O.V. Kazarin
Institute of Information Security Issues, Lomonosov MSU, Michurinsky Pr., 1, Moscow, 119192, Russia;
Institute for Information Sciences and Security Technologies, RSUH, Kirovogradskaya St., 25, bidg 2, Moscow, 117534, Russia, e-mail: okaz2005@yandex.ru, ORCID 0000-0002-5098-0962

Secure Computation in the Problem on Dangerous Closeness

Keywords: secure computation, secure function evaluation, two-party and multi-party protocols of secure computation
This paper showcase protocols of secure computation with complexity characteristics suitable to practical hiding the coordinates of point objects in unspecified local traffic control zone. Hiding of the coordinates will ensure the protection of road users from both semi-honest adversary who, having taken control of one or several objects, may disclose movement coordinates of fair users, thus violating privacy policy in part of objects' locations, or from the malicious adversary, who, having taken control of one or several objects may disclose movement coordinates of fair users and, therefore, affect the speed of movement of the controlled objects to facilitate a dangerous closeness and/or collision of the objects.

О.В. Казарин
Институт проблем информационной безопасности МГУ имени М.В.Ломоносова, Мичуринский просп., 1, Москва, 119192, Россия;
Институт информационных наук и технологий безопасности РГГУ, Кировоградская ул., 25, корп.2, Москва, 117534, Россия, e-mail: okaz2005@yandex.ru, ORCID 0000-0002-5098-0962

КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ В ЗАДАЧЕ ОБ ОПАСНОЙ БЛИЗОСТИ

Ключевые слова: конфиденциальные вычисления, конфиденциальное вычисление функции, двусторонние и многосторонние протоколы конфиденциальных вычислений.
Представлены протоколы конфиденциальных вычислений с хорошими сложностными характеристиками для сокрытия координат точечных объектов в некоторой локальной зоне управления движением. Сокрытие координат позволит обеспечить защиту участников движения как от получестного противника (который, получив контроль над одним или несколькими объектами, может раскрыть координаты движения честных участников, нарушив, таким образом, правила обеспечения конфиденциальности местоположения объектов), так и от злонамеренного противника, который, получив контроль над одним или несколькими объектами, может раскрыть координаты движения честных участников и, таким образом, повлиять на скорость движения подконтрольныхему объектов с тем, чтобы создать опасную близость, столкновение объектов.

Введение и неформальная постановка задачи исследования

Задача об опасной близости (о предотвращении столкновений) возникает в авиации [1], на автомобильном (беспилотном) транспорте [2], в судоходстве [3]. При этом неформально постановка такой задачи может быть следующей.

Рассматриваются два типа движущихся точечных объектов: *объект-запрос* (или просто – *запрос*) движется снизу вверх (с юга на север) в прямоугольнике и *объект-данные* (или просто – *объект*) движутся слева направо (с запада на восток) в этом же прямоугольнике [1, 4, 5]. При этом предположим, что траектории объектов, движущихся в одном из этих направлений внутри прямоугольника, не пересекаются. *Задача об*

опасной близости (или *задача о предотвращении столкновений*) заключается в перечислении для каждого запроса тех и только тех объектов, которые будут находиться в некоторый момент времени в процессе своего движения на расстоянии не более, чем заданное расстояние ρ, где ρ – радиус круга с центром, представляющим собой движущийся объект (рис. 1).

