конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто’2024»

скоринговая инфраструктура

BLOOMTECH

Емельянов П.Н., Митрофанов А.А., Болбачан В.С. / *Блумтех*

О компании

https://bloomtech.ru

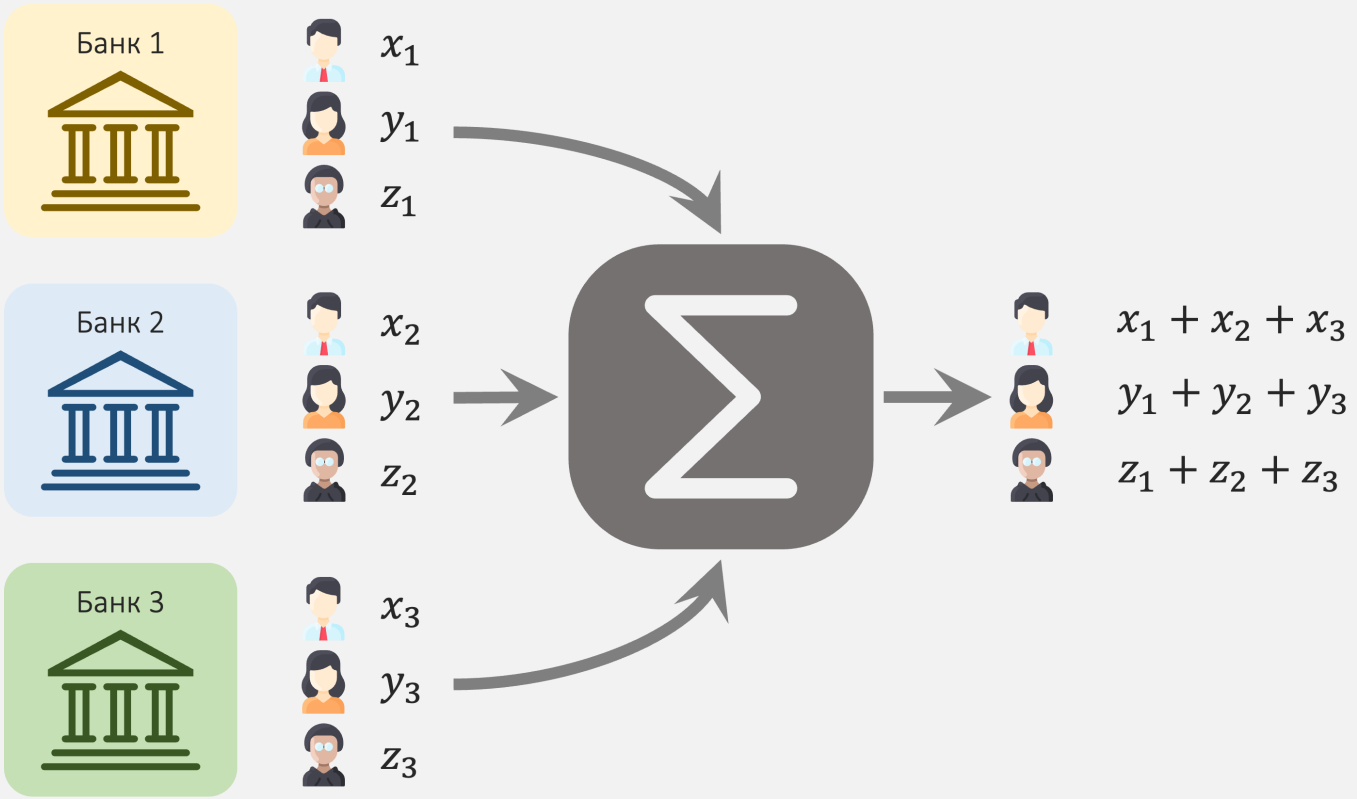
Российская компания, основанная в Москве в 2021

Разрабатываем решения для банковской сферы, изучаем и развиваем технологии совместных конфиденциальных вычислений и их практические приложения в Fintech (и не только).

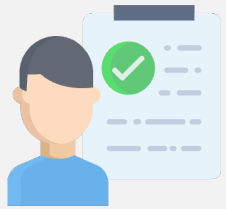
Капитализируем hands-on опыт в искусственном интеллекте, больших данных и их анализе, умеем внедрять сложные продукты в крупнейшие компании и государственные структуры Российской Федерации.

Bloomtech — независимая коммерческая компания, не аффилированная ни с одной кредитной организацией. Наша цель — честное, взаимовыгодное сотрудничество банков между собой и нами.

