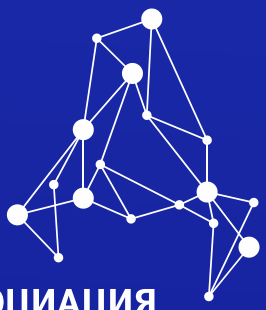


АССОЦИАЦИЯ
БОЛЬШИХ ДАННЫХ

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ

Secure Multiparty Computation

Москва
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современные технологии шифрования позволяют защищать данные на всех этапах их жизненного цикла: классические методы криптографии защищают данные на стадиях их хранения (Data at Rest) и передачи (Data in Transit), а технологии совместных конфиденциальных вычислений обеспечивают защиту данных в ходе их использования (Data in Use).

Существует несколько стратегий защиты данных на стадии использования. Применяемые в них технологические подходы можно условно разделить на два вида — аппаратные и программные. К аппаратным относятся методы (например, TEE), для реализации которых требуется специальное оборудование. Программные подходы, напротив, охватывают алгоритмы и криптографические протоколы, которые могут исполняться на стандартном оборудовании.

Технологии совместных (многосторонних) конфиденциальных вычислений (Secure Multiparty Computation, SMPC) относят к программным методам, защищающим данные во время их использования. MPC позволяют вычислять ряд математических функций на основе данных, распределенных между разными, часто конкурирующими между собой участниками взаимодействия, причем так, что исходные данные остаются засекреченными, а результат целевой функции будет единственным из того, что подконтрольно разглашается одному или нескольким участникам. Кроме того, каждый участник взаимодействия полностью контролирует использование собственных данных, сохраняя их ценность.

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ Secure Multiparty Computation

ОБЗОР ТЕХНОЛОГИИ

Постановка задачи с использованием примера

Используя MPC, можно вычислять достаточно простые функции. Более сложные функции представляются путем комбинации простых.

Рассмотрим пример простой функции. Предположим, что три банкира — Алиса, Боб и Мэллори — хотят узнать, кто из них получил самый большой бонус за год, не раскрывая при этом размеры своих бонусов друг другу или третьей стороне. Пусть x_1 — бонус Алисы, x_2 — бонус Боба, а x_3 — бонус Мэллори. Тогда функцию, которую хотят вычислить банкиры, можно выразить так:

$$y = argmax(x_1, x_2, x_3)$$

где:

- y — имя самого успешного банкира.

Особенность этой функции в том, что Алиса не сможет узнать фактические значения x_2 и x_3, Боб не узнает значения x_1 и x_3, Мэллори не узнает значения x_1 и x_2, и никакая третья сторона не узнает ни x_1, ни x_2, ни x_3. Для этого банкиры обмениваются сообщениями согласно протоколу[1] взаимодействия и совместно вычисляют значение искомой функции.

Цель состоит в том, чтобы на выходе получить только значение вычисляемой функции. В частности, банкиры смогут узнать лишь то, что можно вывести из результата функции и их собственного значения. Так, пусть y = Алиса (Алиса — банкир года) и этот результат узнали все трое. Тогда отношение x_2 и x_3 не должно быть раскрыто, причем ни во время вычисления функции y, ни после того, как результат будет вычислен. Банкиры не должны узнать, кто занял второе и третье места, поэтому вычисляется только имя самого успешного. Другими словами, скрываются не только фактические значения аргументов вычисляемой функции, но и любые отношения между ними, не являющиеся очевидными следствиями результата вычислений.

[1] Протокол — это формализованная последовательность шагов, включающая математические действия и обмен сообщениями, которую должны выполнить два участника или более, чтобы сообща реализовать тот или иной вычислительный алгоритм.

Выражаясь более формально, протокол взаимодействия, который соблюдают банкиры, должен обеспечивать следующие свойства:

- конфиденциальность аргументов: информация, полученная в результате выполнения протокола, не должна допускать возможность извлечь какие-либо выводы о личных данных, хранящихся у сторон, за исключением того, что раскрывает результат вычисляемой функции;
- корректность: стороны, вступившие в сговор или уклоняющиеся от выполнения протокола, не должны иметь возможность влиять на честных участников взаимодействия, вынуждая их выдать предсказуемые результаты.

При реализации того или иного SMPC-протокола необходимо быть готовым к тому, чтобы доказать, что он обладает всеми нужными свойствами. И наоборот: прежде чем использовать SMPC, участники могут потребовать доказательства того, что выбранный протокол позволит безопасно решить конкретную задачу.

Безопасность, которую можно доказать

Совместные конфиденциальные вычисления — это криптографический протокол. Неоспоримым достоинством использования криптографии для защиты информации является то, что в этом случае можно математически строго доказать безопасность информации. В контексте конфиденциальных вычислений эта возможность освобождает стороны от необходимости строить отношения друг с другом или с кем-либо еще на одном лишь доверии в части обеспечения конфиденциальности данных и при этом позволяет совместно выполнять вычисления над данными.

Что значит доказать обеспечение конфиденциальности?

Современная криптография подразумевает получение численных оценок того, что протокол обеспечивает заявленные свойства безопасности. Эти оценки основаны на вычислительной сложности некоторых задач или на теоретико-информационных свойствах протокола.

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ Secure Multiparty Computation

Упрощенно можно утверждать, что эти оценки характеризуют вероятность того, что протокол является безопасным.

Заметим, что есть и другие технологии конфиденциальных вычислений, для которых также можно описать свойства безопасности и математически строго доказать, что эти свойства выполняются. Однако все эти технологии предполагают, что в вычислениях важны не точные значения, а распределение вероятностей этих самых значений. Среди таких технологий — статистическое обезличивание и генерация статистических данных (см. схему). На схеме также отмечено, что точные вычисления можно выполнять с помощью доверенных сред исполнения (TEE). Однако в этом случае доказать свойства строго математически уже нельзя, поэтому придется доверять вычислителю.

Чтобы строго доказать обеспечение конфиденциальности, необходимо определить, что и от кого мы защищаем.

От кого защищаем?

Имеет смысл обеспечивать защиту от действий следующих сторон:

- внешних нарушителей — тех, кто имеет возможность наблюдать за выполнением протокола, но не принимает непосредственное участие во взаимодействии;
- пассивных нарушителей — участников взаимодействия, которые могут анализировать информацию с целью извлечения выгоды, но при этом соблюдают протокол;
- активных нарушителей — участников взаимодействия, которые могут действовать, нарушая протокол.

Что защищаем?

В идеале конфиденциальность при соблюдении протокола безопасных многосторонних вычислений означает, что по окончании вычислений стороны должны обладать только своими входными данными и тем результатом, который предусмотрен протоколом. При этом никто другой не должен получить никакой информации, в том числе о самом факте взаимодействия конкретных сторон.

Однако в реальном мире такого быть не может, поскольку стороны взаимодействуют по физическим каналам связи, анализируют выходные значения, полученные в результате выполнения протокола, и пр. Например, если три банка считают сумму средств на счете одного клиента, а потом к ним присоединяется еще один банк, после чего они снова считают сумму на счете того же клиента, то первые три банка могут узнать сумму денег на счете клиента в четвертом банке. Подобные случаи считаются «тривиальными» случаями нарушения конфиденциальности данных. Заметим также, что эта проблема возникает и при использовании доверенных сред исполнения (например, TEE).

