УДК 004.056.4

І.В. Миронець

Черкаський державний технологічний університет, Черкаси

ЗМЕНШЕННЯ СКЛАДНОСТІ ПРИСТРОЇВ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ НА ОСНОВІ ВВЕДЕННЯ ІНФОРМАЦІЙНОЇ НАДЛИШКОВОСТІ

Дана стаття присвячена оцінці впливу введення надлишковості на складність пристроїв криптографічного перетворення інформації. Введена надлишковість забезпечує зменшення складності пристроїв криптографічного перетворення інформації, а також високий рівень виявлення помилок. Також в статті проведено оцінку впливу введення надлишковості на складність операцій криптографічного перетворення на основі елементарних логічних функцій. Дослідження було проведено при обмеженні дискретним представленням трьохрозрядних елементарних функцій та операцій криптографічного перетворення.

***Ключові слова**: криптографічне перетворення, інформаційна надлишковість, виявлення помилок.*

Вступ

Постановка проблеми. Серед усього спектру методів захисту даних від несанкціонованого доступу особливе місце займають криптографічні методи. На відміну від інших методів, вони спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її обробки, передачі та зберігання.

Широке застосування комп'ютерних технологій та постійне збільшення обсягу інформаційних потоків викликає постійне зростання інтересу до криптографії. Останнім часом збільшується роль програмних засобів захисту інформації, просто модернізованих не потребують великих фінансових витрат в порівнянні з апаратними криптосистемами. Сучасні методи шифрування гарантують практично абсолютний захист даних, але завжди залишається проблема надійності їх реалізації. Свідченням ненадійності може бути інформація про помилки або «дірки» в тій чи іншій програмі (криптоалгоритмі), або про те, що вона була зламана. Це створює недовіру, як до конкретних програм, так і до можливості взагалі захистити що-небудь криптографічними методами не тільки від спецслужб, але і від простих «хакерів». Тому знання атак і «дірок» у криптосистемах, а також розуміння причин, за якими вони мали місце, є одним з необхідних умов розробки захищених систем і їх використання.

В даний час особливо актуальною стала оцінка вже використовуваних криптоалгоритмів. Завдання визначення ефективності та складності засобів захисту найчастіше більш трудомістка, ніж їх розробка, вимагає наявності спеціальних знань і, як правило, більш високої кваліфікації, ніж завдання розробки. Ці обставини призводять до того, що на ринку з'являється безліч засобів криптографічного захисту інформації, про ефективність та складність яких не можна сказати нічого певного. При цьому розробники тримають криптоалгоритм (як показує практика, часто нестійкий) в секреті. Проте завдання спрощення складності криптоалгоритму не може бути гарантовано складним хоча б тому, що він відомий розробникам [1]. Збільшення складності та важливості виконуваних завдань привело до вдосконалення основних показників цифрових пристроїв обчислювальної техніки, продуктивності, надійності, стійкості до збоїв і т.п. У процесі зберігання даних і передачі інформації в комп'ютерних системах та мережах неминуче виникають помилки. Контроль цілісності даних і виправлення помилок - важливе завдання на багатьох рівнях роботи з інформацією.

Розвиток засобів обчислювальної техніки супроводжується зростанням продуктивності обчислювальних пристроїв, спрощенням їх конструкції і розширенням області застосування. Це обумовлює постійний інтерес до проблеми підвищення надійності роботи цифрових пристроїв. Рішення даного завдання припускає введення надлишковості, а серед різноманіття форм введення надлишковості все більшу увагу набувають методи завадостійкого кодування, що дозволяє контролювати помилки при передачі, зберіганні та обробці інформації [2].

Аналіз публікацій і досліджень. Збільшення складності вирішуваних задач і об'ємів інформації, що переробляється, особливо в реальному часі, поставило перед розробниками спеціалізованих обчислювальних систем і систем управління ряд нових задач.

