УДК 003.26:004.056.55 **doi: 10.26906/SUNZ.2018.1.127**

Н.В. Лада, С.Г. Козловська

Черкаський державний технологічний університет, Черкаси

ЗАСТОСУВАННЯ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ДОДАВАННЯ ЗА МОДУЛЕМ ДВА З ТОЧНІСТЮ ДО ПЕРЕСТАНОВКИ В ПОТОКОВИХ ШИФРАХ

В статті досліджено та оцінено ефективність застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах. Розроблено метод підвищення надійності потокового шифрування на основі застосування операцій криптографічного додавання за модулем два з точністю до перестановки.

Ключові слова: *захист інформації, потокові шифри, синтез операцій криптографічного додавання, надійність криптоперетворення.*

Вступ

Постановка проблеми. В сучасному високоінформатизованому суспільстві все більш гострою стає проблема ефективного захисту інформації, як на рівні персональних даних, так і держави вцілому. Одними з найкращих методів захисту інформації були і залишаються криптографічні методи. Але для успішної протидії зловмисникам, кваліфікація і можливості яких зростають, криптографія також потребує постійного вдосконалення.

Вдосконалення та створення нових методів криптографічного захисту інформації в наш час ведеться за багатьма напрямами: збільшення довжини ключа, покращення гамуючої послідовності, збільшення спектру різноманітних операцій, що можуть бути використані при крипто перетвореннях, тощо. Серед напрямків розвитку криптографії можна виділити побудову операцій криптографічного перетворення на основі застосування логічної функції, які забезпечують побудову високошвидкісних криптографічних примітивів. Проте на сьогоднішній день дані операції розроблялися орієнтовано на блочне шифрування. Спеціалізованим операціям для потокового шифрування достатньо уваги не приділялося. Враховуючи вище зазначене, актуальною постає проблема розробки методу підвищення надійності потокового шифрування на основі розширення множини функцій криптоперетворення за рахунок модифікацій операцій криптографічного додавання за модулем два.

Аналіз останніх досліджень і публікацій. У роботах [1] синтезовано і проаналізовано модифікації базової операції криптографічного додавання за модулем два для криптографічного перетворення зі збереженням інформативності.

У роботах [2, 3] представлені результати дослідження щодо використання операцій додавання за модулем два та перестановки для реалізації матричних операцій криптоперетворення, а також виявлено, що взаємозв'язки між операціями, що застосовуються для криптографічного перетворення на основі матричних моделей, характеризуються циклічністю. В роботі [4] на основі обчислювального експерименту по моделюванню прямих і обернених операцій криптоперетворення для використання в матричних алгоритмах проведено аналіз і дослідження взаємозв'язків між прямими та оберненими матричними моделями операцій криптоперетворення інформації, а також доведена коректність їх використання. В роботах [5, 6] узагальнені результати дослідження щодо виконання модифікованих операцій додавання за модулем два з точністю до перестановки, наведено методику синтезу повної групи даних операцій та технологію їх досліджень. Проте в даних роботах відсутня оцінка ефективності застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах, а також не досліджено підвищення надійності потокового шифрування на основі застосування операцій криптографічного додавання за модулем два з точністю до перестановки.

Мета роботи – розробити метод підвищення надійності потокового шифрування на основі застосування операцій криптографічного додавання за модулем два з точністю до перестановки.

Основний матеріал

Дослідимо ефективність застосування повної групи синтезованих модифікацій операцій додавання за модулем два з точністю до перестановки. Всі зазначені операції побудовані на базі однієї операції додавання за модулем два шляхом перестановки операндів та результатів виконання операції і мають однакові властивості.

Математичні моделі даних операцій представлені в табл. 1, де $x_{1.i}, x_{2.j} \in \{0,1\}$ – розряди інформації відповідно, $i, j \in \{1,2\}$, $\oplus$ – операція додавання за модулем два; $P^{op}_{(0123)}$ – перестановка операндів операції, (0123) – варіант перестановки операндів.

Розглянемо можливість використання синтезованої група модифікацій операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах.

