Конфиденциальные вычисления и российская криптография

Смышляев Станислав Витальевич, д.ф.-м.н.
Генеральный директор КриптоПро

КРИПТОПРО

Криптография для решения новых задач

Дистанционное электронное голосование

Банковский скоринг

Мобильная ЭП для применения на массовых устройствах

Распознавание человеческой активности

Выявление фактов мошенничества в финансовом секторе экономики

Вычисление среднего рейтинга пользователя сервисом

Генетические и медицинские исследования

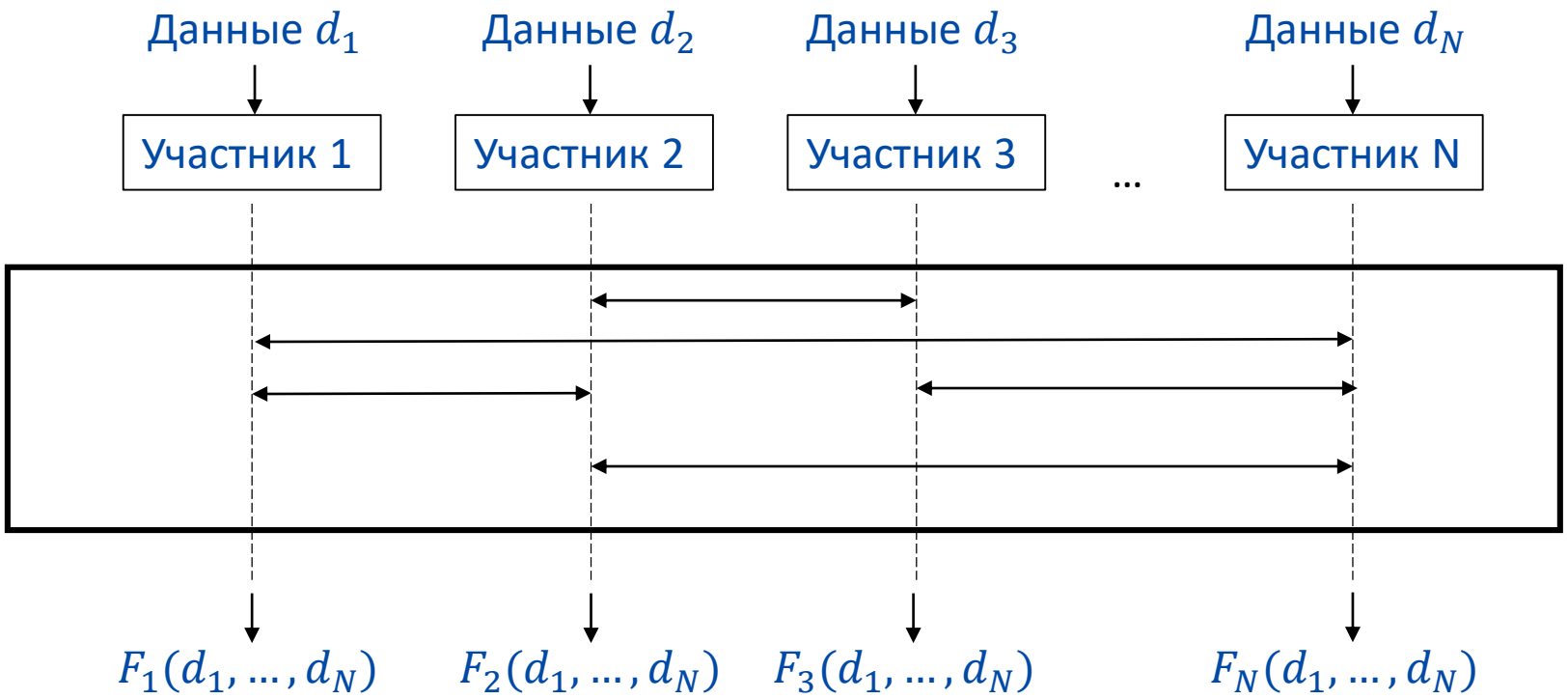
Определение перспективной категории малого бизнеса

Оценка эффективности рекламной кампании

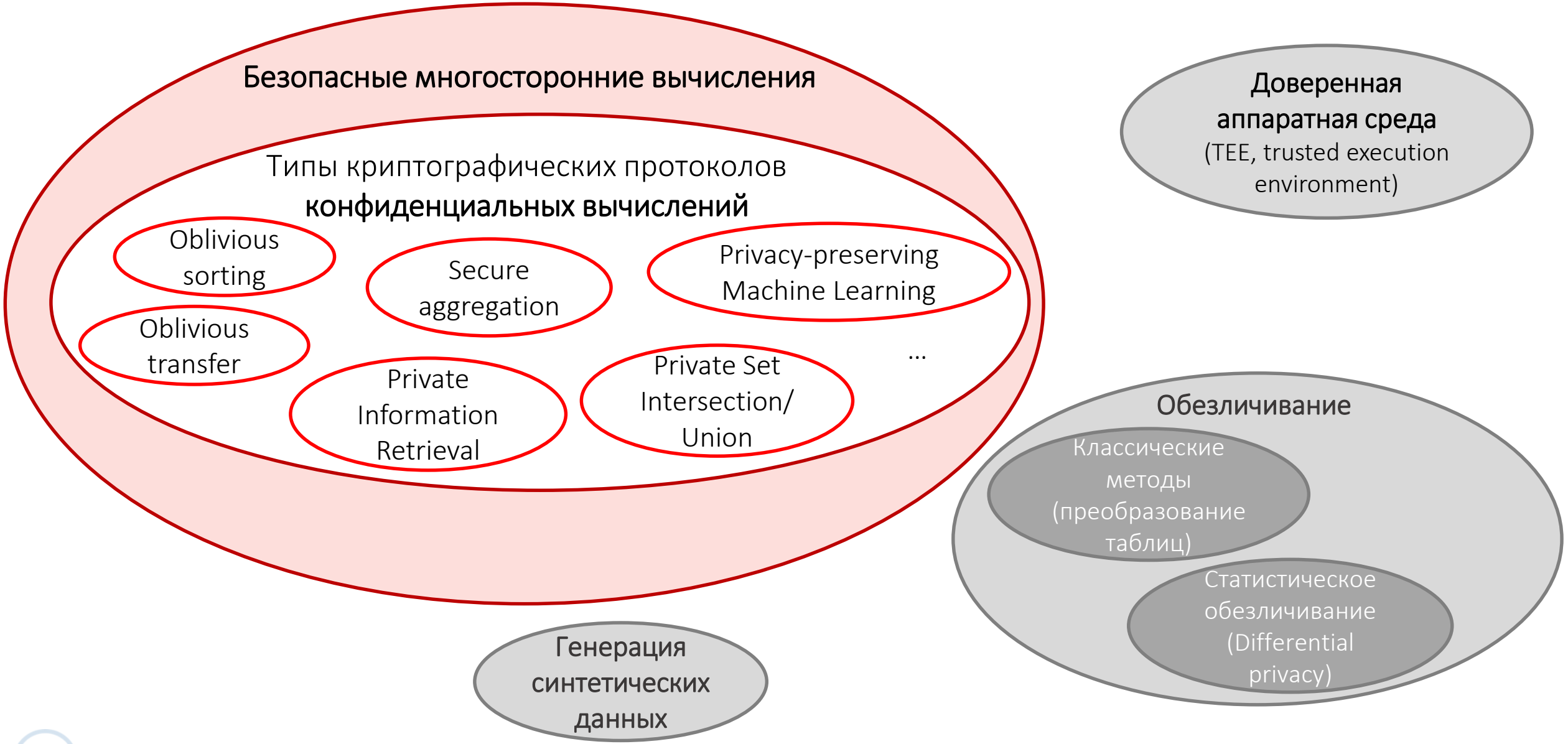
...

