Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ПОЛИНОМИАЛЬНЫЕ ИНВАРИАНТЫ АВТОМОРФИЗМОВ СЕМЕЙСТВА БЧХ-КОДОВ И ИХ ПРИЛОЖЕНИЯ

В.А. ЛИПНИЦКИЙ, Е.В. СЕРЕДА

Военная академия Республики Беларусь
Белорусский государственный университет информатики и радиоэлектроники

Введение. Классическое в теории помехоустойчивого кодирования семейство кодов Боуза – Чоудхури – Хоквингема (БЧХ-кодов) является наиболее популярным в приложениях, особенно в высокоскоростных системах передачи информации [1]. Цикличность этих кодов, возможность представления компонент синдромов ошибок элементами конечного поля позволили развить различные алгебраические методы их обработки. К наиболее известным и применимым относится метод коррекции ошибок примитивными БЧХ-кодами путем решения уравнений в полях Галуа. На рубеже XX и XXI веков белорусской школой помехоустойчивого кодирования разработана теория норм синдромов (ТНС) – инвариантов Γ-орбит ошибок циклической группы Γ автоморфизмов кодов [2, 3]. Вытекающие из ТНС норменные методы коррекции ошибок на порядок эффективнее классических синдромных методов.

Современные условия предъявляют высокие требования к инфокоммуникационным системам (ИКС), прежде всего, к росту объемов информации, передаваемой в единицу времени. Это влечет увеличение длин применяемых кодов и объемов передаваемой информации, что, в свою очередь, замедляет работу норменных декодеров. Одним из выходов из сложившейся ситуации мы видим в применении G-орбит, предлагая их полиномиальные инварианты, для группы автоморфизмов G, $G \supset \Gamma$. В докладе предлагается дальнейшее развитие ТНС введением новых синдромных инвариантов – полиномиальных.

Об автоморфизмах БЧХ-кодов. Для всякого БЧХ-кода C его группа автоморфизмов $AutC$ содержит некоммутативную подгруппу G, порожденную подгруппой Γ и циклотомическим автоморфизмом φ [1, 3], порожденным автоморфизмом Фробениуса поля Галуа $GF(2^m)$ – поля определения кода C. Группа Γ имеет порядок n, а группа G – порядок mn. Подавляющее большинство Γ-орбит имеют мощность n, а G-орбиты имеют, как правило, мощность mn. Каждая G-орбита состоит из Γ-орбит и имеет следующую структуру: $I_G = \{J, \varphi(J), \varphi^2(J), ..., \varphi^{(\mu-1)}(J)\}$ для конкретной Γ-орбиты J. Здесь μ – наименьший делитель m с условием: $\varphi^{\mu}(J) = J$. В большинстве случаев $\mu = m$.

Всякая Γ-орбита J имеет похожую структуру: для автоморфизма σ циклического сдвига координат векторов: $\sigma(e_1, e_2, ..., e_n) = (e_n, e_1, e_2, ..., e_{n-1})$ и для любой своей вектор-ошибки $\bar{e}$: $J = \left\{\bar{e}, \sigma(\bar{e}), ..., \sigma^{\nu-1}(\bar{e})\right\}$, где ν – наименьшее натуральное число с условием: $\sigma^{\nu}(\bar{e}) = \bar{e}$. Известно, что ν делит n, и как правило, совпадает с n. В силу сказанного часто используются обозначения: $J = <\bar{e}>$ или $J = <\bar{e}_{\Gamma}>$.

Нормы синдромов и норменные декодеры для БЧХ-кодов. Классический примитивный БЧХ-код длиной n, исправляющий двойные ошибки, задается проверочной матрицей $H = \{\alpha^i, \alpha^{3i}\}^T$, $0 \le i \le 2^m - 2 = n - 1$, α – примитивный элемент поля $GF(2^m)$. Синдром ошибок в сообщении $\bar{x}$ вычисляется по формуле: $S(\bar{x}) = H \cdot \bar{x}^T$.

В согласии со структурой проверочной матрицы здесь $S(\bar{x}) = (s_1, s_2)^T$, где s_1, s_2 – компоненты синдрома, элементы поля $GF(2^m)$.