Таблиця 1

Математичні моделі модифікацій операцій додавання за модулем два з точністю до перестановки

$P^{op}_{(0123)}(O_1^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.1} \\ x_{1.2}\oplus x_{2.2}\end{vmatrix}$	$P^{op}_{(1032)}(O_1^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.1} \\ x_{1.2}\oplus x_{2.2}\oplus 1\end{vmatrix}$	$P^{op}_{(2301)}(O_1^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.1}\oplus 1 \\ x_{1.2}\oplus x_{2.2}\end{vmatrix}$	$P^{op}_{(3210)}(O_1^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.1}\oplus 1 \\ x_{1.2}\oplus x_{2.2}\oplus 1\end{vmatrix}$
$P^{op}_{(0213)}(O_2^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.2} \\ x_{1.2}\oplus x_{2.1}\end{vmatrix}$	$P^{op}_{(1302)}(O_2^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.2} \\ x_{1.2}\oplus x_{2.1}\oplus 1\end{vmatrix}$	$P^{op}_{(2031)}(O_2^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.2}\oplus 1 \\ x_{1.2}\oplus x_{2.1}\end{vmatrix}$	$P^{op}_{(3120)}(O_2^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.2}\oplus 1 \\ x_{1.2}\oplus x_{2.1}\oplus 1\end{vmatrix}$
$P^{op}_{(0123)}(O_3^{\oplus})=\begin{vmatrix} x_{1.2}\oplus x_{2.1} \\ x_{1.1}\oplus x_{2.2}\end{vmatrix}$	$P^{op}_{(1032)}(O_3^{\oplus})=\begin{vmatrix} x_{1.2}\oplus x_{2.1} \\ x_{1.1}\oplus x_{2.2}\oplus 1\end{vmatrix}$	$P^{op}_{(2301)}(O_3^{\oplus})=\begin{vmatrix} x_{1.2}\oplus x_{2.1}\oplus 1 \\ x_{1.1}\oplus x_{2.2}\end{vmatrix}$	$P^{op}_{(3210)}(O_3^{\oplus})=\begin{vmatrix} x_{1.2}\oplus x_{2.1}\oplus 1 \\ x_{1.1}\oplus x_{2.2}\oplus 1\end{vmatrix}$
$P^{ro}_{(0213)}(O_4^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.1} \\ x_{1.2}\oplus x_{2.2}\end{vmatrix}$	$P^{ro}_{(1302)}(O_4^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.1} \\ x_{1.2}\oplus x_{2.2}\oplus 1\end{vmatrix}$	$P^{ro}_{(2031)}(O_4^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.1}\oplus 1 \\ x_{1.2}\oplus x_{2.2}\end{vmatrix}$	$P^{ro}_{(3120)}(O_4^{\oplus})=\begin{vmatrix} x_{1.1}\oplus x_{2.1}\oplus 1 \\ x_{1.2}\oplus x_{2.2}\oplus 1\end{vmatrix}$

Структурна схема потокового шифрування наведена на рис. 1. Для забезпечення можливості реалізації групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки необхідно проводити додатковий випадковий вибір модифікації операції для кожного елементарного перетворення на основі гамуючої послідовності. Структурна схема потокового шифрування з використанням групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки наведена на рис. 2.

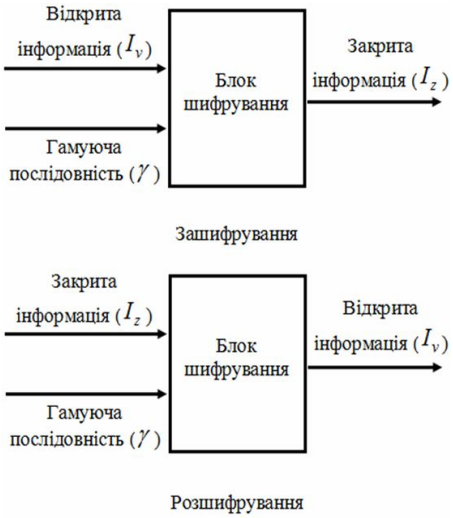

Рис. 1. Структурна схема потокового шифрування

Проведемо оцінку надійності потокового шифрування за допомогою запропонованої схеми, порівняно з класичною. Нехай подія A – правильне функціонування і наявність відкритої вхідної інформації, тоді $\overline{A}$ – відсутність відкритої вхідної інформації, подія B – наявність першої гамуючої послідовності, тоді $\overline{B}$ – відсутність першої гамуючої послідовності, подія C – наявність другої гамуючої послідовності, тоді $\overline{C}$ – відсутність другої гамуючої послідовності. Результати порівняльного аналізу схем потокового зашифрування наведені в табл. 2.

