Алгебраїчно-ймовірнісні методи дослідження стійкості криптографічних алгоритмів і протоколів

Алгебраично-вероятностные методы исследования стойкости и эффективности криптографических алгоритмов и протоколов.

Algebraic-probabilistic methods of investigation of cryptographic algorithms and protocols resistans and effectiveness.

1. **Номер державної реєстрації теми - 0108U001549.**
2. **Науковий керівник -** д.ф.-м.н. Савчук М.М.
3. **Суть розробки, основні результати.**

(укр.)

Мета роботи полягає у розробці та удосконаленні алгебраїчно-ймовірнісних методів дослідження криптографічних перетворень, аналізу симетричних та асиметричних алгоритмів шифрування, способів автентифікації, криптографічних протоколів з урахуванням останніх досягнень криптології і застосування результатів для оцінки стійкості та ефективності сучасних криптосистем та криптографічних протоколів, удосконалення методів криптографічного захисту інформації.

Розроблено ефективні алгоритми розв'язання лінійних систем рівнянь над скінченими полями зі спотвореннями; алгоритми розв'язання цілочислових рівнянь спеціального виду. Удосконалено та розроблено інноваційні методи і програми алгебраїчних атак на потокові шифри. Отримані оцінки характеристик булевих функцій, важкооборотних функцій. Розроблено методи криптоаналізу, що оптимально використовують кореляційні залежності алгебраїчні методи та засоби перебору. Створено нові критерії для перевірки криптографічної якості послідовностей.

(рос.)

Цель работы заключается в разработке и усовершенствование алгебраично-вероятностных методов исследования криптографических преобразований, анализа симметричных и асимметричных алгоритмов шифрования, способов автентификации, криптографических протоколов, с учетом последних достижений криптологии и применения результатов для оценки стойкости и эффективности современных криптосистем и криптографических протоколов, усовершенствования методов криптографической защиты информации.

Разработаны эффективные алгоритмы решения линейных систем уравнений над конечными полями с искажениями; алгоритмы решения целочисленных уравнений специального вида. Усовершенствованы и разработаны инновационные методы и программы алгебраических атак на поточные шифры. Получены оценки характеристик булевых функций, односторонних функций. Разработаны методы криптоанализа, которые оптимально используют корреляционные зависимости, алгебраические методы и средства перебора. Созданы новые критерии для проверки криптографического качества последовательности.

(англ.)

The purpose of work consists in development and improvement probabilistic for algebra methods of research of cryptographic transformations, analysis of symmetric and asymmetric algorithms of enciphering, methods of avtentifikacii, cryptographic protocols, taking into account the last achievements of kriptologii and application of results for the estimation of firmness and efficiency of modern kriptosistem and cryptographic protocols, improvement of methods of cryptographic priv.

The effective algorithms of decision of the linear systems of equalizations are developed above the complete fields with distortions; algorithms of rozv"yazannya of cilochislovikh equalizations of the special kind. Innovative methods and programs of attacks of algebra are improved and developed on potokovi codes. Got estimations of descriptions of boole functions, vazhkooborotnikh functions. The methods of kriptoanalizu are developed, that optimum the methods of algebra and facilities of surplus use cross-correlation dependences.

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

Немає

5. **Порівняння зі світовими аналогами.**

На рівні світових аналогів.

6. **Потенційні користувачі.**

Отримані в роботі результати можуть бути застосовані:

при проведенні наукових досліджень у галузі криптографічного захисту інформації, при оцінці надійності та стійкості систем криптографічного захисту інформації, що проектуються, розробляються та експлуатуються; для створення конкурентноспроможних методик та засобів аналізу криптосистем та оцінки їх стійкості; при підготовці фахівців у галузі безпеки інформації на спеціальних курсах підвищення кваліфікації.

7. **Стан готовності розробки.**

Розроблено та удосконалено алгебраїчно-ймовірнісні методи дослідження криптографічних перетворень; проведено аналіз симетричних та асиметричних алгоритмів шифрування, способів автентифікації, криптографічних протоколів з урахуванням останніх досягнень криптології. Створено нові ефективні методи, процедури та алгоритми аналізу, отримання оцінок ефективності криптоатак на системи захисту інформації, запропоновано методи та засоби захисту від таких атак та удосконалення систем криптографічного захисту інформації.

Систематизовано теоретичні результати, на яких базуються алгебраїчно-ймовірнісні методи, описано і обґрунтовано розроблені алгоритми та методи криптоаналізу. Досліджено різні криптографічні властивості булевих функцій, криптографічних перетворень, хеш-функцій, важко оборотних функцій. Розроблено алгоритми криптоаналізу, які оптимально поєднують алгебраїчні, ймовірнісні методи, а також методи перебору варіантів. Розроблено, теоретично обґрунтовано метод імовірнісних алгебраїчних атак на потокові та блокові шифри. Формалізовано модель постквантових обчислень, зокрема, отримано постквантові оцінки складності обернення односторонніх функцій. Розроблено нові критерії для перевірки криптографічної якості випадкових послідовностей та послідовностей на вузлах шифраторів, методику перевірки незалежності статистичних тестів. Застосовано отримані результати для оцінки стійкості та ефективності сучасних криптосистем та криптографічних протоколів, удосконалення методів криптографічного захисту інформації

.

