УДК 681.3

ДЕКОДИРОВАНИЕ 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 варианты реализации декодера Rijndael-кода на основе алгоритма максимального правдоподобия и алгоритмов Чейза, а также их сравнение на основе зависимости вероятности ошибки от отношения сигнал/шум. Произведена оценка пропускной способности декодеров при параллельной и последовательной реализации алгоритмов декодирования.

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

Введение

Использование помехоустойчивых кодовых конструкций в криптографии дает основание для исследований нелинейных помехоустойчивых кодов на основе криптографических функций. Известны исследования помехоустойчивых свойств Rijndael-кода [1, 2]. Более того существуют работы связываюшие стойкость алгоритмов шифрования против линейного криптоанализа и их расположение относительно границы Варшамова-Гильберта [3].

Криптографические алгоритмы шифрования должны быть устойчивыми против известных методов криптоанализа. Стойкость к корреляционным методам криптоанализа, непредсказуемость (за полиномиальное время) значения кодового слова, крайне низкая вероятность совпадения, а также сбалансированность кодовых слов алгоритмов криптографического преобразования информации обуславливает приемлемые дистанционные свойства нелинейных кодовых конструкций на их основе [4, 5].

Однако нелинейная структура помехоустойчивых кодов на базе криптографических преобразований ведет не только к более высокой вычислительной сложности (по сравнению с линейными структурами) оценки их параметров, но и к более сложным алгоритмам декодирования. Оценка пропускной способности, требований к памяти и корректирующей способности декодеров нелинейного помехоустойчивого кода является важной с точки зрения практического использования последних. В частности, на примере декодера максимального правдоподобия (далее ДМП) помехоустойчивого кода на основе алгоритма Rijndael (далее *R*-кода) можно сделать вывод о максимальной корректирующей способности, наибольшим требованиям к памяти и наименьшей пропускной способности нелинейных декодеров в целом.

Схема формирования *R*-кода

R-кодом с параметрами $(n, k, d_{\min})_q$, определенным над алфавитом $GF(q)$, будем называть множество разрешенных кодовых слов $\{\mathbf{c}_i \mid i = 0,1,\ldots,q^k - 1\} \in GF(q^n)$, с минимальным кодовым расстоянием $d_{\min}$ в метрике Хэмминга [5]. Тогда формирование *R*-кода можно формали-

зовать как отображение некоторого пространства $GF(q^k)$ k-мерных векторов над полем $GF(q)$ $\mathbf{a}=(a_0,a_1,\ldots,a_{k-1})$ в другое пространство $GF(q^n)$ n-мерных q-ичных векторов $\mathbf{c}=(c_0,c_1,\ldots,c_{n-1})$, где $a_i,c_j\in GF(q)$ для любого $i\in\{0,\ldots,k-1\}$ и любого $j\in\{0,\ldots,n-1\}$. Если $n>k$, то *R*-код, как код, основанный на криптографической функции, трактуется как нелинейный избыточный код, корректирующие свойства которого зависят от $d_{\min}$, кодовые слова $\mathbf{c}$ которого нелинейно зависят как от входных информационных слов $\mathbf{a}$, так и от используемого ключа шифрования $\mathbf{s}=(s_0,s_1,\ldots,s_{m-1})\in GF(q^m)$. Тогда функция кодирования *R*-кода задается как векторная функция $\varphi(\mathbf{a},\mathbf{s})$:

$$\mathbf{c}=\varphi(\mathbf{a},\mathbf{s}):GF(q^k)\to GF(q^n). \qquad (1)$$

Практическая реализация функции φ осуществляется на основе алгоритма кодирования линейных кодов в спектральной области [5]:

– информационный вектор $\mathbf{a}$ преобразуется в вектор $\mathbf{a}'$ при помощи отображения:

$$\mathbf{a}'=\psi(\mathbf{a}):GF(q^k)\to GF(q^n),$$

где $\psi(\mathbf{a})=\{a_0,a_1,\ldots,a_{k-1},v_0,v_1,\ldots,v_{r-1}\}$, $\mathbf{v}=(v_0,v_1,\ldots,v_{r-1})\in GF(q^r)$ – вектор избыточности дополняющий информационный вектор до заданной длины *n*, т.е. $r=n-k$. Вектор $\mathbf{v}$ представляет собой фиксированную константу из $GF(q^r)$, которая может формироваться из нулей (как в линейных кодах), а также случайным образом – поскольку в данном случае отсутствует связь нулевых элементов с корнями полиномов на основе преобразования Фурье в поле Галуа [5]. Вектор $\mathbf{v}$ может быть как открытым, так и секретным параметром;

