Опис завершеної д/б розробки № 2618-п

Сучасні методи аналізу і синтезу криптографічних алгоритмів та протоколів
Современные методы анализа и синтеза криптографических алгоритмов и протоколов.
Modern methods of analysis and synthesis of cryptographic algorithms and protocols.

1. **Номер державної реєстрації теми -№**0113U000944**,** НТУУ «КПІ» - 2618-п.
2. **Науковий керівник -** д. ф.-м. н., доцент Савчук М.М.
   д. ф.-м. н., доцент Савчук М.Н.
   doctor, docent Savchuk M.N.

3. **Суть розробки, основні результати.**

(укр.)

Мета роботи полягає в оцінюванні ефективності криптографічного захисту для певних типів криптосистем, отриманні оцінок їх стійкості відносно атак в залежності від умов, в яких вони функціонують, а також - у використанні нових методів для удосконалення систем криптографічного захисту інформації з урахуванням різних моделей обчислень та перспектив розвитку сучасних напрямків криптоаналізу, засобів обчислювальної техніки.

Отримано аналітичні оцінки верхніх границь диференціальних ймовірностей Фейстель-подібних блочних шифрів, характеристики стійкості незбалансованих схем Фейстеля до диференціального і лінійного криптоаналізу. Розроблено формалізований опис та методику обґрунтування стійкості немарковських симетричних блочних шифрів до диференціального криптоаналізу. Досліджено нові схеми каскадного блокового шифрування, до яких застосована розроблена методика для оцінювання стійкості немарковських шифрів. Отримано оцінки стійкості R-схеми блочного шифрування до диференціального криптоаналізу.

Проаналізована стійкість національного стандарту симетричного шифрування ДСТУ ГОСТ 28147:2009 до атак збоїв, визначені максимальні можливості відомих на сьогодні атак на цей шифр. Вдосконалено атаки збоїв на ДСТУ ГОСТ 28147: 2009 з урахуванням особливостей довгострокових ключових елементів. Проведено експериментальні дослідження атак збоїв. Досліджено метод криптоаналізу на основі обертань, можливості застосування цього методу до криптоаналізу ДСТУ ГОСТ 28147:2009. Отримано оцінки складності криптоаналізу на основі обертань. Проналізовано способи перетворення алгебраїчних нормальних форм у кон'юнктивні нормальні форми з метою подальшого використання *SAT*-розв'язувачів для розв'язування систем нелінійних рівнянь в критоаналізі систем блокового шифрування. Розроблено та реалізовано кубічні атаки на блокові шифри з використанням побічного каналу.

Доведено граничні теореми для розподілів кратних колізій в схемах випадкового розміщення частинок. Обґрунтовано та експериментально досліджено модифікації критеріїв перевірки якості випадкових послідовностей, побудованих з використанням профілю лінійної складності. Запропоновано нові статистичні критерії для перевірки криптографічних властивостей за допомогою Мебіус-аналізу. Проведені експериментальні дослідження властивостей хеш-функцій - фіналістів конкурсу SHA-3. Досліджено імовірності успіху і складності циклічних атак в різних умовах для шифру RSA та моделей криптоперетворень як відповідних випадкових підстановок. Проведені числові розрахунки з допомогою ЕОМ. Проаналізовано генератор випадкових чисел ОС LINUX, зроблена оцінка кількості його вхідної ентропії. Запропоновано та програмно реалізовано алгоритми ідентифікації векторних булевих функцій багатьох змінних за допомогою методу Монте-Карло. Проведено дослідження атак на датчики псевдовипадкових послідовностей на основі еліптичних кривих. Досліджено перемішуючі властивості операцій на множині n-вимірних векторів над простим скінченним полем та можливості їх використання в побудові блочних шифрів.

Побудовано квантовий пінг-понг протокол з використанням багатокубітових станів. Представлено аналіз особливостей роботи протоколу обміну ключами з використанням взаємного навчання нейронних мереж, розглянуто існуючі атаки на протокол. Запропоновано новий імовірнісний алгоритм розв'язку часткового випадку задачі про приховану дію абелевої групи в квантовій моделі обчислень, який може використовуватися для перевірки стійкості односторонніх функцій. Запропоновано методи, що посилюють збереження таємності персональних даних, які обробляються в комп'ютерних системах.