Задача спрощення складності обчислювальних систем є однією із важливих та першочергових. Це пояснюється сферою використання спеціалізованих обчислювальних систем. Такі області, як ядерна енергетика, ракетні космічні системи, системи управління хімічним виробництвом, озброєння і військова техніка можуть мати катастрофічні наслідки при збоях і відмовах в досить складних системах управління. Крім того, розширюються області використання ЕОМ, в яких технічне обслуговування майже неможливе або зовсім виключене, і тому забезпечення гара-

нтованого правильного та спрощеного їх функціонування є головною і обов'язковою вимогою.

Одним з ефективних і перспективних шляхів досягнення спрощеного функціонування обчислювальних систем є їх побудова на базі використання вбудованих засобів контролю і діагностики. Дана задача найбільш ефективно розв'язується на рівні форм представлення інформації шляхом введення надлишковості. Інформаційна надлишковість, що вводиться, використовується, перш за все для зменшення складності пристроїв криптографічного перетворення і досягається за допомогою різних підходів [3].

Метою даної роботи є зменшення складності пристроїв криптографічного перетворення інформації на основі введення інформаційної надлишковості.

Виклад основного матеріалу

Інформаційна надлишковість в пристроях обробки інформації має як позитивні, так і негативні сторони. До негативних наслідків введення надлишковості відносять підвищення інтенсивності потоку і збільшення вірогідності виникнення помилок.

У зв'язку з цим найважливішим є створення спеціалізованих обчислювальних систем і систем управління, достовірність функціонування і надійність яких базується на активній надлишковості [4, 5]. Введена надлишковість повинна забезпечити зменшення складності пристроїв криптографічного перетворення інформації, а також високий рівень виявлення та виправлення помилок. При вирішенні поставленого завдання обмежимося використанням трьохрозрядних логічних функцій криптографічного перетворення. Оцінимо вплив введення надлишковості на складність елементарних логічних функцій на основі розгляду наступних прикладів.

Код функції		*Опис функції*
00111001	57	$f_{57} = \bar{x}_1 x_2 \vee x_2 x_3 \vee x_1 \bar{x}_2 x_3$

Якщо в повній множині трьохрозрядних комбінацій вхідних сигналів розглянути комбінації 010, 011 та 100 як помилкові, тобто надлишковими, то дана логічна функція матиме спрощений вигляд:

$$f^*_{57} = x_1 x_2 x_3 . \qquad (1)$$

Модель функції f^*_{57} отримано шляхом мінімізації табличного представлення елементарної функції. Модель функції контролю помилок буде мати вигляд:

$$f^*_{57k} = \bar{x}_1 x_2 \vee x_1 \bar{x}_2 \bar{x}_3 . \qquad (1^*)$$

Аналогічно одержимо:

Код функції		*Опис функції*
01000111	71	$f_{71} = x_1 x_2 \vee \bar{x}_2 x_3$

Якщо в повній множині трьохрозрядних комбінацій вхідних сигналів розглянути комбінації 101, 110 та 111 як надлишкові, то дана логічна функція матиме вигляд:

$$f^*_{71} = \bar{x}_1 \bar{x}_2 x_3 . \qquad (2)$$

Модель функції f^*_{71} отримано шляхом мінімізації табличного представлення елементарної функції. Модель функції контролю помилок буде мати вигляд:

$$f^*_{71k} = x_1 x_2 \vee x_1 x_3 \qquad (2^*)$$

Код функції		*Опис функції*
10001110	142	$f_{142} = x_1 \bar{x}_2 \vee x_1 \bar{x}_3 \vee \bar{x}_2 \bar{x}_3$

Якщо в повній множині трьохрозрядних комбінацій вхідних сигналів розглянути комбінації 100, 101 та 110 як надлишкові, то дана логічна функція матиме вигляд:

$$f^*_{142} = \bar{x}_1 \bar{x}_2 \bar{x}_3 . \qquad (3)$$

Модель функції f^*_{142} отримано шляхом мінімізації табличного представлення елементарної функції. Модель функції контролю помилок буде мати вигляд:

$$f^*_{142k} = x_1 \bar{x}_2 \vee x_1 \bar{x}_3 . \qquad (3^*)$$

Код функції		*Опис функції*
00100111	39	$f_{39} = x_1 x_3 \vee x_2 \bar{x}_3$

Якщо в повній множині трьохрозрядних комбінацій вхідних сигналів розглянути комбінації 101, 110 та 111 як надлишкові, то дана логічна функція матиме вигляд:

