УДК 681.3.06

Б.П. Томашевський

Академія Сухопутних військ імені гетьмана Петра Сагайдачного, Львів

АЛГОРИТМ І СТРУКТУРНА СХЕМА ПРИСТРОЮ ФОРМУВАННЯ КРИПТОГРАМ В КРИПТО-КОДОВИХ СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ НА НЕДВІЙКОВИХ РІВНОВАГОВИХ КОДАХ

Пропонується алгоритм формування криптограм у крипто-кодових системах захисту інформації на недвійкових рівновагових кодах для інтегрованого забезпечення конфіденційності та завадостійкості даних, які оброблюються комунікаційних системах. Запропонована структурна схема пристрою передавання повідомлень з використанням розроблених крипто-кодових схем захисту інформації з недвійковими рівноваговими кодами.

Ключові слова: *несиметричні криптосистеми, рівновагове недвійкове кодування.*

Вступ

Постановка проблеми у загальному виді та аналіз літератури. Проведенні дослідження [1 – 5] показали, що найбільш перспективним напрямом розвитку комплексних механізмів забезпечення потрібної безпеки і достовірності передавання даних є крипто-кодові системи захисту інформації, які дозволяють інтегрувати методи криптографічного перетворення і канального (завадостійкого) кодування даних, які передаються. Найбільшу ефективність захисту даних, що передаються, забезпечують несиметричні крипто-кодові засоби захисту інформації, побудовані на недвійкових завадостійких кодах з швидкими алгоритмами декодування (поліноміальної складності) [4, 5].

Метою статті є розгляд основних кроків алгоритму і структурна схема пристрою формування криптограм в крипто-кодових системах захисту інформації на недвійкових рівновагових кодах. Пропонований алгоритм дозволяє за скінченне число кроків з використанням запропонованих крипто-кодових засобів захисту інформації формувати криптограми за введеним інформаційним повідомленням.

Результати досліджень

1. Алгоритм формування криптограм у запропонованих крипто-кодових засобах захисту інформації представимо в такий спосіб.

Крок 1. Ввід інформаційного повідомлення

$$M_i = (I_0, I_1, \ldots, I_{k-1}),\ \forall_{Ij} \in GF(q),$$

ключових даних і загальносистемних параметрів.

Під загальносистемними параметрами розуміють:

породжуючу і перевірочну матриці, що задають алгебраїчний блоковий код,

сукупність формалізованих даних, які задають правило рівновагового кодування недвійковими послідовностями.

Крок 2. Рівновагове кодування введеного інформаційного повідомлення, тобто перетворення вектору

$$M_i = (I_0, I_1, ..., I_{m-1})$$

на вектор

$$\varepsilon_i = (e_0, e_1, ..., e_{n-1}),\ \forall e_j \in GF(q).$$

Метод і алгоритм рівновагового кодування недвійковими послідовностями запропоновані і детально досліджені в [6].

Крок 3. Розгортання ключових даних і формування перевірочної матриці H_X^j замаскованого алгебраїчного блокового (n, k, d) коду над GF(q).

Крок 4. Формування синдромної послідовності (криптограми) $E_i = (S_{X_0}, S_{X_1}, ..., S_{X_{n-k-1}})$, $\forall S_{X_j} \in GF(q)$ за допомогою множення рівновагової послідовності $\varepsilon_i = (e_0, e_1, ..., e_{n-1})$ на транспоновану матрицю $\left(H_X^j\right)^T$.

Крок 5. Вивід сформованої криптограми $E_i = (S_{X_0}, S_{X_1}, ..., S_{X_{n-k-1}})$.

Блок – схема розробленого алгоритму формування криптограм у шифросистемах з недвійковими рівноваговими і нерівноваговими алгебраїчними блоковими кодами представлена на рис. 1.

2. Структурна схема пристрою формування криптограм.

На основі запропонованого алгоритму сформована структурна схема пристрою формування криптограм в запропонованих крипто-кодових засобах захисту інформації з недвійковими рівноваговими кодами, яка наведена на рис. 2. Пристрій працює в такий спосіб. На вхід 1 поступають інформаційні послідовності, що перетворюються у блоці рівновагового кодування на послідовності фіксованої ваги і довжини.

