Тема: Формалізований метод автоматичного оцінювання Калина-подібних шифрів на стійкість до диференціального криптоаналізу

Автор: Байбуз М.А.

Науковий керівник: Яковлєв С.В.

Актуальність

Задача доказової стійкості схем шифрування до диференціального аналізу була сформульована К. Ніберг та Л.Р. Кнудсеном. В сучасній теорії розрізняють теоретичну та практичну стійкість до диференціального аналізу.

Відповідна задача наразі не розв’язана в загальному виді, існуючі моделі та методи застосовні лише в окремих випадках та часто повертають неадекватні з точки зору практики результати.

Описана проблематика вимагає глибоких та ретельних досліджень.

Мета

- розробка
- аналіз
- уточнення
- застосування

Основні питання

- Аналіз структури SP-мережі
- Дослідження методів побудови матриць верхніх меж імовірностей диференціалів
- Уточнення методів побудови матриць верхніх меж імовірностей диференціалів
- Програмна реалізація алгоритмів

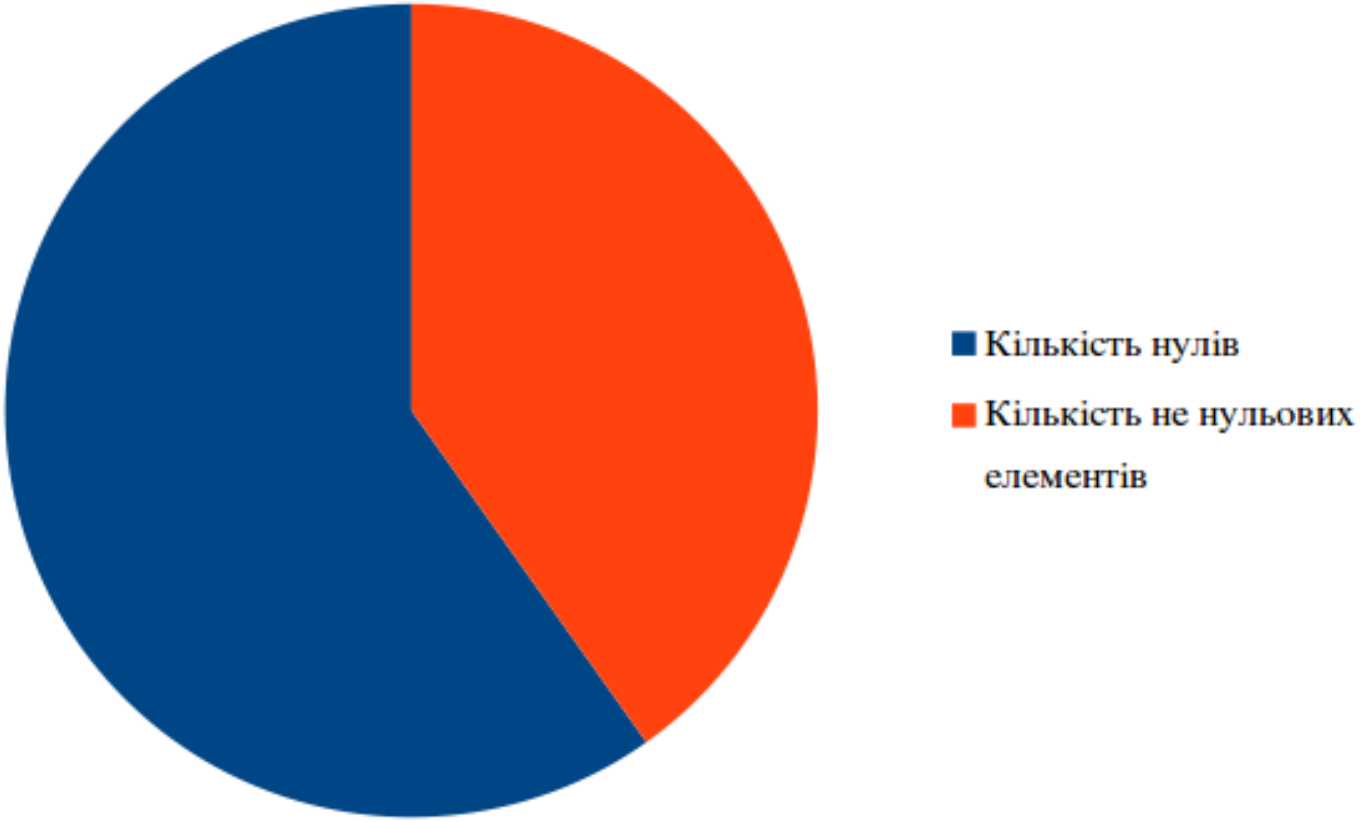
ФОРМАЛЬНИЙ ОПИС SP-МЕРЕЖ

- Сутність диференціального криптоаналізу
- Верхні межі ймовірностей існування нетривіальних диференціалів та диференціаьних характеристик SP-мереж
- Приклад SP-мережі шифр ДСТУ 7624:2014

ФОРМАЛІЗОВАНИЙ МЕТОД ОЦІНКИ СТІЙКОСТІ SP-МЕРЕЖ ДО ДИФЕРЕНАЦІАЛЬНОГО КРИПТОАНАЛІЗУ

- Алгоритми побудови оцінок стійкості SP-мереж
- Передобичслення матриці W
- Властивості матриці UB
- Особливості застосування алгоритмів до шифру ДСТУ 7624:2014
- Оцінка складності та труднощі реалізації

