УДК 681.32

Л. В. Крупельницький
В. П. Семеренко
О. І. Савчук

ЗАХИСТ ДАНИХ
В СИСТЕМАХ ІДЕНТИФІКАЦІЇ ОБ'ЄКТІВ

Вінницький національний технічний університет

Анотація

Запропоновано поєднання циклічних кодів та криптографії для ідентифікації об'єктів на місцевості. Для захисту даних використовується трирівнева система шифрування з максимальним суміщенням в часі. Як математичний апарат використовується теорія лінійних послідовнісних схем (ЛПС).

Ключові слова: криптографія, циклічні коди, лінійна послідовнісна схема, бент-функція.

Abstract

A combination of cyclic codes and cryptography for identification of objects on terrain with a maximum combination by time is suggested. For data protect the three-lavel system of encryption with a maximum combine on time is used. The theory of linear finite-state machine (LFSM) are used as mathematical tools.

Keywords: cryptography, cyclic codes, linear finite-state machine, bent function.

Вступ

В космічних та морських кораблях, в авіації та багатьох інших сферах використовуються пристрої, які посилають спеціальні повідомлення у відповідь на прийняті сигнали. Це дозволяє визначати розташування та ідентифікувати типи різноманітних об'єктів. Велику користь такі технічні пристрої можуть принести також для персональної ідентифікації людей або матеріальних об'єктів на місцевості [1].

При передачі даних по каналам зв'язку можливі спотворення інформації і для їх виявлення використовується завадостійке декодування. Окрім захисту даних від атмосферних завад потрібно також забезпечувати секретність інформації, що передається. Розглянемо можливість одночасного виконання операцій криптографії та завадостійкого кодування в системах ідентифікації об'єктів.

Інтеграція криптографії та завадостійкого кодування

Забезпечити поєднання криптографії та завадостійкого кодування можна за допомогою єдиного математичного аппарату – теорії лінійних послідовнісних схем (ЛПС) [2]. ЛПС, як лінійний автомат, в дискретні моменти часу t задається функцією переходів (станів)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2), \tag{1}$$

та функцією виходів

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2), \tag{2}$$

де A, B, C, D – характеристичні матриці ЛПС, S, U, Y – слова стану, вхідне, вихідне.

Як завадостійкі коди будемо використовувати циклічні коди в двійковому полі Галуа, які можуть бути представлені за допомогою ЛПС [3].

Згідно праць основоположника сучасної криптографії К. Шеннона, стійкий шифр повинен володіти властивостями розсіювання та повноти [4].

Під час несистематичного кодування циклічних кодів інформаційні та контрольні розряди перерозподіляються по всій довжині кодового слова Z_k, завдяки чому забезпечується перша властивість.

Вимога криптографічної повноти буде досягнута в тому випадку, коли кожний вихідний біт буде нетривіальною функцією всіх вхідних бітів. Частково це вже забезпечується в результаті кодування за формулами (1) і (2) за допомогою ЛПС, яку назвемо кодувальною. Введемо ще одну ЛПС – шифрувальну, – на вхід якої буде подаватись кодове слово Z_k з виходу кодувальної ЛПС. Отримане слово Z_c матиме обидві криптографічні властивості за Шенноном.

Однак, лінійна залежність слова Z_c від початкового інформаційного слова робить такий шифр вразливим для багатьох криптоатак. Тому необхідно ввести додатковий рівень захисту за допомогою нелінійних функцій, наприклад, бент-функцій φ() [5].

З іншого боку, нелінійні перетворення кодового слова Z_c зроблять неможливим виявлення та виправлення помилок в ньому по правилам циклічних кодів, які є лінійними кодами. Зберегти лінійні властивості коду й одночасно підвищити ступінь захисту від несанкціонованого доступу можна, якщо нелінійна функція φ() буде зв'язувати сусідні початкові стани $S_i(0)$ і $S_{i+1}(0)$ шифрувальної ЛПС:

$$S_{i+1}(0) = \varphi(S_i(0)). \quad (3)$$

Якщо вважати початковий стан шифрувальної ЛПС як сеансовий ключ, тоді перетворення (3) означає, по суті, формування нелінійного сеансового ключа K_{ns} з лінійного сеансового ключа K_s:

$$K_{ns} = \varphi(K_s). \quad (4)$$

Для формування лінійних сеансових ключів необхідно мати генератор сеансових ключів, що запускається в роботу одним базовим ключем K_b, який є секретним паролем. Для кожного кодового слова формується свій сеансовий ключ.

На боці приймача операції здійснюються таким чином. Спочатку формується ключ K_{ns}, далі здійснюється дешифрування і декодування отриманих даних за допомогою таких же самих ЛПС.

Висновки

Використання єдиного математичного апарату – теорії ЛПС – забезпечує максимальне суміщення в часі операцій завадостійкого кодування та криптозахисту. Запропонована трирівнева система шифрування відповідає як вимогам криптостійкості за Шенноном, так і сучасним вимогам до шифрів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Овчинников С.В. Системы позиционирования и мониторинга / С.В. Овчинников // Технологии и средства связи. – 2014. – № 2. – С. 18–22.

2. Гилл А. Линейные последовательностные машины / А. Гилл. – М. : Наука, 1974. – 288 с.

3. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія / В. П. Семеренко. – Вінниця : ВНТУ, 2015. – 444 с.

4. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон – М. : Изд-во иностр. лит., 1963. – 829 с.

5. Семеренко В. П. Интегрированная защита информации: криптография плюс помехоустойчивое кодирование / В. П. Семеренко // Захист інформації, 2011. – № 3. – С. 44–52.

Леонід Віталійович Крупельницький – канд. техн. наук, доцент, зам. зав. кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця.

Василь Петрович Семеренко – канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: vasilsemerenko@gmail.com

Олександр Ігорович Савчук – студент групи 1КІ-13б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця

Leonid V. Krupelnytskyi – PhD, Associate Professor, vice-head of the Department of computer technique, Vinnytsia National Technical University, Vinnytsia.

Vasyl P. Semerenko – PhD, Associate Professor, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: vasilsemerenko@gmail.com

Oleksandr I. Savchuk – student, Department of computer technique, Vinnytsia National Technical University Vinnytsia.