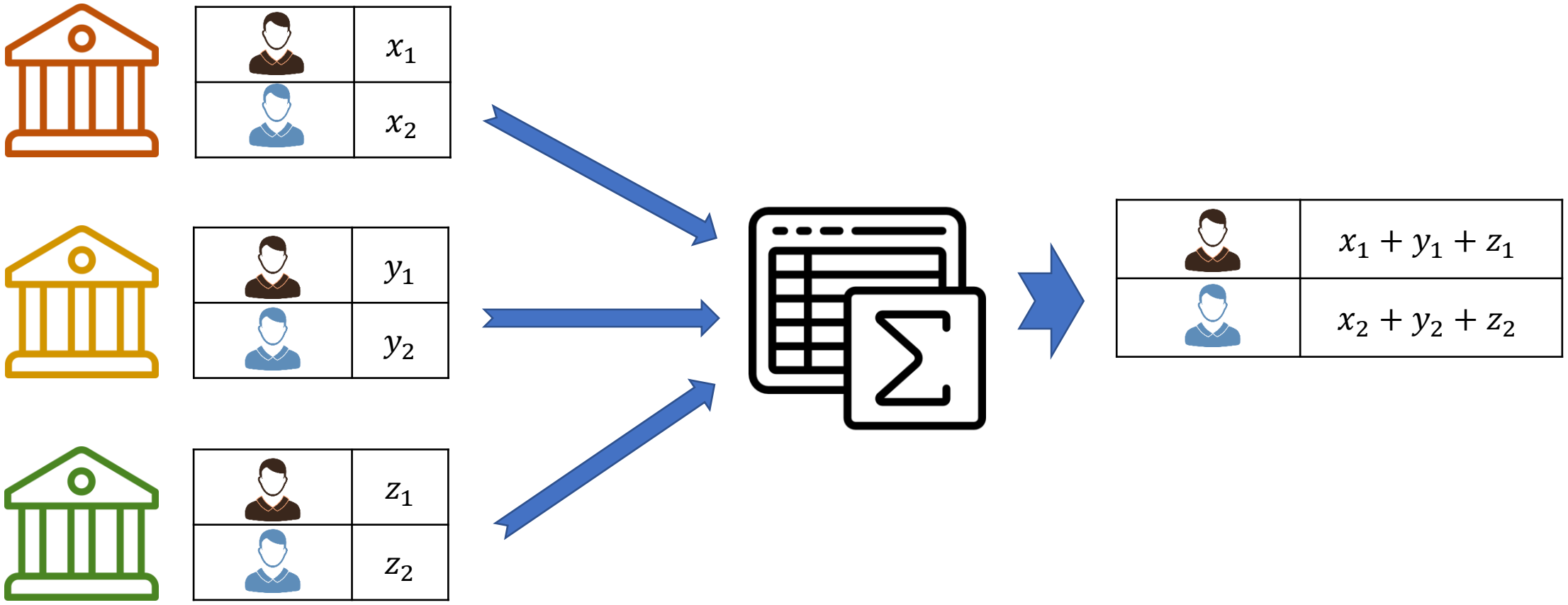
конференция
РусКрипто

Ежегодная международная научно-практическая конференция
«РусКрипто’2023»