– кодовый вектор $\mathbf{c}$ формируется как отображение:

$$\mathbf{c}=\xi(\mathbf{a}',\mathbf{s}):GF(q^n)\to GF(q^n),$$

где функция ξ – криптографическое преобразование информации (зашифрование) при помощи алгоритма Rijndael, т.е. $\varphi(\mathbf{a},\mathbf{s})=\xi(\psi(\mathbf{a}),\mathbf{s})$.

Поскольку длина преобразуемых функцией ξ данных в режиме электронной кодовой книги фиксирована, то для формирования *R*-кодов произвольной длины *n* необходимо использовать режимы с обратной связью [4].

После кодирования вектор $\mathbf{c}$ подвергается воздействию случайных преднамеренных и непреднамеренных воздействий, приводящих к искажению его символов:

$$\mathbf{y}=\varepsilon(\mathbf{c},\mathbf{e}):GF(q^n)\to GF(q^n),$$

где $\varepsilon(\mathbf{c},\mathbf{e})=\{y_i=(c_i+e_i)\bmod q\mid i=0,\ldots,n-1\}$, $\mathbf{y}=(y_0,y_1,\ldots,y_{n-1})\in GF(q^n)$ – вектор искаженных символов, $\mathbf{e}=(e_0,e_1,\ldots,e_{n-1})\in GF(q^n)$ – вектор ошибок.

Задачей декодера является восстановление искаженных символов в векторе $\mathbf{y}$, т.е. поиск вектора ошибок $\mathbf{e}$. Максимальная кратность исправляемых кодом ошибок $t=\left\lfloor\frac{d_{\min}-1}{2}\right\rfloor$.

После того как искаженные символы исправлены, функция восстановления информационного вектора (т.е. функция, обратная к функции представленной в формуле 1) осуществляет обратное отображение:

$$\mathbf{a}=\varphi^{-1}(\mathbf{c},\mathbf{s}):GF(q^n)\to GF(q^k), \qquad (2)$$

где $\varphi^{-1}(\mathbf{c},\mathbf{s})=\psi^{-1}(\xi^{-1}(\mathbf{c},\mathbf{s}))$, ξ^{-1} – функция расшифрования алгоритма Rijndael в заданном режиме, ψ^{-1} – функция восстановления (деконкатенации) вектора $\mathbf{a}=(a_0,a_1,\ldots,a_{k-1})$ из вектора $\mathbf{a}'=(a_0,a_1,\ldots,a_{k-1},v_0,v_1,\ldots,v_{r-1})$.

Оценка декодера маскимального правдоподобия *R*-кода

Декодирование по принципу максимального правдоподобия относится к классу *NP*-полных задач и осуществляет соотнесение принятого кодового слова с ошибкой к ближайшему (в смысле метрики Хэмминга) разрешенному кодовому слову [6]. Последнее означает, что для используемого $(n,k,d_{\min})_q$-кода ДМП содержит в памяти q^k разрешенных кодовых слов $C=\{\mathbf{c}_j \mid j=0\ldots q^k-1\}$ либо вычисляет их динамически по мере необходимости, а при декодировании расчитывает столько же расстояний Хэмминга с целью поиска минимального.

Кроме скорости декодирования и занимаемой памяти существует оценка используемого кода и метода декодирования, отображаемая как зависимость вероятности ошибки, приходящейся на один бит информации от отношения сигнал/шум на входе демодулятора в канале с аддитивным белым гауссовским шумом (АБГШ) [6]. Как правило, такие оценки даются для сигналов с двоичной кодовой манипуляцией по фазе (BPSK) использованием помехоустойчивого кода и без него. На рис. 1 представлена зависимость вероятности ошибки на один бит информации P_b от отношения сигнал/шум E_b/N_0 в канале с АБГШ при использовании BPSK-модуляции (с частотой дискретизации $10f_0$ (f_0 – несущая частота), 12-ти разрядным квантованием и с размещением десяти периодов несущей частоты в одном бите) для некодированного BPSK, $(31,6,7)_2$ *R*-кода с ДМП и $(31,6,15)_2$ БЧХ-кода с декодированием на основе алгоритма Берлекемпа-Месси.

