УДК 004.057.4
DOI: 10.55648/1998-6920-2022-16-2-33-39

Криптографический протокол поиска места встречи участников со свойством конфиденциальности

И. Д. Иогансон, А. А. Голованов, Ж.-М. Н. Дакуо, В. В. Давыдов[1]

Предложен новый криптографический протокол поиска места встречи участников. Такой протокол позволяет нескольким участникам выбрать место встречи, наиболее близкое к их местоположениям, при этом не раскрывая координаты каждого из участников. Протокол также позволяет детектировать ошибку, которая возникла в ходе передачи информации между участниками. Доказана корректность и безопасность используемого подхода, определены его основные достоинства и недостатки.

Ключевые слова: криптографический протокол, свойство конфиденциальности, протоколы конфиденциального вычисления.

1. Введение

Криптографические протоколы занимают очень важное место в современных информационных системах. Построение надёжных протоколов определяет безопасность системы и её корректное функционирование.

Одними из важнейших на сегодняшний день криптографических схем являются протоколы конфиденциального вычисления. Основная идея таких протоколов заключается в том, чтобы вычислить результат некоторой функции от закрытых данных нескольких участников, при этом не нарушая конфиденциальности.

История конфиденциальных вычислений началась с работы Эндрю Яо о «задаче двух миллионеров», в которой два участника хотят выяснить, кто из них богаче, не раскрывая размеры своих состояний [1]. Яо предложил защищённый протокол, позволяющий решить эту задачу, а также ввёл понятие протоколов конфиденциального вычисления. В настоящее время подобные протоколы находят широкое применение в различных областях. Например, они широко используются в медицине для обучения моделей диагностики без раскрытия данных пациентов [2]. Также распространено использование в статистике, например, для анализа различия в заработной плате в зависимости от пола без раскрытия точного размера зарплаты [3].

В данной работе уделено внимание протоколам, которые позволяют вычислить сумму секретных значений нескольких пользователей. В работе [4] приведён пример простейшего варианта такого протокола. Он имеет следующую структуру:

1. Пользователям присваиваются номера от 1 до k.
2. Пользователь 1 генерирует случайное число m_0.
3. Далее, начиная с пользователя 1, каждый пользователь i получает значение m_{i-1} от пользователя $i-1$ (или в случае пользователя 1 это будет просто сгенерированное им значение

[1] Работа выполнена при поддержке программы «Приоритет 2030».

m_0) и отправляет пользователю $i+1$ (пользователь k отправит свое значение пользователю 1) значение $m_i = m_{i-1} + x_i$, где x_i – входное значение пользователя i.

4. В конце пользователь 1 вычисляет значение $m_k - m_0$, равное искомой сумме, и отправляет его остальным пользователям.

В статье [5] описан так называемый «k-Secure Sum Protocol». Этот протокол для n пользователей выглядит следующим образом:

1. Пусть k – целое число, обозначающие параметр безопасности.
2. Пусть пользователи пронумерованы от 0 до $n-1$.
3. Пусть D_i – входное значение, принадлежащее пользователю i.
4. Разобьём D_i на k сегментов $D_{i0},\ldots,D_{i(k-1)}$ таким образом, что $D_i = \sum_{j=0}^{k-1} D_{ij}$.
5. Пусть $S_{00} = 0$.
6. Для j от 0 до $k-1$:
   a. Для i от 0 до $n-1$:
      i. Пользователь i посылает пользователю $(i+1) \bmod n$: $S_{(i+1)j} = S_{ij} + D_{ij}$.
   b. $S_{0(j+1)} = S_{nj}$.
7. Пользователь 0 публикует значение S_{0k}.

У приведённых выше протоколов есть схожий недостаток: в самом конце первый пользователь получает результат и публикует его. Проблема заключается в том, что если первый пользователь является злоумышленником, то ему не составит труда подменить результат на нужный ему.

