УДК 621.391

ДИНАМІЧНІ СХЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА КОДАХ РІДА-СОЛОМОНА

В.І. Грабчак
Науковий центр бойового застосування РВіА Сумського державного університету

У статті запропонована схема захисту інформації, яка ґрунтується на динамічному режимі зміни (n, k, d) параметрів алгебраїчних блокових кодів. Проведено дослідження динамічних схем захисту інформації на кодах Ріда-Соломона. Досліджена уразливість динамічних схем до атаки криптоаналітика методом перебору, надані оцінки часу, необхідного для декодування динамічних схем коду Ріда-Соломона.

ВСТУП

Основоположні праці К. Шеннона [1,2], в яких формулюються завдання завадостійкої передачі інформації з будь-якою наперед заданою точністю і секретної передачі інформації, пропонують як розв'язок задачі використовувати принцип випадковості використовуваних сигналів. У першому випадку для завадостійкої передачі інформації передбачається використовувати випадкові (n, k) – коди, утворені шляхом випадкового вибору з 2^n можливих двійкових комбінацій довжиною n 2^k комбінацій, кожна з яких ототожнюється з однією з інформаційних комбінацій завдовжки k. Використовуючи цю модель сигналів для передачі по каналу зв'язку, К. Шеннон довів теорему про можливість передачі по каналу зв'язку інформації з вірогідністю помилки, залежної від параметрів n та k, що може бути зроблена якомога малою шляхом вибору відповідних значень цих параметрів. Доведення цієї теореми мало фундаментальне значення для створення теорії завадостійкого кодування, хоча не давало конструктивних пропозицій реалізації такої можливості. У другій праці було доведено, що шляхом перетворення інформації, що передається у квазівипадкову послідовність, що надходить в канал зв'язку, можна забезпечити який завгодно високий ступінь секретності інформації, що передається, коли кількість інформації у криптограмі про повідомлення, що передається, залежить від ступеня випадковості сигналів, що передаються.

Відзначимо, що в класичній постановці розв'язання цих задач несумісне, оскільки при передачі блоків випадкового коду в канал надходить тільки підмножина можливих сигналів (2^k з 2^n можливих сигналів).

Різні підходи щодо застосування методів завадостійкого кодування для захисту інформації розглядалися у працях [3-5]. Основна мета досліджень, що проводяться, полягає в пошуку ефективних методів приховування (маскування) швидкого правила декодування блокових алгебраїчних кодів, внаслідок чого криптоаналітик вимушений використовувати складні алгоритми декодування випадкового коду. Взагалі для декодування випадкового лінійного блокового коду криптоаналітик вимушений використовувати кореляційний декодер,

складність якого зростає експоненціально від довжини коду і його виправляючої здатності. Складність декодування уповноваженим користувачем зростає поліноміально від параметрів коду, внаслідок чого вдається визначити односторонню криптографічну функцію, яка використовується при побудові криптосистеми.

Дослідження методів кодування разом з динамічним режимом зміни (n, k, d) параметрів коду, коли закон зміни цих параметрів непередбачуваний, дозволяє підвищити інформаційну прихованість (конфіденційність) та імітозахищеність інформації, що передається, на рівні контуру динамічного кодування [6]. Одночасно досягається значний енергетичний виграш залежно від виду каналу зв'язку і методу кодування. У зв'язку з цим підвищуються вимоги до вибору методу кодування, використання якого передбачається в контурі динамічного кодування.

Тут важливими характеристиками є:

– ансамбль можливих параметрів коду, зміна яких призводить до зміни «тонкої» структури кодового слова;

– спектр можливих довжин n;

– основа алфавіту коду q;

– обчислювальна складність алгоритму кодування-декодування;

– характер помилок, що гарантовано виправляються.

Метою статті є дослідження кодів Ріда-Соломона разом із динамічним режимом зміни (n, k, d) параметрів коду. Оцінка кількості переборів і часу, необхідних криптоаналітику для декодування динамічних схем коду Ріда-Соломона.

