УДК 004.057.4

ПРОТОКОЛ ПЕРЕСЕЧЕНИЯ ЗАКРЫТЫХ МНОЖЕСТВ НА ОСНОВЕ ЗАБЫВЧИВОЙ ПСЕВДОСЛУЧАЙНОЙ ФУНКЦИИ

Иогансон И. Д. (Университет ИТМО)
Научный руководитель – доцент, д. т. н. Беззатеев С. В.
(Университет ИТМО)

Конфиденциальные вычисления являются активно развивающейся областью современной криптографии. Одной из хорошо известных задач в данной области является задача нахождения пересечения множеств двух и более пользователей так, чтобы ни одна из сторон не получила никакой дополнительной информации о множествах других пользователей. В данной работе представлен протокол для решения подобного рода задач, называемый протоколом пересечения закрытых множеств, на основе забывчивой псевдослучайной функции.

Введение. На сегодняшний день широкое распространение находят протоколы конфиденциальных вычислений (secure multi-party computation, MPC), которые позволяют производить вычисления между несколькими сторонами, не раскрывая при этом их входные данные друг другу. Одним из таких протоколов является протокол пересечения закрытых множеств (private set intersection, PSI), и он позволяет группе пользователей, у каждого из которых есть некий набор элементов, найти пересечение их наборов, не раскрывая при этом никакой дополнительной информации.

Основная часть. Основным примитивом, используемым для построения протокола пересечения закрытых множеств, является забывчивая псевдослучайная функция (oblivious pseudorandom function, OPRF). Забывчивая псевдослучайная функция – это протокол, который позволяет получателю узнать значение некой псевдослучайной функции, известной отправителю, причем так, чтобы отправитель не узнал ни входных данных получателя, ни итогового значения. Данный примитив, в свою очередь, основывается на, так называемом, протоколе забывчивой передачи (oblivious transfer, OT), который позволяет получателю узнать одно и только одно из нескольких сообщений, отправленных ему отправителем, причем так, что отправитель не узнает какое из сообщений было принято получателем.

Выводы. Для оценки эффективности представленного решения были посчитаны такие характеристики, как размер переданного трафика, кол-во раундов коммуникации и быстродействие.
Протоколы пересечения закрытых множеств используются, к примеру, когда несколько людей хотят узнать есть ли у них общие контакты, но не хотят раскрывать другим свои связи. Также это может быть использовано, в ситуации, когда две компании хотят объединить данные о клиентах, хранящиеся в их базах данных, но только для тех клиентов, которые пользуются услугами обеих компаний.

Список использованных источников:

1. Kolesnikov, Vladimir & Kumaresan, Ranjit & Rosulek, Mike & Trieu, Ni. Efficient Batched Oblivious PRF with Applications to Private Set Intersection // the 2016 ACM SIGSAC Conference – 2016.
2. BAY, Aslı & KAYAN, Anıl. A new Multi-Party Private Set Intersection Protocol based on OPRFs // Mugla Journal of Science and Technology – 2022.
3. Pinkas, Benny & Schneider, Thomas & Zohner, Michael. Faster private set intersection based on OT extension // ACM Transactions on Privacy and Security – 2018.

Иогансон И. Д. (автор) Подпись

Беззатеев С. В. (научный руководитель) Подпись