КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2019.4.1423
УДК 004.056.55: 003.26

Грищук Руслан Валентинович
доктор технічних наук, професор, начальник кафедри захисту інформації та кібербезпеки
Житомирський військовий інститут імені С. П. Корольова, Житомир, Україна
OrcID:0000-0001-9985-8477
prof.Hry@gmail.com

Грищук Ольга Михайлівна
інженер інформаційно-обчислювального центру
Житомирський військовий інститут імені С. П. Корольова, Житомир, Україна
OrcID: 0000-0001-6957-4748
Ol.Hry@i.ua

УЗАГАЛЬНЕНА МОДЕЛЬ КРИПТОСИСТЕМИ ФРЕДГОЛЬМА

Анотація. Проблема кібербезпеки в епоху створення квантових комп'ютерів набуває особливої актуальності. Особливо під загрозу підпадають дані, які є конфіденційними, або цінність яких залежить від їх цілісності. З метою пошуку виходу з ситуації, що склалася у статі на основі системного підходу було проведено ґрунтовний всебічний комплексний аналіз сучасного стану розвитку відомих криптосистем. Зокрема встановлено переваги та недоліки моделей криптосистем створених на основі когнітивної криптографії, теорії динамічного хаосу, конструктивної, квантової та постквантової криптографії. Також порушено питання про моделі криптосистем на основі алгоритмів ДНК, моделі проксі криптосистем, криптосистем на основі атрибутів, пакетної та некомутативної криптографії. У результаті дослідження встановлено, що найбільший інтерес з точки зору безпеки на сьогодні становить інтегральна криптографія. Відсутність на сьогодні науково обґрунтованих моделей криптосистем на основі інтегральної криптографії спонукала до розроблення однієї з таких моделей. Модель розроблено на основі запропонованого концепту, який ґрунтується на основних положеннях інтегральної криптографії. У результаті проведеного дослідження розроблено узагальнену модель криптосистеми, яку у подальшому запропоновано називати криптосистемою Фредгольма. Показано, що сутність процедур шифрування та дешифрування зводиться до розв'язання прямої та оберненої задачі, яка описується інтегральним рівням Фредгольма першого роду. У статті окремо наголошено на тому, що порівняно з відомими моделями криптосистем, запропонована має ряд суттєвих переваг. Перша перевага – гарантована теоретична та практична криптостійкість, яка обумовлена некоректністю оберненої задачі дешифрування. Друга перевага запропонованої моделі полягає у відсутності дієвих алгоритмів криптоаналізу через недостатньою розповсюдженість інтегральної криптографії в сучасних системах забезпечення кібербезпеки. Розроблена модель виступає теоретичним підґрунтям для подальшого розроблення відповідних криптоалгоритмів та дослідження параметрів їх безпеки.

Ключові слова: модель, криптосистема, інтегральне рівняння Фредгольма першого роду, шифрування, дешифрування, пряма та обернена задача.

1. ВСТУП

Проблема забезпечення кібербезпеки [1] в інформаційному суспільстві залишається однією з наріжних безпекових проблем сучасності [2], [3], [4]. Згідно з доповіддю про глобальні загрози людству на 2019 р. [5], оприлюдненій на Всесвітньому економічному форумі в Давосі, загрози кібербезпеці знаходяться в тренді світових глобальних загроз для людства і в поточному році. Тому не зважаючи на

зусилля світової спільноти щодо вирішення проблеми кібербезпеки вона є і буде актуальною і в найближчій перспективі.

З поміж багатьох підходів до вирішення проблеми кібербезпеки особливе місце та роль відводиться криптографії. Криптографічні методи зокрема використовуються для забезпечення конфіденційності та цілісності інформації або даних, що становлять цінність для їх власника, шляхом їх шифрування [7]. Поряд з тим, зростання потужності обчислювальних засобів та доступність інформаційних технологій до широкого кола користувачів не виключає знаходження ними можливостей для взлому відомих криптоалгоритмів за прийнятний час. Тому задача забезпечення криптостійкості й надалі актуалізується.

