УДК 004.056

Исследование построения забывчивой псевдослучайной функции

Хуцаева А.Ф. (ИТМО)

Научный руководитель – доктор технических наук, доцент Беззатеев С.В. (ИТМО)

Введение.

В эпоху цифровой трансформации вопросы обеспечения информационной безопасности данных приобретают критическую важность. Одним из ключевых инструментов в этой области являются псевдослучайные функции (ПСФ) [1], которые широко используются для генерации ключей шифрования, аутентификации и защиты информации. Однако в классических ПСФ входное значение (seed) передается в открытом виде, что делает их уязвимыми к атакам на память, таким как по сторонним каналам или анализ утечек данных.

Забывчивые псевдослучайные функции (ЗПСФ) [2] направлены на устранение этой уязвимости. Их основная идея заключается в том, что функция «забывает» часть своего внутреннего состояния в процессе работы, что значительно усложняет задачу злоумышленнику, пытающемуся восстановить случайную последовательность. Это делает ЗПСФ особенно актуальными для протоколов конфиденциальных вычислений, например для протокола пересечения частных множеств или поиска частной информации [3]. Данная работа направлена на изучение свойств ЗПСФ, выявление их преимуществ перед традиционными методами и поиск новых подходов к их реализации.

Основная часть.

Забывчивая псевдослучайная функция позволяет вычислить выходные данные (y) таким образом, что одна сторона (S) знает только секретный ключ (sk), а другая сторона (C) знает входное значение (x). Получается, что S не знает о том, какой был выбран x, а C не может по x и y узнать никакой информации о sk.

В работе описаны функциональные свойства ЗПСФ, например проверяемая ЗПСФ или пороговая ЗПСФ. Согласно выделенным функциям проведен анализ современных ЗПСФ и предложены улучшения по их эффективности.

Проведен анализ доказательства безопасности ЗПСФ в моделях активного и пассивного злоумышленника. Также проведен анализ безопасности ЗПСФ в рамках квантовой угрозы и рассмотрены постквантовые ЗПСФ.

Выводы.

Анализ забывчивых псевдослучайных функций является важным направлением исследований, способным обеспечить безопасность данных в условиях растущих требований к эффективности и защищённости информационных систем. В работе проанализированы подходы при построении ЗПСФ с дополнительными функциями, рассмотрена безопасность ЗПСФ. Данная работа служит фундаментом для дальнейшей разработки ЗПСФ.

Список использованных источников:

1. Bogdanov A., Rosen A. Pseudorandom functions: Three decades later //Tutorials on the Foundations of Cryptography: Dedicated to Oded Goldreich. – Cham : Springer International Publishing, 2017. – С. 79-158.
2. Freedman M. J. et al. Keyword search and oblivious pseudorandom functions //Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2. – Springer Berlin Heidelberg, 2005. – С. 303-324.
3. Morales D., Agudo I., Lopez J. Private set intersection: A systematic literature review //Computer Science Review. – 2023. – Т. 49. – С. 100567.