Поэтому всегда важно точно определять, какие именно свойства безопасности должен обеспечивать протокол конфиденциальных вычислений. Для каждой конкретной прикладной задачи эти свойства могут быть разными. Заметим, что информация, конфиденциальность которой обеспечивается, может иметь самый разный вид. В частности, конфиденциальной может быть сама вычисляемая функция —

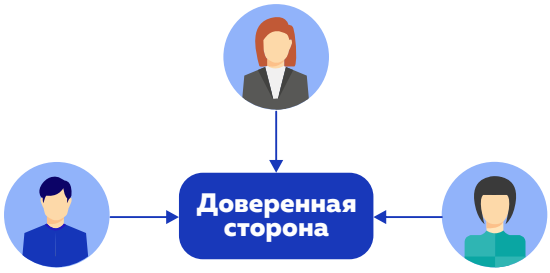
например, модель искусственного интеллекта, обученная на данных множества клиентов, и в этом случае конфиденциальными будут веса модели.

Что в итоге?

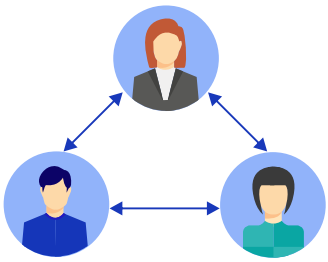
Совместные конфиденциальные вычисления позволяют удостовериться в том, что информация, полученная участниками после выполнения протокола, не отличается от информации, которая была бы получена ими при решении задачи с привлечением доверенной третьей стороны, когда все участники просто передают свои данные третьей стороне и ждут, когда она вернет им результат вычислений.

Безопасный протокол многосторонних вычислений, в отличие от подхода с доверенной третьей стороной, не предполагает раскрытия информации вообще никому. Доверие третьей стороне может быть реализовано полностью административно либо подкреплено техническими средствами (например, TEE), однако в любом случае предполагает наличие уверенности в том, что третья сторона никого не обманывает и не допускает утечек данных. Протоколы безопасных многосторонних вычислений лишены этого недостатка.

Консолидация данных у третьей стороны



Многосторонние вычисления



СТРУКТУРА МЕТОДОВ И ПРОТОКОЛОВ SMPC

Существуют два основных подхода к реализации совместных конфиденциальных вычислений. Первый подход основан на разделении секретов и представляет вычисляемую функцию как последовательность арифметических операций. Подходы, построенные на разделении секретов, как правило, применяются в соответствии с предположением, что большинство участников вычислений являются честными. Кроме того, арифметические вычисления возможны только в том случае, если участников больше двух.

Альтернативный подход основан на целевой функции, представленной в виде логической схемы, — такой способ использовал известный ученый Эндрю Яо в ходе решения задачи миллионеров: два миллионера хотят выяснить, кто из них богаче, но не хотят никому раскрывать суммы своих состояний. Кстати, именно с работы Яо началось развитие совместных конфиденциальных вычислений как отдельной области науки и техники.

Методы с разделением секрета хорошо подходят для операций сложения и умножения и хуже работают с операциями сравнения. Методы, основанные на логических схемах, напротив, эффективно выполняют битовые (логические) операции, поэтому хорошо реализуют действия по сравнению.

Разделение секрета

Разделение секрета (Secret Sharing) — криптографический примитив, позволяющий разделить ответственность за сохранность чувствительных данных между несколькими участниками. Например, схема простого арифметического разделения секрета устроена так:

$$Secret = \sum_{i=1}^{n} R_i \bmod P$$

где:

- *Secret* — число, ответственность за владение которым распределяется между участниками;
- *N* — число участников, разделяющих ответственность за хранение секрета;
- R_i — случайные числа из равномерного распределения;
- *P* — модуль, по которому выполняются вычисления (в дальнейшем для простоты изложения эту деталь будем опускать, предпола-

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ Secure Multiparty Computation

гая, что все вычисления выполняются по некоторому известному всем участникам модулю).

Другими словами, секретное число представляется в виде суммы случайных слагаемых, и в общем случае каждый из участников получает только одно из них. Понятно, что разложить число в сумму других чисел можно бесконечным числом способов, поэтому:

- участник, владеющий одним слагаемым R_i, не сможет восстановить исходный секрет, поскольку число R_i статистически неотличимо от случайного числа из равномерного распределения;
- восстановить число могут только все N участников, если соберутся вместе и обменяются слагаемыми R_i ,которыми владеют (кстати, похожую схему разделения секрета можно реализовать в мире материальных вещей: если на дверь повесить N разных замков, а ключи раздать N разным людям, то открыть дверь они смогут, только собравшись вместе).

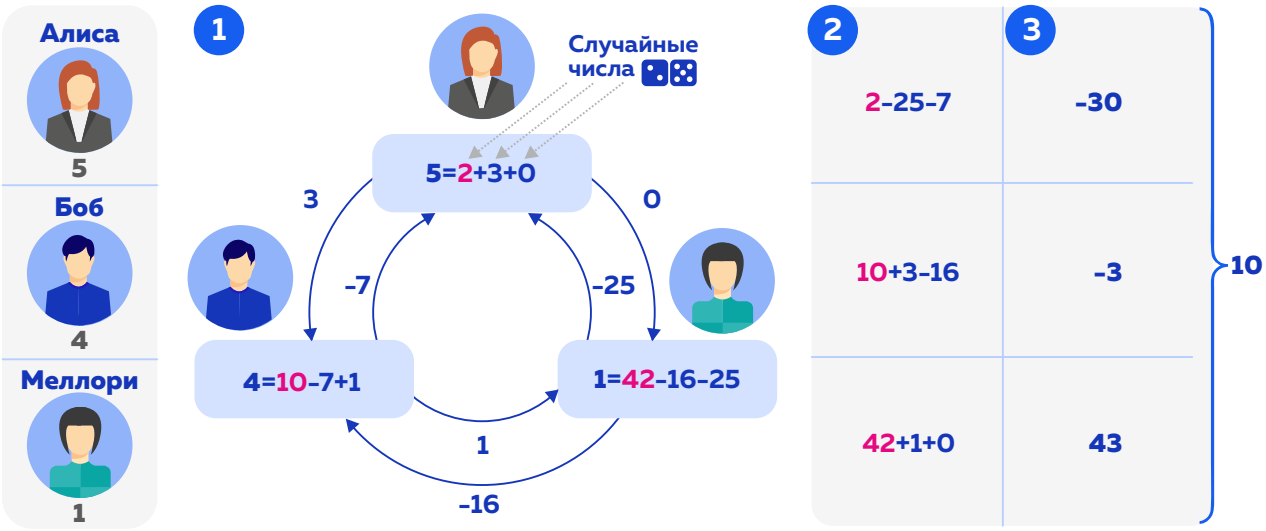
Реализация конкретного протокола зависит от выбранной схемы разделения секрета, но базовые принципы следующие:

- свои секретные данные, являющиеся входными данными протокола, участники разделяют между собой в соответствии с выбранной схемой разделения секрета;
- участники выполняют алгоритм, на каждом шаге которого используют ***либо исходные доли секрета, либо значения математических функций,*** аргументами которых являются доли секрета, ***либо информацию,*** полученную в результате обмена сообщениями, содержащими доли секрета или значения соответствующих математических функций.

