УДК 681.3

ДИСТАНЦИОННЫЕ СВОЙСТВА НЕЛИНЕЙНОГО ПОМЕХОУСТОЙЧИВОГО КОДА НА БАЗЕ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА RIJNDAEL

Д.М. БИЛЬДЮК, С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 24 июля 2012

Рассматривается нелинейный помехоустойчивый код на базе алгоритма криптографического преобразования данных Rijndael. Приведены сравнения дистанционных свойств Rijndael-кода в режимах поточного и блочного шифрования с границами помехоустойчивых кодов.

Ключевые слова: криптографическое преобразование данных, помехоустойчивое кодирование, алгоритм Rijndael, AES, границы помехоустойчивого кодирования, нелинейный код.

Введение

Защита информации от преднамеренных и случайных воздействий требует применения, как криптографических систем, так и методов помехоустойчивого кодирования.

Использование линейных кодов для создания систем защиты информации с открытым ключом привела к криптографическим структурам МакЭлиса и Нидеррайтера [1]. Основным недостатком таких механизмов защиты считается использование кодовых структур большого размера.

В этой связи представляет интерес исследование возможностей стандартных криптографических систем исправлять случайные ошибки, возникающие в каналах передачи информации.

В современных системах защиты информации наиболее востребованной является криптографическая система AES (Rijndael) [2]. Для такого типа систем характерно представление шифруемого блока данных в виде двумерного массива. Алгоритм Rijndael преобразует информацию в сбалансированную, нелинейную булеву функцию и с точки зрения теории кодирования может рассматриваться как нелинейный сбалансированный блочный код с крайне низкой вероятностью повторения выходных кодовых слов.

Для оценки корректирующей способности кода важно определить его дистанционные характеристики (минимальное расстояние Хэмминга – $d_{\min}$) данного кода и позиционирование таких характеристик относительно граничных соотношений.

Нелинейный корректирующий код

Пусть q-ичный алфавит A это конечное множество, а множество $A^n = A \times A \times \ldots \times A$ является оснащенным с метрикой Хэмминга: расстояние $d(\mathbf{a},\mathbf{b})$ определяется как число координат, в которых векторы $\mathbf{a}=(a_1,\ldots,a_n)$ и $\mathbf{b}=(b_1,\ldots,b_n)$ различаются, т.е. $d(\mathbf{a},\mathbf{b}) = \left|\{i \mid a_i \neq b_i\}\right|$.

Непустое подмножество $C \subseteq A^n$ назовем q-ичным кодом длины n с минимальным кодовым расстоянием $d_{\min} = \min\{d(\mathbf{a},\mathbf{b} \in C, \mathbf{a} \neq \mathbf{b}\}$.

Код с такими параметрами называется $(n,k,d_{\min})_q$ кодом. Элементы C называются кодовыми векторами или кодовыми словами, их компоненты – координатами.

Криптографический блочный шифр (или код) C можно определить как обратимую функцию $g: K \times B \to C$, которая отображает ключ множества K и блок множества B в блок C фиксированной длины. Уровень трудности решения обратной задачи $\bar{g}: K \to map(B, C)$, определяет степень защищенности.

В теории кодирования и криптологии используются различные границы существования кодовых структур. Одной из таких границ является асимптотическая форма линейного программирования, известная как граница Варшамова-Гильберта для бинарного $(n, k, d_{\min})$ корректирующего кода [3]. Граница Варшамова-Гильберта гарантирует существование кодов с максимальным $d_{\min}$:

$$1 - H_2\left(\frac{d_{\min}}{n}\right) \le \frac{k}{n} \le \min_{0 \le x \le 1 - \frac{d_{\min}}{n}} \left(1 + G\left(x^2\right) - G\left(x^2 + 2\frac{d_{\min}}{n}x + 2\frac{d_{\min}}{n}\right)\right),$$

где $H_2(p) \overset{\Delta}{=} -p\log_2(p) - (1-p)\log_2(1-p)$, $G(y) \overset{\Delta}{=} H_2\left(\frac{1-\sqrt{1-y}}{2}\right)$.