Конфиденциальные вычисления как криптографические протоколы

Задача: вычислить значение функции с использованием данных нескольких участников, обеспечивая при этом необходимый уровень конфиденциальности входных и выходных данных, вычисляемой функции и промежуточных значений.



Конфиденциальные вычисления – криптографический протокол



Конфиденциальные вычисления в России: ДЭГ

ДИСТАНЦИОННОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ

Задача: посчитать сумму голосов, обеспечив сохранение тайны голосования

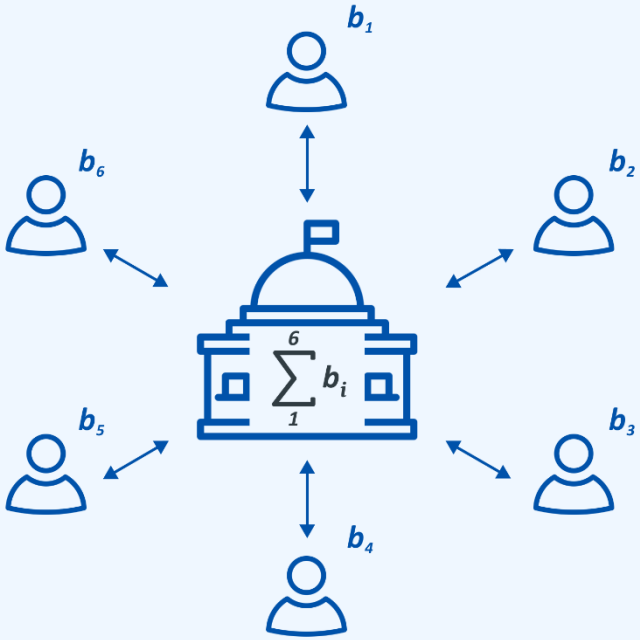


Схема подписи вслепую

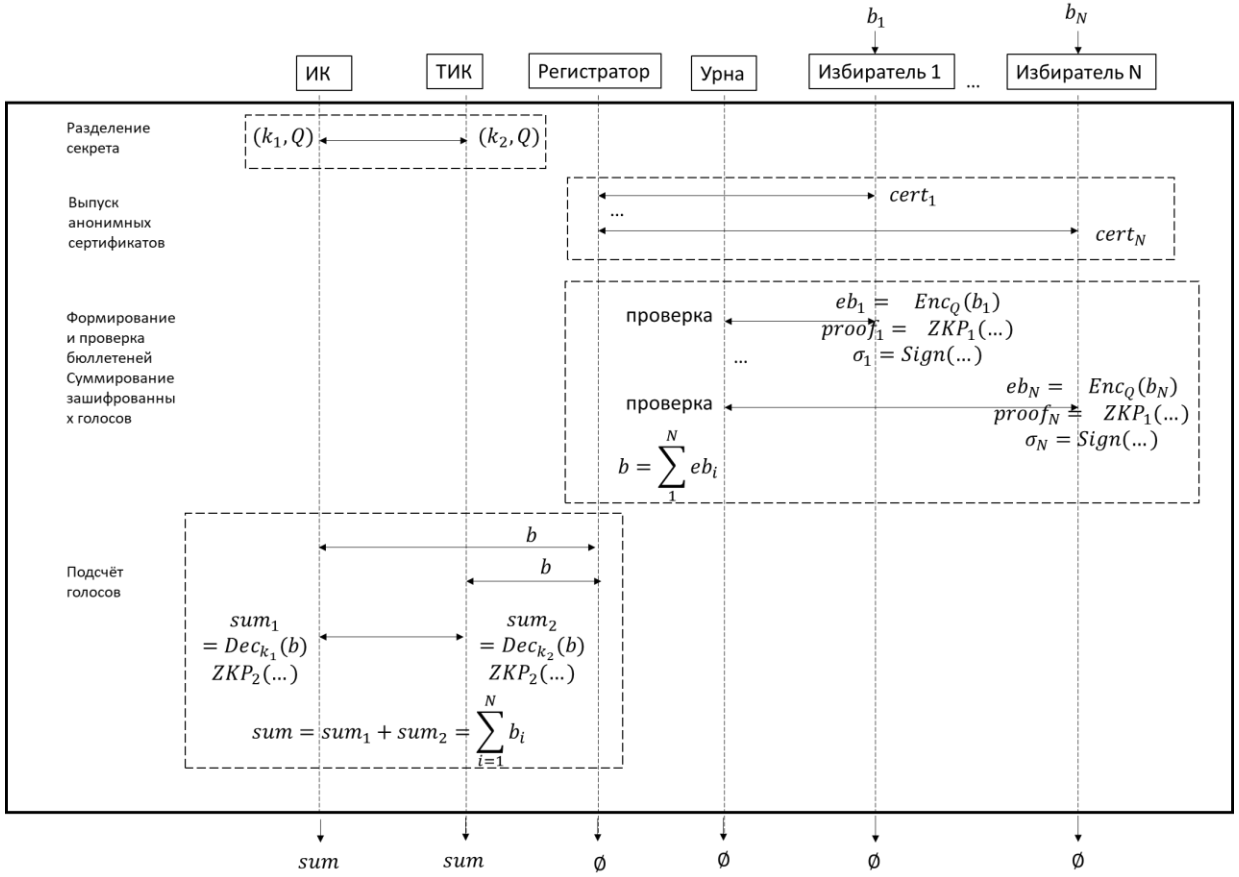
Схема подписи ГОСТ 34.10-2018

Схема разделения секрета

ДЭГ

Два протокола доказательств с нулевым разглашением (ZKP)

Схема гомоморфного шифрования



КРИПТОПРО

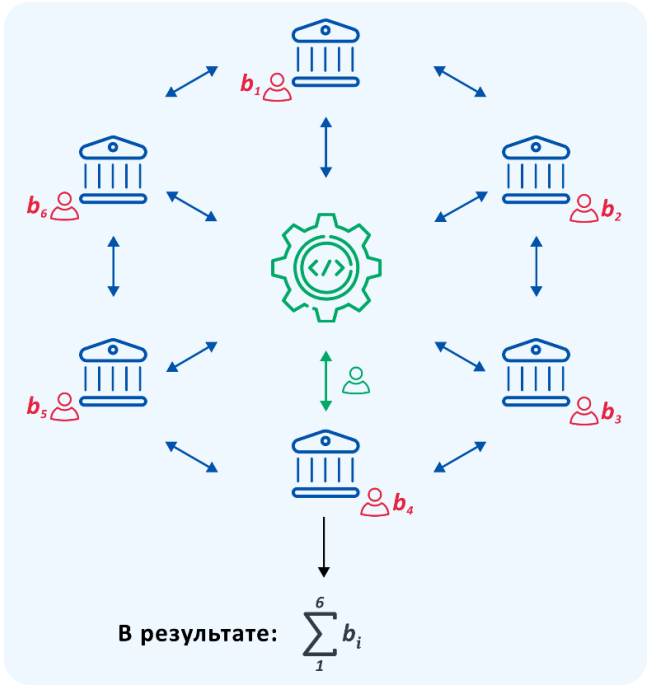
Конфиденциальные вычисления в России: скоринговые платформы

