© Yevseiev S., Rzayev Kh., Tsyhanenko A. Analysis of the software implementation of the direct and inverse transform in non-binary equilibrium coding method // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 2, p. 196-203.

АНАЛИЗ ПРОГРАММНОЙ РЕАЛИЗАЦИИ ПРЯМОГО И ОБРАТНОГО ПРЕОБРАЗОВАНИЯ ПО МЕТОДУ НЕДВОИЧНОГО РАВНОВЕСНОГО КОДИРОВАНИЯ

Сергей Евсеев[1], Хазаил Рзаев[2], Алексей Цыганенко[1]

[1]Харьковский национальный экономический университет им. С. Кузнеца, Украина
[2]Азербайджанский государственный университет нефти и промышленности, Азербайджан

ЕВСЕЕВ Сергей Петрович, к.т.н.

Дата и место рождения: 1969, Харцызск, Донецкая обл., Украина.
Образование: Харьковский военный университет, 2002.
Должность: доцент кафедры информационных систем с 2007.
Научные интересы: информационная безопасность и кибербезопасность в банковских системах.
Публикации: более 180 научных публикаций включая монографии, книги, статьи и патенты.
E-mail: serhii.yevseiev@hneu.net

РЗАЕВ Хазаил Нураддин Оглы, к.т.н.

Дата и место рождения: 1949, Кедабекский р-н, село Дюз Расуллу, Азербайджан.
Образование: Азербайджанский Политехнический Институт им. Чингиз Ильдрыма, 1971.
Должность: доцент кафедры компьютерная инженерия с 1986.
Научные интересы: защита данных в коммуникационных системах управления добычи нефти.
Публикации: более 45 научных публикаций включая монографии, книги и статьи.
E-mail: xazail49@mail.ru

ЦЫГАНЕНКО Алексей Сергеевич

Дата и место рождения: 1993, Новая Водолага, Харьковская обл., Украина.
Образование: Харьковский национальный экономический университет им. С. Кузнеца, 2015.
Должность: магистр с 2015.
Научные интересы: безопасность информации в коммуникационных технологиях.
Публикации: 2 статьи.
E-mail: oleksii.tsyhanenko@gmail.com

Аннотация. *Современные телекоммуникационные системы для обеспечения достоверности, как правило, используют методы помехоустойчивого кодирования, а для обеспечения безопасности – криптографические алгоритмы. Для интегрированного обеспечения (одним механизмом) авторами статьи предлагается использовать несимметричную крипто-кодовую систему на основе теоретико-кодовой схемы Нидеррайтера на алгеброгеометрических кодах. Данная схема относится к модели доказуемой стойкости (стойкость основывается на теоретико-сложностной задаче – декодирование случайного кода), при этом алгеброгеометрический код, позволяет решать задачу обеспечения достоверности при передаче информации. В статье рассматривается протокол обмена данными в несимметричной крипто-кодовой системе (НККС) на основе теоретико-кодовой схемы Нидеррайтера на эллиптических кодах, основные алгоритмы метода недвоичного равновесного кодирования на основе обобщенного биномиально-позиционного представления информации, используемый в несимметричной крипто-кодовой системе Нидеррайтера для формирования кодограммы и раскодирования кодовой последовательности на приемной стороне. Описана программная реализация метода недвоичного равновесного кодирования на основе обобщенного биномиально-позиционного представления информации и алгоритмов прямого и обратного преобразования информации. Приводится внутренняя структура программной реализации и ее особенности, анализ программной реализации позволяет оценить энергетические затраты при практической реализации данного протокола обмена данных.*

Ключевые слова: *несимметричная крипто-кодовая система Нидеррайтера, математическая модель, равновесное кодирование, программная реализация.*

Введение

Развитие телекоммуникационных систем во всех областях их применения выдвигает более жесткие требования к обеспечению оперативности и безопасности всего цикла обработки данных. Для обеспечения данных критериев в телекоммуникационных системах используются программные/программно-аппаратные средства реализации методов помехоустойчивого кодирования (обеспечения достоверности) и методов криптографического преобразования информации, а также протоколы передачи данных на различных уровнях модели ISO/OSI. Перспективным направлением в развитии коммуникационных технологий и систем являются интегрированные механизмы, позволяющие в одной программной/программно-аппаратной реализации обеспечить требуемые показатели надежности и безопасности. С этой целью авторами предлагается использование несимметричной крипто-кодовой системы на основе теоретико-кодовой схемы (ТКС) Нидеррайтера. Вычислительная эффективность выполнения арифметических операций непосредственно зависит от способа представления чисел, над которыми выполняются операции, т.е. от применяемой системы счисления [1, 3, 4]. Наиболее распространенной является позиционная система счисления, в которой один и тот же числовой знак (цифра) в записи числа имеет различные значения, в зависимости от того разряда, где он расположен [1]. Следует отметить, что на системе биномиального счисления основано множество прикладных приложений, в том числе т.н. биномиальные коды, которые относятся к классу нелинейных двоичных избыточных кодов, используемых для повышения помехоустойчивости двоичных ассиметричных каналов передачи данных [3, 4]. Другое, не менее востребованное применение равновесных кодов состоит в построении доказуемо стойких шифросистем, безопасность которых обосновывается сводимостью задачи вычисления секретного ключа к решению теоретико-сложностной задачи синдромного декодирования [6, 7].