$$f^*_{39} = \bar{x}_1 x_2 \bar{x}_3 . \qquad (4)$$

Модель функції f^*_{39} отримано шляхом мінімізації табличного представлення елементарної функції. Модель функції контролю помилок буде мати вигляд:

$$f^*_{39k} = x_1 x_2 \vee x_1 x_2 . \qquad (4^*)$$

Код функції		*Опис функції*
11101000	232	$f_{232} = \bar{x}_1 \bar{x}_3 \vee \bar{x}_1 \bar{x}_3 \vee \bar{x}_2 \bar{x}_3$

Якщо в повній множині трьохрозрядних комбінацій вхідних сигналів розглянути комбінації 000, 001 та 010 як надлишкові, то дана логічна функція матиме вигляд:

$$f^*_{232} = x_1 \bar{x}_2 \bar{x}_3 . \qquad (5)$$

Модель функції f^*_{232} отримано шляхом мінімізації табличного представлення елементарної функції. Модель функції контролю помилок буде мати вигляд:

$$f^*_{232k} = \bar{x}_1 \bar{x}_2 \vee \bar{x}_1 \bar{x}_2 . \qquad (5^*)$$

Розглянуті трьохрозрядні логічні функції називаються функціями розширеного матричного перетворення, тому що вони накладають додаткову умову на матричне перетворення операцій криптографічного перетворення [6]. За результатами обчислювального експерименту в роботі [6] на основі прямих трьохрозрядні елементарних функцій розширеного матричного перетворення були отримані операції криптографічного перетворення інформації: Проведемо оцінку впливу введення надлишковості на складність операцій криптографічного перетворення на основі елементарних логічних функцій. При проведенні дослідження обмежимося дискретним представленням трьохрозрядних елементарних функцій та

операцій криптографічного перетворення. Нехай операція криптографічного перетворення задана у вигляді:

$$F^{k}_{101,75,57} = \begin{bmatrix} x_1x_3 \vee \bar{x}_2x_3 \vee \bar{x}_1x_2\bar{x}_3 \\ x_1\bar{x}_3 \vee x_1x_2 \vee \bar{x}_1\bar{x}_2x_3 \\ \bar{x}_1x_2 \vee x_2x_3 \vee x_1\bar{x}_2x_3 \end{bmatrix}. \qquad (6)$$

Тоді при розгляді трьохрозрядних комбінацій вхідних сигналів 010, 011 та 100 як надлишкових, одержимо таку модель операції криптографічного перетворення:

$$F^{k*}_{101,75,57} = \begin{bmatrix} x_3 \\ x_2 \vee \bar{x}_1x_3 \\ x_2x_3 \end{bmatrix}, \qquad (6^*)$$

а якщо операція криптографічного перетворення:

$$F^{k}_{120,86,99} = \begin{bmatrix} \bar{x}_1x_2 \vee \bar{x}_1x_3 \vee x_1\bar{x}_2\bar{x}_3 \\ \bar{x}_1x_3 \vee \bar{x}_2x_3 \vee x_1x_2\bar{x}_3 \\ x_1x_2 \vee x_2\bar{x}_3 \vee \bar{x}_1\bar{x}_2x_3 \end{bmatrix}, \qquad (7)$$

то при розгляді трьохрозрядних комбінацій вхідних сигналів 001, 010 та 011 як надлишкових, одержимо таку модель операції криптографічного:

$$F^{k*}_{120,86,99} = \begin{bmatrix} \bar{x}_3 \\ x_2\bar{x}_3 \vee x_1\bar{x}_2x_3 \\ x_2 \end{bmatrix}. \qquad (7^*)$$

Аналогічно, для операція у вигляді:

$$F^{k}_{89,30,108} = \begin{bmatrix} \bar{x}_1x_3 \vee x_2x_3 \vee x_1\bar{x}_2\bar{x}_3 \\ x_1\bar{x}_3 \vee x_1\bar{x}_2 \vee \bar{x}_1x_2x_3 \\ x_1\bar{x}_2 \vee \bar{x}_2x_3 \vee \bar{x}_1x_2\bar{x}_3 \end{bmatrix} \qquad (8)$$

