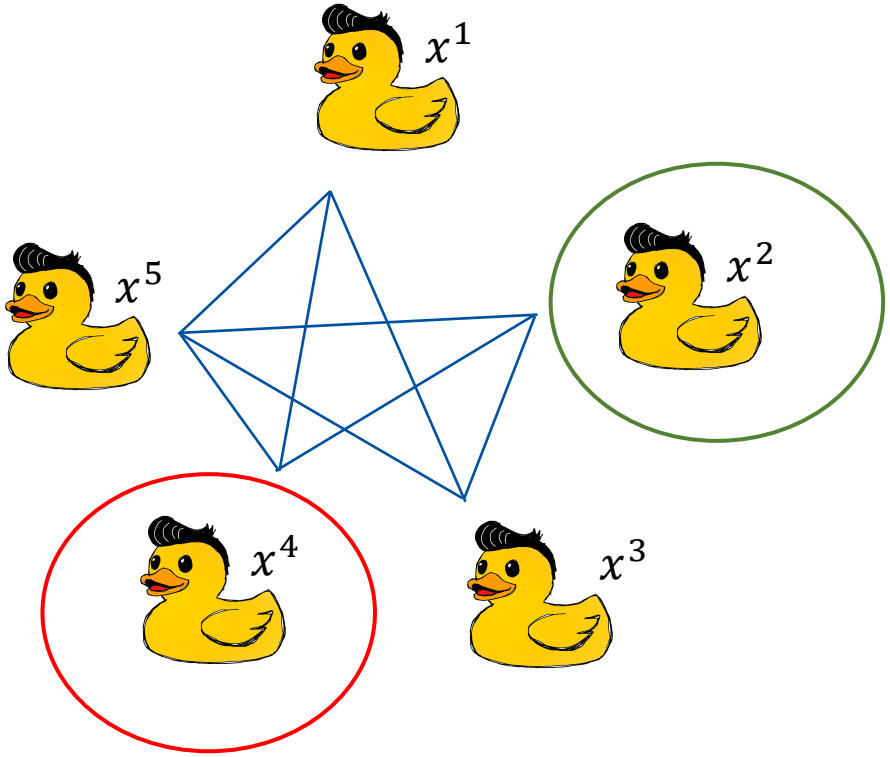
Соотношения



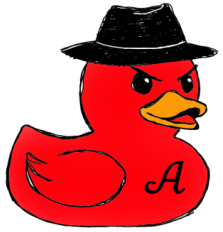
AO-D $*$

$\mathcal{A}$ компрометирует любого и узнаёт граф

$\mathcal{A}$ выбирает в качестве атакуемого любого, кто связан не со всеми другими



