УДК 004.056.5 Столович М.В. (КПІ ім. Ігоря Сікорського)
к.т.н. Яковлєв С.В. (ВІТІ)

ПОБУДОВА РОЗПІЗНАВАЧІВ „КАЛИНА”-ПОДІБНИХ ШИФРІВ НА ОСНОВІ ЇХ АЛГЕБРАЇЧНИХ ТА СТРУКТУРНИХ ВЛАСТИВОСТЕЙ

Державний стандарт ДСТУ 7624:2014 (шифр «Калина») є стандартом симетричного блокового шифрування України. Дослідження структурних та алгебраїчних властивостей даного шифру є актуальною темою з точки зору укріплення безпеки держави. Одним із методів аналізу шифруючого перетворення є знаходження таких властивостей (структурних та алгебраїчних), на основі яких можливо побудувати розпізнавачі шифру, який досліджується. Це дозволяє краще вивчити структуру перетворення, виявити як сильні, так і слабкі сторони шифру, які в майбутньому потрібно посилити. Одним із новітніх методів побудови розпізнавачів для симетричних блокових шифрів є метод аналізу перетворень ланцюгів підпросторів. Цей метод є узагальненням методу інваріантних підпросторів шифруючого перетворення. У роботі розглянуто застосування даного методу для «Калина»-подібних шифрів. Задля спрощення аналізу усі операції додавання за модулем 2^{64}, які присутні в оригінальному шифрі, були замінені на операції додавання за модулем 2. Представлено знайдені ланцюги підпросторів та доведено ряд тверджень, необхідних для застосування даного методу до модифікованого шифру «Калина». Представлено алгоритм побудови розпізнавачів для модифікованих шифрів «Калина» із зменшеною кількістю раундів на основі властивостей розповсюдження ланцюгів підпросторів. Отримано оцінки ефективності побудови таких розпізнавачів.

Столович М.В., Яковлев С.В. Распознаватели «Калина»-подобных шифров на основе их алгебраических и структурных свойств.

Государственный стандарт ДСТУ 7624:2014 (шифр «Калина») является стандартом симметричного блочного шифрования Украины. Исследование структурных и алгебраических свойств данного шифра является актуальной темой с точки зрения укрепления безопасности государства. Одним из методов анализа шифрующего преобразования является нахождение таких свойств (структурных и алгебраических), на основе которых возможно построить распознаватели шифра, который исследуется. Это позволяет лучше изучить структуру преобразования, выявить как сильные, так и слабые стороны шифра, которые в будущем нужно усилить. Одним из новейших методов построения распознавателей для симметричных блочных шифров является метод анализа преобразований цепочек подпространств. Этот метод является обобщением метода инвариантных подпространств шифрующего преобразования. В работе рассматривается применение данного метода для «Калина»-подобных шифров. Для упрощения анализа все операции сложения по модулю 2^{64}, которые присутствуют в оригинальном шифре, были заменены на операции сложения по модулю 2. Представлено найденные цепи подпространств и доказано ряд утверждений, необходимых для применения данного метода к модифицированному шифру «Калина». Представлен алгоритм построения распознавателей для модифицированных шифров «Калина» с уменьшенным количеством раундов на основе свойств распространения цепочек подпространств. Также были получены оценки эффективности построения таких распознавателей.

M. Stolovych, S. Yakovliev. Distinguishers of "Kalyna"-like ciphers based on their algebraic and structural properties.

State standard DSTU 7624: 2014 (“Kalyna” cipher) is a standard of symmetric block encryption of Ukraine. The study of structural and algebraic properties of the cipher is an essential issue in terms of strengthening the security of the State. One of the methods of analyzing the properties of the encryption transformation is to find such properties (structural and algebraic) based on which it is possible to build distinguishers of the studied cipher. This allows us to better study the structure of the transformation, to identify both strengths and weaknesses of the cipher, which need to be strengthened in the future. One of the newest methods of constructing distinguishers for symmetric block ciphers is the method of subspace trails analysis. This method is a generalization of the method of invariant subspaces of encryption transformation. In this paper, we consider the application of this method for “Kalyna”-like ciphers. To simplify the analysis, all additions modulo 2^{64}, which are present in the original cipher, were replaced by additions modulo 2 (XORs). We present found subspace trails and prove the necessary claims for this method application to the modified “Kalyna” cipher. We present an algorithm for constructing distinguishers for modified “Kalyna”-like ciphers with a reduced number of rounds using the propagation properties of subspace trails. Efficiency estimations for constructing of such distinguishers are also presented.

