УДК 004.056

Рудницький В. М.,
д-р техн. наук, професор,
Черкаський державний
технологічний університет,
rvn_2008@ukr.net
Шувалова Л. А.,
канд. техн. наук, доцент,
Черкаський державний
технологічний університет,
shuvalova-l2015@yandex.ru
Нестеренко О. Б.,
Черкаський інститут пожежної
безпеки ім. Героїв Чорнобиля НУЦЗ України,
м. Черкаси, Україна,
nesterenko.apb@gmail.com

АНАЛІЗ ДВОРОЗРЯДНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО КОДУВАННЯ ПО КРИТЕРІЮ СТРОГОГО ЛАВИННОГО ЕФЕКТУ

У статті визначено множину дворозрядних операцій криптографічного кодування, які відповідають критерію строгого лавинного ефекту та розглянуті особливості їх використання в криптоалгоритмах. Визначено в групі дворозрядних операцій криптографічного кодування операції, які гарантовано забезпечують зміну половини бітів вхідної інформації. Розглянуто можливість досягнення строгого лавинного ефекту операціями які відповідають критерію строгого стійкого кодування, для чого представлено послідовність наборів дворозрядних даних таку, щоб два сусідніх набори, а також перший і останній набори відрізнялися лише одним розрядом. Повторне виконання операцій криптографічного кодування приводить до невідповідності результатів кодування критерію строгого лавинного ефекту.

Ключові слова:*лавинний ефект; криптографічне кодування; строге стійке кодування.*

Аналіз публікацій. Однією із характеристик криптоалгоритмів є лавинний ефект. Лавинний ефект (англ. *Avalanche effect*) – поняття в криптографії, зазвичай застосовується до блочних шифрів та хеш-функцій. Це важлива криптографічна властивість для шифрування, яка означає, що зміна значення малої кількості бітів у вхідному тексті або в ключі веде до «лавинної» зміни значень вихідних бітів шифротексту.

Термін «лавинний ефект» вперше був введений Х. Фейстелем у статті Cryptography and Computer Privacy, опублікованій в журналі Scientific American в травні 1978 року, хоча концептуальне поняття використовувалося ще Шенноном.

В алгоритмах з декількома проходами лавинний ефект зазвичай досягається завдяки тому, що на кожному проході зміна одного вхідного біта веде до декількох вихідних [1].

Визначення строгого лавинного критерію (СЛК) вперше було дано С. Таваресом та А. Вебстером в роботі з дослідження S-блоків. Булеву функцію можна розглядати як частину структури S-блоків. Дизайн S-блоків, що задовольняють СЛК, був вивчений в роботах Адамса та С. Тавареса. Починаючи з 1990 року СЛК вивчається в контексті мулевих функцій.

Говорять, що криптографічний алгоритм задовольняє строгому лавинному критерію, якщо при зміні одного біта вхідної послідовності кожний біт вихідної послідовності змінюється з імовірністю одна друга [2].

Проте операції криптографічного кодування, навіть дворозрядні операції, не досліджувались на відповідність критерію строгого лавинного ефекту.

Мета статті визначити множину дворозрядних операцій криптографічного кодування, які відповідають критерію строгого лавинного ефекту, та розглянути особливості їх використання в криптоалгоритмах.

Основна частина

Розглянемо можливість досягнення строгого лавинного ефекту на прикладі дворозрядних операцій криптографічного кодування. Повна множина дворозрядних операцій криптографічного кодування наведена в табл.1.

Таблиця 1

Повна група дворозрядних операцій криптографічного перетворення інформації

№	операція	№	операція	№	операція	№	операція
1	$F_{3,5}=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	**7**	$F_{3,10}=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}$	**13**	$F_{12,5}=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}$	**19**	$F_{12,10}=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}$
2	$F_{6,5}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	**8**	$F_{6,10}=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}$	**14**	$F_{9,5}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}$	**20**	$F_{9,10}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}$
3	$F_{3,6}=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	**9**	$F_{3,9}=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}$	**15**	$F_{12,6}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}$	**21**	$F_{12,9}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
4	$F_{5,3}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	**10**	$F_{5,12}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$	**16**	$F_{10,3}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$	**22**	$F_{10,12}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$
5	$F_{5,6}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	**11**	$F_{5,9}=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}$	**17**	$F_{10,6}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}$	**23**	$F_{10,9}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
6	$F_{6,3}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	**12**	$F_{6,12}=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}$	**18**	$F_{9,3}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}$	**24**	$F_{9,12}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$

Визначимо в групі дворозрядних операцій криптографічного кодування операції які гарантовано забезпечують зміну половини бітів вхідної інформації (критерій строгого стійкого кодування).