В данной работе предлагается новый протокол для конфиденциального вычисления места встречи группы людей, которые хотят сохранить своё исходное местоположение в тайне. Пусть k пользователей $P_1, P_2, \ldots, P_k$ хотят договориться о встрече. Исходное местоположение каждого пользователя выражено числом $x_i \in \mathbb{R}$, где $i \in \{1 \ldots k\}$, которое является координатой в некоторой системе координат. Требуется найти координату встречи y, наиболее удобную для всех участников, что в данной работе понимается как среднее арифметическое значение:

$$y = \frac{\sum_{i=1}^{k} x_i}{k}. \quad (1)$$

При этом предлагаемый протокол обладает следующими свойствами:

1. Значение x_i не раскрывается пользователем P_i ни на одном из этапов.
2. Нет необходимости доверять единственному пользователю вычисление и публикацию итогового значения, так как каждый пользователь может вычислить y.
3. В генерации случайных чисел участвуют все пользователи. Это необходимо, чтобы не концентрировать ответственность за случайную компоненту на единственном пользователе. Если за генерацию случайных чисел отвечает только один пользователь, то он может использовать нестойкий алгоритм генерации псевдослучайных чисел, который позволит предсказывать получаемые значения. Это может открыть возможности для атак на конфиденциальность системы.

2. Описание протокола

Протокол разбит на несколько этапов: инициализация, первый – третий круги и завершение. Опишем каждый этап более подробно.

1. Инициализация.

На этапе инициализации пользователи формируют защищенные каналы между соседями так, как это продемонстрированно на рис. 1. По необходимости каждый пользователь представляет свое значение x_i в виде целого числа умножением на 10^r, где r – это максимально допустимое количество значащих цифр после запятой. Далее каждый пользователь формирует обязательство, подобное тому, что использовал П. Фельдман в своей проверяемой схеме разделения секрета [6], для своего значения x_i: $C_i = x_i \cdot G$, где G – генераторная точка на эллиптической кривой (ЭК) E над полем F_q, где q – простое. ЭК E и точка G известны всем пользователям. Обязательства $C_1 \ldots C_k$ публикуются в свободном доступе для каждого пользователя.

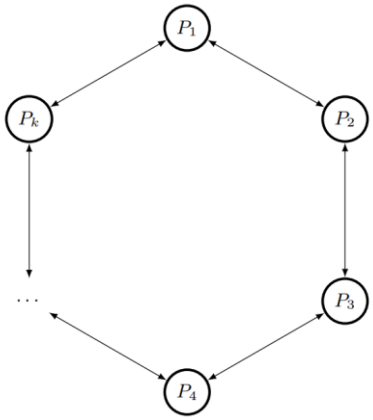

Рис. 1. Общий вид схемы

2. Первый круг.

Каждый пользователь выбирает случайное значение $s_i \in_R \mathbb{Z}$. Далее начинается передача сообщений. Обозначение $P_a \to P_b$: обозначает, что пользователь P_a передаёт информацию пользователю P_b, после двоеточия описана передаваемая информация. Также будем считать, что $P_{k+1} = P_1$.

Передаваемая информация вычисляется по правилу:

$$P_i \to P_{i+1} : m_{1,i} = m_{1,i-1} + x_i + s_i, \tag{2}$$

где $m_{1,0} = 0$.

3. Второй круг.

Пусть

$$m_{2,0} = m_{1,k} = \sum_{i=1}^{k} \left(x_i + s_i \right). \tag{3}$$

Тогда правила вычисления передаваемой информации на данном круге:

$$P_i \to P_{i+1} : m_{2,i} = m_{2,i-1} - 2s_i - x_i. \tag{4}$$

4. Третий круг.

Пусть

$$m_{3,0} = m_{2,k} = -\sum_{i=1}^{k} s_i. \tag{5}$$

Тогда правила вычисления передаваемой информации на данном круге:

$$P_i \to P_{i+1} : m_{3,i} = m_{3,i-1} + s_i. \tag{6}$$

Если в конце протокола пользователь P_1 получил значение $m_{3,k}$. Если $m_{3,k} = 0$, то протокол считается корректно выполненным, и P_1 рассылает сообщение о корректном окончании протокола. Иначе – во время работы протокола возникла ошибка, и P_1 рассылает сообщение о том, что протокол окончился с ошибкой.

5. Завершение.

Каждый пользователь P_i обладает набором значений $\{m_{1,i}, m_{2,i}, m_{3,i}\}$, полученных им на кругах 1, 2 и 3 соответственно. Далее он вычисляет:

$$y = \frac{m_{1,i} + m_{2,i} + m_{3,i}}{k}. \tag{7}$$

Данное значение и является координатой сбора.