8. **Існуючі результати впровадження**.

Результати теоретико-експериментальних досліджень впроваджено в начальний процес у спеціальних курсах: «Симетрична криптографія», «Асиметричні криптографічні системи і протоколи криптографія», «Спеціальні розділи обчислювальної математики», «Основи криптографії», «Методи реалізації криптографічних механізмів», «Методи криптоаналізу», «Спеціальні розділи криптології»

9. **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

10. Перелік публікацій за матеріалами досліджень за період виконання розробки

1. *Яковлев С.* Поширення оцінок Ніберг на каскадні схеми Фейстеля // XIII Международная научно-практическая конференция. Безопасность информации в информационно-телекоммуникационных системах, 18-21 мая 2010, Киев. Тезисы докладов. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2010. –С.39-39.
2. *Ковальчук Л.,Корчагин И.* Улучшение статистических свойств выходной последовательности генераторов псевдослучайных чисел, базирующихся на линейных регистрах сдвига // XIII Международная научно-практическая конференция. Безопасность информации в информационно-телекоммуникационных системах, 18-21 мая 2010, Киев. Тезисы докладов. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2010,. –С.51-51.
3. *Скрыпник Л., Ковальчук Л., Бездетный В.* Методика использования шаблонов для проверки независимости статистических тестов // XIII Международная научно-практическая конференция. Безопасность информации в информационно-телекоммуникационных системах, 18-21 мая 2010, Киев. Тезисы докладов. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2010. –С.23-23.
4. *Ковальчук Л., Яцук А., Чуланов А.* Исследование обобщенной методики проверки независимости статистических тестов при различных параметрах тестирования // XIII Международная научно-практическая конференция. Безопасность информации в информационно-телекоммуникационных системах, 18-21 мая 2010, Киев. Тезисы докладов. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2010. –С.23-24.
5. *L.V.Skrypnik, L.V.Kovalchuk, V.T. Bezditnyi.* Method of statistical tests independence checking // IX International conference. –Minsk, September 7-11, 2010. Computer data analysis and modeling: Complex stochastic data and systems. – V.2, -P.71-74.
6. *L.V.Kovalchuk, V.T. Bezditnyi.* Practical security estimations of block cipher KALINA against integer differential cryptoanalysis // International conference. Modern stochastics: theory and application II. September 7-11, 2010, Kiev, Ukraine. Abstracts. –Kyiv: Taras Shevchenko National University of Kyiv, 2010. –P.25-26.
7. *L.V.Kovalchuk, A.S. Yatsuk, V.T. Bezditnyi.* Practical Using of Metod of Statistical Tests Independence Checking // Proceedings of the International Conference “Statistical Methods of Signal and Data Processing”, Kiev, October 13-14, 2010. - Kyiv: National Aviation University, 2010 -P.161-163.
8. *Єндовицький П.О.* Точна асимптотична оцінка розміру групи в узагальненні парадоксу днів народжень // Сьома міжнародна науково-практична конференція

«Інтернет-Освіта-Наука-2010» 28 вересня – 03 жовтня, 2010: Збірник матеріалів конференції. –Вінниця: ВНТУ, 2010. –С.400.

9. *Єндовицький П.О.* Уточнение асимптотической аппроксимации раз мера группі в парадоксе дней роджений.- Кибернетика и системный анализ.-2010.-№3. –С.185-188.
10. *Єндовицький П.О.* Точна асимптотична оцінка розміру групи в узагальненні парадоксу днів народжень // –Наукові вісті НТУУ «КПІ».-2010. -№4(72). –с.55-59.
11. *Endovytsky P.* Asymtotic behavior of group size in the birthday paradox // International conference Modern stohastics: theory and application 2.Abstracts. –Kyiv, Ukraine.: Taras Shevchenko national University of Kyiv, September 7-11, 2010. –P.23-24.
12. *Yakovlev S.* Upper bounds of r-round differential probability of unbalanced misty-like ciphers // International conference Modern stohastics: theory and application 2. Abstracts. –Kyiv, Ukraine.: Taras Shevchenko national University of Kyiv, September 7-11, 2010. –P.29
13. *Савчук М.Н.* О работах киевской школи теоретической криптографии // Кибернетика и системный анализ. –Том 46, №3, май-июнь 2010. –С.52-68
14. *Михайло Савчук, Олександр Валецький.* Роздільні статистики в схемах розміщення та тести для бінарних послідовностей // «ІНТЕРНЕТ-ОСВІТА-НАУКА-2010», сьома міжнародна конференція (ІОН-2010), 28 вересня-3 жовтня, 2010 : Збірник матеріалів конференції. –Вінниця : ВНТУ, 2010 – С.389.
15. *Андрій Фесенко.* Аналіз стійкості криптосистеми з відкритим ключем на скінченій не комутативній групі в квантовій моделі обчислень // «ІНТЕРНЕТ-ОСВІТА-НАУКА-2010», сьома міжнародна конференція (ІОН-2010), 28 вересня-3 жовтня, 2010 : Збірник матеріалів конференції. –Вінниця : ВНТУ, 2010 – С.393.
16. *Сергій Яковлев, Євген Коробов.* Псевдофейстелевські перетворення та їх диференціальні характеристики // «ІНТЕРНЕТ-ОСВІТА-НАУКА-2010», сьома міжнародна конференція (ІОН-2010), 28 вересня - 3 жовтня, 2010: Збірник матеріалів конференції. –Вінниця : ВНТУ, 2010 – С.395.
17. *Сергій Яковлев, Дмитро Коваль.* Деякі властивості експоненціальних перетворень у скінчених полях // «ІНТЕРНЕТ-ОСВІТА-НАУКА-2010», сьома міжнародна конференція (ІОН-2010), 28 вересня-3 жовтня, 2010: Збірник матеріалів конференції. –Вінниця : ВНТУ, 2010 – С.404.
18. *Savchuk M.N.* Multidimensional statistical tests for binary sequences // International Conference Modern Stochastics: Theory and Applications II, September 7-11, 2010, Kyiv, Ukraine. Abstracts. –Kyiv: Taras Shevchenko National University of Kyiv, 2010. – P.27-28.

