УДК 111.11

ПРИМЕНЕНИЕ КЛАССИЧЕСКИХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ДЛЯ ПЕРЕДАЧИ ИНФОРМАЦИИ МЕТОДОМ ФАНТОМНОЙ ВИЗУАЛИЗАЦИИ

Хорсова И.В. (ИТМО)**, Исмагилов А.О.** (ИТМО)**, Шумигай В.С.** (ИТМО)
Научный руководитель – д.ф.-м.н., руководитель лаборатории фемтосекундной оптики и фемтотехнологий и лаборатории квантовых процессов и измерений Цыпкин А.Н. (ИТМО)

Введение. Фантомная визуализация – технология, которая позволяет получать информацию об объекте в условиях зашумлённого канала при использовании небольшой интенсивности излучения. Одна из её перспективных областей применения – это передача информации. Благодаря большому количеству паттернов (случайных распределений световой интенсивности), пропускаемых через объект, при использовании алгоритмов шифрования можно значительно расширить пространство используемых ключей. Таким образом Алиса с Бобом могут обмениваться данными по открытому пространству с криптостойкостью превосходящей ныне используемые цифровые методы. А алгоритмы, применяемые в работе, позволяют генерировать ключ, используя исключительно открытые каналы связи [1].

Основная часть. В процессе математического моделирования исследования решаются следующие задачи:

1) Подбор оптимальных параметров алгоритмов шифрования на эллиптических кривых [2] и RSA [3] и задающейся фазовой маски для создания паттернов пропускания.
2) Создание алгоритма сжатия паттернов, учитывающего квантовую природу света и позволяющего уменьшить количество накладываемого шума при передаче в зашумлённом канале.
3) Сравнение скорости передачи и затрачиваемой битовой ёмкости при использовании генерации ключа на эллиптических кривых и RSA для выявления более рационального алгоритма в технологии фантомной визуализации.

Основными результатами являются:

1) Кривые графика коэффициентов корреляции между объектом, восстановленным с помощью исходных паттернов, и объектом, восстановленным с использованием паттернов, переданных через зашумлённый канал. Всего три кривые, отображающие коэффициенты корреляции, полученных объектов с разным типом передачи спеклов: без кодировки; с кодировкой на основе ключа, созданного с помощью алгоритма RSA; с кодировкой на основе эллиптических кривых.
2) Значения информационной ёмкости, затрачиваемые на передачу единицы информации методом фантомной визуализации.

Выводы. Создана программа для кодирования и декодирования набора паттернов; создан алгоритм, позволяющий уменьшить аддитивный накладываемый шум математическими методами; выявлен криптографический алгоритм, затрачивающий меньшую информационную ёмкость.

Список использованных источников:

1. Z. Pan, L. Zhang. Optical Cryptography-Based Temporal Ghost Imaging With Chaotic Laser // IEEE Photonics Technology Letters. – 2017.
2. S. Ullah, J. Zheng, N. Din, M.T. Hussain, F. Ullah, M. Yousaf. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey // Computer Science Review. – 2023.
3. N.V. Kondratyonok. Analysis of the RSA-cryptosystem in abstract number rings // Journal of the Belarusian State University. Mathematics and Informatics. – 2020. – С. 13–21.