Протокол сложения чисел

Существуют протоколы (вычислительные алгоритмы), которые позволяют выполнять арифметические действия (сложение и вычитание, умножение и деление, сравнение), оперируя не исходными числами, а разделениями их секретов. Таким образом можно строить вычисления на основе данных участников так, что ни один из них не раскрывает собственные данные: открывается только результат вычислений.

Проще всего устроено сложение. Пусть годовые бонусы наших банкиров Алисы, Боба и Мэллори составили 5, 4 и 1 условную единицу соответственно. Банкиры хотят вычислить, сколько всего денег они получили втроем, не раскрывая, сколько именно у каждого в отдельности.



Для решения задачи нужно выполнить протокол, состоящий из трех основных шагов:

1. Разделение секрета. На этом шаге каждый участник представляет свой бонус в виде суммы трех случайных чисел. На примере Алисы: 5 — это ее бонус, который должен быть сохранен в секрете, а 2, 3 и 0 — это случайные числа[2], доли секрета. Алиса посылает два сообщения своим коллегам-банкирам: она передает одно случайное число Бобу и еще одно — Мэллори. Так, в нашем примере Алиса отправила Бобу число 3, а Мэллори — число 0. Важно заметить, что число 2 Алиса оставила у себя. Мэллори и Боб выполняют аналогичные действия.

2 . Вычисление. На этом шаге у каждого участника есть три случайных числа: одно собственное и по одному от каждого участника-партнера. Ни один из участников не может восстановить секреты других партнеров, потому что числа, которые он знает, статистически неотличимы от случайных чисел из равномерного распределения. На этом шаге каждый участник просто складывает числа, которые знает. Алиса вычисляет 2-25-7=-30, Боб вычисляет 10+3-16=-3, Мэллори вычисляет 42+1+0=43.

3. Восстановление результата. Каждый банкир вычислил одно случайное число (сумма случайных чисел из равномерного распределения является случайным числом из равномерного распределения). Так как операция сложения коммутативна (от перестановки мест слагаемых сумма не изменяется), сумма трех чисел, которые получили банкиры, равна 10, то есть сумме исходных слагаемых — бонусов Алисы, Боба и Мэллори. Обратите внимание на следующее: *результат вычислений уже получен, но существует он в виде долей секретов, распределенных между нашими банкирами.* Дальнейшие действия очевидны: банкиры обмениваются полученными случайными числами, складывают их и получают результат, вычисляя совокупный годовой бонус.

Таким образом, участники посчитали сумму трех слагаемых, сохранив сами слагаемые в тайне. Информация, которой участники обменялись в процессе вычислений, представляет собой случайные числа из равномерного распределения. Ни сами участники вычислений, ни злоумышленник, перехвативший числа в канале связи, не смогут восстановить исходные значения на их основе.

Протоколы, основанные на разделении секрета

BGW (Ben-Or, Goldwasser and Widgerson) был одним из первых протоколов, который позволял выполнять сложение и умножение чисел, разделенных на доли секретов.

Протокол Бивера — канонический протокол, позволяющий генерировать вспомогательные данные, необходимые для эффективного перемножения чисел. Важнейшее свойство протокола Бивера — независимость от чисел, произведение которых вычисляется. Другими словами, протокол Бивера может быть выполнен заранее с разделением вычислений на две фазы:

- на предварительной фазе (офлайн) генерируются вспомогательные данные (в нужном количестве или даже впрок);
- на оперативной фазе (онлайн) вспомогательные данные используются для перемножения чисел согласно условиям задачи.

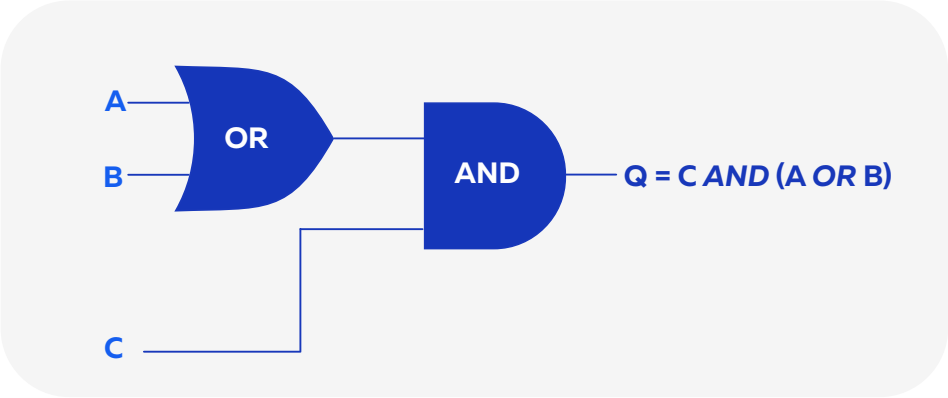
Этот подход можно трактовать и так: если нужно вычислить большую нейронную сеть завтра, готовиться к операциям по перемножению можно уже сегодня.

SPDZ — один из первых протоколов, который использовался в практических задачах. SPDZ совместил арифметическое разделение секрета и протокол Бивера, предоставляющий возможность эффективно реализовать базовый набор арифметических действий. Кроме того, разработчики SPDZ предложили ряд очень удачных оптимизаций, благодаря чему этот протокол стал основой для многих других современных про-токолов совместных вычислений.

[2] Строгий термин псевдослучайное число для простоты заменен на случайное число, поскольку на смысл рассуждений это не влияет.

Запутанные логические схемы

Известно, что любую логическую функцию можно представить в виде схемы (комбинации), состоящей из логических элементов NOT, OR, AND.



**Пример логической схемы,
которая вычисляет «C», «A» и «B», а также операторы AND и OR**

Каждый логический элемент определяется таблицей истинности, которая описывает зависимость значения элемента от его аргументов. Например, ниже приведена таблица истинности элемента AND (логическое И), который принимает истинное значение, если оба его аргумента истинны.

X	Y	X and Y
0	0	0
0	1	0
1	0	0
1	1	1

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ Secure Multiparty Computation

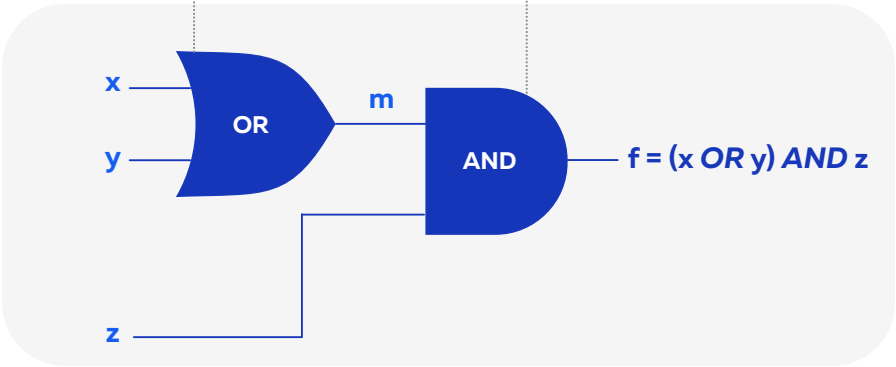
Таблица истинности есть у каждого элемента, который входит в логическую схему.