Информационная посылка в несимметричной крипто-кодовой системе Нидеррайтера [7] должна представлять собой равновесный вектор заданной длинны на указанном алфавите. Протокол обмена информации на основе использования несимметричной крипто-кодовой системы Нидеррайтера приведена на рис. 1.

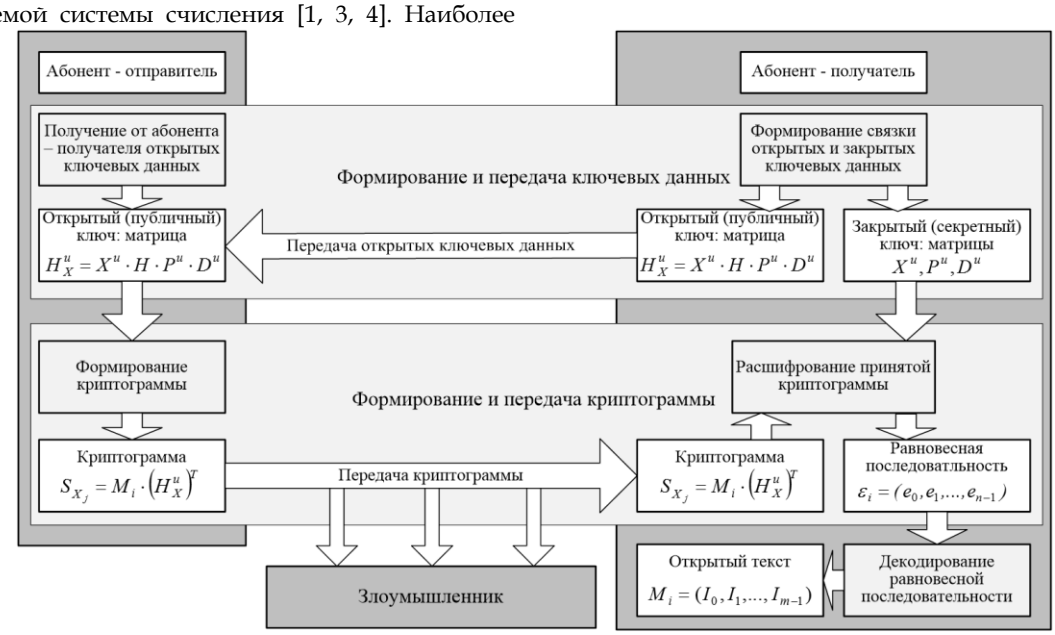

Рис. 1. Протокол обмена в несимметричной криптосистеме на основе ТКС Нидеррайтера

Неотъемлемой частью криптосистемы является алгоритм равновесного кодирования, возможности которого значительно влияют на быстродействие всей системы в целом.

Анализ существующих исследований

Проведенный анализ в работе [5] показал, что быстрый рост числа пользователей и потребителей информации, расширение спектра предоставляемых телекоммуникационных услуг, возросшие объемы обрабатываемых данных приводят к ужесточению вероятностно-временных требований, предъявляемых к основным компонентам телекоммуникационных систем и сетей на всех этапах информационного обмена данными. Так, по данным [6] актуальность создания телекоммуникационных систем и сетей с защищенными каналами передачи данных в последние годы резко возросла. Современные разработчики коммуникационных технологий вынуждены одновременно решать несколько задач одновременно и обеспечить не только безопасность передаваемой информации, но и оперативность передачи больших объемов данных. Для интегрированного обеспечения оперативности, достоверности и информационной скрытности (конфиденциальности) разработчики на сегодняшний день используют несимметричные

крипто-кодовые системы на основе ТКС Мак-Элиса и Нидеррайтера. В работе [7] авторы предлагают использовать НККС Мак-Элиса в программном обеспечении Sequitur, которая позволяет интегрировано решать задачи быстродействия и безопасности при передаче конфиденциальной информации. В работе [8] НККС Мак-Элиса используют в качестве механизма обеспечения целостности в стегасистеме, которая обеспечивает хранение в файле MPEG Layer-III или MP3 информацию об исполнителе, текст песни и ее исполнение. Криптосистема используется для хранения как личного (закрытого) ключа, так и открытого в формате тег ID3v2. В работах [9, 10] предлагается использовать криптосистему Мак-Элиса для решения задач аутентификации (подлинности) и формирования цифровой подписи на основе теории алгебраического кодирования, а также для передачи конфиденциальной (медицинской информации). Авторы работы [11] предлагают использовать криптосистему Мак-Элиса в программном обеспечении Secure Key Management (SKM, фреймворк с высокой степенью масштабируемости по отношению к памяти), для генерации ключевых последовательностей и их распределения.