Граница справедлива для всех видов бинарных кодов, включая нелинейные коды, а также позволяет оценить минимальное кодовое расстояние для наилучших случайных кодов.

В теории криптологии считается, что шифры, удовлетворяющие границе Варшамова-Гильберта, устойчивы против линейного криптоанализа [4].

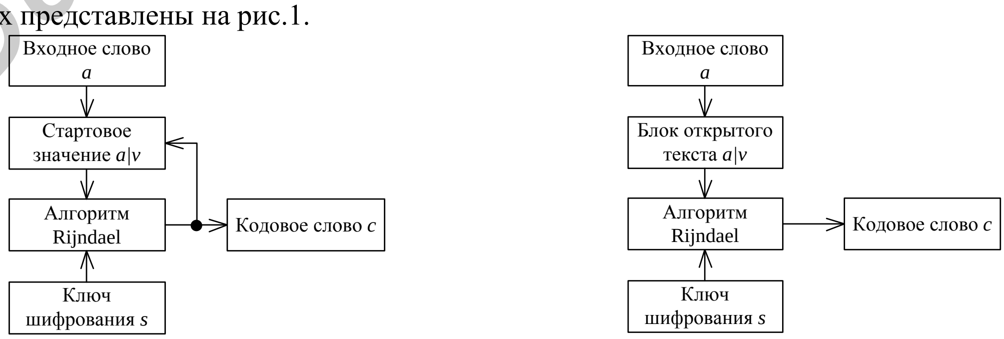
Схема кодирования информации и оценка дистанционных свойств

Шифр Rijndael можно рассматривать как бинарный код, который формируется с помощью 14 раундов шифрования 128-битного информационного сообщения. С точки зрения теории кодирования шифр Rijndael можно ассоциировать (128, k) корректирующий нелинейный код. При этом важными параметрами Rijndael-кода (далее R-код) являются минимальное кодовое расстояние и минимальный вес кодовых слов.

Блочные режимы шифрования алгоритма Rijndael формируют на выходе сбалансированное по весу кодовое слово c длины n, однако последнее имеет фиксированную длину – 128, 192 или 256 бит. Входными параметрами кодирования в таких режимах является входное слово a длины k и ключ шифрования s длины 128, 192 или 256 бит. Для помехоустойчивых кодов справедливо неравенство $n > k$ – это значит, что для формирования шифруемого блока открытого текста необходимо дополнить входное слово до длины n. Формирование открытого текста реализуется конкатенацией входного слова a и избыточности v длины $r=n–k$. Избыточность также можно считать частью расширенного ключа $sv=s|v$ – это увеличит количество возможных R-кодов для заданных параметров (n, k), а также позволит вести обнаружение ошибок при декодировании (поскольку структура открытого текста будет априори известна – $a|v$).

Для построения R-кодов произвольной длины n удобно использовать Rijndael в поточном режиме (с обратной связью). Входные параметры в таком режиме те же, что и в блочном, однако блок открытого текста используется в качестве стартового значения.

Функциональные схемы кодеров на основе алгоритма R-кода в поточном и блочном режимах представлены на рис.1.



а *б*

Рис. 1. Кодер на основе алгоритма R-кода в поточном (*а*) и блочном (*б*) режимах

Для заданных параметров кода (n, k) источником формируется $M = 2^k$ входных слов которые, с использованием R-кодера, отображаются в кодовые слова. Минимальное расстояние Хэмминга $d_{\min}$ определяется по множеству расстояний между всеми парами кодовых слов. Переборный алгоритм вычисления $d_{\min}$ выбирает самое минимальное расстояние из $\left(2^{2k-1} + 2^{k-1}\right)$ таких паросочетаний.