Соотношения

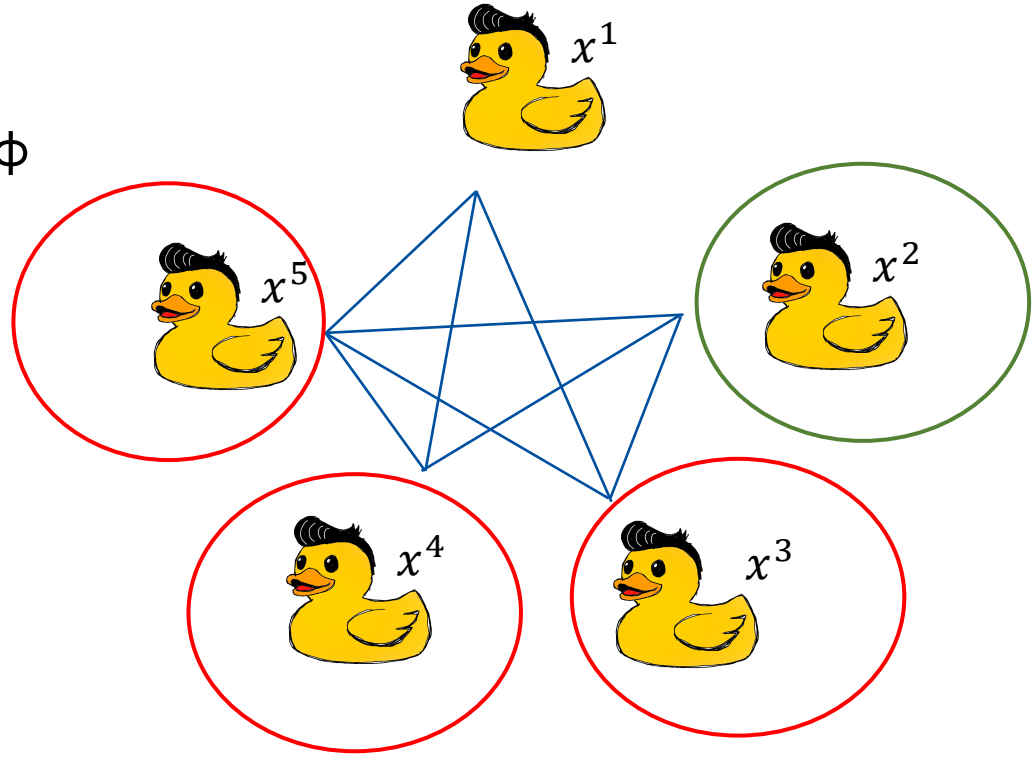


AO-D *

$\mathcal{A}$ компрометирует любого и узнаёт граф

$\mathcal{A}$ выбирает в качестве атакуемого любого, кто связан не со всеми другими

