УДК 681.3.067

ПРИМЕНЕНИЕ ПРИНЦИПА TDD ДЛЯ МОДЕЛИРОВАНИЯ СВОЙСТВ ХЭШ-ФУНКЦИЙ С КОРРЕКЦИЕЙ ОШИБОК

Русанов А. А., Дольнов Д. Ю., Лесин В. С.
Научный руководитель: профессор, Бибиков С. В.
Университет ИТМО, Санкт-Петербург

В настоящее время ведутся активные исследования в области квантовой криптографии, в частности, об аппаратной реализации устройств, принцип действия которых основан на законах квантового взаимодействия.

Одним из направлений разработки в данной области является создание и тестирование хэш-функций с коррекцией ошибок.

Цель работы: разработка методики поиска и коррекции ошибок с использованием принципов TDD и генератора помех в качестве тестирующего модуля.

На текущий момент существует две основные техники написания программ, одной из которых является TDD. Test Driven Development (TDD) – неоспоримо выдающаяся техника, дающая ряд преимуществ. Алгоритм TDD включает в себя три основных этапа: Создание теста, затем написание программного кода под данный тест и при успешном прохождении теста выпуск конечной версии программы.

Моделирование свойств хэш-функций с коррекцией ошибок с применением принципа TDD предполагает создание генератора помех для использования его в качестве тестирующего модуля, написание программы для коррекции ошибок в хэш-функциях, её тестирования на предмет выявления ошибок во входящих данных, измененных с помощью генератора помех и последующей их коррекции.

В ходе нашей работы были разработаны требования для генератора помех и методика поиска и коррекции ошибок хэш-функций с использованием принципов TDD.