Для формирования множества R-кодов (и вычисления множества их $d_{\min}$) используем комбинаторный метод для заданных диапазонов n и k, предполагающий перебор всех возможных пар (n, k) при условии $n > k$. Будем характеризовать каждый такой эксперимент четырьмя параметрами – ($n_{\min}, k_{\min}, n_{\max}, k_{\max}$), где диапазоны $n_{\min} \ldots n_{\max}$ и $k_{\min} \ldots k_{\max}$ определяют возможные значения n и k. Тогда мощность множества R-кодов определяются формулой:

$$W = \sum_{i=n_{\min}}^{n_{\max}} \sum_{j=k_{\min}}^{k_{\max}} \begin{cases} 1, & i < j \\ 0, & j \ge i \end{cases}.$$

Сравнение дистанционных свойств *R*-кода в режиме поточного шифрования с границами помехоустойчивых кодов

Результаты (2, 1, 256, 14)-эксперимента для R-кодов в режиме поточного шифрования представлены на рис. 2.

Исходя из результатов эксперимента, основная масса наилучших R-кодов в режиме поточного шифрования, лежащих выше (по параметру $d_{\min}$) границы Варшамова-Гилберта, – низкоскоростные коды со скоростью $k/n < 0{,}2$. R-коды со скоростью $k/n \ge 0{,}2$, лежащие выше границы Варшамова-Гилберта, являются кодами малой длины с $n < 4$, а R-коды, достигающие границы Синглтона и выше, также коды малой длины с параметрами кодов с повторением вида (n, 1).

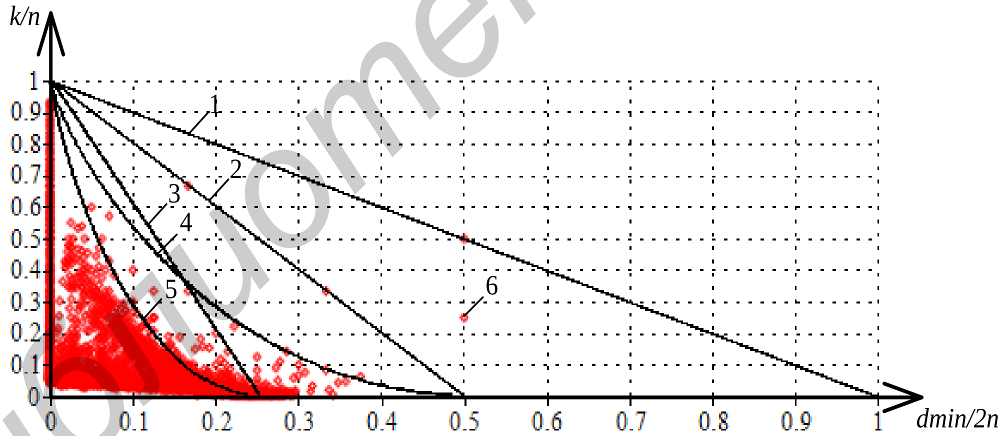
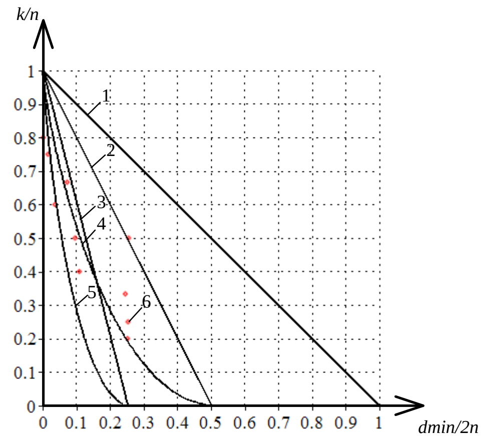


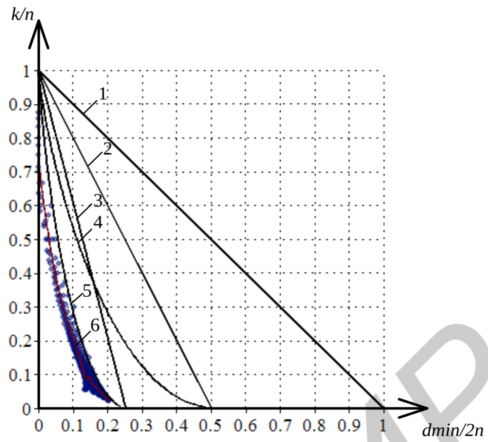
Рис. 2. Зависимость скорости k/n от $d_{\min}/2n$ R-кода в режиме поточного шифрования с параметрами (n, k) в сравнении с границами помехоустойчивых кодов:
1 – граница корректирующей способности помехоустойчивых кодов; 2 – граница Синглтона;
3 – граница Плоткина; 4 – граница Хэмминга; 5 – граница Варшамова-Гилберта;
6 – координата (k/n, $d_{\min}/2n$) R-кода с параметрами (n, k, $d_{\min}$)

