ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем

Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА

Другий (Магістерський)
Освітній рівень

Галузь знань 17 Електроніка та телекомунікації
Шифр і назва спеціальності

Спеціальність 172 Телекомунікації та радіотехніка
Шифр і назва спеціальності

на тему Метод криптографічного захисту вузлів мережі ZigBee

ДРМТР 2020017.00.00

Виконав: студент 2 курсу, група ТРм-19-2 _____ Я.В. Супрунюк
підпис Ініціали, прізвище

Керівник: к-т техн. наук, доц. _____ К.Л. Горященко
підпис Ініціали, прізвище

До захисту допускаю:

Зав. кафедри: д-р техн. наук, проф. _____ С.К. Підченко
підпис Ініціали, прізвище

03 грудня 2020 р.

Хмельницький, 2020

Хмельницький національний університет

Факультет *програмування та комп'ютерних і телекомунікаційних систем*
Кафедра *телекомунікацій, медійних та інтелектуальних технологій*
Освітній рівень *другий (магістерський)*
Галузь знань 17 – *Електроніка та телекомунікації*
Спеціальність 172 – *Телекомунікації та радіотехніка*
Освітня-професійна програма *Телекомунікації та радіотехніка*

ЗАТВЕРДЖУЮ
З.в. кафедрою ТМІТ
С.К. Підченко
« 03 » вересня
2020 р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Супрунюк Ярослав Вікторович

1 Тема роботи: *Методи криптографічного захисту вузлів мережі ZigBee*
керівник роботи Горященко К.Л, к.т.н, доцент.
Затверджено наказом по університету від «1» вересня 2020р. № 118 .
2 Строк подання студентом роботи на кафедру:02.12.2020р.
3 Вихідні дані (характеристика об'єкта, умов дослідження та ін.)
Мета роботи – вирішення задачі підвищення криптографічної безпеки передачі інформації між мережі вузлами ZigBee із застосуванням алгоритму еліптичних кривих
Об'єкт дослідження – бездротова мережа ZigBee на основі мікропроцесорних систем з обмеженою обчислювальною потужністю
Предмет дослідження – методи криптографічного захисту передачі інформації бездротовими каналами зв'язку.
4. Зміст пояснювальної записки (перелік питань, що їх належить розробити)
Розділ 1 Аналіз проблематики дослідження
Розділ 2 Використання криптографії в телекомунікаційних системах
Розділ 3 Використання криптографічних засобів захисту в системах телекомунікацій
Розділ 4 Моделювання алгоритму еліптичних кривих та загальної швидкодії системи

Завдання отримав
Науковий керівник

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	Аналіз літературних		
	джерел	5.09. 20-14.09. 20	*виконано*
2	Написання 1 розділу	5.09. 20-14.09. 20	*виконано*
3	Визначення проблеми		
	дослідження	5.09. 20-14.09. 20	*виконано*
4	Написання 2 розділу	5.09. 20-14.09. 20	*виконано*
5	Розробка моделі	5.09. 20-14.09. 20	*виконано*
6	Написання 3 розділу	5.09. 20-14.09. 20	*виконано*
7	Теоретичне та практичне		
	моделювання	1.11.20-14.11.20	*виконано*
8	Написання 4 розділу	1.11.20-14.11.20	*виконано*
9	Оформлення роботи	20.11.20-30.11.20	*виконано*
10	Оформлення презентації	03.12.20	*виконано*

Студент _____ Підпис _____ Ініціали, прізвище

Керівник роботи _____ Підпис _____ Ініціали, прізвище

ЗМІСТ

Перелік умовних скорочень

AES	Advanced Encryption Standard, Симетричний алгоритм блочного шифрування
DES	Data Encryption Standard, Симетричний алгоритм блочного шифрування
IoT	Internet of Things, мережа Інтернету речей
БСМ	бездротові сенсорні мережі

ВСТУП

Актуальність теми

З невпинним розвитком телекомунікаційних систем, кількість інформації, що передається, зростає в експоненціальній прогресії. Наука, політика, культура, побут, та й будь яка інша сфера – у всьому відбувається обмін великою кількістю інформації, яка є важливим чинником існування тієї чи іншої сфери.

Під час розробки будь-якої системи завжди постає два питання: яким чином передати та яким чином отримати цю інформацію без втрат чи можливих модифікацій(зовнішнього впливу на цю інформацію). Та особливе місце в передачі та отриманні інформації. постає питання про захищеність цієї інформації, яка буде передана тим чи іншим каналом зв’язку.

В повсякденному житті в кожної людини, є пристрої, які самі приймають та передають інформацію. В загальному випадку вони складають свою власну мережу, яка має назву IoT. Прикладом такої мережі є система Smart Home (системи розумного дому) – це набір датчиків, які дозволяють керувати вашим будинком, відстежувати що відбувається всередині, захистити в разі проникнення та багато іншого. Вони збирають інформацію про навколишній стан у вашому будинку, та передають її вам на ваш телефон. Ще одним прикладом можуть бути датчики, які призначені для певних виробничих, агрономічних цілей. Найпопулярнішим стандартом передачі інформації між датчиками є протокол ZigBee.

Зв’язок роботи з науковими програмами, планами, темами.

Магістерська робота виконана відповідно до поточних та перспективних планів наукової роботи Хмельницького національного університету, кафедри телекомунікацій, медійних та інтелектуальних технологій за тематикою покращення методів формування, генерування, прийому та обробки сигналів.

Мета роботи і завдання дослідження

Мета роботи – вирішення задачі підвищення криптографічної безпеки передачі інформації між мережі вузлами ZigBee із застосуванням алгоритму еліптичних кривих.

Для досягнення поставленої мети в роботі необхідно вирішити наступні завдання:

1. Розглянути питання щодо запроваджених криптографічних методів у бездротових телекомунікаційних системах.

2. Визначити перспективні алгоритми криптографічного захисту інформації, що передаються між вузлами такої мережі.

3. Розглянути алгоритми, що використовуються для систем із малою обчислювальною потужністю в ракурсі застосування для обчислювальних систем малої обчислювальної потужності.

4. Виконати моделювання параметрів модулів передачі із застосуванням криптографічного захисту інформації для модулів мережі ZigBee.

Об'єкт дослідження – бездротова мережа ZigBee на основі мікропроцесорних систем з обмеженою обчислювальною потужністю.

Предмет дослідження – методи криптографічного захисту передачі інформації бездротовими каналами зв'язку.

Методи дослідження - теоретичний аналіз мережі ZigBee та криптографічного захисту інформації, практичне зображення за допомогою інструментів візуального моделювання.

Науково-практична новизна роботи. На основі проведених досліджень, представлено оцінку апаратної складності криптографічного перетворення на основі методу еліптичних кривих із застосуванням 8-бітних та 32-бітних контролерів. Розрахована кількість часових витрат на роботу, а також оцінено можлива швидкість генерування пакетів даних для передачі в мережі ZigBee.

Апробація результатів магістерської роботи. Результати досліджень даної магістерської роботи пройшли апробацію на науковій конференції факультету програмування, комп’ютерних та телекомунікаційних систем Хмельницького національного університету.

Публікації. На основі матеріалів магістерської роботи опублікована стаття у збірнику наукових праць студентів ХНУ.

Структура та об'єм магістерської роботи.

Робота складається з 4-х розділів, загальним обсягом 92 сторінок. В роботі використано 50 посилань на літературні джерела.

В роботі 29 рисунків та 7 таблиць.

Ключові слова: еліптична крива, легковісна криптографія.

РОЗДІЛ 1 АНАЛІЗ ПРОБЛЕМАТИКИ ДОСЛІДЖЕННЯ

1.1 Тенденції розвитку безпеки систем телекомунікацій при використанні різних каналів зв'язку

Сьогодні у світі у сфері передачі інформації визначилася стабільна тенденція на посилення ролі технічних засобів захисту даних. Тенденція зовсім не випадкова: неодноразові дослідження в області безпеки даних показали, що використання технічних засобів із елементами криптографії дозволяє звести до мінімуму або виключити негативний вплив самої ненадійної ланки в системі – людини, якій властиві стомлюваність, неуважність, халатність і т. п. При цьому, організація розподіленої мережі контролю і передачі за допомогою технічних засобів обходиться споживачеві значно дешевше, а надійність її вища.

По факту, в середині 90-х років, такими вузлами мережі контролю і передачі ставали системи безпеки для охоронних систем.

У завданнях 2020-х років – розподілені системи контролю за станом здоров'я людей в приміщеннях, на вулиці, в транспорті і так далі. Глобальна пандемія вірусу COVID-19 веде до усвідомленої необхідності створення медичних мереж контролю.

Історично, при створенні систем розподіленого контролю основна увага приділялася таким аспектам, як:

- автоматизація, яка дозволяє до мінімуму спростити процеси введення об'єктів під охорону, скоротити обслуговуючий персонал; суттєво скоротити кількість неправдивих тривог через втручання в роботу системи;

- контроль каналу зв'язку, що забезпечує високу достовірність передачі і виключає втрату тривожної інформації;

- розробка широкої гамми об'єктових пристроїв з різними функціональними і сервісними можливостями, що дозволяють задовольнити потреби найширших верств населення.

З точки зору організації захисту об'єктів від несанкціонованого проникнення, як по устаткуванню технічними засобами охорони, так і по тактиці дій чергових служб, існуючі системи не мають яких-небудь істотних відмінностей.

Проте головним недоліком вказаних систем є різнорідність технічних і конструктивних рішень, а також закрита архітектура побудови, що не дозволяє провести їх об'єднання в єдиний універсальний комплекс технічних засобів одного комплексу. Це, в кінцевому, підсумку призводить до виникнення певних проблем для усіх структур збору даних у впровадженні, експлуатації, обслуговуванні і ремонті різнорідних технічних засобів, в проведенні єдиної технічної політики, забезпеченні належного рівня якості і надійності телекомунікаційного устаткування, а, отже, до додаткових фінансових витрат і збільшення тарифів на послуги.

Саме тому, найбільш актуальною все ще є на сьогодні проблема впорядкування парку систем збору даних, їх оновлення, заміни застарілого телекомунікаційного устаткування сучасним, надійнішим.

Тому в цілях подальшого розвитку і вдосконалення систем збору та передачі інформації до нових розробок останнім часом пред'являються додаткові вимоги:

- імітостійкість і криптозахист, системи, що забезпечують стійкість, до несанкціонованого «обходу» і обумовлені появою «кваліфікованих» втручань;

- висока інформативність системи, що забезпечує формування сигналів про втручання в спільний потік даних мережі;

- можливість інтеграції системи з оптоволоконними каналами зв'язку, обумовлена введенням в експлуатацію підприємствами зв'язку нових цифрових технологій передачі інформації;

- уніфікація створюваних технічних засобів, тобто можливість об'єднання різних пристроїв в єдиний програмно-апаратний комплекс збору та передачі інформації.

Пріоритетним завданням технічної політики в області розвитку таких систем є розробка відсутніх на сьогодні єдиних вимог, що в умовах різноманіття існуючих і нових, дозволить уніфікувати стики систем передачі сповіщень.

1.2 Передача інформації в мережах дротовим зв'язком

Основним шляхом передачі інформації між пристроями, з початком існування техніки став дріт. В загальному випадку для цього використовують відповідний дріт та порт стандарту RJ-45.

Взаємодія дротових мереж з кінцевими пристроями описується загальними стандартами IEEE 802.3. Загалом, на сьогоднішній день використовується два стандарти, а саме:

- IEEE 802.3u;
- IEEE 802.3ab.

Для передачі даних між пристроями використовують два типи кабелю:

1) Дво- або чотирьох парний кабель крученої пари.

2) Багатомодовий (два волокна) оптоволоконний кабель.

Максимальна пропускна здатність в стандарті IEEE 802.3u становить 100 Mb/s, а в стандарті IEEE 802.3ab – 1 Gb/s. В залежності від об'єму даних, що будуть передаватися обирається той чи інший стандарт.

В більшості випадків, побудова мереж типу LAN використовує технологію Ethernet. Якщо взяти до уваги, яким чином будувалися мережі LAN, то основними технологіями були такі протоколи як Frame Realy, Token Ring. Їх використання в сучасному світі стає все меншим і меншим. Проте зустріти дані протоколи можна у спеціалізованих лабораторія, навчальних закладах, або державних службах. Для побудови LAN необхідні такі пристрої як маршрутизатори, комутатори, бездротові маршрутизатори, модеми,

мережеві адаптери, бездротові точки доступу. Рідше використовуються такі пристрої як перетворювачі мережі, підсилювачі сигналів, а також спеціальні антени.

Для передачі інформації на певній території, використовуються LAN. Для утворення LAN щонайменше необхідно два кінцевих пристрої, які між собою будуть зв’язані дротом, на певній відстані один від одного. В залежності від виконуваних завдань, кількість пристроїв може варіюватися.

В прикладі інформації, що передається між пристроями візьмемо IP-пакет. Структура його заголовку має наступний вигляд: перші 4 біта містять в собі інформацію про версію пакета – IPv4 або IPv6, 4 біта вміщують в собі довжину інтернет заголовка, яка вимірюється довжиною в 4 байти, 8 біт описують тип обслуговування, або по іншому QoS, який в загальному випадку описує пріоритет цього пакету, 16 біт показує довжину цього пакету в байтах, 16 біт показують тег ідентифікації, який дозволить відновити весь пакет з декількох фрагментів, 3 біта мають нуль, прапорець дозволу на фрагментування цього пакету, а також прапорець дозволу на подальше його фрагментування, 13 біт вміщують зміщення того чи іншого фрагменту при передачі цього пакету, поле для ідентифікації місцерозташування фрагменту у вихідному коді пакету, 8 біт описують час життя, які визначають яку кількість раз буде дозволено для пакету, перед тим як він зникне, 8 біт описують яким саме протоколом передається даний пакет, 16 біт вміщують контрольну суму, яка необхідна для виявлення помилок в переданому пакеті, 32 біта описують від кого пакет надійшов, та 32 біта для кого даний пакет, має бути переданий.

В загальному випадку об’єм заголовку IP-пакету складатиме 20 байт. Далі до цього пакету також будуть додані дані, які мають бути передані, від одного пристрою, до іншого. Максимальний розмір IP-пакета складає 65535 байт. На рисунку 1.1 графічно зображено структура заголовку IP-пакету.

<table>
<tr><td colspan="2">4 біти
Номер версії</td><td colspan="2">4 біти
Довжина заголовку</td><td colspan="4">8 біт
Тип сервісу
PR | D | T | R</td><td colspan="4">16 біт
Загальна довжина</td></tr>
<tr><td colspan="6">16 біт
Ідентифікатор пакету</td><td colspan="2">3 біта
ФЛАГИ
D | M</td><td colspan="4">13 біт
Зсув фрагменту</td></tr>
<tr><td colspan="3">8 біт
Час життя пакету</td><td colspan="3">8 біт
Протокол верхнього рівня</td><td colspan="6">16 біт
Контрольна сума</td></tr>
<tr><td colspan="12">32 біти
IP-адрес джерела</td></tr>
<tr><td colspan="12">32 біти
IP-адрес призначення</td></tr>
<tr><td colspan="12">Параметри та виравнювання</td></tr>
</table>

Рисунок 1.1 – Структура заголовку IP-пакету

Безсумнівним плюсом використання дротової технології передачі даних є висока швидкість передачі інформації та стабільність роботи, беручи до уваги, що поширена конфігурація мережі з швидкістю передавання інформації 1 Гбіт/с. Така швидкість є доступною для кожного з користувачів такої мережі, до того ж, швидкість не ділиться на кожного з них, а також працює на дві сторони, що дає можливість отримувати максимальну пропускну здатність мережі 2000 Мбіт/с. Окрім високої швидкості роботи, можна заначити ще плюс підтримки передачі великих пакетів даних, так званий Jumbo Frame (це пакети об’ємом 9 кбіт та 16 кбіт), що дозволяє збільшити швидкість передачі даних з великим об’ємом, за рахунок зменшення передачі службової інформації, а також знизити навантаження на центральний процесор, що в свою чергу, надасть швидкодію самої системи. Плюсом дротового з’єднанння також є те, що в кожну материнську плату пристрою (комп’ютера), навіть бюджетного варіанту, уже влаштований високошвидкісний порт Ethernet. А найголовнішим плюсом є безпека, адже

для того, щоб отримати доступ до необхідних даних, потрібне безпосереднє підключення по дроту.

1.3 Передача інформації з використанням бездротових технологій

Разом із зростанням обсягу технологій та розвитком мобільних пристроїв, стало зрозуміло, що дріт використовувати можна на невеликих відстанях, і для пристроїв, що в більшості випадків використовуються стаціонарно, без переміщення по великих площах. Актуальність питання щодо впровадження бездротового з'єднання, для передачі інформації між пристроями на відкритій місцевості також стало нагальним в кінці 20 століття.

Таким чином, почався розвиток бездротового підключення. В залежності від, на якій буде передаватись інформація, можна поділити на три класи: WPA, WLAN, WMAN [12].

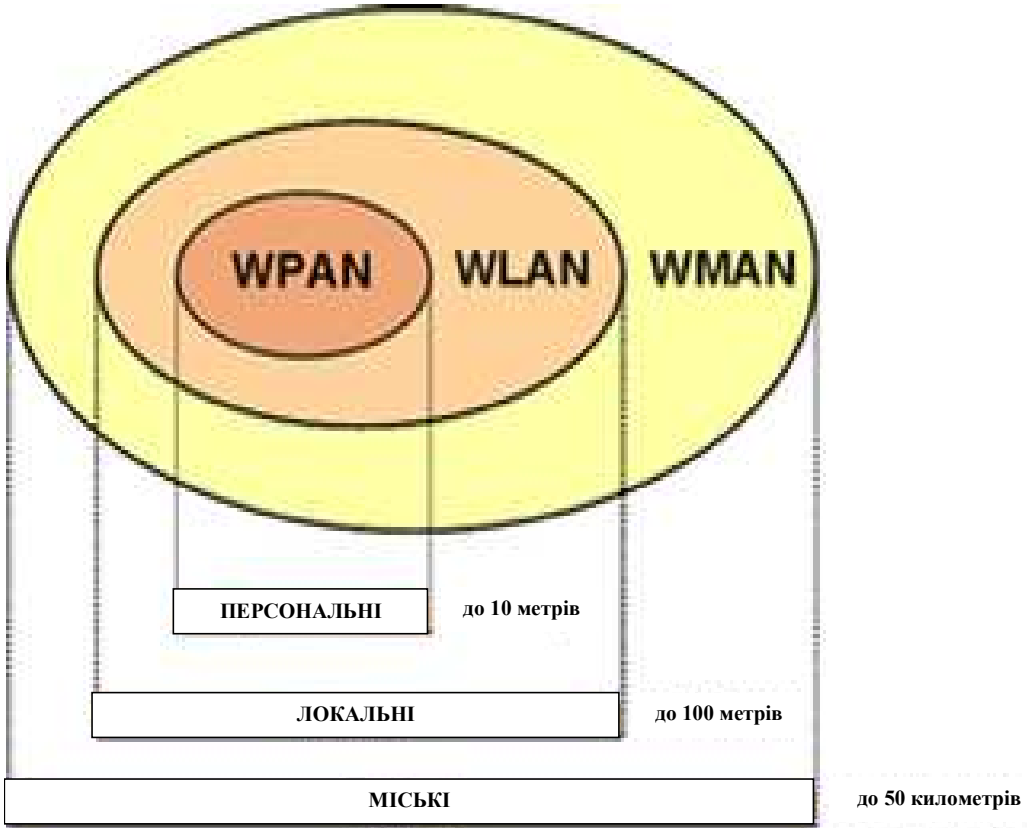

Рисунок 1.2 – Класифікація бездротових технології в залежності від дальності дії [12]

За дальністю дії, бездротові мережі, можна поділити наступним чином:

1) WPAN – бездротова мережа, що охоплює невелику частину території, невелику швидкість передачі інформації, а також передача інформації відбувається лише між декількома пристроями. Прикладом такої технології є Bluetooth, ZigBee [12].

2) WLAN – бездротова мережа, що охоплює середню за розміром ділянку (відстанню до 100 метрів), в залежності від використання стандарту передачі та частоти розміщення, швидкість передачі може сягати до 3,4 Гбіт/с. Прикладом такої технології є Wi-Fi [12].

3) WMAN – бездротова мережа, що охоплює велику територію (область покриття до 50 кілометрів). В залежності від використання стандарту, швидкість передачі може варіюватись, максимальним значенням є 1 Гбіт/с. Прикладом такої технології є WiMax [12].

Залежно від типу пристрою, який використовується кінцевим користувачем, визначається той чи інший клас бездротової передачі інформації.

1.3.1 Бездротові системи передачі інформації та їх історичний розвиток

На сьогодні усі бездротові системи можна розділити на чотири групи:

- системи на основі GSM-рішень;
- радіоканальні вузли малого радіусу взаємодії;
- радіоканальні вузли великого радіусу взаємодії;
- супутникові телекомунікаційні системи.

Як найпростіші телекомунікаційні системи – GSM-системи почали використовуватись в кінці XX – на початку XXI століття після появи мобільного зв'язку та появи зручних рішень – Рисунок 1.3.

Рисунок 1.3 – GSM модуль M590e Neoway 900/1800 Мгц

Спочатку як каналоутворююче телекомунікаційне устаткування використовувались мобільні телефони, які підключалися до систем керування через послідовний канал RS-232 і керувались стандартні AT-команди. Це рішення не було дуже надійним, оскільки телефони могли перестати опрацьовувати команди, крім того, умови експлуатації мобільних телефонів не дозволяли роботу в вологих і неопалюваних приміщеннях, що суттєво обмежувало сферу їх застосування.

Сьогодні, виробники телекомунікаційного устаткування мобільного зв'язку випускають спеціалізовані GSM-модеми підвищеної надійності для побудови на їх основі безпровідних систем. Це рішення суттєво підвищило якість роботи системи, а також надало розробникам систем бездротових рішень додаткові можливості по роботі з сервісами GSM.

Так в якості інструменту передачі даних в GSM-системах почали застосовуватись SMS-повідомлення. А також використовується модемні з'єднання (CSD). Для передачі простих інформаційних повідомлень застосовують передачу тонових посилок – режим DTMF. А для передачі данх – режим пакетної передачі повідомлень GPRS [12].