ОСНОВНА ЧАСТИНА

Одним із основних завдань теорії завадостійкого кодування є завдання побудови коду довжини n з кодовою відстанню d з можливою більшою кількістю елементів, тобто у разі лінійного коду з можливо більшою розмірністю k. За роки розвитку теорії завадостійкого кодування створена велика кількість різноманітних кодів. Проте на практиці застосовується відносно невелика група завадостійких алгебраїчних кодів: коди Боуза-Чоудхурі-Хоквінгема, коди Ріда-Соломона і стиснуті коди. Найширше застосовуються циклічні коди з виявленням помилок у стандартних протоколах HDLC, X.25/2 (LAP-B, LAP-M), протоколах SLIP, PPP.

Циклічні коди є підкласом у класі лінійних кодів, що відповідають додатковій сильній структурній вимозі. Через цю структуру пошук добрих завадостійких кодів була використана теорія полів Галуа. Більшість завершених побудов, що використовують ідеї цієї теорії, належать до циклічних кодів. Крім того, закладені в основу їх визначення ідеї теорії полів Галуа призводять до процедур кодування і декодування, ефективних як з алгоритмічної, так і з обчислювальної точки зору.

Найбільше поширення серед циклічних кодів набули коди Боуза-Чоудхурі-Хоквінгема. Ці коди становлять великий клас кодів, що легко будуються, з довільними довжиною блоку і швидкістю. Важливість цих кодів забезпечується не тільки гнучкістю вибору їх параметрів, але і тим, що при довжинах блоку близько декількох сотень багато з них є оптимальними серед всіх відомих кодів з тією самою довжиною і швидкістю.

Породжувальний поліном кода Боуза-Чоудхурі-Хоквінгема визначається як [7,8]:

$$g(x) = Н.О.К.[f_j(x), f_{j+1}(x), \ldots, f_{j+2t-1}(x)],$$

де $f_j(x)$ – мінімальний многочлен елемента

$$\alpha^i \in GF(q^m), \quad i = j_0, \ldots, j_0 + 2t - 1.$$

Корінням $f_j(x)$ є також всі елементи класу сполучених елементів

$$\left\{ \alpha^i, (\alpha^i), (\alpha^i)^{q^2}, \ldots, (\alpha^i)^{q^{S-1}} \right\},$$

де s – найменше ціле число, яке визначається $\alpha^{q^S} = \alpha, \quad s \prec m.$

Розглянемо циклічні коди для випадку $m = 1$. Тоді поле символів (n, k, d) коду над $GF(q)$ збігається з полем $GF(q^m)$. Якщо код примітивний, то одержимо код Ріда-Соломона [7,8], довжина якого дорівнює

$$n = q^m - 1 = q - 1.$$

Мінімальний многочлен над GF(q) елемента α, узятого з того самого поля, дорівнює

$$f(x) = x - \alpha .$$

У коді Ріда-Соломона, який виправляє t помилок, як правило, беруть $j_0 = 1$, тоді породжувальний многочлен записується у вигляді

$$g(x) = (x - \alpha)(x - \alpha^2)\ldots(x - \alpha^{2t}). \qquad (1)$$

Ступінь многочлена (1) завжди дорівнює $2t$, звідки випливає, що параметри коду Ріда-Соломона пов'язані співвідношенням

$$n - k = 2t .$$

Крім того, у коді Ріда-Соломона можна вибрати також будь-яке інше значення j_0, в цьому випадку породжувальний многочлен має вигляд

$$g(x) = (x - \alpha^{j_0})(x - \alpha^{j_0+1})\ldots(x - \alpha^{j_0+2t-1}),$$

де α – примітивні елементи поля $GF(q)$; $j_0 = \overline{1, n}$ – довільні елементи поля; t – випрямна здатність коду.

Коди Ріда-Соломона є важливою і широко використовуваною підмножиною кодів Боуза-Чоудхурі-Хоквінгема. Код Ріда-Соломона має мінімальну відстань $d = 2t + 1 = n - k + 1$ і є кодом з максимально досяжною кодовою відстанню, тобто при фіксованих n і k не існує коду, у якого мінімальна відстань більша, ніж у коду Ріда-Соломона.