Для уточнения полученных результатов проведены два эксперимента, усредненных по $d_{\min}$ на 100 реализациях: (2, 1, 5, 4)-эксперимент и (5, 3, 256, 14)-эксперимент. Результаты экспериментов приведены на рис. 3.

Результаты, представленные на рис. 3, показывают, что основная масса R-кодов в режиме поточного шифрования длины $n > 4$, лежащих в районе границы Варшамова-Гилберта, имеет скорость $k/n < 0{,}2$ (см. рис. 4, *б*), а коды с большей скоростью, лежащие за указанной границей, имеют длину $n \le 4$ (см. рис. 4, *а*).



а

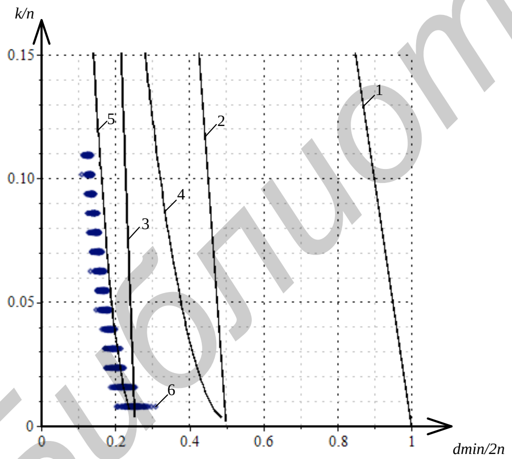


б

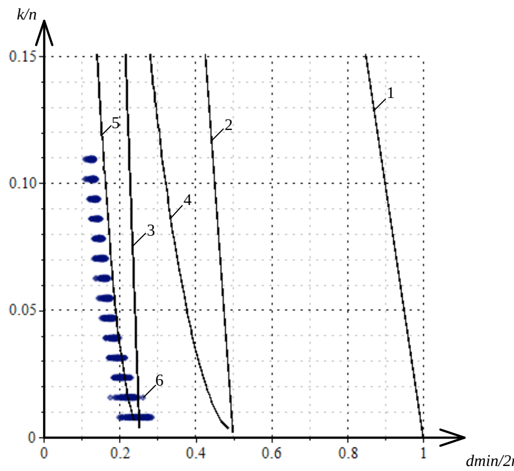
Рис. 3. Зависимость скорости k/n от $d_{\min}/2n$ *R*-кода в режиме поточного шифрования усредненная по $d_{\min}$ на 100 реализациях:
а – (2, 1, 5, 4)-эксперимент; *б* –(5, 3, 256, 14)-эксперимент:
1 – граница корректирующей способности помехоустойчивых кодов; 2 – граница Синглтона;
3 – граница Плоткина; 4 – граница Хэмминга; 5 – граница Варшамова-Гилберта;
6 – координата (k/n , $d_{\min}/2n$) *R*-кода с параметрами (*n*, *k*, $d_{\min}$) усредненная по минимальному расстоянию на 100 реализациях.

Сравнение дистанционных свойств *R*-кода в режиме поточного шифрования с дистанционными свойствами *R*-кода в режиме блочного шифрования

Поскольку длина *R*-кода в режиме блочного шифрования фиксирована (128, 192 или 256 бит) – сравнение с *R*-кодом в режиме поточного шифрования необходимо произвести на фиксированной длине. На рис.4 представлены результаты (128, 1, 128, 14)-экспериментов для *R*-кодов в поточном и блочном режимах шифрования.