Таблица истинности элемента OR

x	y	m
0	0	0
0	1	1
1	0	1
1	1	1

Таблица истинности элемента AND

m	z	f
0	0	0
0	1	0
1	0	0
1	1	1



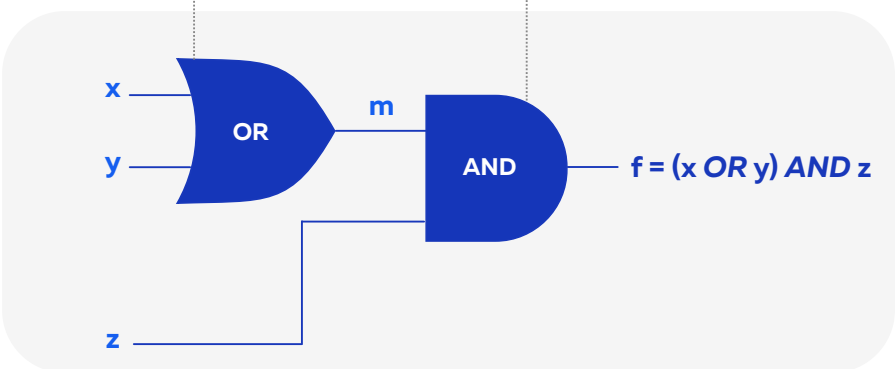
Каждый элемент получает только два аргумента, каждый из которых может принимать лишь два значения — 1 или 0. Количество возможных комбинаций (строк в таблице истинности) ограниченно и невелико — всего четыре. Строго говоря, вычислений в математическом смысле здесь не происходит, вместо этого берется набор аргументов (входов логической схемы), для которых подыскиваются соответствующие им значения в таблицах истинности. Таким образом, задача вычисления логического элемента сводится к задаче поиска, при этом искать можно все что угодно. Этим и воспользовался Яо, предложивший заменить исходные нули и единицы на метки.

Таблица истинности элемента OR с метками вместо 0 и 1

x	y	m
x0	y0	m0
x0	y1	m1
x1	y0	m1
x1	y1	m1

Таблица истинности элемента AND с метками вместо 0 и 1

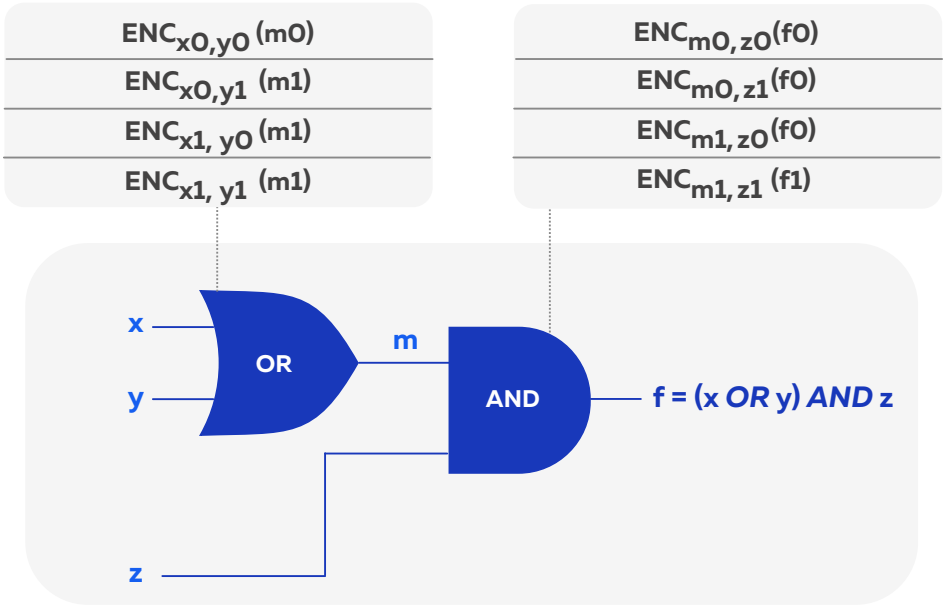
m	z	f
m0	z0	f0
m0	z1	f0
m1	z0	f0
m1	z1	f1



КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ Secure Multiparty Computation

Каждая метка — случайная битовая последовательность заданной длины. От этой длины зависит стойкость всего алгоритма, потому что метки — это ключи шифрования, с помощью которых запутывается логическая схема.

ЗАПУТАННАЯ ЛОГИЧЕСКАЯ СХЕМА



Идея заключается в следующем: чтобы запутать схему, нужно взять метки входных значений элементов и зашифровать ими соответствующее выходное значение (запись $ENC_{x0,y0}(m0)$ означает «зашифровать m0 ключами x0 и y0»). Тогда каждая таблица истинности превратится в четыре шифрограммы, которые (после случайной перестановки) как раз и становятся запутанной логической схемой.

В общем виде протокол запутанных логических схем выглядит так:

1. Алиса запутывает логическую схему (придумывает метки, шифрует с их помощью таблицу истинности каждого элемента и переставляет шифрограммы в случайном порядке), после чего передает ее Бобу вместе с метками, которые соответствуют входным данным Алисы.

2. Боб и Алиса исполняют еще один криптопротокол — протокол «забывчивой передачи (Oblivious Transfer)» посредством которого Боб получает от Алисы метки, соответствующие входным данным Боба, не раскрывая их Алисе.

3. Имея метки собственных входных данных и метки входных данных Алисы, Боб может расшифровать только некоторые строки запутанных таблиц истинности и получить метки соответствующих значений.

4. Боб передает Алисе результирующую метку всей схемы, а в ответ получает соответствующее ей значение — 0 или 1.

Так, определяя бит за битом, элемент за элементом, Алиса и Боб вычисляют сложную логическую схему, не раскрывая свои входные данные друг другу.

Яо, в частности, вычислил логическую схему, которая сравнивала численные величины состояния миллионеров и определяла, кто из них успешнее.

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ Secure Multiparty Computation

Протоколы, основанные на запутанных логических схемах

Yao GC (Yao's Garbled Circuits) — самый известный протокол совместных вычислений, основанный на запутывании логических схем. Преимущество протокола Яо — в независимости количества раундов обмена от глубины (размеров) вычисляемой схемы. Недостаток протокола в том, что он двусторонний и не предусматривает большее количество участников.

BMR (Beaver, Micali, Rogaway) — расширение протокола Яо, позволяющее работать с более чем двумя участниками.

GMW (Goldreich, Micali, Wigderson) — протокол вычисления логических схем, использующий иной принцип запутывания входов логической схемы: GMW реализует разделение секрета битовых входов и поэтому пригоден для совместного использования более чем двумя участниками.

Выбор протокола

В общем виде имеют значение следующие параметры эффективности MPC-протоколов:

1. Сложность локальных вычислений. Каждый участник выполняет часть вычислений локально, и сложность этих вычислений влияет на общую эффективность протокола и определяет требования к вычислительным ресурсам участников. Как правило, в MPC-протоколах не используются «тяжелые» вычисления, однако в ряде случаев требуются типичные для криптографии «дорогие» операции с большими числами, которые требовательны к CPU.

2. Количество раундов обмена. Большинство MPC-протоколов интерактивны: участники обмениваются различной служебной информацией. Общая эффективность протокола зависит от интенсивности этого обмена и объема передаваемой информации.

Как правило, сложность локальных вычислений и количество раундов обмена обратно пропорциональны: одни протоколы подразумевают интенсивный информационный обмен, но используют сравнительно простые («легкие») вычисления, а другие, напротив, не требуют частого обмена данными, но полагаются на серьезные вычисления (запутанные логические схемы относятся как раз к таким).