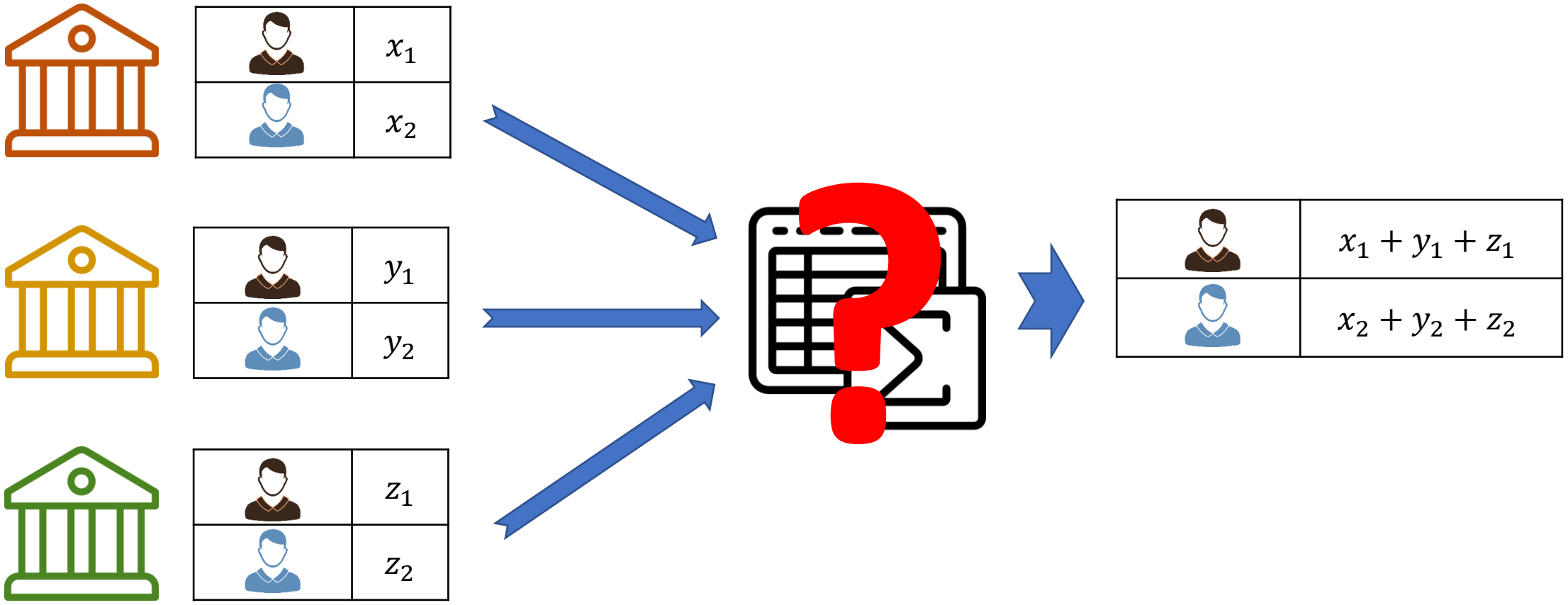
Конфиденциальный скоринг с точки зрения криптографии

Кяжин Сергей Николаевич, к.ф.-м.н., ведущий инженер-аналитик, *КриптоПро*
Алексеев Е. К., Ахметзянова Л. Р., Бабуева А. А., *КриптоПро*
Митрофанов А. А., Ефимов В. К., Болбачан В. С., *Блуттех*

