УДК 004.056.55

М.О. Полуяненко[1], О.В. Ісаєв[2]

[1] *Харківський національний університет ім. В.Н. Каразіна, Харків*
[2] *Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків*

ОЦІНКА КРИПТОГРАФІЧНОЇ СТІЙКОСТІ РЕГІСТРІВ ЗСУВУ З НЕЛІНІЙНИМИ ЗВОРОТНИМИ ЗВ'ЯЗКАМИ

Розглянуто можливість застосування регістрів зсуву з нелінійними зворотними зв'язками (РЗНЗЗ) другого порядку в якості основного елемента системи потокового симетричного шифрування. Запропоновано систему критеріїв та показників оцінки криптографічної стійкості РЗНЗЗ, на підставі якої зроблено обґрунтовану кількісну оцінку переваги застосування у алгоритмах потокового шифрування РЗНЗЗ замість регістрів зсуву з лінійними зворотними зв'язками. Створену модель оцінки рекомендовано використовувати для комплексної оцінки та науково обґрунтованого рішення щодо доцільності застосування обраної конструкції потокового шифрування.

Ключові слова: *регістри зсуву з нелінійними зворотними зв'язками, РЗНЗЗ, криптографічна стійкість, оцінка стійкості шифрів, потокові шифри, системи шифрування.*

Вступ

Практично всі програмно-апаратні методи захисту інформації нерозривно пов'язані з криптографією [1]. Криптографія існує вже багато століть, проте, в тому вигляді, в якому ми її знаємо і використовуємо зараз, вона налічує кілька десятиліть. Сучасний стрімкий розвиток інформаційних технологій, розвиток електронно-цифрового світу, надання електронних довірчих послуг та постійне зростання обсягу обробки інформації у інформаційно-телекомунікаційних системах різного рівня та призначення потребують застосування та постійного вдосконалення систем захисту інформації, які спроможні забезпечити високий рівень інформаційної безпеки нарівні з високою швидкістю передачі даних по каналах зв'язку.

Визначальним на найближчі роки напрямком розвитку Інтернету буде так звані Інтернет Речі (Internet of Things), прийнятий комісіями Європарламенту і Ради Європи в якості магістрального шляху розвитку інформаційних і Інтернет технологій [2]. Цей напрямок характеризується переходом від Інтернету Персональних Комп'ютерів до Інтернету Речей.

Як зазначається в [3], останні півтора десятка років поряд з традиційними Інтернет-пристроями, такими як персональні комп'ютери, ноутбуки, смартфони, стали з'являтися пристрої побутової техніки, транспорту, а також різні датчики, що мають доступ в Інтернет. Це явище отримало назву «Інтернет Речей». Інтернет Речі являють собою бездротову самоконфігуруючу мережу між об'єктами типу побутових приладів, транспортних засобів, різних сенсорів і датчиків, а також міток радіочастотної ідентифікації (Radio Frequency IDentification, RFID).

Дослідники корпорації Cisco IBSG прогнозують, що до 2020 року до Інтернету буде підключено 50 мільярдів різних пристроїв. В їх число входять радіочастотні мітки, безконтактні смарткарти, SIM-карти, засоби системи глобального мобільного зв'язку, засоби автоматизованих систем управління технологічними процесами (SCADA), бездротові сенсори, в тому числі імплантовані медичні сенсори та інші пристрої (стимулятор мозку, електронний стимулятор серця), електронні паспорти та інші електронні засоби ідентифікації особистості, засоби логістики та інші засоби автоматизації поставок, системи проведення банківських операцій через Інтернет, автоматична оплата мит, послуг, дорожніх та інших зборів, громадський транспорт, боротьба з контрафакцією, протиугінні системи автомобілів, засоби контролю за авіабагажем, бібліотечними книгами, тощо. Додамо до цього численні додатки, пов'язані з обробкою біометричних даних, персональних даних медичного характеру, важливої фінансової інформації та інше.

На фоні вищеперерахованого особливу актуальності набуває завдання ефективної реалізації алгоритмів захисту інформації, що забезпечують конфіденційність і цілісність даних. Очевидно, що основу такої безпеки повинні утворювати криптографічні методи захисту інформації. Основним засобом забезпечення інформаційної безпеки в світі Інтернету Речей є так звана «легковагова криптографія» (lightweight cryptography).

В силу умов функціонування інтелектуальних пристроїв, що мають доступ до Інтернет, а також жорстких цінових обмежень, властивих масовому виробництву, зазначені пристрої характеризуються значним обмеженням на ресурси, що використовуються: пам'ять, обчислювальну потужність, джере-

ла живлення тощо. Звідси випливають обмеження на використовувані технології і технологічні рішення, що пред'являються до засобів легковагій криптографії.