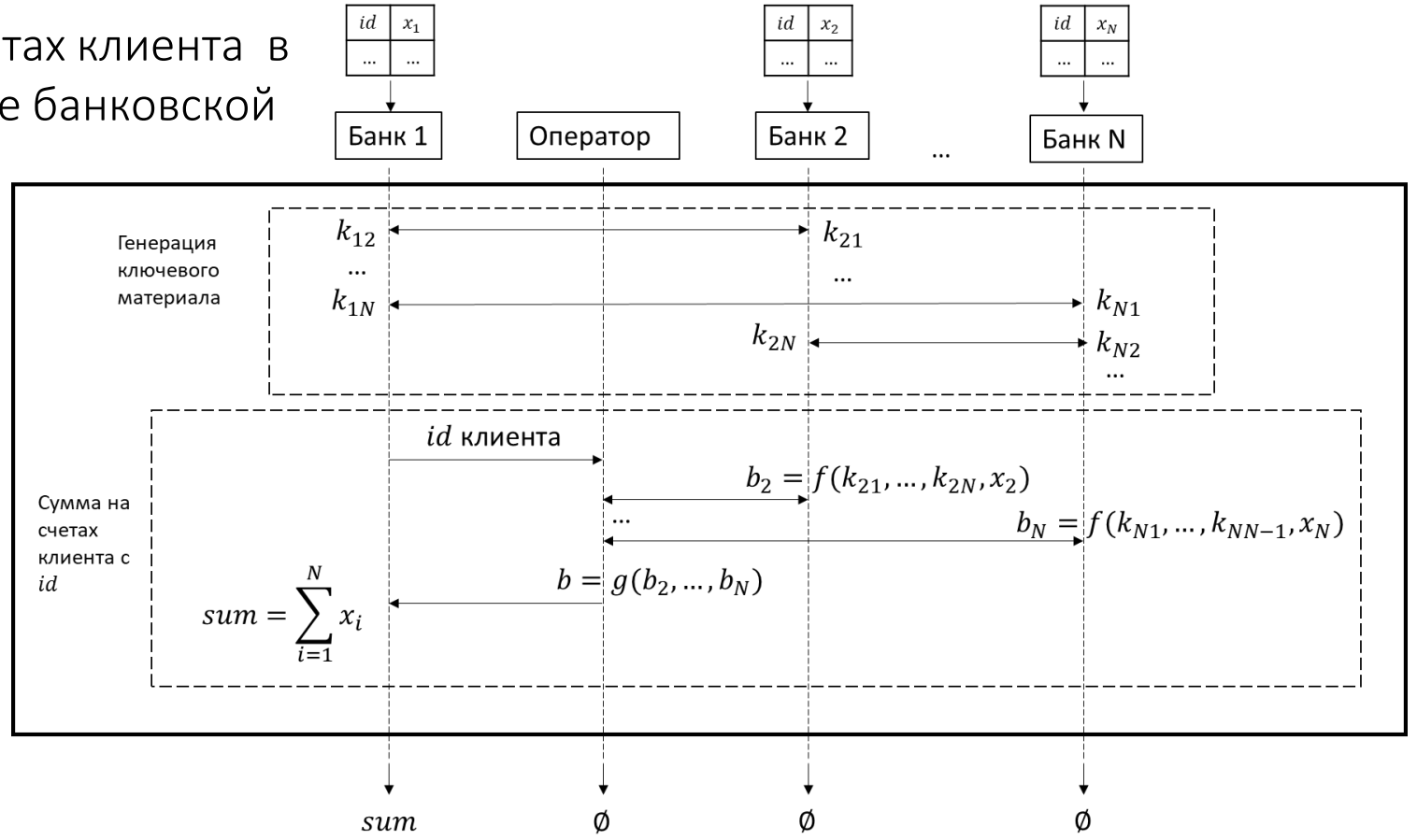
Подробнее:

Межбанковский скоринг на основе технологий конфиденциальных вычислений

– **Митрофанов Александр Александрович**, к.т.н., директор по развитию бизнеса, Блумтех

Задача: посчитать сумму денег на счетах клиента в разных банках, обеспечив сохранение банковской тайны





Мобильная электронная подпись на массовых устройствах

Задача: защита ключей в условиях отсутствия доверия клиенту и серверу (исключая сговор между ними)

Утеря мобильного устройства	Компрометация памяти устройства в любой момент времени	Полная компрометация серверных компонент

Мобильная электронная подпись на массовых устройствах

Задача: защита ключей в условиях отсутствия доверия клиенту и серверу (исключая сговор между ними)

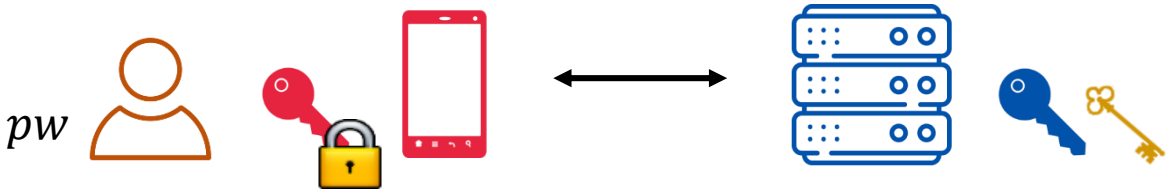
Утеря мобильного устройства

Компрометация памяти устройства в любой момент времени

Полная компрометация серверных компонент

Требуется протокол безопасных многосторонних вычислений

Для получения доступа к ключу необходимо выработать секрет на основе pw и



Подпись на ключе = +

КРИПТОПРО

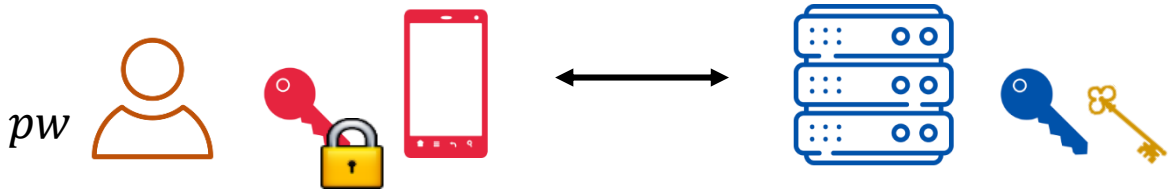
Мобильная электронная подпись на массовых устройствах

Задача: защита ключей в условиях отсутствия доверия клиенту и серверу (исключая сговор между ними)