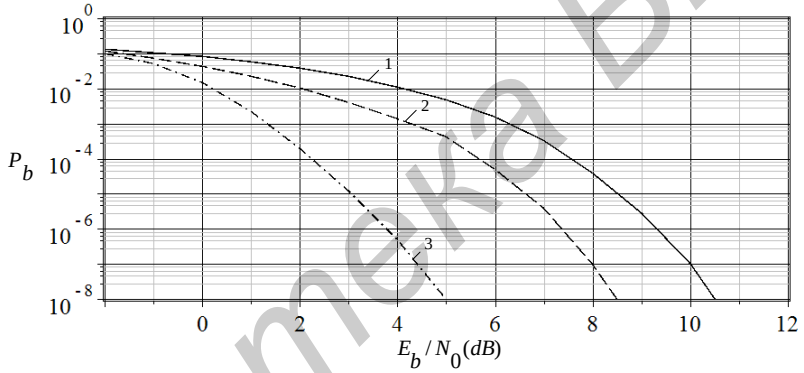

Рис. 1. Оценка характеристик кодовых конструкций в канале с АБГШ:
1 – некодированный BPSK-сигнал; 2 – $(31,6,7)_2$ Rijndael-код с ДМП; 3 – $(31,6,15)_2$ БЧХ-код с декодированием на основе алгоритма Берлекемпа-Месси

Из рисунка видно, что выигрыш *R*-кода с ДМП при вероятности ошибки $P_b=10^{-6}$ по сравнению с некодированным сигналом составляет 1 дБ, в то же время по сравнению с БЧХ-кодом при той же вероятности ошибки проигрыш составляет около 3,5 дБ. С одной стороны, проигрыш сочетается с дополнительными криптографическими свойствами помехоустойчивого *R*-кода, но с другой стороны свидетельствует о необходимости поиска методов увеличения минимального расстояния Хэмминга *R*-кода.

Быстрое декодирование *R*-кода

Декодирование по принципу максимального правдоподобия требует значительных затрат памяти и обладает высокой вычислительной сложностью [5, 6]. Особенно данная проблема актуальна для высокоскоростных *R*-кодов большой длины. Более быстрые декодеры для высокоскоростных *R*-кодов большой длины с меньшими затратами памяти могут быть построены на основе алгоритмов Чейза. Известны три типа алгоритмов Чейза для декодирования $(n,k,d_{\min})_q$-кода [6].

Тип 1. Проверяются все комбинации ошибок на расстоянии не более $(d_{\min}-1)$ от принятого слова.

Тип 2. Проверяются комбинации ошибок веса $t = \lfloor (d_{\min} - 1)/2 \rfloor$ и меньше, размещаемых на любых позициях за исключением $\lfloor d_{\min}/2 \rfloor$ наиболее надежных символов.

Тип 3. Проверяются те комбинации ошибок, для которых i ошибок размещается на i наименее надежных позициях, i нечетно, $1 \le i \le d_{\min} - 1$.

Декодеры на базе алгоритмов Чейза (далее ДЧ), в отличие от ДМП, содержат в памяти либо вычисляют не множество всех кодовых слов, а множество всех возможных ошибок по заданным критериям. Вектор ошибок считается найденным, если функция расшифрования алгоритма Rijndael преобразует текущую оценку кодового слова в вектор $\mathbf{a}'$ заданной структуры (2). Очевидно, что требования к памяти и время декодирования в ДМП и ДЧ зависят от мощности перебираемых множеств в ДМП и ДЧ, а мощность, в свою очередь, в ДМП зависит от параметра k, в ДЧ – от $d_{\min}$ (и n в типе 2). Тогда ДЧ не обязательно является более эффективным чем ДМП или наоборот. Кроме того, ДЧ на основе алгоритмов типа 2 (далее ДЧ2) и 3 требует наличия демодулятора с мягкими решениями для оценки надежности символов [6]. Более эффективным среди ДЧ считается ДЧ2 [6]. Для заданных параметров кода $(n, k, d_{\min})_q$ мощность перебираемого множества в ДМП определеятся мощностью самого кода – $M_{\text{ДМП}} = q^k$, а мощность перебираемого множества ошибок в ДЧ2 – $M_{\text{ДЧ2}} = \sum_{i=1}^{t} C_{n-t+1}^{i}$, как сумма сочетаний из общей длины наименее надежных символов ($n - \left\lfloor \frac{d_{\min}}{2} \right\rfloor = n - t + 1$) кодового слова по всем возможным ошибокам веса i, $i = 1 \ldots t$. Тогда вычислительная сложность ДЧ2, при фиксированной длине кода n, с ростом длины информационного вектора k растет за счет увеличения общей длины наименее надежных символов и одновременно убывает из-за уменьшения максимального веса исправляемых ошибок t. На рис. 2 представлены зависимости мощности перебираемых множеств R-кода от длины информационного вектора k при фиксированом $n = 34$ для ДМП и ДЧ2.