Так, наприклад, жорсткі обмеження накладаються на енерговитратність реалізації криптографічних алгоритмів для пасивних інтелектуальних пристроїв, таких як RFID-мітки та безконтактні смарт-карти. Відповідно до стандарту ISO / IEC [4] пасивні RFID-мітки повинні мати рівень енергоспоживання не більше 15 μW для того, щоб гарантувати роботу пристрою в радіусі до 1 м. Останнє, в свою чергу, обмежує можливості, наприклад, в розпаралелювання обчислень з метою збільшення швидкодії алгоритму.

Інший приклад обмежень дають системи автоматичного здійснення дорожніх зборів (плати за проїзд по платних дорогах): для цих систем автомобіль, що рухається з великою швидкістю, повинен бути ідентифікований пристроєм на значній відстані (10–12 м.) за досить нетривалий час (менше 10 мс.). зрозуміло, що в цьому випадку швидкість роботи значно більш істотна, ніж розміри мікросхеми або її енергоспоживання.

Таким чином, типовими обмеженнями, що зустрічаються у легковаговій криптографії, є: для апаратної реалізації – розмір мікросхеми, споживана енергія, час, витрачений на виконання програми; для програмної реалізації – розмір програмного коду, розмір оперативної пам'яті, час, витрачений на виконання програми.

Проблеми синтезу алгоритмів потокового шифрування для сучасної криптографії

Над проблемою створення сучасних потокових шифрів, які забезпечували б усі вимоги безпеки і універсальності використання, почали роботу ще у 2004 році у рамках масштабного проекту ECRYPT [5]. Мета проекту ECRYPT – об'єднати зусилля провідних європейських дослідників для вирішення відкритих проблем в області захисту інформації. Європейською криптологічною спільнотою в рамках проекту ECRYPT був проведений відкритий конкурс (2004–2008 рр.) на розробку нових потокових шифрів – eSTREAM (ECRYPT Stream Cipher Project) [6].

Як підкреслюється в [7], основним завданням проектування в області легковагової криптографії є відшукання балансу між безпекою, ціною і продуктивністю. Звичайні криптографічні стандарти були оптимізовані для великогабаритних обчислювальних систем, в зв'язку з чим їх складно, а в деяких випадках неможливо застосувати, наприклад, у засобах з обмеженими ресурсами.

У зв'язку з вищезазначеними проблемами, у 2013 році NIST (National Institute of Standards and Technology) ініційовано проект легковагової криптографії для розуміння необхідності виділення легких криптографічних стандартів, і розробки відкритого процесу стандартизації. З 2016 NIST анонсував своє рішення щодо розвитку і підтримки профілю легковагових алгоритмів, які рекомендовані для обмеженого застосування, де звичайні стандарти слабо пристосовані для використання в програмної або апаратної реалізації. У березні 2017 NIST опублікував NISTIR 8114 Report on Lightweight Cryptography [7], який підводить підсумки проекту легковагової криптографії і описав плани NIST по стандартизації легковагових алгоритмів, придатних для забезпечення систем з обмеженою середовищем, створення ультрадешевих сервісних додатків і роботи з обмеженим енергозабезпеченням. В рамках легковагової криптографії, в квітні 2017 NIST опублікував проект профілю стандартизації легковагової криптографії [8], що описує вимоги до безпеки і продуктивності кандидатів.

Для побудови потокових шифрів використовуються різні методи, серед яких найбільш значущими можливо відокремити генератори, в основу яких закладені складні нелінійні перетворення та генератори, побудовані на основі лінійних регістрів зсуву з зворотними зв'язками [9]. Перші мають більшу криптостійкість, проте їх реалізація вимагає використання трудомістких, з точки зору обчислювальних ресурсів, операцій, що істотно знижує оперативність їх роботи. Інші методи більш економічні, оскільки для їх реалізації застосовуються в основному зсувні, логічні і лінійні операції. Вони економно витрачають обчислювальні ресурси і, головне, забезпечують високу продуктивність формованих випадкових чисел. Однак, для забезпечення заданої стійкості, до складу таких генераторів доводиться все ж вводити додаткові нелінійні функції і, в такому випадку, вони представляють собою деякий інженерний компроміс між обома підходами.

Як показав eSTREAM, одними з переможців за профілем 2 (потокові шифри для систем з обмеженими ресурсами) стали ряд криптографічних примітивів, до яких відносяться потокові шифри Trivium [10] та Grain [11]. Основними елементами зазначених шифрів є регістри зсуву з нелінійними зворотними зв'язками (РЗНЗЗ), які, з одного боку, забезпечують просту, низьку за вартістю і ефективну апаратну або програмну реалізацію, а з іншого – дозволяють протистояти алгебраїчним атакам [12].