В работе [2] предлагается метод недвоичного равновесного кодирования на основе обобщенного биномиально-позиционного представления. Данный метод позволяет обобщить известный подход на недвоичный случай и практически реализовать вычислительные алгоритмы формирования недвоичных последовательностей фиксированного веса. Проведенные исследования в работе [10] подтверждают, что их применение обеспечивает быстродействие на уровне применения симметричных криптоалгоритмов с БСШ, доказуемую криптостойкость на основе теоретико-сложностной задачи декодирования случайного кода (обеспечивается 10^{30} – 10^{35} групповых операций), и достоверность на основе использования укороченного алгеброгеометрического кода (обеспечивается Рош 10^{-9} – 10^{-12}).

Целью статьи является рассмотрение алгоритма недвоичного равновесного кодирования на основе обобщенного биномиально-позиционного представления с целью практической реализации несимметричной криптосистемы на основе теоретико-кодовой схемы Нидеррайтера на алгеброгеометрических кодах.

Основная часть. Метод недвоичного равновесного кодирования с использованием обобщенного биномиально-позиционного представления чисел

Процесс формирования недвоичной равновесной кодовой последовательности схематично представлен на рис. 2. Следует отметить, что схема двоичного равновесного кодирования используется как составной элемент, при выполнении операций кодирования числа $A_Б$ в биномиальной системе счисления [2, 11].

Алгоритм недвоичного равновесного кодирования, основанный на методе, преобразует число A в равновесную недвоичную последовательность $C_A = (C_{A_0} \quad C_{A_1} \quad \dots \quad C_{A_{n-1}})$ и состоит из следующих шагов [11]:

1. Ввести параметры n, w, q и число $A < M$, подлежащее недвоичному равновесному кодированию, где M - мощность недвоичного равновесного кода определяется числом векторов длины n и веса w с элементами из множества $\{0,1,\dots,q-1\}$.

$$M = (q-1)^w \frac{n!}{w!(n-w)!}.$$

2. Представить число A в виде $A = A_Б \cdot (q-1)^w + A_П$, т.е. вычислить:

2.1. $A_Б = \left\lfloor \frac{A}{(q-1)^w} \right\rfloor$;

2.2. $A_П = (A) mod \left((q-1)^w\right)$.

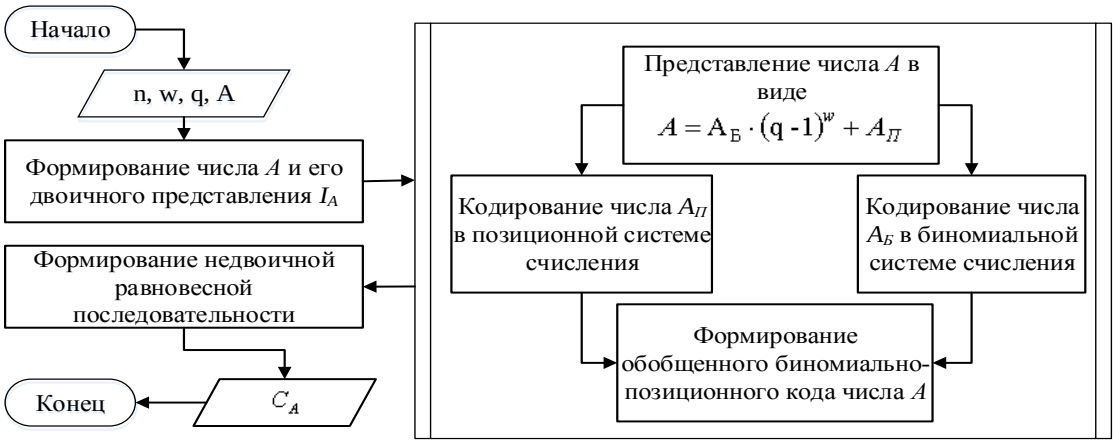

Рис. 2. Схема формирования кодовых слов недвоичного равновесного кода

3. Закодировать число $A_Б$ двоичным биномиальным кодом:

3.1. Принять $x = A_Б$, $i = 0$, $l = 0$;

3.2. Вычислить число $b_i = \binom{n-i-1}{w-l}$;

3.3. Если $b_i > x$:

3.3.1. $A_{Б_{n-i-1}} = 0$;

3.3.2. $i = i+1$ и перейти к шагу 3.2.

3.4. Если $b_i \le x$:

3.4.1. $A_{Б_{n-i-1}} = 1$;

3.4.2. $x = x - b_i$;

3.4.3. $i = i+1$;

3.4.4. $l = l+1$ и перейти к шагу 3.2.

3.5. Сформировать вектор $(a_{Б0} \quad a_{Б1} \quad \dots \quad a_{Бn-1})$.

4. Закодировать число $A_{П}$ позиционным кодом длины w по основанию $q-1$:

4.1. Принять $x = A_{П}$, $l = 0$;

4.2. Вычислить $a_l = (x) mod (q-1) + 1$;

4.3. Вычислить $x = \left\lfloor \frac{x}{q-1} \right\rfloor$;

4.4. $l = l+1$.