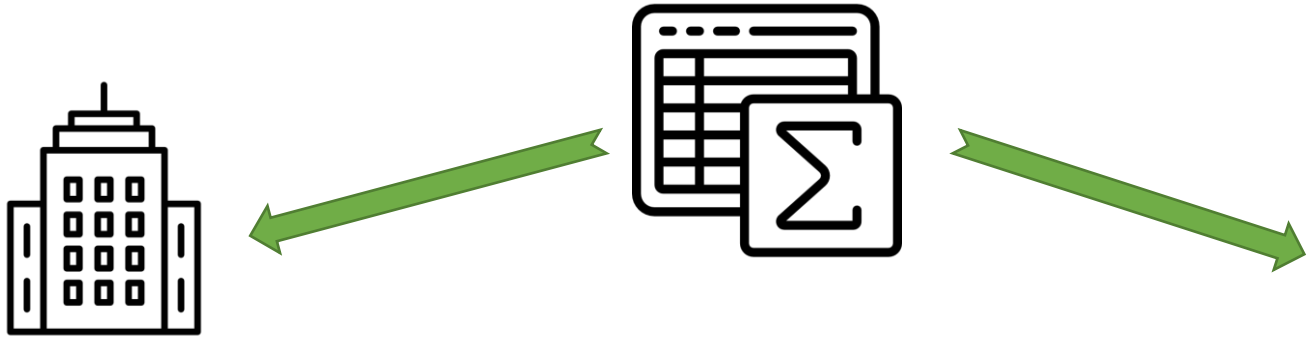
Что такое скоринг



Что такое скоринг

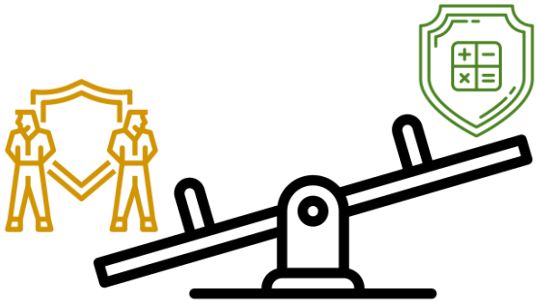


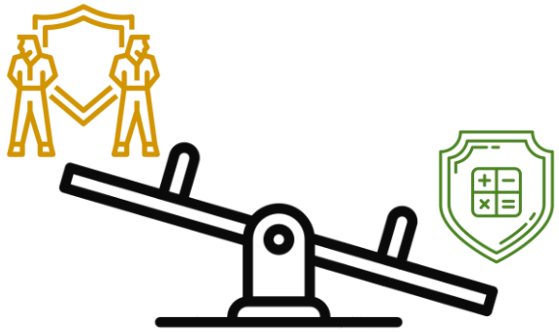
(Де)централизованный скоринг



Отдельная организация (нужны орг.-тех. меры обеспечения доверия)