Однак, простежується відсутність єдиної методики, яка дозволила б адекватно оцінити основні властивості схем шифрування, що значно ускладнює процес дослідження та вибору адекватних рішень. У попередніх проектах, які бралися за рішення схожих

завдань (AES, NESSIE), оцінка зводилася до суб'єктивну вирішення експертів щодо надійності представлених криптоалгоритмів [13]. Одна з перших спроб розробити методику високого рівня оцінки примітивів була зроблена фахівцями в рамках проекту NESSIE. В результаті був запропонований перелік критеріїв і методологічних проблем, які необхідно враховувати при аналізі криптоалгоритмів, однак, як зазначають самі розробники, цей список великий, але не завершений і вимагає подальшого вдосконалення.

Для успішного проведення порівняльного аналізу та дослідження основних властивостей потокових шифрів необхідно, в першу чергу, обґрунтувати і вибрати систему критеріїв і показників оцінки досліджуваних схем, а також розробити методи та створити науково-методичний апарат, який, з огляду на сучасні тенденції проектування схем, дозволив би виділити найкращі з них [13].

Метою даної роботи є створення системи оцінювання основного з елементів сучасних криптопримітивів – РЗНЗЗ, яка може бути застосована у перспективних системах легковагової криптографії, та порівняння щодо можливості їх застосування на ряду з регістрами зсуву з лінійними зворотними зв'язками (РЗЛЗЗ).

Регістри зсуву з нелінійними зворотними зв'язками другого порядку

Для РЗНЗЗ довільного порядку, що складається з L комірок, булева функція зворотного зв'язку $f:\{0,1\}^L \to \{0,1\}$ для $GF(2)$ матиме вигляд:

$$f(x_1, x_2, \ldots, x_L) = \sum_{i=1}^{L} a_i x_i + \sum_{i=1}^{L-1} \sum_{j=i+1}^{L} a_{ij} x_i x_j + \\ + \sum_{i=1}^{L-2} \sum_{j=i+1}^{L-1} \sum_{m=j+1}^{L} a_{ijm} x_i x_j x_m + \ldots,$$

де x відповідає значенню комірки в момент часу t.

В даній роботі ми переважно будемо розглядати РЗНЗЗ другого порядку, тобто функція зворотного зв'язку яких представляється у вигляді:

$$f(x_1, x_2, \ldots, x_L) = \sum_{i=1}^{L} a_i x_i + \sum_{i=1}^{L-1} \sum_{j=i+1}^{L} a_{ij} x_i x_j .$$

Що буде відповідати функції зворотного зв'язку $f(x)$, записаної в алгебраїчно нормальній формі:

$$f(x_1, x_2, \ldots, x_L) = a_0 + a_{11} \cdot x_1 + a_{22} \cdot x_2 + \ldots + a_{LL} \cdot x_L + \\ + a_{12} \cdot x_1 \cdot x_2 + a_{13} \cdot x_1 \cdot x_3 + \ldots + a_{(L-1)L} \cdot x_{(L-1)} \cdot x_L .$$

Будемо називати коефіцієнти зворотного зв'язку a_{ij} *лінійними коефіцієнтами*, якщо $i = j$ та *нелінійними коефіцієнтами* – якщо $i \neq j$. При цьому стан РЗЛЗЗ є окремий випадок РЗНЗЗ при всіх нелінійних коефіцієнтах, що дорівнюють нулю та обчислюється співвідношенням:

$$f(x_1, x_2, \ldots, x_L) = \sum_{i=1}^{L} a_i x_i .$$

Інтерес до РЗНЗЗ викликаний в значній мірі їх здатністю генерувати псевдовипадкові послідовності (ПВП), які, як правило, важко піддаються існуючим криптоаналітичним методам аналізу [14–15]. В роботі [16] показано, що РЗНЗЗ більш стійкі до криптоаналітичних атак, ніж РЗЛЗЗ.

Система критеріїв та показників оцінки криптографічної стійкості РЗНЗЗ

Проблему оцінки ефективності схем потокового шифрування можливо вирішити при комплексному урахуванні різних за своєю природою факторів. Методологічною основою підготовки та обґрунтування рішень щодо можливості застосування досліджуваних криптосистем є системний аналіз [17]. Залучення методологічних засобів системного аналізу обумовлено, перш за все, тим, що рішення доводиться приймати в умовах невизначеності, викликаної наявністю факторів, що не піддаються суворої кількісної оцінки. Прийоми і методи системного аналізу спрямовані на висунення альтернативних варіантів вирішення даної проблеми, виявлення масштабів невизначеності по кожному варіанту і зіставлення варіантів по їх ефективності. Очевидно, що такий підхід буде дієвим і при розробці систем поточного шифрування.

Під *криптографічною стійкістю* будемо розуміти здатність криптографічного алгоритму протистояти криптоаналізу. Стійким вважається алгоритм, який для успішної атаки вимагає від противника недосяжних обчислювальних ресурсів, недосяжного обсягу перехоплених відкритих і зашифрованих повідомлень або ж такого часу розкриття, що за його закінченням захищена інформація буде вже не актуальна. У більшості випадків криптографічна стійкість не можливо математично довести, можливо лише довести уразливості криптографічного алгоритму.