В любом случае совместные конфиденциальные вычисления — развивающаяся область математики и криптографии. Множество алгоритмов и протоколов уже разработано, при этом достаточно часто появляются новые методы и подходы. У каждого из протоколов есть свои преимущества и недостатки.

При решении реальных задач чаще всего применяют несколько протоколов одновременно. В частности, довольно известное семейство фреймворков ABY (Arithmetic, Boolean, Yao) использует протоколы с разделением секретов для арифметических операций и запутанные логические схемы для операций сравнения. Такой подход «смешивания» протоколов — одна из хорошо зарекомендовавших себя практик совместных вычислений, позволяющая эффективно решать задачи с достаточно противоречивыми требованиями.

К сожалению, универсального SMPC-решения в настоящее время не существует. Прежде чем использовать многосторонние вычисления, придется выбирать (и, вероятно, модифицировать) технологическое решение, которое лучше подойдет для конкретной задачи. Опыт российских разработчиков SMPC-решений показывает: задача может быть решена, причем эффективно, и решение может масштабироваться на другие предметные области. Но, чтобы это реализовать, потребуются соответствующие компетенции.

Сопутствующие протоколы

Разделение секрета и запутывание логических схем — это основные методы, используемые для построения комплексных SMPC-систем. Однако существуют и другие алгоритмы и протоколы более общего характера, применяемые в многосторонних конфиденциальных вычислениях.

1. Гомоморфное шифрование (Homomorphic Encryption, HME — способ шифрования, позволяющий выполнять математические действия над зашифрованными данными так, что их результат будет комплементарен математическим действиям, выполненным над исходными

данными. Принято считать, что гомоморфное шифрование — отдельный метод защиты данных на стадии их использования, однако некоторые из протоколов HME могут применяться в протоколах SMPC.

2. Защищенное пересечение множеств (Private Set Intersection, PSI) — набор алгоритмов и протоколов, позволяющих определить количество общих элементов двух и более множеств (например, количество общих клиентов разных организаций) или сами общие элементы (например, идентификаторы общих клиентов разных организаций) без разглашения информации об элементах, которые не входят в это пересечение. PSI является самостоятельной SMPC-техникой, которая может быть использована в более сложных SMPC-системах.

3. Забывчивая передача (Oblivious Transfer, OT) — набор алгоритмов и протоколов, которые позволяют стороне A запросить данные у стороны B так, что сторона B не узнает, какие именно данные были запрошены, но передаст стороне A только запрошенные данные. OT используется и как самостоятельная SMPC-техника, и в составе комплексных протоколов, в том числе SMPC (в частности, в протоколах запутанных логических схем). Существует версия забывчивой передачи с более слабыми требованиями, которая запрещает раскрытие информации о том, какие именно данные были запрошены, но допускает передачу некоторых других данных помимо запрошенных. Такой «упрощенный» вид забывчивой передачи известен как получение скрытой информации (Private Information Retrieval, PIR).

4. Доказательство с нулевым разглашением (Zero-Knowledge Proof, ZKP) — набор алгоритмов и протоколов, позволяющих стороне A доказать стороне B истинность некоторого утверждения, не передавая при этом информации о самом утверждении. Например, один банк может доказать другому, что доход конкретного клиента превышает некоторый порог, не раскрывая при этом точное значение дохода. ZKP применяется в различных задачах, в том числе тесно связанных с задачами многосторонних конфиденциальных вычислений.

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ SMPC

Технология SMPC обладает уникальными преимуществами, выделяющими ее среди других.

- Конфиденциальность: SMPC позволяет работать с данными, сохраняя их конфиденциальность, что очень важно в условиях растущей угрозы утечек и несанкционированного доступа.
- Доказательная защита: многие SMPC-протоколы основаны на фундаментальных криптографических принципах и доказательствах. Для многих известных протоколов уже существуют математические обоснования стойкости. Для новых протоколов в большинстве случаев такое обоснование также может быть построено.
- Независимость от доверенной стороны: в SMPC не требуется наличие доверенной третьей стороны, поскольку участники распределяют данные и вычисления между собой.
- Защита от инсайдеров: SMPC снижает вероятность инсайдерских угроз, так как каждый из участников владеет лишь частью информации.
- Гибкость: MPC-протоколы существуют (или могут быть построены) практически для любой вычислительной задачи.

Однако у SMPC есть и свои ограничения. Вот наиболее значимые из них:

- Вычислительная сложность: для работы многих из протоколов SMPC необходимы значительные вычислительные ресурсы — это требование может стать серьезным ограничением для их интенсивного применения, особенно некрупными участниками рынка.
- Сложность масштабирования: с ростом количества участников сложность SMPC может расти экспоненциально. Вместе с тем существуют протоколы, которые хорошо масштабируются даже на сотни участников. Правда, в настоящий момент такие протоколы могут реально выполнять только простые арифметические операции.

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ Secure Multiparty Computation

- Сложность внедрения: для успешного внедрения MPC-системы потребуется активное вовлечение всех участников вычислений, поскольку необходимо выделить ресурсы, установить и сконфигурировать программное обеспечение, настроить сетевой доступ, политики безопасности и пр. — это существенно увеличивает сроки ввода в эксплуатацию.

- Требования к инфраструктуре и сложность эксплуатации: многие решения, основанные на протоколах MPC, подразумевают, что вычисления возможны, только если все их участники доступны и работоспособны. Для этого, в частности, требуется надежная инфраструктура с резервированием на всех уровнях — от серверов до каналов связи.

Кроме SMPC, существует множество других технологий, обеспечивающих защиту конфиденциальности данных. Каждая из этих технологий обладает своими уникальными особенностями, преимуществами и ограничениями, определяющими возможность и эффективность ее использования в различных сценариях и задачах.

НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ MPC

Финансовый сектор

Финансовый сектор, представленный множеством игроков (прежде всего кредитными организациями), в результате информационного взаимодействия, очевидно, выигрывает. Имеющиеся на российском рынке решения на основе совместных вычислений позволяют банкам совместно использовать данные друг друга для сквозной аналитики без разглашения чувствительных данных и без их консолидации третьими сторонами. К задачам такой аналитики относятся «сквозной» (совместный) кредитный скоринг клиентов, оценка доходов и имеющихся на счетах заемщиков денежных средств, выявление подозрительных финансовых операций (Anti Money Laundering).

Отдельное направление конфиденциальных вычислений в финансовом секторе — противодействие мошенническим операциям. Протоколы MPC могут быть использованы в качестве отдельных вычислительных узлов в составе комплексных антифрод-систем, использующих в числе прочего и другие подходы к конфиденциальным вычислениям (например, TEE).

Используемые протоколы: конфиденциальное вычисление суммы с помощью разделения секрета слагаемых (см. пример в п. 2.2 «Протокол сложения чисел»), протоколы защищенного пересечения множеств, протоколы на базе SPDZ и ABY для конфиденциального машинного обучения.

Медицина

Совместная аналитика на основе данных разных участников очень важна для медицинской отрасли. В частности, оценка влияния генетики на физиологические особенности (например, предрасположенность к различным заболеваниям) — важная задача системы здравоохранения, успешное решение которой не только повысит качество жизни каждого отдельного человека, но и окажет непосредственное влияние на экономическое развитие страны. Стоимость лечения многих заболеваний, обусловленных генетикой, высока, а кроме того, утрата трудоспособности, которая может возникнуть вследствие болезни, наносит труднопрогнозируемый экономический урон.

