«Дослідження та застосування методів криптоаналізу важкооборотних криптографічних перетворень в класичній та квантовій моделі обчислень» *(Фізико-технічний інститут, керівник М.М.Савчук, 2015-2016 р. – 188 690 тис. грн.)*

Исследование и применение методов криптоанализа односторонних криптографических преобразований в классической и квантовой модели вычислений.
Research and application methods of cryptanalysis of unilateral cryptographic transformations in classical and quantum computing model.

1. **Номер державної реєстрації теми – 0115U000254**
2. **Науковий керівник**
   Савчук Михайло Миколайович, д.ф.-м.н, доцент
   Савчук Михаил Николаевич, д.ф.-м.н, доцент
   Savchuk Mikhael

3. **Номер реєстрації в університеті.**

4. **Суть розробки, основні результати.**
   (укр.)

Модифіковано та розвинуто методи криптоаналізу важкооборотних криптографічних перетворень в класичній та квантовій моделі обчислень. Побудовано нові статистичні критерії визначення властивостей та характеристик випадкових, псевдовипадкових послідовностей та генераторів таких послідовностей. Розроблено методи обчислення аналітичних оцінок стійкості немарковських симетричних блочних шифрів до диференціального та лінійного криптоаналізу із урахуванням особливостей внутрішньої структури шифру. Побудовано верхні оцінки середніх ймовірностей цілочисельних диференціалів з урахуванням особливостей внутрішньої структури ітерацій блокового шифру. Досліджено ймовірнісні характеристики подій, пов'язаних з криптоаналізом шифротекстів з перекриттям гамми при інтенсивному їх використанні. Отримано характеристики, оцінки, умови застосування важкооборотних перетворень в легкій криптографії з урахуванням компромісу швидкодії, пам'яті та стійкості. Запропоновано та реалізовано програмно модифікований алгоритм кубічної атаки на шифр Halka.

Опис нових характеристик класу алгебраїчних задач, застосування криптографічних методів для забезпечення безпеки хмарних обчислень та характеристики запропонованих рішень. Дана оцінка можливості застосування методів розв'язання алгебраїчних задач в квантовій моделі. Нові методи отримання оцінок стійкості та ефективності криптосистем певних класів та криптографічних протоколів до атак як з використанням класичної та квантової моделі обчислень. Комп'ютерні реалізації запропонованих методів, алгоритмів криптоаналізу симетричних та асиметричних систем криптографічного захисту інформації.

(рос.)

Модифицированы и развиты методы криптоанализа односторонних криптографичных преобразований в классической и квантовой модели исчислений. Построены новые статистические критерии определения свойств и характеристик случай-ных и псевдослучайных последовательностей и их генераторов. Разработаны методы вычисления аналитических оценок стойкости немарковских симметричных блочных шифров к дифференциальному и линейному криптоанализу с учетом особенностей внутренней структуры шифра. Построена верхняя оценка вероятностей целочисленных дифференциалов с учетом особенностей внутренней структуры итераций блокового шифра. Исследованы вероятностные характеристики событий, связанных с криптоанализом шифротекстов с перекрытием гаммы при интенсивном их использовании. Получены характеристики, оценки, условия использования односторонних преобразований в легкой криптографии с учетом компромиса скорости, памяти и стойкости. Предложен и реализован програмно модифицированый алгоритм кубичной атаки на шифр Halka.

Описаны новые характеристики класса алгебраичных задач использования криптографических методов для обеспечения безопасности вычислений в «облаке» и характеристики предложенных решений. Дана оценка возможности использования методов решения алгебраических задач в квантовой модели. Новые методы получения оценок стойкости и эффективности криптосистем определенных классов и криптографических протоколов к атакам с использованием классической и квантовой моделей исчислений. Компьютерные реализации предложеных методов, алгоритмов криптоанализа симметричных и асимметричных систем КЗИ.

(англ.)