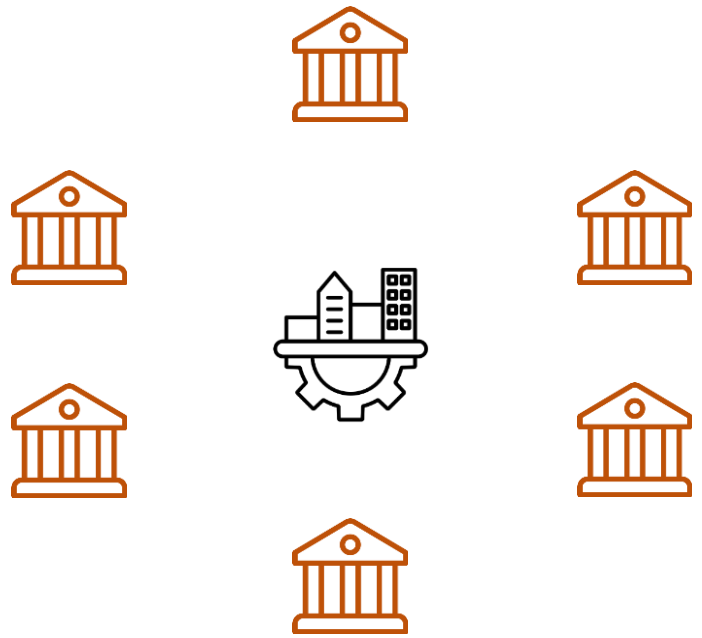
Криптографический протокол

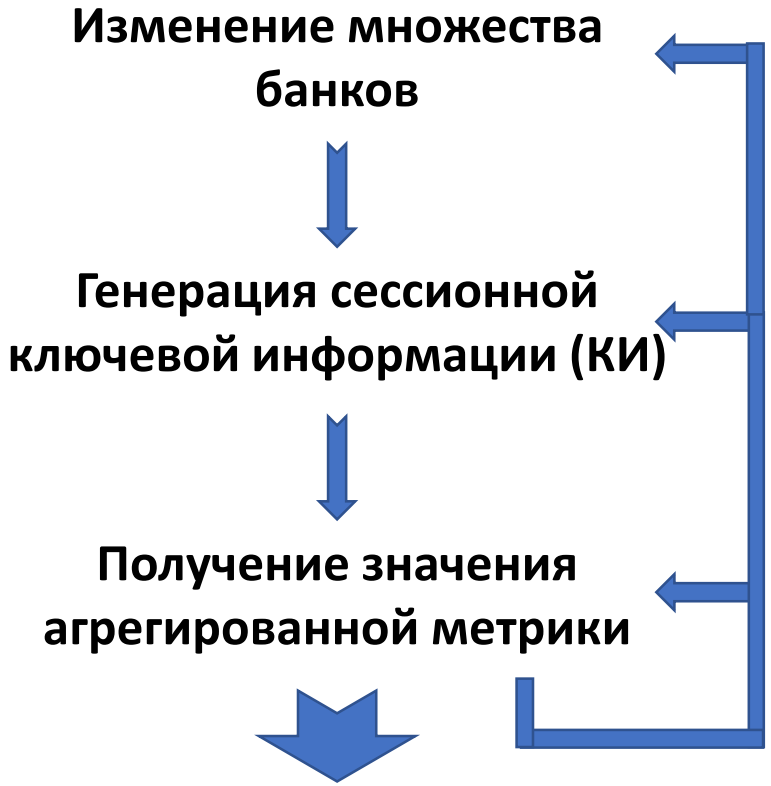




Скоринг как криптографический протокол

В общем случае участники протокола – Банки и Оператор





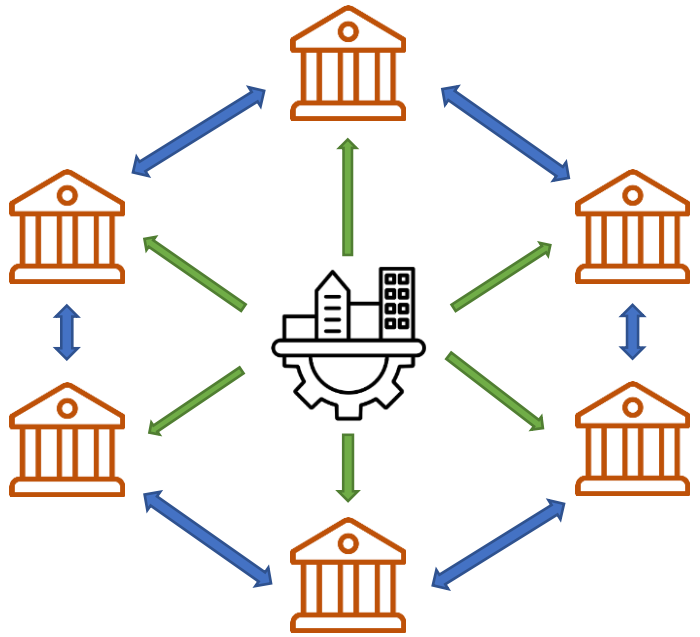
Скоринг как криптографический протокол

До	В процессе	После
ничего нет		

Генерация сессионной ключевой информации

Скоринг как криптографический протокол

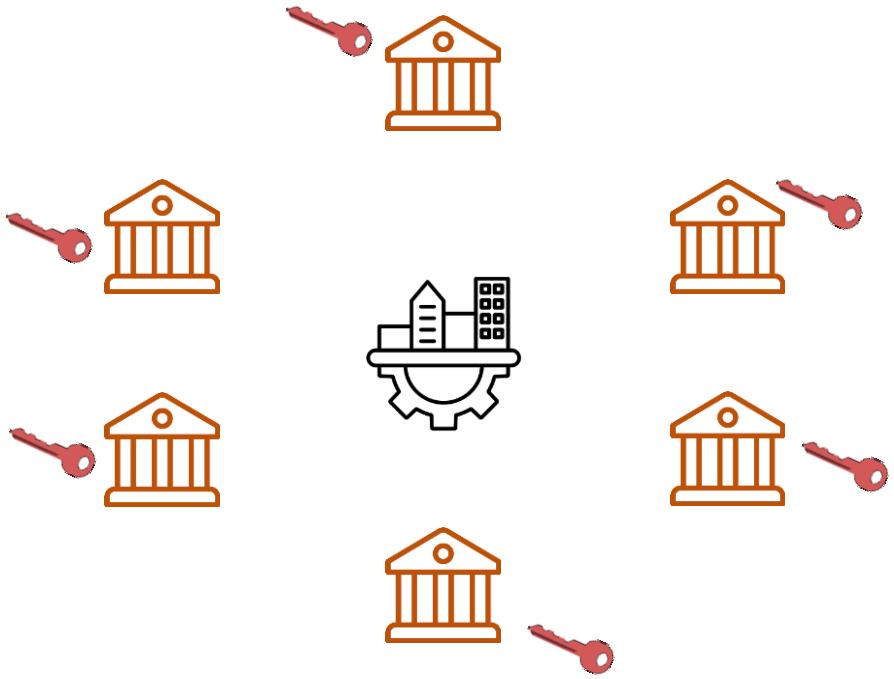
До	В процессе	После
ничего нет	совместная генерация банками ключевой информации (КИ)	