а



б

Рисунок 4 – Зависимость скорости k/n от $d_{\min}/2n$ R-кода с параметрами (*n*, *k*) в сравнении с границами помехоустойчивых кодов в режимах:
а – поточного шифрования; *б* – блочного шифрования:
1 – граница корректирующей способности помехоустойчивых кодов; 2 – граница Синглтона;
3 – граница Плоткина; 4 – граница Хэмминга; 5 – граница Варшамова-Гилберта;
6 – координата (k/n , $d_{\min}/2n$) *R*-кода с параметрами (*n*, *k*, $d_{\min}$).

Как видно из результатов эксперимента, дистанционные свойства блочных и поточных режимов *R*-кода идентичны, что делает поточный режим более приемлемым – последний может иметь произвольную длину кода.

Использование *R*-кодов в системах защиты информации

Существование *R*-кодов с дистанционными свойствами в районе границы Варшамова-Гилберта делает возможным их с пользование для повышения помехоустойчивости системы передачи информации. Декодер может быть построен на основе принципа максимального правдоподобия с последующим расшифрованием кодового слова. Из рис.2 видно, что дистанционные свойства *R*-кодов уступают большинству известных помехоустойчивых кодовых конструкций, однако обладают дополнительными криптографическими свойствами. Данные свойства позволяют организовать систему защиты информации, в которой коррекцию ошибок может осуществлять только приемная сторона обладающая общим секретом (ключом) с передающей стороной. Известно, что кратность исправляемых помехоустойчивым кодом ошибок $t = \lfloor (d_{\min} - 1)/2 \rfloor$. Другим возможным вариантом использования *R*-кодов является система с каналом без помех, в которой случайные ошибки кратностью не выше t вносит передающая сторона. Тогда возможный криптоаналитик, решающий обратную криптографическую задачу, вынужден учитывать и возможные варианты случайной ошибки. В случае атаки переборными методами по всему множеству двоичного ключевого пространства количество вариантов увеличивается на величину 2^t. Более того, без знания ключа криптоаналитик не распологает информацией о минимальном расстоянии используемого кода и вынужден вести атаку по наилучшему представителю *R*-кода с заданными параметрами (n, k). Также возможны комбинированные варианты систем защиты информации со случайными преднамеренными и непреднамеренными ошибками в канале передачи информации.

Заключение

На основании поставленных экспериментов можно рекомендовать использование низкоскоростных *R*-кодов в режиме поточного шифрования (со скоростью $k/n < 0{,}2$) в качестве помехоустойчивых нелинейных кодов. Например, существует *R*-код с параметрами (179, 4, 78). По сравнению с кодами Рида-Соломона, лежащими на границе Синглтона, наилучшие *R*-коды имеют примерно в два раза меньшее минимальное расстояние Хэмминга, однако позволяют повысить сложность решения обратной задачи криптоаналитиком с 2^{256} до 2^{256+t}, при атаке методом грубой силы (прямого перебора ключей) на *R*-код с 256-битным ключом шифрования (величина 2^{256+t} учитывает возможные случайные или преднамеренные ошибки, происходящие в канале).

DISTANCE PROPERTIES OF THE NONLINEAR ERROR CONTROL CODE ON THE BASIS OF CRYPTOGRAPHIC ALGORITHM OF RIJNDAEL

D.M. BILDZIUK, S.B. SALOMATIN

Abstract

The nonlinear error control code on the basis of cryptographic transformation of data through Rijndael algorithm is considered. Hamming distance properties of a Rijndael-code in thread and block modes enciphering with borders of error control codes are compare.

Список литературы

1. *McEliece R.J.* // A public-key cryptosystem based on algebraic coding theory. DNS Progress Reports 42-44, NASA Jet Propulsion Laboratory, Pasadena, Calif., USA, 1978.
2. Specification for the ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, November 26, 2001.
3. *MacWilliams F.J., Sloane N.J.A.* // The Theory of Error- Correcting Codes. North-Holland. 1977.
4. *Matsui M.* //The first experimental cryptanalysis of the Data Encryption Standard, CRYPTO 94 (Springer LNCS 839).