Постановка проблеми. Більшість з відомих на сьогодні підходів до забезпечення криптостійкості ґрунтуються на складності вирішення задач факторизації, дискретного логарифмування тощо (для асиметричних криптосистем) або комбінаторної складності (для симетричних криптосистем). Поряд з тим існує ряд інших математичних задач, складність вирішення яких може бути покладена в основу забезпечення криптостійкості алгоритмів шифрування. Таким чином, у рамках вирішення проблеми забезпечення кібербезпеки актуальним залишається завдання щодо розроблення нових та адекватних моделей криптографічного захисту для подальшого створення на їх основі відповідних криптоалгоритмів та ефективних засобів безпеки нового покоління.

Аналіз останніх досліджень і публікацій показав, що починаючи з 1976 р. після появи відомої роботи *New Directions in Cryptography* американських криптографів У. Діффі та М. Геллмана [8] в світі у цілому та в Україні зокрема інтенсифікувався процес винайдення нових напрямів у криптографії. Найбільш інтенсивно сьогодні розвиваються такі перспективні напрями в криптографії як когнітивна криптографія [9], криптографія на основі хаосу [11], [12] конструктивна криптографія [13], квантова [14], [15], [16], [17] та постквантова криптографія [18].

Когнітивна криптографія є однією з найновіших теоретичних парадигм в галузі кібербезпеки, пов’язаних з універсальними криптосистемами. Вона, як показано в [9], ґрунтується на комплексуванні двох фундаментальних теорій – теорії інформації та когнітивної теорії. Моделі криптосистем, що розробляються на основі когнітивної криптографії об’єднують алгоритми, які гарантують конфіденційність та цілісність даних з біометричними характеристиками людини, дані якої захищаються.

Відомі на сьогодні моделі криптосистем на основі теорії динамічного хаосу наприклад [10], [11], [19], [20] та ін., на практиці ще не набули широкого впровадження. Це пов’язано з такими їх недоліками як низька швидкодія криптоалгоритмів, велика трудомісткістю процедур і значний час дешифрування тощо [21].

Конструктивна криптографія ґрунтується на принципово нових моделях криптосистем [13]. Основний акцент при побудові моделі конструктивної криптосистеми розставлено на забезпеченні захищеності каналу зав’язку, а не даних. За твердженням винахідників конструктивної криптографії У. Маурера та Р. Реннера захищеність – це в першу чергу атрибут каналу зв’язку, а не обов’язкова властивість криптосистеми [22]. Таким чином, практичне впровадження конструктивних криптосистем очевидно потребуватиме внесення деяких змін в телекомунікаційній інфраструктурі через додаткові вимоги, які висуватимуться до захищеності каналів зв’язку. Такий підхід не зважаючи на його переваги, також не завжди є раціональним.

Моделі відомих квантових криптографічних систем, що ґрунтуються на квантових технологіях захисту на сьогодні спроможні забезпечувати теоретичну криптостійкість [15], [17]. Поряд з тим побудова квантових комп’ютерів не виключає

ISSN 2663 - 4023

реалізації таких методів криптоаналізу, як квантового алгоритму факторизації П. Шора [23], квантового алгоритму Л. Гроувера [24] та їх модифікацій [18]. Значну проблему на практиці при реалізації квантових криптографічних систем як і при конструктивній криптографії становить відповідна інфраструктура. У першу чергу необхідність інфраструктурних змін обумовлена обмеженнями, які виникають через затухання світлового сигналу при передачі даних без використання репитерів.

Постквантові моделі криптосистем, як показано в [18], нині перебувають на стадії активного розроблення та верифікації. Такі моделі на відміну від "класичних" криптосистем вважаються квантовостійкими до криптоатак [25]. Не зважаючи на перспективи постквантових криптосистем, вони у найближчому майбутньому не зможуть у повній мірі заміни відомі симетричні та асиметричні криптосистеми.

Нині все більше набувають розвитку моделі криптосистем на основі алгоритмів ДНК [26]. У [27] достатньо ґрунтовно розкриваються такі напрями як проксі криптографія, криптографія на основі атрибутів, пакетна та некомутативна криптографія.

