АНОТАЦІЯ

Поремський М.В. Методи обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно кореляційних атак над скінченними полями порядку 2^r – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології 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.

Забезпечення інформаційної безпеки держави є однією із найважливіших задач в умовах великої кількості внутрішніх та зовнішніх загроз, які безпосередньо впливають на її економічну стабільність та суверенітет. Таким чином, першочерговими задачами у сфері інформаційної безпеки держави є розробка нових та вдосконалення існуючих криптографічних систем. Кожна така система повинна задовольняти певним вимогам, а саме забезпечувати необхідний рівень швидкості роботи (як в сучасних бездротових мережах), забезпечувати достатній рівень стійкості та ефективно працювати на сучасних комп'ютерних процесорах. Усім цим вимогам задовольняють потокові шифри (ПШ), які широко використовуються в сучасних захищених мережевих протоколах, стандартах мобільного зв'язку, системах супутникового зв'язку та в апаратних застосуваннях з обмеженими ресурсами. Потокові шифри широко вивчаються світовою спільнотою, про що говорить низка міжнародних конкурсів, а також конкурсів в окремих державах.

З розвитком інформаційних технологій та комп'ютерної техніки значну увагу привернули до себе слово-орієнтовані 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.

Сучасні методи криптоаналізу потокових шифрів, а також атаки, що будуються на їх основі, звичайно поділяють на методи "зламування", спрямовані на відновлення ключів (або початкових станів генераторів гами), та методи, призначені для виявлення певних відмінностей між вихідними послідовностями генератора і випадковими послідовностями. При цьому, в залежності від інформації, що доступна криптоаналітику класи атак можна поділити на атаки на основі відомого шифрованого тексту, атаки на основі відомого відкритого тексту та атаки на основі відомих або підібраних векторів ініціалізації. Крім перелічених видів атак, які проводяться за умови застосування єдиного невідомого ключа шифрування, розглядають також атаки зі зв'язаними ключами, при проведенні яких противник, маючи доступ до декількох шифрувальних перетворень, намагається відновити відповідні їм ключі, використовуючи певні відомі співвідношення між ними. На сьогодні відомо декілька видів атак, запропонованих на SNOW 2.0, які, в принципі, можуть бути застосовані до будь-якого SNOW 2.0-подібного потокового шифру. Це атаки зі зв'язаними ключами, узагальнена статистична атака та низка пов'язаних з нею атак, алгебраїчна атака та широкий клас кореляційних атак.

Аналіз доступних публікацій показує, що найбільш потужними атаками на SNOW 2.0 (складність яких може бути помітно менше складності повного

перебору ключів) є кореляційні атаки, які базуються на побудові та розв'язанні систем лінійних рівнянь зі спотвореними правими частина над полями порядку 2^r, де $r \geq 2$. При цьому виявляється, що методи, розвинуті для оцінювання стійкості до таких атак саме шифру SNOW 2.0, стають незастосовними у випадку SNOW-2.0-подібних шифрів, які будуються над полями порядку 2^{64} або більше (наприклад, для шифру "Струмок"). В цілому, на сьогодні відсутні методи, які дозволяють обґрунтовувати стійкість SNOW-2.0-подібних ПШ відносно відомих кореляційних атак безпосередньо за параметрами їх компонент.

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 r-розрядних SNOW 2.0-подібних шифрів при $r \geq 64$ 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”.

Ключові слова: кібербезпека, потоковий шифр, кореляційна атака, криптоаналіз, обґрунтування стійкості.

ABSTRACT

Poremskyi M. Methods for security evaluation of SNOW 2.0-like stream ciphers against correlation attacks over finite fields of order 2^r. – Qualifying scientific work as a manuscript.

Ph.D thesis in the field of knowledge 12 Information technologies 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.

Ensuring the information security of the country is one of the most important tasks in the context of a large number of internal and external threats that affect its economic stability and sovereignty. Thus, the priority in the field of information security of the country is the creation of new and improvement of existing cryptographic systems. Each such system must meet certain requirements, namely to provide the necessary level of speed (as in modern wireless networks), to provide a sufficient level of security and to work efficiently on modern computer processors. All of these requirements are met by stream ciphers (SC), which are widely used in modern secure network protocols, mobile communications standards, satellite communications and hardware applications with limited resources. Streaming ciphers are widely studied by the international community, as evidenced by a number of international competitions as well as competitions in separate countries.

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.