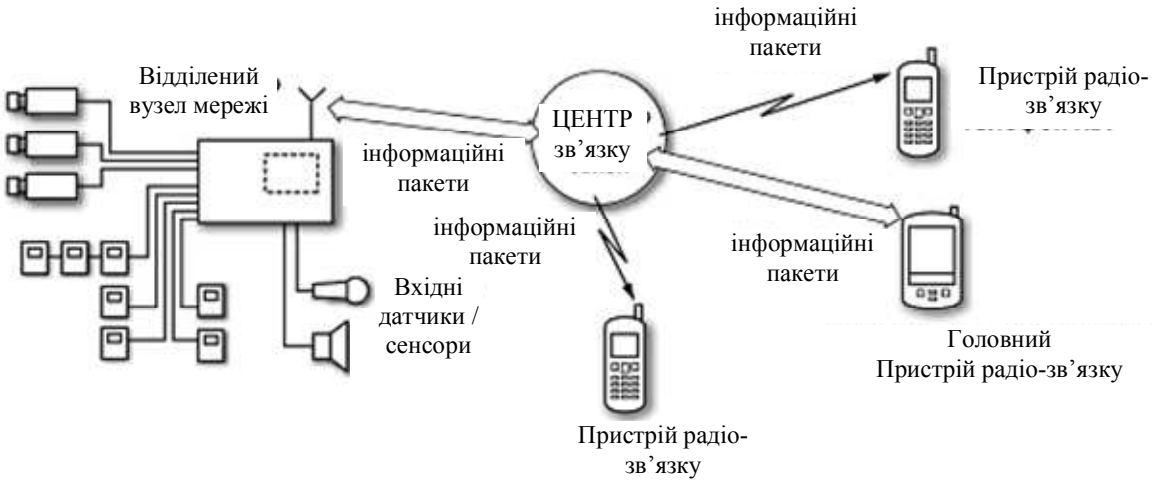

Рисунок 1.4 – Схема передачі інформації в GSM системі при використанні функції SMS-інформування [12]

Саме поява режиму GPRS дозволила суттєво понизити витрати на експлуатацію систем різноманітних бездротових рішень. На сьогодні бездротові телекомунікаційні системи на базі GSM-систем отримали поширення завдяки їх відносно невисокій вартості і простоті установки і експлуатації.

Проте найбільшим недоліком подібних систем є низька завадозахищеність [12]. Відомо, що GSM-канал легко задавити технічними засобами, а самі пристрої придушення GSM каналу знаходяться сьогодні у вільному продажу. Робота мережі GSM також не завжди характеризується високою стабільністю і може відмовити в самий непідходящий момент.

Вказані недоліки обмежують застосування телекомунікаційного устаткування подібного класу при побудові систем зв'язку. Ці системи здебільшого застосовуються як резервні та додаткові канали зв'язку або для побудови систем моніторингу видалених об'єктів для збору телеметричної інформації.

GSM система може включати один або декілька GSM контролерів [12], а також засоби контролю і управління цими GSM контролерами – стільниковими телефонами та/або комп'ютерами.

1.3.2 Технологія ZigBee

Однією з безпровідних технологій, що самих, що швидко розвиваються, є ZigBee, який спочатку розроблялася як низькошвидкісний канал зв'язку для об'єднання в мережу різних датчиків [20, 45]. Стосовно застосуваннння ZigBee – це можуть бути датчики охоронної і пожежної сигналізації, датчики збору телеметричної інформації, датчики медичних служб та інші.

Через темпи розповсюдження та зручності до впровадження, ZigBee має всі шанси потіснити багато з існуючих сьогодні радіоканальних бездротових систем. Адже майже усі вони розроблені поза якими-небудь стандартами. У кожного виробника - свої протоколи обміну, і замінити наявні на об'єкті бездротові датчики на телекомунікаційного устаткування іншого виробника неможливо. Якщо стандарт ZigBee отримає подальше поширення, що цілком імовірно, то замовник отримає можливість використати в бездротових системах практично будь-які датчики на власний вибір.

Тим більше що стандартні специфікації наборів команд і протоколів обміну для конкретних застосувань в області автоматизації будівель і систем безпеки розроблені, опубліковані, і усе це разом узяте гарантує сумісність телекомунікаційного устаткування різних виробників.

Цей стандарт є зручним для з'єднання центрального телекомунікаційного вузла з периферією, яка розміщується на великій території. при чому ще й розподілена. Також, за рахунок включення в систему модулів-ретрансляторів, територія покриття може бути суттєво великою.

Теоретично можна використати ZigBee і в системах контролю та обмеження доступу. Але цей канал має невелику швидкість передачі даних і невелику швидкодію. Нераціонально будувати довгий ланцюжок ретрансляторів заради з'єднання контролера з комп'ютером. Є багато простіших, а головне, дешевих і надійних способів.

Можна сказати, що усі перераховані технології на сьогодні активно розвиваються і широко застосовуються для вирішення завдань охорони стаціонарних об'єктів. Вибір тієї або іншої безпровідної системи визначається залежно від типу об'єктів, їх кількості, вимог до надійності доставки повідомлень і віддаленості об'єктів. В деяких випадках для підвищення надійності використовується резервування каналів зв'язку. Можна сказати, що майбутнє за безпровідними технологіями і скоро вони повністю витіснять з ринку дротяні системи зв’язку.

1.3.3 Бездротові мережі WLAN

Альтернативою GSM-каналу є такі бездротові мережі як WLAN (Wireless Local Area Network – безпровідна локальна мережа). Мережа WLAN – тип локальної обчислювальної мережі (Local Area Network, LAN), що використовує для зв'язку і передачі даних між вузлами за допомогою високочастотних радіохвиль діапазону 2.4 ГГц, а не звичайні кабельні з'єднання.

Стандарт Wi-Fi (англ. Wireless Fidelity - "безпровідна точність" – стандарт на телекомунікаційне устаткування для бездротових мереж).

При застосуванні сучасних алгоритмів стиснення даних, при швидкості 0,5 Мбіт/с цієї швидкості достатньо для передачі одного каналу потокових відео прийнятної якості. Відстань передачі інформації можна збільшувати за допомогою ряду спрямованих антен та проміжних радіоточок доступу.

Призначені для користувача пристрої можна інтегрувати в цю мережу, встановивши на них типові бездротові мережеві адаптери. Найбільш важливий елемент безпровідних мереж – безпровідна точка доступу (англ. Wireless Access Point). Для забезпечення безпровідним користувачам доступу до вже існуючої мережі Ethernet потрібно встановити будь-яку безпровідну точку доступу.

Рисунок 1.5 –Схема побудова відеосистеми на Wi-Fi [20, 45]

Точки доступу WiFi мережі виконують найрізноманітніші функції. До них відносяться:

- підключення групи комп'ютерів (кожен з безпровідним мережевим адаптером) в самостійні мережі;
- функція мосту між безпровідними і кабельними ділянками мережі.

Такі поєднання мережі називають "Інфраструктурою телекомунікаційної мережі" (Infrastructure) і використовуються для доступу до різноманітних баз даних або для підключення мобільних користувачів.

1.4 Місце криптографії як інструменту захисту інформації

Питання про достовірне та безпечне надсилання інформації від приймача до отримувача відоме ще з давніх часів. Основним завданням

криптографії в давні часи було забезпечення конфіденційності, або простіше кажучи шифрування – інформація, що містилася, мала бути змінена таким чином, щоб прочитати та зрозуміти міг лише той, кому дійсно назначено, а не будь-яка інша стороння особа, без відомостей про спосіб, яким було зашифрована відповідна інформація [30, 33].

Криптографічним алгоритмом (шифром) називається така математична функція, що дозволяє виконати над інформацією дію шифрування та дешифрування.

Найпопулярнішим способом в давні часи був так званий шифр Цезаря (або інша назва – шифр зсуву) – шифрування інформації, що передавалася на папері, в якому кожна буква тексту, що був написаний, замінювалась на ту, яка була віддалена (зсунута) на три позиції в буквенному алфавіті. Простий для нинішньої техніки шифр, став основою для складніших способів, до прикладу шифр Віженера чи ROT13 [30, 33].

З розвитком людства і науки, такі способи шифрування інформації ставали все більш неефективними. Наступним кроком стали машини, які виконували шифрування та дешифрування інформації, найвідомішою з яких є Енігма. Та з появою комп’ютерних систем, можна було зашифрувати будь-які дані, представивши їх у двійковому вигляді, а не лише у текстовому вигляді, як це відбувалося доволі довгий період людства.

В наш час це питання так і залишилось актуальним, тільки тепер інформацією обмінюються не лише люди, а й пристрої, які оточують нас. І чим більше є таких пристроїв, тим гостріше стає це питання.

До криптографічних методів зазвичай висувають наступні вимоги, що їх реалізації [30, 33]:

1. Зашифроване повідомлення можливо прочитати лише при наявності ключа;

2. Кількість операцій, що потрібно виконати атакуючою стороною для визначення використаного ключа шифрування стороною шифрування за наявністю фрагмента зашифрованого повідомлення та відповідного

відкритого тексту, повинно бути не менше загального числа можливих ключів, а зазвичай в рази перевищує;

3. Кількість операцій, які необхідні для розшифрування повідомлення способом прямого перебору ключів, а також повинно володіти жорсткій нижній пороговій оцінці й виходити за межі можливостей сучасного обчислювального устаткування, або вимагати надзвичайно високі витрати на обчислення;

4. На надійність ступеня захисту шифрованої інформації не впливає знання всіма сторонами алгоритму шифрування, більш того, зараз практикується надання такого відкритого доступу;

5. Будь-яка мінімальна заміна в ключі шифрування призводить до суттєвих змін великої частини зашифрованої інформації;

6. Незначна зміна даних в вихідному тексті має призводити до істотних змін в зашифрованої інформації при використанні того ж ключа шифрування;

7. Алгоритм, порядок виконання, початкові дані алгоритму шифрування завжди залишаються без змін;

8. Додаткові дані, що вводяться в вихідну інформацію в процесі її шифрування, також повинні бути надійно сховані в зашифрованій інформації;

9. Довжина зашифрованої інформації не повинна перевищувати загальну довжину вихідної інформації;

10. Мають бути виключені прості та легкі залежності, які використовуються для формування ключа шифрування;

11. Будь-який ключ з множини ключів має забезпечувати надійний захист інформації;

12. Реалізація алгоритму повинна бути доступна як на програмному так і на апаратному рівні.

1.4.1 Принцип захисту інформації в телекомунікаційних системах

Загальну структурну схему передачі інформації в телекомунікаційних системах із застосуванням криптографії можна зобразити в наступному вигляді:

Рисунок 1.6 – Загальна структурна схема передачі інформації із застосуванням криптографії [30, 33, 45]

Взаємодію між відправником і отримувачем з урахуванням криптографічної системи описується наступним чином:

1) Відправник отримує з джерела генерування ключів, ключ, яким буде зашифрована інформація;
2) Відправник зашифровує за допомогою ключа необхідну для передачі інформацію, та передає криптограму E відкритими каналами зв’язку в напрямку до одержувача;
3) Отримувач, за допомогою джерела генерування ключів, отримує необхідний ключ, для розшифрування зашифрованої інформації
4) Отримувач розшифровує за допомогою згенерованого ключа зашифровану інформацію, та отримує її в звичайному вигляді для ознайомлення.

1.4.2 Симетрична криптографія

Симетрична криптографія полягає у застосуванні такого шифрування, основою якого було застосування одного й того самого криптографічного ключа [45] для шифрування та дешифрування інформації, що мала бути передана каналами зв'язку. Загальна ідея симетричного шифрування зображена на рисунку 1.6.

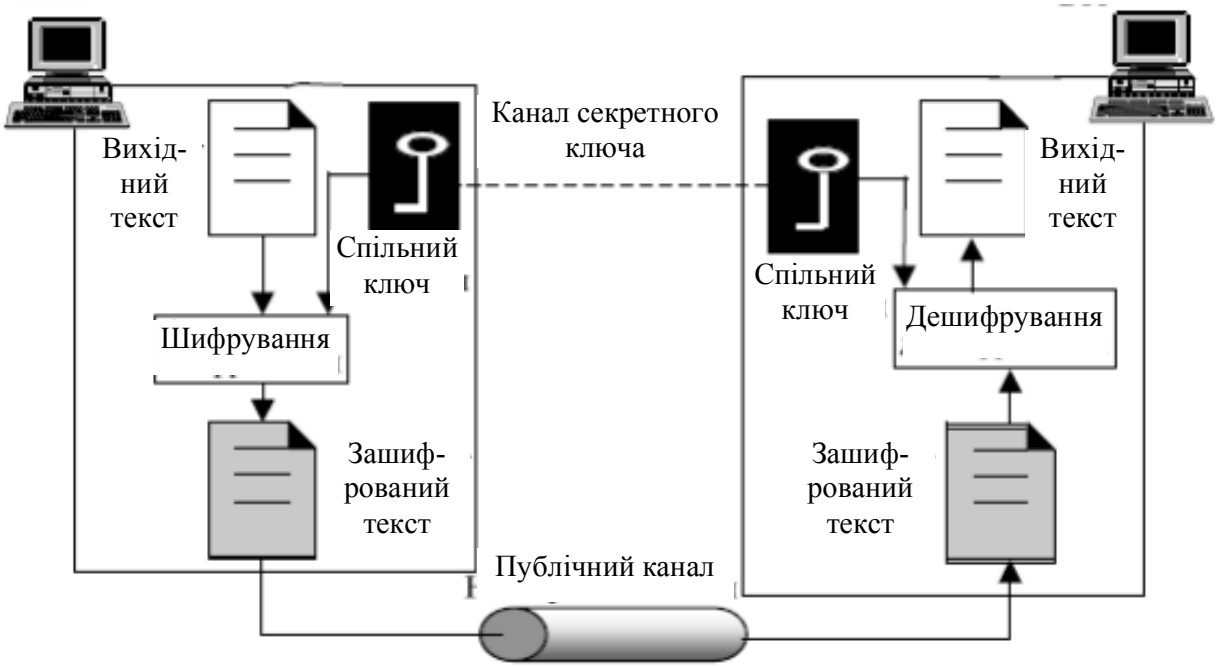

Рисунок 1.7 – Передача інформації між двома користувачами з використанням симетричної криптографії [45]

На рисунку джерело передає інформацію приймачу за допомогою несекретного каналу зв'язку, враховуючи що супротивник, підслуховує по каналу зв'язку зашифроване повідомлення, не розуміючи його сенс.

Первинне повідомлення, називається вихідним текстом; первинне повідомлення, над яким було здійснено дію шифрування називається зашифрованим текстом. Для створення зашифрованого тексту, Передавач використовує деякий алгоритм шифрування, а також спільний ключ засекречування. Для того, щоб Приймач зміг прочитати цю інформацію, він використовує алгоритм дешифрування, і той самий ключ засекречування,

який використовувала Передавач для шифрування. Ключ – це набір певних значень, який оперується алгоритмом шифрування.

Треба взяти до уваги, що ключ яким здійснюється шифрування та дешифрування використовується однаковий ключ (ключ, який містить в собі набір кодових значень). Окрім того, дії шифрування та дешифрування є інверсіями один одного. Однак постає питання про передачу іншим, але вже захищеним каналом зв'язку, секретного ключа. В ідеальному варіанті, припускається, що Передавач та Приймач мали зустріч віч-на-віч, і отримали цей ключ.

В загальному можна виділити наступні симетричні шифри, які використовуються в телекомунікаційних мережах [30, 33, 45]:

- Блочне симетричне шифрування
- Потокове симетричне шифрування

1.4.3 Блочне шифрування для систем телекомунікацій

Блочне шифрування, це є різновид симетричного шифрування, яке виконує дію над групами біт заданої довжини – блоками, в загальному які мають довжину блока в межах 64 – 256 біт.

Якщо відкритий текст має меншу довжину, ніж довжина заданого блока, то перед шифруванням цей блок доповнюється незначущою інформацією. Інакше кажучи, блочне шифрування являє собою підстановку на основі блочного алфавіту, який може бути моно-, або ж поліалфавітним. Найбільшого застосування блочне симетричне шифрування набуло в передачі інформації по мережі, в тому числі для систем пакетного обміну.

Роботу блочного шифрування можна представити наступним чином [30, 33, 45] (рисунок 1.8):

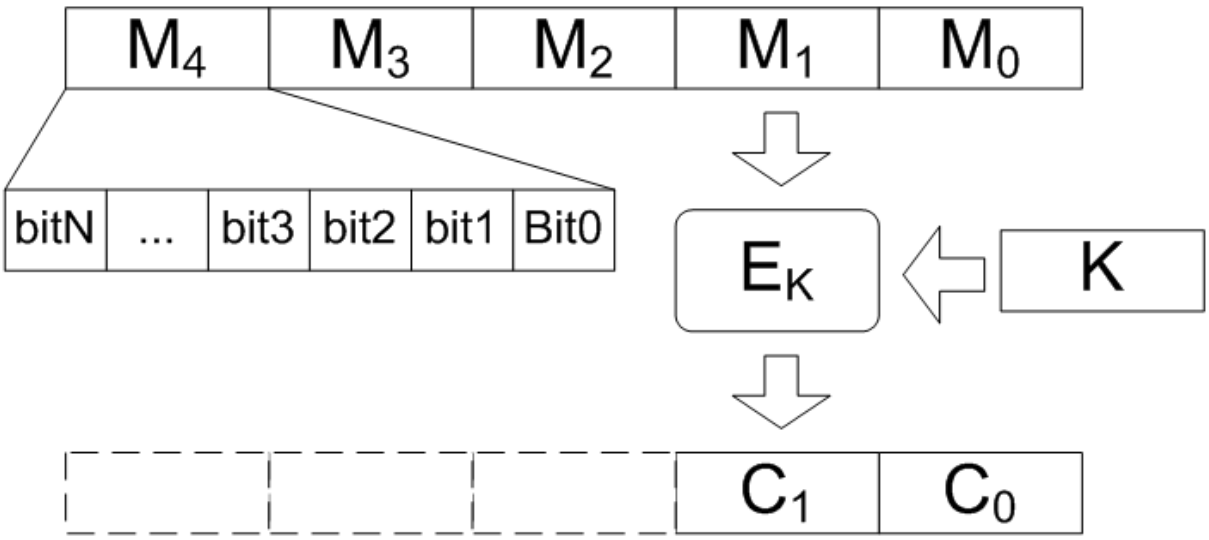

Рисунок 1.8 – Робота блочного шифрування

Блочний шифр здатний зашифрувати одним ключем одне чи навіть декілька повідомлень, які в загальній сумі їх довжин будуть більшими, аніж довжина ключа шифрування. Однак постає питання про надійність такого шифрування. Ще одним з мінусів блочного шифрування є мала швидкість шифрування, в порівнянні з потоковим шифруванням.

Основними алгоритмами в блочному шифруванні, які почали використовувати були [45]:

- DES
- AES

Стандарт DES став першим затвердженим симетричним блочним шифром, який використовувався як федеральний стандарт обробки інформації в США з 1977 року. Формування шифрованої інформації відображена на рисунку:

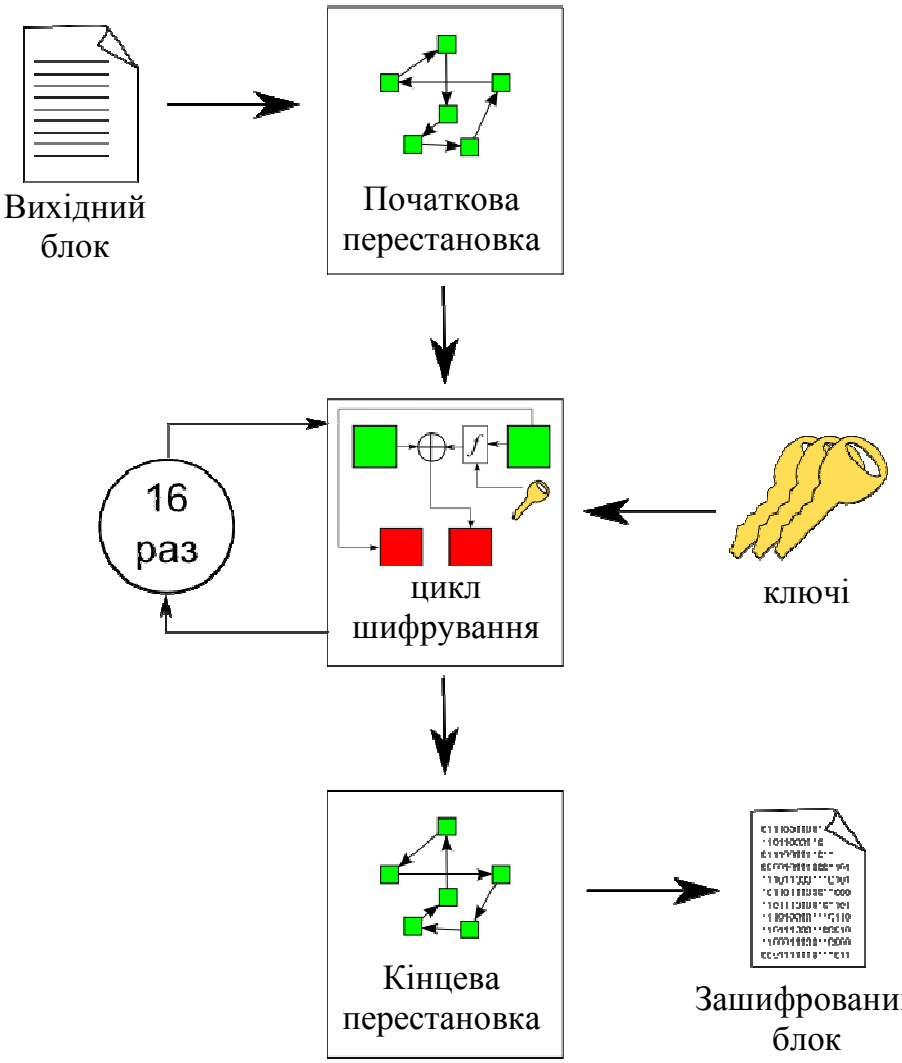

Рисунок 1.9 – Формування шифрованого повідомлення алгоритмом DES

В зв’язку з малою довжиною ключа, алгоритм блочного шифрування DES через деякий час був знятий з користування для роботи з комерційними даними.

Наступником алгоритму DES став алгоритм AES [45, 49]. Заснований даний алгоритм був на основі алгоритму Rijndael. Основний недолік, який був в DES, був виправлений, і алгоритм був змінений 26 травня 2002 року.

Діаграма формування шифрованого повідомлення та його дешифрування зображена на рисунку.