В Україні починаючи з 2014 р. набуває розвитку криптографія нового покоління, яку її основоположниками названо інтегральною. Інтегральна криптографія згідно з [28], [29], [30], [31], [32] та [33] має ряд переваг. Однією з головних її переваг є гарантована криптостійкість. Наприклад, якщо в процесі шифрування задіяно формалізований алгоритм на основі інтегральних рівнянь Фредгольма першого роду, як це показано в [30], то задача криптоаналізу у силу некоректності по Ж. Адамару, є практично нерозв'язуваною [34]. Тому враховуючи широкі перспективи, які відкриваються при забезпеченні кібербезпеки на основі інтегральної криптографії, особливої актуальності набуває задача розроблення узагальненої моделі криптосистеми Фредгольма, яка у відомих публікаціях не розкрита в явному вигляді, що і **є метою статті.**

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Подамо концепт створюваної узагальненої моделі відповідно до основних положень інтегральної криптографії [28].

1. Незалежно від обраного, удосконаленого або вперше розробленого криптоалгоритму, а також закладеного в нього фундаментального теоретичного підґрунтя, створювана узагальнена модель криптосистеми повинна належати до одного з відомих класів криптосистем. Криптостійкість повинна мати строге математичне обґрунтування та зводитися до вирішення класу некоректних задач.
2. Створювана узагальнена модель криптосистеми повинна будуватися у відповідності до принципу Керкгоффса, тобто: криптостійкість криптосистеми повинна залежати тільки від ключа, а сам криптоалгоритм може бути загальнодоступним.
3. Ключ відповідно до основних положень інтегральної криптографії слід обирати з класу неперервних функцій з довільним (невиродженим) неперервним ядром, що забезпечить безумовне виконання принципу Керкгоффса.
4. Вихідні дані для шифрування повинні описуватися класом інтегрованих неперервних функцій.
5. Криптоалгоритм повинен забезпечувати максимально можливу швидкість шифрування та характеризуватися найкращими показниками безпеки в частині, що стосується криптостійкості, порівняно з найближчими аналогами.

ISSN 2663 - 4023

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Відповідно до закладеного теоретичного концепту з усієї множини відомих класів криптосистем [6], в якості досліджуваної пропонується обрати клас симетричних криптосистем як таких, що мають строге математичне обґрунтування криптостійкості [35]. Додержуючись загальної методології моделювання в галузі кібербезпеки [1], [36] та опираючись на основні положення теорії зв'язку в секретних системах К. Шеннона [37], нижче у формалізованому вигляді опишемо модель розроблюваної криптосистеми.

Процедура шифрування (пряма задача).

Нехай відправник A (відповідно до загальноприйнятих позначень в криптології даний архетип названий Алісою) повинен відправити незахищеним каналом зв'язку деяке повідомлення $z(s)$ отримувачу B (за аналогією – Бобу). Повідомлення $z(s)$ є вихідними даними, що підлягатимуть шифруванню Алісою та дешифруванню Бобом відповідно.

Процедура шифрування, яка здійснюється відправником A у відношенні до повідомлення $z(s)$ полягає у вирішенні прямої задачі, яка може бути описана інтегральним рівнянням Фредгольма першого роду

$$\int_a^b K(x,s)\, z(s)\, ds = u(x), \tag{1}$$

де $K(x,s)$ – секретний ключ (ядро інтегрального рівняння Фредгольма першого роду); $z(s)$ – вихідні дані, що підлягають шифруванню/дешифруванню (відкритий текст, вихідні дані); $u(x)$ – зашифровані дані (шифрограма).

Умова 1. Для повного виконання першої вимоги згідно розробленого вище концепту межі інтегрування $[a,b]$ рівня (1) повинні бути скінченними та такими, що відповідають умовам нерівності $a \le x$, $s \le b$. При цьому секретний ключ та зашифровані дані повинні задовольняти умовам

$$\begin{cases} K(x,s) \in C(a \le x,\, s \le b); \\ u(x) \in C([a,b]). \end{cases} \tag{2}$$

Таким чином, по відкритому каналу від відправника A до одержувача B передаються зашифровані дані $u(x)$.

Умова 2. Передбачається, що відправник A має власне джерело секретних ключів. У розглядуваному прикладі (1) – це секретний ключ загального вигляду $K(x,s)$.

Процедура дешифрування (обернена некоректна задача).

Одержувач B отримує від відправника A зашифровані дані $u(x)$. Задача одержувача B полягає у дешифруванні зашифрованих даних $u(x)$ та прочитанні вихідного повідомлення $z(s)$ відправника A.

ISSN 2663 - 4023

Умова 3. Передбачається, згенерований відправником A секретний ключ $K(x,s)$ надійним каналом зв'язку був переданий одержувачу B.