$\mathcal{A}$ компрометирует тех, с кем связан атакуемый, и узнаёт его данные

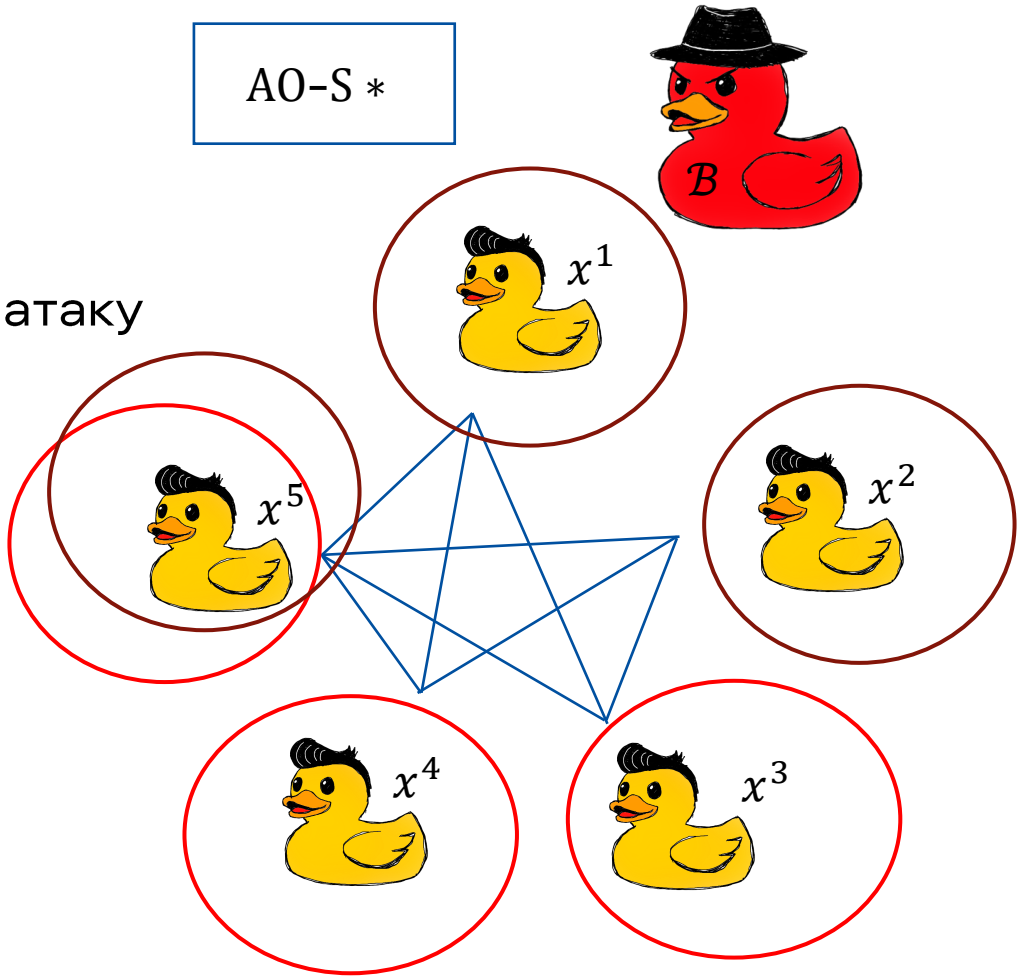


Соотношения

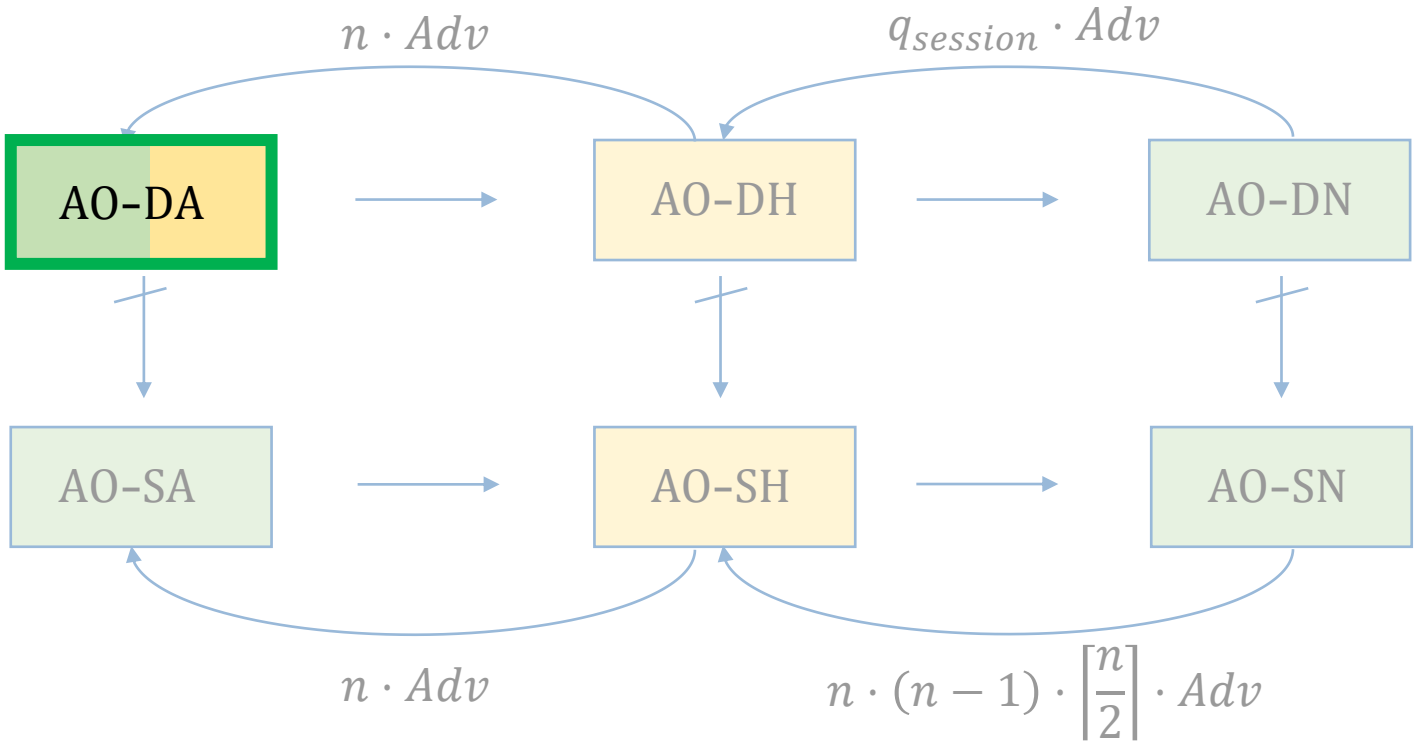
2 тройки, которые позволят реализовать атаку

Всего 60 способов выбрать троих участников

Вероятность реализовать угрозу $\frac{1}{30}$



Вывод



Важно получать оценку непосредственно в релевантной модели.
Получение оценки в более сильной модели на основе оценки в слабой модели может привести к её существенному ухудшению.