4.5. Если $l < w$ перейти к шагу 4.2;

4.6. Сформировать вектор $(a_0 \quad a_1 \quad \dots \quad a_{w-1})$.

5. Сформировать недвоичную равновесную последовательность:

5.1. Принять $i = 0$, $l = 0$;

5.2. Если $a_{Б_i} \ne 0$:

5.2.1. $C_{A_i} = a_l$;

5.2.2. $l = l+1$;

5.2.3. $i = i+1$ и перейти к шагу 5.2.

5.3. Если $a_{Б_i} = 0$:

5.3.1. $C_{A_i} = 0$;

5.3.2. $i = i+1$ и перейти к шагу 5.2.

5.4. Сформировать вектор $(C_{A_0} \quad C_{A_1} \quad \dots \quad C_{A_{n-1}})$.

6. Вывести вектор $C_A = (C_{A_0} \quad C_{A_1} \quad \dots \quad C_{A_{n-1}})$.

Пример. **Шаг 1**: пусть, $n = 3$, $w = 2$, $q = 3$. $M = (3-1)^2 \frac{3!}{2!(3-2)!} = 12$. Тогда $0 \le A < 12$.

Шаг 2: пусть, $A = 8$. Вычислим $A_Б = \left\lfloor \frac{8}{(3\text{-}1)^2} \right\rfloor = 2$ и $A_П = (8) \bmod \left((3\text{-}1)^2\right) = 0$.

Шаг 3: закодируем число $A_Б$ двоичным биномиальным кодом: $x = A_Б = 2$, $i = 0$, $l = 0$.

$$b_0 = \binom{3-0-1}{2-0} = \binom{2}{2} = \frac{2!}{2!(2-2)!} = 1, \qquad a_{Б_2} = 1,$$

$x = 1$, $i = 1$, $l = 1$;

$$b_1 = \binom{3-1-1}{2-1} = \binom{1}{1} = \frac{1!}{1!(1-1)!} = 1, \; a_{Б_1} = 1, \; x = 0$$

, $i = 2$, $l = 2$;

$$b_2 = \binom{3-2-1}{2-2} = \binom{0}{0} = \frac{0!}{0!(0-0)!} = 1, \; a_{Б_0} = 0,$$

$x = 0$.

В итоге формируем вектор $(a_{Б0} \quad a_{Б1} \quad a_{Б2}) \Rightarrow (0 \quad 1 \quad 1)$.

Шаг 4: закодируем число $A_{П}$ позиционным кодом длины 2 по основанию 2: $x = 0$, $l = 0$.

$$a_0 = (0) mod (3-1) + 1 = 1, \; x = \left\lfloor \frac{0}{3-1} \right\rfloor = 0, \; l = 1;$$

$$a_1 = (0) mod (3-1) + 1 = 1, \; x = \left\lfloor \frac{0}{3-1} \right\rfloor = 0, \; l = 2.$$

В итоге формируем вектор $(a_0 \quad a_1) \Rightarrow (1 \quad 1)$.

Шаг 5: формируем недвоичную равновесную последовательность:

$(C_{A_0} \quad C_{A_1} \quad C_{A_2}) \Rightarrow (0 \quad 1 \quad 1)$.

Обратные преобразования по методу недвоичного равновесного кодирования. Обратное преобразование (рис.3) состоит из разбиения полученного вектора на биномиальную и позиционную составляющую, вычисление из полученных векторов $A_{П}$ и $A_Б$:

$$A_{П} = \sum_{i=0}^{w-1} (q-1)^i \cdot (a_i - 1)$$

$$A_Б = \sum_{i=0}^{n-1} \sum_{l=0}^{w-1} a_{Б_{n-i-1}} \cdot \binom{n-i-1}{w-l}.$$

И вычислении A:

$$A = A_Б \cdot (q-1)^w + A_{П}.$$

Пример. Пусть получен вектор $C_A = (0 \quad 1 \quad 1)$, запишем его в виде $(a_{Б0} \quad a_{Б1} \quad \dots \quad a_{Бn-1})$ и $(a_0 \quad a_1 \quad \dots \quad a_{w-1})$ векторов: $(0 \quad 1 \quad 1)$ и $(1 \quad 1)$. Вычислим $A_{П}$: $A_{П} = \left((3-1)^0 \cdot (1-1)\right) + \left((3-1)^1 \cdot (1-1)\right) = 0$, и $A_Б$

$$A_Б = \left(1 \cdot \binom{2}{2}\right) + \left(1 \cdot \binom{1}{1}\right) + \left(0 \cdot \binom{0}{0}\right) = 1+1+0 = 2.$$

Далее вычисляем A:

$$A = 2 \cdot (2-1)^2 + 0 = 8.$$

Результат работы алгоритма в виде полученного соответствия всех чисел A, их двоичных представлений $I_A = (I_{A_0} \quad I_{A_1} \quad \dots \quad I_{A_{k-1}})$ в позиционном двоичном коде длины $k = \lceil log_2 M \rceil = \lceil log_2 12 \rceil = 4$, чисел $A_Б$ и $A_{П}$, соответствующих им векторов $(a_{Б0} \quad a_{Б1} \quad a_{Б2})$ и $(a_0 \quad a_1)$ сформированных недвоичных равновесных векторов $C_A = (C_{A_0} \quad C_{A_1} \quad C_{A_2})$ приведен в табл. 1. В таблице столбец $A_Б$ и вектор

$(a_{Б0} \quad a_{Б1} \quad a_{Б2})$ определяет позицию кода, а $A_П$. и $(a_0 \quad a_1)$ – его кратность.

