Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0821U100094

Особливі позначки: відкрита

Дата реєстрації: 19-01-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Поремський Михайло Васильович

2. Poremskyi Mykhailo Vasylovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 29-12-2020

Спеціальність за освітою: Безпека державних інформаційних ресурсів

Місце роботи здобувача: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код за ЄДРПОУ: 34979237

Місцезнаходження: вул. Верхньоключова, 4, 27 корпус, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Адміністрація державної служби спеціального зв'язку та захисту інформації

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 26.002.003

Повне найменування юридичної особи: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код за ЄДРПОУ: 34979237

Місцезнаходження: вул. Верхньоключова, 4, 27 корпус, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Адміністрація державної служби спеціального зв'язку та захисту інформації

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код за ЄДРПОУ: 34979237

Місцезнаходження: вул. Верхньоключова, 4, 27 корпус, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Адміністрація державної служби спеціального зв'язку та захисту інформації

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 28.29, 49.03, 83.03.51

Тема дисертації:

1. Методи обґрунтування стійкості snow 2.0-подібних потокових шифрів відносно кореляційних атак над скінченними полями характеристики 2^r

2. Methods for security evaluation of SNOW 2.0-like stream ciphers against correlation attacks over a finite fields of order 2^r

Реферат:

1. Поремський М.В. Методи обґрунтування стійкості snow 2.0-подібних потокових шифрів відносно кореляційних атак над скінченними полями характеристики 2^r – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека». – Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, 2020. Дисертаційна робота присвячена вирішенню актуальної наукової задачі, яка полягає у розробці методів обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно відомих кореляційних атак. З розвитком інформаційних технологій та комп'ютерної техніки значну увагу привернули до себе слово-орієнтованих ПШ, які є програмно-

орієнтованими та можуть ефективно працювати на сучасних процесорах. Порівняльні дослідження алгоритмів потокового шифрування показують, що одним із найкращих серед сучасних ПШ є шифр SNOW 2.0, що є на сьогодні міжнародним стандартом. В свою чергу, взявши шифр SNOW 2.0 як прототип, було створено важливий клас SNOW 2.0-подібних ПШ. До цього класу відноситься і нещодавно створений в Україні шифр “Струмок”, прийнятий як національний стандарт ДСТУ 8845:2019. Важливою частиною процесу розробки таких шифрів, що зумовлює вибір окремих компонент і параметрів для їх побудови, є обґрунтування їх стійкості відносно усіх відомих на сьогодні атак. В роботі удосконалено аналітичну оцінку інформаційної складності кореляційних атак на потокові шифри. На відміну від раніше відомої (евристичної) оцінки, отримана аналітична оцінка має належне наукове обґрунтування, містить явну залежність від ймовірності помилки атаки та є справедливою для будь-яких кореляційних атак на потокові шифри незалежно від способу побудови або методу розв’язання системи рівнянь зі спотвореними правими частинами, яка складається на першому етапі атаки. Вперше отримано аналітичне співвідношення для квадратичної евклідової незбалансованості розподілу ймовірностей спотворень у правих частинах рівнянь, що використовуються для побудови кореляційних атак на SNOW 2.0-подібні шифри. На відміну від відомих співвідношень, які визначають квадратичну евклідову незбалансованість, отримане співвідношення встановлює вираз цього параметра в термінах коефіцієнтів Фур’є розподілу спотворень у правих частинах рівнянь єдиної системи, яка не залежить від конкретної атаки. Це дозволяє отримувати нижні оцінки трудомісткості й обсягу матеріалу, потрібного для реалізації кореляційних атак на SNOW 2.0-подібні шифри та порівнювати за трудомісткістю та обсягом матеріалу кореляційні атаки, що будуються над полями різних порядків. Вперше розроблено метод обґрунтування стійкості двійкових SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2. На відміну від відомих підходів до побудови кореляційних атак на полем з двох елементів, розроблений метод базується на отриманому дисертантом аналітичному співвідношенні для параметра, який характеризує ефективність атаки, та дозволяє обґрунтовувати стійкість двійкових SNOW 2.0-подібних потокових шифрів безпосередньо за параметрами їх компонент. Отримав подальший розвиток метод обґрунтування стійкості модулярних SNOW 2.0-подібних шифрів відносно кореляційних атак над скінченними полями характеристики 2. На відміну від відомих підходів до побудови кореляційних атак на SNOW 2.0, розроблений метод базується на отриманих дисертантом аналітичних співвідношеннях, які узагальнюють низку окремих результатів про матричні представлення незбалансованості відображень, що реалізуються скінченними автоматами. Розроблений метод є застосовним до модулярних -розрядних SNOW 2.0-подібних шифрів при і дозволяє отримувати нижні оцінки ефективності відомих кореляційних атак безпосередньо за параметрами компонент алгоритму шифрування. Практичне значення одержаних результатів полягає в тому, що дисертантом розроблено програмні реалізації, які дозволяють в режимі реального часу обчислювати значення нижніх меж трудомісткості та обсягу матеріалу, потрібного для здійснення будь-якої з відомих кореляційних атак на довільний двійковий чи модулярний SNOW 2.0-подібний шифр з вузлами заміни довжини 8 бітів. Розроблені програми застосовані для обґрунтування стійкості шифру “Струмок”, а також його двійкової версії. Вони можуть бути використані на практиці при дослідженні стійкості інших SNOW 2.0-подібних потокових шифрів у СІТС України. Наукові та практичні результати дисертаційної роботи реалізовані в Службі зовнішньої розвідки України – в результаті виконання НДР “Корифена” та в науково-технічних розробках ЗАО “Інститут інформаційних технологій”.