Результати аналізу по критерію строгого стійкого кодування наведені в табл. 2.

Таблиця 2

Результати аналізу по критерію строгого стійкого кодування

Вхідна інформація		Результати перетворення вхідної інформації							
		$F_{3,10}=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}$		$F_{12,5}=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}$		$F_{10,3}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$		$F_{5,12}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$	
0	0	0	1	1	0	1	0	0	1
0	1	0	0	1	1	0	0	1	1
1	0	1	1	0	0	1	1	0	0
1	1	1	0	0	1	0	1	1	0

Криптографічний алгоритм задовольняє лавинному критерію, якщо при зміні одного біта вхідної послідовності змінюється в середньому половина вихідних бітів.

Формально для функції може бути дано таке визначення:

Функція $f:\{0,1\}^n\to\{0,1\}^n$ задовольняє лавинному критерію, якщо зміна одного біта на вході викликає зміну в середньому половини вихідних бітів [3].

Булева функція $f(x)$, де x – вектор з *n* змінних, задовольняє СЛК, якщо при зміні одного з *n* вхідних бітів вихідний біт змінюється з імовірністю рівною ½.

Розглянемо можливість досягнення строгого лавинного ефекту операціями, які відповідають критерію строгого стійкого кодування. Для цього представимо послідовність наборів дворозрядних даних (по аналогії з картами Карно) таку, щоб два сусідніх набори, а також перший і останній набори відрізнялися лише одним розрядом (табл. 3).

Як видно з таблиці 3 зміна одного розряду вхідної інформації приводить до зміни одного розряду результату, тобто до зміни вихідних бітів з ймовірністю ½.

Таблиця 3

Результати аналізу на сторогий лавинний ефект

Вхідна інформація		Результати аналізу на сторогий лавинний ефект							
		$F_{3,10}=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}$		$F_{12,5}=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}$		$F_{10,3}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$		$F_{5,12}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$	
0	0	0	1	1	0	1	0	0	1
0	1	0	0	1	1	0	0	1	1
1	1	1	0	0	1	0	1	1	0
1	0	1	1	0	0	1	1	0	0

Можна стверджувати, що визначені функції $F_{3,10}$, $F_{12,5}$, $F_{10,3}$, $F_{5,12}$ забезпечують при кодуванні не тільки зміну половини бітів вхідної інформації, а також відповідають критерію строгого лавинного ефекту.

Двораундове криптографічне кодування операціями зі строгим лавинним ефектом. Довизначимо операції двораундового кодування підставивши у вираз для кодування в другому раунді значення виразу для кодування в першому раунді. Отримані результати наведені в таблиці 4.

Таблиця 4

Результат довизначення операції двораундового кодування

	$F_{3,10}=\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}$	$F_{12,5}=\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}$	$F_{10,3}=\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}$	$F_{5,12}=\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}$
$F_{3,10}=\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}$	$F_{3,10}(F_{3,10})=\begin{bmatrix}x_1\\ x_2\end{bmatrix}$	$F_{3,10}(F_{12,5})=\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}$	$F_{3,10}(F_{10,3})=\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}$	$F_{3,10}(F_{5,12})=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$
$F_{12,5}=\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}$	$F_{12,5}(F_{3,10})=\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}$	$F_{12,5}(F_{12,5})=\begin{bmatrix}x_1\\ x_2\end{bmatrix}$	$F_{12,5}(F_{10,3})=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$	$F_{12,5}(F_{5,12})=\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}$
$F_{10,3}=\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}$	$F_{10,3}(F_{3,10})=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$	$F_{10,3}(F_{12,5})=\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}$	$F_{10,3}(F_{10,3})=\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}$	$F_{10,3}(F_{5,12})=\begin{bmatrix}x_1\\ x_2\end{bmatrix}$
$F_{5,12}=\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}$	$F_{5,12}(F_{3,10})=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$	$F_{5,12}(F_{12,5})=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$	$F_{5,12}(F_{10,3})=\begin{bmatrix}x_1\\ x_2\end{bmatrix}$	$F_{5,12}(F_{5,12})=\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}$