Результати даної НДР отримані з використанням сучасних методів дослідження стійкості систем захисту інформації, криптографічних атак, способів захисту від них та знаходяться на рівні світових аналогів. Запропоновані в роботі модифіковані та нові методи дають можливість отримувати оцінки стійкості для існуючих систем криптографічного захисту інформації, а також використовувати отримані результати при розробці та реалізації нових криптоалгоритмів, визначенні умов безпечного функціонування систем зберігання та передачі інформації, що захищається криптографічними засобами.

(рос.)

Цель работы заключается в оценке эффективности криптографической защиты определенных типов криптосистем, получении оценок их устойчивости относительно атак в зависимости от условий, в которых они функционируют, а также - в использовании новых методов для совершенствования систем криптографической защиты информации с учетом различных моделей вычислений и перспектив развития современных направлений криптоанализа, средств вычислительной техники.

Получены аналитические оценки верхних границ дифференциальных вероятностей фейстель-подобных блочных шифров, характеристики устойчивости несбалансированных схем Фейстеля к дифференциальному и линейного криптоанализу. Разработано формализованное описание и методика обоснования устойчивости немарковских симметричных блочных шифров к дифференциальному криптоанализу. Исследованы новые схемы каскадного блочного шифрования, к которым применена разработанная методика для оценки устойчивости немарковских шифров. Получены оценки устойчивости R-схемы блочного шифрования к дифференциальному криптоанализу.

Проанализирована устойчивость национального стандарта симметричного шифрования ГОСТ 28147: 2009 к атакам сбоев, определены максимальные возможности известных на сегодня атак на этот шифр. Усовершенствованы атаки сбоев на ГОСТ 28147: 2009 с учетом особенностей долгосрочных ключевых элементов. Проведены экспериментальные исследования атак сбоев. Исследован метод криптоанализа на основе вращений, возможности применения этого метода к криптоанализу ГОСТ 28147: 2009. Получены оценки сложности криптоанализа на основе вращений. Проанализировано способы преобразования алгебраических нормальных форм в конъюнктивные нормальные формы с целью дальнейшего использования SAT-решателей для решения систем нелинейных уравнений в критоанализе систем блочного шифрования. Разработаны и реализованы кубические атаки на блочные шифры с использованием побочного канала.

Доказано предельные теоремы для распределений кратных коллизий в схемах случайного размещения частиц. Обосновано и экспериментально исследовано модификации критериев проверки качества случайных последовательностей, построенных с использованием профиля линейной сложности. Предложены новые статистические критерии для проверки криптографических свойств с помощью Мебиус-анализа. Проведены экспериментальные исследования свойств хеш-функций - финалистов конкурса SHA-3. Исследованы вероятности успеха и сложности циклических атак в различных условиях для шифра RSA и моделей криптопреобразования как соответствующих случайных подстановок. Проведенны числовые расчеты с помощью ЭВМ. Проанализирован генератор случайных чисел ОС LINUX, произведена оценка количества его входной энтропии. Предложен и программно реализован алгоритм идентификации

векторных булевых функций многих переменных с помощью метода Монте-Карло. Исследованы перемешивающие свойства операций на множестве n-мерных векторов над простым конечным полем и возможности их использования в построении блочных шифров.

Построен квантовый пинг-понг протокол с использованием многокубитных состояний. Представлен анализ особенностей работы протокола обмена ключами с использованием взаимного обучения нейронных сетей, рассмотрены существующие атаки на протокол. Предложен новый вероятностный алгоритм решения частного случая задачи о скрытом действии абелевой группы в квантовой модели вычислений, который может использоваться для проверки устойчивости односторонних функций. Предложены методы, усиливающие сохранение секретности персональных данных, обрабатываемых в компьютерных системах.

Результаты данной НДР полученны с использованием современных методов исследования стойкости систем защиты информации, криптографических атак, способов защиты от них и находятся на уровне мировых аналогов. Предложенные в работе модифицированые и новые методы позволяют получать оценки стойкости для существующих систем криптографической защиты информации, а также использовать полученные результаты при разработке и реализации новых криптоалгоритмов, определении условий безопасного функционирования систем хранения и передачи защищаемой криптографическими средствами.

(англ.)

The purpose of the work is to assess the effectiveness of encryption for certain types of cryptosystems, obtaining estimates of their relative resistance against attacks depending on the environment in which they operate, and to use new methods to improve cryptographic protection of information according to different models of computation and prospects of modern trends of cryptanalysis and computer abilities.