Утеря мобильного устройства

Компрометация памяти устройства в любой момент времени

Полная компрометация серверных компонент

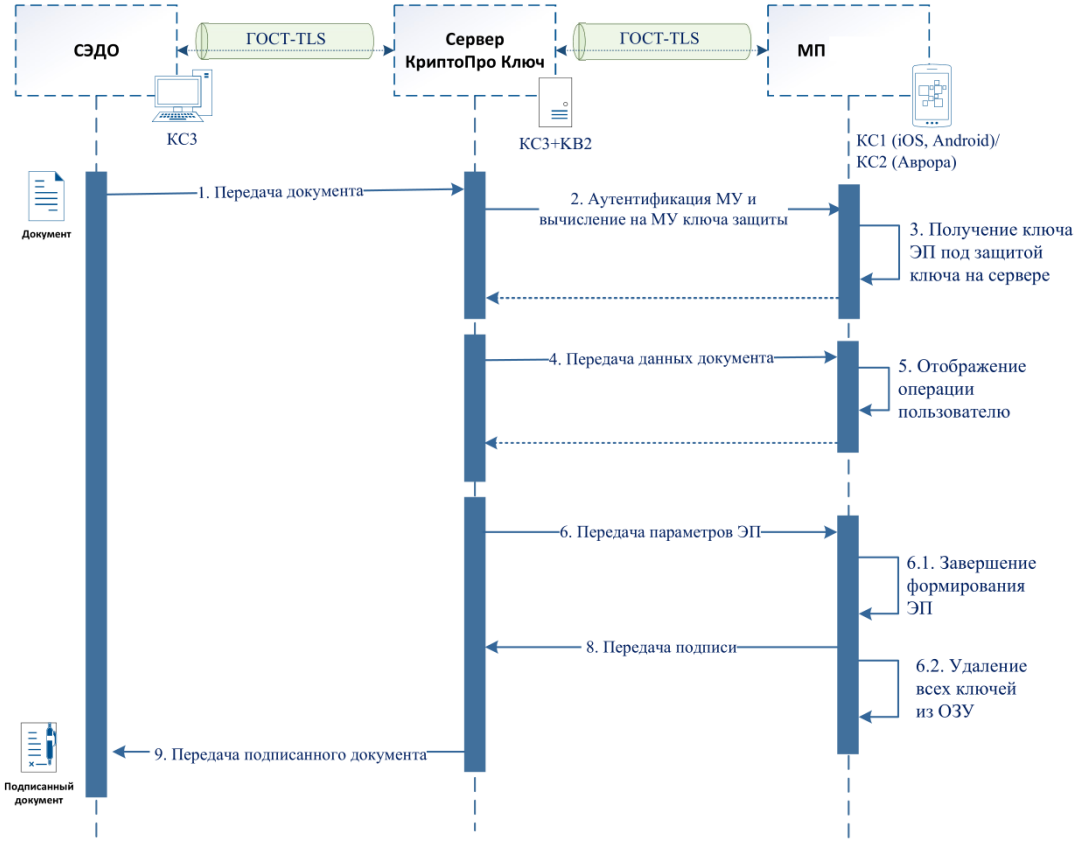


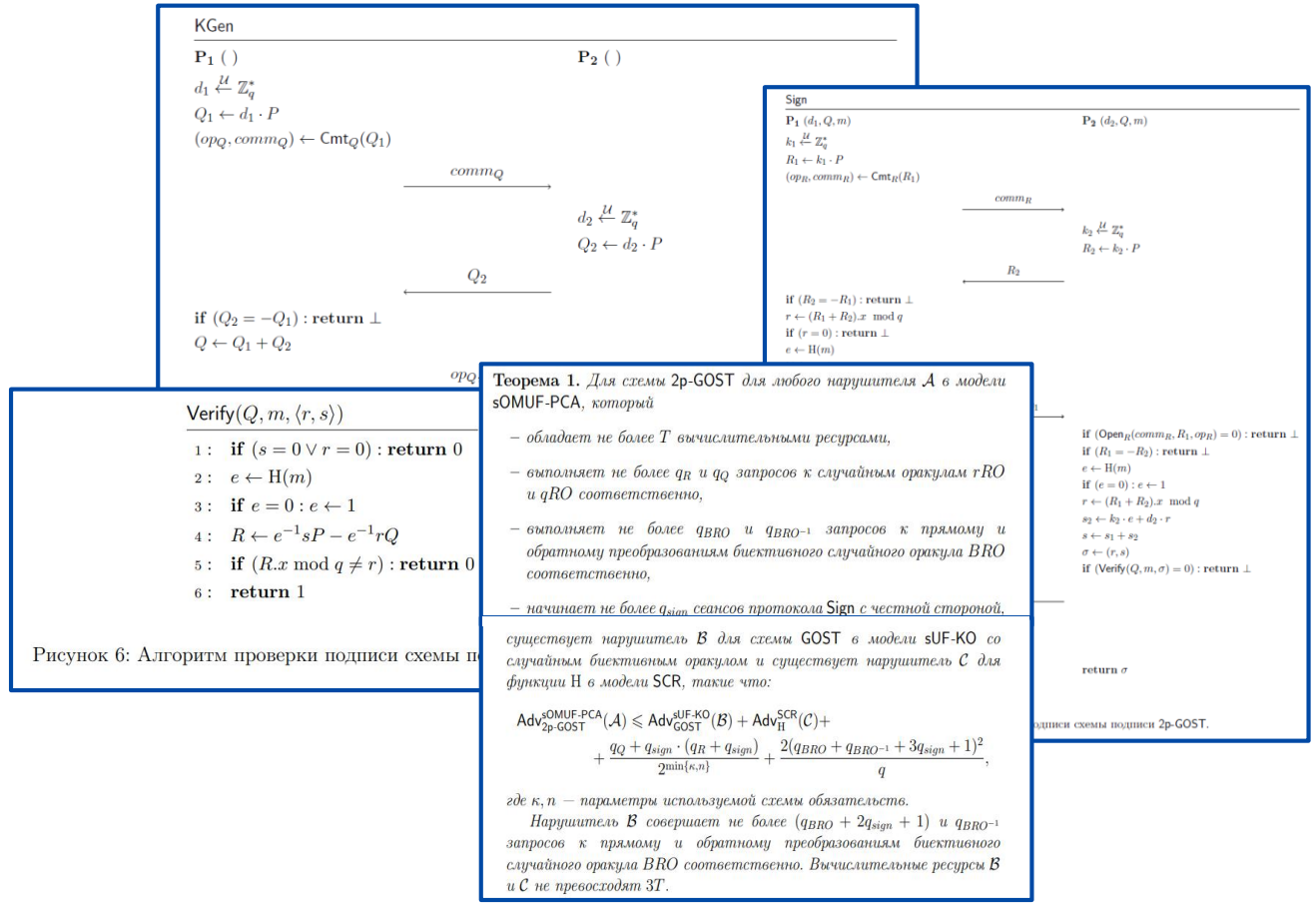
Механизмы защиты:

Защита на высокоэнтропийных секретах, вычисленных **распределённым образом**

Ключ ЭП ни в один момент времени не появляется в «собранном» виде, не известен ни клиенту, ни серверу. **Все операции с ключом подписи – распределённым образом**

Решение: схема DKSSP





KGen

$\mathbf{P}_1$ ( )

$d_1 \xleftarrow{u} \mathbb{Z}_q^*$

$Q_1 \leftarrow d_1 \cdot P$

$(op_Q, comm_Q) \leftarrow \mathsf{Cmt}_Q(Q_1)$

$comm_Q$

$\mathbf{P}_2$ ( )