Нормы синдромов – синдромные инварианты группы Γ циклических сдвигов – подгруппы группы $AutC$ автоморфизмов всякого циклического БЧХ-кода C, кодов Хемминга, реверсивных кодов, – являются своеобразными индикаторами Γ-орбит. Установлено, что нормы синдромов Γ-орбит ошибок декодируемой совокупности попарно различны. Декодер всякой ИКС, построенный на основе любого БЧХ-кода, в обязательном порядке вычисляет синдром $S(\bar{x})$ каждого принятого блока-сообщения $\bar{x}$. Условие $S(\bar{x}) \neq 0$ означает наличие в сообщении $\bar{x}$ ненулевого вектора-ошибки $\bar{e}$, который декодер должен откорректировать. Вычислив $N(S(\bar{x}))$ по установленным в [2, 3] формулах через компоненты синдрома $S(\bar{x})$, мы тем самым идентифицируем Γ-орбиту J, которой принадлежит искомая ошибка $\bar{e}$ в сообщении $\bar{x}$. Не представляет особой сложности установить точное значение $\bar{e}$ внутри Γ-орбиты J [2, 3]: сравнивая синдромы искомой ошибки и образующей Γ-орбиты J, легко устанавливается величина циклического сдвига образующей для получения искомого корректируемого вектора-ошибки.

Норменные методы оказались в n раз быстрее стандартных методов коррекции ошибок, где n – длина кода. Декодеры на их основе хорошо реализуются на БИС нейросетевого типа.

Согласно предложению 3.1 [2], $S(\sigma(\bar{e})) = (\alpha \cdot s_1, \alpha^3 \cdot s_2)^T$. В силу этой формулы норма $N(S(\bar{x}))$ синдрома $S(\bar{x})$ вычисляется по формуле (см. [2], глава 4):

$$N(S(\bar{x})) = s_2 / s_1^3. \qquad (1)$$

При заданном формулой (1) определении легко выясняется, что норма синдрома одинакова для всех ошибок Γ-орбиты $J = <\bar{e}_\Gamma>$, то есть является инвариантом этой орбиты, а потому и называется нормой этой Γ-орбиты. Согласно теореме 4.1 [2] нормы множества T Γ-орбит одиночных и двойных ошибок попарно различны. Составив список ET образующих $\bar{e}_i$ Γ-орбит множества T, список ST синдромов образующих $S(\bar{e}_i)$ и список NST норм синдромов образующих $N(S(\bar{e}_i))$ мы можем реализовать работу норменного декодера по отмеченному выше алгоритму (см. [2] главы 4 и 5).

С ростом длины применяемых кодов, с увеличением кратности исправляемых векторов-ошибок (последнее особенно типично при применении не примитивных БЧХ-кодов, см., например, [4]) резко возрастают объемы ошибок подлежащих исправлению, что существенно увеличивает названные выше списки и замедляет работу с ними. Для преодоления создавшейся проблемы мы предлагаем перейти от Γ-орбит к более крупным группам ошибок – G-орбитам.

G-орбиты и их полиномиальные инварианты. В силу предложения 3.17 [3] $S(\varphi(\bar{e})) = (s_1^2, s_2^2)^T$. Отсюда следует, что $N(S(\varphi(\bar{e}))) = (N(S(\bar{e})))^2$. Действие φ на координаты векторов-ошибок подробно изложено в [3], стр. 40 – 41. Таким образом, почти автоматически строится селекция орбит множества T в G-орбиты, а также списков ST и NST. Список EG образующих G-орбит строится из списка ET и, практически, в m раз меньше списка ET.

Возьмём образующую $\bar{e}_i \in EG$. Ее норма $N_i = N(S(\bar{e}_i)) = \alpha^j$ – конкретный ненулевой элемент поля Галуа $GF(2^m)$. Как правило, G-орбита $<\bar{e}_i>_G$ состоит из m

Γ-орбит. Нормы этих Γ-орбит получаются последовательным возведением в квадрат $N_i = \alpha^j$. Но возведение в квадрат элементов поля Галуа $GF(2^m)$ равносильно действию на $N_i = \alpha^j$ автоморфизма Фробениуса, образующей φ циклической группы Галуа этого поля. Таким образом, список норм Γ-орбит G-орбиты $<\overline{e}_i>_G$ имеет вид: $N(<\overline{e}_i>_G) = \left\{N_i, \varphi(N_i), ..., \varphi^{m-1}(N_i)\right\} = \left\{\alpha^j, \alpha^{2j}, ..., \alpha^{2^{m-1}j}\right\}$. Аналогично строятся и синдромы образующих этих Γ-орбит. Построенный список норм Γ-орбит, составляющих G-орбиту $<\overline{e}_i>_G$ есть множество всех сопряженных друг другу под действием группы Галуа элементов поля. Такие элементы составляют полный список корней неприводимого полинома над минимальным подполем $Z/2Z = GF(2)$. Этот полином называют минимальным полиномом любого из элементов названного списка и, как правило, обозначают $p(\alpha^j, x)$ [5, 6]. Итак, полином

$$p(\alpha^j, x) = (x - \alpha^j)(x - \alpha^{2j}) \cdot ... \cdot (x - \alpha^{2^{m-1}i}) = p(<\overline{e}_i>_G, x) \qquad (2)$$

очевидно, является однозначной характеристикой G-орбиты $<\overline{e}_i>_G$. G-орбита $<\overline{e}_i>_G$ содержит $\mu < m$ Γ-орбит тогда и только тогда, когда α^j принадлежит подполю $GF(2^\mu)$ поля $GF(2^m)$.