Як приклад знайдемо породжувальний многочлен $g(x)$ для (7,5,3) коду Ріда-Соломона з випрямною здатністю над $GF(2^3)$.

Розширене скінчене поле $GF(2^3)$, побудоване за примітивним многочленом $g(x) = x^3 + x + 1$, класи зв'язаних елементів і мінімальні многочлени для кожного класу наведені в табл.1.

Для побудови породжувального многочлена $g(x)$ може бути вибране будь-яке j_0, для прикладу візьмемо мінімальні многочлени $f_1(x) = (x - \alpha^1)$ і $f_2(x) = (x - \alpha^2)$ і отримаємо

$$g(x) = (x - \alpha^1)(x - \alpha^2) = x^2 + \alpha^4 x + \alpha^3,$$

де $\alpha \in GF(2^3)$.

Таблиця 1 – Структура розширеного скінченного поля $GF(2^3)$

У двійковому вигляді	У логарифмічному вигляді	Класи зв'язаних елементів	Мінімальні многочлени
000	$\alpha^{-\infty}$	-	-
001	α^0	$\{\alpha^0\}$	$f_0(x) = (x - \alpha^0)$
010	α^1	$\{\alpha^1\}$	$f_1(x) = (x - \alpha^1)$
100	α^2	$\{\alpha^2\}$	$f_2(x) = (x - \alpha^2)$
011	α^3	$\{\alpha^3\}$	$f_3(x) = (x - \alpha^3)$
110	α^4	$\{\alpha^4\}$	$f_4(x) = (x - \alpha^4)$
111	α^5	$\{\alpha^5\}$	$f_5(x) = (x - \alpha^5)$
101	α^6	$\{\alpha^6\}$	$f_6(x) = (x - \alpha^6)$

Вибираючи будь-які інші мінімальні многочлени, наприклад, $f_5(x) = (x - \alpha^5)$ і $f_6(x) = (x - \alpha^6)$, також отримаємо породжувальний многочлен $g(x)$ для (7,5,3) коду Ріда-Соломона:

$$g(x) = (x - \alpha^5)(x - \alpha^6) = x^2 + \alpha^1 x + \alpha^4.$$

Таким чином, зміна будь-якого з параметрів (n, k, j_0, t) породжувального многочлена коду Ріда-Соломона призводить до утворення нового суміжного класу коду. В цьому випадку, якщо на приймальній стороні не відомий закон зміни параметрів $g(x)$, то декодування є складним обчислювальним завданням. Крім того, коди Ріда-Соломона мають добрі ансамблеві структурні властивості; змінюючи q-ну основу алфавіту, можна виправляти як поодинокі, так і пакети помилок.

Проведемо дослідження інформаційної скритності, яку можуть забезпечити динамічні схеми захисту інформації на кодах Ріда-Соломона.

Зафіксуємо (n, k, d) код Ріда-Соломона над GF(q). Потенціальна стійкість динамічних схем захисту інформації буде визначатися параметрами (n, k, j_0, d) породжувального многочлена коду Ріда-Соломона. Складність злому S такої схеми визначається кількістю переборів,

необхідних криптоаналітику для декодування коду Ріда-Соломона, і визначається величиною

$$S = \prod_{i=1}^{N} (2^m)_i ,$$

де $N = \deg g(x)_i$.

У табл.2 наведені рахункові дані верхньої границі кількості переборів, які необхідно зробити криптоаналітику для декодування кодів Ріда-Соломона залежно від швидкості коду $R = \frac{k}{n}$ та величини поля GF(q), над яким він побудований.

