АНАЛИЗ ХЭШ-ФУНКЦИЙ НА ОСНОВЕ СЛУЧАЙНЫХ РЯДОВ

С.Б. САЛОМАТИН, И.О. МОРОЗОВ

Целью данного исследования является моделирование и выявление взаимосвязей, называемых каузальными, между различными хеш-функциями представленными в виде временных рядов. Для исследования были выбраны самые распространенные на данный момент хеш-функции: MD5, SHA-1 и SHA-256.

Поиск каузальных связей использовал базовый тест Грейнджера, который определил, что между дайджестами одной хеш-функции существует причинная зависимость после шестого порядка с 96 процентной вероятностью.

Анализ пошаговой регрессии показал, что среди дайджестов алгоритма MD5 существуют каузальные зависимости, которые в дальнейшем могут быть использованы для выявления коллизий. Алгоритмы SHA-1 и SHA-256 показали высокую криптостойкость.

Оптимальный каузальный метод дает оценки на основе анализа матрицы дистанций, а также поиска кратчайшего пути в направленном графе и оптимального пути конечной температуры. Данный метод оказался нечувствителен к связи дайджестов алгоритма MD5. Среди дайджестов SHA-1 метод нашел стабильные связи. Наибольшее количество взаимосвязей было найдено у дайджестов алгоритма SHA-256. В основном перевешивают связи в прямом направлении.

Регрессия метода опорных векторов показала, что данный метод позволяет точно восстановить исходную последовательность данных.