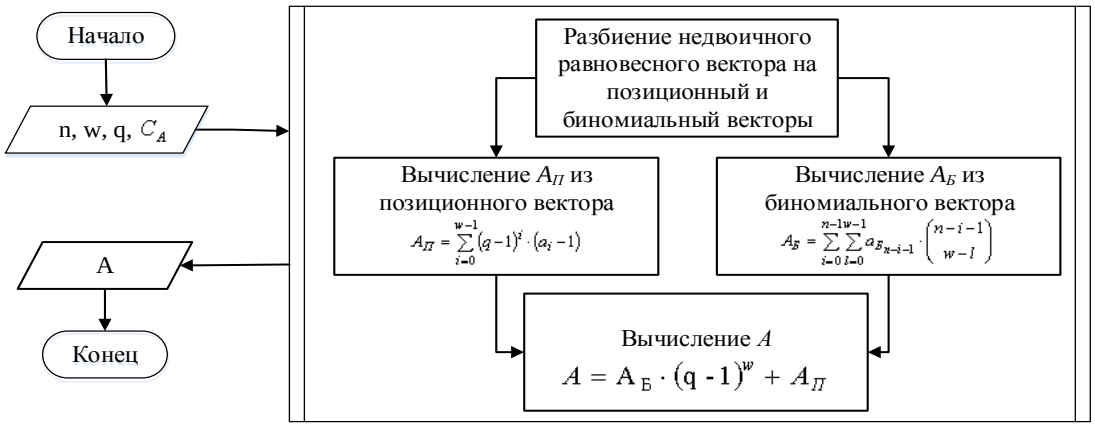

Рис. 3. Схема формирования кодовых слов недвоичного равновесного кода

Результат работы алгоритма в виде полученного соответствия всех чисел A, их двоичных представлений $I_A = (I_{A_0} \quad I_{A_1} \quad \ldots \quad I_{A_{k-1}})$ в позиционном двоичном коде длины $k = \lceil log_2 M \rceil = \lceil log_2 12 \rceil = 4$, чисел $A_Б$ и $A_П$, соответствующих им векторов $(a_{Б0} \quad a_{Б1} \quad a_{Б2})$ и $(a_0 \quad a_1)$ сформированных недвоичных равновесных векторов $C_A = (C_{A_0} \quad C_{A_1} \quad C_{A_2})$ приведен в табл. 1. В таблице столбец $A_Б$ и вектор $(a_{Б0} \quad a_{Б1} \quad a_{Б2})$ определяет позицию кода, а $A_П$. и $(a_0 \quad a_1)$ - его кратность. Зная граничные значения чисел $A_Б$ и $A_П$, можно ограничить вычисления векторов $(a_{Б0} \quad a_{Б1} \quad a_{Б2})$ и $(a_0 \quad a_1)$ к одному разу для каждого $A_Б$ и $A_П$. Данное упрощение хоть и уменьшит вычислительную сложность, но потребует дополнительный объем выделяемой памяти поэтому, нужно исходить из требований к реализации.

Результати роботи алгоритму Таблица 1

A	I_A	$A_Б$	$(a_{Б0} \quad a_{Б1} \quad a_{Б2})$	$A_П$	$(a_0 \quad a_1)$	$(C_{A_0} \quad C_{A_1} \quad C_{A_2})$
0	(0 0 0 0)	0	(1 1 0)	0	(1 1)	(1 1 0)
1	(1 0 0 0)	0	(1 1 0)	1	(2 1)	(2 1 0)
2	(0 1 0 0)	0	(1 1 0)	2	(1 2)	(1 2 0)
3	(1 1 0 0)	0	(1 1 0)	3	(2 2)	(2 2 0)
4	(0 0 1 0)	1	(1 0 1)	0	(1 1)	(1 0 1)
5	(1 0 1 0)	1	(1 0 1)	1	(2 1)	(2 0 1)
6	(0 1 1 0)	1	(1 0 1)	2	(1 2)	(1 0 2)
7	(1 1 1 0)	1	(1 0 1)	3	(2 2)	(2 0 2)
8	(0 0 0 1)	2	(0 1 1)	0	(1 1)	(0 1 1)
9	(1 0 0 1)	2	(0 1 1)	1	(2 1)	(0 2 1)
10	(0 1 0 1)	2	(0 1 1)	2	(1 2)	(0 1 2)
11	(1 1 0 1)	2	(0 1 1)	3	(2 2)	(0 2 2)