Таблиця 2 – Рахункові дані верхньої границі кількості переборів, які необхідні криптоаналітику для декодування кодів Ріда-Соломона

$GF(2^m)$		2^3	2^4	2^5	2^6	2^7	2^8
S	$R = \frac{2}{3}$	64	1048576	$3,6 \cdot 10^{16}$	$8,5 \cdot 10^{37}$	$4 \cdot 10^{90}$	$5 \cdot 10^{204}$
	$R = \frac{1}{2}$	512	$4,2 \cdot 10^{9}$	$1,2 \cdot 10^{24}$	$6,2 \cdot 10^{57}$	$7,2 \cdot 10^{134}$	$1,1 \cdot 10^{308}$
	$R = \frac{1}{4}$	262144	$2,8 \cdot 10^{14}$	$1,4 \cdot 10^{42}$	$5 \cdot 10^{86}$	$1,9 \cdot 10^{202}$	$2,4 \cdot 10^{462}$

Одним з основних показників оцінки криптографічної стійкості є безпечний час $T_Б$, що характеризує час безпечної роботи даної схеми динамічного кодування (криптоалгоритму) за умови застосування криптоаналітиком різних методів криптоаналізу.

Безпечний час визначається за критерієм мінімального ризику [9]:

$$T_Б = \min\left\{T_{Б_1},\ T_{Б_2},\ \ldots,\ T_{Б_L}\right\}, \qquad (2)$$

де $T_{Б_i}$ – час безпечної роботи даного криптоалгоритму за умови застосування криптоаналітиком i-го ($i = \overline{1,L}$) методу криптоаналізу; L – кількість відомих методів криптоаналізу для даного криптоалгоритму.

Розглянемо величину, яка характеризує безпечний час за умови застосування криптоаналітиком і-го методу криптоаналізу. При цьому якщо є деякий алгоритм, який реалізує і-й метод криптоаналізу, то складність розв'язання задачі криптоаналізу оцінюють як складність реалізації відповідного алгоритму S_i [9]. Тоді відповідний показник безпечного часу $T_{Б_i}$ запишеться у вигляді

$$T_{Б_i} = \frac{S_i}{\gamma \cdot \Psi}, \qquad (3)$$

де $\gamma = 31622400$ – числовий коефіцієнт для перерахунку секунд в роки; Ψ – продуктивність обчислювальної системи, яка доступна криптоаналітику.

Тоді з урахуванням (3) вираз (2) перепишеться у вигляді

$$T_{\text{Б}} = \min\left\{\frac{S_i}{\gamma \cdot \Psi},\ \frac{S_i}{\gamma \cdot \Psi},\ \ldots,\ \frac{S_i}{\gamma \cdot \Psi}\right\},$$

що еквівалентно такому запису:

$$T_{\text{Б}} = \frac{S_{\min}}{\gamma \cdot \Psi},$$

де $S_{\min}$ – часова складність алгоритму, що реалізовує найкращий відомий метод криптоаналізу $S_{\min} = \min\left\{S_1,\ S_2,\ \ldots,\ S_L\right\}$.

У табл. 3 наведені розрахункові значення часу, необхідного криптоаналітику для злому криптоалгоритму при різних довжинах і швидкостях коду Ріда-Соломона, а також залежно від доступних криптоаналітику обчислювальних потужностей.

Таблиця 3 – Розрахункові значення часу, необхідного криптоаналітику для злому криптоалгоритму

$\Psi \setminus GF(2^m)$		2^3	2^4	2^5	2^6
10^{-3} GFlops	$R = \frac{2}{3}$	режим реального часу	режим реального часу	1161 років	$2{,}7 \cdot 10^{24}$ років
	$R = \frac{1}{2}$	режим реального часу	11 год	$3{,}8 \cdot 10^{10}$ років	$2 \cdot 10^{44}$ років
	$R = \frac{1}{4}$	режим реального часу	9 років	$4{,}5 \cdot 10^{28}$ років	$1{,}6 \cdot 10^{73}$ років
1 GFlops	$R = \frac{2}{3}$	режим реального часу	режим реального часу	1,161 років	$2{,}7 \cdot 10^{21}$ років
	$R = \frac{1}{2}$	режим реального часу	40 с	$3{,}8 \cdot 10^{7}$ років	$2 \cdot 10^{41}$ років
	$R = \frac{1}{4}$	режим реального часу	32 доби	$4{,}5 \cdot 10^{25}$ років	$1{,}6 \cdot 10^{70}$ років
10^3GFlops	$R = \frac{2}{3}$	режим реального часу	режим реального часу	10 годин	$2{,}7 \cdot 10^{18}$ років
	$R = \frac{1}{2}$	режим реального часу	режим реального часу	$3{,}8 \cdot 10^{4}$ років	$2 \cdot 10^{38}$ років
	$R = \frac{1}{4}$	режим реального часу	7,6 годин	$4{,}5 \cdot 10^{22}$ років	$1{,}6 \cdot 10^{67}$ років
10^6GFlops	$R = \frac{2}{3}$	режим реального часу	режим реального часу	36 с	$2{,}7 \cdot 10^{15}$ років
	$R = \frac{1}{2}$	режим реального часу	режим реального часу	380 років	$2 \cdot 10^{35}$ років
	$R = \frac{1}{4}$	режим реального часу	27 с	$4{,}5 \cdot 10^{19}$ років	$1{,}6 \cdot 10^{64}$ років