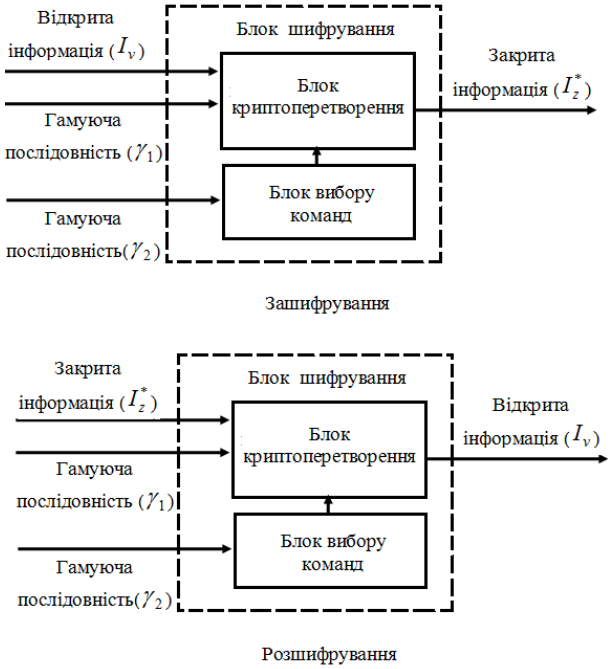

Рис. 2. Структурна схема потокового шифрування з використанням групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки

Таблиця 2

Результати порівняльного аналізу схем потокового зашифрування

Потокове шифрування	Вхідні канали			Вихідний канал	Коментар за результатами шифрування
	I_v	γ_1	γ_2		
Із використанням однієї операції (рис. 1)	+	+		I_z	Зашифрована інформація
	+	-		I_v	Незашифрована інформація (витік інформації)
	-	+		γ_1	Гамуюча послідовність, (створена передумова до зламу ключа)
	-	-		-	Вихідна інформація відсутня
Із використанням групи операцій (рис. 2)	+	+	+	I_z^*	Зашифрована інформація з покращеною якістю щифрування
	+	+	- (+)	I_z	Зашифрована інформація
	+	-	-	I_v	Незашифрована інформація (витік інформації)
	-	+	+	$\gamma_2(\gamma_1)$	Зашифрована гамуюча послідовність
	-	+ (-)	- (+)	γ_1 або γ_2	Гамуюча послідовність, (створена передумова до зламу ключа)
	-	-	-	-	Вихідна інформація відсутня

Повна група подій відмов вхідних каналів схеми потокового шифрування (рис. 1) буде такою:

$$A\,B \quad A\,\bar{B} \quad \bar{A}\,B \quad \bar{A}\,\bar{B}.$$

Повна група подій відмов вхідних каналів схеми потокового шифрування з використанням групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки (рис. 2) буде такою:

$$A\,B\,C \quad A\,B\,\bar{C} \quad A\,\bar{B}\,C \quad A\,\bar{B}\,\bar{C}$$
$$\bar{A}\,B\,C \quad \bar{A}\,B\,\bar{C} \quad \bar{A}\,\bar{B}\,C \quad \bar{A}\,\bar{B}\,\bar{C}.$$

Розглянемо вихідні події. Нехай подія D – правильне функціонування і наявність закритої вихідної інформації, тоді $\bar{D}$ – неправильне функціонування, що приведе до витоку інформації чи відсутності можливості розшифрувати закриту вихідну інформацію. Нехай подія D_+ – правильне функціонування і наявність закритої вихідної інформації з покращеною якістю шифрування. Нехай подія W – неправильне функціонування пристрою через відмову вхідних каналів, що привело до повтору на його виході незашифрованої інформації, створивши тим самим передумову витоку інформації. Нехай подія G – неправильне функціонування пристрою через відмову вхідних каналів, що привело до повтору на його виході гамуючої послідовності, створивши тим самим передумову до зламу ключа. Нехай подія H – неправильне функціонування пристрою через відмову вхідних каналів, що привело до формування на виході зашифрованої гамуючої послідовності, не створивши передумову до зламу ключа. Нехай подія F – неправильне функціонування пристрою через відмову вхідних каналів, що привело до створення передумови витоку інформації чи зламу ключа.

Оцінимо ймовірність виникнення вихідних подій за умови рівномірного розподілу вхідних відмов (вхідних подій). Для цього розглянемо взаємозв'язки між вхідними і вихідними подіями для повної групи вхідних подій. Взаємозв'язки між вхідними і вихідними подіями наведено у табл. 3.