Технологии совместных вычислений позволяют проводить исследования и выявлять статистически значимые закономерности между фенотипическими и генотипическими признаками (например, между факторами полигенных рисков и подтвержденными диагнозами в анамнезе) без риска нарушения конфиденциальности данных отдельных пациентов.

Используемые протоколы: протоколы защищенного пересечения множеств, протоколы на базе SPDZ и ABY для конфиденциального машинного обучения.

Отраслевая статистика

Совместные вычисления используются в задачах вычисления сквозной (агрегированной) статистики по компаниям, работающим в одной или смежных отраслях. Например, известны следующие варианты применения MPC:

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ Secure Multiparty Computation

- вычисление суммарного времени работы водителя во всех агрегаторах такси без разглашения времени, в течение которого водитель работал в каждом из агрегаторов (соблюдение коммерческой тайны);
- вычисление усредненных рейтингов — например, водителей такси, курьеров служб доставки, пользователей кикшеринговых и каршеринговых компаний;
- подсчет общего количества целевых действий, совершенных пользователями на сайтах поставщиков схожих услуг, — например, прослушиваний одной и той же музыкальной композиции пользователями разных стриминговых сервисов.

Существует огромное количество задач по вычислению агрегированной статистики, которые могут быть решены посредством технологий MPC с гарантированным уровнем конфиденциальности исходных данных.

Используемые протоколы: конфиденциальное вычисление суммы с помощью разделения секрета слагаемых (см. пример в п. 2.2 «Протокол сложения чисел»), протоколы защищенного пересечения множеств.

Реклама и маркетинг

Решения, основанные на совместных вычислениях, находят широкое применение в рекламе и цифровом маркетинге. Этому способствует ужесточение требований к защите данных (GDPR в Европе, CCPA в США, Федеральный закон 152-ФЗ в РФ). Кроме того, привычные технические средства, используемые в цифровом маркетинге (например, Third-Party Cookies), уже стали или вскоре станут недоступны.

Совместные вычисления — одна из технологических альтернатив. Существуют протоколы, позволяющие находить пересечения аудиторий паблишеров (владельцев рекламных пространств) и рекламодателей и обеспечивать активацию рекламных объявлений без применения механизмов явного отслеживания пользователей. Такие алгоритмы становятся технологической основой Data Clean Room — концепции, подразумевающей конфиденциальную обработку персональных данных в маркетинге в целях поиска пересечения аудиторий, активации объявлений, оценки рекламных эффектов.

Используемые протоколы: конфиденциальное вычисление суммы с помощью разделения секрета слагаемых (см. пример в разделе «Протокол сложения чисел», стр. 7).

Машинное обучение

Универсальность технологии MPC и большой набор математических операций, которые можно вычислить конфиденциально, позволяют обучать и применять модели машинного обучения на данных, не допуская их рассекречивания. В частности, конфиденциальное машинное обучение на базе MPC применялось в моделях, объединяющих данные кредитных организаций и операторов связи (https://www.rst-com.ru/news/2021/07/22/16741/).

Используемые протоколы: протоколы защищенного пересечения множеств, протоколы на базе SPDZ и ABY для конфиденциального машинного обучения.

Конфиденциальный запрос данных

Встречаются задачи, в которых один участник запрашивает данные о конкретном объекте у другого участника таким образом, что отвечающий не может узнать, в отношении какого именно объекта выполняется запрос. В качестве примера рассмотрим новую реализацию функции Live Caller ID от компании Apple. Представим, что есть участник A, владеющий большой телефонной книгой с информацией о номерах и их владельцах, и мы хотим, получив звонок с неизвестного номера, узнать, есть ли этот номер в телефонной книге участника A, а если есть, то кому номер принадлежит. При этом мы также хотим, чтобы участник A не узнал, кто нам звонит и что звонят именно нам. Похожие задачи есть и в других областях: в частности, банк может получать информацию об окружении клиента телеком-оператора, не раскрывая данные этого клиента.
Используемые протоколы: забывчивая передача (Oblivious Transfer, OT) и получение скрытой информации (Private Information Retrieval, PIR).

МОДЕЛЬ РИСКОВ ДЛЯ SMPC

Формальная модель рисков SMPC

Модель рисков — это инструмент для систематической оценки вероятности возникновения угроз и их потенциального воздействия на систему. Модель позволяет измерять риски, выявлять слабые места и принимать меры для их минимизации.

Формальная модель рисков — это их математическое представление, выражающее риски через взаимосвязанные компоненты и количественные показатели. Такая модель дает возможность более точно оценивать угрозы и принимать решения на основе количественных данных.

Основные компоненты модели

Оценка риска основана на анализе вероятностей негативных событий и их последствий, которые в совокупности определяют общий уровень риска. В ходе его расчета учитываются как зависимые, так и независимые события. При этом независимые события (например, изолированные ошибки) факторизуются, то есть их совместная вероятность представляется в виде произведения вероятностей отдельных событий. Зависимые события требуют более сложного анализа через условные вероятности, поскольку наступление одного события может повысить вероятность другого.

Два ключевых показателя при оценке риска — вероятность события и его влияние.

- Влияние события помогает оценить потенциальные последствия атаки. Выделение влияния отдельно от вероятности позволяет измерить ущерб, который может возникнуть в результате события, — например, в виде финансовых или репутационных потерь.
- Вероятность события помогает понять, насколько часто может возникать угроза. Это особенно важно для рисков, связанных с масштабными последствиями, но низкой вероятностью и наоборот.

Эти два показателя формируют основу формальной модели риска. Их можно объединить в формулу:

$$R=\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l}P(X_i)\times(Y_j\,|\,X_i,Z_k)\times I(Y_j)$$

Где:

- $P(X_i)$ — это вероятность уязвимости X_i,
- $P(Y_j\,|\,X_i, Z_k)$ — условная вероятность успешной атаки Y_j при наличии уязвимости X_i и применении меры защиты Z_k,
- $I(Y_j)$ — влияние события Y_j (наносимый ущерб).

Формула позволяет учесть и вероятность возникновения события, и его последствия, что дает более полное представление о рисках.

Применяя такой подход для SMPC, можно выделить три группы атак, вероятность оценки успешности которых позволяет оценить риск количественно:

1. Риск компрометации ключей R_{key}: этот компонент связан с возможностью раскрытия криптографических ключей, используемых для защиты данных и обмена между участниками. Этот риск определяется управлением ключами и применяемыми криптографическими механизмами. Компрометация ключей может ослабить защиту системы.

2. Риск компрометации данных R_{data}: если в результате атак на систему передачи и хранения данных возникла утечка конфиденциальной информации, существенными факторами оказываются объем конфиденциальных сведений и их чувствительность. Утечка может произойти, например, из-за уязвимостей в ходе обмена данными с использованием недостаточно защищенных каналов. Оценка этого риска позволяет определить меры для минимизации вероятности утечки данных.

3. Риск протокола $R_{protocol}$: компонент отражает уязвимости, которые могут возникнуть из-за недостатков в архитектуре и параметрах безопасности протоколов SMPC. В силу особенности криптографических механизмов, к которым относятся эти протоколы, значение вероятности реализации угрозы определяется в ходе обоснования стойкости (см. раздел «Безопасность, которую можно доказать», стр. 4).