Критерії криптографічної стійкості – правила, що дозволяють оцінити та вибрати показники, які характеризують криптографічну стійкість схем потокового шифрування у відповідності необхідному рівню надійності. Оцінка включає кількісну оцінку, отриману аналітичним або емпіричним шляхом, та критерії відповідності («так» або «ні»).

Оцінка ефективності здійснюється за допомогою критерію W, що відображає ступінь виконання схемою функціонального завдання. Оскільки забезпечення криптографічної стійкості досягається лише при виконанні безлічі різноманітних умов, то ре-

зультат функціонування системи описується безліччю умов, а показник ефективності є векторним, тобто містить безліч значень W_i окремих показників ефективності, а саме,

$$W = \left| W_1, W_2, \ldots, W_n \right|,$$

де n – кількість окремих критеріїв, за якими проводиться дослідження.

Для криптографії практичний інтерес представляють *М-РЗНЗЗ*, тобто РЗНЗЗ, що генерують М-послідовність. Під *М-послідовністю* або послідовністю максимальної довжини будемо розуміти псевдовипадкову двійкову послідовність, яка породжена регістром зсуву та має максимальний період.

РЗНЗЗ досліджуються лише як базовий елемент схеми потокового шифрування, в якості альтернативи РЗЛЗЗ. Оцінка криптографічної безпеки проводиться лише з боку РЗНЗЗ як складової частини схеми потокового шифрування та ні в якому разі як достатнього елементу генерування ПВП.

У відповідності до основних методів криптоаналізу алгоритмів, побудованих на основі РЗНЗЗ, дослідження стійкості будемо проводити на основі системи безумовних та умовних критеріїв та показників на яких гуртуються обрані критерії. Нижченаведені показники були окремо досліджені у роботах [18–24].

Безумовними критеріями будемо вважати ті критерії, виконання яких є обов'язковими, тобто безумовними. До показників, що входять до безумовних критеріїв віднесемо наступні:

– Лінійна складність ПВП, що генерує окремо взятий РЗНЗЗ.

Лінійною складністю (Li) ПВП називається найкоротший регістр зсуву, який генерує задану періодичну послідовність, за умови, що перші L значень послідовності є початковим заповненням регістра. Оцінка лінійної складності є одним з основних параметрів системи. Будь-яка послідовність, яку можна згенерувати автоматом (лінійним або нелінійним) над кінцевим полем, має кінцеву лінійну складність. Таким чином, можлива побудова алгоритму, який визначить лінійну складність будь-якій послідовності, незалежно від способу її генерації. Для обчислення Li застосовано алгоритм Берлекампа-Мессі, суть якого докладно викладена в [25].

– Квадратична складність ПВП що генерує окремо взятий РЗНЗЗ.

Квадратичною складністю (Li^2) будемо називати найменшу довжину РЗНЗЗ другого порядку, за допомогою якої можливо відтворити вихідну послідовність. Відновлення РЗНЗЗ другого порядку проводиться шляхом вирішення системи лінійних рівнянь.

– Лінійна та квадратична складність сумарної послідовності.

Під *сумарною послідовністю* будемо розуміти послідовність, отриману у результаті операції побітового додавання двох і більше послідовностей від М-РЗНЗЗ. Генерація послідовностей в кожному з М-РЗНЗЗ, що беруть участь в додаванні, проводиться незалежно один від одного. Сумарна лінійна (Li_{sum}) та сумарна квадратична (Li^2_{sum}) складності визначається від сумарної послідовності.

– Період сумарної послідовності, утвореної у результаті підсумовування послідовностей від двох та більше М-РЗНЗЗ.

Періодом послідовності (T) називається кількість бітів, що генеруються регістром до значення, коли згенерована послідовність починає повторюватися. *Сумарний період* (T^{sum}) – це найменший отриманий період, який визначається від сумарної послідовності. Для генерації послідовності заданої довжини доволі часто використовують суму послідовностей від більш коротких М-РЗНЗЗ другого порядку.

– Статистичні властивості послідовностей, що сформовано від М-РЗНЗЗ.

Статистичні властивості ПВП є однією зі складових, які визначають стійкість схем перетворення. Стійкість схеми залежить від того, наскільки близько вона апроксимує генератор випадкових чисел, тобто наскільки ПВП буде обчислювально непередбачувана та невиразна у порівнянні з істинно випадковою послідовністю.