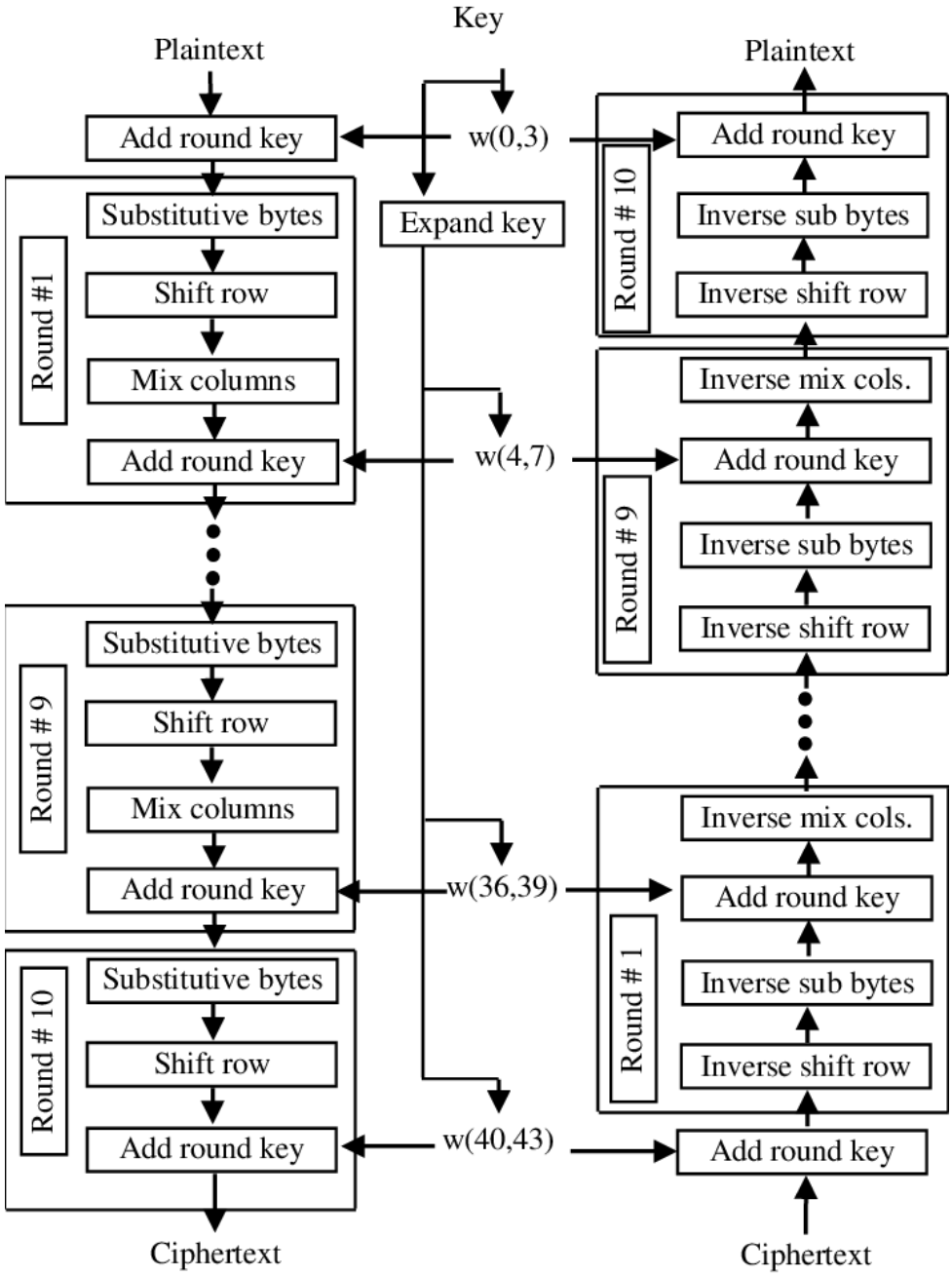

Рисунок 1.10 – Процес шифрування та дешифрування повідомлення, використовуючи алгоритм AES [49]

1.4.4 Потокові шифри

Для роботи з потоками даних знайшли своє застосування так звані потокові шифри [30, 33, 45]. Це є різновид симетричного шифрування, який полягає в тому, що кожен символ вихідного тексту під дією алгоритму шифрування перетворюється на символ зашифрованого тексту в залежності не лише від використовуваного ключа шифрування, але й від місця в потоці

відкритого тексту. Потоковий шифр реалізовує інший підхід до шифрування, аніж в блочному шифруванні.

Найпростіше зображення того, як працює потоковий шифр, можна зобразити наступним чином:

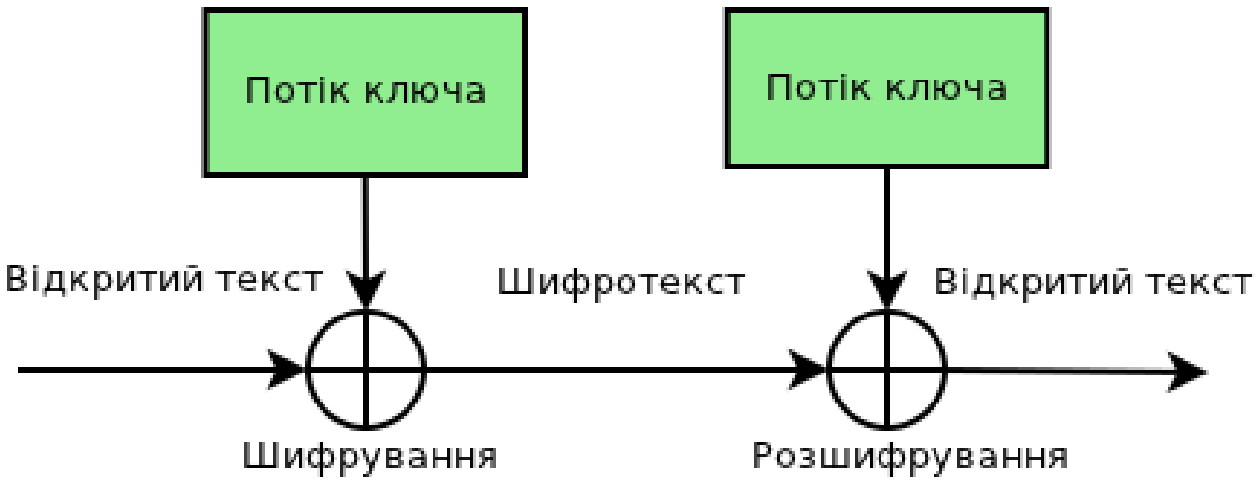

Рисунок 1.11 – Робота потокового шифру [30, 33, 45]

Формування шифрованого повідомлення відбувається наступним чином: з генератора потоку ключів генерується ключовий потік a_1, a_2 $a_3 ... a_L$. Назвемо потік вхідного тексту b_1, b_2, $b_3 ... b_L$. При виконанні над цими бітами дії XOR, буде сформовано новий біт c_1, c_2, $c_3 ... c_L$. Нові біти, які будуть сформованими, будуть утворювати потік уже зашифрованого повідомлення. Розшифрування ж даного зашифрованого повідомлення також буде виконуватися операцією XOR.

Послідовність бітів генератора потоку ключів не має якогось певно визначеного періоду, вони будуть обиратися зовсім випадково, що в свою чергу буде давати для такого шифру високу ступінь безпеки.

Основними видами потокових шифрів є [30, 33, 45]:

- Синхронні потокові шифри;
- Самосинхронні потокові шифри.

1.4.5 Синхронні потокові шифри

Синхронні потокові шифри – такий вид потокового шифрування, в якому генерування потоку ключів для шифрування та дешифрування відбувається самостійно, а не в залежності від зашифрованого чи відкритого тексту повідомлення. Коли відбувається момент шифрування повідомлення, генератор потоку ключів генерує такі ж самі потоки, які необхідні для того, щоб дешифрувати повідомлення. В разі, якщо один з символів зашифрованого повідомлення буде втрачений чи змінений, відбудеться збій в синхронізації генераторів, що в результаті призведе до неможливості подальшого коректного дешифрування всього зашифрованого повідомлення.

Використання цього виду потокових шифрів має декілька переваг, а саме:

- Захист в разі зміни, вставлення додаткових частин, або ж видалення певної частини в шифрованому повідомленні, призведе до десинхронізації, внаслідок чого, повідомлення неправильно чи невірно буде розшифроване;
- Відсутність проблем з розповсюдженням помилки в шифрованому тексті. В разі, якщо був викривлений один біт, неправильно буде дешифрований лише він.

Разом з перевагами, є і недоліки в даному шифрі:

- Можливість внесення змін зловмисником, в разі, якщо він має в своєму розпорядженні зміст відкритого тексту. Тоді він може скорегувати його таким чином, яким буде йому вигідно.

Основними алгоритмами шифрування інформації в синхронних потокових шифрах є: A5, Oryx, RC4, SEAL, та багато інших різновидів [45]:

A5 – криптографічний алгоритм потокового шифрування, який використовується забезпечення в GSM конфіденційності даних що передаються між базовою станцією та стільниковим телефоном.

Oryx – алгоритм потокового шифрування що був використаний в мережах стільникового зв’язку IS-6 та CDMA2000 для захисту голосових даних.

RC4 – алгоритм потокового шифру, який набув широкого застосування в захисті інформації комп'ютерних мереж (протоколи SSL, TLS, а також використовується в протоколах безпеки бездротових мереж WEP, WPA).

SEAL – алгоритм потокового шифру, який оптимізований під реалізацію на програмному рівні. Схема роботи алгоритму зображена на рисунку.

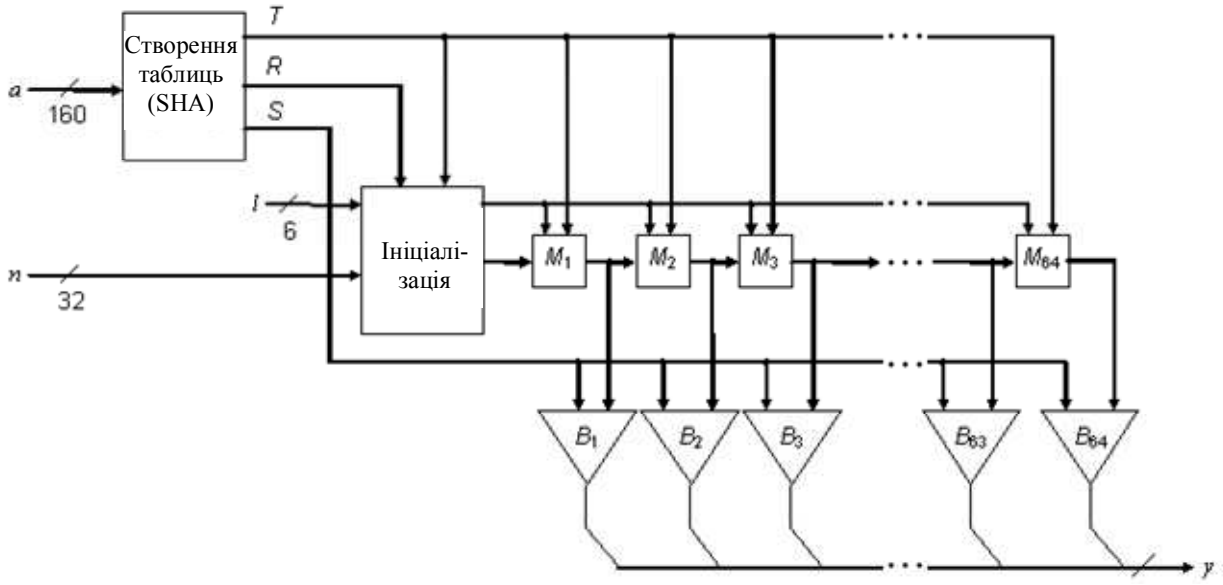

Рисунок 1.7 – Схема роботи алгоритму SEAL [28, 29, 45]

1.4.6 Асиметрична криптографія

Асиметрична криптографія, або криптографія з відкритим ключем – різновид криптографічного захисту інформації в якому для передачі зашифрованої інформації використовується один ключ, а для дешифрування такої інформації – інший [45].

З використанням такої схеми пішла назва – асиметрична. Загальна схема відправлення та отримання зашифрованого повідомлення з використанням асиметричної криптографії зображена на наступному рисунку.

В асиметричній криптографії використовується два ключі:

- публічний ключ;
- приватний ключ.

Відправник використовує публічний ключ для шифрування відкритого тексту для Отримувача, якщо знати вміст відкритого тексту має знати лише він. Дане зашифроване повідомлення відправляється будь-яким способом. Приватний ключ є таємним ключем, і не розголошується. Для того що виконати дешифрування такого повідомлення, необхідно використати приватний ключ.

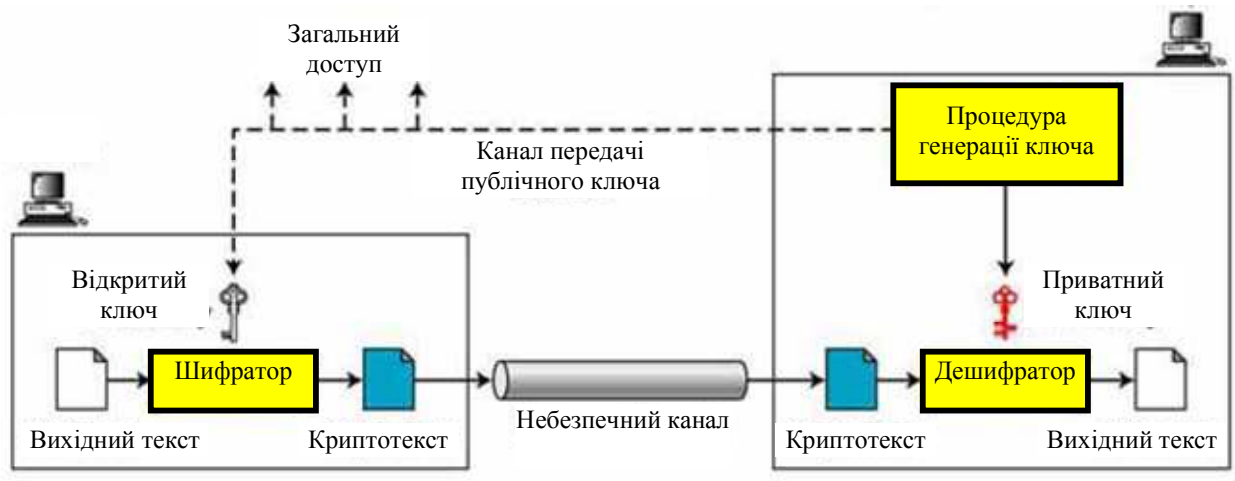

Рисунок 1.12 – Загальна схема асиметричної криптографії [49]

В загальному, асиметричне шифрування можна описати наступними принципами:

- Для відкритого і закритого ключа можна згенерувати пару достатньо великих чисел, щоб не було можливості вирахувати приватний ключ через значення публічного ключа, враховуючи що спосіб генерації є загальнодоступним;

- Присутні високонадійні методи шифрування, які дозволять зашифрувати відкритий текст публічним ключем таким чином, що для дешифрування цього повідомлення тільки і лише приватним ключем. Спосіб генерування є загальновідомим;

- Власник публічного та приватного ключа не повідомляє про значення приватного ключа, але публічний ключ може бути переданий довіреним особам і він буде загальнодоступним.

Висновки до розділу

1. Розглянуто базові принципи побудови дротових та бездротових систем телекомунікацій. Встановлено основні засади розвитку бездротових технологій.

2. Розглянуто процес криптографічного перетворення в загальному. Показані існуючі методи, що забезпечують симетричне та асиметричне шифрування інформації. Показані їх властивості, а також основні вимоги до алгоритмів. Найбільш важливими є – відкритість алгоритмів та суттєва зміна даних при мінімальній зміні вхідних даних або ключа.

РОЗДІЛ 2 ВИКОРИСТАННЯ КРИПТОГРАФІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

2.1 Застосування сенсорних мереж

Зазвичай бездротові сенсорні мережі (БСМ) застосовується для збору даних з пристроїв, оснащених сенсорами : датчиком температури, вологості, освітлення, тобто моніторингу. Наприклад, мініатюрні сенсори можуть бути використані в медицині для спостереження за пацієнтами. Пристрої, які пацієнт носить з собою, можуть контролювати роботу життєво важливих органів і у разі якихось небезпечних ситуацій повідомляти лікаря.

Невеликі розміри пристроїв дозволяють проводити не лише «поверхневі» спостереження за пацієнтом, але і досліджувати внутрішні органи людини. Так при проведенні гастроскопії в лікарнях, поліклініках застосовують спеціальні апарат, з гастроскопической трубкою, але не усі пацієнти можуть її проковтнути. На ринку вже існують пристрої у вигляді пігулок для проведення таких досліджень. Ці пристрої з батарейним живленням мають запас енергії, достатній того, щоб безперервно працювати впродовж годин або діб і відправляти свідчення іншому пристрою, який пацієнт носить з собою впродовж цього часу. Після цього лікар може аналізувати отримані результати і поставити точний діагноз.

Сенсори можуть використовуватися для автоматичного включення освітлення, коли людина входить в кімнату, використовуватися для управління яких-небудь пристроїв (у системі «Розумний будинок»).

Іноді вимагається стежити за рухливістю або руйнуванням яких-небудь об'єктів, де важко прокласти кабелі. Для цього знову ж таки вигідніше застосувати сенсорні мережі, оскільки датчики мають автономне джерело живлення і вони бездротові.

Також технологія безпровідних сенсорних мереж може бути використана для передачі звукових даних - в якості домофонной системи, мультимедіа системи з низьким енергоспоживанням.

2.2 Вибір стандарту безпровідних мереж

Існує велика кількість різних стандартів безпровідних мереж. Проте ці стандарти можна підрозділити на три групи:

- WPAN (Wireless Personal Area Network - безпровідна персональна мережа);
- WLAN (Wireless Local Area Network - безпровідна локальна мережа),
- WMAN.

З цих груп найбільш відповідними можуть бути стандарти групи WPAN, оскільки вони розраховані на низькошвидкісні мережі.

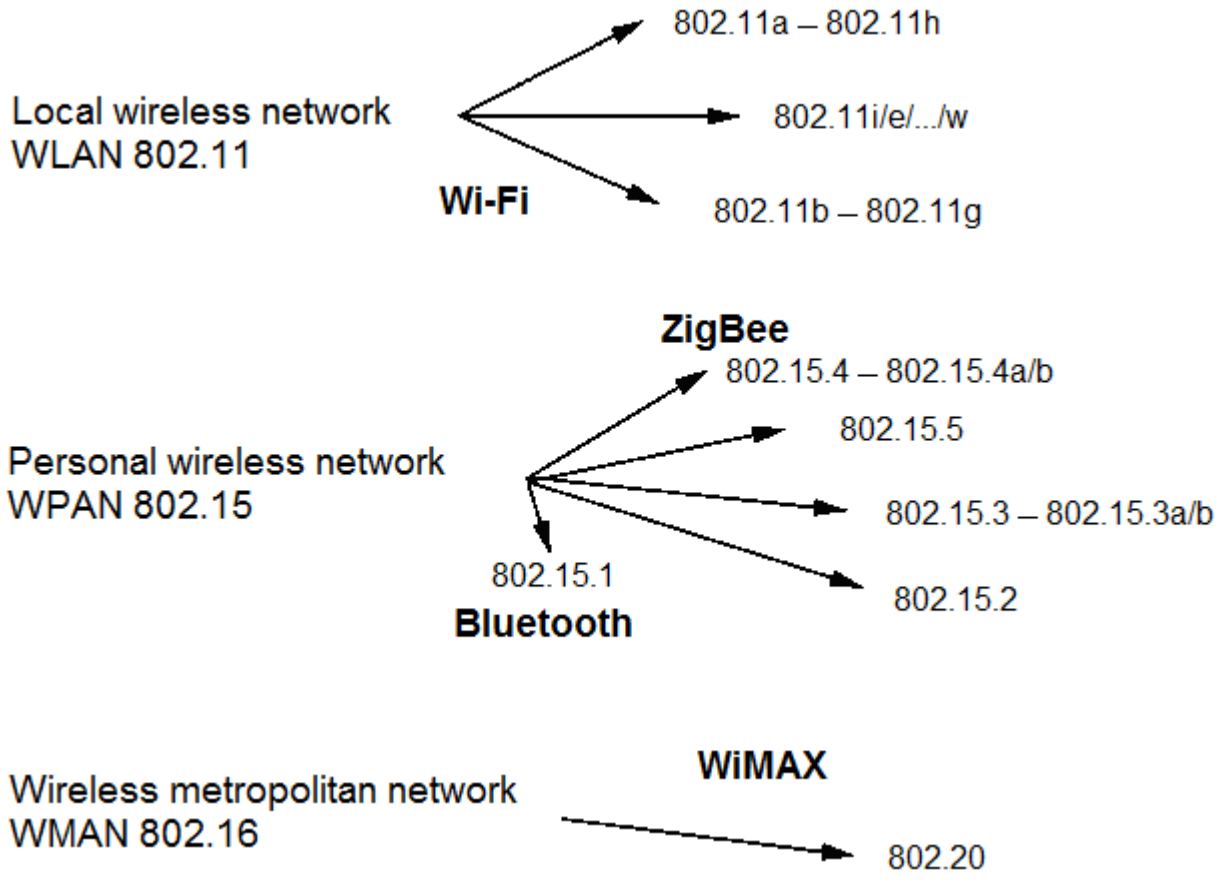

Рисунок 2.1 – Стандарти безпровідних мереж

WPAN (Wireless Personal Area Network) безпровідна мережа, що призначена для організації бездротового зв'язку між різними типами пристроями на обмеженій площі (наприклад – квартира, офісне, або робоче місце).

Стандарти, що визначають методи функціонування WPAN мережі описані в частині сімейства специфікацій IEEE 802.15.

Стандарт IEEE 802.15.3 розроблявся як високошвидкісний стандарт WPAN-сереж для застосування високотехнологічних побутових застосувань . Ці застосування призначені як правило для передачі мультимедійних даних.

Використання смуги частот 2,4 ГГц і також технологія модуляції OQPSK (Offset Quadrature Phase Shift Keying, квадратурна маніпуляція фазовим зсувов зі зміщенням) дозволяє досягнути швидкості передачі в 55 Мб/с на відстань до 80-125 метрів. Для захисту даних використовується такий криптографічний стандарт як AES.

У модифікації стандарту 802.15.3a передбачається зростання пропускної здатності до майже 500 Мб/с, а у разі специфікації 802.15.3b пропускна спроможність складе від 0,1 до 0,4 Гб/с. Отже цей стандарт передбачається для передачі на великих швидкостях при передачі даних, а як наслідок, пристрої за цим стандартом матимуть високе енергоспоживання.

802.15.4 і Zigbee часто ототожнюються між собою, адже в основі стандарту Zigbee лежить стандарт 802.15.4 [12].

Проте консорціум ZigBee Alliance вніс ряд змін і розширив його – стандарт 802.15.4a та 802.15.4б. Стандарт 802.15.4 є відкритим і його можна вільно викачати з Інтернету і використати, Zigbee же є наполовину відкритим стандартом: так при використанні його в комерційних цілях необхідно вступати в ZigBee Alliance. До мінусів цього стандарту можна віднести його закритість, а також велика сфера застосування, а не «заточенность» під конкретні цілі.

Стандарт Bluetooth (802.15.1) [12] на сьогодні добре розвинений і застосовується для зв'язку мобільних телефонів, КПК, периферії. Проте він

не розрахований на мережі з низьким енергоспоживанням, що суттєво обмежує його поширення в сенсорних мережах. Пристрої за стандартом Bluetooth можуть об'єднуватися в пикосети (не більше 7 на одну мережу). У мережі є провідний і ведений пристрій.