Генерация сессионной ключевой информации

Скоринг как криптографический протокол

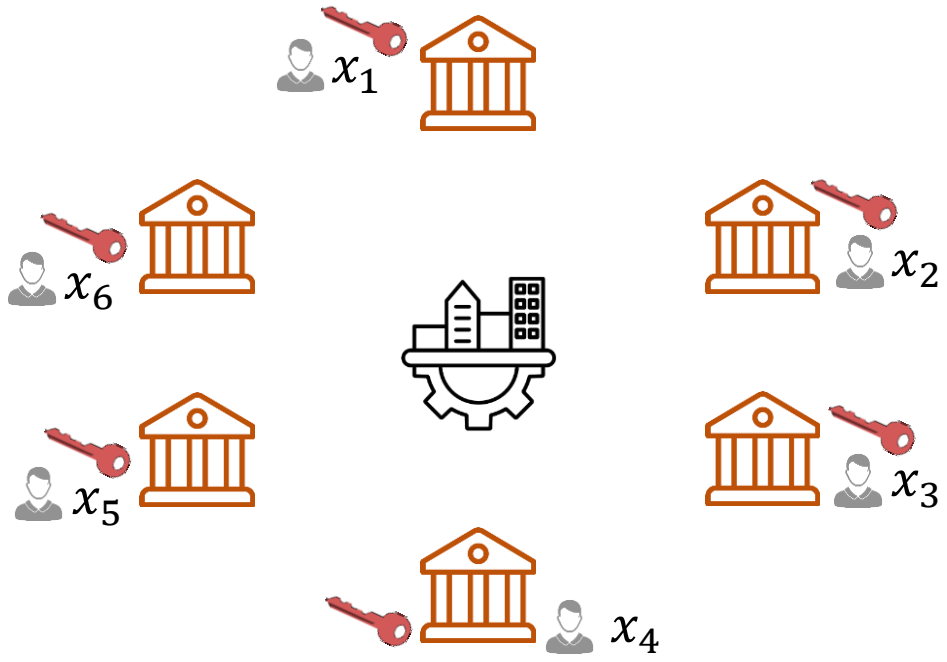
До	В процессе	После
ничего нет	совместная генерация банками ключевой информации (КИ)	у банков КИ



Генерация сессионной ключевой информации

Скоринг как криптографический протокол

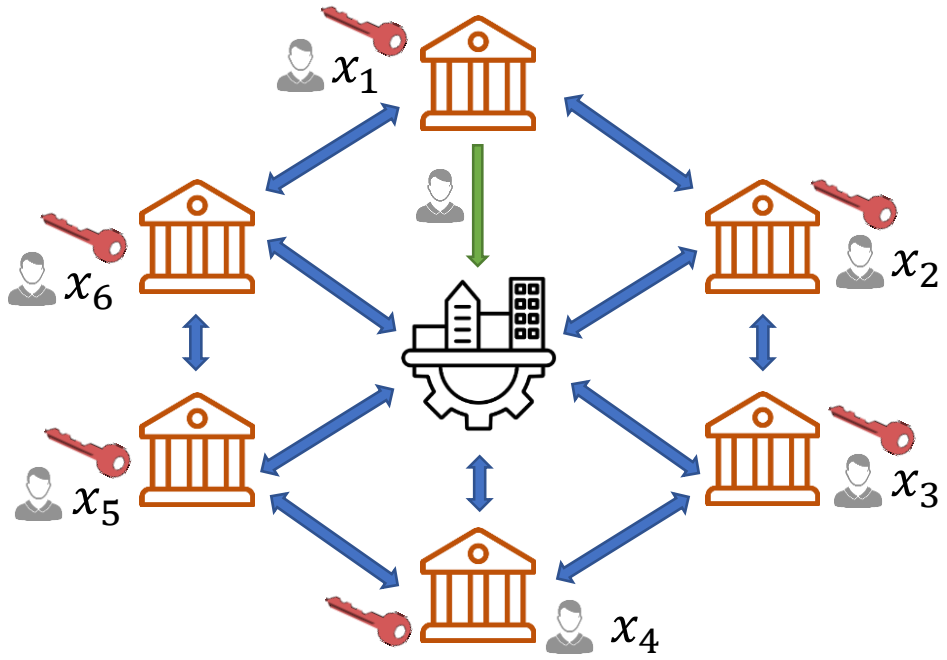
До	В процессе	После
у банков КИ и метрики		