при розгляді трьохрозрядних комбінацій вхідних сигналів 011, 100 та 101 як надлишкових, одержимо таку модель операції криптографічного перетворення:

$$F^{k*}_{89,30,108} = \begin{bmatrix} x_3 \\ x_1x_2\bar{x}_3 \\ \bar{x}_1\bar{x}_2x_3 \vee \bar{x}_1x_2 \end{bmatrix}. \qquad (8^*)$$

Отже, вплив введення надлишковості забезпечує зменшення складності пристроїв криптографічного перетворення інформації.

Висновки

За результатами дослідження було проведено оцінювання впливу введення надлишковості на складність пристроїв криптографічного перетворення інформації. Наведені дискретні моделі елементарних функцій та операцій криптографічного перетворення показують, що введення інформаційної надлишковості до 40% приводить до зменшення складності моделей до 50%. Крім того, введена надлишковість забезпечує виявлення та виправлення до 40% помилок. А сумарна складність моделей пристроїв та моделей виявлення помилок не перевищує складність безнадлишкового перетворення інформації.

Список літератури

1. Защита информации в системах и средствах информатизации и связи. Учебн. пос. / В.М. Баранов и др. – СПб., 1996. – 111 с.

2. Дадаев Ю.Г. Теория арифметических кодов / Ю.Г. Дадаев. - М.: Радио и связь, 1981. – 244 с.

3. Рудницкий В.Н. Исследование методов синтеза структурных кодов / В.Н. Рудницкий, Н.Н. Пантелеева // Электроника и связь. – 2003. – № 18. – С. 62-64.

4. Рудницкий В.Н. Обобщенные результаты исследования структурных кодов с ограниченной серией символов / В.Н. Рудницкий, Н.Н. Пантелеева, О.В. Нечипоренко // Вістник КДПУ. – Кременчуг: КДПУ, 2003. – № 2 (19). – С. 38-40.

5. Рудницкий В.Н. Анализ форм представления информации / В.Н. Рудницкий, О.В. Нечипоренко // Электроника и связь. – К.: КПИ, 2003. – № 19. – С. 150-152.

6. Криптографическое кодирование: методы и средства реализации (ч. 2): моногр. / В.Н. Рудницкий и др. – Х.: ООО «Щедрая усадьба плюс», 2014. – 224 с.

Надійшла до редколегії 1.10.2015

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський національний університет радіоелектроніки, Харків.

УПРОЩЕНИЕ УСТРОЙСТВА КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ ВВЕДЕНИЯ ИНФОРМАЦИОННОЙ ИЗБЫТОЧНОСТИ

И.В. Миронец

Данная статья посвящена оценке влияния введения избыточности на сложность устройства криптографического преобразования информации. Введенная избыточность обеспечивает уменьшение сложности устройства криптографического преобразования информации, а также высокий уровень обнаружения ошибок. Также в статье проведена оценка влияния введения избыточности на сложность операций криптографического преобразования на основе элементарных логических функций. Исследование было проведено при ограничении дискретным представлением трехразрядных элементарных функций и операций криптографического преобразования.

Ключевые слова: *криптографическое преобразование, информационная избыточность, обнаружение ошибок.*

REDUCTION OF THE COMPLEXITY OF THE CRYPTOGRAPHIC INFORMATION TRANSFORMATION DEVICE THROUGH THE INTRODUCTION OF INFORMATION REDUNDANCY

I.V. Mironets

This article is devoted to assessing the impact of the introduction of redundancy on the complexity of the cryptographic information transformation devices. Introduction of redundancy provides a reduction in the complexity of the cryptographic information transformation devices, as well as a high level of error detection. The article also assessed the impact of the introduction of redundancy on the complexity of the operations of cryptographic transformations through the elementary logic functions. The study was conducted by limiting the discrete representation of three-digit basic functions and operations of the cryptographic transformation.

Keywords: *cryptographic transformation, information redundancy, error detection.*