Analytical evaluation of the upper boundary of the Feistel-like block ciphers differential probabilities, resistance characteristics of unbalanced Feistel circuits to differential and linear cryptanalysis are obtained. A formalized description and method of study of non-Markov symmetric block ciphers resistance to differential cryptanalysis are developed. New schemes of cascade block encryption are investigated, to which a developed method is used for evaluate the stability non-Markov ciphers. The estimates of R-block encryption schemes resistance to differential cryptanalysis are obtained.

The resistance of the national standard of symmetric encryption GOST 28147: 2009 to fault attacks is analysed, maximal possibilities of known attacks on this cipher are identified. The fault attacks on GOST 28147: 2009 with the peculiarities of long-term key elements are improved. Experimental research of fault attacks are done. The complexity of the method of cryptanalysis based on rotations and the possibility of using this method to cryptanalysis of GOST 28147: 2009 are estimated. The ways to convert algebraic normal forms in conjunctive normal forms for further use SAT-solvers for solving systems of nonlinear equations in crytanalysis of blockciphers are analysed. The side channel cube attacks on block ciphers are developed and implemented.

The limit theorems for distributions of multiple collisions schemes in the random placement of particles are proved. The modifications of the tests for quality control of random sequences using linear complexity profile are constructed and experimentally compared. The new statistical criteria for checking cryptographic properties using Mobius analysis are proposed. Experimental study of the properties of hash functions - finalists SHA-3 is done. Investigated The probability of success and complexity of cyclic attacks on RSA encryption and models of cryptoschemes as appropriate random permutations are investigated in different conditions. The relevant numerical calculations on computer are done. The random number generator OS LINUX is analyzed, its input entropy is estimated. A program algorithm for identification of vector Boolean functions of many variables and checking some of their cryptographic characteristics is implemented using the Monte Carlo method. Scramble properties of operations on the set of n-dimensional vectors on simple finite field and their possible use in the construction of block ciphers is investigated.

A quantum ping-pong protocol using poly-q-bites is constructed. The analysis of the features of key exchange protocol using mutual learning neural networks is made, the known attacks on the protocol are analysed. A new probabilistic algorithm for solving a particular case of the problem of hidden action on Abelian groups in quantum computing model that can be used to test the stability of one-way functions is proposed. The methods enhancing the confidentiality of personal data processed in computer systems are proposed.

The results of this research were obtained with the use of modern methods of investigation of information security systems stability, cryptographic attacks, defenses against them and are at international counterparts. The suggested modified and new methods make it possible to estimate security of the existing systems of cryptographic information protection, and use the results in the development and implementation of new encryption algorithms and determination of the conditions of safe operation of the systems storing and transmitting information that is protected by cryptographic means.

4. Наявність охоронних документів на об'єкти права інтелектуальної власності.

Не має

5. Порівняння зі світовими аналогами.

Результати відповідають світовому рівню, а, наприклад, розробки з диференціального криптоаналізу немарковських шифрів, методи дослідження важкозворотних криптографічних перетворень в квантовій моделі обчислень не мають аналогів у світовій практиці.

6. Економічна привабливість

Результати роботи можуть бути застосовані: при проведенні наукових досліджень у галузі криптографічного захисту інформації (структури та підрозділи МО та СБ України, НАН та МОН України); при оцінці надійності та стійкості систем криптозахисту інформації, що проектуються, розробляються та експлуатуються; для створення конкурентноспроможних методик та засобів аналізу криптосистем, оцінки їх стійкості, способів покращення, модифікації; при підготовці фахівців у галузі безпеки інформації. Від застосування розроблених методів для створення нових криптоалгоритмів та покращення існуючих дадуть суттєвий економічний ефект.

7. Потенційні користувачі (галузі, міністерства, підприємства, організації)

МОН України, НАН України, структури та підрозділи міністерства оборони України, СБ України, СВР України, комерційні структури.

8. Стан готовності розробки.

Звіт, документація, програми.

9. Існуючі результати впровадження.

Результати дослідження та застосування диференціального криптоанализу криптографічних блокових симетричних алгоритмів впроваджено в Приватному акціонерному товаристві «Інститут Інформаційних технологій» (м.Харків). Результати роботи використовувались та будуть використовуватись при виконанні науково-дослідних робіт за договором з СЗР України.