Як видно із табл. 4 повторне виконання операцій криптографічного кодування приводить до невідповідності результатів кодування критерію строгого лавинного ефекту, а в випадках $F_{3,10}(F_{3,10})$, $F_{12,5}(F_{12,5})$, … до розкодування інформації, в випадках $F_{12,5}(F_{3,10})$, $F_{3,10}(F_{12,5})$ … до інверсії вхідної інформації. Виходячи з цього, можна стверджувати, що операції криптографічного кодування, які відповідають критерію строгого лавинного ефекту доцільно використовувати лише в одному раунді шифрування.

Висновки. Досліджено дворозрядні операції криптографічного кодування на відповідність критерію строгого лавинного ефекту. Розглянуто особливості використання дворозрядних операцій криптографічного кодування, які відповідають критерію строгого лавинного ефекту, в криптоалгоритмах. В операціях, які відповідають критерію строгого стійкого кодування, зміна одного розряду вхідної інформації приводить до зміни одного розряду результату, тобто до зміни вихідних бітів з ймовірністю ½.

Результат виконання операцій криптографічного кодування в другому раунді не відповідає критерію строгого стійкого кодування, отже, такі операції доцільно використовувати в одному раунді шифрування.

ЛІТЕРАТУРА

1. Richard A. Mollin, «Codes: the guide to secrecy from ancient to modern times», Chapman & Hall/CRC, 2005. – С. 142.
2. Thomas W. Cusick, Pantelimon Stanica, Pantelimon Stănică. Cryptographic Boolean Functions and Applications. – Academic Press, 2009. – С. 25.
3. Isl Vergili, Melek D. Yucel. // Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen n X n S-Boxes. – Turk J Elec Engin, 2001. – С. 137.

В. М. Рудницкий,
Черкасский государственный технологический университет,
г. Черкассы, Украина
Л. А. Шувалова,
Черкасский государственный технологический университет,
г. Черкассы, Украина
О. Б. Нестеренко,
Черкасский институт пожарной безопасности
им. героев Чернобыля НУЦЗ Украины,
г. Черкассы, Украина

АНАЛИЗ ДВОРОЗРЯДНИХ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО КОДИРОВАНИЯ ПО КРИТЕРИЮ СТРОГОГО ЛАВИННОГО ЭФФЕКТА

В статье определено множество двухразрядных операций криптографического кодирования, которые отвечают критерию строгого лавинного эффекта и рассмотрены особенности их использования в криптоалгоритмах. Рассмотрена возможность достижения строгого лавинного эффекта операциями которые отвечают критерию строгого устойчивого кодирования, для чего представлена последовательность наборов двухразрядных данных такую, чтобы два соседних набора, а также первый и последний наборы отличались только одним разрядом.

Ключевые слова: *лавинный эффект; криптографическое кодирование; строгое стойкое кодирование.*

V. M. Rudnitsky,
Cherkasy state technological University,
Cherkassy, Ukraine
L. A. Shuvalova,
Cherkasy state technological University,
Cherkassy, Ukraine
O. B. Nesterenko,
Cherkasy Institute of fire safety named heroes
of Chernobyl NUCS Ukraine,
Cherkassy, Ukraine

ANALYSIS DORASDADDY OPERATIONS OF CRYPTOGRAPHIC ENCODING ACCORDING TO THE CRITERION OF THE STRICT AVALANCHE EFFECT

The article identifies many double operations cryptographic encoding which meet the criteria of strict avalanche effect, and the peculiarities of their use in cryptographic algorithms. The possibility of achieving the strict avalanche effect transactions which meet the strict criteria of sustainable encoding for which the sequence of sets double data such that the two adjacent sets, as well as the first and last sets differed only by one digit.

Key words: *avalanche effect of cryptographic coding; strict coding.*

Рецензенти: д. т. н., проф. ***М. П. Мусієнко;***
к. т. н., доц. ***І. М. Журавська.***

Дата надходження статті до редколегії 05.04.16