$d_2 \xleftarrow{u} \mathbb{Z}_q^*$

$Q_2 \leftarrow d_2 \cdot P$

Q_2

if $(Q_2 = -Q_1)$: return $\perp$

$Q \leftarrow Q_1 + Q_2$

op_Q

Sign

$\mathbf{P}_1\ (d_1, Q, m)$ $\mathbf{P}_2\ (d_2, Q, m)$

$k_1 \xleftarrow{u} \mathbb{Z}_q^*$

$R_1 \leftarrow k_1 \cdot P$

$(op_R, comm_R) \leftarrow \mathsf{Cmt}_R(R_1)$

$comm_R$

$k_2 \xleftarrow{u} \mathbb{Z}_q^*$

$R_2 \leftarrow k_2 \cdot P$

R_2

if $(R_2 = -R_1)$: return $\perp$

$r \leftarrow (R_1 + R_2).x \mod q$

if $(r = 0)$: return $\perp$

$e \leftarrow \mathrm{H}(m)$

if $(\mathsf{Open}_R(comm_R, R_1, op_R) = 0)$: return $\perp$

if $(R_1 = -R_2)$: return $\perp$

$e \leftarrow \mathrm{H}(m)$

if $(e = 0)$: $e \leftarrow 1$

$r \leftarrow (R_1 + R_2).x \mod q$

$s_2 \leftarrow k_2 \cdot e + d_2 \cdot r$

$s \leftarrow s_1 + s_2$

$\sigma \leftarrow (r, s)$

if $(\mathsf{Verify}(Q, m, \sigma) = 0)$: return $\perp$

return σ

Verify$(Q, m, \langle r, s \rangle)$

1 : if $(s = 0 \vee r = 0)$: return 0

2 : $e \leftarrow \mathrm{H}(m)$

3 : if $e = 0$: $e \leftarrow 1$

4 : $R \leftarrow e^{-1}sP - e^{-1}rQ$

5 : if $(R.x \bmod q \neq r)$: return 0

6 : return 1

Рисунок 6: Алгоритм проверки подписи схемы п

Теорема 1. *Для схемы* 2p-GOST *для любого нарушителя* $\mathcal{A}$ *в модели* sOMUF-PCA, *который*

- *обладает не более* T *вычислительными ресурсами,*
- *выполняет не более* q_R *и* q_Q *запросов к случайным оракулам* rRO *и* qRO *соответственно,*
- *выполняет не более* q_{BRO} *и* $q_{BRO^{-1}}$ *запросов к прямому и обратному преобразованиям биективного случайного оракула* BRO *соответственно,*
- *начинает не более* q_{sign} *сеансов протокола* Sign *с честной стороной,*

существует нарушитель $\mathcal{B}$ *для схемы* GOST *в модели* sUF-KO *со случайным биективным оракулом и существует нарушитель* $\mathcal{C}$ *для функции* H *в модели* SCR, *такие что:*

$$\mathsf{Adv}^{\mathsf{sOMUF\text{-}PCA}}_{\mathsf{2p\text{-}GOST}}(\mathcal{A}) \leqslant \mathsf{Adv}^{\mathsf{sUF\text{-}KO}}_{\mathsf{GOST}}(\mathcal{B}) + \mathsf{Adv}^{\mathsf{SCR}}_{\mathrm{H}}(\mathcal{C}) + \\ + \frac{q_Q + q_{sign} \cdot (q_R + q_{sign})}{2^{\min\{\kappa, n\}}} + \frac{2(q_{BRO} + q_{BRO^{-1}} + 3q_{sign} + 1)^2}{q},$$

где κ, n *— параметры используемой схемы обязательств.*

Нарушитель $\mathcal{B}$ *совершает не более* $(q_{BRO} + 2q_{sign} + 1)$ *и* $q_{BRO^{-1}}$ *запросов к прямому и обратному преобразованиям биективного случайного оракула* BRO *соответственно. Вычислительные ресурсы* $\mathcal{B}$ *и* $\mathcal{C}$ *не превосходят* $3T$.

одписи схемы подписи 2p-GOST.

Е.К. Алексеев, Л.Р. Ахметзянова, А.А. Бабуева, Л.О. Никифорова, С.В. Смышляев, «Двусторонняя схема подписи ГОСТ», Математические вопросы криптографии, 15:2 (2024), 7–28

Схема DKSSP: ключевые свойства безопасности

Компрометация устройства клиента не приводит к компрометации ключа

Для создания подписи/регистрации нового ключа нарушителем необходима компрометация аутентификации в ходе взаимодействия с сервером (аутентификация за счёт обладания устройством и знания пароля).

Компрометация сервера не приводит к компрометации ключа или возможности создания подписи нарушителем.

Даже одновременная компрометация устройства клиента и его пароля не приводит к компрометации ключа или возможности создания подписи нарушителем в обход протокола (подлежащего аудиту).

Реализация DKSSP – в средстве электронной подписи **КриптоПро Ключ**

Подробнее:

ТЕМАТИЧЕСКАЯ СЕКЦИЯ

ТЕХНОЛОГИИ ЭЛЕКТРОННОЙ ПОДПИСИ

ВЕДУЩИЕ

МАЛИНИН Юрий Витальевич
Президент, Ассоциация «РОСЭУ»

СМИРНОВ Павел Владимирович
К.т.н., директор по развитию, КриптоПро, эксперт РОСЭУ

Преимущество ГОСТ 34.10-2018 перед ECDSA: распределенная подпись

- ГОСТ 34.10-2018

$$r \leftarrow (k \cdot P).x \bmod q \qquad k = k_1 + k_2 \qquad r \leftarrow (k_1 \cdot P + k_2 \cdot P).x \bmod q$$
$$s \leftarrow ke + dr \bmod q \qquad d = d_1 + d_2 \qquad s \leftarrow (k_1 + k_2)e + (d_1 + d_2)r$$

- ECDSA

$$r \leftarrow (k \cdot P).x \bmod q \qquad ?\, k^{-1} = k_1 + k_2 \qquad r \leftarrow (k_1 \cdot k_2 \cdot P).x \bmod q$$
$$s \leftarrow k^{-1}(e + dr) \bmod q \qquad k = k_1 \cdot k_2 \qquad s \leftarrow k_1^{-1} \cdot k_2^{-1}(e + d_1 \cdot d_2 \cdot r)$$
$$d = d_1 \cdot d_2$$