Примітка. 1 GFlops дорівнює швидкодії обчислювальної машини 10^9 оп/с [9]

Аналіз табл.3 показує, що на сьогодні коди над розширенням скінченного поля $GF(2^3)$ - $GF(2^4)$ є слабкими до злому методом простого перебору. З урахуванням прогнозу розвитку обчислювальних засобів на найближчі роки безпечна ефективна довжина n коду Ріда-Соломона становить значення 64 і більше символів (розширення скінченного поля $GF(2^5)$ і більше).

ВИСНОВКИ

Перспективним напрямом у розвитку теорії криптографії є методи захисту інформації, що базуються на використанні блокових алгебраїчних кодів. Їх застосування дозволяє поєднувати завадостійке кодування із спеціальним перетворенням інформації. Це дає можливість інтегровано (одним прийомом) підвищувати інформаційну прихованість і достовірність передачі інформації.

Дослідження динамічних схем захисту інформації на кодах Ріда-Соломона показали, що зміна будь-якого з параметрів (n, k, j_0, t) породжувального многочлена коду Ріда-Соломона призводить до утворення нового суміжного класу коду. В цьому випадку якщо для криптоаналітика невідомий закон зміни параметрів, то декодування є складним обчислювальним завданням.

Встановлено, що найефективніше, за кількістю переборів, є застосування коду Ріда-Соломона, побудованого над розширенням скінченного поля $\geq GF(2^5)$.

SUMMARY

DYNAMIC SCHEME OF INFORMATION PROTECTION ON REEDE-SALMON'S CODES

V.I. Grabchak

Scheme of information protection based on dynamic conditions change of the block codes parameters is proposed. The investigation of the dynamic scheme of information protection on Reede-Salmon's codes is conducted. The vulnerability of dynamic scheme to the cryptoanalyst attack by surplus method is investigated, the evaluations of time necessary for the decoding of Reede-Salmon's code dynamic scheme are proposed.

СПИСОК ЛІТЕРАТУРИ

1. Шеннон К. Связь при наличии шума // Теория информации и ее приложения. Сборник переводов. – М.:Физматгиз, 1959. – С. 12-82.
2. Шеннон К. Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – С.333-402.
3. Сидельников В.М. Криптография и теория кодирования // Материалы конференции «Московский университет и развитие криптографии в России». – Москва: МГУ, 2002. – 22 с.
4. H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory // Probl. Control and Inform. Theoty. – 1986. – V.15. – P. 19-34.
5. 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.
6. Онанченко Е.Л., Кузнецов А.А., Лисенко В.Н., Грабчак В.И., Королев Р.В. Исследование методов защиты информации, основанных на использовании алгебраических блоковых кодов // Системи обробки інформації. – Харків: ХУПС,2007. – Вып. 7 (65). – С.53 – 59.
7. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.
8. Кларк Дж.-мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. / Под ред. Б.С. Цыбакова. – М.: Радио и связь, 1987. – 392 с.
9. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.

Грабчак В.І., кандидат техн. наук

Надійшла до редакції 21 серпня 2008 р.