Cryptanalytical methods of one-way mappings are modified and developed in classical and quantum computational model. New statistical criteria are proposed for evaluation of random and pseudorandom generators' quality. Security evaluation methods against differential and linear cryptanalysis are developed for non-Markov symmetric block ciphers with their structural specific taken into consideration. Upper bounds of average probabilities of integral differentials are estimated for some classes of mappings. Probabilistic properties of events are investigated in cryptanalysis of keystream overlapping with intensive usage. New estimates, conditions and features are proposed for lightweight cryptography with time/memory/security tradeoffs. Modified cubic attack for Halka cipher are proposed and implemented.

New parameters and features are described for cryptographic methods of cloud security computations. Applicability of algebraic methods are evaluated in quantum model, also as their implementation to security estimation of specific cryptosystems in different computational models. Proposed methods and algorithms are implemented in software.

5. **Наявність охоронних документів на об'єкти права інтелектуальної власності.** Немає
6. **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.

7. **Економічна привабливість для просування на ринок.**
Покращення характеристик існуючих методів, алгоритмів та способів криптографічного захисту інформації, застосування яких суттєво зменшить затрати в процесі розробки, побудови, тестування та експлуатації систем криптографічного захисту інформації.
8. **Потенційні користувачі (галузі, міністерства, підприємства, організації).** Результати роботи можуть бути застосовані:
при проведенні наукових досліджень у галузі криптографічного захисту інформації; 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, зокрема, в структурах та підрозділах міністерства оборони України, СБ України, НАН України, МОН України.
9. **Стан готовності розробки:** Методи, алгоритми, способи криптоаналізу і синтезу систем криптографічного захисту інформації, комп'ютерні програми. Звіт, документація.

10. **Існуючі результати впровадження**.

Захищено 1 кандидатську дисертацію.

1.Створено 2 нових лекційний курса для магістрів за напрямами «Прикладна математика»:

- «Спеціальні розділи сучасної криптології 1» за робочою назвою «Диференціальний, лінійних та інтегральний криптоаналіз блокових шифрів»;
- та «Спеціальні розділи сучасної криптології 2» за робочою назвою «Інфраструктура відкритих ключів».

2. Створено 3 нових лабораторні роботи до курсу «Спеціальні розділи сучасної криптології 1»:

- Диференціальний криптоаналіз блокових шифрів;
- Лінійний криптоаналіз блокових шифрів;
- Інтегральний криптоаналіз блокових шифрів.

3. Використано у вигляді нового розділу «Лінійний і інтегральний криптоаналіз блокових шифрів» в курсі «Методи крипто аналізу» для магістрів за напрямами «Прикладна математика».

За результатом роботи укладено **2** госпдоговори на НДР зі Службою зовнішньої розвідки України: «Дослідження та застосування сучасних математичних методів аналізу окремих перетворень у системах криптографічного захисту інформації» (шифр «Мокрель»); «Дослідження методів криптоаналізу в застосуванні до сучасних систем криптографічного захисту інформації з урахуванням перспектив розвитку квантових обчислень» (шифр «Кобія»).

11. **Форма участі інвестора** (*яка краща форма участі в реалізації результатів проекту інвестора: частка в проекті%, частка від прибутку%, інше*) не має
12. **Обсяг інвестицій** (*необхідна для результатів проекту сума інвестицій в доларах США*). Не має
13. **Мета інвестицій** (*розширення бізнесу, створення нового підприємства, інше*). Інвестиції не використовуються.
14. **Назва підрозділу, телефон, e-mail. ФТІ, кафедра ММЗІ, 204-81-76, mmzi@pti.kpi.ua**

15. **Перелік публікацій за матеріалами досліджень за період виконання розробки**

Публікації в журналах, що входять до наукометричних баз даних Scopus:

1. L Kovalchuk, A. Bessalov. Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to Edvards Curves Over Prime Field// Cybernetics and Systems Analysis, volume 51, issue 2, 2015, p. 165-172.
2. Завадська Л.О., Семибаламут М.А. Профиль линейной сложности как средство оценки качества случайных последовательностей // Проблемы управления и информатики, 2015, №2(18). –с.124-136.
3. В. К. Задирака, А. М. Кудин, П. В. Селюх, И. В. Швидченко // Облачные технологии: новые возможности вычислительного криптоанализа // Проблемы управления и информатики : международный научно-технический журнал. - 2016. - N 1. - С. 148-155.
4. Алексейчук А.М., Ковальчук Л.В. Шевцов А.С., Яковлев С.В. О криптографических свойствах нового национального стандарта шифрования Украины// Кибернетика и системный анализ.- 2016.-Том 52,№3.-С.16-31.
5. Ковальчук Л.В., Бессалов А.В., Беспалов А.Ю. Алгоритмы генерации базовой точки кривой Эдвардса с использованием критериев делимости точки // Кибернетика и системный анализ.- 2016.-Том 52,№5.-С.14-24.

Публікації в журналах, що входять до інших наукометричних баз даних:

6. Ковальчук Л.В. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композицій ключового суматора, блоку підстановки та лінійного (над деяким кільцем) оператора./ Ковальчук Л.В., Кучинська Н.В. Скрипник Л.В.// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - вип. 1(29). – 2015р.

Публікації в фахових журналах:

7. Яковлев С. В. Атаки збоїв на шифр ДСТУ ГОСТ 28147:2009 // Інформаційна безпека. – 2015. – № 2(18). – С. 124–136.

Участь у міжнародних конференціях:

1. Savchuk M.N. Functional limit theorem for a non-equiprobable allocation of particles by series // International Conference "Probability, Reliability and Stochastic Optimization", April 7-10, 2015, Kyiv, Ukraine, Conftrence Materials. – P.82.

2. Savchuk M.N. Classical and modern cryptography // International Conference "Probability, Reliability and Stochastic Optimization", April 7-10, 2015, Kyiv, Ukraine, Conftrence Materials. – P.29.

3. Фаль О.М., Шевченко А. Side channel cube attack on cipher Halka// International Conference "Probability, Reliability and Stochastic Optimization", April 7-10, 2015, Kyiv, Ukraine, Conftrence Materials.

4. Fesenko A.V. Polinomial equivalence of known-plaintext attacks on symmetric and endomorfhic ciphers// International Conference "Probability, Reliability and Stochastic Optimization", April 7-10, 2015, Kyiv, Ukraine, Conftrence Materials.

5. Yakovliev S.V. Provable Security of SAFER-like Substitution-Permutation Network against Differential Cryptanalysis// International Conference "Probability, Reliability and Stochastic Optimization», April 7-10, 2015, Kyiv, Ukraine, Conftrence Materials.

6. Yakovliev S.V. Improved Security Evaluation of DSTU 7624:2014 Cipher against Differential and Linear Cryptanalysis// The Fifth International Scientific Conference "Information Technology and Computer Engineering", - Івано-Франківськ – Вінниця - 27.05.2015

7. Яковлєв С. Доказова стійкість ускладнених схем Фейстеля до диференціального та лінійного криптоаналізу// XVII Міжнародна науково-практична конференція "Безпека інформації в інформаційно-телекомунікаційних системах. – Київ, 26.05.2015

8. Ковальчук Л. Порівняльний аналіз алгоритмів генерації базової точки на кривій Едвардса./ Ковальчук Л., Бессалов А., Беспалов О.// Матеріали XVII міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах» 26-28 травня 2015року м. Київ, с/к «Пуща-Озерна» - с.32-33.

9. Ковальчук Л. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композицій ключового суматора, блоку підстановки та лінійного (над деяким кільцем) оператора./ Ковальчук Л., Кучинська Н. // Матеріали XVII міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах» 26-28 травня 2015року м. Київ, с/к «Пуща-Озерна» -С.34-35.

