УДК 004.057.4

ОБЗОР И АНАЛИЗ ПРОТОКОЛОВ ЗАБЫВЧИВОЙ ПЕРЕДАЧИ

Леевик А.Г. (Университет ИТМО)
Научный руководитель – доктор технических наук, доцент Беззатеев С.В.
(Университет ИТМО)

Введение. Конфиденциальные вычисления — быстро развивающаяся область современной криптографии. На сегодняшний день протоколы конфиденциальных вычислений уже активно используются в медицине, машинном обучении, облачных вычислениях, а также в других областях, использующих распределенные вычисления, а также требующих сохранения конфиденциальности входных данных. Протокол забывчивой передачи является одним из важнейших частей существующих протоколов конфиденциальных вычислений. Безопасность, а также производительность протокола конфиденциальных вычислений базируется в первую очередь на безопасности протокола забывчивой передачи, поэтому требуется проанализировать существующие протоколы забывчивой передачи с точки зрения безопасности и производительности.

Основная часть. Протокол забывчивой передачи — такой протокол, позволяющей одной стороне (получатель) получить выбранные данные у другой стороны (отправитель), не раскрывая отправителю никакой информации о том, какие данные получил получатель, а также не раскрывая получателю оставшихся данных, которыми владеет отправитель. Существует три вариации протокола: 1-из-2, 1-из-n, k-из-n. Безопасность протокола вне зависимости от вариации обычно рассматривается в двух моделях злоумышленника: semi-honest и malicious. Более сильной моделью является модель malicious, именно для данной модели рекомендуется доказывать безопасность протокола забывчивой передачи.

Также с появлением квантовых компьютеров появилась угроза атак с помощью таких компьютеров на криптографические схемы, поэтому требуется оценить новые постквантовые варианты протоколов забывчивой передачи. Для таких протоколов также требуется оценить их безопасность относительно разных моделей, а также размер затрачиваемых ресурсов.

Выводы. В ходе работы были рассмотрены существующие конструкции протокола забывчивой передачи, построенные на разных примитивах. Различные схемы были сравнены между собой по параметрам безопасности и производительности, выявлены основные достоинства и недостатки данных схем. На основе анализа предложены подходы по улучшению данных схем.

Список использованных источников:

1. Evans D. et al. A pragmatic introduction to secure multi-party computation //Foundations and Trends® in Privacy and Security. – 2018. – Т. 2. – №. 2-3. – С. 70-246.
2. Zhao C. et al. Secure multi-party computation: theory, practice and applications //Information Sciences. – 2019. – Т. 476. – С. 357-372.
3. Yadav V. K. et al. A survey of oblivious transfer protocol //ACM Computing Surveys (CSUR). – 2022. – Т. 54. – №. 10s. – С. 1-37.

Леевик А.Г. (автор)

Беззатеев С.В. (научный руководитель)