Для дослідження статистичної безпеки використовувалась методика тестування NIST STS (Statistical Test Suite) [26]. У роботі [27] запропонована методика статистичного тестування криптографічних алгоритмів, в основі яких є оцінка математичного сподівання числа пройдених тестів криптоалгоритму, що досліджується. Застосовуючи вказаний підхід, було проведено експериментальне дослідження криптографічних властивостей М-РЗНЗЗ.

До *умовних критеріїв* віднесено ті критерії, виконання яких відбувається лише за визначеної умови та є бажаними, але не обов'язковими. До показників, що входять до умовних критеріїв віднесено:

– Профіль лінійної складності ПВП, що сформовано окремим М-РЗНЗЗ.

Критерій перевірки якості ПВП, заснований на обчислені лінійної складності її відрізків та на порівнянні вибіркового розподілу отриманих значень з їх розподілом для випадкової послідовності, що є ідеальним.

– Профіль лінійної складності сумарної послідовності від різних М-РЗНЗЗ.

Теж саме, що й профіль лінійної складності ПВП, але обчислений від сумарної послідовності.

– Можливість застосування децимації М-послідовності, що сформована М-РЗНЗЗ.

Децимація М-послідовності за індексом $k\,(k=1,2,3,\ldots)$ є вибірка k-х елементів даної М-послідовності. Якщо період М-послідовності та коефіцієнти децимації k взаємно прості значення, то децимація вважається власною або нормальною.

Для РЗЛЗЗ результатом будь-якої нормальної децимації також є М-послідовність. Якщо коефіцієнти децимації відносяться до одного циклотомічного класу, то вони будуть відповідати одній і тій же М-послідовності з точністю до певного зсуву. Якщо коефіцієнти децимації належать до різних циклотомічних класів, то за результатом децимації створюється М-послідовність, відмінна від похідної. Причому, якщо перебрати всі коефіцієнти децимації від 1 до 2^L-1 (далі не має сенсу, так як, в силу своєї циклічності послідовності будуть повторюватися), то можливо отримати всі можливі М-послідовності для РЗЛЗЗ для заданого L, а використовуючи алгоритм Берлекемпа-Мессі можливо відновити утворюючий поліном РЗЛЗЗ.

– Можливість застосування властивості групового додавання М-послідовності, що сформована М-РЗНЗЗ.

Властивість групового додавання: якщо додати (по модулю 2) деякі розряди РЗЛЗЗ, то результатом такої операції буде М-послідовність, така ж, як на виході РЗЛЗЗ, тільки з деяким зсувом. Таким чином, додаючи різні розряди РЗЛЗЗ можливо отримати усі 2^L-1 зсуву. Використовуючи властивості групового додавання, знаючи утворюючий поліном та провівши попередні обчислення, можливо отримати послідовність, яку буде генерувати РЗЛЗЗ через певну кількість ітерацій, не виконуючі прогін усіх станів регістру до потрібної ітерації, що принципово неможливо з великими значеннями L.

– Обсяг можливих різних структур РЗНЗЗ другого порядку для фіксованого значення L (M).

Під вказаним обсягом розуміємо повну множену різних РЗНЗЗ другого порядку при заданому значенні розміру регістра, тобто кількісне значення окремих структур, які можливо створити, використовуючи регістр з L комірок.

– Обсяг ансамблю М-РЗНЗЗ (M_0) в *GF*(2).

Під терміном *обсяг ансамблю* будемо розуміти кількість різних М-послідовностей, що можуть згенерувати М-РЗНЗЗ другого порядку фіксованого розміру L.

– Проведення порівняльної оцінки продуктивності М-РЗНЗЗ та М-РЗЛЗЗ при програмної реалізації алгоритму.

Під *продуктивністю* програмної реалізації розуміємо кількість даних, що згенеровано в одиницю часу конструкціями на основі М-РЗНЗЗ другого порядку (М-РЗЛЗЗ). При проектуванні систем потокового шифрування важливою характеристикою є швидкість роботи системи, яка обмежена швидкістю генерації у РЗНЗЗ. При тестуваннях не застосовувались методи прискорення у вигляді генерування декількох біт за такт або проведення оптимізації обчислень під певну структуру зворотних зв'язків.

Критеріями та показниками оцінки стійкості РЗНЗЗ, крім перерахованих, можуть бути: збалансованість; критерій розповсюдження; кореляційна імунність; критерій обчислювальної складності та інші. Однак, РЗНЗЗ є збалансовані тому, що генерує модифіковану послідовність де Брейна, кореляційна імунність має сенс якщо використовувати РЗНЗЗ в якості фільтруючих функцій. Тому, обмежимося розглядом лише вищенаведеними показниками, які на наш погляд, є доцільними.

Оцінка криптографічної стійкості РЗНЗЗ, як базового елементу схем потокового симетричного шифрування

Сформулюємо модель оцінки криптографічної стійкості РЗНЗЗ, яка враховує введені показники. Модель оцінює здатність РЗНЗЗ протистояти деяким розповсюдженим атакам заснованих на використанні вразливості, що включають у себе будь-який з показників, що входять до запропонованої моделі.