необходимо существенно усложнять протокол, добавляя гомоморфное шифрование

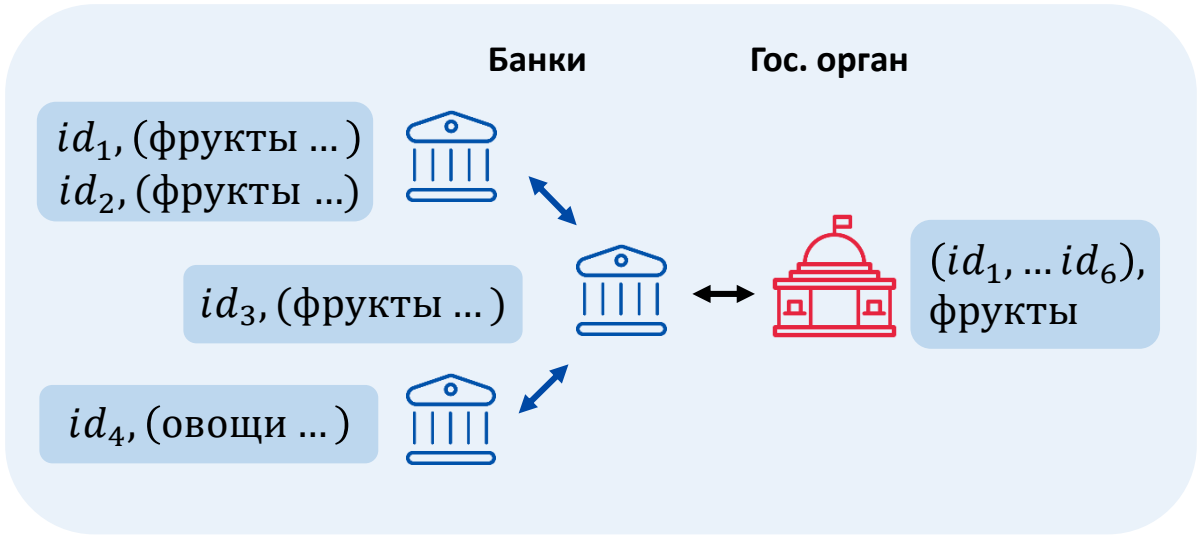
Подробнее:

О скрытых возможностях отечественного варианта уравнения Эль-Гамаля

– **Гуселев Антон Михайлович**, Академия криптографии РФ

Перспективные задачи в области конфиденциальных вычислений

Задача: посчитать количество граждан определённой категории, которые покупают товары заданного типа

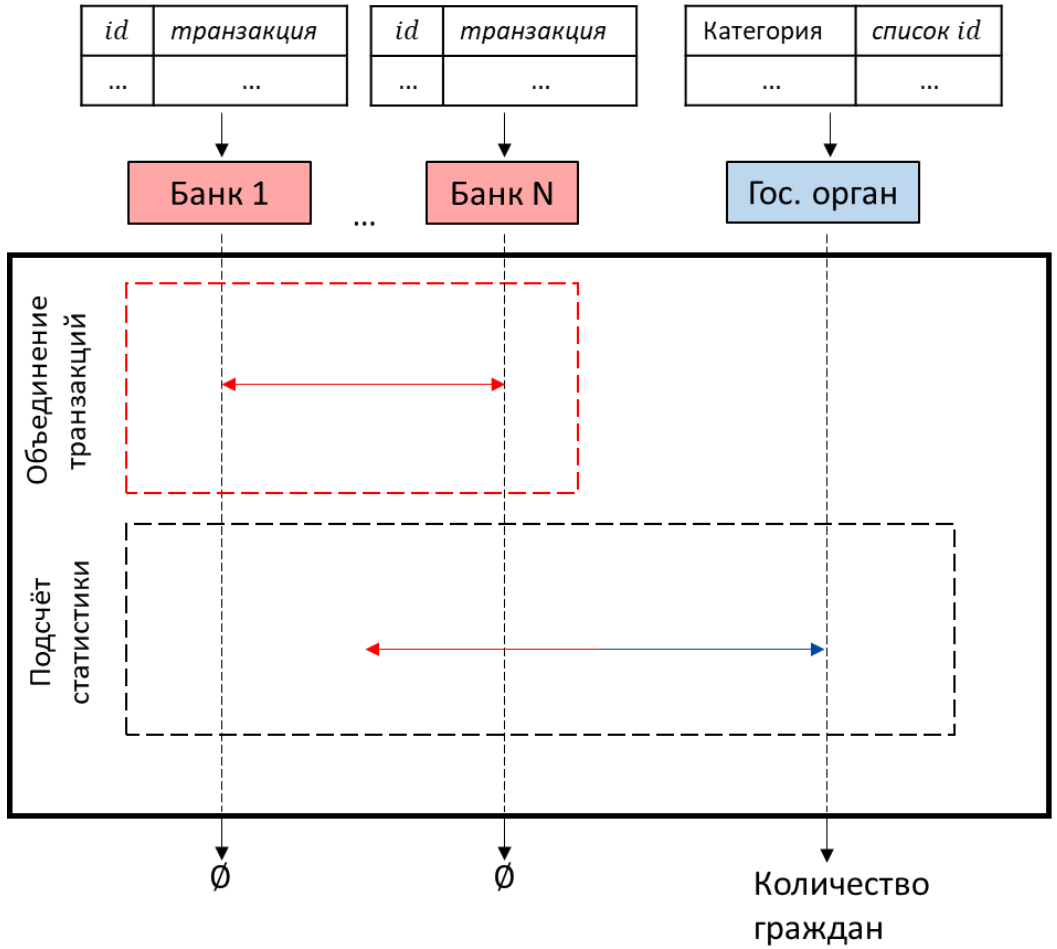


В результате

Количество id клиентов банков, содержащихся в списке гос. органа, у которых в транзакциях есть товары заданного типа

