АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА RIJNDAEL В РАМКАХ ТЕОРИИ ДЕКОРРЕЛЯЦИИ

Танько С.В., Ермаков А.С., Федоров А.В.
Научный руководитель: Федоров А.В.
Харьковский национальный университет радиоэлектроники, Украина
E-mail: andryerm@mail.ru

Аннотация — Работа посвящена вопросам оценки информационной безопасности алгоритма *Rijndael* в рамках теории декорреляции. С позиций этой теории шифр должен являться так называемым декорреляционным модулем, эффективно блокирующим распространение линейных и дифференциальных характеристик

1. Введение

Rijndael (*AES*) — это симметричный блочный *SPN* шифр с размером блока 128 битов и использующий ключи шифрования длиной 128, 192 и 256 битов [1]. Блоки в алгоритме *Rijndael* представляют собой матрицы байтов размера 4×4. *AES* включает в себя четыре преобразования: *SubBytes, ShiftRows, MixColumns* и *AddRoundKey*. *SubBytes* — нелинейная подстановка байт, которая преобразует каждый байт состояния независимо. *ShiftRows* оперирует с каждой из последних трех строк состояния отдельно, циклично переставляя байты в строке. *MixColumns* осуществляет перемешивание данных в столбцах состояния. *AddRoundKey* прибавляет раундовый ключ к состоянию с помощью побитовой операции *XOR*. Шифр *Rijndael* проектировался так, чтобы быть устойчивым к линейному и дифференциальному криптоанализу. Целью данной работы является оценка информационной безопасности алгоритма *Rijndael* с позиций теории декорреляции.

2. Основная часть

Приведем основные положения теории декорреляции [2]. Будем рассматривать шифры как случайные перестановки C в пространстве сообщений $M=\{0,1\}^m, m=8$. Пусть $M=M_1\cup M_2$, F — случайная функция из данного пространства M_1 в M_2 и d — целое число. Определим d-мерную матрицу распределения $[F]^d$ функции F как $M_1^d\times M_2^d$-матрицу, где точка (x,y) матрицы $[F]^d$ соответствует мультиточкам $x=(x_1,\ldots,x_2)\in M_1^d$ и $y=(y_1,\ldots,y_2)\in M_2^d$ и определяется как вероятность $F(x_i)=y_i$ для $i=\overline{1,d}$, т.е. $[F]^d_{x,y}=\Pr[x\to y]$. Очевидно, что d-мерная матрица распределения $[F]^d$ случайной функции определяет ее декорреляцию, которую можно сравнивать с так называемой идеальной декорреляцией, соответствующей перестановке C^* с равномерным распределением. Две случайные функции имеют одинаковую d-мерную декорреляцию в случае когда их d-мерные матрицы распределения совпадают. Для количественного сравнения декорреляций используется следующий метод. Пусть даны две случайные функции F и G из данного пространства M_1 в M_2, целое число d и расстояние D над матричным пространством $R^{M_1^d\times M_2^d}$. Определяем $D([F]^d,[G]^d)$ как d-мерное D-расстояние декорреляции между F и G. Если G - это идеальная версия F, то она называется $D([F]^d,[G]^d)$ d-мерным D-расстоянием декорреляции функции F. В качестве расстояния D обычно используются различные матричные нормы в L_2

$$\|A\|_2=\sqrt{\sum_{x,y}(A_{x,y})^2},\quad N_\infty(A)=\max_{x,y}\frac{|A_{x,y}|}{\Pr[x\xrightarrow{C^*}y]},\quad (1)$$

где $A=[C]^d-[C^*]^d$, C^* — идеальный шифр. В формуле $N_\infty(A)$ предполагается, что $0/0=0$ и $c/0$ не определено для $c\neq0$, $\Pr[x\xrightarrow{C^*}y]$ = $[F]^d_{x,y}$ (точки матрицы распределения).

В работе выполнен расчет расстояния декорреляции для $d=1,2$ по формулам (1) относительно преобразований *SubBytes* и *MixColumns*. Кроме того, было выполнено исследование равномерности байтов в шифртексте алгоритма *Rijndael*. Для этого в СКМ Maxima создана программная модель шифра. С помощью указанной модели для одного и того же входного блока на различных случайных ключах получены блоки шифртекста. Затем для каждой пары блоков шифртекста вычислялась величина $\sqrt{\frac{1}{16}\sum_{i,j=1}^{4}(x_{i,j}-y_{i,j})^2}$. По полученным значениям строилась гистограмма, которая сравнивалась с аналогичной гистограммой построенной для гаммы шифрующей поточного шифра RC4. В эксперименте использовалось 200 различных ключей, что соответствует объему выборки равному 19900.

3. Заключение

По результатам сравнения гистограмм сделан вывод, что шифртекст, формируемый алгоритмом *Rijndael,* имеет распределение близкое к равномерному.

4. Список литературы

[1] AES standard / NIST. — http://www.nist.gov. — 20.02.2013.
[2] Vaudenay S. Decorrelation: a theory for block cipher security / S. Vaudenay // Journal of Cryptography. — 2003. — Vol 16. — P. 1 — 28.

THE RIJNDAEL CIPHER INFORMATION SECURITY ANALYSIS WITHIN A DECORRELATION THEORY

Tanko S.V., Yermakov A.S., Fedorov A.V.
Scientific adviser: Fedorov A.V.
Kharkov National University of Radioelectronics, Ukraine

Abstract — The work is devoted to the Rijndael cipher information security estimating within a Decorrelation Theory. In accordance with this theory, a cipher should be a so-called decorrelation module that efficiently prevents linear and differential characteristics propagation.