Ключові слова: *блоковий шифр, розпізнавачі, перетворення ланцюгів підпросторів, шифр «Калина».*

Постановка завдання

Багато сучасних симетричних шифрів побудовано із застосуванням принципу замішування структурних та алгебраїчних властивостей відкритого тексту та ітеративного застосування шифруючого перетворення, щоб зашифрований текст виглядав як набір випадкових символів. Завдяки такому підходу у побудові шифруючих перетворень більшість

сучасних шифрів є практично незламними. Через це значну увагу зараз приділяють глибинному аналізу структури шифруючих перетворень.

Одним із способів дослідження структури шифруючого перетворення є побудова розпізнавачів шифрів. Розпізнавач – це алгоритм, завдяки якому ми можемо відповісти на питання, чи є даний текст шифротекстом, одержаним у результаті роботи відповідного шифру, або випадковою послідовністю бітів. Сучасні симетричні шифри в більшості випадків мають ітеративну структуру, яка має таку властивість: якщо невірно підібрати раундовий ключ під час аналізу, то «розшифрування» на такому ключі рівноцінно зашифруванню тексту ще на один раунд. Правильно побудований розпізнавач шифру також дозволить відповісти, чи правильно був підібраний раундовий ключ.

Одним із сучасних методів побудови розпізнавачів симетричних шифрів є метод, який використовує перетворення ланцюгів підпросторів. У роботі ми розглянемо застосування даного методу для побудови розпізнавачів „Калина”-подібних шифрів. Буде розглянуто модифікацію державного стандарту блокового шифрування ДСТУ 7624:2014 [1] без додавання за модулем 2^{64} та із зменшеною кількістю раундів перетворення.

Аналіз публікацій за темою дослідження

Криптоаналіз на основі аналізу перетворень ланцюгів підпросторів вперше було розглянуто Лоренцо Грассі, Крістіаном Рехбергергом та Сондре Рьонйомом [2] у застосування до шифру AES. У роботах [2 – 4] побудовано декілька розпізнавачів різних типів для усічених версій шифру AES із 2, 3 та 4 раундами перетворень.

Атаку на основі аналізу ланцюгів підпросторів можна розглядати як узагальнену атаку на основі інваріантних підпросторів шифруючого перетворення. Ланцюгове перетворення підпросторів вхідних текстів розглядається як оператор, який визначається послідовністю підпросторів текстів та послідовно видображує лінійні многовиди (або лінійні зсуви підпросторів) станів шифрування упродовж деякої кількості раундів. Ланцюги підпросторів зазвичай визначаються підпросторами, розмірність яких збільшується під час застосування шифруючого перетворення. Хоча розмірності підпросторів постійно зростають, за умови малої розмірності стартового підпростору відносно розміру блоку можна побудувати достатньо довгий ланцюг, який буде накривати багато раундів.

Підпростори, аналогічні за структурою до підпросторів шифру AES, було представлено для модифікованого шифру „Калина” [6].

Метою даної роботи є побудова розпізнавачів на основі аналізу перетворень ланцюгів підпросторів для модифікованого шифру «Калина» та оцінка стійкості шифру до побудови розпізнавачів цим методом.

Виклад основного матеріалу

Шифр „Калина” – це державний стандарт блокового шифрування України, який було розроблено вітчизняними спеціалістами та обрано в результаті конкурсу. Його структура дуже подібна до шифру AES.