Сформированное множество из 12 недвоичных равновесных векторов $C_A = (C_{A_0} \quad C_{A_1} \quad C_{A_2})$ образует недвоичный равновесный код

$$C = \{C_0, C_1, \ldots, C_{11}\} =$$
$$\{(1 \quad 1 \quad 0), (2 \quad 1 \quad 0), (1 \quad 2 \quad 0),$$
$$(2 \quad 2 \quad 0), (1 \quad 0 \quad 1), (2 \quad 0 \quad 1), (1 \quad 0 \quad 2),$$
$$(2 \quad 0 \quad 2), (0 \quad 1 \quad 1), (0 \quad 2 \quad 1), (0 \quad 1 \quad 2), (0 \quad 2 \quad 2)\}.$$

Программная реализация недвоичного равновесного кодирования на основе обобщенного биномиально-позиционного представления

Для реализации алгоритма предлагается использовать объектно-ориентированную парадигму программирования.

В качестве языка программирования был выбран C++ и фреймворк Qt.

Для разработки и отладки программного кода использовалась интегрированная среда разработки Visual Studio 2013.

Были разработаны следующие классы: nBinEqvVec – описывает недвоичный равновесный вектор; nBinEqvCod – описывает недвоичный равновесный код.

Описание полей и методов классов представим в виде диаграммы классов (рис. 4).

Листинг функций преобразования числа в недвоичный равновесный вектор и обратно, позволяет формировать кодовую последовательность для дальнейшего преобразования в криптограммы в НККС Нидеррайтера на стороне отправителя, и обратную операцию после вычисления недвоичного вектора ошибки в НККС на приемной стороне.

```
void nBinEqvCod::calc_eVec(int A, nBinEqvVec* v)
{
 v->A = A;
 v->n = n;
 v->w = w;
 int Ab = A / qw;
 int Ap = A % qw;
 v->Ab = Ab;
 v->Ap = Ap;
 v->ab = new int[n];
 v->a = new int[w];
 v->CaInt = new int[n];
 int x = Ab;
 int l = 0;
 for (int i = 0; i < n; ++i) {
 int b = fact(n - i - 1) / (fact(w - l)*fact((n - i - 1) - (w - l)));
 if (b > x)
  v->ab[n - i - 1] = 0;
 else {
  v->ab[n - i - 1] = 1;
  x -= b;
  l++;
 }
 }
 x = Ap;
 l = 0;
 while (l < w) {
 v->a[l] = (x % (q - 1)) + 1;
 x = x / (q - 1);
 l++;
 }
 for (int i = 0, l = 0; i < n; ++i) {
 if (v->ab[i]) {
  v->Ca += QString::number(v->a[l]);
  v->CaInt[i] = v->a[l];
  l++;
 }
 else {
  v->CaInt[i] = 0;
  v->Ca += "0";
 }
 v->Ca += " ";
 }
}.
```

```
void nBinEqvCod::calc_eVec_byStr(nBinEqvVec* v)
{
 v->n = n;
 v->w = w;
 v->ab = new int[n];
 v->a = new int[w];
 v->CaInt = new int[n];
 QStringList list = v->Ca.split(' ', QString::SkipEmptyParts);
 if (list.count() != n)
 qDebug() << "Split err!";
 for (int i = 0, j = 0; i < n; ++i) {
 v->CaInt[i] = list[i].toInt();
 if (v->CaInt[i] != 0) {
  v->ab[i] = 1;
  v->a[j] = v->CaInt[i];
  ++j;
 }
 else
  v->ab[i] = 0;
 }
 v->Ab = 0;
 for (int i = 0, l = 0; i < n; ++i) {
 if (v->ab[n - i - 1] == 1) {
  int j = (fact(n - i - 1) / (fact(w - l)*fact((n - i - 1) - (w - l))));
  if (j >= 0) {
  v->Ab += j;
  ++l;
  }
 }
 }
 v->Ap = 0;
 for (int i = 0; i < w; ++i) {
 v->Ap += qPow((q - 1), i) * (v->a[i] - 1);
 }
 v->A = v->Ab * qPow((q - 1), w) + v->Ap;
}.
```

Конструктор класса nBinEqvCod инициализирует набор недвоичных равновесных векторов и позволяет сформировать кодовую последовательность для дальнейшего использования в НККС Нидеррайтера при формировании криптограммы:

```
nBinEqvCod::nBinEqvCod(int n, int w, int q) : n(n), w(w), q(q)
{
 omp_set_dynamic(1);
 omp_set_num_threads(8);
 qw = qPow((q - 1), w);
 /*Шаг 1*/
 M = qw * (fact(n)) / (fact(w)*fact(n - w));
 code = new nBinEqvVec[M];
 #pragma omp parallel for
 for (int i = 0; i < M; ++i)
 {
 calc_eVec(i, code[i]);
 mapNBEV.insert(code[i].Ca, &code[i]);
 }
}.
```