Для обміну даними використовується так званий нижній ISM -диапазон (Industry, Science and Medicine - промисловий, науковий і медичний) 2,4-2,5 ГГц, який поширений в побутових приладах і безпровідних мережах. Для використання цих частот ліцензію не потрібно. Потужність передавача-кристала складає 1 - 2,5 мВт і дальність дії до 10 м, а при збільшенні потужності до 100 мВт - 100 м. Цей стандарт міг би підійти для розробки, проте на ринку не є пристрої, працюючі за цим стандартом з низьким енергоспоживанням, вони тільки передбачаються до випуску на ринок.

Стандарт Wibree розроблений фірмою Nokia в 2001 році [12]. Wibree призначений для роботи пліч-о-пліч з стандартом Bluetooth. Він також працює в діапазоні 2,4 ГГц з фізичною швидкістю передачі 1 Мбіт/с. Основні сфери застосування включають такі пристрої, як наручний годинник, бездротові клавіатури, іграшки і спортивні датчики, де низьке енергоспоживання є однією з ключових вимог. Стандарт Wibree можна віднести до одного з варіантів стандарта Bluetooth, тому у нього є такі ж недоліки - кількість пристроїв, що підключаються, обмежена, відсутні на ринку модулі з низьким енергоспоживанням.

Порівняльна характеристика деяких стандартів виглядає таким чином (Таблиця 1).

Найбільш відповідний стандарт 802.15.4, оскільки він є відкритим, призначений для низькошвидкісних мереж з низьким енергоспоживанням.

Таблиця 2.1 – Порівняння стандартів безпровідних мереж

	Bluetooth	Wibree	ZigBee
Частота	2,4 ГГц	2,4 ГГц	2,4 ГГц
Споживана потужність	100 мВт	~10 мВт	30 мВт
Термін роботи батареї	до 6 місяців	1 - 2 роки	0,5 - 2 роки
Діапазон	10 - 30 м	10 м	10 - 75 м
Швидкість передачі	1 - 3 Мб/с	1 Мб/с	25-250 Кб/с
Ціна	3$	3,2$	2$
Топології	Зірка, точка-точка, змішана		
Безпека	128-бітове шифрування		
Час відгуку	3 с	3 с	15 мс

2.3 MAC–рівень застосування методів криптографії для задач телекомунікацій

Протоколи, регламентовані стандартами IEEE 802.15.4 і ZigBee 2007 Specification, забезпечують формування і функціонування безпровідної сенсорної мережі.

Стандарт IEEE 802.15.4 визначає фізичний і MAC рівні, а специфікація ZigBee визначає мережевий рівень і рівень додатків. На рисунку нижче показаний стек протоколів ZigBee.

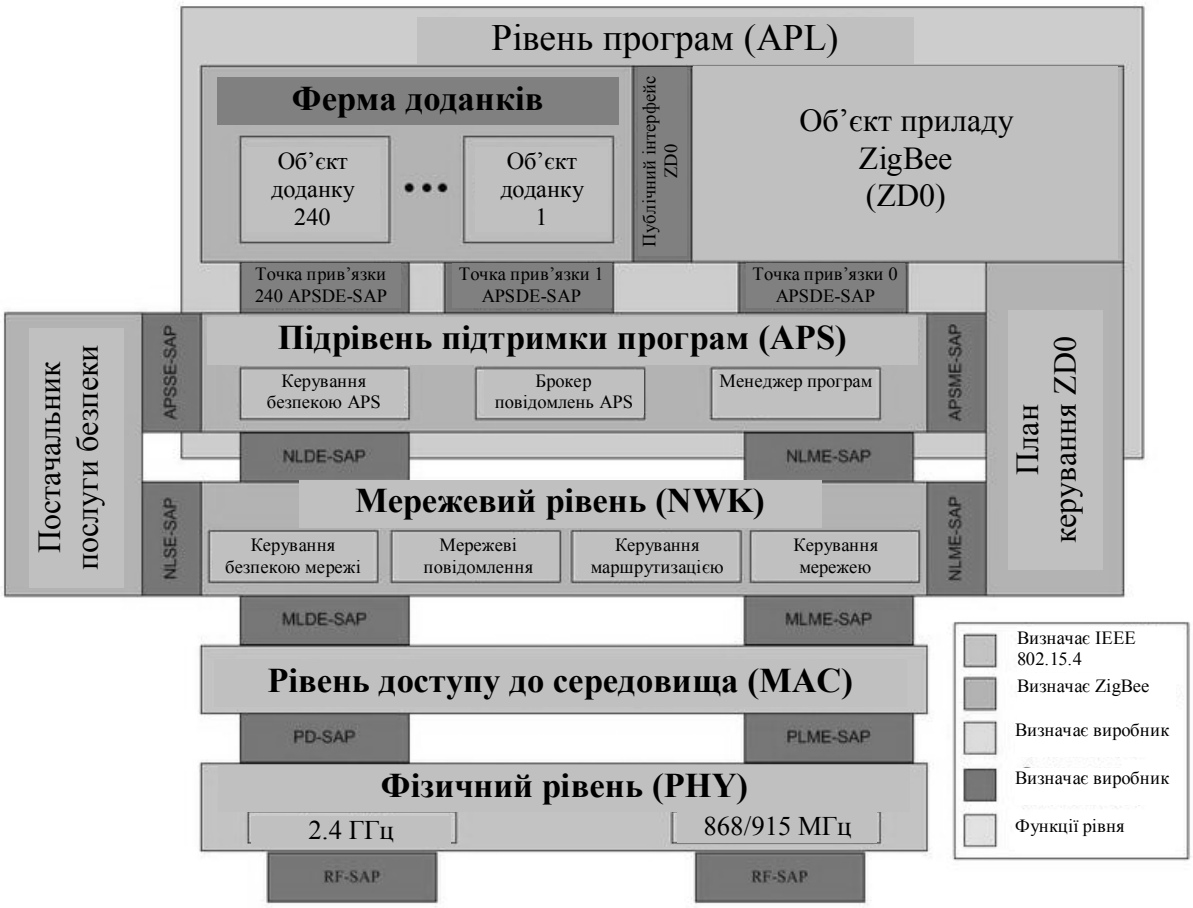

Рисунок 2.2 – Структура мережевих стеку протоколів ZigBee [49]

Фізичний рівень реалізації стандарту IEEE 802.16 забезпечує безпосередню доставку потоків різнорідних даних між її рівнями. Усі покладені завдання в стандарті пов'язані з формуванням певної структури даних, а також управлінням роботою системи – всі навантажуються на MAC (Medium Access Control), - рівні [49].

Телекомунікаційне устаткування стандарту IEEE 802.16 формує необхідне транспортне середовище для надання різних послуг (сервісів).

Перше завдання, що вирішується в IEEE 802.16, - це механізм підтримки різноманітних сервісів верхнього рівня.

Розробники стандарту IEEE 802.16 прагнули створити універсальний, спільний для всіх реалізацій протоколу MAC-рівня, незалежно від фізичних реалізацій особливостей довільного каналу (Рисунок2.3). Це суттєво спрощує зв'язок між терміналами кінцевих користувачів з робочою мережею передачі

даних. У свою чергу фізична частина середовища передачі в різних фрагментах WMAN може бути різною, але структура переданих даних єдина.

<table>
<tr><td>Додатки верхніх рівнів</td><td colspan="2">VoIP</td><td>IP</td><td>E1</td></tr>
<tr><td rowspan="3">MAC-рівень</td><td colspan="4">Підрівень перетворення CS</td></tr>
<tr><td colspan="4">Основний підрівеь</td></tr>
<tr><td colspan="4">Підрівень безпеки</td></tr>
<tr><td>Фізичний рівень</td><td>Кадр n-1</td><td>Кадр n</td><td>Кадр n+1</td><td>Кадр n+2</td></tr>
<tr><td>Схема передачі</td><td colspan="4">  </td></tr>
</table>

Рисунок 2.3 – MAC-рівні стандарту IEEE 802.16

У одному каналі можуть працювати сотні різних одиниць термінального обладнання великого числа кінцевих користувачів.

Цим користувачам потрібний доступ до різних сервісів (додатки):

- передача голосу і даних з тимчасовим розділенням;
- з'єднання по протоколу IP;
- пакетна передача мови через IP (VoIP) і тому подібне.

Структурно MAC-рівень IEEE 802.16 розділений на три підрівні:

- підрівень перетворення сервісів CS (Convergence Sublayer);
- основний підрівень CPS (Common Part Sublayer);
- підрівень захисту PS (Privacy Sublayer).

На підрівні захисту PS реалізуються функції, що надають потрібний рівень криптозахисту даних і механізми аутентифікації/запобігання несанкціонованому доступу.

Для цього передбачені набори алгоритмів криптозахисту і протокол управління ключем шифрування. Ключ шифрування (асиметричний або

симетричний) кожна базова станція може передавати самостійно в процесі авторизації, використовуючи схему роботи «клієнт - сервер». [17]

На підрівні перетворення сервісу CS відбувається трансформація потоків цих різнорідних протоколів верхніх рівнів для передачі їх через мережі-носії. Фактично для кожного типу додатків верхніх рівнів передбачено свій механізм перетворення. Специфікації стандарту IEEE 802.16 містять механізми роботи в режимі ATM і пакетної передачі. Під пакетною передачею мають на увазі досить широкий набір різних пакетів типу IP, PPP і IEEE Std 802.3 (Ethernet).

Мета роботи на CS - підрівні - оптимізація передаваних потоків даних кожного застосування верхнього рівня з урахуванням їх специфіки. Розрізняють 4 типи трафіку за вимогами до затримок: - Unso licited Grant Service - передача в реальному часі сигналів і потоків телефонії (E1) і VoIP.

RTPS - Real Time Polling Service - потоки реального часу з пакетами змінної довжини (MPEG відео) - Time Polling Service - підтримка потоків змінної довжини при передачі файлів в широкосмуговому режимі BE - Best Effort - інший трафік.

На Рисунок 2.4 вказані операції, що виконуються на окремих підрівнях рівня MAC.

Підрівень перетворення
- Упаковка PDU для нижчого рівня
- Упаковка PDU для вищого рівня
Загальна частина MAC
– Введення та подавлення заголовків
- Режим запиту повторної передачі
– Фрагментація
– Встановлення підключення/відключення
– Керування якістю (QoS)
– Багатокористувацькі послуги
– З’єднання/відключення з мережею
– Керування використаною смугою частот
Підрівень безпеки
– Підтримка режиму шифрування
– Обмін даними при переході до шифрування
– Обмін ключем авторизації
– Взаємна аутентифікація

Рисунок 2.4 – Основні операції на рівні MAC

Сформовані пакети даних MAC PDU [12] (MAC Protocol Data Unit, блоки даних MAC-рівня) далі передають на фізичний рівень і транслюють по каналу зв'язку. Пакет MAC PDU включає заголовок і поле даних (його може і не бути), за яким може йти контрольна сума CRC (cyclic redundant check). Визначені два формати заголовка MAC:

- перший - основний заголовок MAC, з якого розпочинається кожен протокольний блок даних рівня MAC PDU і що містить або повідомлення управління MAC або дані CS;
- другий - заголовок запиту додаткової пропускної спроможності. Загальний заголовок використовують в пакетах, у яких є присутнім поле даних. Формат основного заголовка MAC приведений на Рисунок 2.5.

1	1	6	1	1	2	1	11	16	8
HT	EC	Type	ESF	CI	EKS	Rsv	LEN	CID	HCS

48 біт

Рисунок 2.5 – Формат основного заголовку MACC+

Заголовок запиту смуги використовують, коли АС звертається до БС із запитом про виділення або збільшення смуги пропускання у висхідному каналі. При цьому в заголовку вказують CID і розмір необхідної смуги. Полі даних після заголовка запиту смуги відсутній [2].

Поля основного заголовка MAC визначені в таблиці 2.1

Таблиця 2.2 – Поля основного заголовка MAC

Полі	Довжина (біт)	Опис
HT	1	Покажчик типу заголовка. HT=0 - заголовок загального типу HT=1 - заголовок запиту пропускної спроможності
EC	1	Ознака шифрування поля даних. EC=0 - вміст поля даних не шифрується EC=1 - вміст поля даних шифрується
Type	6	Тип поля даних.
ESF	1	Покажчик наявності розширеного підзаголовка.
CI	1	Ознака наявності контрольної суми CRC.CI=0 - контрольна сума відсутня CI=1 - контрольна сума CRC міститься в пакеті
EKS	2	Індекс ключа шифрування
Rsv	1	Rsv=0 - не використовується
LEN	11	Довжина у байтах пакету MAC PDU, включаючи MAC заголовок і контрольну суму CRC, якщо вона є присутньою
CID	16	Ідентифікатор з'єднання.
HCS	8	Контрольна сума заголовка.

2.4 Бездротові сенсорні мережі

Нині бурхливо розвивається технологія безпровідних сенсорних мереж. Бездротові сенсорні мережі – це розподілені мережі, що здатні до самоорганізації, стійкі до відмови окремих елементів, що обмінюються інформацією по безпровідному зв'язку. Кожен елемент мережі має автономне джерело живлення, мікрокомп'ютер, приймач/передавач. Область покриття мережі може складати від декількох метрів до декількох кілометрів, залежно від типу модуля і антени, а також за рахунок здатності ретрансляції повідомлень від одного елементу до іншого. Обмін даними між двома кінцевими пристроями може здійснюватися через ретранслятор, у тому

випадку, якщо дальність роботи цих пристроїв не дозволяє їх взаємне виявлення. Таким чином, пристрою з малим радіусом дії за допомогою системи ретрансляторів можуть спілкуватися один з одним.

Виділяють наступні основні стандарти для малопотужних безпровідних мереж:

- IEEE 802.15.4;
- ZigBee;
- Bluetooth;
- Wibree.

На сьогодні існує безліч варіантів доступу до мережі Інтернет. Вони діляться на кабельні або дротяні і бездротові або радіомережі. У рамках цієї роботи основний акцент (тобто нас цікавитимуть) робиться на існуючих безпровідних технологіях, зокрема на LTE, Wi-Fi, WiMAX, ZigBee. Для складання детальнішої порівняльної картини, розглянемо кожну з них окремо.

2.4.1 Технічні параметри та захист даних в технології Wi-Fi

Технологія безпровідного доступу розроблена консорціумом Wi-Fi Alliance на базі стандартів IEEE 802.11, а термін «Wi-Fi» — торгова марка, що належить «Wi-Fi Alliance».

Технологію назвали Wireless-Fidelity (дослівно «безпровідна точність») по аналогії з Hi-Fi. Встановлення пристроїв Wireless LAN рекомендується там, де розгортання кабельної системи є неможливим через ряд факторів – наприклад через економічну недоцільність, або через технічну складність, або через необхідність реалізації мережі з невідомою кількістю вузлів.

У багатьох організаціях використовується Wi-Fi мережа. За певних умов швидкість роботи мережі не потребна в 100 Мбіт/сек. А користувачі можуть переміщатися між точками доступу по території покриття мережі Wi-Fi мережі без необхідності додаткових дій.

Частотний діапазон прив'язаний до діапазону 2.4 ГГц, який в США і низці інших країн не належить до необхідності обов’язковості ліцензування. Стандарти зв’язку 802.11b\g\n орієнтовані на діапазон з насійною частотою від 2.412 ГГц до 2.484 ГГц. Стандарти 802.11a\h\j орієнтовані на частоти 5.170-5.905 ГГц. Стандарт 802.11y на частотний діапазон 3.6575-3.690 ГГц.

Подібно до проводового Ethernet, стандарт IEEE 802.11 визначає протокол використання єдиного фізичного середовища передачі даних, що дістав назву carrier sense multiple access collision avoidance (CSMA/CA).

Вірогідність виникнення колізій при передачі повідомлень у безпровідних вузлів мінімізується шляхом попередньої посилки стартового короткого повідомлення, що називається "ready to send" (RTS). Повідомлення RTS інформує інші вузли про тривалість майбутньої передачі і адресата.

Завдяки введенню короткого повідомлення RTS підвищується шанс на передачу тільки від одного вузла мережі. У свою чергу це дозволяє іншим вузлам затримати передачу на якийсь час, що дорівнює оголошеній тривалості повідомлення.

Приймальна станція повинна відповісти на пакет RTS посилкою пакету "clear to send" (CTS). Це дозволяє вузлу-ініціатору дізнатися, чи вільне середовище і чи готовий приймальний вузол до продовження прийому значно більшого пакету. Після отримання пакету даних від передавача, приймальний вузол повинен передати пакет підтвердження – ACK. Пакет ACK підтверджує факт безпомилкового прийому. Але якщо ACK не отримане, то передачу пакету даних слід спробувати ще раз.

Важливою вимогою у технології є безпека передачі даних. На MAC-рівні передбачено механізм захисту даних, що включає аутентифікацію станцій і власне шифрування передаваної інформації.

Цей механізм повинен забезпечувати такий же рівень захисту, як і в звичайних мережах Ethernet, тому його назвали WEP (Wired Equivalent Privacy — еквівалент дротяної конфіденційності). Алгоритм WEP заснований на використанні чотирьох спільних для однієї мережі секретних ключів

завдовжки 40 біт. Саме шифрування відбувається по алгоритму RC4 компанії RSA Security.

Алгоритм використовує перемноження блоків початкових даних на псевдовипадкову послідовність такої ж довжини, що і блок шифрованих даних. Генератор псевдовипадкової послідовності ініціалізувався 64-разрядпым числом, що складається з 24-разрядног'о вектору ініціалізації (IV — initialization vector) і 40-розрядного секретного ключа.

Суттєво важливим є те, що якщо секретний ключ відомий облаштуванням мережі і незмінний, то вектор TV може змінюватися від пакету до пакету. Для захисту від несанкціонованого зміні передаваної інформації кожен шифрований пакет захищається 32-розрядною контрольною сумою (ICV — integrity check value).

Таким чином, при шифруванні до передаваних даних додається 8 байт: 4 для ICV, 3 для IV, і ще 1 байт містить інформацію про номер використовуваного секретного ключа (одного з чотирьох). Відмітимо, що секретний ключ може бути набагато довший — 64, 128 біт і т. д. Це не суперечить стандарту, більше того, таке телекомунікаційного устаткування випускається, проте законодавство США перешкоджає експорту пристроїв, що підтримують шифрування даних з ключем довше 40 біт. Саме тому виробники і обмежуються 240 варіантами ключа. Додаткові методи захисту інформації і аутентифи-кации в мережах 802.11 описані в стандарті IEEE 802.11i.

Стандарт IEEE 802.11 передбачає два режими управління мережею: коли функції управління розподілені між усіма вузлами мережі IEEE 802.11 — так званий режим DCF (Distributed coordination function) — і коли вони зосереджені в одній визначеній точці доступу — режим PCF (Point coordination function).

Увесь обмін в мережах IEEE 802.11 відбувається за допомогою окремих кадрів (frames). По їх структурі чітко видно, що вони розділенені на

фізичному та MAC-рівні. Фактично сам кадр формується на MAC-рівні, де на фізичному рівні до нього додається заголовок фізичного рівня (PLCP).

На MAC-рівені пакети передаються від застосунків верхнього рівня. Якщо їх розмір перевищує максимально допустимий в IEEE 802.11, відбувається типовий процес дефрагментації. Дефрагментація має на меті розбиття великого пакету на декілька менших, розміри яких допустимі згідно того ж стандарту IEEE 802.11, які передаються за спеціальною процедурою.

Самі ж кадри MAC-рівня можуть бути трьох типів: кадри даних, контрольні (як вже вище описувальось – ACK, RTS, CTS а також інші), в тому числі кадри управління (наприклад, Beacon). Їх структура однакова (Рисунок 2.6). Кожен MAC-кадр включає :

- MAC-заголовок, поле даних (Frame Body)
- контрольну суму CRC.

У заголовку передається повна інформація про :

- версію протоколу стандарту групи IEEE 802.11;
- тип кадру;
- захист
- інші данні (поле Frame Control);
- тривалість процедури передачі пакету (Duration/ID);
- адреси одержувача/посилача (Addressl — 4; чотири адресні поля потрібні, якщо пакети передаються з підмережі однієї точки доступу до підмережі інший)
- інформація про послідовність пакетів (Sequence Control).

2	2	6	6	6	2	6	Від 0 до 2312	4
Контроль фрейму	Тривалість	Адрес 1	Адрес 2	Адрес 3	Контроль послідовності	Адрес 4	Корисні дані	Контрольна сума
MAC-заголовок								

Рисунок 2.6 – Структура кадра MAC-уровня стандарта IEEE 802.11 (розмір у байтах)

2.4.2 Технічні параметри та захист даних в WiMAX

До кінця 90-х років необхідність розробки технології дешевого широкосмугового доступу (BWA, Broadband Wireless Access) до послуг зв'язку стала очевидною. Дорожнеча інсталяції фіксованого і супутникового телекомунікаційного устаткування, особливо у важкодоступних і малонаселених районах, частенько призводило до щонайповнішої відсутності послуг зв'язку на досить великих територіях. Велика кількість телекомунікаційних корпорацій і фірм вела роботи по проектуванню і побудові безпровідних мереж проблеми «останньої милі», що забезпечують рішення, і що надають широкосмуговий доступ на істотній (у декілька десятків кілометрів) відстані від базової станції. Майже усі корпоративні рішення були приречені на провал в силу таких об'єктивних чинників як дорожнеча телекомунікаційного устаткування і його несумісність з телекомунікаційного устаткуванням інших фірм.

Для вирішення ситуації, що склалася, в 2003 році фірмами Nokia, Harris Corp., Ensemble і Crosspan був заснований некомерційний консорціум WiMAX Forum (Worldwide Interoperability for Microwave Access, Глобальна Сумісність для Мікрохвильового Доступу). Головним завданням консорціуму стало створення стандарту для технології безпровідного широкосмугового доступу з такою пропускною спроможністю, щоб сучасний користувач не відчував би різниці в порівнянні з будь-якою існуючою транспортною технологією. На сьогодні в консорціум WiMAX Forum входить 180 компаній-виробників сучасного телекомунікаційного телекомунікаційного устаткування.

Головним завданням WiMAX Forum можна визначити виконання тих же кроків, які були зроблені альянсом WiFi Alliance для технології IEEE 802.11 WLAN (Wireless Local Area Networks, Бездротові Локальні Мережі) :

- визначення і гармонізація стандартів;

- сертифікація взаємодії телекомунікаційного устаткування різних постачальників;

- просування технології WiMAX.

Сьогодні термін WiMAX став комерційним ім'ям стандарту IEEE 802.16 WMAN (Wireless Metropolitan Area Networks, Бездротові Міські Мережі Зв'язку).

