УДК 004.056.55

IS-BASED VRF: Проверяемо случайная функция основанная на изогениях.

Дакуо Ж.-М. Н. (Университет ИТМО)
Научный руководитель – д. т. н., доцент Беззатеев С. В.
(Университет ИТМО)

В данной работе была разработана VRF основанная на методах криптографии на суперсингулярных изогений эллиптических кривых.

Введение. В современном мире криптография, в частности проверяемые случайные функции (VRF), играют жизненно важную роль. Они используются в огромном спектре различных задач: от ключа домофона до защиты облачных вычислений и блокчейна. Проверяемые случайные функции— это криптографические примитивы, которые были впервые представлены Микали, Рабином и Вандамом в [1]. Они представляют собой более продвинутую форму псевдослучайной функции, которые не только генерирует псевдослучайные выходные данные, но и предоставляет не интерактивные и публично проверяемые доказательства для полученных значений. Безопасность VRFS сохраняется даже тогда, когда многочисленные копии входных данных, выходных данных и доказательств становятся общедоступными.

Основная часть. Как известно один из претендентов в области выработки общего ключа основанный на суперсингулярных изогениях [2] (Supersingular isogeny key encapsulation SIKE) был взломан в 2022 году [3]. Многие ученые поставили крест на изогениях, но данная область все также бурно развивается. В конце 2023 году была разработана новая схема выработки общего ключа при помощи теоремы Кани и изогений высших размерностей [4]. В разработанной схеме используются четыре алгоритма: ParamGen, KeyGen, VRFEval и Verify. ParamGen создает набор публичных параметром. KeyGen на вход принимает публичные параметры, полученные на предыдущем шаге выдает псевдо случайное число и проверку на него. Verfiy проверяет выходное значение и возвращает 1 или 0 в зависимости от успешности проверки. Также, используя свойства группового действия и колец эндоморфизмов, доказывается корректность всех математических преобразований в предложенной криптографической схеме.

Выводы. Разработана VRF с использованием нового криптографического примитива в области криптографии на суперсингулярных изогениях на эллиптических кривых. Показана корректность преобразований. В дальнейшем будет доказана безопасность в более строгой манере.

Список использованных источников:

1. Micali S., Rabin M., Vadhan S. Verifiable random functions //40th annual symposium on foundations of computer science (cat. No. 99CB37039). – IEEE, 1999. – С. 120-130.
2. Azarderakhsh R. et al. Supersingular isogeny key encapsulation. Submission to the NIST Post-Quantum Standardization project, 2017.
3. Castryck W., Decru T. An efficient key recovery attack on SIDH //Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Cham : Springer Nature Switzerland, 2023. – С. 423-447..
4. Moriya T. IS-CUBE: An isogeny-based compact KEM using a boxed SIDH diagram //Cryptology ePrint Archive. – 2023.