Методы построения коллизий функций хеширования

Марчук Вадим Владимирович

Научный руководитель: Бурделёв Александр Владимирович

Кафедра математического моделирования и анализа данных, специальность компьютерная безопасность

33 страницы, 14 иллюстраций, 7 источников

Ключевые слова: хеш-функция, MD5, коллизия, метод модификации сообщений, туннель, туннелирование, IHV, X.509

Цель работы: исследовать и реализовать существующие методы построения коллизий.

Реализован метод туннелирования построения коллизий второго рода MD5; с помощью метода туннелирования построены два сообщения с детерминированными префиксами, вступающие в коллизию; для законно выпущенного X.509 сертификата сгенерирован поддельный X.509 сертификат с корректной электронной цифровой подписью.