**Кирилащук Т.Г.**

**Павловська А.В.**

# ЛЕГКА КРИПТОГРАФІЯ ДЛЯ IoT:ГАРАНТУВАННЯ БЕЗПЕКИ В УМОВАХ ОБМЕЖЕНИХ РЕСУРСІВ

Вінницький національний технічний університет

***Анотація***

*IoT інтегрує фізичний світ у кіберпростір, вимагаючи конфіденційності, цілісності та автентифікації. Обмежені ресурси IoT-пристроїв вимагають легкої криптографії. Ця галузь спрямована на створення ефективних криптографічних алгоритмів(хеш-функцій, потокових та блокових шифрів), переважно у вигляді програмної реалізації. У тезі аналізуються легкі блокові шифри для IoT, їхні переваги та недоліки,результати крипто аналізу. Окрім цього,визначено напрями для подальшого розвитку.*

**Ключові слова**: Інтернет речей (IoT),легка криптографія ,блокові шифри, безпека даних, конфіденційність, автентифікація , SPN (Substitution Permutation Network) ,Feistel.

***Abstract***

*The IoT integrates the physical world into cyberspace, requiring confidentiality, integrity, and authentication. The limited resources of IoT devices require lightweight cryptography. This field aims to create efficient cryptographic algorithms (hash functions, stream and block ciphers), mainly in the form of software implementations. The thesis analyses lightweight block ciphers for IoT, their advantages and disadvantages, and the results of cryptanalysis. In addition, directions for further development are identified*.

**Keywords:** Internet of Things (IoT), lightweight cryptography, block ciphers, data security, privacy, authentication, SPN (Substitution Permutation Network), Feistel.

## Вступ

Інтернет речей (IoT) об'єднує фізичні предмети та живих організмів, формуючи "розумні" системи. Витоки цієї ідеї пов'язані з RFID та WSN, що дають змогу сенсорам надсилати дані через бездротові канали зв'язку. З розширенням 5G, IoT стає більш вразливим до різноманітних кібернетичних загроз, що наголошує на необхідності забезпечення безпеки даних та збереження приватності.

Криптографія відіграє центральну роль. Враховуючи обмежені ресурси IoT-пристроїв, активно розвивається поле легкої криптографії, що надає компактні та продуктивні алгоритми, зокрема блокові шифри. У нашому дослідженні проводиться аналіз цих шифрів, їхніх сильних та слабких аспектів, а також стійкості до атак, з особливим акцентом на програмних реалізаціях, що вирізняються економічністю та гнучкістю. Ця робота сприяє створенню надійних криптографічних рішень для забезпечення безпеки в IoT.

**Результати дослідження**

«В неоднорідному середовищі IoT, ключовим аспектом є шифрування даних задля гарантування конфіденційності, цілісності та автентифікації інформації. Через обмежені обчислювальні можливості, обсяг пам'яті та розмаїття операційних середовищ численних IoT-пристроїв, традиційні стандарти безпеки, як-от AES та DES, виявляються недоцільними через великі вимоги до ресурсів. Це стало поштовхом до появи легкої криптографії.»[1]

«Легкі шифри, на кшталт PRESENT, RECTANGLE, SIMON, SPECK та інші, розроблені для програмних та апаратних реалізацій, причому програмні реалізації пропонують меншу вартість та більшу гнучкість.

Характеристиками якісного легкого шифру є : незначна складність, надійна архітектура, висока пропускна здатність, багатий стандарт шифрування, потребує менше пам’яті, програмна реалізація, потрібна менша апаратна реалізація, споживає менше апаратної реалізації, хороший імунітет проти лінійних та диференціальних атак, запобігання можливим атакам на випередження, таким як атака Бікліка, атака з нульовою кореляцією, атака «Зустріч у середині», алгебраїчна атака.»[2]

«Було розглянуто два існуючі методи такі як:

1) Шифр: **PRESENT.**

PRESENT – блоковий шифр типу SPN (Мережа підстановок та перестановок), що оперує з 64-бітовими блоками, використовує ключі розміром 80/128 біт та має 31 раунд обробки. Завдяки використанню одного й того ж 4-бітового S-блоку (16 разів паралельно в шарі нелінійної заміни) та бітової перестановки для забезпечення лінійного розсіювання, він демонструє придатність до апаратної реалізації. Незважаючи на помірні властивості розсіювання, які роблять його вразливим до лінійного та насиченого криптоаналізу, PRESENT набув широкої популярності та цитованості серед легких шифрів. Його простота та продуктивність в апаратному виконанні зробили його еталоном для наступних досліджень.

