

Распознавание криптографических генераторов на основе условно-авторегрессионных моделей.

Скормахович В.А., студент 5го курса ФПМИ БГУ

Харин Ю. С., зав. кафедрой математического моделирования и анализа данных ФПМИ, доктор физико-математических наук, профессор, член-корреспондент НАН Беларуси

Кафедра математических методов анализа данных, компьютерная безопасность, <специализация>

Дипломная работа, 54с., 4 рис., 3 таблицы, 11 источников.

Ключевые слова: условно-авторегрессионная модель, метод максимального правдоподобия, итерационный метод, локальная аппроксимация, кластерный анализ.

Цель – разработка алгоритма и программного комплекса распознавания криптографических генераторов по их выходным последовательностям на основе условно-авторегрессионной модели.

В данной работе получены следующие основные результаты:

1. Разработан алгоритмы оценки параметров моделей $CAR(s)$, $CAR(s, r)$.
2. Проведено теоретическое и компьютерное исследование свойств полученных оценок, сложности алгоритмов.
3. Разработан алгоритм распознавания для $L \geq 2$ классов генераторов в пространстве коэффициентов модели $CAR(s, r)$.
4. Разработан программный комплекс для имитации двоичных последовательностей, соответствующих моделям $CAR(s)$, $CAR(s, r)$, оценивания параметров моделей $CAR(s)$, $CAR(s, r)$, распознавания выходных последовательностей криптографических генераторов.