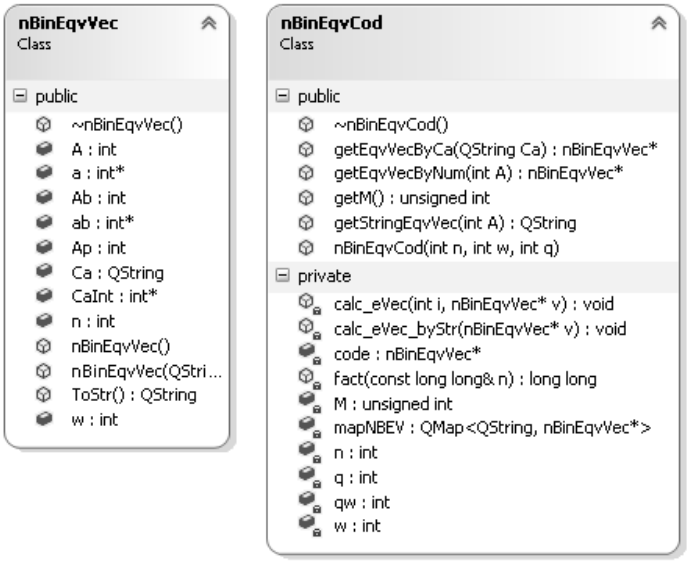

Рис. 4. Диаграмма классов программной реализации

Анализ представленной реализации

Следует обратить внимание на некие особенности реализации, а конкретно на строку «#pragma omp parallel for». Данная директива позволяет задействовать технологию OpenMP – открытый стандарт для распараллеливания программ на многопроцессорных системах [13]. Вызовом функции «omp_set_dynamic(1)» мы определяем возможность динамического создания потоков, а функцией «omp_set_num_threads(8)» – их максимальное количество. Данные технологии позволяют нам использовать ресурсы системы в полном объеме – вычисление недвоичных равновесных векторов будет производится параллельно в нескольких потоках, оптимальным для системы (в общем случае по количеству ядер процессора).

Для анализа реализованных функций воспользуемся утилитой Valgrind а конкретно модулем для профилирования – Callgrind. Данное ПО позволяет локализировать высоконагруженные места в программе, а нам оно поможет численно оценить реализованные функции. Далее представлена сложность выполнения функций в количестве инструкций за вызов функции.

Сложность выполнения функций Таблица 2

Название функции	Количество инструкций
calc_eVec	29415
calc_eVec_byStr	11234

Как видно: прямое преобразование требует почти в 3 раза большего количества инструкций, чем обратное преобразование, что подтверждает различные сложности алгоритмов, описанных выше. Данная особенность положительно сказывается в рамках программной (программно-аппаратной) реализации НККС Нидеррайтера. Так в программной реализации модуля шифратора – расшифрование принятой криптограммы требует большего количества инструкций, чем ее формирование. В результате, совместив данные модули получаем выравнивание этапов шифрования/расшифрования по количеству инструкций, что способствует синхронизации клиентов и стабильности работы в различных режимах.

Выводы

Несимметричная крипто-кодовая система на основе ТКС Нидеррайтера на АГК позволяет интегрировано решать задачи оперативности и информационной скрытности и может быть использована в открытых протоколах SSL/TLS Метод недвоичного равновесного кодирования на основе обобщенного биномиально-позиционного представления позволяет реализовывать несимметричную криптосистему на основе теоретико-кодовой схемы Нидеррайтера с использованием алгеброгеометрических кодов на эллиптических кривых, что существенно усиливает уровень ее статистической криптостойкости и обеспечить требуемые показатели оперативности и информационной скрытности передаваемых данных. Метод недвоичного равновесного кодирования имеет низкую сложность наивной реализации, которая в свою очередь является ресурсно-затратной и требует технического упрощения и модификации.

Литература

[1] Гашков С.Б. Системы счисления и их применение. – М.: МЦНМО, 2004. – 52 с.

[2] Дудикевич В.Б. Метод недвійкового рівноважого кодування / В.Б. Дудикевич, О.О. Кузнєцов, Б.П. Томашевський // Сучасний захист інформації. – 2010. – №3. – С. 57 – 68.

[3] Методи і алгоритми адаптивного рівноважного кодування для інформаційних систем. Автореф. дис.. канд. техн. наук: 05.13.06 / О.В. Бережна; Харк. нац. ун-т радіоелектрон. – Х., 2002. – 19 с.

[4] Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

[3] Телекоммуникационные услуги в мировой экономике [Электронный ресурс]. – Режим доступа : http://goo.gl/VGz1Mn.

[4] Рзаев Х. Н. Анализ состояния и путей совершенствования протоколов безопасности современных телекоммуникационных сетей [Текст]: монография / под. ред.

В.С. Пономаренко. / Х. Н. Рзаев, О. Г. Король // Информационные технологии в управлении, образовании, науке и промышленности: монография/– Х. : Издатель Рожко С. Г. 2016. – С. 217.

