УДК 681.322.067

ПРИМЕНЕНИЕ КОДОВ С ЕСТЕСТВЕННОЙ ИЗБЫТОЧНОСТЬЮ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Яблоновский Юрий Анатольевич
к.т.н.
Военная академия связи (филиал) г. Краснодар, Россия

Лойко Валерий Иванович
д.т.н., профессор
Кубанский государственный аграрный университет, Краснодар, Россия
Винокуров Александр Владимирович
к.т.н., доцент
Военная академия связи (филиал) г. Краснодар, Россия

Махичев Вячеслав Николаевич
к.в.н., доцент
Военная академия связи (филиал) г. Краснодар, Россия

В статье дан обзор криптографических систем на основе помехоустойчивого кодирования, предложен вид кодов с естественной избыточностью для решения задачи одновременной защиты информации и обнаружения и исправления ошибок, приведено доказательство, что коды с естественной избыточностью являются групповыми кодами.

Ключевые слова: ЗАЩИТА ИНФОРМАЦИИ, КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ, ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ, КОДЫ С ЕСТЕСТВЕННОЙ ИЗБЫТОЧНОСТЬЮ

UDC 681.322.067

APPLICATION OF CODES WITH NATURAL REDUNDANCY FOR INFORMATION PROTECTION

Jablonovsky Yury Anatolevich
Cand.Tech.Sci.
Military academy of connection (branch) Krasnodar, Russia

Lojko Valery Ivanovich
Dr.Sci.Tech., professor
Kuban state agrarian university, Krasnodar, Russia

Vinokurov Alexander Vladimirovich
Cand.Tech.Sci., senior lecturer
Military academy of connection (branch) Krasnodar, Russia

Makhichev Vyacheslav Nikolaevich
Cand.Mil.Sci., associate professor
Military academy of connection (branch) Krasnodar, Russia

In the article we provide a survey of cryptographic systems on the basis of unjammable coding; we offer the aspect of codes with natural redundancy for the solution of a problem of simultaneous protection of the information and detection and correction of errors; the demonstration is resulted that codes with natural redundancy are group codes

Keywords: INFORMATION PROTECTION, CRYPTOGRAPHIC SYSTEMS, UNJAMMABLE CODING, CODES WITH NATURAL REDUNDANCY

Внедрение современных информационных технологий в повседневную жизнь общества привело к проблемам обеспечения информационной безопасности. Одним из решений этой проблемы является широкое применение криптографии. На данный момент к криптографическим алгоритмам предъявляют жесткие технологические требования не только по стойкости, но и по скорости и простоте реализации [2].

Возросшие требования по скорости связаны с необходимостью сохранения высокой производительности автоматизированных систем после встраивания в них механизмов защиты. Простота аппаратной

реализации необходима для снижения стоимости средств шифрования, что будет способствовать их массовому применению и более широким возможностям встраивания в портативную аппаратуру. В силу специфики представления информации в цифровых устройствах наибольший интерес представляют блочные шифры, проблемно-ориентированные на использование их в вышеперечисленных устройствах и системах.

Таким образом, разработка проблемно-ориентированных систем шифрования является важной и актуальной задачей прикладной криптографии.

Все известные алгоритмы криптографических систем, обладающие свойством помехоустойчивости, имеют в своей основе коды, обнаруживающие и исправляющие ошибки.

Наиболее известной криптосистемой с открытыми ключами на основе теории алгебраического кодирования является криптосистема Мак Элиса на основе класса кодов, исправляющих ошибки, называемых кодами Гоппа (Goppa). Основная идея заключается в том, чтобы создать код Гоппа и замаскировать его под обычный линейный код. Существует быстрый алгоритм декодирования кодов Гоппа, но общая проблема нахождения слов кода по данному весу в линейном двоичном коде является NP-полной задачей[3].

Анализ криптостойкости данного алгоритма показывает, что для надежной защиты информации требуются следующие минимальные значения параметров: $n = 1024$, $k = 524$. Помехозащищенные свойства алгоритма напрямую зависят от параметра t, значение которого необходимо выбирать из условия $t \geq 50$. Данная оценка является оптимальной для каналов связи с вероятностью появления ошибки 10^{-4}.

Для надежной криптографической защиты необходимо получить такую сложность декодирования, которая соответствовала бы современным криптографическим стандартам (порядка 2^{50}). Данная

сложность в рассматриваемой криптосистеме обеспечивается, если количество используемых столбцов проверочной матрицы кода Гоппа составляет 750-800 [3].