Позначимо через $W_{бі}^{РЗНЗЗ}$ безумовні, а через $W_{уі}^{РЗНЗЗ}$ умовні критерії оцінки для РЗНЗЗ, де $і$ відповідають обраному критерію. Значення $W_{бі}^{РЗНЗЗ}$ та $W_{уі}^{РЗНЗЗ}$ розраховувати у діапазоні $[0,2]$. Вважатиме: $W_i^{РЗНЗЗ}=0$, якщо i-й показник має гірше значення, ніж відповідний показник для РЗЛЗЗ; $W_i^{РЗНЗЗ}=1$, якщо показники для РЗНЗЗ та для РЗЛЗЗ однакові; $W_i^{РЗНЗЗ}=2$, якщо i-й показник має краще значення, ніж відповідний показник для РЗЛЗЗ.

Сумарний нормований критерій оцінки ($W_б^{РЗНЗЗ}$ для безумовних та $W_у^{РЗНЗЗ}$ для умовних критеріїв) РЗНЗЗ визначимо як:

$$W_б^{РЗНЗЗ}=\frac{\sum_i W_{бі}^{РЗНЗЗ}}{n} \text{ та } W_у^{РЗНЗЗ}=\frac{\sum_i W_{уі}^{РЗНЗЗ}}{n},$$

де n – кількість показників, які входять до безумовних (у нашому випадку $n=6$) та умовних ($n=7$) критеріїв. Значення $W^{РЗНЗЗ}$ надає можливість провести кількісне порівняння конструкції з регістрів з лінійними та нелінійними зворотними зв'язками та, як наслідок, зробити обґрунтований висновок щодо криптографічної стійкості. Зведені результати отриманих показників стійкості та значення критеріїв оцінки відображені у табл. 1 (для безумовних) та у табл. 2 (для умовних критеріїв).

Таблиця 1

Зведені показники стійкості РЗНЗЗ для безумовних критеріїв

Показник	**М-РЗЛЗЗ**	**М-РЗНЗЗ**	$W_i^{РЗНЗЗ}$
Лінійна складність (Li)	$Li = L$	$Li \approx 2^L - 2$	2
Лінійна складність сумарної послідовності (Li_{sum})	$Li_{sum} \le L_1 + L_2 + \dots$	$Li_{sum} \le \left(2^{L_1} - 2\right) + \left(2^{L_2} - 2\right) + \dots$	2
Квадратична складність (Li^2)	$Li^2 = L$		1
Квадратична складність сумарної послідовності (Li_{sum}^2)	$Li_{sum}^2 > \max(Li_1^2, Li_2^2)$		1
Період сумарної послідовності (T^{sum})	$T^{sum} = НСК(T^1, T^2, T^3, ...)$		1
Статистичні властивості	ні	так	2

Таблиця 2

Зведені показники стійкості РЗНЗЗ для умовних критеріїв

Показник	**РЗЛЗЗ**	**РЗНЗЗ**	$W_i^{РЗНЗЗ}$
Обсяг різних регістрів зсуву з фіксованим розміром L (M)	$M = 2^L$	$M = 2^{\frac{L(L+1)}{2}}$	2
Обсяг ансамблю М-регістрів (M_0)	$M_0 = \frac{\phi(2^L - 1)}{L}$	$M_0 \le 2^{\frac{L(L-1)}{2} - L + 2}$	2
Показник	**М-РЗЛЗЗ**	**М-РЗНЗЗ**	
Відповідність профілю лінійної складності математичному очікуванню	так	так	1
Відповідність профілю лінійної складності сумарної послідовності математичному очікуванню	так	так	1
Можливість застосування децимації	так	ні	2
Можливість застосування властивості групового додавання	так	так (підвищена складність)	1
Висока швидкість генерування	так	так	1

З приведених зведених даних отримуємо сумарний нормований безумовний критерій оцінки $W_б^{РЗНЗЗ} = 1,5$ та сумарний нормований умовний критерій оцінки $W_у^{РЗНЗЗ} = 1,43$.

За введеною системою оцінки РЗНЗЗ другого порядку мають явну та значну перевагу у порівнянні з РЗЛЗЗ за кількістю можливих конструкції, включаючи конструкції, що формують М-послідовність; за лінійною складністю, як М-послідовності від окремого М-РЗНЗЗ так і від суми декількох М-послідовностей; М-послідовності, що згенеровано РЗНЗЗ успішно проходять статистичне тестування, на відміну від М-послідовностей, що згенеровано РЗЛЗЗ; до М-РЗНЗЗ неможливо (у класичному сенсі) застосувати децимацію та властивості групового додавання. Інші показники мають однакові значення.