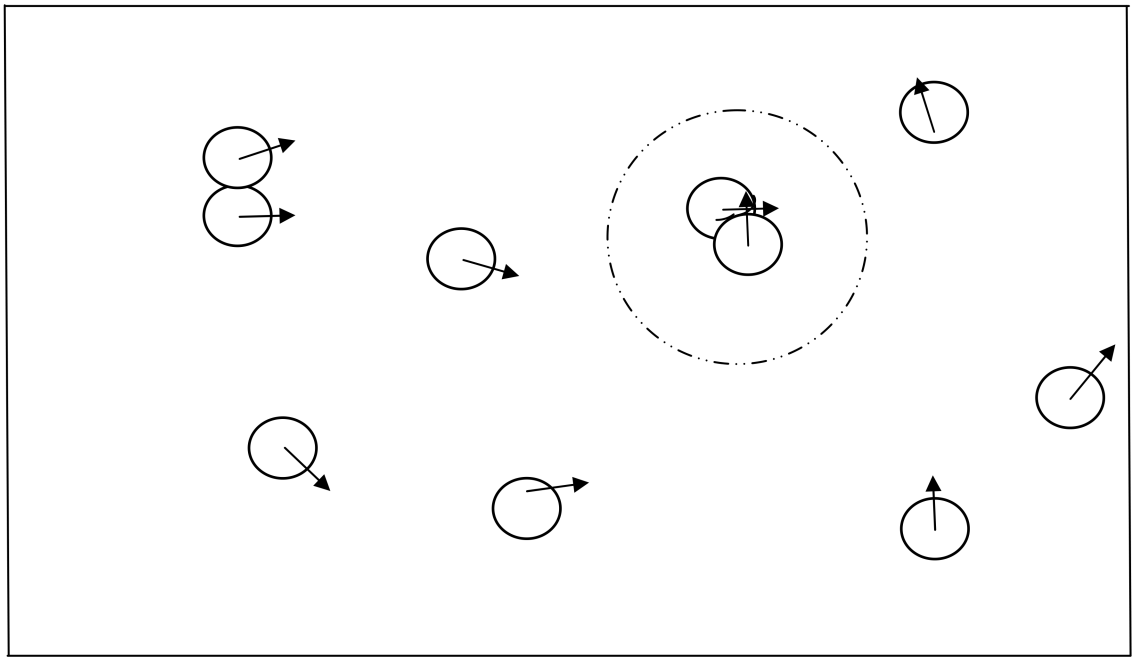

Рис. 1. Иллюстрация движения точечных объектов в задаче об опасной близости

Предположим далее, что при движении объектов и запросов нам необходимо обеспечить не только невозможность их столкновения, но и *конфиденциальность местоположения объектов и запросов* при этом. Для этого может использоваться концепция *многосторонних конфиденциальных вычислений*, суть которых может сводиться к *следующей постановке задачи*. Имеется процесс интерактивного взаимодействия (распределенный протокол взаимодействия) объектов и запросов между собой, для управления которым необходимо реализовать функциональность f,[1] с выполнением условий:

корректности, когда f должна обеспечивать невозможность столкновения, даже если некоторая ограниченная часть объектов и запросов отклоняется от предписанных им действий;

конфиденциальности, когда в результате взаимодействия ни один из объектов и запросов не получает никакой непредназначенной ему информации о других объектах и запросах.

Например, злоумышленник, контролирующий некоторую ограниченную часть объектов и запросов, получив такую информацию (предположим, координаты движения каких-либо объектов и запросов), может несанкционированно повлиять на процесс их взаимодействия с целью создания конфликтной ситуации (столкновения) с их участием.

[1] Функциональность, обеспечивающую невозможность столкновения.

В случае успешной стратегии получестного[2] противника, который получил контроль над одним или несколькими[3] из объектов и запросов, противник раскроет координаты движения честного(-ых) участника(-ов) взаимодействия, нарушив, таким образом, правила обеспечения конфиденциальности местоположения объектов и запросов (если они установлены). В случае успешной стратегии злонамеренного[4] противника, который получил контроль над одним или несколькими из объектов и запросов, противник раскроет координаты движения честного(-ых) участника(-ов) и, таким образом, повлияет на скорость движения подконтрольного(-ых) ему объектов и запросов с тем, чтобы создать опасную близость (столкновение).

Протоколы конфиденциальных вычислений должны противостоять и первому, и второму типу противников, в том числе и при многостороннем взаимодействии с большим количеством участников движения и его интенсивностью и с установленным порогом на количество участников движения, находящихся под контролем противника.

В настоящей работе будет рассматриваться частный случай таких вычислений – случай с двумя участниками (одним запросом и одним объектом) и с получестным противником.

Основные определения, модели, используемые протоколы

Обозначим *длину входа задачи* и *параметр безопасности* через n. Будем говорить, что *функция* $\mu(\cdot)$ является *пренебрежимо малой* (по n), если для любого положительного полинома $p(\cdot)$ и всех достаточно больших n верно $\mu(n)<1/p(n)$. Пусть S – бесконечное множество, а $X=\{X_s\}_{s\in S}$ и $Y=\{Y_s\}_{s\in S}$ – ансамбли распределений. Будем говорить, что X и Y *вычислительно неразличимы*, обозначаются как $X \equiv^c Y$, если для любого вероятностного полиномиально-временного алгоритма D и всех достаточно больших $s\in S$, $|\Pr[D(X_s)=1]-\Pr[D(Y_s)=1]|$ является пренебрежимо малым по $|s|$.

Задачу конфиденциальных вычислений, которая решается посредством многостороннего интерактивного протокола, неформально можно описать в следующей общей постановке. Имеется n участников протокола, соединенных сетью связи. Изначально каждому участнику известна своя «часть» некоторого набора входных значений. Требуется реализовать функциональность f, которая «известна» всем участникам системы, таким образом, чтобы выполнились условия:

корректности, когда f должна быть реализована правильно, даже если некоторая ограниченная часть участников протокола произвольным образом отклоняется от предписанных им действий;

конфиденциальности, когда в результате выполнения вычислений не один из участников протокола не получает никакой дополнительной информации о входных значениях других участников.