Робочою групою IEEE 802.16 за стандартами широкосмугового доступу (BWA, Broadband Wireless Access), яка спочатку займалася розробкою технології WLL (Wireless Local Loop), до початку 2005 року були розроблені наступні стандарти серії 802.16:

- IEEE 802.16 або IEEE 802.16-2001 (схвалений в грудні 2001 року), був першим стандартом в області WMAN, а також був орієнтований на роботу в спектрі від 10 до 65 ГГц і, як наслідок, вимагав знаходження передавача і приймача в зоні видимості (LOS, Line of Sight), що є досить істотним недоліком.

- IEEE 802.16a (схвалений в січні 2003 року) став першим «завершеним» стандартом де було усунено більшість недоліків попереднього стандарту; також в нього було додано істотну кількість нових функціональних можливостей: зокрема, одним з головних кроків в порівнянні з попереднім стандартом, було пониження робочої частоти і, як наслідок, реалізація функціонування в зоні непрямої видимості (NLOS, Near Line of Sight).

- IEEE 802.16REVd або IEEE 802.16-2004 (схвалений в липні 2004 року), є виправленою версією стандарту 802.16a.

- IEEE 802.16e (передбачуваний час виходу – липень 2005 року, останній чорновий варіант стандарту за номером 5a був опублікований в грудні 2004 року). Цей стандарт буде розвитком ідей попередніх стандартів з фокусом на мобільності крайового користувача.

Таким чином, досягнення максимальних значень швидкості передачі даних понад 70 Мбіт/с при знаходженні телекомунікаційного устаткування користувача на відстані більше 15 км, враховуючи фізичний стан системи, на сьогодні не представляється можливим навіть при знаходженні в зоні прямої

видимості. Проте, оператори можуть досить гнучко настроювати системи WiMAX відповідно до своїх потреб.

Стандарт 802.16 забезпечує високий рівень конфіденційності і безпеки повідомлень, шифрування трафіку в межах усієї безпровідної мережі. Для шифрування даних в 802.16 використовується алгоритм DES (Data Enscryption Standart).

Алгоритм DES був розроблений для шифрування і дешифрування даних розрядністю 64 біт на основі 64-бітового ключа. Дешифрування виконується по тому ж ключу, що і шифрування.

Захист реалізований на MAC рівні. Аутентифікація використовує двоключову криптографію на основі цифрових сертифікатів X.509. Після аутентифікації робиться генерація і розподіл сесійних ключів шифрування. Ключі міняються з певною періодичністю, а також кожних 24 години пристрій проходить переаутентифікацію, підтверджуючи свою достовірність.

Використовується режим шифрування, заснований на лічильнику. Тобто схема найбільш близька до <ідеальному шифру>, оскільки кожен фрейм MAC рівня зашифровується на своєму унікальному ключі, який не повторюється. Окрім цього кожен фрейм містить імітовставку (свого роду контрольна сума), яка вираховується по алгоритму CMAC.

2.4.3 Уразливості захисту WiMAX, можливі шляхи їх подолання

До вразливостей відносяться:

- Атаки фізичного рівня, такі як глушення передачі сигналу, що ведуть до відмови доступу або лавинний наплив кадрів (flooding), що має на меті розрядити батарею станції. Ефективних способів протистояти таким загрозам немає.

- Незашифрована інформація, що передається по повітрю, може бути перехоплена будь-якою особою, у якої є приймач, налагоджений відповідним чином;

- Уразливість, пов'язана з не випадкової генерації базовою станцією ключів авторизації. Взаємна участь базової і абонентської станції, можливо, розв'язала б цю проблему;

- Проведення DoS-атак. Зареєстрований користувач може бути скомпрометований, а зловмисники можуть видавати себе зареєстрованими користувачами;

- Віруси і інші шкідливі програми. Існує загроза блокування інформації в каналі, яка є підготовчим етапом для атаки man, - in - the - middle, коли між клієнтом і точкою доступу з'являється третій пристрій, який перенаправляє трафік між ними через себе. В результаті виникає вже не лише загроза перехоплення інформації, але і її спотворення.

Обмін даними між легальними клієнтами і точкою доступу незначний або практично відсутній, зловмисник може змусити жертву генерувати велику кількість трафіку, при цьому, не знаючи секретного ключа. В результаті перехоплюючи правильний пакет, не розшифровувавши, досить ретранслювати його знову.

Актуальним засобом на сьогодні для проведення моніторингу мережі використовується програма CommView, яка є потужним інструментом, що включає мережевий аналізатор і декодер протоколів. З а допомогою CommView у користувачів є можливість бачити список мережевих з'єднань, IP -статистику і досліджувати окремі пакети. Пакети можна дешифрувати з використанням призначених для користувача WEP або WPAPSK ключів і декодувати аж до найнижчого рівня з повним аналізом поширених протоколів. Надається повний доступ до необроблених даних. Перехоплені пакети можуть бути збережені у файл для подальшого аналізу.

Необхідність аналізу мережевого трафіку може виникнути з кількох причин. Контроль безпеки комп'ютера, відладка роботи локальної мережі, контроль витікаючого трафіку для оптимізації роботи підключення, що розділяється, до Інтернету — з цими завданнями стикаються системні адміністратори, а також прості користувачі.

Для їх вирішення існує безліч утиліт, як спеціалізованих, спрямованих на рішення вузької області завдань, так і багатофункціональних «комбайнів», що надають користувачеві широкий вибір інструментів. Програми дозволяють наочно бачити повну картину трафіку, що проходить через комп'ютер або сегмент локальної мережі, дозволяє попереджати про наявність в трафіку підозрілих пакетів, появі в мережі вузлів з нештатними адресами або підвищенні мережевого навантаження.

2.4.4 Технічні параметри ZigBee IEEE 802.15.4

Для вирішення багатьох завдань не потрібно високу швидкість передачі інформації. Наприклад, для передачі текстових або числових даних, або для зв'язку комп'ютерів під час проведення інтерактивної гри не потрібно швидкість передачі зверху 250кбит/с., різні завдання автоматизації процесів і збору інформації вимагають не більше 20 кбит/с. Тут, в першу чергу, потрібно низьку вартість передавача, простоту, низьке споживання енергії. У зв'язку з цими вимогами був розроблений стандарт IEEE 802.15.4. Його розробником виступив альянс компаній (Invensys, Honeywell, Mitsubishi Electric, Motorola, Philips), що назвав себе ZigBee. Малося на увазі, що топологія мережі нагадуватиме траєкторію руху бджоли від квітки до квітки. Під такою ідентично назвою технологія ZigBee і набуває все більшого поширення.

Стандарт IEEE 802.15.4 (ZigBee) передбачає роботу в трьох діапазонах: один канал 868,0-868,6 Мгц (для Європи), 10 каналів в диапазопе 902-928 Мгц (крок центральних частот 2 Мгц, сама ниж-няя з них 906 Мгц) і 16 каналів в діапазоні 2400-2483,5 Мгц (таблиця. 2.3).

У радіоканалі використаний метод широкосмугової передачі з розширенням спектру прямою послідовністю (DSSS). Модуляція і розширення послідовності для діапазонів 868-915 і 2450 Мгц різні.

Таблиця 2.3 Частотні діапазони і швидкості передачі в мережах ZigBee

Частотний діапазон, Мгц	Чіпова швидкість, Кчип/с.	Модуляція	Бітова швидкість Кбит/с.	Швидкість символів Ксимв/с
868-868,6	300	BPSK	20	20
902-928	600	BPSK	40	40
2400-2483.5	2000	O - QPSK	250	62,5

У діапазоні 2450 Мгц потік модульованих цих розбивається па групи по чотири біти. Кожна група замінюється однією з 16 квазіортогональних послідовностей завдовжки 32 біт (чіпа). Послідовності приведені в стандарті. Модуляція даних – квадратурна фазова (QPSK). Парні чіпи квазіортогональної послідовності (починаючи з нульового) модулюють синфазний (I) канал, непарні -- квадратурний (Q) канал. В результаті послідовність в квадратурному каналі зміщена відносно синфазного на період одного чіпу, тому модуляція називається Offset - QPSK. Тривалість імпульсу після квадратурного модулятора удвічі більше, чим тривалість одного чіпа.

Для захисту інформації використовуються протоколи AES. Проте при експорті в країни Европи та Азії діє обмеження щодо довжини ключа. Ключ обмежується до 64 біт. За таких умов, передані внутрішні дані можуть бути розкриті із застосуванням потужних процесорних систем. Але час підбору ключів та вартість самої системи є прийнятними для реалізації такого втручання при необхідності. Тому запропонований протокол AES та його реалізація в ZigBee не надає потрібного рівня захисту даних.

Висновки до розділу

1. Забезпечення інформаційної безпеки безпровідної системи доступу є проблемою. Для її вирішення використовуються різні засоби, починаючи від категоричної заборони використання бездротового доступу в корпоративній системі (з організацією спеціальної служби радіомоніторингу і радіопротидії) до повного ігнорування цієї проблеми як такої в інших системах.

2. Для захисту безпровідних мереж доступу від вторгнень компанії виробники поставляють телекомунікаційне устаткування зі вбудованими або накладеними системами моніторингу. Системи моніторингу не лише ідентифікують атаку, але і визначають місце, звідки вона ведеться. Для бездротових систем, для захисту використовуються складні алгоритми криптографічного перетворення, але вони вимагають потужне енергоспроживання для своєї роботи.

3. Певний вплив на розвиток ринку безпровідного доступу роблять виробники шлюзів, що встановлюються між відкритою системою і корпоративною мережею, що захищається. Шлюз забезпечує аутентифікацію користувачів, шифрування даних і необхідну якість обслуговування трафіку, реалізує безпечний роумінг між підмережами.

4. Існуючі рішення щодо захисту інформації не дозволяють використовувати криптографічне перетворення з високим рівнем захисту, оскільки присутнє законодавче обмеження щодо довжини використаних ключів захисту. Запропонований протокол AES та його реалізація в модулях ZigBee не надає потрібного рівня захисту даних за існуючих обмежень.

РОЗДІЛ 3 ВИКОРИСТАННЯ КРИПТОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ В СИСТЕМАХ ТЕЛЕКОМУНІКАЦІЙ

3.1 Пристрої шифрування для захисту інформації в телекомунікаційних мережах

Для захисту інформації використовуються як звичайний блоковий пристрій криптографічного перетворення який реалізує функцію як прохідного так і потокового шифрування (ПШ).

ПШ реалізуються як окремий пристрій або інтегровані у повноцінний мережевий адаптер Ethernet. Тобто блок ПШ та мережевий адаптер виконані в виді однієї плати. Його перевага в тому, що він постійно контролює увесь обмін даними через мережу до пристрою, виявляючи закриптовані блоки, а обійти його напряму неможливо як з зовні, так і з внутрішній стороні. Але ПШ не замінює собою пристрої захисту від мережевих атак, якщо такі будуть мати місце.

Технічно ПШ є досить складними автономними пристроями, оскільки вони замість центрального процесора комп'ютера виконують операцію обробки даних на власних процесорних потужностях.

Ідея яка покладена в апаратну реалізацію ПШ – застосування двох процесорів: один з процесорів відповідає за криптографічну обробку даних, що відправляються через пристрій, а другий виявляє криптографічні дані та керує загальним потоком обміну на рівні фізичної моделі.

При необхідності, в пам’яті такого пристрою може зберігатись довільна кількість ключів, виходячи з їх довжин (64, 128 і до 2048 біт в залежності від алгоритмів), щоб кожен блок інформації був зашифрований із застосуванням свого власного алгоритму захисту, відмінному від інших, або відмінному за ключем. Це робить ключі захищеними від втручання, від зміни зловмисникам, але ускладнює процес управління ними. Інтеграція ключів в пристрій захищає ключі від копіювання.

Технічні труднощі впродовж певного часу не дозволяли розробляти надійні і швидкодіючі ПШ. Проте з появою на ринку дорогих, але дуже якісних мікросхем PLD, наприклад FLEX10K від Altera, вдалося вирішити багато проблем створення складних багатофункціональних пристроїв, що стимулювало випуск перших вітчизняних прохідних шифраторів.

3.2 Сучасні реалізація бездротової мережі на базі ZigBee модулів

зазвичай є готовими до застосування пристроями, здатними самостійно об'єднуватися у бездротові мережі з різною топологією, — точка-точка, зірка, MESH (комірчаста мережа). Підключений до мережі модуль забезпечує передачу даних на будь-який інший вузол мережі або на усі вузли одночасно. Передача даних здійснюється по інтерфейсу UART від зовнішнього хост-процессора, яким може виступати персональний комп'ютер або простий 8-розрядний мікроконтроллер вартістю менше $1. Завдяки ПО у ZigBee-модулі, усі операції по формуванню мережі, приєднанню нових пристроїв, прокладенню оптимальних маршрутів повідомлень виконуються в модулі, без участі зовнішнього мікроконтролера.

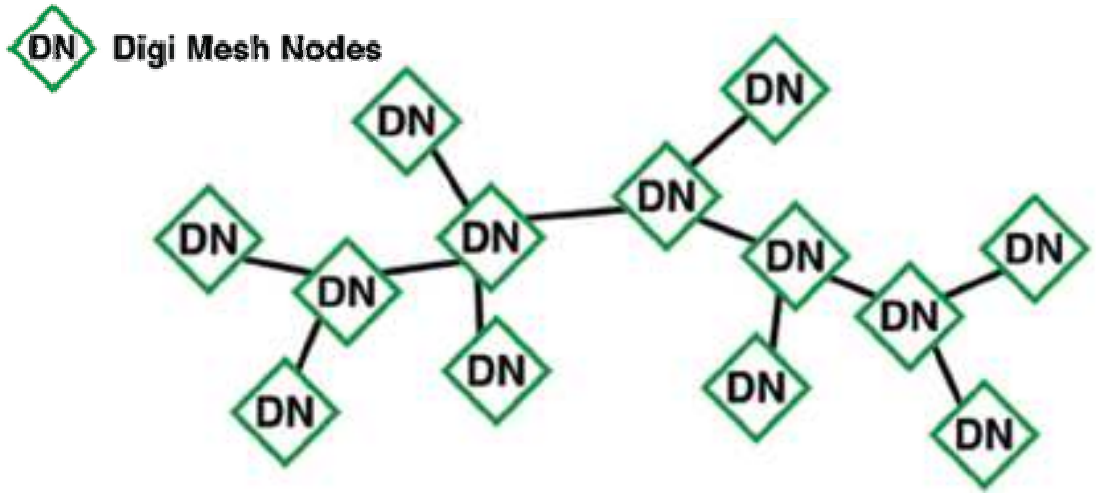

Рисунок 3.1 – Структура Mesh–мережі ZigBee

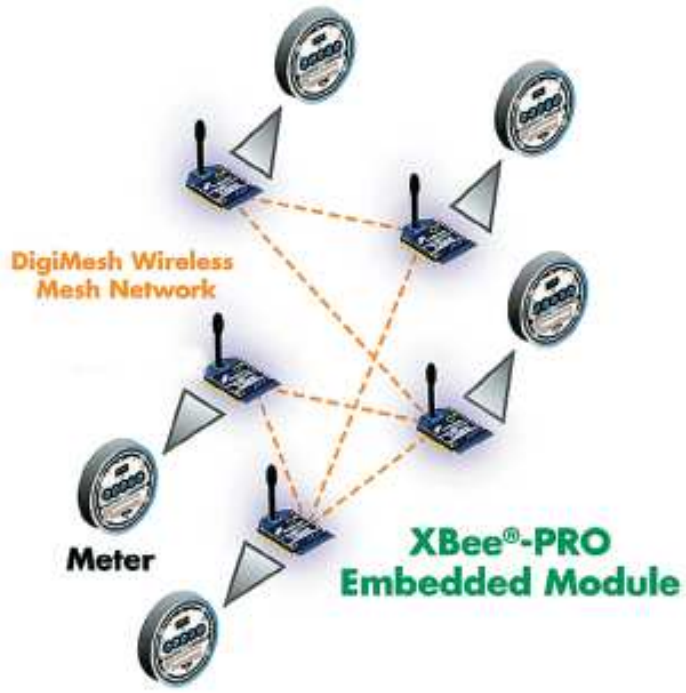

Рисунок 3.2 – Приклад ZigBee мережі на основі вузлів XBee від компанії Digi[1]

Зовнішній вигляд модулів показано на Рисунок 3.3.

Рисунок 3.3 – Зовнішній вигляд модулів XBee (https://www.digi.com)

[1] https://www.digi.com/products/embedded-systems/digi-xbee/rf-modules

Основні параметри модулів:

- розмір 13 х 19 мм;
- підтримка протоколів Zigbee, 802.15.4, DigiMesh® and BLE;
- вбудований контролер з підтримкою MicroPython;
- підтримка підключення до Bluetooth® Low Energy, Bluetooth сенсорів;
- підтримка IoT безпеки – програмна безпека поверх шару передачі інформації в пристрої IoT.

3.3 Математичне забезпечення криптозахисту для пристроїв Інтернету речей

Інтернет речей (IoT) існує менше 15 років, але розвивається з величезною швидкістю. Одночасно з нововведеннями виникають серйозні проблеми, що пов'язані з інформаційною безпекою. Алгоритми, на яких заснована сучасна криптографія занадто складні та використовують багато ресурсів, а їх використання є складним завданням для малопотужних процесів Інтернету речей [44, 45, 49].

Так компанія Hewlett Packard провела дослідження, та в 2015 році виявила, що 70 % пристроїв IoT мають вразливості у безпеці своїх паролів, існують проблеми з шифруванням даних і з дозволом доступу і багато що інше. Так IOT дав поштовх для розвитку нової гілки криптографії – Low Weight Cryptography, LWC.

На сьогодні є близько 50 низкоресурсних алгоритмів, але в більшості, вони абсолютно непридатні для використання. Розробники часто не мають змоги обрати алгоритм і чи зможе він працювати на певному пристрої. На Рисунок 3.4 показано деякі алгоритми та їх застосування.

SPONGENT	176-bit, на основі AES	алгоритми хешування	**Симетричні шифри**
PHOTON	64-bit, на основі AES		
LESAMNTA - LW	128-bit, на основі AES		
PRESENT	80, 128-bit	алгоритми блокового шифрування	
SPECK	64-256-bit		
CLEFIA	128-bit		
TRIVIUM	64-128-bit	алгоритм потокового шифрування	
Еліптичні криві	128-bit	алгоритм потокового шифрування	**Асиметричний шифр**

Рисунок 3.4 – Light Weight Cryptography (LWC) алгоритми (частина) [38, 43, 44, 47, 49]

У асиметричній криптографії використовуються наступні операції алгебри і алгоритми [4, 36]:

- алгоритми перевірки числа на простоту;
- операції алгебри над великими числами: модульне множення, модульне піднесення до степеня, знаходження залишку від ділення, обчислення зворотного числа по модулю.

Найбільш трудомісткими операціями в асиметричній криптографії є операції модульного множення великих чисел і модульного піднесення до степеня великих чисел.

Слід зазначити, що модульне піднесення до степеня складається з ітераційної послідовності модульних множень. Якщо врахувати, що піднесення до степеня в криптографічних алгоритмах застосовується як безпосередньо, так і побічно (перевірка на простоту, обчислення зворотного

числа по модулю та ін.), то стає очевидним, що головним завданням, яке необхідно реалізувати в арифметичному співпроцесорі являється апаратне модульне множення великих чисел [47]:

$$M = a\ b \pmod{n} \tag{3.1}$$

де a, b - множники;

M – добуток;

n - модуль (просте число);

$a, b, M < n$; усі величини - великі позитивні цілі числа.

У основі операцій лежить необхідність знаходження залишку від ділення результату операції на модуль. При використанні великих чисел операція ділення є найбільш трудомісткою і вимагає найбільшого часу виконання. Особливо складною вона стає для процесорних систем малої потужності. Тому, постановкою завдання є реалізація ефективних алгоритмів виконання операції модульного множення без використанні операції ділення.

На сьогодні розроблені декілька ефективних алгоритмів модульного множення великих чисел, що виключають необхідність операції ділення. Найбільш популярними з них є:

- алгоритм Баррета [4, 36];
- алгоритм Монтгомери [4, 36].

Виходячи з приведеного аналізу, можна зробити висновок, що сам по собі алгоритм модульного множення Баррета великої трудомісткості не представляє і цілком міг би бути реалізований апаратно. Проте, ефективність алгоритму Баррета повністю залежить від того, наскільки ефективно будуть виконані попередні обчислення. У останньому випадку це константа μ, яка має бути вичислена діленням великих чисел (3). Якщо прийняти, що в течії багатократного використання криптографічного алгоритму модуль N буде незмінний, тоді константу можна обчислювати усього один раз і тимчасові

витрати на її обчислення (тобто на виконання алгоритму ділення) на загальному фоні будуть незначні.

Алгоритм Монтгомери [4, 36] є множенням двох чисел по модулю третього непарного числа без операції ділення. Алгоритм заснований на так званій «редукції Монтгомери» :

$$M = Mon\Pr o(A, B, N) = A\,B\,r^{-1} (\mathrm{mod}\ N), \qquad (3.2)$$

де $Mon\Pr o(A, B, N)$ - операція редукції Монтгомери;

A, B - множники;

r^{-1} - додатковий множник;

N - непарний модуль.

Як видно з (3.2) в точності повторює шукану формулу (1), за винятком паразитного множника r^{-1}, виконання операції *MonPro*, що з'являється в результаті. Ця величина є зворотним числом r по модулю N таким, що [4, 36]:

$$r^{-1} r \equiv 1 \ (\mathrm{mod}\ N)$$

де $r = 2n$, n - довжина модуля N у бітах.

Для того, щоб позбавитися від цього множника, множені числа заздалегідь необхідно привести до виду «представлення Монтгомери» [4, 36]:

$$A\ (A\,r\ (mod\ N), B\ (B\,r\ (mod\ N) \qquad (3.3)$$

Тоді, відповідно до (3.3) буде отримано [4, 36]:

$$\begin{aligned} &MonPro(Ar, Br, N) = Ar\ Br\ r^{-1} (mod\ N) = \\ &= ABr2r^{-1} (mod\ N) = ABr\ (mod\ N) \end{aligned} \qquad (3.4)$$

і відповідно до (3.1) можна вважати, що

$$MonPro(Ar, Br, N) = ABr \pmod N = Mr \pmod N.$$

Той факт, що результат операції *MonPro()* дорівнює *Mr* а не *M* є зручний, оскільки при необхідності багатократного перемножування, кожен результат множення необхідно передавати у функцію *MonPro* як аргумент, для чого відповідно до (3.2) *M* необхідно переводити в представлення Монтгомері [4, 36]:

$$M \ (Mr \ (mod \ N)).$$

На практиці, обчислення робляться над числами з базисом [4, 36]:

$$d = 2k \tag{3.5}$$

де *k* - розрядність одного слова обчислювальної системи.