Current methods of cryptanalysis of stream ciphers, as well as the attacks based on them, are usually divided into "hacking" methods aimed at recovering keys (or initial states of gamma generators), and methods designed to detect certain differences between the original sequences of the generator and random sequences. However, depending on the information available to the crypto analyst, the classes of attacks can be divided into attacks based on known encrypted text, attacks based on known plaintext, and attacks based on known or selected initialization vectors. In addition to the types of attacks that are conducted using a single unknown encryption key, attacks with related keys, during which the adversary, having access to several encryption transformations, attempts to recover their respective keys using certain known ratios between them are also considered. Today, there are several types of attacks proposed on SNOW 2.0 that, in principle, can be applied to any SNOW 2.0-like stream cipher. These are related-key attacks, a generalized statistical attack and a set of related attacks, algebraic attack and a wide range of correlation attacks.

Analysis of available scientific publications was carried out. It shows that the most powerful attacks on SNOW 2.0 (the complexity of which can be much less than complexity of a complete key search) are correlation attacks, which are based on creating and solving systems of linear equations with right sides corrupted by noise

over the fields of order 2^r, where $r \geq 2$. It turns out that the methods developed for security evaluation against such attacks, namely SNOW 2.0, become inapplicable in the case of SNOW-2.0-like ciphers that are built over fields of order 2^{64} or more (for example, for cipher "Strumok"). In general, there are currently no methods that can evaluate a security of SNOW-2.0-like ciphers against known correlative attacks directly by the parameters of their components.

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 security 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».

Keywords: cybersecurity, correlation attack, cryptanalysis, security evaluation.

Список основних публікацій здобувача:

1. Олексійчук А.М., Поремський М.В. Нижні межі інформаційної складності кореляційних атак на потокові шифри над полями порядку 2^r. *Захист інформації.* 2017. Т. 19, № 2, с. 126-131.

2. Олексійчук А.М., Ігнатенко С.М., Поремський М.В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Серія: Технічні науки.* 2017. Випуск 15, с. 150-155.

3. Олексійчук А.М., Поремський М.В. Загальна схема побудови кореляційних атак на SNOW 2.0-подібні потокові шифри. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2018. Випуск 1 (32), с. 70-79.

4. Олексійчук А.М., Конюшок С.М., Поремський М.В. Обґрунтування стійкості потокового шифру «Струмок» відносно кореляційних атак над скінченними полями характеристики 2. *Математичне та комп'ютерне моделювання. Серія: Технічні науки.* 2019. Випуск 19, с. 114-119.

5. Alekseychuk A.N., Koniushok S.M., Poremskyi M.V. Upper Bounds on the Imbalance of Discrete Functions Implemented by Sequences of Finite Automata. *Cybernetics and Systems Analysis.* 2019. Volume 55, Issue 5, pp. 752-759.

6. Alekseychuk A.N., Koniushok S.M., Poremskyi M.V. A Method of Evaluating the Security of SNOW 2.0-Like Ciphers Against Correlation Attacks Over the Finite Extensions of Two Element Fiel. *Cybernetics and Systems Analysis*. 2020. Volume 56, Issue 1, pp. 40-52.

7. Олексійчук А.М., Поремський М.В. Нижні межі інформаційної складності кореляційних атак на потокові шифри над полями порядку 2^r // *III Міжнародна науково-практична конференція «Актуальні питання забезпечення кібербезпеки і захисту інформації».* 22-25 лютого 2017 р., К., 2017, с. 131.

8. Олексійчук А.М., Поремський М.В Застосування алгоритму BKW для побудови швидких кореляційних атак на словоорієнтовані потокові шифри. // *XIX міжнародна науково-технічна конференція* «*Безпека інформації в інформаційно-телекомунікаційних системах».* 25-26 лютого 2-17 р., К., 2017, с. 123-124.

9. Олексійчук А.М., Поремський М.В, Стрателюк Д.П. Кореляційні атаки на спрощені версії SNOW 2.0-подібних потокових шифрів // *XX міжнародна науково-технічна конференція «Безпека інформації в інформаційно-телекомунікаційних системах».* 22-24 травня 2018 р., К., 2018, с. 90.

10. Олексійчук А.М., Поремський М.В Метод обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно кореляційних атак над полями порядку 2^r // *Науково-практичної конференція «Сучасні інформаційні технології та кібербезпека».* 15-16 листопада 2018 р., К., 2018, с. 41-43.

11. Поремський М.В. Експериментально-статистичне дослідження розподілу параметра вузлів заміни, що визначає стійкість SNOW 2.0-подібних потокових шифрів відносно кореляційних атак // *Науково-практична конференція «Інформаційно–телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання».* 19-20 листопада 2019 р., К., 2019, с. 37.