Агрегация данных



Кредитный скоринг

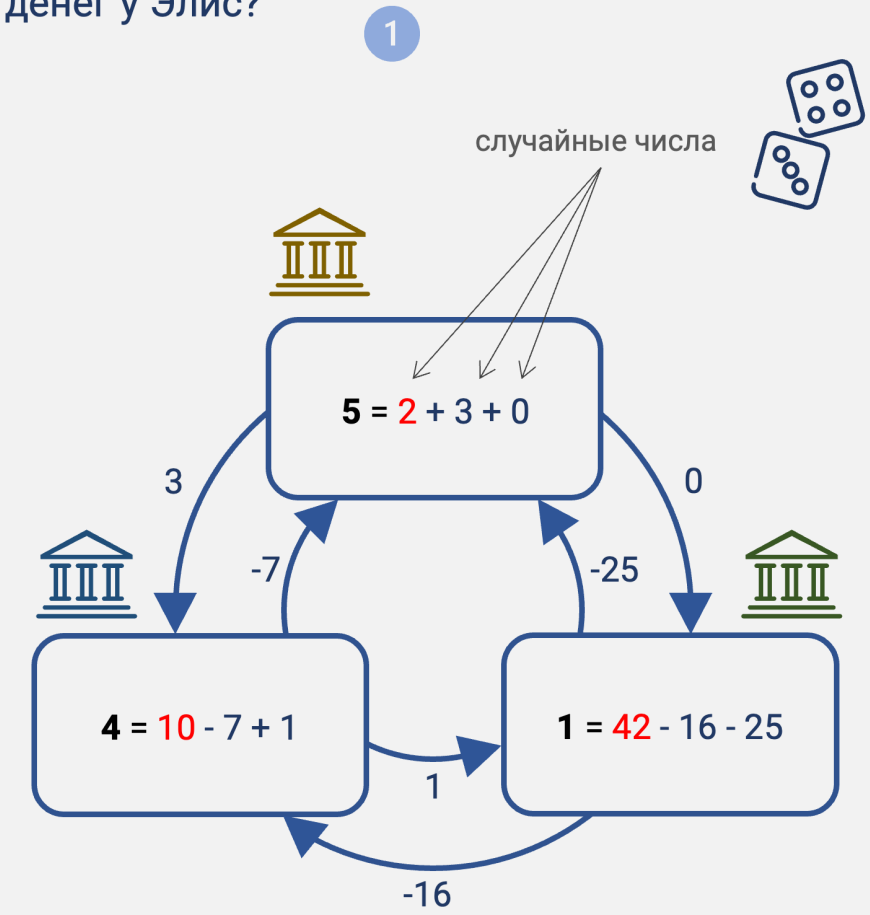


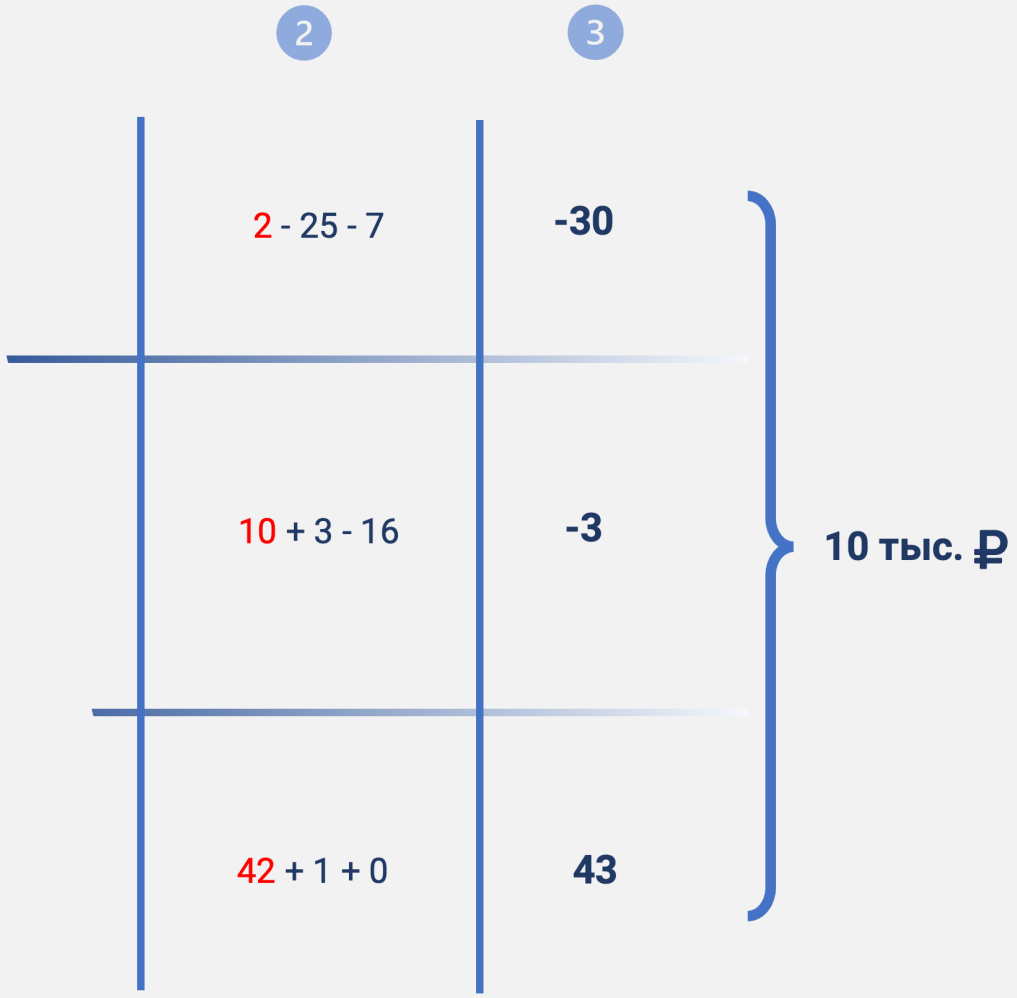
AML/KYC

Оценка дохода/PTI

Проще простого!

Сколько денег у Элис?





Не тут то было

Банковская тайна!

Криптографический протокол

Участники

Банки

Оператор

Протокол

Модель угроз

Банковская тайна ≈ 5 свойств безопасности

Конфиденциальность метрик

Протокол не позволяет участнику (участникам, вступившим в сговор) установить, какие операции по счетам совершало физическое лицо, а также ненулевой размер остатков денежных средств на указанных счетах.

Анонимность обслуживания клиентов

Протокол не позволяет участнику (участникам, вступившим в сговор) установить, в каком конкретно банке у физического лица открыты счета (заключены иные договоры с банком).

Анонимность инициатора запроса

Протокол не позволяет участнику (кроме оператора) определить участника, который направил запрос информации о конкретном физическом лице.

Анонимность клиента в запросе

Протокол не позволяет оператору получать информацию о том, в отношении какого физического лица (серия/номер паспорта) участники направляют свои запросы

Конфиденциальность агрегированной метрики

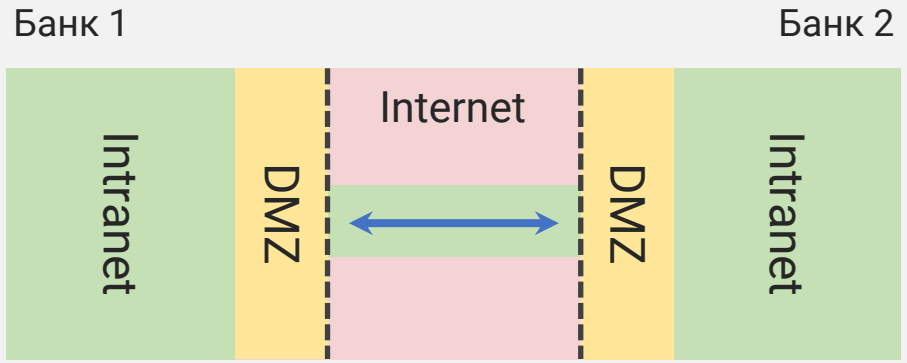
Никто, кроме банка-инициатора запроса, не может получить ненулевые значения агрегированных метрик физического лица, по которому другие банки не выполняли запросов на получение тех же агрегированных метрик.

Модель нарушителя

Внешний нарушитель

