Додаток 1
Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

Авторська довідка

(кваліфікаційної роботи магістра)

Назва кваліфікаційної роботи бакалавра *Практичні аспекти дослідження стійкості S-блоків до диференціального криптоаналізу*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Practical Aspects of Research on Resistance of S-Blocks to Differential Cryptanalysis*
переклад англійською

Освітній ступінь : магістр

Шифр та назва спеціальності: 125 «Кібербезпека»
напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: Екзаменаційна комісія № 41
напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя
напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 27 грудня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 68

УДК: 004.056.55

Автор роботи
Прізвище, ім'я, по батькові (укр.): Ярема Олег Михайлович
розкривати ініціали

Прізвище, ім'я (англ.): Yarema Oleh
використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м. Тернопіль, Україна

Керівник
Прізвище, ім'я, по батькові (укр.): Загородна Наталія Володимирівна
повністю

Прізвище, ім'я (англ.): Zagorodna Nataliya
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна

Вчене звання, науковий ступінь, посада: к.т.н., доцент, завідувач кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Дуда Олексій Михайлович
повністю

Прізвище, ім'я (англ.): Duda Oleksiy
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра комп'ютерних наук, м.Тернопіль, Україна
Вчене звання, науковий ступінь, посада: к.т.н., доцент, доцент кафедри комп'ютерних наук

Ключові слова
українською s-блок, криптологія, блоковий шифр, таблиця підстановки, диференціальний криптоаналіз, диференціальна рівномірність

до 10 слів

англійською s-box, cryptology, block cipher, substitution table, differential cryptanalysis, differential uniformity

до 10 слів

Анотація

українською:

В кваліфікаційній роботі виконано дослідження практичних аспектів стійкості S-блоків до диференціального криптоаналізу. Для цього було реалізовано програмне забезпечення для генерації S-блоків та проведення їх диференціального аналізу на основі використання згенерованих S-блоків в експериментальному одноразундовому блоковому шифрі. Проведено аналіз результатів диференціального криптоаналізу згенерованих S-блоків з різними значеннями криптографічних властивостей.

англійською:

In this paper the practical aspects of S-boxes' resistance to differential cryptanalysis were studied. For this purpose, software was implemented to generate S-boxes and conduct their differential analysis based on the use of the generated S-boxes in an experimental single-round block cipher. The results of the differential cryptanalysis of the generated S-boxes with different values of cryptographic properties are analysed.

Бібліографічний опис:

Ярема О. М. Практичні аспекти дослідження стійкості S-блоків до диференціального криптоаналізу: кваліфікаційна робота магістра за спеціальністю 125 — Кібербезпека / Ярема Олег Михайлович. – Тернопіль : ТНТУ, 2023. – 68 с.