Задачу двустороннего конфиденциального вычисления функции, которая решается посредством двустороннего интерактивного протокола, можно описать в следующей постановке. Изначально каждому из участников известно значение своего числа x_1 и x_2. Требуется вычислить $f(x_1,x_2)$, таким образом, чтобы в результате выполнения протокола не один из участников не получил бы никакой дополнительной информации о началь-

[2] См. [7, п. 7.2.2]. *Получестный противник* (Semi-HonestAdversary) – участник вычислений, который следует инструкциям протокола, за одним исключением, – он сохраняет все промежуточные результаты вычислений, хотя должен их стирать.

[3] Числом не более заданного порога.

[4] См. [7, п. 7.2.3]. *Злонамеренный противник* (MaliciousAdversary) – участник вычислений, который независимым образом отклоняется от предписанных инструкций протокола.

ных значениях другого участника (кроме той, которая содержится в вычисленном значении функции).

Всюду далее, по сложившейся в современной теории криптографических протоколов традиции их абонентов в двухстороннем сценарии, будем именовать абонент **A** (Алиса) и абонент **B** (Боб).

Далее нам понадобится двусторонний протокол конфиденциального вычисления пересечения двух окружностей. Решение *задачи конфиденциального вычисления пересечения двух окружностей*, которая решается посредством двухстороннего интерактивного протокола, было предложена в работе [6]. Протокол можно описать в следующей постановке. Есть два участника, имеющих у себя конфиденциальные координаты центров окружностей (x_1,y_1) и (x_2,y_2). Обоим задан радиус этих окружностей – ρ.[5] Цель протокола, который далее будет обозначаться как протокол **ПП2О**, состоит в решении задачи, имеют ли окружности с этими координатами их центров пересечение, не раскрывая значения координат. Обозначается далее это следующим образом: b=**ПП2О**$((x_1,y_1),(x_2,y_2))$, где b=true, окружности с этими центрами пересекаются, b=false, в противном случае.

В *модели противника*, которая рассматривается в настоящей работе, *статический получестный противник* контролирует одного из участников протокола (статический противник означает, что такой контроль устанавливается в начале вычислений) и далее участники точно следуют транскрипции протокола, за некоторым исключением, – получестный участник протокола может записывать и сохранять информацию на всех промежуточных этапах вычислений и попытаться что-либо узнать о конфиденциальном входе «контрагента» из нее (хотя в случае честного поведения они должны стирать такую информацию).

Двусторонний протокол конфиденциального вычисления функции, как правило, инициирует случайный процесс, который отображает пару входов в пару выходов (для каждого из участников). Такой процесс назовем *функциональностью* и обозначим как $f:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*$, где $f=(f_1,f_2)$. То есть для каждой пары входов $x,y\in\{0,1\}^n$ парой выходов является случайная величина $(f_1(x,y),f_2(x,y))$ над парами строк. Первый участник (со входом x) желает получить $f_1(x,y)$, а второй участник (со входом y) желает получить $f_2(x,y)$. Будем обозначать такую функциональность как $(x,y)\to(f_1(x,y),f_2(x,y))$. Интуитивно, протокол является безопасным, если всё, что может быть вычислено участником протокола может быть вычислено только на основе его входа и выхода. Это обычно формализуется в соответствии с некоторой парадигмой моделирования (симуляции) [7].

Определение 1. Пусть $f=(f_1,f_2)$ – вероятностная полиномиально-временная функциональность и пусть π – двусторонний протокол, реализующий функциональность f. Тогда:

транскрипция i-го участника ($i\in\{1,2\}$) во время выполнения π на (x,y), обозначается как $\text{view}_i^{\pi}(x,y)$, составляет $(x,r^i,m_1^i,\ldots,m_t^i)$, где r^i – некоторое случайное значение i-того участника, а m_j^i представляет собой j-тое сообщение, которое он получил;

выход i-го участника во время выполнения π на (x,y), обозначается как $\text{output}_i^{\pi}(x,y)$, может быть вычислен во время выполнения протокола π.

Обозначим $\text{output}^{\pi}(x,y)=(\text{output}_1^{\pi}(x,y),\text{output}_2^{\pi}(x,y))$.

[5] В оригинальной работе [12] – для каждой из окружностей задан свой радиус ρ_1и ρ_2.