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ Secure Multiparty Computation

Стоит отметить, что упоминаемые выше аналитические методы оценки вероятности, дающие максимальную уверенность в этих значениях, достаточно сложны. Кроме них, существуют также эмпирические (экспериментальные) методы, позволяющие провести моделирование различных атак и оценку доли случаев их успешной реализации. Однако, как правило, на практике используют протоколы с доказанным уровнем стойкости. Ущерб при этом оценивают исключительно экспертным способом. Общий риск R для SMPC можно представить как взвешенную сумму перечисленных компонентов, что позволяет получить целостную оценку угроз, упрощая полный расчет по предыдущей формуле:

$$R=\alpha R_{key} + \beta R_{data} + \gamma R_{protocol}$$

Здесь α, β, γ — весовые коэффициенты, отражающие значимость каждой группы рисков.

ЮРИДИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ ТЕХНОЛОГИИ

Учитывая то, что MPC являются разновидностью конфиденциальных вычислений, так же как и доверенные среды исполнения (ДСИ, в иностранной терминологии — TEE), мы не будем дублировать описание базовых положений законодательства РФ о персональных данных (ПДн), приведенное приведенное в Докладе по ДСИ, а коснемся юридических вопросов, специфических для MPC.

Основные нюансы законодательства РФ о персональных данных

Признание факта обработки персональных данных при использовании MPC

Как указывалось в Докладе по ДСИ, применение к ПДн технологий шифрования и обезличивания не влияет на квалификацию полученных в результате этих операций данных (зашифрованных или обезличенных) именно как персональных.

В соответствии со статьей 3 Федерального закона «О персональных данных» от 27.07.2006 152-ФЗ, под «обработкой персональных данных» понимаются любое действие (операция) или совокупность действий, совершаемых с ПДн как с использованием средств автоматизации, так и без их применения.

Следовательно, как само помещение ПДн в контур MPC, так и осуществление любых действий с ними в рамках этого контура будут рассматриваться как обработка этих ПДн.

Правовое основание обработки ПДн при использовании MPC

Признание факта обработки ПДн при использовании MPC требует от стороны, имеющей доступ к таким данным, наличия соответствующего правового основания (часть 1 статьи 6 Федерального закона 152-ФЗ), если эта сторона считается оператором таких ПДн, либо наличия корректно оформленного поручения на обработку ПДн (часть 3 статьи 6 Федерального закона 152-ФЗ).

Поскольку одной из целей использования MPC является как раз совместный доступ к информации каждого из участников без непосредственного обмена ею и консолидации ее у третьей стороны, целесообразно исходить из того, что каждый участник выступает как самостоятельный оператор всех ПДн, обрабатываемых с использованием MPC.

Следовательно, встает тот же вопрос о наличии правового основания для обработки ПДн, что рассматривался в Докладе о ДСИ.

Обеспечение конфиденциальности — ключевое преимущество MPC

Одной из важнейших обязанностей оператора, согласно закону любой страны о ПДн, является обеспечение конфиденциальности этих данных и воспрепятствование доступа к ним неавторизованных лиц и сторон.

Использование MPC для совместной обработки ПДн (при соответствующей настройке параметров ПО) позволяет не допустить раскрытия исходных ПДн другим участникам MPC в результате операций, совершаемых с данными с помощью MPC.

Рекомендации для участников MPC

Сложность создания унифицированного юридического подхода к MPC объясняется высокой вариативностью условий применения этой технологии и объема прав участников в части доступа к исходным данным, а также широтой возможностей использования данных внутри MPC и детализации результатов анализа этих данных. Это создает риски применения технологии MPC для обогащения ПДн, уже имеющихся у участников, при отсутствии согласия на это со стороны самого субъекта ПДн.

С учетом этого считаем целесообразным оценивать законность совместной обработки ПДн с использованием MPC лишь в конкретных условиях. Фиксация таких условий, в том числе на уровне криптографических и иных алгоритмов в используемом программном обеспечении, создаст требуемый фундамент для прочной правовой позиции участников и нужные условия для взаимодействия с регулятором.

Примером успешного согласования с регулятором использования технологии MPC может служить платформа «Блумтех», позволяющая банкам совместно формировать агрегированные выписки по счетам клиента, открытым в разных кредитных организациях, не обмениваясь исходными данными и не передавая их третьей стороне[3] . Важно отметить несколько факторов, позволивших достичь результата в этом случае:
1) готовность к диалогу со стороны регуляторов;
2) настойчивость и постоянный поиск возможных решений со стороны разработчика;
3) закрепление криптографических и иных алгоритмов в используемом ПО;
4) описание порядка работы платформы в технической документации, которая согласовывалась с регулятором.

Факторы успеха для согласования кейса с регулятором

[3] Публикация РБК «ЦБ разрешил банкам сообща оценивать долговую нагрузку россиян» (https://www.rbc.ru/finances/29/10/2024/671fa35d9a79479ced770acf).

Варианты стимулирования регулятором использования MPC

Как указано выше и в докладе о ДСИ, одной из ключевых юридических сложностей при использовании MPC является необходимость сбора согласий субъектов ПДн. Возможная альтернатива — использовать законный интерес как основание обработки ПДн (пункт 7 части 1 статьи 6 Федерального закона 152-ФЗ), если в рассматриваемой ситуации невозможно применять MPC для обогащения имеющихся у участников ПДн. Это избавит участников MPC от необходимости сбора согласий, хотя и потребует от них соблюдения всех принципов обработки ПДн, включая требования законности и справедливости обработки, а также обеспечения соответствия объема обрабатываемых ПДн целям обработки.

Подтверждение такой возможности со стороны регулятора повысит прозрачность и предсказуемость обработки с точки зрения участников MPC и будет стимулировать другие компании рассмотреть MPC в качестве технологии для совместной обработки данных.

Важно подчеркнуть, что такое подтверждение со стороны регулятора целесообразно обсуждать применительно к конкретной ситуации использования MPC, описанной как документально, так и на уровне алгоритмов в программном обеспечении.

ПЕРСПЕКТИВЫ ПРИМЕНИМОСТИ SMPC

Общие тезисы о применимости

Технологии многосторонних конфиденциальных вычислений уже используются в таких отраслях, как финансы, медицина, реклама и маркетинг. Однако каждый случай их применения уникален. Масштабирование MPC — почти всегда нетривиальная (хотя и решаемая) задача даже для разных кейсов в рамках одной предметной области. Другими словами, SMPC — работающая технология, но ее использование требует специфических компетенций.

Перспективы внедрения и использования SMPC в разных отраслях

SMPC — полностью программный метод, не зависящий от производителя аппаратного обеспечения. Он основывается на протоколах, для которых существует (или может быть построено) доказательство требуемого уровня безопасности[4], поэтому SMPC может использоваться в задачах с повышенными требованиями к безопасности данных (например, в государственном управлении).

Общий прогноз: количество кейсов и областей применения SMPC будет расти в России и в мире. Каждый новый кейс повышает интерес и доверие к технологии. Кроме того, от количества кейсов зависит масштабирование: чем больше задач решается с помощью SMPC, тем универсальнее становится технология.

Рекомендации для разных категорий пользователей

Рекомендация для бизнеса — исследовать рынок и существующие кейсы применения SMPC. Это поможет найти ответы на следующие вопросы:

- подходят ли технологии многосторонних конфиденциальных вычислений для решения конкретной бизнес-задачи;
- какие затраты могут при этом потребоваться и какой экономический эффект может быть получен.