У формалізованому вигляді процедура дешифрування зводиться до вирішення зворотної некоректної задачі (1).

Задача противника E (за аналогією – Єва), який має доступ до каналу зв'язку полягає у перехопленні зашифрованих даних $u(x)$ та читанні вихідного повідомлення $z(s)$ у разі злому криптоалгоритму (підбору секретного ключа $K(x,s)$), або їх модифікації.

Зауваження 1. Перед шифруванням вихідні дані, що підлягають шифруванню $z(s)$ та секретний ключ $K(x,s)$ перетворюються у числові шляхом застосування довільної відомої процедури. Це саме зауваження справедливе і при зворотному переході.

Таким чином, принципи функціонування запропонованої криптосистеми зводиться до вирішення прямої (коректної) задачі – процедура шифрування та оберненої (некоректної) задачі – процедура дешифрування, які описуються інтегральним рівнянням Фредгольма першого роду (1). Тому тут і в подальшому модель такої криптосистеми пропонується називати криптосистемою Фредгольма.

Подамо приведений вище формалізований опис криптосистеми у вигляді рис. 1.

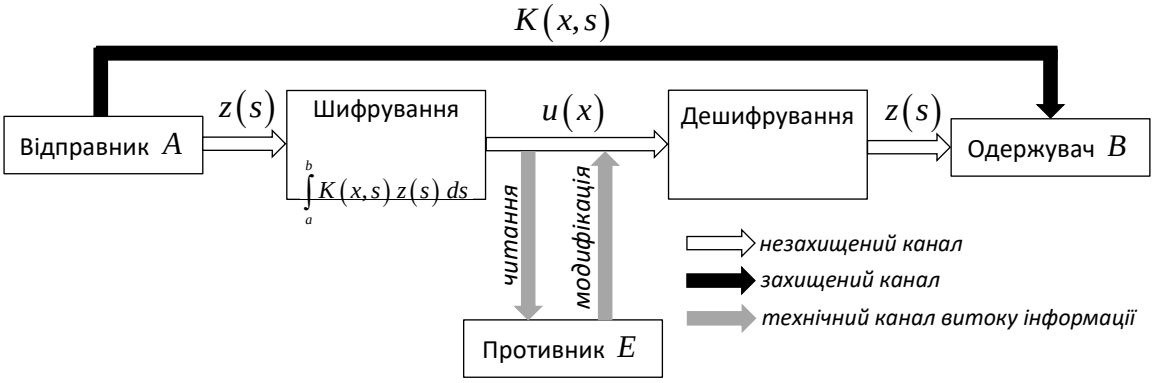

Рис. 1. Узагальнена модель криптосистеми Фредгольма

Як випливає з рис. 1 узагальнена модель криптосистеми Фредгольма побудована за класичною моделлю симетричної криптосистеми. Відмінність між моделями проявляється на рівні застосовуваних процедур шифрування та дешифрування. Отже, додержання класичного принципу побудови криптосистеми дозволяє стверджувати, що розроблені та покладені в основу узагальненої моделі концепти є повністю впровадженими, а сама модель є адекватною.

Перевага розробленої узагальненої моделі криптосистеми Фредгольма над існуючими проявляється на двох основних рівнях. По-перше, безпека шифрування гарантується теоретичною та практичною нерозв'язністю зворотної некоректної задачі Фредгольма першого роду існуючими на сьогодні методами. Дане твердження підтверджується гіпотезою Н. Фергюсона про залежність безпеки шифру від складності вирішення певного типу рівнянь [38]. По-друге, інтегральна криптографія, вперше запропонована авторським колективом [28], на сьогодні тільки набуває становлення, а тому не має ефективних алгоритмів криптоаналізу даних, що захищаються.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, у статті на основі всебічного системного аналізу розглянуто сучасні та перспективні моделі криптосистем. На основі аналізу їх переваг і недоліків зроблено висновок про перспективність подальшого розвитку інтегральної криптографії, як такої, що має суттєвий запас криптостійкості. Показано, що її подальше впровадження потребує обґрунтування та розроблення відповідних моделей криптосистем. Виходячи з того, що дослідження за цією тематикою носять уривчастий характер у статті на основі вивчення та узагальнення відомого матеріалу було розроблено узагальнену модель криптосистеми, яку запропоновано назвати криптосистемою Фредгольма.