Как видно из приведенного анализа, при выполнении необходимых граничных требований к параметрам системы, обеспечивается достаточно надежная криптографическая защита информации. О стойкости, например, системы Мак Элиса говорит тот факт, что, несмотря на ряд попыток ее криптоанализа, ни одна из них не увенчалась успехом. Но основной недостаток ряда помехоустойчивых кодов – искусственная информационная избыточность, вносимая алгоритмами кодирования для обнаружения и исправления ошибок. Данное обстоятельство приводит к существенному увеличению закрытого текста по отношению к исходному (в системе МакЭлиса – в 2 раза). Кроме того, открытый ключ имеет огромный по современным меркам размер – 2^{19} бит в системах Мак Элиса и Нидеррейтера [4].

Таким образом, помехоустойчивые криптоалгоритмы имеют высокие требования к аппаратной реализации, скорости работы, используемой памяти, криптозащищенности и помехоустойчивости, которые напрямую зависят от свойств применяемых кодовых алгоритмов, использующих искусственную избыточность.

Однако, существует целое направление в теории кодирования, которое рассматривает коды с естественной избыточностью [7].

Рассмотрим локализацию и обнаружение ошибок на основе F(p,s,m)-кодов как наиболее общего случая кодов с естественной избыточностью. Эти коды позволяют обнаруживать множество тех ошибок, которые нарушают свойство следования подряд не менее p и не более s нулей между двумя единицами, а также локализовать группу символов, среди которых располагаются ошибочные [6].

Логическое условие нарушения свойства следования не менее p нулей между двумя единицами для символов a_i, принимающих значение 0 либо 1, при p> 0 можно записать таким образом:

$$Q_{pi} = a_i \wedge (a_{i-p} \vee a_{i-p+1} \vee ... \vee a_{i-1} \vee a_i \vee ... \vee a_{i+p}). \quad (1)$$

Логическое условие нарушения свойства следования не более s нулей между двумя единицами для символов ai, при s<m можно записать так:

$$Q_{si} = a_i \wedge a_{i+1} \wedge ... \wedge a_{i+s}. \quad (2)$$

Общее выражение для ошибки определим как:

$$Q_{p,s} = Q_p \vee Q_s. \quad (3)$$

То, что логические условия связаны с текущими индексами i, означает, что при наличии ошибки Qpi = 1 или Qsi = 1 происходит ее локализация. При этом условие Qpi всегда определяет переход типа 0 → 1, а условие Qsi – переход типа 1 → 0.

Возможности ошибкообнаруженияF(p,s,m)-кодов в соответствие с интегральным коэффициентом Iош, определяемым для F(p,s,m)-кодов как Iош = 1 – [φp,s(m)]/2m, достаточно высоки. Практически при p ≥ 1 и m> 20 всегда Iош> 0,99 [6] .

Высокая ошибкообнаруживающая и корректирующая способность F(p,s,m)-кодов, ориентированная на конкретный характер ошибок в автоматизированной информационной системе, позволяет оптимизировать структуру информационного взаимодействия при однородности (все комбинации одной длины), малой задержке декодирования (практически на длину пакета ошибок), сохранении иерархических уровней. Все эти преимущества достигаются без существенного сокращения пропускной способности каналов системы.

Для того, чтобы обосновать применение кодов с естественной избыточностью в криптографических алгоритмах, приведем

доказательство, что данный класс кодов является линейным (групповым) кодом, или, другими словами, эти коды являются коммутативной группой на множестве двоичных чисел, в котором определена операция суммирования на основе микроопераций свертки, развертки, поглощения и перемещения.

Для доказательства примем следующие исходные данные:

а) пусть задано множество кодовых слов H, образующих оптимальную форму F=1-кода из семейства кодов с естественной избыточностью [6];

б) на множестве H определены одноместные микрооперации свёртки, развёртки, двуместные микрооперации поглощения и перемещения [7].

Доказательство. Известно, что множество G, на котором проведена какая-либо операция, называется группой, если выполняются свойства коммутативности, ассоциативности, наличие нулевого элемента, наличие противоположного элемента[1].

Для доказательства в качестве базовой примем операцию суммирования на основе микроопераций свёртки, развёртки, поглощения и перемещения.

Тогда, рассмотрим основные свойства аддитивной группы, определенной на множестве H.

1. Докажем свойство коммутативности: для любых кодовых слов A и B из H выполняется условие:

$$A+B=B+A. \qquad (4)$$

34 2113 8 5 3 2 1 1

Пусть A= 0 1 0 1 0 0 1 0 0 = 31.