Тоді, алгоритм множення Монтгомері для обчислення $\mathrm{MonPro(Ar, Br, N)} = \mathrm{Mr} \pmod{\mathrm{N}}$, узагальнено можна виразити таким чином: k - розрядність одного слова у бітах, m - довжина модуля N в словах (по k біт в кожному) [1, 4].

Великі числа зберігаються у вигляді масивів слів. Аргументи A, B приведені до виду представлення Монтгомери (3.3).

Крок 1. Прийняти $X = 0,\ \mathrm{d} = 2\mathrm{k}$

Крок 2. Прийняти $\mathrm{i}=0$.

Крок 3. Вичислити $\mathrm{q(d - n0) - 1} \pmod{\mathrm{d}}$.

Крок 4. Вичислити $\mathrm{X = (X + ai\,B + q\,N) / d}$.

Крок 5. Якщо $\mathrm{i < m}$, прийняти $\mathrm{i = i + 1}$ і перейти на крок 4.

Крок 6. Якщо $\mathrm{X \geq N}$ вичислити X = X - N.

Крок 7. Видати результат «Mr (mod N) = X». Кінець алгоритму.

Проаналізуємо алгоритм з точки зору його апаратної реалізації.

На кроці 3 обчислюється проміжне значення q з трьох складових:

- складова $\left(x_0 + a_i\, b_0\right)$ обчислюється легко, оскільки обчислення робляться над однослівними величинами;

- складова $\left(d - n_0\right) - 1$ є однослівне число, зворотна величина N по модулю d, її обчислення особливої трудомісткості не представляє. Ця величина не міняється на усіх ітераціях, а значить її можна вичислити один раз на початкових кроках алгоритму. Більше того, якщо модуль N все ще є незмінним (а це так для більшості операцій криптографічного алгоритму), цю величину доцільно вичислити одноразово і зберігати як константу на всьому протязі «життя» модуля N;

- відповідно до (7), складова $\left(\mathrm{mod}\, d\right)$ говорить про те, що результат перемножування перших двох складових просто відсікається до розміру одного слова. У зв'язку з цим, першу складову доцільно обчислювати також на рівні одного слова, без урахування перенесень в операціях множення і складання.

Таким чином, алгоритм Монтгомері [4, 36] дозволяє робити модульне множення двох великих чисел, без необхідності застосування трудомісткої операції ділення на модуль.

По закінченню множення, якщо необхідно, результат $Mr\ \left(mod\ N\right)$ можна легко привести до виду $M\ \left(mod\ N\right)$, знову використовуючи редукцію Монтгомері, задаючи одиницю в якості одного з аргументів [1, 4]:

$$MonPro\left(1,\, Mr,\, N\right) = Mr\ r^{-1}\left(mod\ N\right) = M \quad (8)$$

Алгоритм множення Монтгомері застосовується у більшості розробників імплементацій криптопротоколів. для ефективного застосування

такого множення, необхідно вирішити, яким чином приводити великі множники до виду представлення Монтгомері.

3.4 Алгоритм обчислення еліптичних кривих

Математичний апарат обчислення еліптичних кривих над кінцевими полями використовуються для побудови різноманітних криптографічних систем, а також реалізації їх в криптографічних протоколів. В той же час апарат теорії обчислення еліптичних кривих над кінцевими полями виявляється продуктивним при створенні і реалізації алгоритмів генерації псевдовипадкових чисел.

Еліптичну криву E над певним полем F можна визначити як безліч пар точок $(x, y) \in F^2$, що задовольняють рівнянню [1, 4, 40]:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in F\ . \qquad (3.6)$$

На безлічі $E(F)$, що складається з точок еліптичної кривої і ще одного елементу – нескінченно видаленої точки кривої O, можна визначити операцію, що має властивості операції абелевої групи. Групу, що виходить, розглядають як адитивну групу, операцію називають операцією складання і означають знаком плюс. Нескінченно видалена точка кривої О виконує роль нейтрального елементу (нуля) групи [1, 4].

Еліптичні криві можуть використовуватися для отримання псевдовипадкових послідовностей на основі вже відомих генераторів (алгоритмів). До таких генераторів відносяться лінійний конгруентний генератор і його модифікації, BBS-генератор, регістр зсуву і інші.

Так, в роботі [5] розглядаються лінійні рекурентні послідовності на еліптичних кривих. У статтях [2] і [8] розглядаються моделі побудови псевдовипадкових послідовностей на основі лінійних рекурент на еліптичній кривій. Слід зазначити публікацію [7], у якій описується алгоритм побудови псевдовипадкових послідовностей на еліптичних кривих на основі

генератора «Вихор Мерсена». Дослідниками розробляються і інші варіації генераторів, зокрема з використанням ізоморфних трансформацій кривої [3] чи нейронних мереж [7].

Наведемо приклад алгоритму генерації послідовностей на еліптичній кривій на основі конгруентного або інверсивного генераторів, запропонований в [4]. Згідно з цим алгоритмом необхідно [4]:

– вибрати кінцеве поле $GF(q)$;

– вибрати криву E;

– вибрати генератор. Наприклад, лінійний конгруентний генератор, заданий рівнянням $X_{i+1} = cX_i + P$ або інверсивний генератор з рівнянням $X_{i+1} = c(X_i)^{-1} + P$;

– вибрати фіксоване ціле число, початкову точку X_0 і фіксовану точку P, причому $cX_0 + P \neq X_0$.

– вичислити послідовність станів генератора X_0, X_1, X_2, використовуючи формулу $X_{i+1} = cX_i + P$ або формулу $X_{i+1} = c(X_i)^{-1} + P$.

У цій же роботі [4] приведений алгоритм формування псевдовипадкової послідовності над еліптичною кривою на основі регістрів зрушення з лінійними зворотними зв'язками.

Тому еліптичні криві частіше знаходять використання у криптографії. Причиною такого стану речей є те, що еліптичні криві над скінченними полями створюють скінченні групи значень, але які, навіть за великої кількості елементів, легко піддаються арифметичним операціям завдяки визначеній структурі даних [4].

Наразі в криптографії найбільше всього використовували значення з мультиплікативними групами над скінченними полями. А за своїми властивостями, поля значень за виразами для еліптичних кривих нагадують мультиплікативними групи, і їхня перевага полягає в тому, що має місце великий вибір значень формул еліптичної кривої, ніж у скінченного поля.

А для того щоб зламати криптографічну систему на основі еліптичних кривих [4] потрібно вирішити зворотну проблему визначення дискретного логарифма для еліптичних кривих. Ця задача є складною обчислювальною задачею, що вимагає великий обсяг часу.

Розглянемо означення еліптичної кривої [38, 40, 41].

Означення 1 Нехай K – певне кільце з характеристикою $K \neq 2, 3$, і нехай є рівняння $x^3 + ax + b$ (де $a, b \in K$) є поліномом третього степеня без кратних коренів. Тоді *еліптичною кривою над кільцем K* називають сукупність точок (*x, y*), де елементи $x, y \in K$ та одночасно задовольняють рівняння [38]:

$$y^2 = x^3 + ax + b \tag{3.7}$$

разом з елементом О, який називається – '*точкою на нескінченності*'.

Також використовується загальний вигляд рівняння еліптичних кривих над довільним кільцем [38]:

$$y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_5x + a_6 \tag{3.8}$$

яке в кільці K характеристики $\neq 2$ можна записати у вигляді $y^2 = x^3 + ax^2 + bx + c$ (або $y^2 = x^3 + ax + b$, коли характеристика > 3).

Перепишемо попередні рівняння у вигляді $F(x, y) = 0$. В цьому випадку $F(x, y)$ буде мати вигляд [38]:

$$F(x, y) = y^2 - x^3 - ax - b$$

або

$$F(x,y) = y^2 - x^3 - ax^2 - bx - c$$

і т.д. Тоді точка, яка лежить на еліптичній кривій, називають *неособливою*, якщо щонайменше одна з часткових похідних $\frac{\partial F}{\partial x}$, $\frac{\partial F}{\partial y}$ у цій точці набуває значення, яке відмінне від нуля.

Твердження про те, що багаточлени в правих частинах рівнянь (3.8) не мають кратних коренів визначає те, що кожна точка кривої повинна бути неособливою, тобто,наприклад, виконується умова [38, 43, 44, 47, 49]:

$$4a^3 + 27b^2 = 0. \qquad (3.9)$$

За будь-яких нових чисел $a\,i\,b$ ми отримуємо рівняння іншої еліптичної кривої. Якщо виконується умова (3.8), то еліптична крива, описана базовим рівнянням $y^2 = x^3 + ax + b$ створює групу чисел.

Така група еліптичних кривих над полем дійсних чисел складається з сукупності точок, що відповідають позиції еліптичній кривій. Еліптичні криві, визначені над полем дійсних чисел та над полем Z_{23}, зображені на Рисунок 3.5,3.6., відповідно.

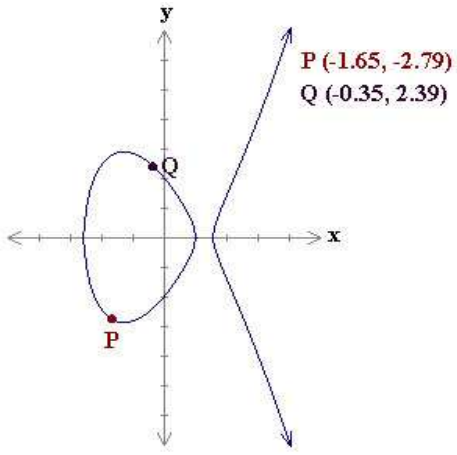

Рисунок 3.5. $y^2 = x^3 - 5x + 4$

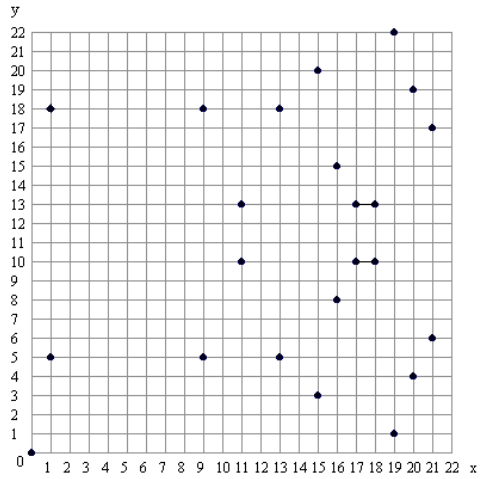

Рисунок 3.6.
$y^2 \pmod n = x^3 + x \pmod n, n = 23$

Відомо також правило додавання двох точок на еліптичній кривій [38], результатом додавання яких є нова – третя точка на тій же самій кривій. Щодо операції додавання, то множина всіх точок цієї еліптичної кривої разом з точкою O утворює групу, де точка O відіграє роль нейтрального елемента відносно додавання. Саме з використанням цієї групи будуються криптосистеми на основі еліптичних кривих.

Означення [38]. Нехай $P=(x_1,y_1)$, $Q=(x_2,y_2)$ – дві різні точки на еліптичній кривій E (тут ми будемо розглядати еліптичні криві над полем дійсних чисел). Суму P і Q позначимо як точку $R=(x_3,y_3)$, визначену так. Спочатку побудуємо пряму, що проходить через точки P і Q. Вона перетне криву в третій точці; R буде симетричним відображенням цієї точки відносно осі абсцис. Геометрично це зображено на Рисунок 3.7.

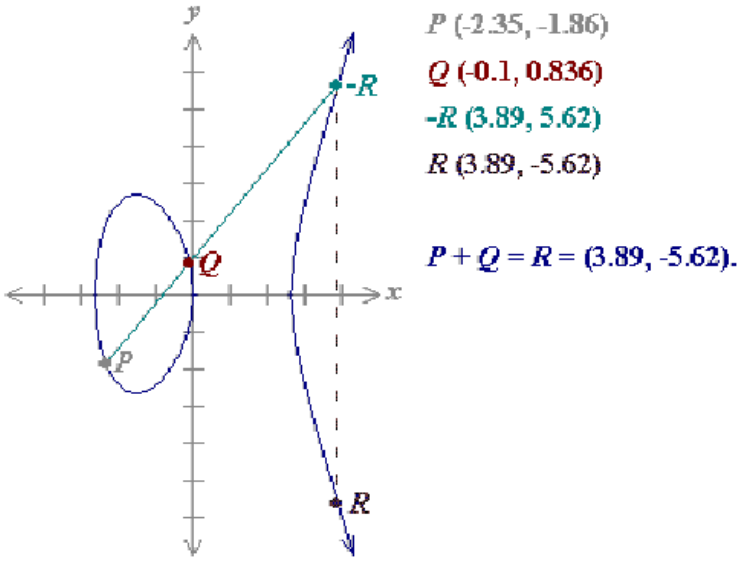

Рисунок 3.7 – Зразок додавання двох точок кривої для рівняння $y^2=x^3-7x$

Формально операція додавання визначається так:

1) $P+O=O+P=P$ для всіх $P\in E$ (E – еліптична крива);

2) якщо $P=(x,y)\in E$, тоді $(x,y)+(x,-y)=O$. (Точку $(x,-y)$ позначають як "-P" і називають протилежною до точки "P". Встановлено, що -P також належить заданій еліптичній кривій)*;*

3) нехай $P=(x_1,y_1)$, $Q=(x_2,y_2)\in E$, де $P\neq -Q$. Тоді $P+Q=(x_3,y_3)$, де

$$x_3=\lambda^2-x_1-x_2$$

$$y_3=\lambda(x_1-x_3)-y_1$$

$$\lambda=(y_2-y_1)/(x_2-x_1),\ \text{якщо } P\neq Q$$

$$\lambda=(3x_1^{\,2}+a)/(2y_1),\ \text{якщо } P=Q$$

У випадку поля Zn всі ці операції будуть виконуватися за модулем *n*.

Можна довести [38, 43], що визначена операція ‘+’ має властивість комутативності, що є ознакою абелевої групи. Я і у випадку довільних абелевих груп, через nP позначаємо точку *P*, додану *n* разів, якщо *n* – додатне, та точку -*P*, додану $|n|$ разів, якщо *n*-від'ємне. Отже, піднесення точки *P* до *n*-го степеня в Zn^* еквівалентне множенню *P* на *n*.

Зазначимо, що для швидшого обчислення nP не обов’язково додавати ту саму точку *P* *n* разів, а можна використати *метод ітераційного подвоювання*. Наприклад у випадку, коли $(b_k b_{k-1}\ldots b_1 b_0)$ – двійкове зображення, то тоді $nP=b_0P+2(b_1P+2(b_2P+\ldots+2b_k)\ldots)$. Зокрема для обчислення $100P$ потрібно врахувати, що $100=1100100_2$ і далі:

$$100P=2(2(P+2(2(2(P+2P)))))).$$

Тобто для отримання $100P$ ми виконуємо всього вісім операцій: шість подвоєнь та два додавання точок кривої.

Цей метод дає змогу значно пришвидшити процедуру виконання арифметичних операцій над еліптичними кривими. Можна довести, що обчислення *kP* (де *P* – точка на еліптичній кривій над полем *Zn*) здійснюється за допомогою $O(\log k \log^3 n)$ операцій.

Означення. Порядком *n* точки *P*, що належить еліптичній кривій, називають найменше натуральне число, таке що $nP = O$.

Звичайно таке число може і не існувати, однак для криптографії дуже важливо відшукання точки на кривій скінченного порядку.

Нехай ми маємо скінченне поле F_q, що містить $q = p^r$ елементів.

Означення. Порядком еліптичної кривої, що визначена над довільним скінченним полем F_q, називають число, що відповідає кількості точок кривої, яке позначають $\#E\left(F_q\right)$.

Потрібно зауважити, що еліптична крива *E* може мати щонайменше $2q+1$ точку: точка на нескінченності та $2q$ пар $(x, y) \in F_q$, що задовольняють рівняння (1). Крім того, для кожного значення *x* існує щонайменше два значення *y*, що в парі з *x* задовольняють рівняння (3.6). Та, оскільки лише половина ненульових елементів поля F_q мають корені квадратні, то ми могли б сподіватися, що кількість точок на кривій є у двічі меншою.

3.5 Аналіз арифметичних операцій сучасної криптографії і способи їх апаратної реалізації

Процес розробки апаратних або апаратно-програмних засобів криптографічного захисту інформації на основі сучасних асиметричних криптографічних алгоритмів, у тому числі і національних асиметричних криптографічних алгоритмів [36], безпосередньо пов'язаний з необхідністю реалізації арифметичних операцій, що лежать в основі алгоритмів. Так, один з закордонних стандартів республіки Узбекистан DST 1092:2009 базується на

числах розмірністю не менше 256 біт, що в десятковому уявленні складає ≈ 10^{77} (сімдесят сім десяткових цифр) [37].

Ряд таких операцій пов'язаний з обробкою відносно великих об'ємів інформації, що веде до необхідності вибору елементної бази з підвищеною продуктивністю.

В той же час, застосування високопродуктивних елементів, що мають обчислювальні можливості, такі як микропроцесори і мікроконтроллери (далі - процесори) накладають деякі істотні обмеження, що перешкоджають їх використання в конкретних розробках. До таких обмежень, зокрема відносяться:

- великі габарити, що робить неможливим їх застосування в малогабаритних і переносних пристроях;

- велике споживання електроенергії, що знижує ефективність їх використання в пристроях з батарейним живленням;

- велика кількість виводів: більшість високопродуктивних процесорів мають кількість виводів від 300 і вище, що призводить до небажаних ускладнень схемотехнік проектованих пристроїв. Крім того, конструктивне розташування виводів в сучасних корпусах спричиняє за собою необхідність в дорогому спеціалізованому устаткуванні, що унеможливлює широкий розвиток розробок такого роду (як правило, усі процесори з числом виводів ≥ 200 випускаються в корпусах з кульковими виводами BGA);

- неоптимізована система команд під конкретне завдання: ефективність програмного коду (а значить і швидкість виконання програми) безпосередньо залежить від фіксованої системи команд конкретного процесора;

- обмежена розрядність даних : сучасні процесори мають фіксовану розрядність даних (8, 16 або 32 розряди), що призводить до збільшення програмного коду при виконанні криптографічних операцій, і як наслідок - до зниження продуктивності пристрою в цілому;

- лінійність програмного коду : в процесорах відсутні можливості незалежного і паралельного виконання декількох трудомістких операцій одночасно;

- висока вартість, яка росте пропорційно збільшенню продуктивності.

Виходячи з вищезгаданого, можна зробити висновок, що використання високопродуктивних процесорів для виконання криптографічних операцій в апаратних засобах частенько малоефективно і недоцільно.

Одним із способів підвищення ефективності виконання криптографічних операцій в апаратних засобах є їх побудова за принципом «ведучий - ведений». Спосіб припускає використання процесора загального призначення як центрального керівника модуля пристрою («ведучий»), і спеціалізований арифметичний співпроцесор («ведений»), що виконує усі трудомісткі операції під управлінням ведучого.

3.6 Визначення швидкодії системи

Будь-якому користувачеві систем криптозахисту потрібно, щоб програмне забезпечення не відбивалася на зручності роботи програмного забезпечення та роботі. Але виконання циклу криптографічного перетворення даних віднімає деякий час, причому раніше доводилося просто чекати, коли закінчиться шифрування, наприклад, локального диска.

Потокова швидкість обробки даних – це один з основних параметрів, по яких оцінюють реалізації криптографічного перетворення даних. Швидкість змінюється в мегабайтах в секунду і залежить передусім від складності алгоритму шифрування. Найпростіше оцінити швидкість по формулі [22]:

$$V = \frac{F \cdot K}{n},$$

де F - тактова частота;

K - розмір блоку, що підлягає криптографічному перетворенню;

n - число тактів, що вимагається на виконання циклу перетворення цього блоку.

Або за більш зручною формулою:

$$V = \frac{D_R + D_W + D_{CR}}{T_{CLK}},$$

де D_R – обсяг даних, що зчитується;

D_W – обсяг даних, що записується;

D_{CR} – обсяг даних, що обробляється за один такт криптографічного перетворення;

T_{CLK} – час одного такту криптографічного перетворення.

Наприклад, такий відомий алгоритм як ГОСТ 28147-89 (або просто "ГОСТ") має швидкодію 32 такти на 8-байтовий блок для криптографічного процесору, тобто теоретична швидкість криптографічного перетворення повинна сягнути 270 Мбайт/с при тактовій частоті в 1000 Мгц. Проте реальна швидкість апаратної реалізації алгоритму – 8-9 Мбайт/с. Обмеження є чисто технологічним: через відсутність необхідного рівня розробок або елементної бази.

Програмна реалізація криптографічного перетворення при тактовій частоті процесора в 1 ГГц досягає до 18 Мбайт/с. Хоча в цьому випадку апаратна швидкість шифрування теоретично могла сягнути близько 240 Мбайт/с, що близьке до теоретичної межі.

Висновки до розділу

1. Для шифрування інформації в мережах використовуються програмні та апаратні засоби захисту інформації. Існуючі обмеження по розміру ключа не дозволяють використовувати схеми шифрування з високою стійкістю до взлому.

2. Розглянуто стандарти малопотужних безпровідних мереж. Найбільш перспективним є стандарт IEEE 802.15.4-2006 для ZigBee. Існуючі на ринку рішення дають змогу реалізовувати мережу ZigBee на основі автономних модулів, що виконують всі операції зі з’єдання між собою.

3. Показано, що найбільш ефективними є асиметричні алгоритми, оскільки забезпечується максимальна надійність шифрування. Показано, що алгоритм шифрування на основі еліптичних кривих володіє здатністю шифрування ключем 128 біт та є оптимізованим до математичних операцій обрахунку чисел з великим ступенем.

РОЗДІЛ 4 МОДЕЛЮВАННЯ АЛГОРИТМУ ЕЛІПТИЧНИХ КРИВИХ ТА ЗАГАЛЬНОЇ ШВИДКОДІЇ СИСТЕМИ

4.1 Визначення порядку моделювання

За допомогою еліптичних кривих можна зашифрувати довільну інформацію. Для цього використовуються такі дії як шифрування блоку так і шифрування потоку. Для задачі моделювання найбільш зручним є застосування процесу «гамування».

Процес "гамування" у накладанні на поток вхідних даних певного випадкового потоку. Для розшифрування потрібно виконати зворотню дію – повторно накласти ідентичну послідовність випадкового потоку.

Ступінь захисту вихідної інформації буде залежати від кількості можливих значень, що досягає потік випадкових значень. В нашому випадку, процес гамування полягає в накладанні точок еліптичної кривої, що відповідають гаммі, з тими, що відповідають символам алфавіту точками еліптичної кривої. Для виконання операції гамування використовується операція "виключне АБО" (таблиця 4.1).

