УДК 621.391.25

А.П. Мельник[1], В.І. Грабчак[2]

[1]*Науковий центр бойовового застосування РВіА Сумського державного університету, Суми*
[2]*Львівський інститут Сухопутних військ ім. гетьмана П. СагайдачногоНУ «ЛП», Львів*

ДИНАМІЧНІ СХЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА КОДАХ РІДА-СОЛОМОНА

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

Різні підходи щодо застосування методів завадостійкого кодування для захисту інформації розглядалися в роботах [1 – 4]. 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 виправляючій здатності. Складність декодування уповноваженим користувачем зростає полиноміально 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 конфіденційність та імітозахищеність інформації, що передається, на рівні контуру динамічного кодування [4]. 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.

Доцільно застосувати в контурі динамічного кодування, кодів з високою виправною здатністю, зокрема кодів Ріда-Соломона. Коди Ріда-Соломона є

важливою і широко використовуваною підмножиною кодів БЧХ. 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 [5].

За визначенням ці коди будуються на довжинах N = q – 1 у полі GF(q) за породжувальним многочленом

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

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

Дослідження динамічних схем захисту інформації на кодах Ріда-Соломона показали, що зміна будь-якого з параметрів (n, α, j_0, t) породжувального многочлену 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-ічну основу алфавіту, можна виправляти як одиночні, так і пакети помилок.

Проведені розрахунки значення часу, необхідного криптоаналітику, для злому крипто алгоритму при різних довжинах і швидкостях коду Ріда-Соломона, в залежності від доступних обчислювальних потужностей показали, що найефективніше, за кількістю переборів, є застосування в контурі динамічного кодування коду Ріда-Соломона, побудованого над розширенням скінченого поля $\geq GF(2^5)$.

Список літератури

1. Сидельников В.М. Криптография и теория кодирования / В.М. Сидельников // Материалы конференции «Московский университет и развитие криптографии в России». – МГУ, 2002. – 22 с.

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

3. McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory / R.J. McEliece // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.

4. Исследование методов защиты информации, основанных на использовании алгебраических блоковых кодах / Е.Л. Онанченко, А.А. Кузнецов, В.Н. Лисенко, В.И. Грабчак, Р.В. Королев // Системи обробки інформації: зб. наук. пр. – Х.: ХУ ПС, 2007. – Вип. 7 (65). – С. 5-59.

5. Блейхут Р. Теория и практика кодов, контролирующих ошибки: пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.