Определение 2 (безопасности получестного поведения). Пусть $f=(f_1,f_2)$ – *функциональность*. Будем говорить, что π безопасно вычисляет f *в присутствии статического получестного противника*, если существуют вероятностные полиномиально-временные алгоритмы S_1 и S_2, такие, что

$$\{(S_1(x,f_1(x,y)),f(x,y))\}_{x,y\in\{0,1\}^*}\equiv^c\{\mathrm{view}_1{}^{\pi}(x,y),\mathrm{output}^{\pi}(x,y))\}_{x,y\in\{0,1\}^*} \quad (1)$$

$$\{(S_2(y,f_2(x,y)),f(x,y))\}_{x,y\in\{0,1\}^*}\equiv^c\{\mathrm{view}_2{}^{\pi}(x,y),\mathrm{output}^{\pi}(x,y))\}_{x,y\in\{0,1\}^*}, \quad (2)$$

где $|x|=|y|$.

Выражения (1) и (2) устанавливают, что транскрипция участника протокола может быть смоделирована с помощью вероятностного полиномиально-временного алгоритма с доступом только ко входу и выходу участника. Подчеркнем, что противник здесь является получестным и поэтому транскрипция точно соответствует определениям протокола [7].

Определение 3 (для детерминированных функциональностей). Упрощенная формулировка для детерминированных функциональностей может быть следующей. Совместное распределение выхода симулятора и выхода протокола не рассматривается. Скорее, отдельно требуется, чтобы

$$\{\mathrm{output}^{\pi}(x,y)\}_{x,y\in\{0,1\}^*}\equiv^c\{f(x,y)\}_{x,y\in\{0,1\}^*}$$

и, кроме того, что существуют S_1 и S_2такие что:

$$\{(S_1(x,f_1(x,y))\}_{x,y\in\{0,1\}^*}\equiv^c\{\mathrm{view}_1{}^{\pi}(x,y)\}_{x,y\in\{0,1\}^*},$$

$$\{(S_2(y,f_2(x,y))\}_{x,y\in\{0,1\}^*}\equiv^c\{\mathrm{view}_2{}^{\pi}(x,y)\}_{x,y\in\{0,1\}^*}.$$

Причина того, что этого будет достаточно, заключается в том, что когда f является детерминированной $\{\mathrm{output}^{\pi}(x,y)\}$ должна равняться $f(x,y)$. Кроме того, различающий алгоритм для ансамблей распределений может вычислить $f(x,y)$ сам ([7, п. 7.2.2]).

Определение 4 (для детерминированных функциональностей с одним выходом). Будем говорить, что функция $f(x,y)$ является *функциональностью с одним выходом*, если $f_1=f_2$.

Здесь мы покажем, как безопасно вычислить только детерминированную функциональность с одним выходом.

Формальная постановка задачи об опасной близости для двух участников

Формально *задача об опасной близости для двух участников* формулируется следующим образом. Пусть заданы две функции $\varphi_o:[0,\tau^o{}_{max}]\to[0,h]$ и $\varphi_q:[0,\tau^q{}_{max}]\to[0,s]$. Функции являются непрерывными и строго монотонными на всей области определения и удовлетворяют условию $\varphi_o(0)=\varphi_q(0)=0$, $\varphi_o(\tau^o{}_{max})=h$, $\varphi_q(\tau^q{}_{max})=s$, где h,s – вещественные числа.

Имеются запрос и объект, движущиеся таким образом, что их координаты в зависимости от функций φ_o, φ_q и времени t_i задаются парами $(x_o,y_o),(x_q,y_q)$, где $i\in\mathbb{N}$, $x_o,x_q\in[0,s]$, $y_o,y_q\in[0,h]$, а t_i образует строго возрастающую последовательность вещественных чисел. Дифференцируемые строго возрастающие функции φ_o и φ_q называются *законом движения объекта* и *законом движения запроса*.

В задаче требуется определить момент времени для запроса, с которым объект в процессе своего движения будет находиться на расстоянии меньшем, чем $\rho<s,h$, то есть определить, существует ли момент времени $t\in\mathbb{R}$ такой, что окружности с радиусом ρ и центрами $(x_o,y_o),(x_q,y_q)$ имеют пересечение.

Одно из решений задачи об опасной близости для объекта и запроса **A** и **B**, движущихся к навстречу друг другу, с одновременным обеспечением конфиденциальности их местоположения может заключаться в следующем. Попав в некоторую локальную зону управления движением, запрос начинают осуществлять поиск ближайшего объекта и, в случае нахождения такого объекта, начинает устанавливать их взаимное расположение. Установив, что они пересекают некоторую точку одновременно, объект должен снизить (или повысить) скорость с тем, чтобы проехать его позже (раньше) своего «визави», не разгласив при этом своих координат.