2. Poremskyi M. Methods for security evaluation of SNOW 2.0-like stream ciphers against correlation attacks over a finite fields of order 2^r . – Qualifying scientific work as a manuscript. Thesis for a Candidate of Technical Science degree in specialty 125 «Cybersecurity». – Institute of Special Communication and Information Protection of National technical university of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, 2018. This thesis is devoted to solving actual scientific problem of development the methods for security evaluation of SNOW 2.0-like stream ciphers against correlation attacks. With the advancement of information and computer technologies, significant attention has been drawn to word-based SC that are software-oriented and can run efficiently on modern processors. Comparative studies of stream encryption algorithms show that one of the best among

current SC is SNOW 2.0, which is currently the international standard. In turn, using SNOW 2.0 cipher as a prototype, an important class of SNOW 2.0-like ciphers was created. This class includes the recently created in Ukraine cipher "STRUMOK", adopted as the national standard DSTU 8845: 2019. An important part of the process of developing such ciphers, which determines the choice of individual components and parameters for their construction, is their security evaluatin against all known attacks. The analytical estimation of information complexity of correlation attacks on stream ciphers is improved in thesis. Unlike the previously known (heuristic) estimate, the analytical estimate obtained has a scientific basis, contains a clear dependence on the probability of an error of attack and is valid for any correlation attacks on stream ciphers, regardless of the method of creation or solving the system of equations with right parts corrupted by noise, which is creating on the first stage of the attack. For the first time, an analytical relation was obtained for the quadratic Euclidean imbalance of the probability distribution of corruptions in the right part of the equations that are used to construct correlation attacks on SNOW 2.0-like ciphers. Unlike the known correlations that determine the quadratic Euclidean imbalance, the obtained relation determines the expression of this parameter in terms of the Fourier coefficients of the corruption in the right part of the equations of a single system that does not dependent on particular attack. This allows us to obtain lower bounds of the complexity and amount of material required to SNOW 2.0-like correlation attack on SNOW 2.0-like ciphers and to compare the complexity and amount of material for different correlation attacks that are built over fields of different orders. For the first time a method of security evaluation of binary SNOW 2.0-like ciphers against correlation attacks over finite fields of characteristic 2 was developed. In contrast to the known approaches of creating correlation attacks over a field of two elements, the developed method is based on the analytic correlation obtained by researcher for the parameter that characterize the attack efficiency and allows to evaluate the security of binary SNOW 2.0-like stream ciphers directly by the parameters of their components. A method of security evaluation of modular SNOW 2.0-like ciphers against correlation attacks over finite fields of characteristic 2 was further developed. In contrast to the known approaches of creating SNOW 2.0 correlation attacks, the developed method is based on analytical correlations obtained by the thesis, which summarize a number of separate results on matrix representations that are implementing by finite state machines. The developed method is applicable to modular SNOW 2.0-like ciphers and allows to obtain lower bounds of the efficiency of known correlation attacks directly by the parameters of the components of the encryption algorithm. The practical significance of the obtained results consists in developing the software implementations that allow in real time to calculate the values of the lower bounds of the complexity and amount of material required to process any of the known correlative attacks on an arbitrary binary or modular SNOW 2.0-like cipher with 8 bit s-boxes. The developed programs are used to evaluate ofsecurity of the cipher "Strumok", as well as its binary version. They can be used in practice to evaluate the security of other SNOW 2.0-like stream ciphers in SITS of Ukraine. The scientific and practical results of the thesis were implemented at the Foreign Intelligence Service of Ukraine (in the research scientific work «Korifena») and in the scientific and technical developments of CJSC «Institute of Information Technologies».

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Олексійчук Антон Миколайович
2. Oleksiychuk Anton M.

Кваліфікація: д. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Ковальчук Людмила Василівна
2. Kovalchuk Liudmyla V.

Кваліфікація: д. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Кузнецов Олександр Олександрович

2. Kuznetsov Oleksandr

Кваліфікація: д. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Цуркан Василь Васильович
2. Tsurkan Vasyl V.

Кваліфікація: к. т. н., 21.05.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Савчук Михайло Миколайович
2. Savchuk Mykhailo M.

Кваліфікація: д. ф.-м. н., 01.05.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Рома Олександр Миколайович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Рома Олександр Миколайович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.