Блок шифрування представляє собою матрицю елементів поля F_2^8 розміром $8xN$. Далі будемо позначати матрицю стану як елемент F_2^{n*m}, де n – це кількість стовпчиків, а m – кількість рядків. Залежність кількості раундів від розміру вхідного блоку можна побачити у таблиці 1.

Алгоритм шифрування шифру „Калина” складається з таких операцій: додавання раундового ключа за модулем 2^{64}, нелінійне відображення ($SubBytes$), зсув елементів (ShiftRows), лінійне перетворення ($MixColumns$). Детальніше шифр описано у [1, 2].

У оригінальному шифрі „Калина” усі операції додавання ключа виконуються за модулем 2, окрім додавання раундового ключа за модулем 2^{64} спочатку та в кінці шифрування. У подальшому ми розглядаємо модифікацію шифру „Калина”, де усі операції проводяться за модулем 2. Ми будемо називати ці модифікації „Калина”-128, „Калина”-256, „Калина” -512 відповідно до розміру блоку шифрування.

Таблиця 1

Залежність кількості ітерацій від розміру блоків для шифру „Калина”

Розмір блоку	Довжина ключа	Кількість ітерацій
128	128	10
	256	14
256	256	14
	512	18
512	512	18

Далі позначимо R як раундову функцію ітеративного блокового шифру і нехай $(V_1, V_2, \dots, V_{r+1})$ позначає послідовність з $r + 1$ підпростору, де $dim(V_i) \leq dim(V_{i+1})$. Якщо для кожного $i = 1, \dots, r$ та для будь-якого a_i існує a_{i+1}такий, що $R(V_i \oplus a_i) \subseteq V_{i+1} \oplus a_{i+1}$, тоді $(V_1, V_2, \dots, V_{r+1})$ — це ланцюг підпросторів довжини r для функції R. Нехай R^t позначає застосування t раундів із фіксованими ключами, тоді в термінах підпросторів $R^t(V_1 \oplus a_1) \subseteq V_{t+1} \oplus a_{t+1}$.

Далі визначимо типові підпростори, які використовуються при побудові множини текстів для використання розпізнавачем за даним методом [2, 6].

Нехай I – це множина індексів стовпчиків матриці стану шифрування. Типовими підпросторами для $i \in I$ є:

– стовпчиковий підпростір C_i, який визначається як $C_i = \langle e_{0,i}, e_{1,i}, \dots, e_{j-1,i} \rangle$, де j – це кількість рядків у матриці стану;

– зсунутий підпростір D_i, який визначається як $D_\text{i} = ShiftRows^{-1}(C_i)$;

– інверсно-зсунутий підпростір ID_i, який визначається як $ID_i = ShiftRows(C_i)$;

– змішаний простір M_i, який визначається як $M_i = MixColumns(ID_i)$.

На рисунку 1 представлено приклади типічних підпросторів для шифру AES, а на рисунку 2 представлені приклади типічних підпросторів для шифру „Калина”.