Также каждый пользователь проводит валидацию полученного значения с помощью обязательств $C_1 \ldots C_k$, полученных на этапе инициализации, по формуле:

$$\sum_{i=1}^{k} C_i = (k \cdot y) \cdot G. \tag{8}$$

3. Доказательства корректности и безопасности

3.1. Доказательство корректности

На конце 1-го и 2-го кругов пользователь P_1 получает значения:

$$m_{1,k} = \sum_{j=1}^{k} (x_j + s_j); \tag{9}$$

$$m_{2,k} = -\sum_{j=1}^{k} s_j. \tag{10}$$

Пользователь P_i по итогу каждого круга имеет значения:

$$m_{1,i} = \sum_{j=1}^{i} (x_j + s_j); \tag{11}$$

$$m_{2,i} = \sum_{j=1}^{k} (x_j + s_j) - \sum_{j=1}^{i} (x_j + 2s_j) = \sum_{j=i+1}^{k} (x_j + s_j) - \sum_{j=1}^{i} s_j; \tag{12}$$

$$m_3 = -\sum_{j=1}^{k} s_j + \sum_{j=1}^{i} s_j = -\sum_{j=i+1}^{k} s_j. \tag{13}$$

Тогда

$$y = \frac{1}{k}\left(m_{1,i} + m_{2,i} + m_{3,i}\right) = \\ = \frac{1}{k}\left(\sum_{j=1}^{i}\left(x_j + s_j\right) + \sum_{j=i+1}^{k}\left(x_j + s_j\right) - \sum_{j=1}^{i} s_j - \sum_{j=i+1}^{k} s_j\right) = \frac{1}{k}\sum_{j=1}^{k} x_j . \quad (14)$$

3.2. Доказательство безопасности

Каждый пользователь i знает следующий набор значений: $\{k, x_i, s_i, m_{1i}, m_{2i}, m_{3i}, y\}$. Обозначим:

$$x_a = \sum_{j=1}^{i-1} x_j ,\ x_b = \sum_{j=i}^{k} x_j ; \\ s_a = \sum_{j=1}^{i-1} s_j ,\ s_b = \sum_{j=i}^{k} s_j . \quad (15)$$

Тогда сообщения m_{1i}, m_{2i}, m_{3i}:

$$m_{1i} = x_a + s_a ; \\ m_{2i} = x_b + s_b - s_a ; \quad (16) \\ m_{3i} = -s_b .$$

Система из четырёх уравнений с четырьмя переменными x_a, x_b, s_a, s_b:

$$\begin{cases} x_a + s_a = m_{1i} \\ x_b + s_b - s_a = m_{2i} \\ -s_b = m_{3i} \\ x_a + x_b = y * k \end{cases} \quad (17)$$

является линейно зависимой, так как сумма первых трех уравнений равна четвертому:

$$+\begin{cases} x_a + s_a = m_{1i} \\ x_b + s_b - s_a = m_{2i} \\ -s_b = m_{3i} \end{cases} \quad . \quad (18)$$

$$x_a + x_b = m_{1i} + m_{2i} + m_{3i} = y * k$$

Следовательно, данная система не имеет единого решения относительно этих переменных. Таким образом, из имеющегося набора значений пользователь i не может получить информацию об x_j других пользователей (кроме y).

Применяемая схема обязательств основана на проблеме дискретного логарифмирования [7] и не позволяет злоумышленнику раскрыть значение секрета. Также в представленной схеме обязательств отсутствует возможность подмены значения секрета создателем этого обязательства.

4. Оценки протокола

4.1. Обобщение

Данный протокол в базовом варианте работает в 1-мерном пространстве, однако его очевидным образом можно обобщить на n-мерное пространство, где координаты каждого пользователя i задаются n-мерным вектором $X_i = \left(x_{i1}, x_{i2}, \ldots, x_{in}\right)$. В таком случае необходимо

просто произвести данный протокол для каждой из координат по отдельности и на выходе получить $Y = (y_1, y_2, \ldots, y_n)$.

4.2. Ограничения

Данный протокол проводится для k участников. Однако при $k = 2$ оба пользователя очевидным образом, зная $y = \frac{x_1 + x_2}{2}$ и свой x_i, могут найти x_{3-i} другого пользователя. Поэтому число k участников протокола всегда должно быть больше 2.

Также в случае, если у пользователя i были скомпрометированы оба ключа $K_{(i-1)i}$ и $K_{i(i+1)}$, то злоумышленник, перехватив сообщения, которые пользователь принимает и посылает в процессе действия протокола, сможет однозначно установить значение x_i. Аналогичное действие могут совершить пользователи $i+1$ и $i-1$, если сговорятся и поделятся друг с другом сообщениями, которые они посылали и принимали от пользователя i.