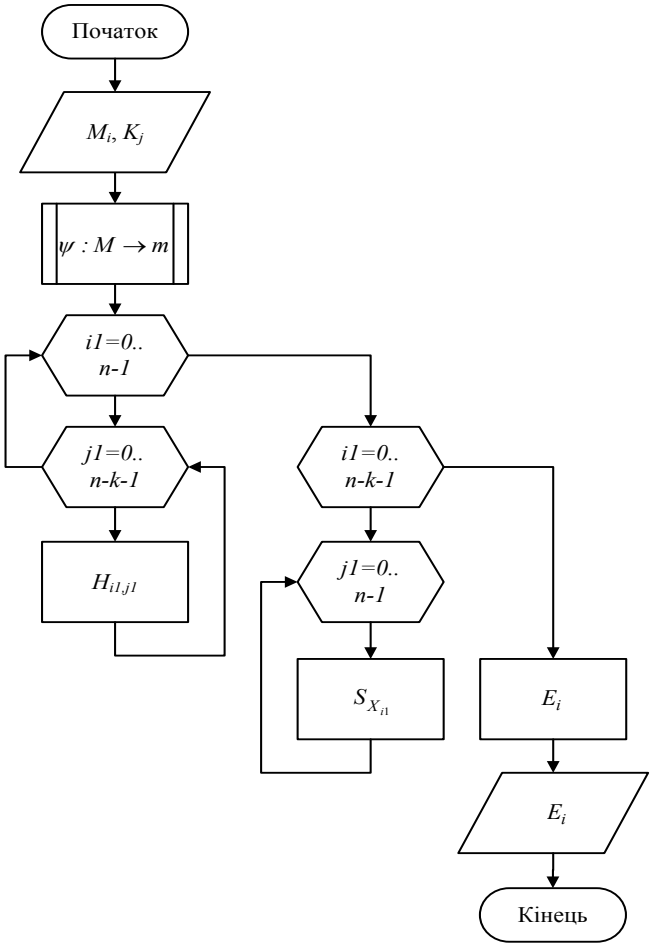

Рис. 1. Алгоритм формування криптограм

Ці показники, а також інші загальносистемні параметри поступають на вхід 2, після чого перетворюються в блоці керування та узгодження і поступають у вигляді керуючих сигналів і сигналів узгодження на інші блоки пристрою. На третій вхід пристрою поступають ключові дані, за допомогою яких у блоці маскування алгебраїчного коду обчислюється замаскована перевірочна матриця алгебраїчного блокового коду. Параметри алгебраїчного блокового коду і показники маскування поступають з виходу блоку керування та узгодження. За допомогою сформованої перевірочної матриці і рівновагової послідовності в блоці формування синдромної послідовності обчислюється вектор-синдром (криптограма).

Керування даною процедурою здійснюється за допомогою керуючих сигналів і сигналів узгодження, що поступають з відповідного пристрою. Сформована синдромна послідовність поступає на вихід пристрою.

Формування криптограм у запропонованих крипто-кодових засобах захисту інформації здійснюється за допомогою виконання процедур і функцій рівновагового і нерівновагового алгебраїчного кодування, методів маскування відповідних кодів під випадкову послідовність і функціональних операцій над кінцевими полями.

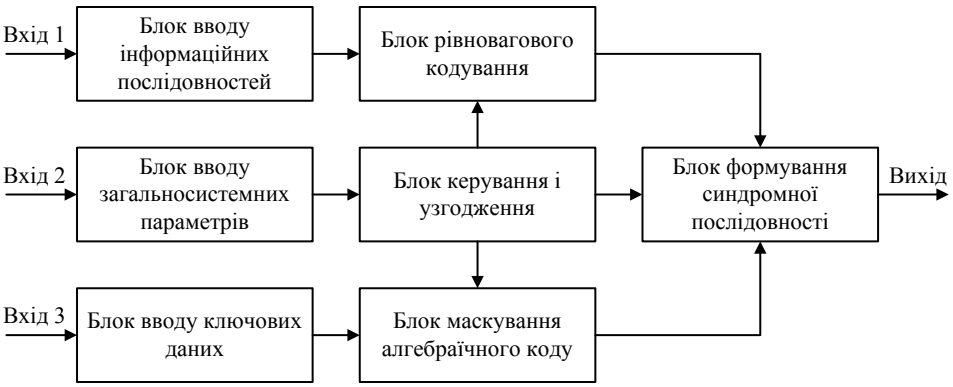

Рис. 2. Структурна схема пристрою формування криптограм

3. Експериментальні дослідження статистичної безпеки розроблених крипто-кодових засобів захисту інформації. Для експериментальної оцінки того, наскільки близько криптоалгоритми апроксимують генератори "випадкових" послідовностей, використовуються статистичні тести. Запропонований NIST пакет тестів NIST STS для тестування генераторів випадкових чи псевдовипадкових чисел є одним із підходів до реалізації задачі оцінки статистичної безпеки криптографічних примітивів. У відповідності з методикою рішення про проходження статистичного тестування приймається у разі, якщо виконуються правила:

1. Правило. Відбулося тестування з усіх q тестів, (q = $\overline{1,189}$), і якщо значення коефіцієнта r_j знаходиться всередині довірчого інтервалу [0.96, 1.00];
2. Правило. Відбулося тестування з усіх q тестів, (q=$\overline{1,189}$), і якщо для всіх тестів за критерієм $\chi 2$ Пірсона виконується умова $P(\chi^2) > 0{,}0001$.

Для проведення експериментальних досліджень властивостей розроблених кодових криптосистем розроблена програмна реалізація запропонованих засобів захисту інформації. Опис програмного пакету, що реалізує кодові криптосистеми, наведено у додатку.