B = 0 0 1 0 1 0 1 0 0 = 20.

Проведём суммирование A и B, используя операции перемещения, свёртки, развёртки и поглощения.

Вышеуказанные операции обозначим ↓, ×, , соответственно.

Просуммируем А и В:

A_0 = 0 1 0 1 0 0 1 0 0

↓ - перемещение.

B_0 = 0 0 1 0 1 0 1 0 0

A_1 =0 0 0 0 0 0 1 0 0 – развёртка.

B_1=0 1 1 1 1 0 1 0 0 - свёртка.

B_2=1 0 0 1 1 0 1 0 0 – свёртка.

A_2=0 0 0 0 0 0 0 1 1

↓↓ - перемещение.

B_3 =1 0 1 0 0 0 1 0 0

A_4=0 0 0 0 0 0 0 0 0.

B_4 = 1 0 1 0 0 0 1 1 1 – свёртка.

34 21 13 8 5 3 2 1 1

B_5=1 0 1 0 0 1 0 1 0 = 51.

Следовательно, результат сложения А+В = 51.

Теперь просуммируем В+А.

B_0 = 0 0 1 0 1 0 1 0 0

↓↓ - перемещение.

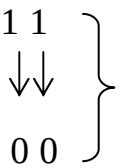
A_0 = 0 1 0 1 0 0 1 0 0

B_1 = 0 0 0 0 0 0 1 0 0 – развёртка.

A_1=0 1 1 1 1 0 1 0 0 - свёртка.

A_2=1 0 0 1 1 0 1 0 0 – свёртка.

B_2=0 0 0 0 0 0 0 1 1



A_3 =1 0 1 0 0 0 1 0 0 - перемещение.

B_4=0 0 0 0 0 0 0 0 0.

A_4 = 1 0 1 0 0 0 1 1 1 – свёртка.

34 21 13 8 5 3 2 1 1

A_5=1 0 1 0 0 1 0 1 0 = 51.

Следовательно, свойство коммутативности: для любых кодовых слов A и B из H выполняется.

2. Докажем свойство ассоциативности: для любых кодовых слов A, B, C из H выполняется условие:

$$(A+B)+C=A+(B+C) \quad (5)$$

34 2113 8 5 3 2 1 1

ПустьA= 0 1 0 1 0 0 1 0 0 = 31.

B = 0 0 1 0 1 0 1 0 0 = 20.

C = 0 0 0 0 0 0 1 0 0 = 2.

Тогда, проведём суммирование A,B,C, используя операции перемещения, свёртки, развёртки и поглощения.

Просуммируем A и B:

A_0= 0 1 0 1 0 0 1 0 0

↓↓ - перемещение.

B_0= 0 0 1 0 1 0 1 0 0

A_1 =0 0 0 0 0 0 1 0 0 – развёртка.

B_1=0 1 1 1 1 0 1 0 0 - свёртка.

B_2=1 0 0 1 1 0 1 0 0 – свёртка.

A_2 =0 0 0 0 0 0 0 1 1

↓↓ - перемещение.

B_3=1 0 1 0 0 0 1 0 0

A_4=0 0 0 0 0 0 0 0 0.

B_4= 1 0 1 0 0 0 1 1 1 – свёртка.

Проведём сложение $(A+B)+C$:

$(A+B)_0$ =1 0 1 0 0 1 0 1 0

↓↓↓↓ перемещение

C_0 = 0 0 0 0 0 0 1 0 0

$(A+B)_1$ = 0 0 0 0 0 0 0 0 0.

C_1 = 1 0 1 0 0 1 1 1 0 - свертка.

C_2 = 1 0 1 0 1 0 0 1 0.

34 21 13 8 5 3 2 1 1

Следовательно, $(A+B)+C$ = 1 0 1 0 1 0 0 1 0 = 53.

Проведём суммирование правой части равенства (4):

B_0=0 0 1 0 1 0 1 0 0

↓↓ - перемещение.

C_0=0 0 0 0 0 0 1 0 0

B_1=0 0 0 0 0 0 1 0 0 – развёртка.

C_1 =0 0 1 0 1 0 1 0 0.

B_2=0 0 0 0 0 0 0 1 1

↓↓ - перемещение.

C_2=0 0 1 0 1 0 1 0 0

B_3=0 0 0 0 0 0 0 0 0.

C_3=0 0 1 0 1 0 1 1 1 – свёртка.

C_4=0 0 1 0 1 1 0 0 1 – свёртка.

C_5=0 0 1 1 0 0 0 1 0 – свёртка.