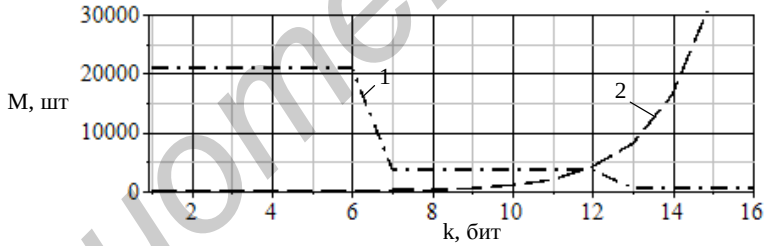

Рис. 2. Зависимость мощности перебираемых множеств R-кода от длины информационного вектора k при фиксированом $n = 34$ для ДМП и ДЧ2:
1 – мощность перебираемого множества для ДЧ2; 2 – мощность перебираемого множества для ДМП

Из рисунка видно, что ДМП более эффективен для низкоскоростных кодов, а для высокоскоростных кодов – ДЧ2. Граница эффективности для случая представленного на рис. 2 лежит в районе $k = 12$, т.е. при скорости R-кода $k / n = 0{,}353$. Указанная граница с ростом фиксированного n растет в смысле параметра k, при этом скорость кода на границе стремится к $k / n = 0{,}38$ (см. рис. 3).

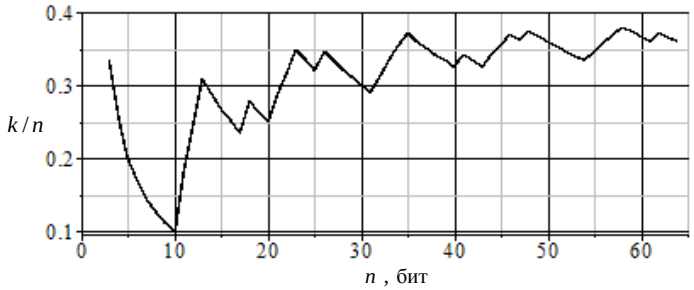

Рис. 3. Зависимость границы эффективности от длины фиксированного n

Однако оценка дистанционных свойств высокоскоростного *R*-кода, особенно при больших *n*, для современной вычислительной техники может представлять собой вычислительно сложную задачу, неразрешимую за разумное время. Тогда корректирующие свойства можно оценить, исходя из вероятности ошибки на информационный бит в зависимости от отношения сигнал/шум в кнале с АБГШ (рис. 1), ограничившись некоторой приемлемой мощностью множества возможных ошибок, начиная перебор наиболее вероятных ошибок, располагающихся на наименее надежных позициях. При такой реализации алгоритмы Чейза типа 2 и 3 заменяются одним модифицированным алгоритмом. Более того, скорость обработки кодовых слов в декодере на основе модифицированного алгоритма (далее ДЧМ) может быть выше чем в ДМП при равных мощностях $M_{\text{ДМП}}$ и $M_{\text{ДЧМ}}$, поскольку декодирование в ДЧМ может закончиться раньше, чем алгоритм декодирования переберет все возможные значения ошибок (в ДМП перебор всех кодовых слов обязателен).

На рис. 4 представлена оценка корректирующей способности высокоскоростного *R*-кода $(127,106)_2$ на основе зависимости вероятности ошибки от отношения сигнал/шум в канале с АБГШ при использовании ДЧМ с ограниченной мощностью $M'_{\text{ДЧМ}} = 2^{20}$ (условия те же, что и при формировании зависимости на рис.1), а также $(127,106,7)_2$ БЧХ-кода с декодированием на основе алгоритма Берлекемпа-Месси.