Запропонована криптосистема на відміну від відомих узагальнює принцип Керкгоффса в частині, що стосується залежності криптостійкості не тільки від секретного ключа, а й від точності вирішення оберненої некоректної задачі, яка описується інтегральним рівнянням Фредгольма першого роду та має нескінченну множину можливих розв’язків.

Перспективи подальших розвідок зводяться до вибору функції, яка описує ядро інтегрального рівня, обґрунтування вимог до його виродженості/невиродженості, симетричності/несиметричності. Також у подальшому планується розроблення криптоалгоритму на основі запропонованої моделі та проведення досліджень з його ефективності, швидкодії та безпеки.

ПОДЯКА

Авторський колектив виражає подяку колективам кафедри захисту інформації та кібербезпеки й науково-дослідного відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П. Корольова за надану можливість у проведенні наукового дослідження.

Особлива подяка від авторського колективу засновникам інтегральної криптографії – Г. Броншпаку, І. Громиці, С. Доценку та Є. Перчику, – за натхнення та можливість повернення до досліджень над якими роботу було розпочату ще в далекому 2005 році.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Грищук Р.В. та Даник Ю.Г., Основи кібернетичної безпеки : Монографія. Житомир: ЖНАЕУ, 2016, с. 636.
[2] Microsoft Security Intelligence Report Volume 24, 2019. [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/en-us/security.
[3] ESET Security Report 2018, 2019. [Електронний ресурс]. – Режим доступу: https://empresas.eset-la.com/novedad/eset-security-report-2018.
[4] Cisco 2018 Annual Cybersecurity Report, 2018. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.
[5] "The Global Risks Report 2019 14th Edition", World Economic Forum, 2019. – Режим доступу: http://wef.ch/risks2019.
[6] Шнайер Б., Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003, с. 806.
[7] W. Diffie та M. E. Hellman, “New Directions in Cryptography,”: IEEE Transactions on Information Theory, 1976, pp. 644-654.
[8] M. Ogiela та L. Ogiela, On Using Cognitive Models in Cryptography. Crans-Montana: IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 2016, pp. 1055-1058.
[9] L. Kocarev and S. Lian, Chaos-based Cryptography Theory, Algorithms and Applications. Springer-Verlag Berlin Heidelberg: Studies in Computational Intelligence, 2011, p. 390.