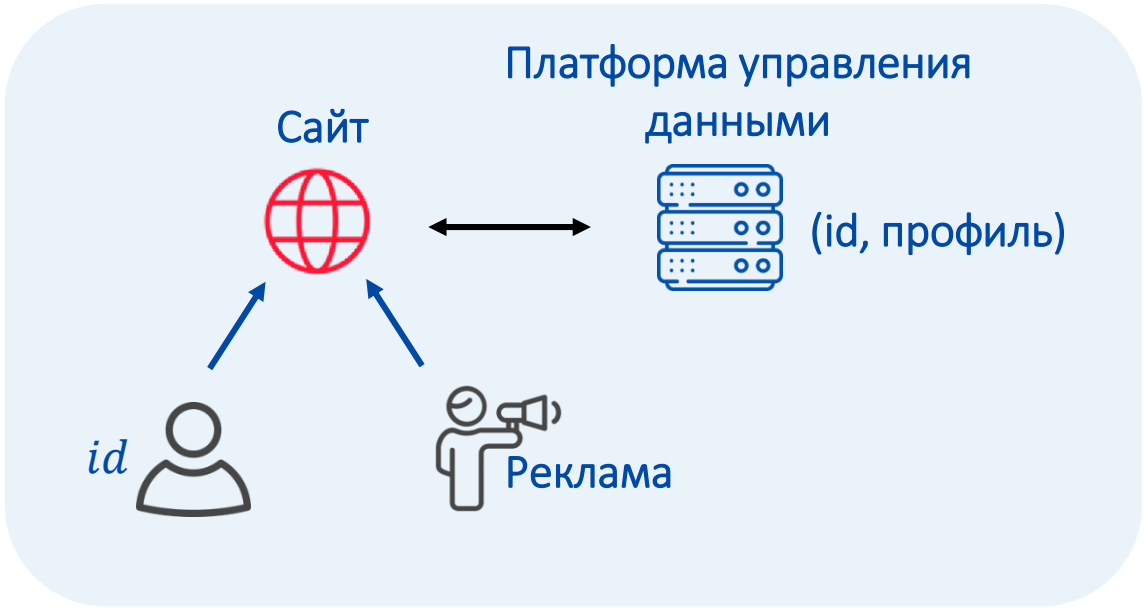
= 3

Возможный подход к решению



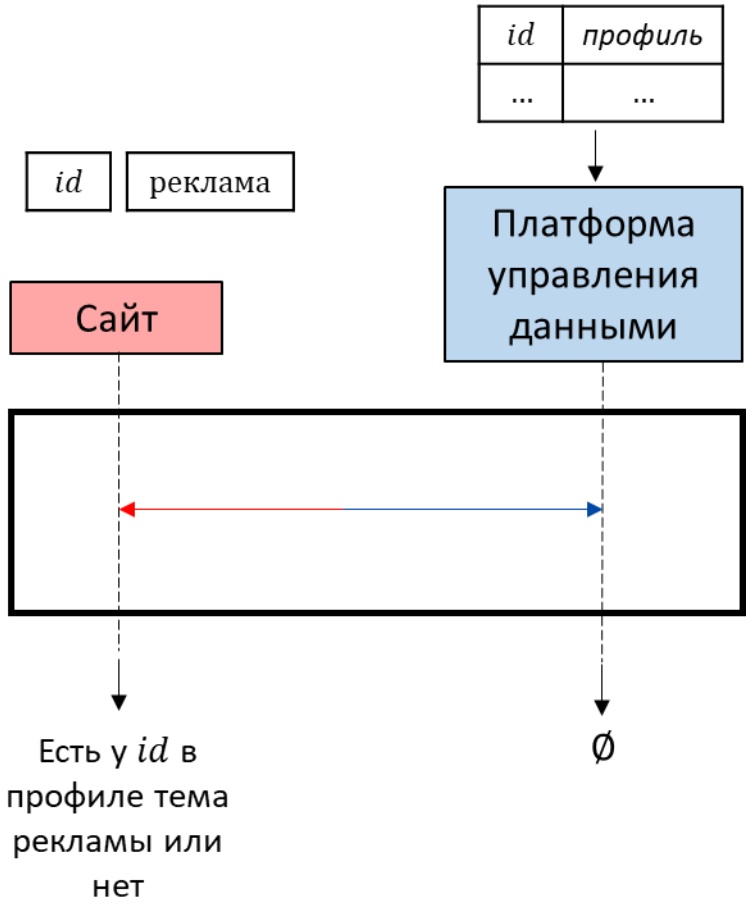
Перспективные задачи в области конфиденциальных вычислений

Задача: показывать контекстную рекламу только тем пользователям, которые интересовались схожей темой



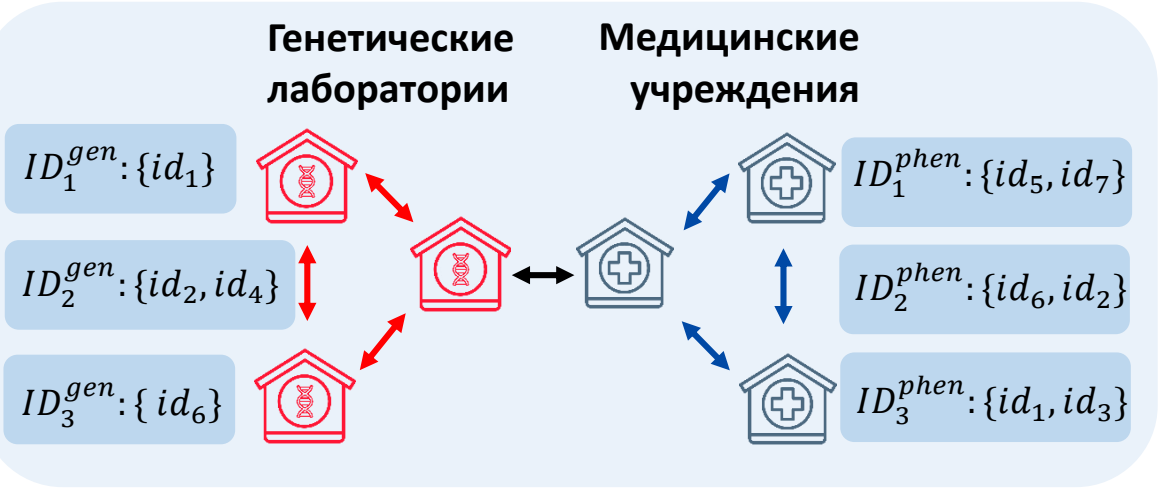
В результате

Соответствует ли реклама профилю пользователя



Перспективные задачи в области конфиденциальных вычислений

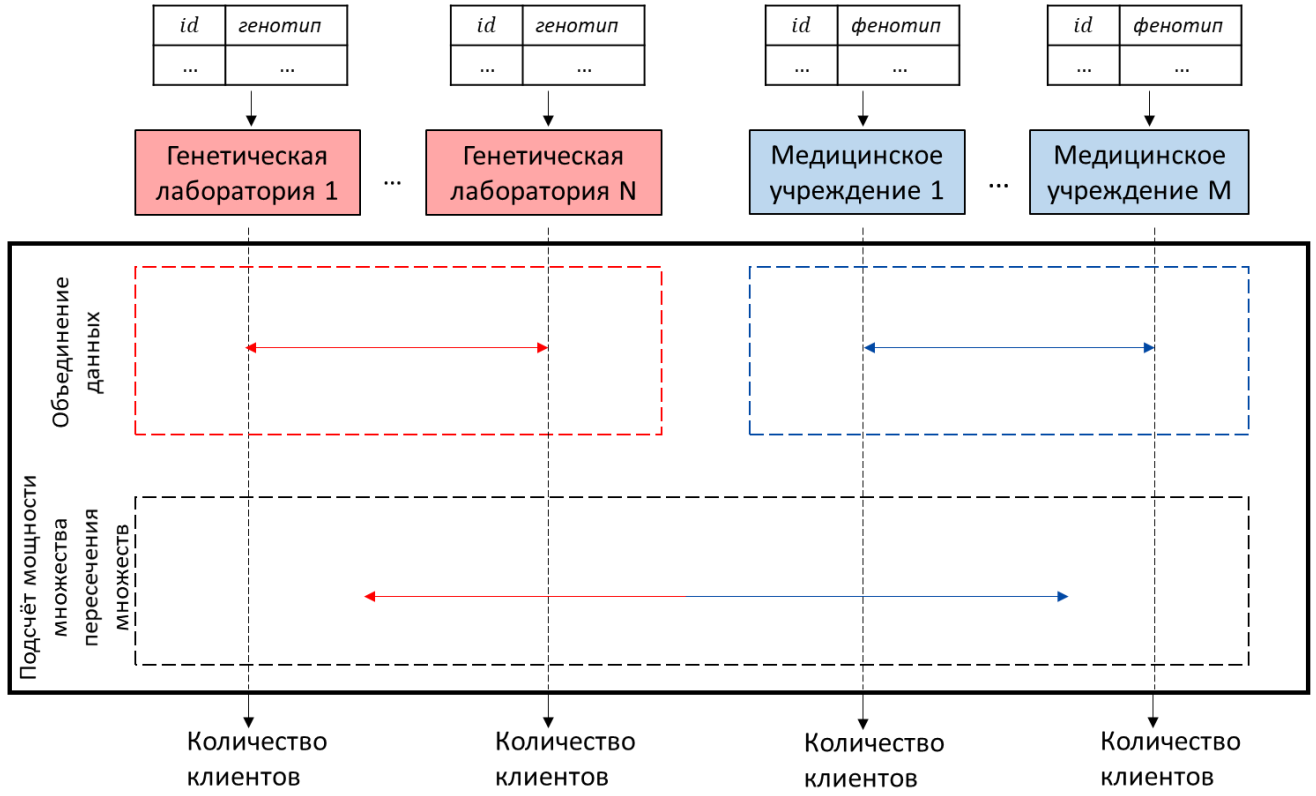
Задача: посчитать количество клиентов, которые одновременно обладают заданными генотипическими и фенотипическими признаками, сохраняя врачебную тайну