C_6 =0 1 0 0 0 0 0 1 0 =>(B+C)=22.

Произведём сложениеA+(B+C):

A_0 =0 1 0 1 0 0 1 0 0

↓ ↓ -

$(B+C)_0$ =0 1 0 0 0 0 0 1 0 } перемещение.

A_1 =0 1 0 0 0 0 0 0 0 – развёртка.

$(B+C)_1$ =0 1 0 1 0 0 1 1 0 – свёртка.

A_2 =0 0 1 1 0 0 0 0 0

↓ -

$(B+C)_2$=0 1 0 1 0 1 0 0 0 } перемещение.

A_3 =0 0 0 1 0 0 0 0 0 - развертка.

$(B+C)_3$ =0 1 1 1 0 1 0 0 0 – свертка.

A_4=0 0 0 0 1 1 0 0 0 }

↓ - перемещение.

$(B+C)_4$ =1 0 0 1 0 1 0 0 0

A_5=0 0 0 0 0 1 0 0 0 – развёртка.

$(B+C)_5$ =1 0 0 1 1 1 0 0 0 – свёртка.

A_6 =0 0 0 0 0 0 1 1 0

↓↓ -

$(B+C)_6$=1 0 1 0 0 1 0 0 0 } перемещение.

$(B+C)_7$ =1 0 1 0 0 1 1 1 0 - свертка.

$(B+C)_8$ =1 0 1 0 1 0 0 1 0.

34 21 13 8 5 3 2 1 1

Следовательно, $A+(B+C)$= 1 0 1 0 1 0 0 1 0 = 53.

Таким образом, результаты суммирования левой и правой части выражения (4) равны.

Следовательно, кодовые комбинации кодов с естественной избыточностью обладают свойством ассоциативности.

3. Докажем наличие нулевого элемента:

$$a+0 = 0+a = a. \qquad (6)$$

Для этого кодовое слово Апросуммируем с нулевым кодовым словом D. Тогда получим следующие выражения.

Просуммируем левую часть выражения (5):

A_0=0 1 0 1 0 0 1 0 0

↓ ↓ ↓ -перемещение.

D_0=0 0 0 0 0 0 0 0 0

A_1=0 0 0 0 0 0 0 0 0 0.

D_1=0 1 0 1 0 0 1 0 0 – результат сложения.

Просуммируем правую часть выражения (5):

D_2=0 0 0 0 0 0 0 0 0 0.

A_2=0 1 0 1 0 0 1 0 0 – результат сложения.

Результаты сложения левый и правой частей равны. Следовательно, A+D=D+A=A, где D - нулевой элемент.Что и требовалось доказать.

4. Докажем наличие обратного элемента:

$$a+(-a)=(-a)+a=0. \quad (7)$$

Для этого используем кодовый вектор A=0 1 0 1 0 0 1 0 0. Найдём для него обратный. Кроме оптимальной формы F-коды, принадлежащие семейству кодов с естественной избыточностью, имеют множество других форм. Среди них есть минимальная форма, которая является единственной и имеет минимальное число единиц и максимальная форма, которая имеет максимальное число единиц. Следовательно, в этом смысле максимальная форма является обратной по отношению к минимальной. Для доказательства этого проведём некоторые преобразования. Рассмотрим левую часть выражения (7):

$$a+(-a)=0. \quad (8)$$

Тогда, можно записать, что a-a=0.Проверим это утверждение.

Пусть A=0 1 0 1 0 0 1 0 0 имеет следующий обратный элемент:

A*=0 0 1 1 1 1 0 1 1.

Тогда,

*A**=0 0 1 1 1 1 0 1 1

×

A = 0 1 0 1 0 0 1 0 0

} - поглощение.

A_1=0 1 0 0 0 0 1 0 0 – развёртка.

A^*_1=0 0 1 0 1 1 0 1 1.

A_2=0 0 1 1 0 0 0 1 1

×××

A^*_2=0 0 1 0 1 1 0 1 1 } - поглощение.

A_3 =0 0 0 1 0 0 0 0 0.

A^*_3=0 0 0 0 1 1 0 0 0 – свёртка.

A_4=0 0 0 1 0 0 0 0 0

×

A^*_4=0 0 0 1 0 0 0 0 } - поглощение. 0

A_5 =0 0 0 0 0 0 0 0 0.

A^*_5=0 0 0 0 0 0 0 0 0.

Следовательно, левая часть выражения (7) истинна. Рассмотрим правую часть выражения (7):

$$(-a)+a=0. \quad (9)$$

Перепишем это выражение в таком виде:

$$(-a)+a=(-a)-(-a)=0. \quad (10)$$

Проверим это утверждение.