Получение значения агрегированной метрики

Скоринг как криптографический протокол

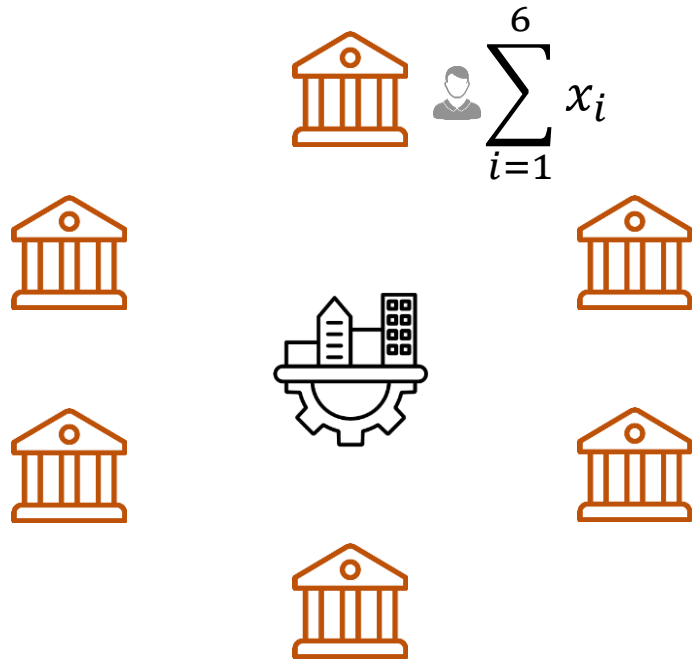
До	В процессе	После
у банков КИ и метрики	совместное вычисление значения агрегированной метрики	



Получение значения агрегированной метрики

Скоринг как криптографический протокол

До	В процессе	После
у банков КИ и метрики	совместное вычисление значения агрегированной метрики	у банка-инициатора значение агрегированной метрики



Получение значения агрегированной метрики

Что мы хотим от конфиденциального скоринга?

Банковская тайна

Что мы хотим от конфиденциального скоринга?

Банковская тайна

⇓

Вывод. Использование криптографического протокола скоринга «*Название протокола*» не нарушает банковскую тайну

Обоснование.

Что мы хотим от конфиденциального скоринга?

Банковская тайна

⇓

Вывод. Использование криптографического протокола скоринга «*Название протокола*» не нарушает банковскую тайну

Обоснование. Обосновать невозможно…

Тернистый путь от желаемого к возможному

Модель безопасности криптографического протокола

=

модель нарушителя
(перечисление потенциальных возможностей)

+

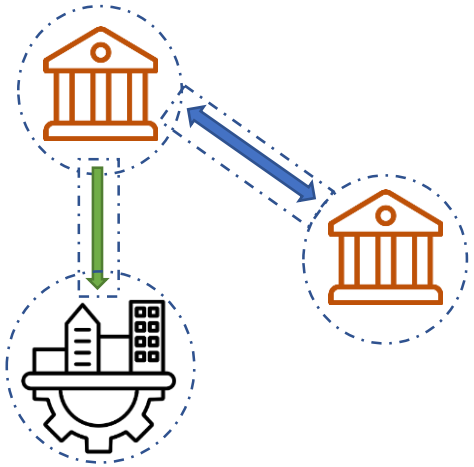
модель угроз
(определение ситуаций, которые могут привести к ущербу на практике)