[10] Ю. Бобало, С. Галюк, М. Климаш and Р. Політанський, Прикладне застосування теорії хаотичних систем у телекомунікаціях : Монографія. Львів: Дрогобич : Коло, 2015, с. 184.
[11] U. Maurer, Constructive Cryptography – A New Paradigm for Security Definitions and Proofs. Springer-Verlag Berlin Heidelberg, 2012, pp. 33-56.
[12] R. Hughes, D. Alde and P. Dyer, Quantum Cryptography, 2019. – Режим доступу: https://arxiv.org/pdf/quant-ph/9504002.pdf.
[13]В. Думачев, Модели и алгоритмы квантовой информации: Монография. Воронеж: ВИМВД, 2009, с. 231.
[14] І. Калюжний, "Квантова криптографія: принципи, проблеми та перспективи", Інформаційні системи, механіка та керування, № 13, сс. 29-37, 2015. – Режим доступу: http://nbuv.gov.ua/UJRN/Ismk_2015_13_5.
[15] Richard J. Hughes D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan and M. Schauer,Quantum Cryptography. NM 87545: University of California Physics Division Los Alamos National Laboratory Los Alamos.
[16] І. Горбенко, О. Кузнєцов та О. Потій, "Проблемы постквантовой криптографии и возможные направления их разрешения в будущем", Радиотехника, № 186, сс. 32-52, 2016.
[17] Н. Птицын, Приложение теории детерминированного хаоса в криптографии. МГТУ им. Баумана, 2002, с. 80.
[18] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems", International J. of Bifurcation and Chaos, № 16(8), pp. 2129-2151, 2006.
[19] В. Шашихин, Н. Богач and В. Чупров, "Проблема малого количества ключей в алгоритме шифрования двумерных данных на основе TENT-отображения", Научно-технические ведомости СПбГПУ, № 2, сс. 19-24, 2012.
[20] U. Maurer and R. Renner, Abstract Cryptography. 2011, pp. 1-21.
[21] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM J. Comput, № 26(5), pp. 1484-1509, 1997.
[22] L. Grover, "A fast quantum mechanical algorithm for database search". – Режим доступу: https://arxiv.org/pdf/quant-ph/9605043.pdf.
[23] L. Chen, S. Jordan and Y. Liu, "Report on Post-Quantum Cryptography", NIST, 2016. – Режим доступу: http://dx.doi.org/10.6028/NIST.IR.8105.
[24] X. Guozhen, L. Mingxin, Q. Lei and L. Xuejia, "New field of cryptography: DNA cryptograph", Chinese Science Bulletin, pp. 1412-1420, 2006.
[25] C. Zhenfu, New Directions of Modern Cryptography. Boca Raton: CRC Press, 2012, p. 400.
[26] Г. Броншпак, И. Громыко, С. Доценко and Е. Перчик, "Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии", Прикладная электроника, № 3, сс. 337-349, 2014. DOI: 10.13140/RG.2.1.1973.2645.
[27] Г. Броншпак, А. Ващенко, И. Громыко, С. Доценко and Е. Перчик, "Криптография нового поколения: интегральные уравнения как альтернатива алгебраической методологии." DOI: 10.13140/RG.2.1.3897.0325.
[28] Г. Броншпак, А. Ващенко, И. Громыко, С. Доценко and Е. Перчик, "Криптография нового поколения: интегральные уравнения как альтернатива алгебраической методологии." DOI: 10.13140/RG.2.1.2497.5523.
[29] И. Громыко, Общая парадигма защиты информации: проблемы защиты информации в аспектах математического моделирования: монография. Харків: ХНУ имени В.Н. Каразина, 2014, с. 216.
[30] И. Громыко, "Криптография сопряженных дискрет." – Режим доступу: https://www.researchgate.net/publication/289980230/.
[31] И. Громыко и К. Швагер, "JAVA-Реализация элементов криптографии сопряженных дискрет", Збірник наукових праць Харківського університету Повітряних Сил, № 3, сс. 79-85, 2016.
[32] Р. Грищук, Зв'язок інтегральних рівнянь Фредгольма першого роду із задачами відновлення інформативних параметрів за матеріалами космічного моніторингу. Житомир: ЖВІРЕ, 2006, сс. 22-23.
[33] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography. CRC Press, 2001, p. 816.
[34] Р. Грищук, Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія. Житомир: РУТА, 2010, с. 280.
[35] C. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, pp. 656-715, 1949.
[36] N. Ferguson, R. Schroeppel and D. Whiting, A simple algebraic representation of Rijndael. Heidelberg: Springer, 2001, pp. 103-111.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023

Ruslan V. Hryshchuk
doctor of Science (Engineering), Professor, Head of the Information Protection and Cyber Security Department.
Serhiy Korolyov Zhytomyr Military Institute, Zhytomyr, Ukraine.
OrcID: 0000-0001-9985-8477
prof.Hry@gmail.com

Olga M. Hryshchuk
engineer.
Serhiy Korolyov Zhytomyr Military Institute, Zhytomyr, Ukraine.
OrcID: 0000-0001-6957-4748
Ol.Hry@i.ua

A GENERALIZED MODEL OF FREDHOLM'S CRYPTOSYSTEM

Abstract. The problem of cyber security in the era of the creation of quantum computers is of particular relevance. Specifically, the data are at risk which are confidential or whose value depends on their integrity. In order to find a way out of the situation which happened in the article, a thorough comprehensive analysis of the current state of the known cryptosystems was carried out, based on a systematic approach. In particular, the advantages and disadvantages of models of cryptosystems which were created on the basis of cognitive cryptography are stated, the theory of dynamic chaos, constructive, quantum and post-quantum cryptography. The issue of cryptosystem models based on DNA algorithms is also raised, proxy cryptosystem models, attribute cryptosystems, packet and non-commutative cryptography. As a result of the research, it was found out that the greatest interest in terms of security today is integral cryptography. The lack of scientifically justified models of cryptosystems based on integrated cryptography has led to the development of one of these models. The model is developed on the basis of the proposed concept, which is based on the main principals of integral cryptography. As a result of the research, a generalized model of the cryptosystem was developed, which in the future is proposed to be called the cryptosystem of Fredholm. It is shown that the essence of the encryption and decryption procedures is reduced to solving the direct and inverse problem, which is described by the integral equation of Fredholm of the first-order. The article emphasizes in particular that compared to the known models of cryptosystems, the proposed model has a number of significant advantages. The first advantage is the guaranteed theoretical and practical cryptostability, which is due to the incorrectness of the inverse decryption problem. The second advantage of the proposed model is the absence of effective algorithms for cryptanalysis due to the lack of prevalence of integral cryptography in modern cyber security systems. The developed model serves the theoretical basis for the further development of appropriate cryptographic algorithms and research of their security parameters.