[5] Transmission of Picturesque content with Code Base Cryptosystem [Электронный ресурс]. – Режим доступа: https://doaj.org/article/6714b60516cc4aa79e56d0c421febaf3.

[6] Steganography application program using the ID3v2 in the MP3 audio file on mobile phone [Электронный ресурс]. – Режим доступа: https://goo.gl/s3FBmP.

[7] Space-Age Approach To Transmit Medical Image With Codebase Cryptosystem Over Noisy Channel [Электронный ресурс]. – Режим доступа: https://doaj.org/article/5c7da3a1e3ec4f83b552199034bd3241.

[8] An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel [Электронный ресурс]. – Режим доступа: https://doaj.org/article/39a3ac65d5b24b348f069dfc82eb6248.

[9] A Novel Approach For Information Security In Ad Hoc Networks Through Secure Key Management [Электронный ресурс]. – Режим доступа: ttps://doaj.org/article/378b88837cdf4cab9f8010a38a6aeb2b.

[10] Евсеев С.П. Разработка модифицированной несимметричной крипто-кодовой системы Мак-Элиса на укороченных эллиптических кодах //С.П. Евсеев, Х. Н. Рзаев, О. Г. Король / Восточно-европейский журнал передовых технологий – Харьков – 2016 – №82 – С. 4.

[11] Цыганенко А. С. Недвоичное равновесное кодирование / А. С. Цыганенко // Міжнародна науково-практична конференція молодих вчених, аспірантів та студентів «Інформаційні технології в сучасному світі: дослідження молодих вчених»: тези доповіді, 11-12 лютого 2016 р. – Харків. – ХНЭУ им. Семена Кузнеца, 2016 – С. 68.

[12] OpenMP и C++ / Канг Су Гэтлин, Пит Айсенси [Электронный ресурс]. – Режим доступа: https://msdn.microsoft.com/ru-ru/library/dd335940.aspx.

[13] McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory. // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January-February, 1978. – P. 114.

[14] Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theory. – 1986. –V.15. – P. 19-34.

УДК 681.3.06 (045)

Євсеєв С.П., Рзаєв Х.Н., Циганенко О.С. Аналіз програмної реалізації прямого та зворотного перетворення за методом недвійкового рівноважного кодування

Анотація. *Сучасні телекомунікаційні системи для забезпечення достовірності, як правило, використовують методи завадостійкого кодування, а для забезпечення безпеки – криптографічні алгоритми. Для інтегрованого забезпечення (одним механізмом) авторами статті пропонують використовувати несиметричну крипто-кодову систему на основі теоретико-кодової схеми Нідеррайтера на алгеброгеометричних кодах. Дана схема відноситься до моделі доказової стійкості (стійкість ґрунтується на теоретико-складному завданню - декодування випадкового коду), при цьому алгеброгеометричний код, дозволяє вирішувати задачу забезпечення достовірності при передачі інформації. У статті розглядається протокол обміну даними в несиметричної крипто-кодової системі (НККС) на основі теоретико-кодової схеми Нідеррайтера на еліптичних кодах, основні алгоритми методу недвійкового рівноважного кодування на основі узагальненого біноміальної-позиційного представлення інформації, що використовується в несиметричною крипто-кодової системи Нідеррайтера для формування кодограми і розкодування кодової послідовності на приймальній стороні. Описана програмна реалізація методу недвійковий рівноважного кодування на основі узагальненого біноміальної-позиційного представлення інформації і алгоритмів прямого і зворотного перетворення інформації. Наводиться внутрішня структура програмної реалізації і її особливості, аналіз програмної реалізації дозволяє оцінити енергетичні витрати при практичної реалізації даного протоколу обміну даних.*

Ключові слова: *несиметрична крипто-кодова система Нідеррайтера, математична модель, рівноважний кодування, програмна реалізація*

Yevseiev S., Rzayev Kh., Tsyhanenko A. Analysis of the software implementation of the direct and inverse transform in non-binary equilibrium coding method

Abstract. *Modern telecommunication systems tend to use noise-immune coding methods to ensure reliability and cryptographic algorithms to provide security. For integrated security (in one mechanism) the authors suggest using symmetric crypto-code system based on Niederraiter theoretical code scheme on algebrogeometric codes. This scheme relates to models with provable resistance (resistance based on theoretical and difficult task - random code decoding), while algebrogeometric code can solve the problem of ensuring the reliability of information transmission. Article considers the data exchange protocol in asymmetric crypto-code system (NKKS) based on Niederraiter theoretical-code scheme on elliptic codes, general algorithms of non-binary equilibrium coding based on the generalized binomial-way presentation of information used in Niederraiter asymmetric crypto-code system to form codegram and decode the code sequence on the receiving side. An internal structure of the program implementation and its features, software implementation analysis to evaluate energy consumption in the practical implementation of the protocol data are presented.*

Key words: *asymmetric Niederraiter crypto-code system, mathematical model, equilibrium encoding, software implementation.*

Отримано *9 травня 2016 року*, затверджено редколегією *23 травня 2016 року*