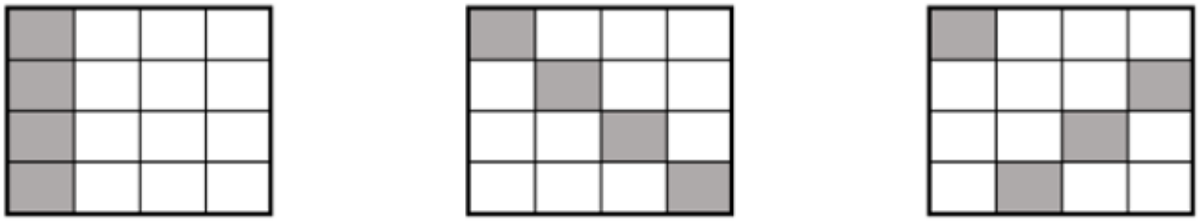

Рис 1. Схематичне зображення елементів підпросторів C_0, D_0, ID_0 для шифру AES

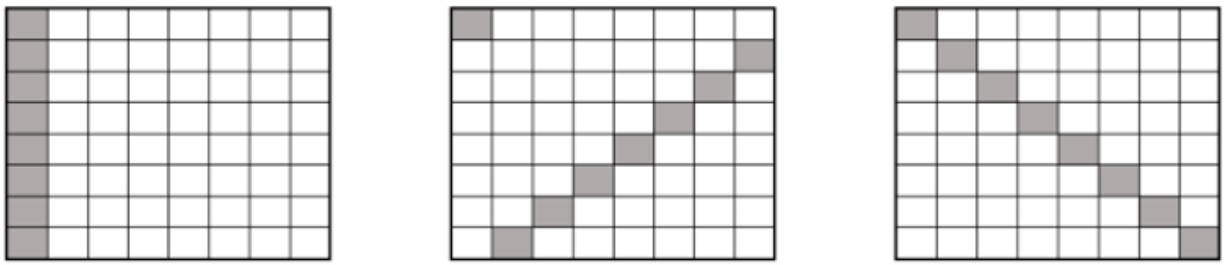

Рис. 2 Схематичне зображення елементів підпросторів C_0, D_0, ID_0 для шифру «Калина»

Розглянемо аналогічні підпростори C_I, D_I, ID_I, M_I тільки для множини індексів I. Визначимо їх таким чином:

$$C_I = \oplus_{i \in I} C_i, \quad D_I = \oplus_{i \in I} D_i,$$
$$ID_I = \oplus_{i \in I} ID_i, \quad M_I = \oplus_{i \in I} M_i.$$

Ортогональне доповнення підпростору $D_I^{\perp}$ – це підпростір векторів, всі вектори в якому є ортогональними до всіх векторів у певному підпросторі D_I. Наступна теорема показує, яким чином раундова функція змінює вид підпростору.

Теорема 1 ([2]). Для множини індексів стовпчиків $I \subset \{0,\dots,j\}$ та для кожного $a \in D_I^{\perp}$ існує єдиний елемент $b \in C_I^{\perp}$, так що $R(D_I \oplus a) = C_I \oplus b$.

Лема 1 ([2]). Для усіх $x, y \in F_{2^8}^{n*m}$, де n – це кількість стовпчиків матриці стану, а m – це кількість рядків, та для довільної множини індексів $I \subseteq \{0,..,n\}$ справедлива така рівність: $Pr\{R(x) \oplus R(y) \in C_I | x \oplus y \in D_I\} = 1$.

Інакше кажучи, ми можемо зробити висновок, що для кожного $c \in C_I^{\perp}$, існує тільки один $d \in D_I^{\perp}$, такий що $R^{-1}(C_I \oplus c) = D_I \oplus d$.

В загальному випадку маємо:

$$Pr\{R^{-1}(x) \oplus R^{-1}(y) \in D_I | x \oplus y \in C_I\} = 1.$$

Принцип побудови розпізнавача такий: шифруємо деяку кількість відкритих текстів та очікуємо після першого раунду, що отриманий шифртекст буде належати множині $D_K \cap C_0$, де K – це множина індексів. Далі будемо сприймати цей шифртекст як вхід для 4-раундового шифру. Після цього будемо очікувати із відповідною ймовірністю побачити збереження властивості нульової різниці для шифруючого перетворення.

Далі будемо розглядати побудову розпізнавача для модифікованого 5-раундового шифру „Калина” - 128. Розпізнавачі для інших розмірів шифру можна побудувати за аналогією. Для подальших обчислень нам знадобиться наступна лема.

Лема 2. Для будь-яких підпросторів C_I та D_J та множин індексів I, J для „Калина” 128 вірно наступне твердження:

$$Pr(x \in (C_I \cap D_J) | x \in C_I) = (2^{-8})^{2*|I|-|I|*|J|},$$
$$Pr(x \in (C_J \cap D_I) | x \in D_I) = (2^{-8})^{2*|I|-|I|*|J|}.$$