Keywords: model, cryptosystem, integral equation of Fredholm of the first-order, encryption, decryption, direct and inverse problem.

REFERENCES

[1] Grischuk R.V. and Danyk Yu.G., Osnovy kibernetychnoyi bezpeky _ Monografiya [Fundamentals of cyber security], Zhytomyr: ZhNAEU_ 2016_ p. 636. (In Ukrainian).
[2] Microsoft Security Intelligence Report Volume 24, 2019. Available: https://www.microsoft.com/en-us/security.
[3] ESET Security Report 2018, 2019. Available: https://empresas.eset-la.com/novedad/eset-security-report-2018.
[4] Cisco 2018 Annual Cybersecurity Report, 2018. Available: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.
[5] "The Global Risks Report 2019 14th Edition", World Economic Forum, 2019. Available: http://wef.ch/risks2019.

[6] Shnaier B., Prikladnaya kriptografiya. Protokoly algoritmy ishodnyie teksty na yazike Si, [Applied cryptography. Protocols, algorithms, source texts in the C language] , M. Triumf, 2003 p. 806. (In Ukrainian).
[7] W. Diffie та M. E. Hellman, “New Directions in Cryptography,”: IEEE Transactions on Information Theory, 1976, pp. 644-654.
[8] M. Ogiela and L. Ogiela, On Using Cognitive Models in Cryptography. Crans-Montana: IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 2016, pp. 1055-1058.
[9] L. Kocarev and S. Lian, Chaos-based Cryptography Theory, Algorithms and Applications. Springer-Verlag Berlin Heidelberg: Studies in Computational Intelligence, 2011, p. 390.
[10] Yu. Bobalo, S. Galyuk, M. Klimash and R. Politanskii «Prikladne zastosuvannya teoriyi haotichnih sistem u telekomunikaciyah _ Monografiya, [Applying the theory of chaotic systems in telecoms: Monographs], Lviv: Drogobich Kolo, 2015, p. 184.
[11] U. Maurer, Constructive Cryptography – A New Paradigm for Security Definitions and Proofs. Springer-Verlag Berlin Heidelberg, 2012, pp. 33-56. (In Ukrainian).
[12] R. Hughes, D. Alde and P. Dyer, Quantum Cryptography, 2019. Available: https://arxiv.org/pdf/quant-ph/9504002.pdf.
[13] V. Dumachev, Modeli i algoritmi kvantovoi informaciyi: Monografiya, [Quantum Information Models and Algorithms: Monograph], Voronej:VIMVD, 2009, p. 231. (In Ukrainian).
[14] I. Kalyujnii "Kvantova kriptografiya principi problemi ta perspektivi", Informaciini sistemi mehanika ta keruvannya, [Quantum cryptography: principles, problems and prospects ", Informatsiyni systems, mechanics and management], № 13_ pp. 29-37, 2015. Available: http://nbuv.gov.ua/UJRN/Ismk_2015_13_5.
[15] Richard J. Hughes D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan and M. Schauer,Quantum Cryptography. NM 87545: University of California Physics Division Los Alamos National Laboratory Los Alamos.
[16] I. Gorbenko, O. Kuzniecov ta O. Potii "Problemi postkvantovoi kriptografii i vozmojnie napravleniya ih razresheniya v buduschem", [Problems of post-quantum cryptography and possible directions for their resolution in the future], Radiotehnika, № 186,pp. 32-52, 2016. (In Ukrainian)
[17] N. Pticin, «Prilojenie teorii determinirovannogo haosa v kriptografii», [Application of the theory of deterministic chaos in cryptography], MGTU im. Baumana, 2002, p. 80. (In Ukrainian).
[18] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems", International J. of Bifurcation and Chaos, № 16(8), pp. 2129-2151, 2006.
[19] V. Shashihin, N. Bogach and V. Chuprov, "Problema malogo kolichestva klyuchei v algoritme shifrovaniya dvumernih dannih na osnove TENT otobrajeniya", [The problem of a small number of keys in a two-dimensional data encryption algorithm based on TENT-mapping], Nauchno tehnicheskie vedomosti SPbGPU, № 2, pp. 19-24, 2012.
[20] U. Maurer and R. Renner, Abstract Cryptography. 2011, pp. 1-21.
[21] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM J. Comput, № 26(5), pp. 1484-1509, 1997.
[22] L. Grover, "A fast quantum mechanical algorithm for database search". Available: https://arxiv.org/pdf/quant-ph/9605043.pdf.
[23] L. Chen, S. Jordan and Y. Liu, "Report on Post-Quantum Cryptography", NIST, 2016. Available: http://dx.doi.org/10.6028/NIST.IR.8105.
[24] X. Guozhen, L. Mingxin, Q. Lei and L. Xuejia, "New field of cryptography: DNA cryptograph", Chinese Science Bulletin, pp. 1412-1420, 2006.
[25] C. Zhenfu, New Directions of Modern Cryptography. Boca Raton: CRC Press, 2012, p. 400.
[26] G. Bronshpak, I. Gromiko, S. Docenko and E. Perchik, "Kriptografiya novogo pokoleniya Integralnie uravneniya kak alternativa algebraicheskoi metodologiyi",[New generation cryptography: Integral equations as an alternative to algebraic methodology], Prikladnaya elektronika, № 3, pp. 337-349, 2014. DOI: 10.13140/RG.2.1.1973.2645. (In Ukrainian).
[27] G. Bronshpak, I. Gromiko, S. Docenko and E. Perchik, "Kriptografiya novogo pokoleniya Integralnie uravneniya kak alternativa algebraicheskoi metodologiyi",[New generation cryptography: Integral equations as an alternative to algebraic methodology]. DOI: 10.13140/RG.2.1.3897.0325. (In Ukrainian)
[28] G. Bronshpak, I. Gromiko, S. Docenko and E. Perchik, "Kriptografiya novogo pokoleniya Integralnie uravneniya kak alternativa algebraicheskoi metodologiyi",[New generation cryptography: Integral equations as an alternative to algebraic methodology]. DOI: 10.13140/RG.2.1.2497.5523. (In Ukrainian).