Литература

1. *Yao A. C.* Protocols for secure computations // 23rd IEEE Annual symposium on foundations of computer science (SFCS), 1982. P. 160–164.
2. *Dugan T., Zou X.* A survey of secure multiparty computation protocols for privacy preserving genetic tests // 2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2016. P. 173–182.
3. *Lapets A. et al.* Secure MPC for analytics as a web application // 2016 IEEE Cybersecurity Development (SecDev), 2016. P. 73–74.
4. *Clifton C. et al.* Tools for privacy preserving distributed data mining // ACM Sigkdd Explorations Newsletter. 2002. V. 4, №. 2. P. 28–34.
5. *Sheikh R., Kumar B., Mishra D. K.* Privacy preserving k secure sum protocol // arXiv preprint arXiv:0912.0956. 2009.
6. *Feldman P.* A practical scheme for non-interactive verifiable secret sharing // 28th IEEE Annual Symposium on Foundations of Computer Science (SFCS), 1987. P. 427–438.
7. *Silverman J. H., Pipher J., Hoffstein J.* An introduction to mathematical cryptography. Springer New York, 2008.

Статья поступила в редакцию 25.04.2022;
переработанный вариант – 01.05.2022.

Иогансон Иван Дмитриевич
инженер факультета безопасности информационных технологий Университета ИТМО (197101, Санкт-Петербург, Кронверкский просп., д. 49, литер А), e-mail: ivan.iogan-son@yandex.ru.

Голованов Андрей Андреевич
инженер факультета безопасности информационных технологий Университета ИТМО, e-mail: agolovanov2403@gmail.com.

Дакуо Жан-Мишель Никодэмович
инженер факультета безопасности информационных технологий Университета ИТМО, e-mail: jeandakuo@mail.ru. .

Давыдов Вадим Валерьевич
преподаватель факультета безопасности информационных технологий Университета ИТМО, e-mail: vvdavydov@itmo.ru.

Cryptographic protocol for finding the meeting place of participants with confidentiality property

Ivan D. Ioganson
Engineer, ITMO University (St. Petersburg, Russia), ivan.ioganson@yandex.ru.

Andrei A. Golovanov
Engineer, ITMO University (St. Petersburg, Russia), agolovanov2403@gmail.com.

Zhan-Mishel N. Dakuo
Engineer, ITMO University (St. Petersburg, Russia), jeandakuo@mail.ru.

Vadim V. Davydov
Lecturer, ITMO University (St. Petersburg, Russia), vvdavydov@itmo.ru.

In this paper a new cryptographic protocol for finding the meeting place of participants is proposed. This protocol allows several participants to choose the meeting place closest to their locations not revealing the coordinates of each of the participants. The protocol also allows to detect an error occurring during the transfer of information between participants. The correctness and security of the used approach are proved, and the main advantages and disadvantages are determined.

Keywords: cryptographic protocol, confidentiality property, secure multi-party computation.

References

1. Yao A. C. Protocols for secure computations. *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*, 1982, pp. 160-164. DOI: 10.1109/SFCS.1982.38.
2. Dugan T., Zou X. A survey of secure multiparty computation protocols for privacy preserving genetic tests. *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, 2016, pp. 173-182. DOI: 10.1109/CHASE.2016.71.
3. Lapets A., Volgushev N., Bestavros A., Jansen F. and Varia M. Secure MPC for analytics as a web application. *2016 IEEE Cybersecurity Development (SecDev)*, 2016, pp. 73-74. DOI: 10.1109/SecDev.2016.027.
4. Clifton C., Kantarcioglu M., Jaideep V., Lin X. and Zhu M. Y. Tools for privacy preserving distributed data mining. *ACM SIGKDD Explorations*, 2003, vol. 4, pp. 28-34.
5. Sheikh R., Kumar B., Mishra D. K. Privacy preserving k secure sum protocol. *International Journal of Computer Science and Information Security*, 2009, vol. 6.
6. Feldman P. A practical scheme for non-interactive verifiable secret sharing. *28th Annual Symposium on Foundations of Computer Science (sfcs 1987),* 1987, pp. 427-438. DOI: 10.1109/SFCS.1987.4.
7. Silverman J. H., Pipher J., Hoffstein J. *An introduction to mathematical cryptography*, Springer New York, 2008. vol 1.