Метод декодирования ошибок на основе G-орбит предполагает составление списка PEG неприводимых полиномов (2) норм синдромов образующих G-орбит двухступенчатую систему идентификации ошибки: найдя ненулевой синдром ошибки, вычисляем ее норму, затем находим неприводимый полином этой нормы, данный полином сравниваем со списком PEG. Отождествив вычисленный полином с каким-то полиномом списка PEG, далее мы сравниваем вычисленную норму только со списком норм Γ-орбит соответствующей G-орбиты. Дальнейшие действия с Γ-орбитами уже описаны выше.

Заключение. Предложенные полиномиальные инварианты G-орбит обеспечивают трехэтапную итерационную процедуру декодирования ошибок кодами семейства БЧХ, примерно в mn раз более эффективную, чем стандартные синдромные методы. Особенность названной процедуры в последовательной уточняющей идентификации искомой ошибки: сначала с помощью полиномиального инварианта определяем G-орбиту, которой принадлежит искомая ошибка; затем с помощью норм Γ-орбит, принадлежащих найденной G-орбите, определяем конкретную Γ-орбиту, содержащую корректируемую ошибку; наконец, сравнивая синдромы образующей найденной Γ-орбиты и декодируемой ошибки, определяем величину циклического сдвига образующей для получения точного значения искомой ошибки.

Список литературы

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: пер. с англ. М.: Связь, 1979.

2. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Минск: БГУИР, 2000. 242 с.

3. Липницкий В. А., Конопелько В. К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск: БГУ, 2007.

4. Липницкий В.А., Олексюк А.О. Теория норм синдромов и плюс-декодирование. // Доклады БГУИР, 2014, №8. – С. 71 – 78.

5. Лидл Р., Нидеррайтер Г. Конечные поля: в 2 т.: пер. с англ. М.: Мир, 1988.
6. Липницкий В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. 2-е изд. Минск: БГУИР, 2006.

О СТОХАСТИЧЕСКОМ МОДЕЛИРОВАНИИ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ НА ОСНОВЕ МАЛОПАРАМЕТРИЧЕСКИХ МОДЕЛЕЙ

М. В. МАЛЬЦЕВ, Ю. С. ХАРИН

НИИ прикладных проблем математики и информатики БГУ

Для надежного шифрования необходимы криптографические генераторы – программные, аппаратные или программно-аппаратные устройства, вырабатывающие последовательности случайных или псевдослучайных чисел [1, 2]. Выходные последовательности стойкого криптографического генератора должны быть неотличимы от равномерно распределенной случайной последовательности (РРСП) [1]. Элементы РРСП независимы в совокупности, но псевдослучайные последовательности вырабатываются генераторами по определенным детерминированным алгоритмам и в таких последовательностях присутствуют зависимости, как правило, большой глубины. Для описания таких зависимостей адекватной моделью является цепь Маркова порядка $s >> 1$ (ЦМ(s)) [3]. К сожалению, использовать ее на практике зачастую невозможно, поскольку число параметров D этой модели с N состояниями увеличивается экспоненциально с ростом s:

$$D = N^s(N–1).$$

В связи с этим необходимы так называемые малопараметрические (parsimonious) марковские модели, число параметров которых зависит от s полиномиально [4]. Примерами малопараметрических моделей являются MTD-модель Рафтери [5], цепь Маркова переменного порядка [6], цепь Маркова условного порядка [7]. Поскольку по мере развития криптографии усложняется структура разрабатываемых генераторов, то возникает потребность в построении новых математических моделей для их анализа. В данной работе представлены две новые модели, построенные на основе цепи Маркова s-го порядка с r частичными связями (ЦМ(s, r)) [8].

Первая модель, рассматриваемая в данной работе, – цепь Маркова с частичными связями с переменным шаблоном. Модель ЦМ(s, r), разработанная в Белорусском государственном университете, является вероятностной моделью регистра сдвига с линейной обратной связью. Для этой модели условное распределение вероятностей будущего состояния временного ряда зависит не от всех s предыдущих состояний, а лишь от r избранных, определяемых так называемым шаблоном связей. ЦМ(s, r) с переменным шаблоном описывает более сложные зависимости, при которых шаблон изменяется с течением времени. Подобная ситуация встречается в криптографических генераторах. К примеру, в прореживающем (self-shrinking) генераторе на каждом такте при выработке очередного бита выходной последовательности происходит выбор одного из двух полиномов обратной связи [9].

Приведем математическое описание ЦМ(s, r) с переменным шаблоном.