На рис. 2 показано движение точек $\boldsymbol{P}_\mathbf{A}$ и $\boldsymbol{P}_\mathbf{B}$ (объекта и запроса) к точке пересечения их движения $\boldsymbol{P}_\mathbf{П}$ (потенциальной точке столкновения). В каждый предопределенный момент времени они устанавливают, пересекаются ли «их окружности» с радиусом ρ, то есть устанавливают

$$\exists\, t:\ \text{true}=\mathbf{ПП2О}((x_1,y_1),(x_2,y_2)). \qquad (3)$$

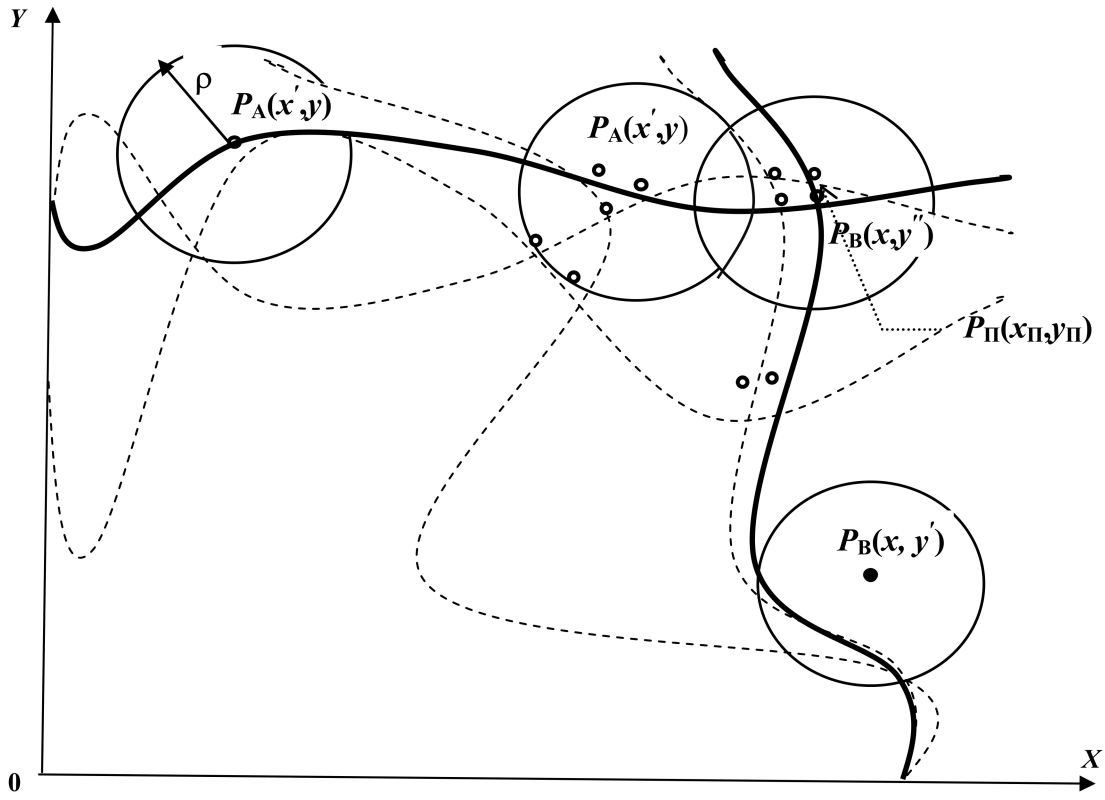

Рис. 2. Иллюстрация потенциального движения запроса и объекта в момент их появления на границах зоны

Таким образом, *задачей о предотвращении столкновения участников* **A** *и* **B** *с одновременным обеспечением конфиденциальности их местоположения* является тройка

($\varphi_{\mathbf{A}},\varphi_{\mathbf{B}},\rho$), а ($x_{\mathbf{A}},y_{\mathbf{A}}$) и ($x_{\mathbf{B}},y_{\mathbf{B}}$) – конфиденциальные координаты центров окружностей **A** и **B** до и после начала вычислений, соответственно.

Задача решается посредством реализации двустороннего протокола π, конфиденциальными входами которого являются ($x_{\mathbf{A}},y_{\mathbf{A}}$) и ($x_{\mathbf{B}},y_{\mathbf{B}}$), а выходом – значение предиката b, где b=1, означает объекту **A** «снизить скорость» (или «повысить скорость»), b=0, в противном случае. Протокол π вычисляет функцию f на аргументах (($x_{\mathbf{A}},y_{\mathbf{A}}$),($x_{\mathbf{B}},y_{\mathbf{B}}$)) с получением значения b, где $b=f_1(x_{\mathbf{A}},y_{\mathbf{A}})=f_2(x_{\mathbf{B}},y_{\mathbf{B}})$.

