УДК 004.056.55

Программная реализация схемы WaveVRF

Дакуо Ж.-М.Н. (ИТМО), **Калянский А. Г.** (Политех)
Научный руководитель – доктор технических наук, доцент Беззатеев С. В.
(ИТМО)

Введение. Проверяемая псевдослучайная функция (VRF) представляет собой криптографический механизм, позволяющий генерировать псевдослучайные значения с возможностью их последующей проверки, что нашло широкое применение в блокчейн системах[1], мессенджерах[2] и других цифровых платформах. Традиционные решения, например, на основе RSA[3] и эллиптических кривых[4] уязвимы к квантовым атакам, а существующие постквантовые методы зачастую сталкиваются с проблемами высокой вычислительной сложности и непростой масштабируемости [5,6,7]. В данной работе предложен новый подход на основе схемы подписи Wave[8] с использованием проблемы синдромного декодирования, обеспечивающий устойчивость к квантовым атакам.

Основная часть. В ходе исследования [9] разработана и реализована новая схема VRF, сопровождаемая программой, предназначенной для вычисления ключевых параметров: размеры ключей, размеры подписи, время формирования подписи и время её проверки. Такой подход не только повышает безопасность криптографических протоколов, но и демонстрирует потенциал применения WaveVRF в системах, где требуется надёжная верификация случайных данных.

Для эмпирической проверки псевдослучайности предложенной схемы проведены тесты по стандартам NIST, что позволило выполнить детальный сравнительный анализ с аналогичными решениями. Полученные результаты подтверждают высокую эффективность и масштабируемость разработанной методики, которая сочетает устойчивость к квантовым атакам с практической применимостью в современных условиях кибербезопасности.

Выводы. Предложенная схема VRF, основанная на подписи Wave и использовании проблемы синдромного декодирования, демонстрирует высокую степень безопасности и эффективности. Разработанная методика открывает новые перспективы для оптимизации криптографических протоколов в условиях растущей угрозы квантовых вычислений и может быть успешно интегрирована в современные системы защиты информации.

Список использованных источников:

1. Kiayias A. et al. Ouroboros: A provably secure proof-of-stake blockchain protocol // Annual international cryptology conference. Cham: Springer International Publishing, 2017. P. 357-388.
2. Chagas V., Da-Costa G. WhatsApp and transparency: an analysis on the effects of digital platforms´ opacity in political communication research agendas in Brazil // Profesional de la información. 2023. V. 32. N 2.
3. Micali S., Rabin M., Vadhan S. Verifiable random functions // 40th annual symposium on foundations of computer science (cat. No. 99CB37039). IEEE, 1999. P. 120–130.
4. Dodis Y., Yampolskiy A. A verifiable random function with short proofs and keys // International Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005. P. 416–431.
5. Esgin M.F. et al. Efficient hybrid exact/relaxed lattice proofs and applications to rounding and VRFs // Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2023. P. 484–517.
6. Leroux A. Verifiable random function from the Deuring correspondence and higher dimensional isogenies. 2023.

7. Esgin M.F. et al. A new look at blockchain leader election: Simple, efficient, sustainable and post-quantum // Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security. 2023. P. 623–637.
8. Gasparovic R.F., Apel J.R., Kasischke E.S. An overview of the SAR internal wave signature experiment // Journal of Geophysical Research: Oceans. 1988. V. 93. N C10. P. 12304–12316.
9. Дакуо Ж.Н. WaveVRF: постквантовая проверяемая псевдослучайная функция,основанная на кодах, исправляющих ошибки Научно-технический вестник информационных технологий, механики и оптики [Scientific and Technical Journal of Information Technologies, Mechanics and Optics] - 2025. в печати