Таблиця 3

Взаємозв'язки між вхідними і вихідними подіями

Потокове шифрування	Вхідні події	Вихідні події						
		D	$\bar{D}$	D_+	W	H	G	F
Із використанням однієї операції (рис. 1)	A B	+	–		–		–	
	A $\bar{B}$	–	+		+		–	+
	$\bar{A}$ B	–	+		–		+	+
	$\bar{A}$ $\bar{B}$	–	+		–		–	
Із використанням групи операцій (рис. 2)	A B C	+	–	+	–	–	–	–
	A B $\bar{C}$	+	–	–	–	–	–	–
	A $\bar{B}$ C	+	–	–	–	–	–	–
	$\bar{A}$ B C	–	+	–	–	+	–	–
	A $\bar{B}$ $\bar{C}$	–	+	–	+	–	–	+
	$\bar{A}$ B $\bar{C}$	–	+	–	–	–	+	+
	$\bar{A}$ $\bar{B}$ C	–	+	–	–	–	+	+
	$\bar{A}$ $\bar{B}$ $\bar{C}$	–	+	–	–	–	–	–

На основі табл. 4 можна встановити таке:

ймовірність правильного функціонування запропонованого пристрою буде більшою, оскільки

$$P_D(ABC) = 3/8 > P_D(AB) = 1/4,$$

що забезпечить збільшення надійності до 12,5 %;

ймовірність правильного функціонування запропонованого пристрою і наявність закритої вихідної інформації з покращеною якістю шифрування буде більшою, оскільки

$$P_{D_+}(ABC) = 1/8 > P_{D_+}(AB) = 0;$$

ймовірність неправильного функціонування пристрою через відмови вхідних каналів, що призвело до повтору на його виході незашифрованої інформації, буде меншою, оскільки

$$P_W(ABC) = 1/8 < P_W(AB) = 1/4;$$

ймовірність неправильного функціонування пристрою через відмови вхідних каналів, що призвело до передумов зламу ключа, не зміниться, бо

$$P_G(ABC) = 2/8 = P_G(AB) = 1/4;$$

ймовірність додаткового захисту гамуючої послідовності при виникненні відмов вхідних каналів запропонованого пристрою буде більшою, оскільки

$$P_H(ABC) = 1/8 > P_H(AB) = 0;$$

ймовірність неправильного функціонування пристрою через відмови вхідних каналів, що призвело до створення передумови витоку інформації чи зламу ключа, буде визначатися як $P_F = P_W + P_G$, і для запропонованого пристрою буде меншою, оскільки

$$P_F(ABC) = 3/8 < P_F(AB) = 2/4.$$

Проте на практиці ймовірність події одночасного виникнення двох відмов набагато більша за ймовірність однієї відмови. При паралельному функціонуванні пристроїв відмова одного з них не призводить до неправильного функціонування іншого.

Оцінимо і порівняємо ймовірнісні показники роботи пристрою при виникненні однієї відмови в каналах вхідної інформації.

ймовірність правильного функціонування запропонованого пристрою буде більшою, так як

$$P_D^*(ABC) = 3/4 > P_D^*(AB) = 1/3,$$

що забезпечить збільшення надійності до 41,6 %;

ймовірність правильного функціонування запропонованого пристрою і наявність закритої вихідної інформації з покращеною якістю шифрування буде більшою, оскільки

$$P_{D_+}^*(ABC) = 1/4 > P_{D_+}^*(AB) = 0;$$

ймовірність неправильного функціонування пристрою через відмови вхідних каналів, що призвело до повтору на його виході незашифрованої інформації, буде дорівнювати нулю:

$$P_W^*(ABC) = 0 < P_W^*(AB) = 1/3;$$

ймовірність неправильного функціонування пристрою через відмови вхідних каналів, що при-

звело до передумов зламу ключа, буде дорівнювати нулю:

$$P_G^*(ABC) = 0 < P_G^*(AB) = 1/3;$$

ймовірність додаткового захисту гамуючої послідовності при виникненні відмов вхідних каналів запропонованого пристрою буде більшою, оскільки

$$P_H^*(ABC) = 1/4 > P_H^*(AB) = 0;$$

ймовірність неправильного функціонування пристрою при однократних відмовах вхідних каналів, які призводять до створення передумови витоку інформації чи зламу ключа, буде дорівнювати нулю, оскільки

$$P_F^*(ABC) =$$

$$= P_W^*(ABC) + P_G^*(ABC) = 0 < P_F^*(AB) = 1/2.$$

За результатами порівняння можна зробити висновок, що використання групи операцій додавання за модулем два з точністю перестановки на основі додаткової гамуючої послідовності забезпечить підвищення якості шифрування і надійності роботи, а при однократних відмовах каналів вхідної інформації – виключить можливість створення передумови витоку інформації чи зламу ключа.