2) **SIMON та SPECK.**

Опис: SIMON та SPECK – це сімейства легких блокових шифрів, розроблені Агентством Національної Безпеки США. Вони базуються на ARX-операціях (Додавання-Зсув-XOR), що забезпечує високу ефективність як у програмній, так і в апаратній реалізації. Кожне сімейство містить десять варіацій шифрів, що забезпечує можливість вибору безпеки в залежності від потреб. SIMON та SPECK використовують циклічні зсуви бітів та фіксовані параметри ротації. Ці шифри здобули популярність завдяки своїй компактності та швидкодії, хоча SIMON продемонстрував вразливість до атак відновлення ключа з використанням лінійних наближень на скорочених версіях. Розробка цих шифрів підкреслила важливість гнучких сімейств, що адаптуються до різних умов обмежених ресурсів.»[3]

Ці дві команди дослідників та їхні шифри важливі тим, що вони запропонували архітектури, які стали базою для подальших розробок у легкій криптографії, а також актуалізували проблему балансу між безпекою та продуктивністю в контексті IoT з його обмеженнями.

**Висновок**

Дослідження виділяє ключову важливість легкої криптографії для IoT, де обмеження ресурсів диктують необхідність оптимізованих рішень для безпеки. Аналіз блокових шифрів, зокрема PRESENT, SIMON, SPECK, розкриває баланс між захистом і продуктивністю. Ці шифри, особливо в програмних втіленнях, закладають фундамент для гарантування захисту даних. Майбутні зусилля мають зосереджуватися на розробці ще надійніших та стійкіших алгоритмів, що відповідають потребам IoT-середовища, яке динамічно еволюціонує.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1) Головач, Р., Мосійчук, І., Балянда, Т., & Гаранюк, С. (2021). ПРОБЛЕМИ ТА ЗАГРОЗИ БЕЗПЕЦІ IoT ПРИСТРОЇВ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 31–42.*
2) Заяць, В. С. (2025). *Алгоритми шифрування даних на основі кодів*. Західноукраїнський національний університет.
3) Елембовський, М. М., & Корнійчук, Б. В. (2023). АНАЛІЗ СУЧАСНИХ НАУКОВИХ ПУБЛІКАЦІЙ ЗА НАПРЯМКОМ ТЕМАТИКИ КІБЕРБЕЗПЕКИ ІОТ ТЕХНОЛОГІЙ. *Міжнародний науковий журнал «Грааль науки», 25*, 203.
4) РОЗРОБКА СИМЕТРИЧНОГО КРИПТОГРАФІЧНОГО ДИФЕРЕНЦІЙНОГО РОЗРІЗНЮВАЧА НА ОСНОВІ ГЛИБОКОГО НАВЧАННЯ (2024). *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*.



***Анастасія Вячеславівна Павловська***– студентка групи 1БС-24Б, факультет інформаційних технологій та комп’ютерної інженерії. Вінницький національний технічний університет, Вінниця, email: nastyapav2006@gmail.com

Науковий керівник: ***Кирилащук Тетяна Геннадіївна*** - аспірант групи 125-23а, асистент кафедри захисту інформації факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: kgt0998@gmail.com

***Pavlovska Anastasiia V.***—student of group 1BS-24B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mai: lnastyapav2006@gmail.com

Supervisor: ***Kyrylashchuk Tatyana Gennadiyevna*** — graduate student of group 125-23a, assistant of the department of information protection of the faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com