Дослідження методів криптографічного аналізу систем захисту інформації в класичній та квантовій моделях обчислень з урахуванням додаткових даних та умов функціонування

Исследования методов криптографического анализа систем защиты информации в классической и квантовой моделях вычислений с учетом дополнительных данных и условий функционирования

Research methods of analysis of cryptographic information security systems in classical and quantum computing models with the additional data and operating conditions

1. **Номер державної реєстрації** . 0117U000500

2. **Науковий керівник** (вчений ступінь, звання)
Савчук Михайло Миколаєвич, Савчук Михаил Николаевич, Savchuk Mikhael

3. Суть розробки, основні результати

(укр.)

Побудовано моделі для немарковських SP-мереж, які використовують декілька різних S - блоків на одному раунді шифрування, уточнено алгоритми обчислення верхніх меж ймовірностей диференціалів. Розроблено критерії практичного відбору ARX- криптопримітивів з певними властивостями на основі автоматичного оцінювання стійкості. Проведено криптоаналіз нового стандарту блокового шифрування України "Калина" та окремих вузлів стандарту блокового шифрування республіки Білорусь СТБ 34.101.31-2011 «BeLT».

Виконано модифікацію кубічної атаки на шифр SIMECK з використанням інформації з побічного каналу. Отримано оцінки складності групових операцій для скручених еліптичних кривих Едвардса та доцільності розробки нового національного стандарту України, що базується на кривих Едвардса. Побудовано чотири моделі зловмисника в залежності від його обчислювальних можливостей з урахуванням квантових обчислень та доступу до оракулу, який обчислює досліджуване криптографічне перетворення. В постквантовій моделі обчислень розроблено критерій ефективного часткового розв'язку узагальненої задачі симетричної декомпозиції.

Розроблено формальні моделі системи зв'язку та зловмисника в клептографічному сенсі, способи виявлення потенційних клептографічних механізмів, методів усунення або зменшення прихованих каналів.

(рус.)

Построены модели для немарковских SP-сетей, которые используют несколько разных S-блоков на одном раунде шифрования, уточнен алгоритм вычисления верхних границ вероятностей дифференциалов. Разработаны критерии практического отбора ARX-криптопримитивов с определенными свойствами на основании автоматической оценки стойкости. Проведен криптоанализ нового стандарта блокового шифрования Украины «Калина» и отдельных узлов стандарта блокового шифрования республики Беларусь СТБ 34.101.31.2011 «BeLT».

Выполнена модификация кубической атаки на шифр SIMECK с использованием информации из побочного канала. Получена оценка сложности групповых операций для скрученных эллиптических кривых Эдвардса и целесообразности разработки нового национального стандарта Украины, который базируется на кривых Едвардса. Построены четыре модели злоумышленника в зависимости от его вычислительных возможностей с учетом квантовых вычислений и доступа к оракулу, который вычисляет исследуемое криптографическое преобразование. В постквантовой модели вычислений разработан критерий эффективного частичного решения обобщенной задачи симметричной декомпозиции.

Разработаны формальные модели системы связи и злоумышленника в клептографическом смысле, способы определения потенциальных клептографических механизмов, методов устранения или уменьшения скрытых каналов.

(англ.)

Models for non-Markov SP networks that use several different S-blocks in one encryption round are built, and algorithms for calculating upper bounds for differential probabilities are specified. The criteria for the practical selection of ARX cryptographic primitives with certain properties based on the automatic

evaluation of stability are developed. The cryptanalysis of the new blockchain encryption standard of Ukraine "Kalina" and separate units of the blockchain encryption standard of the Republic of Belarus STB 34.101.31-2011 "BeLT" has been carried out. A modification of the cubic attack on the SIMECK cipher using information from the side channel was made. The complexity of group operations for twisted Edwards curves and the expediency of developing a new national standard of Ukraine based on the Edwards curves were obtained. Four models of the attacker, depending on its computing capabilities, quantum computing and access to the oracle, which calculates the studied cryptographic transformation, are constructed. The criterion for the effective partial solution of the generalized symmetric decomposition problem in the post-quantum model of calculations is developed. Formal models of the communication system and the attacker in terms of kleptography, ways to identify potential kleptographic mechanisms and methods of eliminating or reducing hidden channels have been developed.

4. **Наявність охоронних документів** на об'єкти права інтелектуальної власності (*заявка на патент, патент, свідоцтво на авторське право*). немає
5. **Порівняння зі світовими аналогами.** Робота відповідає світовому рівню.
6. **Економічна привабливість для просування на ринок** (*вартість реалізації проекту, терміни впровадження та окупності, показники*). Результати роботи можуть просуватися на вітчизняному ринку.
7. **Потенційні користувачі** (*галузі, міністерства, відомства, підприємства, організації*). Результатами роботи можуть користуватися установи різної форми власності при проведенні наукових досліджень у галузі криптографічного захисту інформації, при оцінці надійності та стійкості систем криптозахисту інформації, що проектуються розробляються та експлуатуються, для створення конкурентоспроможних методик і засобів аналізу криптосистем, оцінки їх стійкості, способів покращення, модифікації.
8. **Стан готовності розробки** (*лабораторний або промисловий зразок, технічна документація, бізнес-план, готова до впровадження*). Технічний звіт про НДР.
9. **Існуючі результати впровадження**.

   Результати роботи впроваджено в начальний процес у нових розділах 2 курсів: «Методи криптоаналізу», «Спеціальні розділи криптології»; оновлено 2 лабораторні роботи для дисципліни «Розділи сучасної криптології»: «Лінійний криптоаналіз шифру Хейса»; для дисципліни «Методи криптоаналізу»: «Криптоаналіз з використанням швидких алгоритмів розв'язку систем лінійних рівнянь над скінченним полем зі спотворенними правими частинами»
10. **Назва підрозділу, телефон**, e-mail. Кафедра математичних методів захисту інформації ФТІ КПІ ім. Ігоря Сікорського, 044-204-81-76, mmzi.ipt.kpi.ua@gmail.com .
11. **Перелік публікацій за матеріалами** досліджень за період виконання (*вагомі монографії, підручники, посібники, наукові статті, дисертації, інші публікації*).

    Захищено: 1 кандидатську дисертацію.

    Опубліковано: 11 статей у фахових наукових журналах,

    Опубликовано 50 тез та доповідей за тематикою НДР у матеріалах конференцій,

    Захищено: 21 магістерську дисертацію,

    Захищено: 25 бакалаврських дипломних робіт.

12. Надати ключові слова до розробки

Криптоаналіз, блокове шифрування, кубічна атака, оцінка складності, криві Едвардса, постквантова модель обчислень