Разработчикам систем многосторонних конфиденциальных вычислений можно рекомендовать:

- популяризировать возможности технологий SMPC, демонстрируя реальные примеры их применения;
- взаимодействовать с бизнес-заказчиками, искать новые варианты использования этой технологии;
- взаимодействовать с регуляторами, учитывать их рекомендации, соблюдать установленные ограничения.

[4] В рамках заданных моделей нарушителя и угроз.

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ И ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ Secure Multiparty Computation

Рекомендация техническим специалистам и ИБ — повышать осведомленность о новых подходах и тенденциях в обработке и анализе данных, в том числе в области повышения конфиденциальности данных.

Направления дальнейших исследований и развития

- Исследования и разработка в области оптимизации методов и алгоритмов SMPC: производительность — узкое место технологий многосторонних конфиденциальных вычислений, ограничивающее их применение.
- Развитие стандартов и интероперабельности: унификация и стандартизация протоколов по типу задач повысит совместимость и взаимозаменяемость их решений.
- Открытый диалог между сторонами: тесное взаимодействие разработчиков SMPC-решений, потенциальных бизнес-заказчиков и регуляторов позволит найти взаимно приемлемые варианты реализации.

ОСНОВНЫЕ ВЫВОДЫ О ТЕХНОЛОГИИ SMPC

+ Преимущества	− Недостатки
Есть успешные примеры использования, в том числе в России.	SMPC — сложная технология, для успешного внедрения и использования которой требуются время и компетенции.
Для SMPC-протоколов существует или может быть построено доказательство требуемого уровня безопасности.	Чтобы достичь требуемой производительности, необходимо оптимизировать протокол для конкретной задачи.
SMPC — программная технология, работающая на стандартном оборудовании.	Решения могут быть требовательными к инфраструктуре, особенно если необходимы высокая надежность и отказоустойчивость.
SMPC — это не универсальный метод, а набор практик и протоколов, из которых можно «собрать» решения для широкого спектра задач из разных предметных областей.	Для многих типов задач нет универсальных решений.

ГЛАВНЫЙ ВЫВОД:

SMPC — активно развивающаяся область науки и техники с уже имеющимися примерами практического применения. В долгосрочной перспективе SMPC может стать неотъемлемой частью цифровой инфраструктуры — технологией, которая позволит решать задачи, связанные с приватностью, безопасностью и совместным использованием данных.

АВТОРЫ ДОКЛАДА

ПЕТР ЕМЕЛЬЯНОВ
CEO
ООО «Блумтех»

АЛЕКСЕЙ НЕЙМАН
Исполнительный директор
Ассоциации больших данных,
руководитель FIT Academy of Russia,
Master of Data Science, CDMP, PMP

АЛЕКСАНДР МИТРОФАНОВ
Product Owner
ООО «Блумтех»

ЛИДИЯ НИКИФОРОВА
Ведущий инженер-аналитик отдела
криптографических исследований
ООО «КРИПТО-ПРО»

СЕРГЕЙ КЯЖИН
Заместитель начальника отдела
криптографических исследований
ООО «КРИПТО-ПРО»

АЛЕКСЕЙ МУНТЯН
Генеральный директор
Privacy Advocates,
внешний менеджер по защите данных
нескольких транснациональных холдингов,
соучредитель Regional Privacy
Professionals Association (RPPA.pro),
сопредседатель
Privacy & Legal Innovation
и кластера РАЭК

ДЕНИС БЕЗРУКОВ
Технический директор
и соучредитель Aggregion,
соучредитель SuperProtocol

АРТЁМ АЛЕКСЕЕВ
Управляющий партнер
Aggregion

АЛЕКСАНДР ПАРТИН
Адвокат и партнер
Privacy Advocates,
соучредитель «РППА.Офис»,
сопредседатель Privacy & Legal Innovation
кластера РАЭК, CIPP/E, CIPM

ВАЛЕРИЙ ХВАТОВ
Специалист по кибербезопасности
и распределенным вычислениям,
технический директор DGT Network

ИСТОЧНИКИ

1. Briongos, Samira, Ghassan Karame, Claudio Soriente, and Annika Wilde. "No Forking Way: Detecting Cloning Attacks on Intel SGX Applications." Annual Computer Security Applications Conference, December 4, 2023, 744–58. https://doi.org/10.1145/3627106.3627187.

2. ISO/IEC TR 27563:2023, Security and privacy in artificial intelligence use cases — Best practices.

3. ISO/IEC 29134:2023(en), Information technology — Security techniques — Guidelines for privacy impact assessment.

4. ГОСТ Р 59991-2022 Системная инженерия. Системный анализ процесса управления рисками для системы.

5. ГОСТ Р 59407-2021 Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных.

6. ITU-T X.1170 Technical guidelines for secure multi-party computation, ttps://www.itu.int/rec/T-REC-X.1770-202110-I, 2021.

7. NIST IR 8214C (Initial Public Draft) NIST First Call for Multi-Party Threshold Schemes, 2023, https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8214C.ipd.pdf.

8. Zhou, Ian, Farzad Tofigh, Massimo Piccardi, Mehran Abolhasan, Daniel Franklin, and Justin Lipman. "Secure Multi-Party Computation for Machine Learning: A Survey." IEEE Access 12 (January 1, 2024): 53881–99. https://doi.org/10.1109/ACCESS.2024.3388992.

9. Andreea, Ionita. "Private Set Intersection: Past, Present and Future:" In Proceedings of the 18th International Conference on Security and Cryptography, 680–85. SCITEPRESS — Science and Technology Publications, 2021. https://doi.org/10.5220/0010525806800685.

10. Zhao, Chuan, Shengnan Zhao, Minghao Zhao, Zhenxiang Chen, Chong Zhi Gao, Hongwei Li, and Yu an Tan. "Secure Multi-Party Computation: Theory, Practice and Applications." Information Sciences 476 (February 1, 2019): 357–72. https://doi.org/10.1016/J.INS.2018.10.024.

11. "IEEE Recommended Practice for Secure Multi-Party Computation." IEEE. Accessed November 13, 2024. https://doi.org/10.1109/IEEESTD.2021.9604029.

12. Alfarano, Gianira N., Karan Khathuria, and Violetta Weger. "A Survey on Single Server Private Information Retrieval in a Coding Theory Perspective." Applicable Algebra in Engineering, Communications and Computing, April 12, 2021, 1–24. https://doi.org/10.1007/S00200-021-00508-5/TABLES/1.

13. Sedghighadikolaei, Kiarash, and Attila Altay Yavuz. "A Comprehensive Survey of Threshold Signatures: NIST Standards, Post-Quantum Cryptography, Exotic Techniques, and Real-World Applications." arXiv, September 17, 2024. https://doi.org/10.48550/arXiv.2311.05514.

Редакторы доклада

ЖАННА ПОКРОВСКАЯ
Руководитель пресс-службы
Ассоциации больших данных

АЛИЯ ТРУНАЕВА
PR-менеджер
Ассоциации больших данных

АССОЦИАЦИЯ БОЛЬШИХ ДАННЫХ

www.rubda.ru

Адрес: Москва,
Пресненская набережная, 10с2

+7 (495) 252-72-60
info@rubda.ru