Протокол конфиденциального предотвращения столкновения КПС

Описание протокола КПС

Протокол π далее именуется *протоколом конфиденциального предотвращения столкновения* и обозначается **КПС**. В протоколе **КПС** необходимо определить существует ли t, удовлетворяющее (3), и вычислить b без раскрытия Бобу координаты ($x_{\mathbf{A}},y_{\mathbf{A}}$) и, соответственно, Алисе координаты ($x_{\mathbf{B}},y_{\mathbf{B}}$)**.**

Протокол КПС

Конфиденциальный вход Алисы: ($x_{\mathbf{A}},y_{\mathbf{A}}$); *конфиденциальный вход Боба*: ($x_{\mathbf{B}},y_{\mathbf{B}}$).

Следующие шаги выполняются l раз, где шаг устанавливается каким-либо очевидным образом между моментом появления **A** на границе зоны (на границе прямоугольника) и моментом пересечения траектории движения **B** плюс один шаг.

1. Алиса и Боб выполняют протокол **ПП2О** со своими входами ($x_{\mathbf{A}},y_{\mathbf{A}}$) и ($x_{\mathbf{B}},y_{\mathbf{B}}$), соответственно[6].

2. Как только выходом протокола **ПП2О** становится значение «true», то существует момент времени t, при котором возможно столкновение.

3. Если такой момент t существует, то присвоить b:=true, в противном случае b:=false.

Выход протокола. Если b=true, выдать «команду на понижение скорости» Алисе, если b=false, в противном случае.

Безопасность протокола КПС

Необходимо показать, что протокол **КПС** является безопасным, то есть получестным сторонам «не хватает» информации или ресурсов для раскрытия значений координат (x_A,y_A), принадлежащей Алисе, и координаты **($x_{\mathbf{B}},y_{\mathbf{B}}$)**, принадлежащей Бобу. Если протокол **ПП2О** безопасен в отношении разглашения координат центров окружностей, то протокол **КПС** безопасен в смысле определения 3 для функциональностей с одним выходом в смысле определения 4.

В работе [6] показаны корректность и конфиденциальность протокола **ПП2О**. Сам протокол строится на известных протоколах конфиденциального вычисления функции: *протоколе конфиденциального сравнения двух чисел* (протоколе Яо [8]) и *протоколе конфиденциального вычисления скалярного произведения двух векторов* (протоколе Ду-Аталлаха [9]).

Доказательство корректности, как правило, следует из правильно построенной арифметической или геометрической структуры протоколов, а для доказательства конфиденциальности моделируется «поведение» Алисы и Боба с помощью вероятностных полиномиально-временных алгоритмов (симуляторов) S_i, i = 1,2, для создания строк, неотличимых (в одном цикле)

[6] Если x и y представлены географическими координатами, то $0<x<360$ и $0<y<180$ (с точностью до 1 градуса) и $0<x<3600000$и $0<y<1800000$ (с точностью до 1 секунды).

$$\{(S_1(x, f_1(x,y))\}_{x,y\in\{0,1\}^*} \equiv^c \{\text{view}_1^{\pi}(x, f_1(x,y))\}_{x,y\in\{0,1\}^*}, \quad (4)$$

$$\{(S_2(y, f_2(x,y))\}_{x,y\in\{0,1\}^*} \equiv^c \{\text{view}_2^{\pi}(y, f_2(x,y))\}_{x,y\in\{0,1\}^*} \quad (5)$$

$$\{\text{output}^{\pi}(x,y)_{x,y\in\{0,1\}^*} \equiv^c \{f(x,y)\}_{x,y\in\{0,1\}^*}, \quad (6)$$

где x – координата, принадлежащая Алисе, а y – координата, принадлежащая Бобу.

Симуляторы S_1 и S_2 должны создавать такие же распределения вероятностей своих параметров, как Алиса и Боб в протоколе **КПС**, а «точнее», в протоколе **ПП2О**. Так как по предположению он безопасен, то параметры взаимодействия при моделировании имеют те же распределения вероятностей (или, по крайней мере, они вычислительно неразличимы), что и при реальном выполнении протокола **ПП2О.** Следовательно, если ансамбли распределений (4) – (6) не различимы никаким полиномиальным алгоритмом, то протокол **КПС** следует считать безопасным.