Розглянемо випадок, коли шифртекст після першого раунда шифрування належить до $D_K \cap C_0$, де $|K| = 1$. Після першого раунда шифрування подія $R(p_i) \oplus R(p_j) \in D_K \cap C_0$, де $|K| = 1$, відбудеться з ймовірністю $((2^4 - 1) + (2^4 - 1)) \cdot (2^{-8}) = 30 \cdot 2^{-8}$. В нас для нульового стовпчика матриці стану $(2^4 - 1) = 15$ варіантів заповнення перших 4-ьох байтів, що відповідає належності матриці стану до простору D_0, та $(2^4 - 1) = 15$ варіантів для останніх 4-ьох байтів, що відповідає належності до простору D_1. Кожний варіант D_K згідно леми 2 має ймовірність $2^{-8}(2 \cdot 1 - 1 \cdot 1) = 2^{-8}$. Якщо ми відповідно до теореми 1 змінимо значення стовпчиків шифртекстів, то

$$R^{-4}(\rho_v(c_i, c_j)) \oplus R^{-4}(\rho_v(c_j, c_i)) \in D_K,$$
$$R^{-4}(\rho_v(c_i, c_j)) \oplus R^{-4}(\rho_v(c_j, c_i)) \in D_K \cap C_L,$$

де із ймовірністю $2 \cdot 2^{-8} |L| = 1$. Це означає, що, згідно леми 2, після ще одного раунда розшифрування два нових відкритих текста p'_j, p'_i будуть належати простору D_L із ймовірністю $30 \cdot 2^{-8} \cdot 2 \cdot 2^{-8} = 30 \cdot 2^{-15} \approx 2^{-10}$.

Приклад розповсюдження диференціальної характеристики, використаної в цьому випадку, зображено на рисунку 3.

Після обрахунків маємо, що ймовірність того, що пара відкритих текстів $p'j \oplus p'i$ належить до C_L, де $|L| = 1$, дорівнює 2^{-10}.

Ймовірність, що пара випадкових відкритих текстів $p'_j \oplus p'_i$ належить до C_L, де $|L| = 1$, дорівнює $\approx 2^{-63}$. Загалом, кількість потрібних текстів дорівнює 2^{12}.

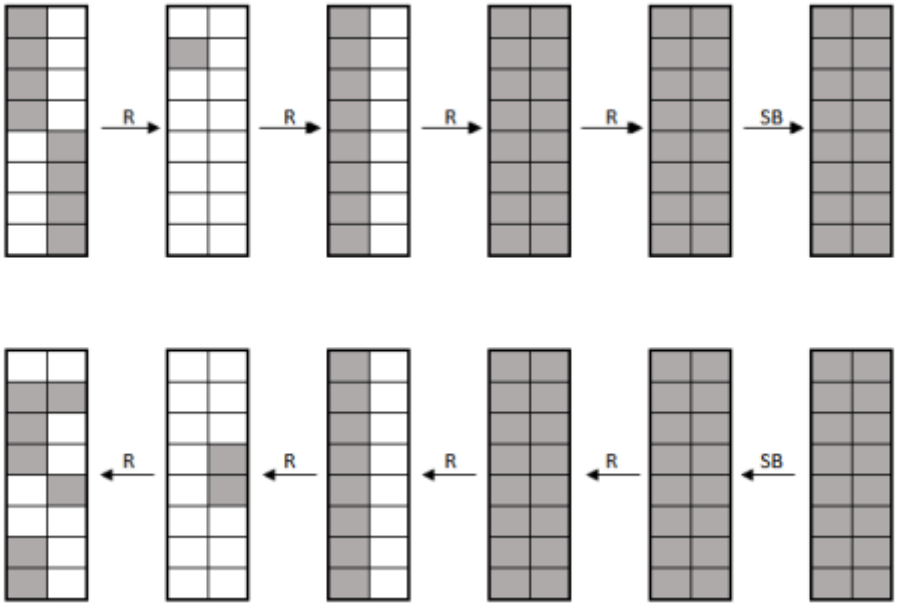

Рис 3. Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 128 при $|K| = 1$

Аналогічним чином ми можемо провести обрахунки для шифрів „Калина”-256 та „Калина”-512. Для них потрібно проаналізувати випадки, коли $|L| \in \{1,2,3\}$ та $|L| \in \{1,..,7\}$ відповідно. Отримані результати можна побачити у таблиці 2.