В результате каждый участник

$$\left|\left(ID_1^{phen} \cup ID_2^{phen} \cup ID_3^{phen}\right)\right|$$

Возможный подход к решению



Перспективные задачи в области конфиденциальных вычислений

НИР «Камин», НТЦ ЦК (ответственный исполнитель: Никифорова Л. О.):

1. Оценка эффективности рекламной кампании
2. Вычисление среднего рейтинга пользователя сервисом
3. Распознавание человеческой активности
4. Определение перспективной категории малого бизнеса
5. Выявление фактов мошенничества в финансовом секторе экономики

Подробнее:

КРУГЛЫЙ СТОЛ

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ

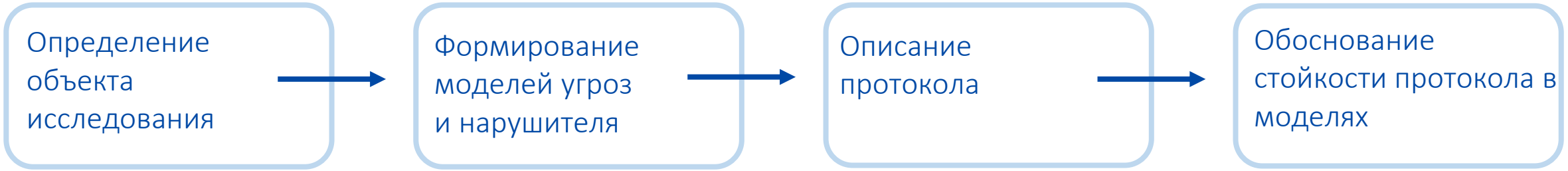
ВЕДУЩИЕ

МАРШАЛКО Григорий Борисович
ТК 26

КЯЖИН Сергей Николаевич
К.ф.-м.н., зам. начальника отдела криптографических исследований, КриптоПро, доцент НИЯУ МИФИ

Эквивалентность общих подходов к исследованиям

Подходы и принципы – привычные для современной криптографии



Подробнее:

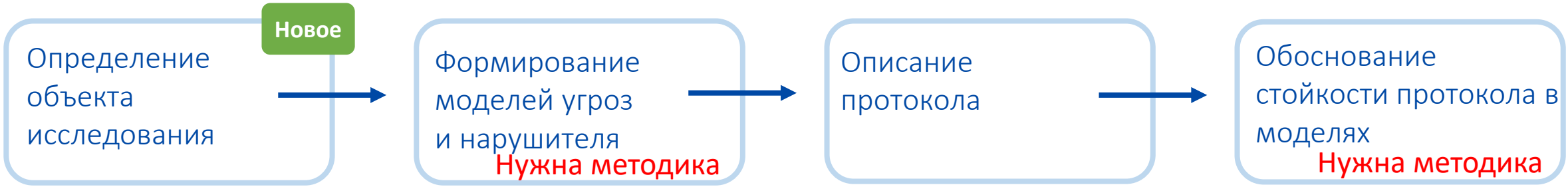
Аналитический доклад «Конфиденциальные вычисления и доверенные среды исполнения. Secure Multiparty Computation».

Раздел «Безопасность, которую можно доказать».

Авторы: ведущие эксперты области из Ассоциации больших данных, Bloomtech, КриптоПро, Privacy Advocates и Aggregion.

Эквивалентность общих подходов к исследованиям

Подходы и принципы – привычные для современной криптографии



Подробнее:

Аналитический доклад «Конфиденциальные вычисления и доверенные среды исполнения. Secure Multiparty Computation».

Раздел «Безопасность, которую можно доказать».

Авторы: ведущие эксперты области из Ассоциации больших данных, Bloomtech, КриптоПро, Privacy Advocates и Aggregion.

Эквивалентность общих подходов к исследованиям

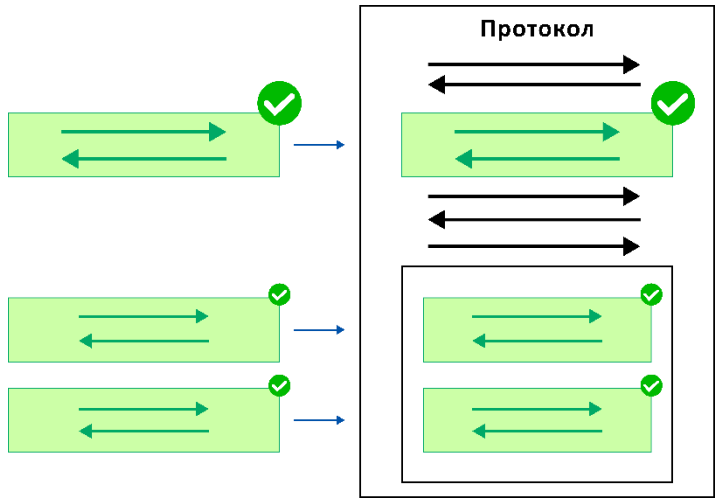
Подходы и принципы – привычные для современной криптографии

Новое

Определение объекта исследования → Формирование моделей угроз и нарушителя → Описание протокола → Обоснование стойкости протокола в моделях

Нужна методика

Нужна методика



Важна **модульность** – возможность переиспользования результатов анализа.

Внедрение новых технологий и решение проблем старых

- «В существующих СКЗИ, нормативной базе, внедрениях много проблем, сперва бы с ними разобраться!»
- Те же опасения высказывались в процессе обсуждений следующих тем:
  - Биометрические системы (ЕБС, КБС)
  - Цифровой Рубль
  - Мобильная электронная подпись
  - Криптография для «умных счетчиков», «умных пломб» и пр.
  - Криптография в дистанционном электронном голосовании
  - Криптография в платежных системах

– каждое из этих направлений подсвечивало необходимость доработок или совершенствования ранее разработанных средств, НПА, подходов.

Внедрение новых технологий и решение проблем старых

- Благодаря упомянутым направлениям появились:
  - «Оптимизированные порядки» проведения оценки влияния
  - «Супербелые» API
  - Подходы к выпуску сертификатов без воздушного зазора в средствах УЦ
  - Способы массового распространения программных СКЗИ
  - Подходы к долгой жизни ключей/смене ключей
  - Средства с поддержкой ГОСТ/RSA для обеспечения плавного перехода на ГОСТ

Таким образом, новые направления могут положительно влиять на весь фундамент российской криптографии в части СКЗИ, общих подходов, НПА, **делая сильнее всю отрасль, всю российскую криптографию.**

Подробнее – на секциях и круглых столах РусКрипто’2025

Спасибо за внимание!