В то же время если точное определение координат ($x_{\mathbf{A}}$,$y_{\mathbf{A}}$) и ($x_{\mathbf{B}}$,$y_{\mathbf{B}}$) вычислительно невозможно, **А** и **В** всё же могут получить частичную информацию о местоположении своего «визави». Так, команда «на понижение скорости» Алисе дает ей информацию о том, что Боб находится от нее на расстоянии менее, чем 2ρ, а знание траектории движения, по которой движется Боб (строго с юга на север), может дать ей информацию о примерном отрезке пути, на котором он находится в определенный момент времени. И наоборот. По всей вероятности, от извлечения из протокола такого рода частичной информации «избавиться» невозможно, по крайней мере, в протоколе **КПС**.

Сложность протокола КПС

Сложность протокола **ПП2О** составляет сложность выполнения двух протоколов Яо и двух протоколов Ду-Аталлаха [6]. В случае эффективности двух последних (их полилогарифметические реализации можно найти сегодня в криптографической литературе), протокол **ПП2О** – эффективен.

Раундовая сложность протокола **КПС**составляет l раз выполнения протокола **ПП2О**. Следовательно, весь протокол **КПС** – достаточно эффективен.

Решение задачи об опасной близости для многих участников

Пусть множество J состоит из пронумерованных объектов, находящихся в опасной близости: $J(\rho,q,V)=\{o_i \in V \mid \exists\, t : \text{true}=\mathbf{ПП2О}((x_1,y_1),(x_2,y_2))$, $i=1,2,\ldots$. *Библиотека* V является множеством объектов, находящихся в текущий момент времени t внутри рассматриваемого прямоугольника. Тройку (ρ,q,V) будем называть *задачей об опасной близости для многих участников.*

Алгоритмом А решения задачи об опасной близости будем называть совокупность процедур поиска, вставки и удаления в множестве *J. Вставкой* объекта *о* в множество *J* является такое его преобразование, при котором библиотека V преобразуется в $V\cup\{o\}$ и алгоритм A при этом решает задачу *поиска* для задачи (ρ,q,V). А *удалением* объекта *о* из множества *J* является такое его преобразование, при котором библиотека V преобразуется в $V\setminus\{o\}$ и алгоритм A при этом решает задачу *поиска* для задачи (ρ,q,V).

Формулировку задачи об опасной близости в терминах информационных графов, можно найти в [4], где информационный граф рассматривается как модель данных с возможностью поиска, вставки и удаления в нем. В этой же работе предлагаются алгоритмы решения задачи об опасной близости путем ее сведения к задаче одномерного интервального поиска и доказываются утверждения о существовании таких алгоритмов с *логарифмической сложностью операций поиска, вставки и удаления*.

Таким образом, решение задачи об опасной близости для многих объектов сводится к реализации операций поиска, вставки и удаления над множеством J *с* библиотекой V (решению задачи одномерного интервального поиска в информационном графе), а конфиденциальность координат этих объектов, по-прежнему, можно обеспечить использованием протокола **КПС**.

Заключение

Конечно, здесь представлена упрощенная ситуация с постановкой и решением задачи об опасной близости с одновременным обеспечением конфиденциальности местоположения объектов и запросов в самом упрощенном виде (в случае с двусторонним протоколом конфиденциального вычисления функции и в случае с получестным противником). Приведены только самые общие соображения по доказательству безопасности предложенного протокола **КПС**.

Во-первых, сама задача об опасной близости (о предотвращения столкновений) в общем случае предполагает множество решений (см., например, анализ в [1]), и какие из них допускают (и допускают ли?). Эффективность решения в конфиденциальном сценарии только предстоит выяснить.

Во-вторых, если построение протоколов для решения такого рода задач возможно, это предполагает доказательство их корректности и конфиденциальности, что (даже в случае статических получестных противников), скорее всего, будет весьма нетривиально [1, 11].

Представленное здесь решение позволяет «двигаться дальше» в направлении создания протоколов для многосторонних конфиденциальных вычислений в модели со злонамеренным противником[7], для трехмерного пространства (то есть с обеспечением конфиденциальности трех координат точечных объектов[8] соответственно), что дает возможность решать более общие задачи, поставленные во введении.