[29] I. Gromiko, «Obschaya paradigma zaschiti informacii_ problemi zaschiti informacii v aspektah matematicheskogo modelirovaniya: monografiya», [The general paradigm of information security: problems of information security in aspects of mathematical modeling: a monograph], Harkiv: HNU imeni V.N. Karazina, 2014, p. 216. (In Ukrainian).

[30] I. Gromiko, "Kriptografiya sopryajennih diskret", [Discrete Related Cryptography]. Available: https://www.researchgate.net/publication/289980230/. (In Ukrainian).

[31] I. Gromiko and K. Shvager, "JAVA Realizaciya elementov kriptografii sopryajennih diskret",[JAVA-Implementation of the elements of cryptography associated discrete], Zbirnik naukovih prac Harkivskogo universitetu Povitryanih Sil, № 3, pp. 79-85, 2016. (In Ukrainian).

[32] R. Grischuk, «Zv'yazok integralnih rivnyan Fredgolma pershogo rodu iz zadachami vidnovlennya informativnih parametriv za materialami kosmichnogo monitoringu», [The connection of Fredholm integral equations of the first kind with the tasks of restoration of informative parameters on the basis of space monitoring materials], Zhytomyr: ZhVIRE, 2006, pp. 22-23. (In Ukrainian).

[33] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography. CRC Press, 2001, p. 816.

[34] R. Grischuk, Teoretichni osnovi modelyuvannya procesiv napadu na informaciyu metodami teorii diferencialnih igor ta diferencialnih peretvoren monografiya, [Theoretical bases of modeling the attacks on information by methods of theories of differential games and differential transformations: monograph], Zhytomyr: RUTA, 2010, p. 280. (In Ukrainian).

[35] C. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, pp. 656-715, 1949.

[36] N. Ferguson, R. Schroeppel and D. Whiting, A simple algebraic representation of Rijndael. Heidelberg: Springer, 2001, pp. 103-111.