При виконанні тестування обрані такі параметри: довжина послідовності, яка тестується $n = 10^6$ біт; кількість тестованих послідовностей $m = 100$. Таким чином, обсяг тестованої вибірки склав $N = 10^6 \times 100 = 10^8$ біт; рівень значущості $\alpha = 0.01$; кількість тестів $q = 189$.

Результати статистичного тестування і статистичні портрети розроблених засобів захисту інформації наведено у додатку. Підсумкові значення та результати кращих світових криптоалгоритмів зведені в табл. 1.

Таблиця 1

Результати експериментального тестування

Генератор	Кількість тестів, в яких тестування пройшло більше:	
	99% посл.	96%посл.
BBS	134 (71%)	189 (100%)
FIPS 197	126 (67%)	189 (100%)
Розроблені криптокодові засоби	132 (69%)	189 (100%)

Як видно з представлених даних у табл. 1, розроблені криптографічні засоби захисту інформації володіють добрими статистичними властивостями. Таким чином, аналіз отриманих результатів експериментальних досліджень показав, що за своїми властивостями запропоновані конструкції не поступаються кращим світовим аналогам. Отже, практичне застосування розроблених засобів захисту інформації дозволяє отримати хороші статистичні властивості формованих послідовностей і ефективно забезпечують безпеку даних, які обробляються і передаються.

Висновки

Таким чином, аналіз отриманих результатів експериментальних досліджень показав, що за своїми властивостями запропоновані конструкції не поступаються кращим світовим аналогам. Отже, практичне застосування розроблених засобів захисту інформації дозволяє отримати хороші статистичні властивості формованих послідовностей і ефективно забезпечують безпеку даних, які обробляються і передаються.

Список літератури

1. *R.J. McEliece. A Public-Key Criptosystem Based on Algebraic Theory. // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.*
2. *H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theory. – 1986. –V. 15. – P. 19-34.*
3. *Сидельников В.М. Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ / В.М.. Сидельников – 2002. – 22 с.*
4. *Стасев Ю.В., Кузнецов А.А. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов // Кибернетика и системный анализ: Международный научно-теоретический журнал. – Киев: НАНУ. – 2005. – №3. – С. 47-57.*
5. *Кузнецов А.А. Несимметричные криптосистемы доказуемой стойкости на алгебраических блоковых кодах // Радіоелектронні і комп'ютерні системи. Науково-технічний журнал – Х.: ХАИ. – 2007.– №8(27) – С.130-144.*
6. *Дудикевич В.Б. Метод недвійкового рівноважого кодування / В.Б. Дудикевич, О.О. Кузнєцов, Б.П. Томашевський // Сучасний захист інформації. – 2010. – №3. – С. 57 – 68.*
7. *Дудикевич В.Б. Крипто–кодовий захист інформації з недвійковим рівноваговим кодуванням / В.Б. Дудикевич, О.О. Кузнєцов, Б.П. Томашевський // Сучасний захист інформації. – 2010. – № 2. – С. 14 – 23*
8. *Пат. Україна, МПК (2006.01) H 03 M 7/06. Спосіб формування рівновагових недвійкових послідовностей / заявник і власник патенту Національний університет «Львівська політехніка». – № 94308; заявка 03.08.09; опублікований 26.04.11, Бюл.№8*
9. *Шеннон К. Теория связи в секретных системах / К. Шен нон // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы. - 1963. – С. 333-402.*

Надійшла до редколегії 5.10.2012

Рецензент: д-р техн. наук. проф. В.Б. Дудикевич, Національний університет «Львівська Політехніка», Львів.

АЛГОРИТМ И СТРУКТУРНАЯ СХЕМА УСТРОЙСТВА ФОРМИРОВАНИЯ КРИПТОГРАММ В КРИПТО-КОДОВЫХ СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ НА НЕДВОИЧНЫХ РАВНОВЕСНЫХ КОДАХ

Б.П. Томашевский

Предлагается алгоритм формирования криптограмм в крипто-кодовых системах защиты информации на недвоичных равновесных кодах для интегрированного обеспечения конфиденциальности и помехоустойчивости данных в коммуникационных системах, структурная схема устройства передачи сообщений с использованием разработанных крипто-кодовых схем защиты информации с недвоичными равновесными кодами.

***Ключевые слова**: несимметричные криптосистемы, равновесное недвоичное кодирование.*

ALGORITHMS AND STRUCTURED SCHEME DEVICE SHAPING CRYPTOGRAMS IN CRYPTO-CODE SYSTEM OF PROTECTION TO INFORMATION ON BALANCED MULTIPLE CODE

B.P. Tomashevskiy

The algorithm of the shaping the cryptograms is Offered in crypto-code system of protection to information on multiple balanced code for integrated provision of confidentiality and noise-immunity given in communication system. The structured scheme device transmissions of the messages is Offered with use designed crypto-code schemes of protection to information with multiple balanced code.

***Keywords**: asymmetrical cryptosystem's, balanced multiple coding.*