Алгебраїчно-ймовірнісні методи дослідження стійкості криптографічних алгоритмів і протоколів

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.