Алгоритм роботи розпізнавача опишемо таким чином. Беремо в k разів менше текстів, ніж отримали при розрахунках, тому що ми можемо перемішати шифртекст таким чином, що властивість, якщо вона була присутня, не зменшиться. Для шифрів „Калина” із розміром блоку 128, 256 та 512 маємо $k = 2, 7$ та 29 відповідно.

Після генерації потрібної кількості відкритих текстів з D_0 шифруємо їх 5-раундовим шифром та методом заміни стовпчиків матриці стану отримуємо ще додаткові шифртексти для аналізу.

Потім беремо пари c_i, c_j шифртекстів, дешифруємо їх та перевіряємо властивість: $p'_j \oplus p'_i \in D_L$, де $|L| = 1,..,m-1$, m – кількість стовпчиків матриці стану шифрування. Якщо властивість виконується, то це означає, що досліджуване перетворення є модифікованим шифром «Калина». У іншому випадку, якщо для деяких пар текстів властивість не виконалась, тоді із ймовірністю 95 % перед нами випадкова перестановка.

Таблиця 2

Складність побудови розпізнавача для 5-раундового шифру «Калина» із ймовірністю успіху 95%

Версія шифру	Необхідна кількість текстів
«Калина»-128	2^{12}
«Калина»-256	2^{39}
«Калина»-512	2^{55}

Висновки

У роботі було побудовано розпізнавачі „Калина”-подібних шифрів за допомогою аналізу перетворень ланцюгів підпросторів. Для побудови розпізнавача за допомогою цього методу було доведено необхідні теоретичні твердження, що дозволило отримати обґрунтовані оцінки складності побудови таких розпізнавачів. Розпізнавачі було побудовано

для модифікованих шифрів „Калина” із зменшеною кількістю раундів та з заміною операції додавання за модулем 2^{64} на операції додавання за модулем 2.

Побудовані нами розпізнавачі вимагають достатньо невеликої кількості підібраних вхідних текстів для ефективної роботи. Однак слід зазначити, що із-за структури шифруючого перетворення даним способом поки неможливо побудувати розпізнавачі для шифрів, які мають більше п’яти раундів, оскільки із збільшенням кількості раундів втрачаються структурні властивості, які використовуються для побудови розпізнавача.

Напрямками подальших досліджень є пошук нових властивостей, які використовують інваріантні підпростори та перетворення ланцюгів підпросторів шифру „Калина”, та побудова ефективних розпізнавачів „Калина”-подібних шифрів на основі таких властивостей.

ЛІТЕРАТУРА

1. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Держспоживстандарт України, 2015. – 238 с.

2. Oliynykov Roman, Gorbenko Ivan, Kazymyrov Oleksandr et al. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. Cryptology ePrint Archive, Report 2015/650. 2015. https://eprint.iacr.org/2015/650.

3. Grassi Lorenzo, Rechberger Christian, Rønjom Sondre. Subspace Trail Cryptanalysis and its Applications to AES. Cryptology ePrint Archive, Report 2016/592. 2016. https://eprint.iacr.org/2016/592.

4. Grassi Lorenzo. Mixture Differential Cryptanalysis and Structural Truncated Differential Attacks on round-reduced AES. Cryptology ePrint Archive, Report 2017/832. 2017. https://eprint.iacr.org/2017/832.

5. Bardeh Navid Ghaedi, Rønjom Sondre. Practical Attacks on Reduced-Round AES. Cryptology ePrint Archive, Report 2019/770. 2019. https://eprint.iacr.org/2019/770.

6. Коляда М. Ланцюги підпросторів Калина-подібних шифрів / Марія Коляда, Сергій Яковлєв. // Матеріали статей Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерне моделювання» (15-20 травня 2017 р., Івано-Франківськ – Яремче). – Івано-Франківськ: ПНУ ім. В. Стефаника, 2017. – стор. 248 – 251.