Модель нарушителя

Внешний нарушитель

Можно обеспечить защиту не на уровне протокола скоринга:

- контролируемая зона
- защита каналов связи



Внутренний нарушитель

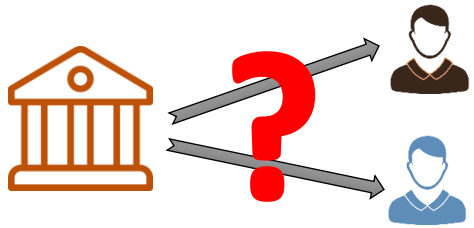
Есть банки и оператор, которые:

- не следуют протоколу (могут выбирать и отправлять произвольные сообщения, прерывать выполнение протокола)
- используют произвольные входные параметры
- навязывают честным участникам значения их входных параметров (принцип максимизации возможностей)
- вступают в сговор

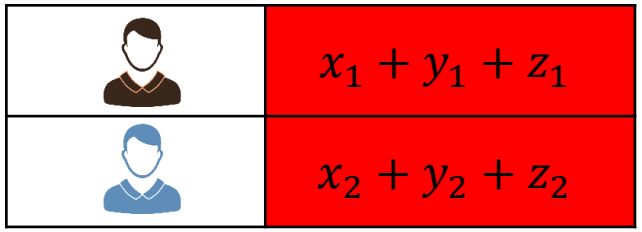
Модель угроз

Конфиденциальность метрик в банках

Анонимность обслуживания клиентов

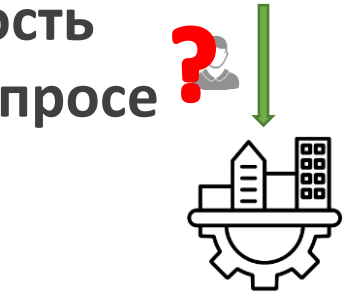


Конфиденциальность агрегированной метрики



Анонимность клиента в запросе

Анонимность инициатора запроса



Что мы хотим от конфиденциального скоринга?

Банковская тайна

⇓ 5 свойств безопасности

Вывод. Использование криптографического протокола скоринга «*Название протокола*» не нарушает банковскую тайну

5 свойств безопасности

Обоснование. Обосновать невозможно…

Что мы хотим от конфиденциального скоринга?

Банковская тайна

⇓ 5 свойств безопасности

Вывод. Использование криптографического протокола скоринга «*Название протокола*» не нарушает банковскую тайну

5 свойств безопасности

Обоснование. Обосновать невозможно… ?

Уточнение модели безопасности

- Проверить «крайние» случаи

  Если значение агрегированной метрики для клиента равно 0, то во всех банках $x_i = 0$

  ? Возможна ли такая ситуация на практике? Если да, является ли она угрозой?

- Ограничить возможность изменения множества банков

  Если после изменения множества банков в системе стало на один банк меньше, то по значениям агрегированной метрики до и после изменения можно однозначно восстановить значение метрики в банке

  ⇒ Необходимо определить правила «безопасного» изменения множества банков и реализовать доп. меры по контролю их выполнения

Уточнение модели безопасности

- Ограничить возможности нарушителя в рамках протокола

  Если в системе только один честный банк, то по значению агрегированной метрики можно однозначно восстановить значение метрики в банке

  ⇒ Необходимы орг.-тех. меры, обеспечивающие наличие не менее 2 честных банков

- Ограничить возможности нарушителя, внешние по отношению к протоколу

  Если известно, что в настоящий момент клиент А пришёл к банку 1 за кредитом, то по времени можно связать клиента с запросом

  ⇒ Необходимы орг.-тех. меры, обеспечивающие отсутствие информации о защищаемых значениях, полученной внешним образом

Вместо заключения

- Анализ безопасности протокола конфиденциального скоринга может быть проведён только в модели
- Модель безопасности протокола конфиденциального скоринга определяется возможными сценариями его использования и потенциальным ущербом от них с точки зрения практики
- При определении модели безопасности следует учесть множество аспектов, которые не видны «невооружённым» взглядом

Спасибо за внимание!

Контактная информация:

kyazhin@cryptopro.ru

amitrofanov@bloomtech.ru