Вказана модель не є вичерпною та представляє собою розвиток існуючих моделей для оцінки криптографічної стійкості ПВП, що генеруються РЗНЗЗ другого порядку для їх практичного застосування в системах потокового симетричного шифрування.

Висновки

Запропонована система критеріїв та показників дозволяє збудувати ефективний механізм оцінки криптографічної стійкості РЗНЗЗ другого порядку, як базового елемента схем потокового шифрування та веде до зменшення невизначеності експерта відносно оцінювання складових алгоритму потокового шифрування.

Параметри, що увійшли до моделі оцінки, достатньо вичерпне характеризують РЗНЗЗ як базовий елемент системи потокового шифрування. Введені критерії оцінювання ефективності дозволили зробити обґрунтовану кількісну оцінку переваги застосування у алгоритмах потокового шифрування РЗНЗЗ замість РЗЛЗЗ.

Описану модель корисно використовувати для дослідження ефективності складових як відомих алгоритмів потокового шифрування так і алгорит-

мів, що розробляються, а також для науково обґрунтованого рішення щодо доцільності застосування обраної конструкції потокового шифрування. Модель являє собою певний крок до створення комплексної методики оцінювання систем потокового шифрування на основі регістрів з нелінійними зворотними зв'язками.

Список літератури

1. Бабенко Л.К. Применение параллельных вычислений при решении задач защиты информации [Електронний ресурс] / Л.К. Бабенко, Е.А. Ищукова, И.Д. Сидоров // Программные системы: теория и приложения: электрон. научн. журн. 2013. – Т. 4. – № 3(17). – С. 25-42. URL: http://psta.psiras.ru/read/psta2013_3_25-42.

2. European Research Cluster on the Internet of Things. [Електронний ресурс]. – URL: www.internet-of-things-research.eu/documents.htm.

3. Жуков А.Е. Легковесная криптография. Часть 1 / А.Е. Жуков // Вопросы кибербезопасности. – 2015. – № 1(9). – С. 26-43.

4. ISO/IEC 18000-3:2004 Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13.56 MHz.

5. ECRYPT Project – European Network of Excellence for Cryptology. [Електронний ресурс]. – URL: http://www.ecrypt.eu.org.

6. eSTREAM: the ECRYPT Stream Cipher Project [Електронний ресурс]. – URL: http://www.ecrypt.eu.org/stream/.

7. National Institute of Standards and Technology (2017) Report on Lightweight Cryptography (U.S. Department of Commerce, Washington, D.C.), National Institute of Standards and Technology Internal Report 8114. [Електронний ресурс] // URL: https://doi.org/10.6028/NIST.IR.8114.

8. Profiles for the Lightweight Cryptography Standardization Process [Електронний ресурс]. – URL: http://csrc.nist.gov/publications/drafts/whitepapers/2017/profiles-lwc-std-proc-draft.pdf.

9. Казакова Н.Ф. Проблемы построения комбинированных линейных генераторов псевдослучайных чисел / Н.Ф. Казакова, Ю.В. Щербина // Інформаційна безпека. – 2013. – №2 (10). – С. 58-64.

10. The eSTREAM Project - eSTREAM Phase 3. Trivium (Portfolio Profile 2). [Електронний ресурс]. – URL: http://www.ecrypt.eu.org/stream/triviumpf.html.

11. The eSTREAM Project - eSTREAM Phase 3. Grain (Portfolio Profile 2). [Електронний ресурс]. – URL: http://www.ecrypt.eu.org/stream/grainpf.html.

12. Knellwolf S., Meier W., Naya-Plasencia M. Conditional Differential Cryptanalysis of NLFSR-Based Cryptosystems. [Електронний ресурс] // 2010 URL: https://link.springer.com/chapter/10.1007/978-3-642-17373-8_8.

13. Орлова С. Методика оценки эффективности поточных шифров / С. Орлова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник. – 2004. – Вип. 9. – С. 141-152.

14. Zeng, K. Pseudorandom bit generators in stream – cipher cryptography / K. Zeng, C. Yang, D. Wei, T. R. N. Rao // Computer. – 1991.

15. Программирование алгоритмов защиты информации / А.В. Домашев, М.М. Грунтович, В.О. Попов, Д.И. Правиков, И.В. Прокофьев, А.Ю. Щербаков. – М.: Изд-во «Нолидж», 2002. – 416 с.

16. Dubrova, E. On analysis and synthesis of (n,k) – non – linear feedback shift registers / E. Dubrova, M. Teslenko, H. Tenhunen // Design and Test in Europ, 2008. – P. 133-137.

17. Надежность и эффективность в технике: справочн.: Н17 В 10 т. / Ред. совет: С. Авдуевский (пред.) и др. (В пер.). Т-3. Эффективность технических систем: Под общ. В.Ф. Уткина, Ю.В.Крючкова. – М.: Машиностроение. 1988. – 328 с.