Защита обеспечивается не средствами протокола.

- Авторизованная зона
- Защита каналов связи



Внутренний нарушитель

Участники могут:

- Отклоняться от протокола, отправлять недостоверную информацию, прерывать протокол
- Использовать произвольные входные параметры
- Навязывать честным участникам значения их входных параметров
- Вступать в сговор

Инженерные ограничения

– Масштабируемость (банков много)

– Строгие SLA (1 секунда на ответ)

– Множество подключенных банков непостоянно (банки могут подключаться, отключаться и “моргать”)

– Сетевое взаимодействие (все со всеми)

В результате

- Разработали протокол (совместно с компанией КриптоПРО), удовлетворяющий 5 требованиям безопасности*
- Реализовали программную инфраструктуру, учитывающую инженерные ограничения
- Вышли в эксплуатацию (5 банков подключены, 5+ банков – на разных этапах подключения)
- Работаем над стандартом в ТК26 вместе с компаниями КриптоПРО, Актив, СПБ и АФТ

*При соблюдении организационно-технических мер

Выводы

- Безопасность межбанковского скоринга может быть доказана только в модели
- Строгость модели угроз для межбанковского скоринга определяется компромиссом между потенциальной выгодой и потенциальным ущербом
- Рынок демонстрирует запрос на системы конфиденциальных вычислений
- “Новизна” таких систем – основной ограничивающий фактор их применения

конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто’2024»

Спасибо!

Емельянов П.Н., Митрофанов А.А., Болбачан В.С. / *Блумтех*