Передобчислення матриці W



Оцінювання стійкості модифікованого (спрощеного) шифру ДСТУ 7624:2014

Таблиця 3.2 – Значення верхніх меж в залежності від номеру раунду (формула 3.3)

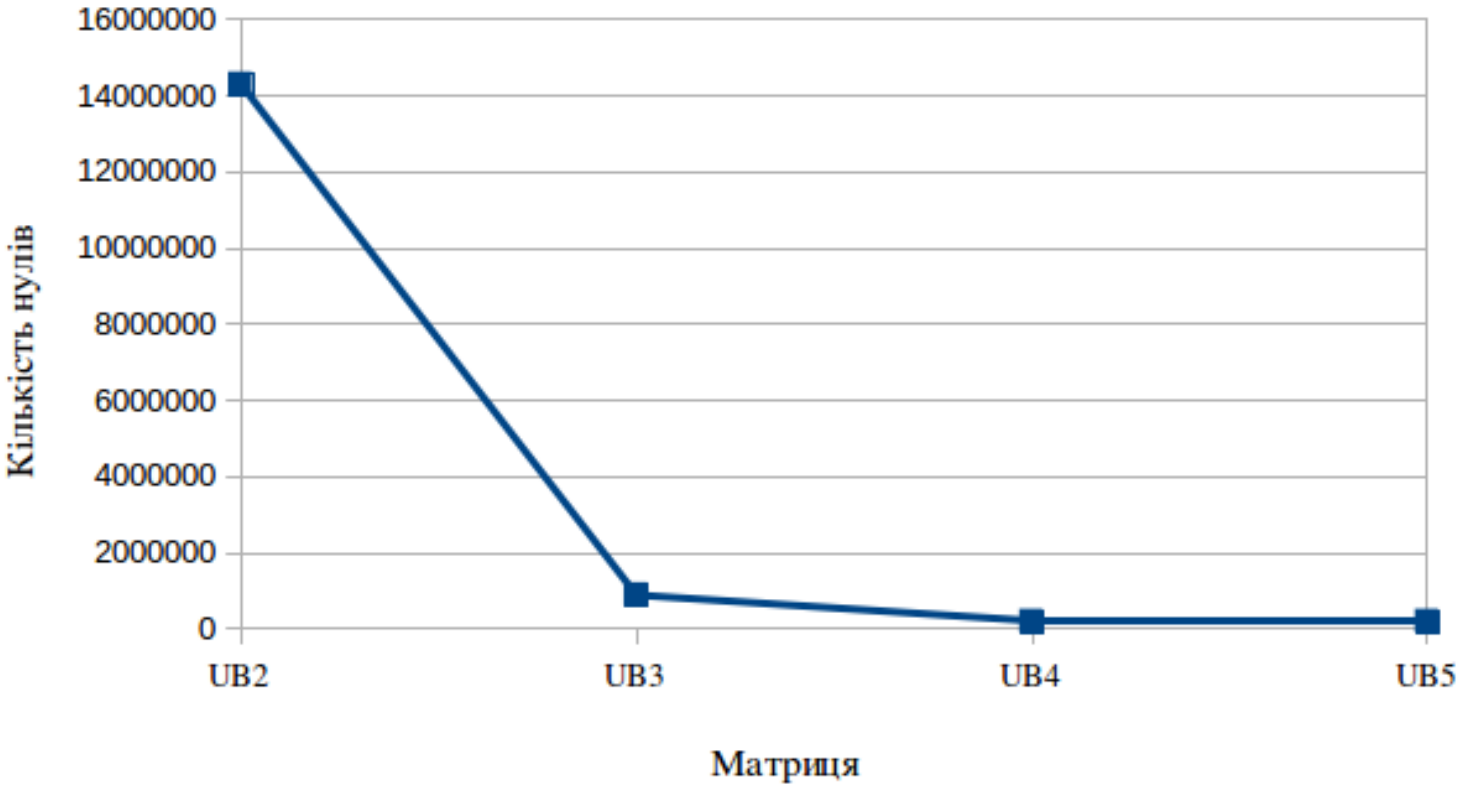
Номер раунду	Значення верхньої межі імовірності диференціалів
2	$2^{-23.6131}$
3	$2^{-33.1688}$
4	$2^{-33.1688}$
5	$2^{-33.1688}$
6	$2^{-33.1688}$
7	$2^{-33.1688}$
8	$2^{-33.1688}$
9	$2^{-33.1688}$

Оцінювання стійкості модифікованого (спрощеного) шифру ДСТУ 7624:2014

Таблиця 3.3 – Кількість нульових диференціалів в залежності від номеру раунду.

Номер раунду	Кількість диференціалів
2	56190
3	12800
4	900
5	0
6	0
7	0
8	0
9	0

Оцінювання стійкості шифру ДСТУ 7624:2014 з розміром блоку 128 біт



Висновки

- Проаналізовано структуру SP-мережі,як приклад було розглянуто алгоритм шифрування ДСТУ 7624:2014.
- Досліджено методи побудови матриць верхніх меж імовірностей диференціалів для SP-мереж.
- Уточнено методи побудови матриць верхніх меж імовірностейдиференціалів для маркіських SP-мереж.
- Програмно реалізовано алгоритми.
- Уточнені алгоритми дають грубу оцінку.

Дякую за увагу!