Таблиця 4.1 – Гамування

Вхідні дані	Ключ	Результат	Повторний ключ	Результат
Накладання гамми шифру				
0	**0**	0	**0**	0
0	**1**	0	**1**	0
1	**0**	1	**0**	1
1	**1**	0	**1**	1
Приклад гамування з різними ключами				
0	**1**	0	**0**	0
1	**0**	1	**1**	0

Для того, щоб реалізувати алгоритм стохастичного шифрування і "гамування", використовуючи абелевую групу точок еліптичної кривої [38, 43, 44], застосовується наступний алгоритм:

1. За допомогою генератора псевдовипадкових чисел (ГПВЧ) генератора псевдовипадкової послідовності № 1 з ключем k_1 для кожного сеансу зв'язку створюється новий алфавіт з перевіркою кожного символу на унікальність, якому відповідає деяка точка, що належить еліптичній кривій.

2. Поблочно прочитуються з файлу початкові дані, що підлягають шифруванню.

3. У алфавіті, який попередньо згенеровано, визначаються порядкові номери символів блоку початкових даних.

3.1 Задається кількість випадкових символів, за допомогою яких буде додано в блок з початковими даними.

3.2 За допомогою ГПВЧ №2 з ключем k_2 генеруються випадкові символи і визначаються порядкові номери цих символів в алфавіті.

3.3 Створюється одновимірний цілочисельний масив, при цьому його довжина дорівнює кількості лічених символів блоку початкових даних разом з кількістю згенерованих випадкових символів. Порядкові номери цих символів в алфавіті записуються в масив. Скориставшись ГПВЧ №3 з ключем k_3, стохастично перемішуються елементи цього масиву.

4. Алфавіт, згенерований в пункті 1, записується в двомірний масив.

5. За допомогою ГПВЧ № 4 з ключем k_4 здійснюються циклічні зрушення рядків і стовпців двомірного масиву, отриманого в попередньому пункті, тим самим відбувається стохастичне перемішування алфавіту для кожного шифрованого символу.

6. Прочитується порядковий номер чергового шифрованого символу з одновимірного масиву, отриманого в пункті 3.3, і здійснюється заміна цього номера на відповідний порядковий номер з перемішаного в пункті 5 алфавіту, у такий спосіб відбувається стохастична заміна кожного символу.

7. Шифрування, засноване на еліптичній кривій, робиться таким чином:

7.1 Визначаємо генеруючу точку *G* еліптичної кривої.

7.2 Генеруємо випадкове число *k.*

7.3 В якості відкритого ключа користувач вибирає довільну точку *Рв* еліптичної кривої, а секретним ключем вибирає деяке число *пв*. Рівняння має вигляд:

$$cm = \{\mathrm{k} - \mathrm{G},\ \mathrm{Pm} + \mathrm{k} - \mathrm{PB}\}$$

де *Pm* точка еліптичної кривої, що відповідає шифрованому символу.

8. Прочитується з ключового файлу черговий символ «гамми».

9. Точки еліптичної кривої, що відповідають символу початкових даних і символу «гамми», складаються за алгоритмом викоючного АБО.

10. Результат шифрування записується у файл.

У цій системі шифрування секретним ключем є символи «гамми» і ключі генераторів ПСП.

Відновлення даних відбувається у зворотному порядку таким чином:

1. З відповідних файлів прочитується черговий символ зашифрованої інформації і символ гамми.

2. Знаходиться різниця точок еліптичної кривої, що відповідають символу зашифрованої інформації і символу гамми.

3. Застосовується наступні рівняння:

$$Pm + \mathrm{k} - \mathrm{PB} - \mathrm{nB} - (\mathrm{k} - \mathrm{G}) = \mathrm{PB} + \mathrm{k} - (\mathrm{nB} - \mathrm{G}) - \mathrm{nB} - (\mathrm{k} - \mathrm{G})$$

4. Після того, як вийшли розшифровані координати точок еліптичної кривої, визначаються порядкові номери символів, що відповідають цим координатам, тобто символів заміни, що записуються в одновимірний масив.

5. Для визначення порядкових номерів символів початкової інформації і випадкових символів здійснюються зворотні циклічні зрушення рядків і

стовпців двомірного масиву, в якому міститься алфавіт. Порядковий номер в алфавіті чергового зашифрованого символу прочитується з одновимірного масиву, отриманого в пункті 4, і здійснюється його заміна на відповідний порядковий номер з алфавіту в двомірному масиві. Отримані таким чином порядкові номери символів записуються в одновимірний масив.

6. За допомогою ГПВЧ №3 з ключем k_3 відкидаються випадкові символи в одновимірному масиві з пункту 5, і таким чином відновлюється первинний порядок початкових символів.

Дамо оцінку обчислювальній стійкості запропонованого алгоритму стохастичного шифрування та гамування з використанням абелевой групи точок еліптичної кривої.

Для кожного сеансу зв'язку був згенерований алфавіт, який містить 144 символи і включає рядкові і прописні букви кирилиці і латинського алфавіту, а також розділові знаки і інші необхідні символи. Наприклад, якщо модуль, по якому робляться обчислення, рівний p=751, то число точок на цій еліптичній кривій складає n=727.

Загальну кількість різних алфавітів можна знайти по формулі для числа розміщень

$$A_n^m = \frac{n!}{(n-m)!}.$$

Так як n=727, а m=144, то $A_{727}^{144} \approx 10^{405}$.

Будь-який символ алфавіту може бути замінений на якій-небудь інший, оскільки використання циклічних зрушень рядків і стовпців двомірного масиву, в якому записаний згенерований алфавіт, визначає стохастичне перемішування елементів цього масиву.

4.2 Моделювання обрахунку значень еліптичних кривих

На Рисунок4.1 наведений приклад пошуку точок кривою над полем $GF(29)$, заданою рівнянням $y = x^3 + 4x + 4$, за допомогою конгруентного генератора, рівняння якого має вигляд :

$$X_{i+1} = 11X_i + P,$$

де $P(2,7)$.

В якості початкової точки вибрана точка $X_0 = (0,2)$.

Крива виду: $y^2 = x^3 + 4x + 4$

X1 = 11X0 + P = 11(0;2) + (2,7) = (2,7) + (2,7) = (5;2)
X2 = 11X1 + P = 11(5;2) + (2,7) = (23,24) + (2,7) = (28;12)
X3 = 11X2 + P = 11(28;12) + (2,7) = (0,2) + (2,7) = (26;20)
X4 = 11X3 + P = 11(26;20) + (2,7) = (1,26) + (2,7) = (10;0)
X5 = 11X4 + P = 11(10;0) + (2,7) = (10;0) + (2,7) = (1;3)
X6 = 11X5 + P = 11(1;3) + (2,7) = (5;27) + (2,7) = (2;22)
X7 = 11X6 + P = 11(2;22) + (2,7) = (13;7) + (2,7) = (14;22)
X8 = 11X7 + P = 11(14;22) + (2,7) = (26;20) + (2,7) = (24;27)
X9 = 11X8 + P = 11(24;27) + (2,7) = (28;12) + (2,7) = (5;27)
X10 = 11X9 + P = 11(5;27) + (2,7) = (23;5) + (2,7) = (24;2)
X11 = 11X9 + P = 11(24;2) + (2,7) = (28;17) + (2,7) = (23;5)
X12 = 11X10 + P = 11(23;5) + (2,7) = (11;4) + (2,7) = (0;2)

Рисунок 4.1 – Пошук точок послідовності на основі лінійного конгруентного генератора

На Рисунок 4.2 наведений приклад пошуку точок кривою над полем $GF(13)$, заданою рівнянням $y = x^3 + 11x + 8$, за допомогою инверсивного генератора, рівняння якого має вигляд :

$$X_{i+1} = 9(X_i)^{-1} + P,$$

де $P(7,5)$.

В якості початкової точки вибрана точка $X_0 = (2,5)$.

На закінчення відмітимо, що реалізовані алгоритми побудови послідовностей точок еліптичних кривих можуть послужити основою для практичної імплементації алгоритмів.

Крива виду: $y = x^3 + 11x + 8$

```
X1 = 9(X0)^(-1) + P = 9(2;5)^(-1) + (7;5)= 9(2;8) + (7;5)=(2;8) + (7;5)= (8;6)
X2 = 9(X1)^(-1) + P = 9(8;6)^(-1) + (7;5) = 9(8;7) + (7;5)= (4;8) + (7;5)= (3;4)
X3 = 9(X2)^ (-1) + P = (3;4)^(-1) + (7;5)= 9(3;9) + (7;5)= (12;3) + (7;5)= (3;9)
X4 = 9(X3)^ (-1) + P = (3;9)^(-1) + (7;5) = 9(3;4) + (7;5)= (12;10) + (7;5)= (8;7)
X5 = 9(X4)^ (-1) + P = (8;7)^(-1) + (7;5) = 9(8;6) + (7;5)= (4;5) + (7;5)= (2;8)
X6 = 9(X5)^ (-1) + P = (2;8)^(-1) + (7;5) = 9(2;5) + (7;5)= (2;5) + (7;5)= (4;8)
X7 = 9(X6)^ (-1) + P = (4;8)^(-1) + (7;5) = 9(4;5) + (7;5)= (8;6) + (7;5)= (12;3)
X8 = 9(X7)^ (-1) + P = (12;3)^(-1) + (7;5) = 9(12;10) + (7;5)= (3;4) + (7;5)= (12;10)
X9 = 9(X8)^ (-1) + P = (12;10)^(-1) + (7;5) = 9(12;3) + (7;5)= (3;9) + (7;5)= (4;5)
X10 = 9(X9)^ (-1) + P = (4;5)^(-1) + (7;5) = 9(4;8) + (7;5)= (8;7) + (7;5)= (2;5)
```

Рисунок 4.2 – Пошук точок послідовності
на основі инверсивного генератора

Наприклад, для створення генераторів ускладнення послідовностей, що виходять, з метою проходження послідовностями тестів, перевіряючих властивості випадковості, виявлення характеристик еліптичних кривих і генераторів, що дозволяють отримувати послідовності, вживані в криптографічних застосуваннях.

4.3 Ефективна швидкість передачі даних

У стандарті 802.15.4 для частот в діапазоні 2,4 ГГц визначена максимальна швидкість передачі 250 Кбит/с.

На практиці вона виявляється менше із-за додаткових службових полів, включених в кожен передаваний пакет. У стандарті визначений алгоритм доступу до середовища передачі даних CSMA/CA.

Розрахуємо час, витрачений на підготовку до передачі даних :

а) Кожного разу, коли пристрій передає дані, воно чекає випадковий проміжок часу з діапазону $[0,2^{BE}-1]$, після чого визначає зайнятість каналу (CCA). Якщо канал вільний, пристрій передає дані, інакше воно знову

чекає випадковий проміжок часу. Зазвичай показник BE встановлюється рівним 3, тому в самому гіршому випадку час, витрачений на підготовку до передачі, буде рівне:

$$InitialBackOffPeriod + CCA = (2^3 - 1) \cdot aUnitBackOffPeriod + CCA =$$
$$= 7 \cdot 0,32 + 0,128 = 2,368 \text{ мс}$$

Час CCA дорівнює 8 символьним періодам, час aUnitBackOffPeriod дорівнює 20 символьним періодам, один символьний період дорівнює 16 мкс.

Тепер розглянемо необхідний час на передачу даних :

б) Згідно із стандартом 802.15.4 максимальний розмір корисного навантаження фрейма рівний [12]:

$$aMaxMACFrameSize = aMaxPHYPacketSize - aMaxFrameOverhead,$$

де $aMaxFrameOverhead = 25$,

$aMaxPHYPacketSize = 127$.

Як видно, розмір корисної частини залежить від довжини службових полів. Пізніша версія стандарту 802.15.4b дозволяє збільшити корисне навантаження фрейма, коли використовуються короткі адреси (16 біт замість 64). В цьому випадку об'єм даних дорівнюватиме 114 байтам.

Таким чином, час передачі даних складе [12]:

$$\frac{(aMaxPHYPacketSize + SHR + PHR) \cdot 8}{250 \cdot 10^3} = \frac{(127 + 5 + 1) \cdot 8}{250 \cdot 10^3} = 4,256 \text{ мс}$$

в) Після відправки пакету даних необхідно відправити кадр підтвердження. Кадр підтвердження прийому даних складається з 11 байт. Якщо прийняти швидкість на вході рівної 250 Кбіт/с, то передача займе час в

0,352 мс. Слід зазначити, що при передачі підтверджень не використовується алгоритм вирішення конфліктів CSMA - CA.

Перед відправкою підтвердження є затримка в 192 мкс, пов'язана з тим, що пристрій повинен перейти з режиму прийому в режим передачі. Крім того, щоб дати пристроям досить часу на обробку прийнятих даних, в стандарті визначені мінімальні затримки, які слідують після кадру підтвердження :

- для кадрів завдовжки до 18 байт включно - 18 символьних періодів.
- для кадрів завдовжки більше 18 байт - 40 символьних періодів. Як правило, ці затримки охоплюються при підготовці до передачі чергового кадру даних.

Використовуючи приведені вище розрахунки, визначимо ефективну швидкість передачі за стандартом 802.15.4 [12]:

Таблиця 4.2. Часові втрати

Дія	**Час (у мс)**
CSMA/CA	2,368 мс
Передача кадру	4,256 мс
Затримка після передачі	0,192 мс
Передача підтвердження	0,352 мс
Загальний час (T_Σ)	7,168 мс

Таким чином, загальний час передачі інформаційного пакету з корисною інформацією в 63 байт складає 7,168 мс.

Пізніша версія стандарту 802.15.4b дозволяє збільшити корисне навантаження фрейма, коли використовуються короткі адреси (16 біт замість 64). В цьому випадку об'єм даних дорівнюватиме 114 байтам. В такому випадку економиться час передачі, проте зростає обсяг корисних даних.

Виконаємо визначення обчислювальної складності.

Фізичний час для обрахунку алфавітів визначається як:

$$T_A(n) = \frac{n \cdot \tau_b + n^2 \cdot \tau_k}{f_{CPU}}, \text{ секунд,}$$

де n – розмірність очикуваного алфавіту;

τ_b – операційна складність обрахунку одної букви алфавіту;

τ_k – кількість операцій для виконання математичної операцій пошуку;

f_{CPU} – швидкодія процесора.

Таблиця 4.3 – Операційні витрати на обрахунок одної математичної операції, для 32 бітного блоку даних

Тип процесора	τ_b, такти	τ_k ,такти	f_{CPU}, МГц
	Ключ 32 біта		
8-біт, AVR RISC	24	140	24
32-біт, ARM RISC	7	42	200
	Ключ 64 біта		
8-біт, AVR RISC	180	2270	24
32-біт, ARM RISC	33	320	200

Результат моделювання T_A для опрацювання розміру блока від 32 до 256 байт показано на Рисунок 4.3, 4.4

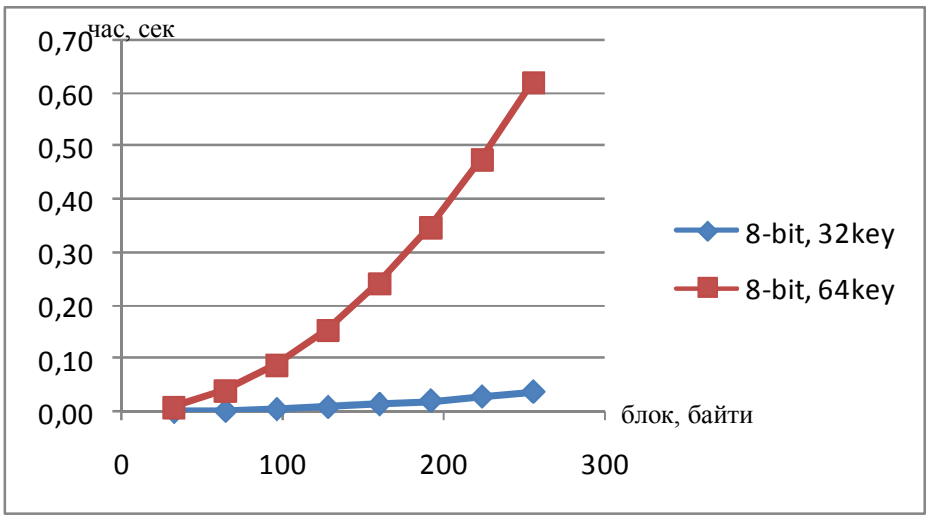

Рисунок 4.3 – Обчисленння алфавітів для 8-бітного контролера

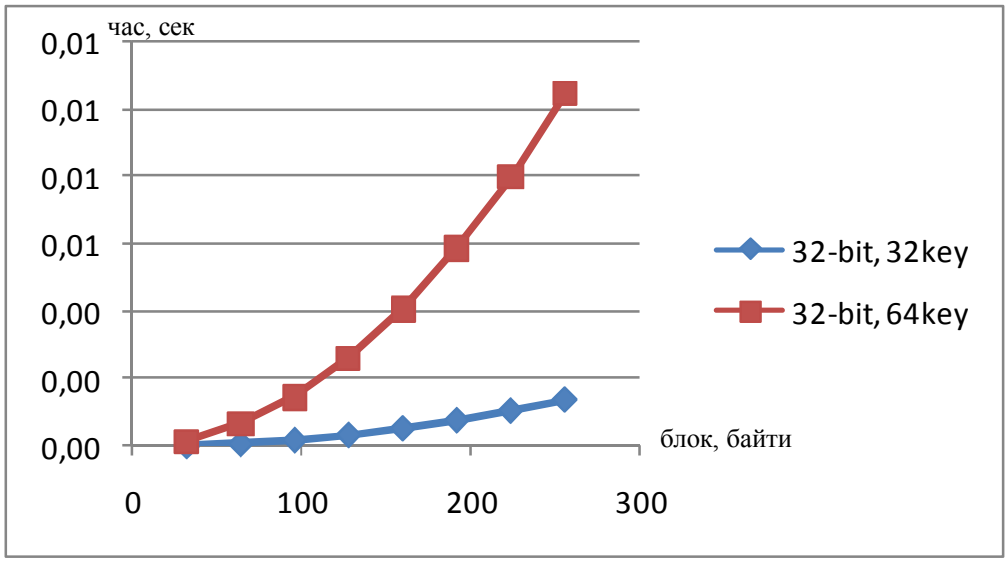

Рисунок 4.4 – Обчисленння алфавітів для 32-бітного контролера

Як видно з рисунків 4.3, 4.4 для 8-бітного контролера, час обрахунку одного значення алфавіту для 8-бітних контролерів є суттєвим значенням.

Отже, як було встановлено, загальний час (T_Σ) на передачу інформаційного блоку складає 7,168 мс. Визначимо вихідну швидкість передачі інформації, що виникає при операції шифрування алгоритмом елемтичних кривих, прийнявши, що виконується тільки операція шифрування без операції дешифрування в проміжному вузлі.

В загальному видно, що застосування 32 бітної архітектури дозволяє отримати більш ніж 70 разову перевагу.

Таким чином, з таблиці видно, що тільки для 8 бітного контролера з ключем в 64 біти не досягається можливість обробки блоків за 1 секунду.

Враховуючи, що модулі ZigBee часто працюють в режимі інтервальної передачі даних, як то передача в інтервалі хвилин або навіть годин, то в такому випадку, встановлено, що 8-бітний контролер забезпечить роботу з шифрування та передачі її на основний модуль.

Таблиця 4.3 – шифрування та підготовка даних для передачі згідно стандартів 802.15.4b та 802.15.4a

Розмір блоку шифрування, біти	Час на 1 байт	802.15.4b		802.15.4a	
		Час підготовки блоку, 63 байт	Кількість блоків за 1 сек	Час підготовки блоку, 127 байт	Кількість блоків за 1 сек
	8 бітний контролер, ключ 32 біти				
32	0,00033	0,020808	48,05733	0,041947	23,83946
64	0,001318	0,083012	12,04643	0,167342	5,975787
96	0,002962	0,186611	5,35874	0,376184	2,658272
128	0,005264	0,331605	3,015635	0,668474	1,495945
160	0,008222	0,517994	1,930523	1,044211	**0,957661**
192	0,011838	0,745779	1,34088	1,503396	**0,665161**
224	0,01611	1,014959	0,985262	2,046028	**0,488752**
256	0,02104	1,325533	0,754413	2,672107	**0,374236**
	8 бітний контролер, ключ 64 біти				
32	0,00534	0,336428	2,972401	0,678197	1,474498
64	0,021334	1,34405	0,74402	2,709435	**0,369081**
96	0,047982	3,022866	0,330812	6,093714	**0,164104**
128	0,085284	5,372875	0,18612	10,83103	**0,092327**
160	0,133239	8,394078	0,119132	16,9214	**0,059097**
192	0,191849	12,08647	0,082737	24,3648	**0,041043**
224	0,261112	16,45006	0,06079	33,16124	**0,030156**
256	0,341029	21,48485	0,046544	43,31073	**0,023089**
	32 бітний контролер, ключ 32 біти				
32	1,19E-05	0,000749	1335,123	0,00151	662,3053
64	4,74E-05	0,002988	334,6478	0,006024	166,0064
96	0,000107	0,006718	148,8613	0,013542	73,84456
128	0,000189	0,011937	83,77075	0,024064	41,55557
160	0,000296	0,018647	53,62723	0,03759	26,60248
192	0,000426	0,026847	37,24759	0,054121	18,47715
224	0,00058	0,036538	27,36897	0,073655	13,57673
256	0,000757	0,047718	20,95631	0,096194	10,39565

Розмір блоку шифрування, біти	Час на 1 байт	802.15.4b		802.15.4a	
		Час підготовки блоку, 63 байт	Кількість блоків за 1 сек	Час підготовки блоку, 127 байт	Кількість блоків за 1 сек
	32 бітний контролер, ключ 64 біти				
32	9,04E-05	0,005695	175,5818	0,011481	87,09963
64	0,000361	0,022745	43,96607	0,045851	21,80994
96	0,000812	0,051148	19,55096	0,103109	9,698507
128	0,001443	0,090906	11,00036	0,183255	5,456874
160	0,002254	0,142018	7,041367	0,28629	3,492962
192	0,003246	0,204484	4,890363	0,412213	2,425928
224	0,004418	0,278304	3,593196	0,561025	1,782451
256	0,005769	0,363478	2,751199	0,732725	1,364768

4.4 Розрахунок енергоспоживання і часу роботи сенсорних мереж

Енергоспоживання - одне з ключових питань для сенсорних мереж, оскільки пристрої живляться в основному від батарей.

Інформація про споживання енергії в різних режимах узята з технічного опису компанії Digi, що виробляє готові модулі за стандартом 802.15.4.

Таблиця 4.4 – Енергоспоживання модулі за стандартом 802.15.4 фірми Digi

Режим	**Споживання струму, мА**
Активний	10
Режим сну	0,003
Передача	125
Прийом	40

Таблиця 4.4 показує, що сенсор у базовому (активному) режимі споживає приблизно в декілька тисяч разів більше енергії, ніж в режимі сну. Відправка повідомлень збільшує енергоспоживання в порівнянні з базовим режимом. Цілком природно, що співвідношення між показниками може відрізнятися для різних виробників. Але у будь-якому випадку очевидне те, що сплячий режим вимагає найменшої кількості енергії.