Пусть (-a)=A*=0 0 1 1 1 1 0 1 1.

Тогда, a= A=0 1 0 1 0 0 1 0 0.

Следовательно,

A^*=0 0 1 1 1 1 0 1 1

×

A = 0 1 0 1 0 0 1 0 0 } - поглощение.

A^*_1=0 0 1 0 1 1 0 1 1.

A_1 = 0 1 0 0 0 0 1 0 0 – развёртка.

A^*_2=0 0 1 0 1 1 0 1 } 1
××× - } поглощение.
A_2 = 0 0 1 1 0 0 0 1 } 1

A^*_3=0 0 0 0 1 1 0 0 0.

A_3=0 0 0 1 0 0 0 0 0 – развертка.

A^*_4=0 0 0 0 1 1 0 0 0
×× - поглощение.
A_4 =0 0 0 0 1 1 0 0 0

A^*_5=0 0 0 0 0 0 0 0 0. A_5= 0 0 0 0 0 0 0 0 0.

Следовательно, правая часть выражения (7) истинна, так как левые и правые части выражения (7) равны. Это доказывает наличие обратного элемента.

Таким образом, все свойства доказаны и можно утверждать, что коды с естественной избыточностью являются групповыми кодами.

Полученные результаты открывают возможность использования кодов с естественной избыточностью в информационных системахразличного назначения, в которых предъявляются жесткие требования к защищенности обрабатываемой информации в условиях зашумления каналов связи, а также к аппаратному обеспечению в части минимизации его размеров, стоимости и энергопотребления.

Список литературы

1. Яглом А.М., Яглом И.М. Вероятность и информация. – М.: Наука, 1973. – 512 с.

2.Молдовян А.А. Криптография: Скоростные шифры [Текст] /Н.А. Молдовян, Н.Д. Гуц, Б.В. Изотов. – СПб. : БХВ-Петербург, 2002. – 496 с.: ил. ; 25 см. – 3000 экз. – ISBN 5-94157-214-X.

3.Саломаа А. Криптография с открытым ключом [Текст]: пер. с англ. – М. : Мир, 1995. – 318 с. : ил. ; 23 см – 2000 экз. – ISBN 5-03-001991-X.

4. Kabatyanski G. A Digital Signature Scheme Based on Random Error-Correcting Codes. Lecture notes in computer science [Текст] / Krouk E., Smits B. – Springer-Verlag, 1997. – vol.1355; pp.161-167.

5.Симмонс Г.Дж. Обзор методов аутентификации информации [Текст] // ТИИЭР. – 1988. - №5. – С. 105-126.

6.Ключко В.И. Синтез устройств АСУ в t-системах счисления [Текст] : учеб.пособие / А.В. Ткаченко ; М-во обороны СССР, 1986. – 330 с. ; 21 см. – 100 экз.

7.Стахов А.П. Компьютер Фибоначчи [Текст] // PCWeek/RE. – 2002. - № 32. – С. 23.

References

1. Jaglom A.M., Jaglom I.M. Verojatnost' iinformacija. – M.: Nauka, 1973. – 512 s.

2. Moldovjan A.A. Kriptografija: Skorostnyeshifry [Tekst] /N.A. Moldovjan, N.D. Guc, B.V. Izotov. – SPb. : BHV-Peterburg, 2002. – 496 s.: il. ; 25 sm. – 3000 jekz. – ISBN 5-94157-214-X.

3. Salomaa A. Kriptografija s otkrytymkljuchom [Tekst]: per. s angl. – M. : Mir, 1995. – 318 s. :il. ; 23 sm – 2000 jekz. – ISBN 5-03-001991-X.

4. Kabatyanski G. A Digital Signature Scheme Based on Random Error-Correcting Codes. Lecture notes in computer science [Tekst] / Krouk E., Smits B. – Springer-Verlag, 1997. – vol.1355; pp.161-167.

5. Simmons G.Dzh. Obzormetodovautentifikaciiinformacii [Tekst] // TIIJeR. – 1988. - №5. – S. 105-126.

6. Kljuchko V.I. Sintezustrojstv ASU v t-sistemahschislenija [Tekst] :ucheb. posobie / A.V. Tkachenko ; M-vooborony SSSR, 1986. – 330 s. ; 21 sm. – 100 jekz.

7. Stahov A.P. Komp'juterFibonachchi [Tekst] // PC Week/RE. – 2002. - № 32. – S. 23.