10. Ковальчук Л. Порівняння операцій модульного та по компонентного додавання на множині п-мірних вкторів над простим скінченним полем./ Ковальчук Л., Лисенко Н., Красніков С. // Матеріали XVII міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах» 26-28 травня 2015року м. Київ, с/к «Пуща-Озерна» - С.36-37.

11. Kovalchuk L.V. The upper bounds of the integer differentials average probabilities for composition of the key adder, substitution blocks and the blockstructured linear operator.// L.V. Kovalchuk, N.V. Kuchinska, V.T. Bezditnyi// International conference Probability, reliability and stochastic optimization, Kiyv, Ukraine.. - april 7-10. - 2015. – p. 28-29. (Матеріали конференції Імовірність, надійність та стохастична оптимізація Міжнародна конференція PRESTO)

12. Фесенко А.В. Побудова загальної моделі атаки на основі обертань для шифрів на основі мережі Фейстеля / А.В. Фесенко // Матеріали міжнародної наукової конференції “Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту (ISDMCI’2015)”, с. Залізний Порт, 25-28 травня. – Херсон: Видавництво ХНТУ, 2015. – С. 164.

13. Фесенко А.В. Узагальнена модель симетричного шифру / А.В. Фесенко // Тези доповідей XVII Міжнародної науково-практичної конференції “Безпека інформації у інформаційно-телекомунікаційних системах”, м. Київ, 26-28 травня 2015 р.

14. Ковальчук Л.В., Теліженко А.Б. Модифікація тестів Уілкоксона та Манна-Уітні для перевірки однорідності виборок з дискретним розподілом // Матеріали XVIII Міжнародної

науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Випуск 18 (26-28 травня 2016р., м. Київ, Україна) - С.26.
15. Лессік Д.М., Фаль О.М.Сертифікація систем менеджменту інформаційної безпеки у відповідно до вимог міжнародного стандарту ISOO/IEC 27001:2013 // Матеріали XVIII Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Випуск 18 (26-28 травня 2016р., м. Київ, Україна) - С. 85.
16. Ковальчук Л.В., Кучинська Н.В. Оцінки практичної стійкості модифікованих гост-подібних та калино-подібних алгоритмів відносно цілочисельного різницевого криптоаналізу // Матеріали XVIII Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Випуск 18 (26-28 травня 2016р., м. Київ, Україна) - С. 27.
17. Ковальчук Л.В., Беспалов О.Ю. Використання апарату еліптичних кривих для факторизації і перевірки незвідності поліномів над скінченним полем // Матеріали XVIII Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Випуск 18 (26-28 травня 2016р., м. Київ, Україна) - С. 28
18. Яковлєв С.В., Байбуз М.А. Метод оцінювання стійкості калина-подібних блокових шифрів до диференціального та лінійного криптоаналізу // Матеріали XVIII Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Випуск 18 (26-28 травня 2016р., м. Київ, Україна) - С.69.
5 публікацій зі студентами,зокрема, в наведеному переліку - під номерами 15, 18.

За результатами науково-дослідної роботи опубліковано **7 статей** в фахових наукових журналах з них: **4 - SKOPUS** , **1** в інших **НМБ** , 2 в фахових журналах, **36 тез** матеріалів конференцій, з них **18 тез** наукових міжнародних конференцій, **5** доповідей на наукових семінарах. **Залучення студентів до виконання НДР:** кількість студентів, які залучалися до НДР – **12**; за темою НДР захищено **23** бакалаврських, **5** робіт спеціалістів та **15** магістерських робіт студентами Фізико-технічного інституту.

16. Ключові слова до розробки:

стійкість систем криптографіного захисту, криптоаналіз, складність алгоритмів, хмарні обчислення, легка криптографія, диференціальний аналіз, квантова модель обчислень, псевдовипадкові послідовності, постквантова стійкість