СПИСОК ЛИТЕРАТУРЫ:

1. Снегова Е.А. Критерий сводимости задачи об опасной близости к одномерному интервальному поиску // Дискретная математика. 2011. Т. 23. Вып. 5. С. 138 – 159.
2. Казарин О.В. Практически реализуемые системы многосторонних конфиденциальных вычислений // Защита информации. INSIDE. 2016. № 3. С. 36 – 42.
3. Астреин В.В. Системы предупреждения столкновения судов, тенденции развития // Вестник АГТУ. Сер. Морская техника и технология. 2013. № 3. С. 7 – 17.
4. Скиба Е.А. Логарифмическое решение задачи об опасной близости // Интеллектуальные системы. 2007. 11: 1–4. С. 693–719.
5. Снегова Е.А. Сложность задачи о предотвращении столкновении // Автореферат диссертации на соискание ученой степени кандидата физико-математических наук. МГУ имени М.В. Ломоносова, 2012. URL: http://mech.math.msu.su/~snark/files/vak/arzg0.pdf (дата обращения: 20.01.2017).
6. Yang B., Sun A., Zhang W. Secure two-party protocols on planar circles // Journal of Information & Computational Science. 2011. № 8. P. 29 – 40.
7. Goldreich O. Foundations of cryptography: Volume 2 – Basic Applications. Cambridge University Press, 2004.
8. Yao A.C. Protocols for secure computations (extended abstract) // Proc. of 23-rd IEEE Symp. on Founda-tions of Computer Science. 1982. P. 160 – 164.
9. Du W., Attalach M. J. Privacy-preserving cooperative scientific computations // Proceeding of the 2002 Workshop on New Security Paradigms, NSPW'2002, Virginia Beach, VA, 23–26 September 2002, New York, NY, ACM Press. P. 127–135.
10. Казарин О. В.Методология защиты программного обеспечения. М.: МЦНМО, 2009.

[7] Тем более что теоретические результаты в области конфиденциальных вычислений предполагают (при некоторых условиях) возможность построения компиляторов, которые преобразуют любые протоколы для модели с получестным противником в эквивалентные протоколы для двух моделей со злонамеренным противником. См. аргументацию в [2, § 3.6].

[8] Например, в случае перспективных систем управления беспилотными летательными аппаратами (дронами).

11. Казарин О. В. О возможности сокрытия местоположения абонента сотовой связи с использованием методов конфиденциальных вычислений // Вопросы защиты информации. 2016. № 1. С. 39 – 47.

REFERENCES:

1. Snegova E.A. Kriterij svodimosti zadachi ob opasnoj blizosti k odnomernomu interval'nomu poisku // Diskretnaya matematika, 2011, Vol. 23, no. 5, pp. 138 – 159 (in Russian).
2. Kazarin O.V. Prakticheski realizuemye sistemy mnogostoronnikh konfidentsial'nykh vychislenij // Zashhita informatsii. INSIDE, 2016, no 3, pp. 36 – 42 (in Russian).
3. Astrein V.V. Sistemy preduprezhdeniya stolknoveniya sudov, tendentsii razvitiya. Vestnik AGTU. Ser.: Morskaya tekhnika i tekhnologiya, 2013, no. 3, pp. 7 – 17 (in Russian).
4. Skiba E.A. Logarifmicheskoe reshenie zadachi ob opasnoj blizosti // Intellektual'nye sistemy, 2007, Vol. 11: 1–4. Pp. 693–719 (in Russian).
5. Snegova E.A. Slozhnost' zadachi o predotvrashhenii stolknovenii // Avtoreferat dissertatsii na soiskanie uchenoj stepeni kandidata fiziko-matematicheskikh nauk. MGU imeni M.V. Lomonosova, 2012. Available at: http://mech.math.msu.su/~snark/files/vak/arzg0.pdf (accessed: 20.01.2017)/ (in Russian).
6.Yang B., Sun A., Zhang W. Secure two-party protocols on planar circles // Journal of Information & Com-putational Science. 2011. № 8. Pp. 29 – 40.
7.Goldreich O. Foundations of cryptography: Volume 2 – Basic Applications. Cambridge University Press, 2004.
8.Yao A.C. Protocols for secure computations (extended abstract) // Proc. of 23-rd IEEE Symp. on Founda-tions of Computer Science. 1982. Pp. 160 – 164.
9.Du W., Attalach M. J. Privacy-preserving cooperative scientific computations // Proceeding of the 2002 Workshop on New Security Paradigms, NSPW'2002, Virginia Beach, VA, 23–26 September 2002, New York, NY, ACM Press, pp. 127–135.
10.Kazarin O.V. Metodologiya zashhity programmnogo obespecheniya. M.: MTSNMO, 2009.
11.Kazarin O.V. O vozmozhnosti sokrytiya mestopolozheniya abonenta sotovoj svyazi s ispol'zovaniem metodov konfidentsial'nykh vychislenij // Voprosy zashhity informatsii, 2013, no 1, pp. 39 – 47 (in Russian).