ПОСТРОЕНИЕ СТОЙКИХ К ЧАСТОТНОМУ АНАЛИЗУ КРИПТОСИСТЕМ НА ОСНОВЕ АФФИННОГО ОТОБРАЖЕНИЯ ЛИНЕЙНЫХ ПРОСТРАНСТВ НАД КОНЕЧНЫМИ ПОЛЯМИ

Амербаев В.М., Корнеева М.В.

Московский институт электронной техники (Технический университет)

Проблемы защиты информации на современном уровне развития информационных технологий, благодаря существенному скачку в развитии современных вычислительных ресурсов, стимулировали в сфере творческого поиска новых шифр-систем смещение парадигм от разработок абсолютно стойких (К. Шеннон [1]) к построению вычислительно стойких шифров (У. Диффи, М. Хелман [2]). При этом для симметричных систем шифрации, главным образом в «гражданской криптографии», на первый план выступили простота реализации криптографического преобразования и рандомизированная управляемость ключевым материалом, благодаря чему достигается стойкость к частотному криптоанализу. Так возникли парадигмы: управляемых подстановок (А.А. Молдавен, Н.А. Молдавен и др. [3]), управляемых бинарных отношений (В.Г. Скобелев, Е.В. Тыкулов и др. [4,5]), управляемого детерминированного хаоса.

Идея введения параметра управления в криптографические преобразования возникла еще в дошенноновский период развития криптографии (1929 г.) и принадлежит она Л. Хиллу [6, 7].

В докладе рассматривается шифр-система Л. Хилла (матричная система по Шеннону), определяемая аффинным отображением линейного пространства F^n на себя F^n: $a \mapsto K_t a + b_t = c_t$, где F - конечное поле, a – сообщение ($a \in F^n$), t – дискретный управляемый параметр, K_t, b_t, соответственно, ключевая матрица размерности $n \times n$ и ключевой вектор размерности n, c_t - криптограмма.

Основное внимание в докладе уделено: эффективным методам порождения невырожденных случайных квадратных матриц K_t и эффективным методам их обращения; изучению различных типов матриц K_t, имеющим удобную форму для вычислительной реализации; введению избыточности в шифрограммы для обеспечения свойств самокоррекции криптографического преобразования и шумового сокрытия криптограмм [8].

Рассмотрены различные формы итерации, включающие случайные управляемые подстановки. Приведены результаты численного эксперимента. Даны оценки хаотичности (дробная размерность), показатель Херста.

Литература

1. Shannon C. Communication theory of secret systems, Bell System Tech., J., 28, N 4 (1949) p. 656-715.
2. Диффи У., Хеллман М., Защищенность и имитостойкость. Введение в криптографию., ТИИЭР, 1979, т.67, N 3.
3. Молдавян А.А., Молдавян Н.А. и др., Криптография. Скоростные шифры СПб. БХВ –Петербург. 2002.
4. Скобелев В.В., Построение стойких частотному анализу криптосистем на основе регулярных комбинаторных структур. Ж. Искусственный интеллект. 2004, N 1.
5. Тыкулов Е.В., Построение нестационарных поточных криптосистем на основе автоматных моделей. Ж. Искусственный интеллект. 2004, N 1
6. Hill L.S., Concerning certain liner transformation apparatus of cryptography, Amer. Math. Monthly, 38(1931), N 1, p.135-154.
7. Hill L.S., Cryptography in algebraic alphabet, Amer. Math. Monthly, 36(1929), N 6, p.306-312.
8. Блейхут Р., Теория и практика кодов, контролирующих ошибки, М., Мир, 1986.