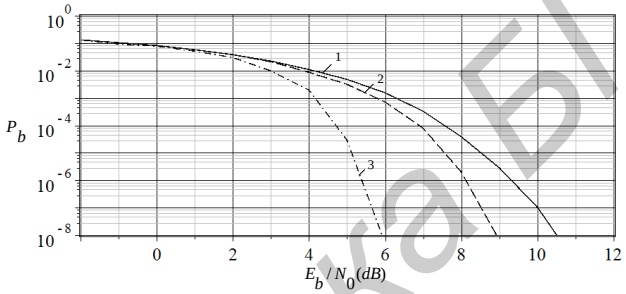

Рис. 4. Оценка корректирующей способности высокоскоростного $(127,106)_2$ *R*-кода:
1 – некодированный BPSK-сигнал; 2 – $(127,106)_2$ *R*-код с ДЧМ; 3 – $(127,106,7)_2$ БЧХ-код
с декодированием на основе алгоритма Берлекемпа-Месси

Оценка, представленная на рис. 4, показывает, что высокоскоростные *R*-коды также обладают помехоустойчивыми свойствами (при вероятности ошибки $P_b = 10^{-6}$ выигрыш по сравнению с некодированным сигналом составляет 1 дБ, в то же время по сравнению с БЧХ-кодом при той же вероятности ошибки проигрыш составляет около 2,8 дБ), а ДЧМ делает возможным коррекцию ошибок при их использовании. Также следует заметить, что вероятность ошибки при низких отношениях сигнал/шум может зависить от ограниченной мощности $M'_{\text{ДЧМ}}$, поскольку вероятность возникновения ошибок (в том числе и большой кратности) при этом будет достаточно высокой, что приведет к повышению необходимой для корректировки мощности $M_{\text{ДЧМ}} > M'_{\text{ДЧМ}}$. На рис. 5 представлена зависимость времени выполнения операции декодирования кодового слова для низкоскоростного $(127,14,33)_2$ *R*-кода (ДМП) и высокоскоростного $(127,106)_2$ *R*-кода (ДЧМ) при фиксированной мощности $M'_{\text{ДЧМ}} = 2^{14}$ от отношения сигнал/шум (условия те же, что и при формировании зависимости на рис. 1).

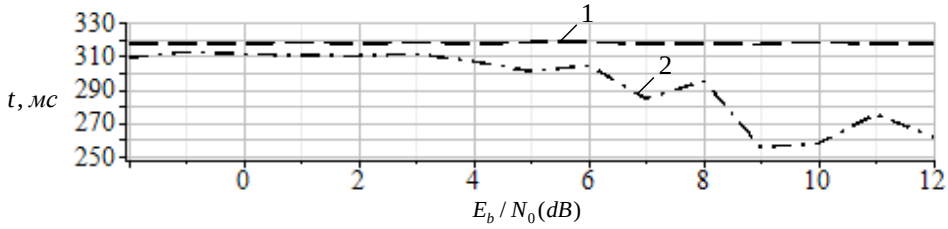

Рис. 5. Зависимость времени выполнения декодирования высокоскоростного и низкоскоростного
R-кодов от отношения сигнал/шум:
1 – декодирование с ДМП; 2 – декодирование с ДЧМ

Выводы

Полученные результаты показывают, что криптографические функции типа Rijndael могут быть использованы в качестве нелинейных помехоустойчивых кодовых конструкций. Более того, существуют методы декодирования таких конструкций. Для декодирования низкоскоростных *R*-кодов более эффективным является ДМП, а для низкоскоростных – ДЧ2.
Рассмотренные *R*-коды обладают меньшей корректирующей способностью, чем коды БЧХ, однако имеют дополнительные криптографические свойства. Также перспективным является поиск методов повышения дистанционных свойств *R*-кода.

DECODING 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. Correction properties and fast decoding algorithms of a Rijndael-code are compare.

Список литературы

1. *Elumalai R., Reddy A.R.* // International Journal of Scientific Research. 2011. Vol. 2, Issue 3.
2. Specification for the ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, November 26, 2001.
3. *Matsui M.* //The first experimental cryptanalysis of the Data Encryption Standard, CRYPTO 94 (Springer LNCS 839) 1-11.
4. *Фомичев В.М.* Дискретная математика и криптология. Курс лекций. М.: ДИАЛОГ-МИФИ, 2003.
5. *MacWilliams F.J., Sloane N.J.A.* The Theory of Error- Correcting Codes. North-Holland, 1977.
6. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М., 2005.