19. *Савчук М.М.* Векторні випадкові процеси і статистичні тести для бінарних послідовностей // Наукові вісті КПІ. - №4(72). – С.100-104.
20. *Maksym Semybalamut, Ludmyla Zavadska.* Linear Complexity Profile Test LP-test // Statistical methods of signal and data processing (SMSDP-2010). Proceeding October 13-14, 2010 Kiev, Ukraine. Kyiv: National Aviation University, 2010 –P.141-142.
21. *Andrey Fesenko.* Postquantum Resistance Crypto Primitiv over Finite Non-commutative Groups // Statistical methods of signal and data processing (SMSDP-2010). Proceeding October 13-14, 2010 Kiev, Ukraine. Kyiv: National Aviation University, 2010 –P.156-157.
22. *Байденко П. В.* Ефективні по швидкодії алгоритми факторізації для різних моделей обчислення // Теоретичні і прикладні проблеми фізики, математики та інформатики. 7-а Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 23 квітня 2010 р. –Збірка тез доповідей. Частина 2. – Київ: Київський політехнічний інститут, 2010 –С.15-16.
23. *Андросов А.В.* Дослідження ефективності алгоритмів факторизації чисел з експоненційною та субекспоненційною складністю // Теоретичні і прикладні проблеми фізики, математики та інформатики. 7-а Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 23 квітня 2010 р. – Збірка тез доповідей. Частина 2. –Київ: Київський політехнічний інститут, 2010 – С.68-69.
24. *Довгань К.* Емпіричні оцінки стійкості незбалансованих схем Фейстеля до криптоаналітичних атак // Теоретичні і прикладні проблеми фізики, математики та інформатики. 7-а Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 23 квітня 2010 р. –Збірка тез доповідей. Частина 2. – Київ: Київський політехнічний інститут, 2010 –С.78-79.
25. *Зайцева Н.Ю.* Про генерування псевдовипадкових послідовностей на основі еліптичних кривих // Теоретичні і прикладні проблеми фізики, математики та інформатики. 7-а Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 23 квітня 2010 р. –Збірка тез доповідей. Частина 2. – Київ: Київський політехнічний інститут, 2010 –С.80-81.
26. *Комаров С.*С. Емпіричні оцінки криптографічних властивостей булевих функцій з відомим рівнем стійкості до алгебраїчних атак // Теоретичні і прикладні проблеми фізики, математики та інформатики. 7-а Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 23 квітня 2010 р. –Збірка тез доповідей. Частина 2. –Київ: Київський політехнічний інститут, 2010 –С.86-87.
27. *Лях С.* Побудова та дослідження системи електронного голосування на основі алгоритму сліпого підпису // Теоретичні і прикладні проблеми фізики, математики

та інформатики. 7-а Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 23 квітня 2010 р. –Збірка тез доповідей. Частина 2. – Київ: Київський політехнічний інститут, 2010 –С.90-91.

28. *Завадська Л.*В., *Семибаламут М.* Побудова тесту для оцінки якості випадкових послідовностей на основі профілю лінійної складності // Теоретичні і прикладні проблеми фізики, математики та інформатики. 7-а Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 23 квітня 2010 р. – Збірка тез доповідей. Частина 2. –Київ: Київський політехнічний інститут, 2010 – С.98-99.
29. *Яцук А., Чуланов А.* Исследование методики проверки независимости текстов // Теоретичні і прикладні проблеми фізики, математики та інформатики. 7-а Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 23 квітня 2010 р. –Збірка тез доповідей. Частина 2. –Київ: Київський політехнічний інститут, 2010 –С.110-111.