18. Потий А.В. К вопросу о максимальном периоде последовательностей генерируемых регистрами сдвига с линейной обратной связью второго порядка / А.В. Потий, Н.А. Полуяненко // Системи обробки інформації. – Х.: ХНУПС, 2016. – Вип. 8 (145). – С. 121-123,

19. Полуяненко Н.А. Сравнение объема ансамбля М-РСЛОС и М-РСНОС, скорости генерации на их основе, для GF(2) и в расширениях поля $GF(2^2)$ / Н.А. Полуяненко, А.В. Потий // Радиотехника: Всеукраинский межведомственный научно-технический сборник. – 2016. – № 186/2016. – С. 153-159.

20. Полуяненко М.О. Статистичні властивості регістрів зсуву з нелінійним зворотнім зв'язком / О.В. Потій, М.О. Полуяненко // Безпека інформації в інформаційно-телекомунікаційних системах: матеріали XVIII Міжнародної науково-практичної конференції. – К., 2016. – С. 16.

21. Полуяненко Н.А. Анализ линейной и квадратичной сложности РСНОС второго порядка / А.В. Потий, Н.А. Полуяненко // Захист інформації і безпека інформаційних систем: матеріали V Міжнародної науково-технічної конференції . – Львів, 2016. – С. 102-103.

22. Полуяненко Н.А Период последовательности РСНОС второго порядка / А.В. Потий, Н.А. Полуяненко // Інформаційна та економічна безпека (INFECO-2016): матеріали III Міжнародної науково-практичної конференції. – Х., 2016. – С. 269-272.

23. Полуяненко Н.А. Исследование свойств регистров сдвига с нелинейной обратной связью / Н.А. Полуяненко // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: матеріали II Науково-практичної конференції. – Київ, 2017. – С. 154-159.

24. Аналіз, розробка та дослідження постквантових криптографічних примітивів та обґрунтування умов їхнього застосування в Україні: звіт про НДР (проміжний). Том 1. – Аналіз та порівняльні дослідження симетричних криптографічних перетворень на постквантовий період / ХНУ ім. В.Н. Каразіна; кер. Кузнецов О.О.; вик.: Сватовський І.І. [та інш., всього 13 осіб]. – Х.: ХНУ ім. В.Н. Каразіна, 2016. –119 с.

25. Захаров И.Д. Использование порождающих полиномов m-последовательностей при построении псевдослучайных кодовых шкал / И.Д. Захаров, А.А. Жиганов // Изв. вузов. приборостроение. – 2011. – Т. 54, № 6.

26. Special Publication 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. [Електронний ресурс]. – URL: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf.

27. Кузнецов А.А. Методика статистического тестирования криптографических алгоритмов / А.А. Кузнецов, Р.И. Мордвинов, Е.П. Колованова, А.В. Самойлова // Спеціальні телекомунікаційні системи та захист інформації. – К., 2014. – № 1 (25). – С. 54-61.

Надійшла до редколегії 7.06.2017

Рецензент: д-р техн. наук проф. О.І. Тімочко Харківський Національний університет Повітряних Сил ім. І. Кожедуба, Харків.

ОЦЕНКА КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ РЕГИСТРОВ СДВИГА С НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ

Н.А. Полуяненко, А.В. Исаев

Рассмотрена возможность применения регистров сдвига с нелинейными обратными связями (РСНОС) второго порядка в качестве основного элемента системы потокового симметричного шифрования. Предложено систему критериев и показателей оценки криптографической стойкости РСНОС, на основе которой получено обоснованную количественную оценку преимущества применения в алгоритмах потокового шифрования РСНОС вместо регистров сдвига с линейными обратными связями. Созданную модель оценки рекомендовано использовать для комплексной оценки и научно обоснованного решения о целесообразности применения выбранной конструкции потокового шифрования.

Ключевые слова: *регистры сдвига с нелинейной обратной связью, РСНОС, криптографическая стойкость, оценка стойкости шифров, потоковые шифры, системы шифрования.*

EVALUATION OF CRYPTOGRAPHIC PROTECTION OF NONLINEAR FEEDBACK SHIFT REGISTERS

N. Poluyanenko, A. Isaev

Opportunity of using nonlinear feedback shift registers (NLFSR) of the second order as the main element of the stream cipher system is considered. The system of criteria and indicators of evaluation of cryptographic protection of NLFSR is proposed; on the basis of the evaluation quantitative assessment of the benefits of applying NLFSR instead of linear feedback shift registers in stream cipher algorithm is substantiated. This model of evaluation is recommended to use for complex evaluation and scientifically grounded decision on expediency of application of the chosen stream cipher structure.

Keywords: *nonlinear feedback shift registers, NLFSR, cryptographically strong, evaluation of cipher protection, stream cipher, security encryption systems.*