Слід зазначити, що при реалізації даного підходу виникає необхідність збільшення ключової послідовності для забезпечення генерації другої гамуючої послідовності, що, в свою чергу, приведе до збільшення не тільки теоретичної, а й практичної стійкості (збільшення довжини ключа).

Отримані результати дозволяють сформулювати метод підвищення стійкості й надійності потокового шифрування, який полягає у виборі для кожного етапу шифрування модифікацій операції за модулем два з точністю до перестановки на основі додаткової гамуючої послідовності, що виключить, при однократних відмовах, можливість витоку інформації чи спрощення зламу ключа.

Висновки

В статті здійснено аналіз результатів використання операцій додавання за модулем два з точністю до перестановки в потоковому шифруванні. Розроблено метод підвищення надійності потокового шифрування, який полягає у виборі для кожного етапу шифрування модифікацій операції за модулем два з точністю до перестановки на основі додаткової гамуючої послідовності, що виключить, при однократних відмовах, можливість витоку інформації чи спрощення зламу ключа.

Список літератури

1. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 2 (118). С. 116–118.

2. Бабенко В. Г., Лада Н. В., Лада С. В. Дослідження взаємозв'язків між операціями в матричних моделях криптографічного перетворення. Вісник Черкаського державного технологічного університету. 2016. № 1. С. 5–11.

3. Бабенко В. Г., Лада Н. В., Лада С. В. Аналіз множин операцій, синтезованих на основі додавання за модулем два. Методи та засоби кодування, захисту й ущільнення інформації: тези доп. П'ятої міжнар. наук.-практ. конф., (Вінниця, 19–21 квіт. 2016). Вінниця: Ніланлтд, 2016. С. 54–57.

4. Лада Н. В. Аналіз коректності взаємозв'язків між прямими та оберненими матричними моделями операцій криптографічного перетворення інформації. Системи управління, навігації та зв'язку: Полтава : ПНТУ, 2015. - Вип. 4 (36). - С. 73-78.

5. Бабенко В. Г., Лада Н. В. Аналіз результатів виконання модифікованих операцій додавання за модулем два з точністю до перестановки. The scientific potential of the present: proceedings of the Internat. sci. conf., (St. Andrews, Scotland, UK, December, 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogalska I. O., 2016. С. 108–111. (Шотландия, Логос)

6. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій за модулем два. Smart and Young: щомісячний наук. журн. 2016. № 11–12. Ч. 1. С. 49–54.

Надійшла до редколегії 27.12.2017

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет імені М.Є. Жуковського «ХАІ», Харків.

ПРИМЕНЕНИЕ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО СЛОЖЕНИЯ ПО МОДУЛЮ ДВА С ТОЧНОСТЬЮ ДО ПЕРЕСТАНОВКИ В ПОТОКОВЫХ ШИФРАХ

Н.В. Лада, С.Г. Козловская

В статье исследовано и оценено эффективность применения операций криптографического сложения по модулю два с точностью до перестановки в потоковых шифрах. Разработан метод повышения надежности потокового шифрования на основе применения операций криптографической сложение по модулю два с точностью до перестановки.

Ключевые слова: *защита информации, потоковые шифры, синтез операций криптографического сложения, надежность криптопреобразования.*

APPLYING CRYPTOGRAPHIC ADDITION OPERATIONS BY MODULE TWO WITH ACCURACY OF PERMUTATION IN STREAM CIPHERS

N.V. Lada, S.H. Kozlovska

The paper studies and evaluates the effectiveness of applying cryptographic addition operations by module two with accuracy of permutation in stream ciphers. The method of increasing reliability of streaming encryption based on the use of cryptographic addition operations by module two with accuracy of permutation is developed.

Keywords: *information security, stream ciphers, synthesis of cryptographic addition operations, reliability of cryptographic transformation.*