УДК 004.056.55

Односторонняя функция для генерации псевдослучайных подстановок, применимая в криптосистемах на основе корректирующих кодов

Ниткин И.С. (ИТМО)

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

Введение.

Постквантовая криптография изучает криптографические схемы устойчивые к атакам с использованием квантового компьютера [1]. Криптография на основе корректирующих кодов является одним из востребованных направлений постквантовой криптографии [2]. Преимуществом построения криптографических схем на кода является возможность использования NP-полной задачи синдромного декодирования произвольного линейного кода в спектре весов [3] в качестве основы для обоснования стойкости. При этом основным недостатком является избыточность хранения и генерации длинных подстановок, ограничивающая практическую применимость криптосистем на основе корректирующих кодов [4]. Для решения задачи функциональной оптимизации криптографических схем на основе корректирующих кодов может быть разработана односторонняя функция, которая принимает в качестве аргумента числовое значение, результатом которой является подстановка заданной длины. При этом такая функция должна обладать рядом свойств криптографических хеш-функций.

Основная часть.

В рамках исследования определен набор свойств вышеописанной односторонней функции, в том числе лавинный эффект, необратимость. На основе набора требуемых свойств разработана методика оценки криптографических свойств для односторонней функции, которая принимает в качестве аргумента числовое значение, результатом которой является подстановка заданной длины.

Рассмотрены основные процедуры, на основе которых может быть построена такая функция, в том числе алгоритмы нумерации подстановки, процедура мутации подстановки – преобразование, в рамках которого подстановка выступает одновременно и функцией, и аргументом для преобразования.

На основе разработанной методики определено оптимальное сочетание и последовательность преобразований, которые позволяют построить одностороннюю функцию, обладающую необходимыми свойствами.

Проведена оценка производительности такой хэш-функции.

Заключение.

Таким образом, в рамках проведенного исследования предложены критерии для оценки криптографических свойств для односторонних функций, которые принимают в качестве аргумента числовое значение, результатом которых является подстановка заданной длины. На основе заданных критериев, спроектирована такая функция на основе алгоритмов нумерации и процедуры мутации подстановки.

Список использованных источников:

1. The state of the art in integer factoring and breaking public-key cryptography / F. Boudot, P. Gaudry, A. Guillevic [и др.] // IEEE Security & Privacy. — 2022. — Vol. 20, № 2. — P. 80–86. — DOI: 10.1109/MSEC.2022.3141512.

2. Weger, V. A Survey on Code-Based Cryptography / V. Weger, N. Gassner, J. Rosenthal. — 2022. – URL: https://arxiv.org/pdf/2201.07119 (дата обращения: 01.06.2025). – DOI: 10.48550/arXiv.2201.07119.

3. Chailloux, A. On the (in)security of optimized Stern-like signature schemes / A. Chailloux, S. Etinski // Designs, Codes and Cryptography. – 2024. – № 92. – P. 803–832. – DOI: 10.1007/s10623-023-01329-y.

4. Ниткин, И. С. Применение метода компактного описания подстановки для модификации схемы цифровой подписи на основе протокола аутентификации Штерна / И. С. Ниткин // Информационно-управляющие системы. – 2025. – № 1. – С. 48–56. – DOI: 10.31799/1684-8853-2025-1-48-56.