Результати роботи впроваджено в начальний процес у нових 2 курсах: «Розділи сучасної криптології» та «Інфраструктура відкритих ключів» для магістрів Фізико-технічного інституту. Створено 2 нових розділу: «Методи диференціального криптоаналізу» у магістерському фаховому курсі «Методи криптоаналізу» та «Локально комутативні відображення в класичній та квантовій моделі обчислень» для дисципліни «Спеціальні розділи криптології». Створено 3 лабораторні роботи: «Диференціальний криптоаналіз шифру Хейса» та «Лінійний криптоаналіз шифру Хейса» для дисципліни

«Розділи сучасної криптології»; «Атака на криптографічний протокол з нульовим розголошенням» для дисципліни «Асиметричні криптосистеми та протоколи». За результатами науково-дослідної роботи подано до захисту кандидатську дисертацію Яковлєва С.В. «Аналітичні оцінки стійкості немарковських симетричних блочних шифрів до диференціального криптоаналізу».

10. Назва організації, телефон, E-mail

НТУУ"КПІ", Фізико-технічний інститут, кафедра математичних методів захисту інформації, р.т.406-81-76, mmzi@ntu-kpi.kiev.ua

11. Перелік публікацій за матеріалами досліджень за період виконання розробки

1. Завадская Л.А., Семибаламут М.А. Профиль линейной сложности как средство оценки качества случайных последовательностей // Проблемы управления и інформатики. – 2014 (в редакції).
2. Ковальчук Л., Беспалов О., Огнев П. Рекурентні алгоритми обчислення кореня довільного степеню у кільці лишків // «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013,№1(25). - С. 58-67.
3. Ковальчук Л.В., Бездетній В.Т. «Верхние оценки средних вероятностей разностных характеристик блочного шифра с чередованием марковских и обобщённо-марковских преобразований», «Кибернетика и системный анализ», том 50, №3, 2014, стр. 71-79.
4. Ковальчук Л.В., Алексейчук А.М. Результати досліджень криптографічних властивостей алгоритму шифрування «Калина»» // Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації», вип. 1(25), 2014, с. 5-24.
5. Ковальчук Л.В., Лисенко Н.В., Скрипник Л.В. Порушення структури факторгрупи групи при заміні операцій модульного додавання на по компонентне додавання // Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації», вип. 1(25), 2014, с. 24-34.
6. Savchuk M. Cryptografy: Classical and Modern // INFORMATION SECURITY. International Training Workshop. – Kyiv-2014.-International Training Conference and Workshop on. Information Security and Responsible Science as Integral Components of a Safe and Secure Global Knowledge Society - p. 54-68.
7. Фаль А.М. Стандартизация в сфере защиты персональных даннях // Кибернетика и системный анализ. – 2014. №2. – С.181-184
8. Фаль А.М.,Козак В.Ф. Проблемы защиты персональных данных при использовании облачных вичислений // Кибернетика и системный анализ. – 2014. - №5. – С.132 -138.
9. Фесенко А. В. Складність задачі про приховану дію абелевої групи в квантовій моделі обчислень // Східно-Європейський журнал передових технологій. – 2013. – №5(65). – с. 45-49.
10. Фесенко А. В. Сведение атаки на основе открытого текста на локально коммутативный шифр к алгебраическим задачам в классической и квантовой моделях вычислений // Проблемы управления и информатики. – 2014. – № 3. – с. 148-156.
11. Фесенко А. В. Зведення задачі обернення кусково-лінійноговідображення до задачі про прихованудію на торсор над абелевою групою // Наукові записки НаУКМА. Серія Комп'ютерні науки. – 2014, №163.
12. Фесенко А. В. Уязвимости криптопримитивов на основе задачи поиска сопрягающего элемента и степени в квантовой модели вычислений // Кибернетика и системный анализ. – 2014. – Т. 50. - №5. – с. 184-186.

13. Фесенко А. В. Поліноміальна еквівалентність атак з відомимвідкритим текстом на довільний симетричний і ендоморфний шифри // Вісник Київського національного університету імені Тараса Шевченка. Серія кібернетика. (в редакції)

14. Яковлєв С.В. Доказова та практична стійкість R-схеми блочного шифрування до диференціального криптоаналізу // Вісник Національного університету "Львівська політехніка" (секція "Комп'ютерні науки та інформаційні технології"). - 2013 р. – с.107-113.

15. Яковлєв С.В. Методика обґрунтування стійкості немарковських симетричних блочних шифрів до диференціального криптоаналізу // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013, „№1(25). – С.74-80.

Рішенням Вченої ради ФТІ протокол № 11/2014 від 26.11.2014 р. науково-дослідна робота визнана виконаною.

Науковий керівник НДР **Савчук М.М.**

Керівник структурного підрозділу **Новіков О.М.**