Час активності пристрою за один раз складає 16мс.

Час в 3мс витрачається на передачу зібраних даних і стільки ж витрачається на їх прийом. Час підготовки до передачі даних складає приблизно 2мс. Таким чином, один цикл складає 24мс.

Тепер необхідно розрахувати скільки разів в секунду буде пристрій працювати в активному режимі, в режимі прийому і в режимі передачі :

$$\frac{1000}{24} = 41\,(\text{пакет/с})\,.$$

Час, що залишився, 16мс пристрій збиратиме дані для передачі.

У стандарті 802.15.4 вказана максимальна швидкість передачі даних 250 Кбит/с. Реальна швидкість, яка була розрахована вище, дещо менше, оскільки кадри мають певний формат, що включає адреси приймача і передавача і деякі інші поля. Зробимо розрахунок для обох швидкостей.

Мікроконтроллер може занурюватися в режим сну при якому струм споживання є мінімальним. Цей режим застосовується в сенсорах для тривалішого терміну служби батареї, а, отже, і великим часом роботи пристрою, проте, в нашому випадку, пристрій не може переходити в режим сну при роботі на прийом, передачу і при формуванні даних. Тому розрахунки робитимуться виходячи з цих трьох режимів.

Розрахуємо середнє споживання струму за час t = 1с. Воно буде рівне:

$$I_{\text{ср}} = \frac{41\left(0{,}016 \cdot 10 + 0{,}003 \cdot 125 + 0{,}003 \cdot 45 + 0{,}002 \cdot 12\right) \times 10^{-3}}{1} = 28{,}454 \text{ (мА).}$$

Припустимо, для живлення сенсорної плати використовуються LiOn батарея. Місткість батареї приблизно дорівнює 6000 мАч. Тоді пристрій працюватиме протягом:

$$t_p = \frac{6000}{28{,}454} = 210{,}86 \text{ годин або 8 діб.}$$

Таким чином, пристрій забезпечить беззупинну передачу інформації протягом 8 діб. Неважко помітити, що основна енергія витрачається при передачі даних. У випадку, якщо пристрій працює тільки на прийом, а інший час знаходиться в стані накопичення, обробки даних, то час може сягати:

$$t_p = \frac{6000}{(40 \cdot 7{,}16 \cdot 10^{-3}) + (0{,}003 \cdot 10^{-3} \cdot (1 - 7{,}16 \cdot 10^{-3}))} = 20949{,}5 \text{ годин, або 2,39 роки.}$$

Якщо порівняти час роботи цього облаштування з часом роботи аналогів, то неважко помітити, що воно значно перевищує його, і тому система, побудована з таких пристроїв, може стати конкурентоздатному на ринку радіозв'язку.

Обрахунок потужності, що необхідна для роботи процесора криптографічної обробки слід виконувати у прив’язці до робочих умов.

Висновки до розділу

1. Метод еліптичних кривих використовується для криптографічного перетворення дозволяє виконувати операції гамування та шифрування блоків. При цьому, як було показано вище, однією з складних операцій є операція генерування алфавіту, що буде використовуватись для операції гамування.

2. Існуючі 8- та 32-бітні контролери цілком здатні виконувати операцію шифрування блоків за методом еліптичної криптографії. Встановлено, що збільшення розрядності процесора дозволяє суттєво збільшити обчислювальну потужність, а отже і зменшити витрати часу та енергії для обрахунку.

3. Застосування методу еліптичної криптографії для передачі через модулі стандарту ZigBee є не оптимальною при передачі шифрованих блоків даних через нерівність розміру блоку даних для методу еліптичної криптографії (32, 64, 96, 128 і так далі) та для модулів ZigBee – 117 байтів для IEEE 802.15.4b та 63 байти для IEEE 802.15.4a. В такому випадку потрібно виконувати вирівнювання шляхом додавання додаткового обсягу байтів, що не несуть навантаження, та передавати додаткові блоки даних. Метод еліптичної криптографії натомість зручно використовувати для генерування псевдовипадкової послідовності для операції гамування.

ВИСНОВКИ

1. Визначені проблеми застосування криптографічних процесів у цілому та в ракурсі забезпечення надійності від втручання третьою стороною зокрема. Показано як прості алгоритми, симетричні, так і сучасні алгоритми – асиметричні.

2. Встановлено, що більшість нових алгоритмів базується на основі симетричного алгоритму AES. Визначено, що асиметричні алгоритми є найбільш надійними, оскільки вони забезпечують захист інформації, шляхом використання публічного ключа для шифрування, а приватного ключа для дешифрування інформації. В такому випадку, при втручанні в пристрій передачі, приватний ключ все ще є захищеним, оскільки в самому пристрої не зберігається.

3. Розглянуто алгоритми шифрування в розрізі застосування для обчислювальних систем малої обчислювальної потужності. Представлено порівняння математичного базису. Для асиметричних алгоритмів відносять різні моделі, але для легковісних алгоритмів відносяться алгоритми на основі роботи з модульною арифметикою. Складність виконання цих обчислень і обумовлює складність підтримки асиметричних протоколів в системах обмеженої потужності. Один з таких алгоритмів є алгоритм на основі еліптичних кривих. Цей алгоритм характеризується зменшеною обчислювальною потужністю.

4. Виходячи із специфікацій цього стандарту була емпірично обраховано часові показники, що показують витрати на сам процес передачі інформації (на прикладі стандартів 802.15.4a та 802.15.4b), визначена ефективна швидкість передачі даних при застосуванні алгоритму шифрування за допомогою гамування в програмі для 8- та 32-бітного контролера загального призначення. Виконано обрахунок для 32 та 64 бітного ключа для блоків від 32 до 256 байт. Показано, що навіть 8-бітний контролер здатний забезпечити шифрування. Проте особливістю є те, що розмір блоку шифрування не співпадає з блоками даних, що передається

через модулі ZigBee. Також розраховано теоретичне споживання струму і час роботи пристроїв при заявленій швидкості передачі даних.

ПЕРЕЛІК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Бабенко, М.Г. Генератор псевдослучайных чисел на эллиптической кривой / М.Г. Бабенко // Информационное противодействие угрозам терроризма. – 2010. – № 14. – С. 182–187.

2. Бабенко, М.Г. Разработка генератора псевдослучайных чисел на точках эллиптической кривой / М.Г. Бабенко, Н.Н. Вершкова, Н.Н. Кучеров, В.А. Кучуков // Инженерный вестник Дона. – 2012. – № 4–2(23). – С. 68.

3. Бессалов, А.В. Метод генерации псевдослучайных последовательностей на основе изоморфных трансформаций эллиптической кривой // А.В. Бессалов, В.Е. Чевардин // Прикладная радиоэлектроника. – 2012. – Т. 11. – № 2. – С. 234–237.

4. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов, И.В. Чугунков. – Москва: НИЯУ МИФИ, 2012. – 400 с.

5. Тараканов, В.Е. Линейные рекуррентные последовательности на эллиптических кривых и их применение в криптографии / В.Е. Тараканов // Труды по дискретной математике. – 2006. – Т. 9. – С. 340–356.

6. Фролов А.Б. Элементарное введение в эллиптическую криптографию. Книга 1. Алгебраические и алгоритмические основы / А.Б. Фролов, С.Б. Гашков. – М.: Едиториал УРСС, 2019. – 376 с.

7. Червяков, Н.И. Реализация ЕС-последовательностей на точках эллиптической кривой с использованием нейронных сетей / Н.И. Червяков, М.Г. Бабенко, А.С. Назаров, И.С. Крисина // Высокопроизводительные параллельные вычисления на кластерных системах. Материалы XIII Всероссийской конференции (Н. Новгород, 14–16 ноября 2013 г.) – Нижний Новгород: Изд-во Нижегородского госуниверситета. – 2013. – С. 274–278.

8. Червяков, Н.И. Линейные рекуррентные последовательности на эллиптической кривой / Н.И. Червяков, М.Г. Бабенко // Научно-технические ведомости СПбГТУ. – 2010. – № 2. – С. 164–166.

9. Сердюков П.Н. Защищенные радиосистемы цифровой передачи информации / П.Н. Сердюков, А.В. Бельчиков, А.Е. Дронов и др. – М.: АСТ, 2006. – 403 с.

10. Баушев С.В., Передрий А.В. Разработка перспективных систем связи вооруженных сил США и объединенных вооруженных сил НАТО // Зарубежная электроника. – 2002. - №4.

11. Котельников В.А. Теория потенциальной помехоустойчивости. – М.: Госэнергоиздат, 1956. – 151с.

12. Семенов Ю.В. Проектирование сетей связи следующего поколения. – М.: ОАО «ГИПРОСВЯЗЬ», 2005. – 240 с.

13. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: ЮНИОР, 2003. – 504 с.

14. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. – М.: Горячая линия-Телеком, 2005. – 416 с.

15. Шеннон К. Теория связи в секретных системах / К. Шеннон // Работы по теории информации и кибернетике. – М.: Изд. иностр. лит., 1963. – С.333-369.

16. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. – М.: Техносфера, 2005. – 592 с.

17. Сюваткин В.С., Есипенко В.И., Ковалев И.П., Сухоребров В.Г. WiMAX технология беспроводной связи: теоретические основы, стандарты, применение. – Сн. Пб.: БХВ-Перербург, 2005. – 268 с.

18. Заключний звіт по науково-дослідній роботі №08-02 «Розробка макету пристрою цифрової обробки складних сигналів» Рег. № 0108U010273.

19. Шокало В.М. Концепция создания отечественных специальных цифровых систем передачи информации / В.М. Шокало, А.И. Цопа // Науково-технічний журнал «Захист інформації». – Київ: ДУІКТ, 2006. – Вип. №3. – С. 51-57.

20. Стрельницкий А.А. Волновые каналы архитектурных сооружений. Усовершенствованная модель и новый эксперимент / А.А. Стрельницкий, А.Е. Стрельницкий, А.И. Цопа, В.М. Шокало // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2007. – Выпуск №151. – С. 158-163.

21. Стрельницкий А.А. Экспериментальные исследования волновых каналов архитектурных сооружений при функционировании системы WiMAX в условиях города / А.А. Стрельницкий, А.Е. Стрельницкий, А.И. Цопа, В.М. Шокало // Научно-технический журнал «Прикладная радиоэлектроника». – Харьков: ХНУРЭ, 2008. – Том 7. - №1. – С. 77-84.

22. Цопа А.И. Способы повышения и качественной оценки качества передачи видеоинформации по беспроводным каналам связи / Стрельницкий А.А, Цопа А.И., Шокало В.М. // Вісник Національного університету «Львівська політехніка». Радіоелектроніка та телекомунікації. – Львів, 2008. – Випуск № 618.– С. 168-173.

23. Цопа А.И. Критерии оценки и пути повышения защищенности каналов связи цифровых систем передачи информации на физическом уровне // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2010 – Выпуск №161. – С. 87-96.

24. Стрельницкий А.Е. Вариант повышения помехозащищенности радиоканала фиксированной связи WiMAX / А.А. Стрельницкий, А.И. Цопа, В.М. Шокало // Труды 8-й Международной научно-практической конференции «Современные информационные технологии» /СИЭТ’2007/. – Одесса, 2007. – С. 173.

25. Цопа А.И. Пути повышения защищенности каналов связи цифровых систем передачи информации на физическом уровне / А.А. Дудка, А.В. Стрельницкий, А.А. Стрельницкий, А.И. Цопа, В.М. Шокало // Сборник тезисов докладов 20 Международной Крымской конференции «СВЧ-техника и телекоммуникационные технологии» /CriMiCo’2010/. Пленарный доклад. – Севастополь: СевНТУ, 2010. – Том.1. – С. 28-31.

26. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования.— М.: ФОРУМ: ИНФРА-М, 2004.

27. Крысин А.В. Информационная безопасность. Практическое руководство. — М.: СПАРРК, К.:ВЕК+,2003.

28. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение — М.: СОЛОН-Пресс, 2004.

29. Лукашов И. В. Криптография? Железно! //Журнал «Мир ПК». 2003. № 3.

30. Панасенко С.П., Защита информации в компьютерных сетях // Журнал «Мир ПК» 2002 № 2.

31. Бунин О. Занимательное шифрование // Журнал «Мир ПК» 2003 №7.

32. Панасенко С. П., Ракитин В.В. Аппаратные шифраторы // Журнал «Мир ПК». 2002. № 8.

33. Панасенко С. П. Чтобы понять язык криптографов // Журнал «Мир ПК». 2002. № 5.

34. Панасенко С. П. Чтобы понять язык криптографов // Журнал «Мир ПК». 2002. № 6 .

35. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.., Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. - М.: КомКнига, 2006. – 324 с.

36. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003. — 325 с.

37. Бабаш А. В., Шанкин Г. П. Криптография (аспекты защиты). — М.: СОЛОН-ПРЕСС, 2007. – 512 с.

38. Чмора А. Л. Современная прикладная криптография. – М.: “Гелиос АРВ”, 2001. – 256 с.

39. ГОСТ 34.10-2018. Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Дата введения 2019-06-01

40. Теория эллиптической криптографии [Электронный ресурс] // криптография, информационная безопасность. 09.08.2013. URL: https://habrahabr.ru/post/188958/

41. Болотов А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы / А.А. Болотов, С. Б. Гашков, А. Б. Фролов. – М.: КомКнига, 2006. – С. 89 – 98.

42. Болотов А.А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. – М.: КомКнига, 2006. – С. 9 – 90.

43. Соловьев Ю.П. Эллиптические кривые и современные алгоритмы теории чисел / Ю. П. Соловьев, В. А. Садовничий, Е.Т. Шавгулидзе. – М.: Ижевск, 2003. – С. 60 – 92.

44. Ростовцев А.Г. Алгебраические основы криптографии / А. Г. Ростовцев. – СПб.: Мир и семья, Интерлайн, 2000. – С. 112 – 220.

45. Хоффман Л.Дж. Современные методы защиты информации / Л. Д. Хоффман. – М.: Советское радио, 1980. – С. 87 – 164 с.

46. Montgomery P.L. Speeding the Pollard and Elliptic Curve Methods of Factorization / P. L. Montgomery. – Mathematics of computation. 1987. – P. 243 – 264.

47. Lopez J. Fast multiplication on elliptic curves over GF(2n) without precomputation / J. Lopez, R. Dahab. – Lecture Notes in Computer Science. 2000. № 1965. – P. 317 – 327.

48. Claus H. Frobenius manifolds: quantum cohomology and singularities / H. Claus. – University Manheim. 2004 – P. 146 – 178.

49. Шнейер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С / Б. Шнейер – М.: Триумф, 2002. – С. 12 – 216 с.

50. Omura J., Massey J. Computational method and apparatus for finite field arithmetic. / J. Omura, J. Massey. – U. S. Patent No. 4587627, 1986.

Дипломна робота

магістра із спеціальності 172 Телекомунікації та радіотехніка

тема роботи: **МЕТОД КРИПТОГРАФІЧНОГО ЗАХИСТУ ВУЗЛІВ МЕРЕЖІ ZIGBEE**

Студент: **Супрунюк Ярослав Вікторович, гр. ТРм-19-2**

Керівник **к.т.н., доц. Горященко Костянтин Леонідович**

Мета роботи: **вирішення задачі підвищення криптографічної безпеки передачі інформації між мережі вузлами ZigBee із застосуванням алгоритму еліптичних кривих**

Об’єкт дослідження **бездротова мережа ZigBee на основі мікропроцесорних систем з обмеженою обчислювальною потужністю**

Предмет дослідження **методи криптографічного захисту передачі інформації бездротовими каналами зв'язку**

ЗАДАЧІ ДОСЛІДЖЕННЯ

1. Розглянути питання щодо запроваджених криптографічних методів у бездротових телекомунікаційних системах.

2. Визначити перспективні алгоритми криптографічного захисту інформації, що передаються між вузлами такої мережі.

3. Розглянути алгоритми, що використовуються для систем із малою обчислювальною потужністю в ракурсі застосування для обчислювальних систем малої обчислювальної потужності.

4. Виконати моделювання параметрів модулів передачі із застосуванням криптографічного захисту інформації для модулів мережі ZigBee.

Науково-практичне значення отриманих результатів

1. На основі проведених досліджень, представлено оцінку апаратної складності криптографічного перетворення на основі методу еліптичних кривих із застосуванням 8-бітних та 32-бітних контролерів. Розрахована кількість часових витрат на роботу, а також оцінено можлива швидкість генерування пакетів даних для передачі в мережі ZigBee.

КЛАСИФІКАЦІЯ БЕЗДРОТОВИХ СИСТЕМ

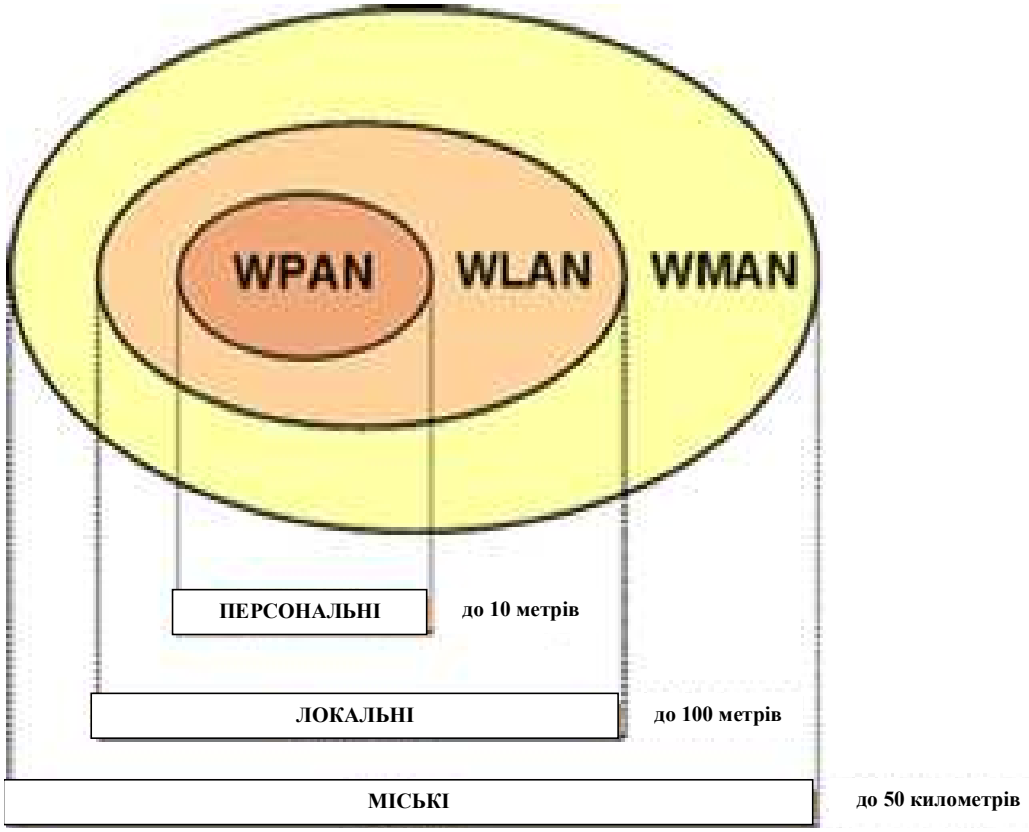

Рисунок 3.1 – Класифікація бездротових технології в залежності від дальності дії

1) **WPAN** – бездротова мережа, що охоплює невелику частину території, невелику швидкість передачі інформації, а також передача інформації відбувається лише між декількома пристроями. Прикладом такої технології є Bluetooth, ZigBee

2) **WLAN –** бездротова мережа, що охоплює середню за розміром ділянку (відстанню до 100 метрів), в залежності від використання стандарту передачі та частоти розміщення, швидкість передачі може сягати до 3,4 Гбіт/с. Прикладом такої технології є Wi-Fi

3) **WMAN –** бездротова мережа, що охоплює велику територію (область покриття до 50 кілометрів). В залежності від використання стандарту, швидкість передачі може варіюватись, максимальним значенням є 1 Гбіт/с. Прикладом такої технології є WiMax

МІСЦЕ КРИПТОГРАФІЇ ЯК ІНСТРУМЕНТУ ЗАХИСТУ ІНФОРМАЦІЇ

Рисунок 4.1 – Загальна структурна схема передачі інформації із застосуванням криптографії

Взаємодію між відправником і отримувачем з урахуванням криптографічної системи описується наступним чином:

1) Відправник отримує з джерела генерування ключів, ключ, яким буде зашифрована інформація;
2) Відправник зашифровує за допомогою ключа необхідну для передачі інформацію, та передає криптограму Е відкритими каналами зв’язку в напрямку до одержувача;
3) Отримувач, за допомогою джерела генерування ключів, отримує необхідний ключ, для розшифрування зашифрованої інформації
4) Отримувач розшифровує за допомогою згенерованого ключа зашифровану інформацію, та отримує її в звичайному вигляді для ознайомлення.

ПРИНЦИП РОБОТИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

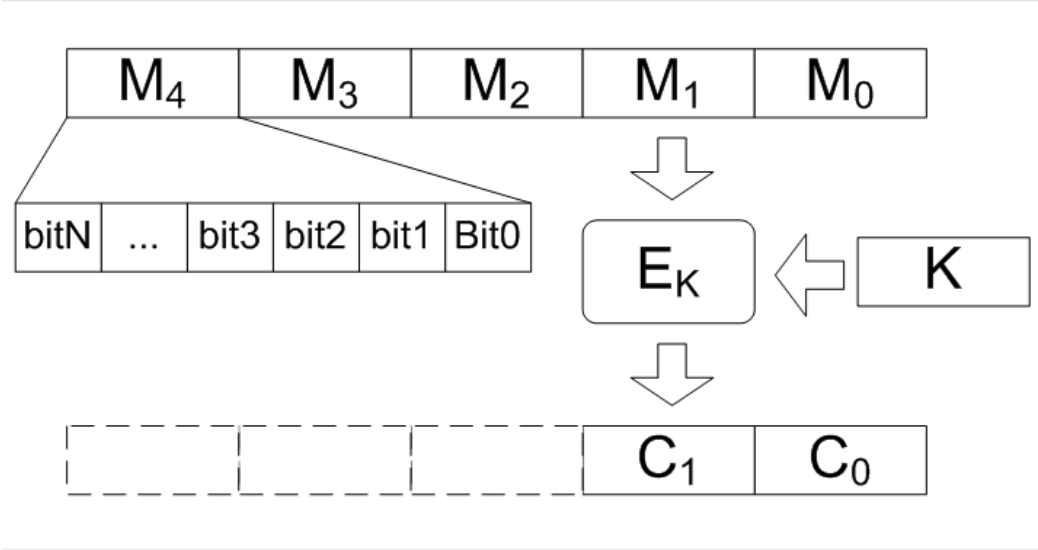

Рисунок 5.1 – Робота блочного шифрування

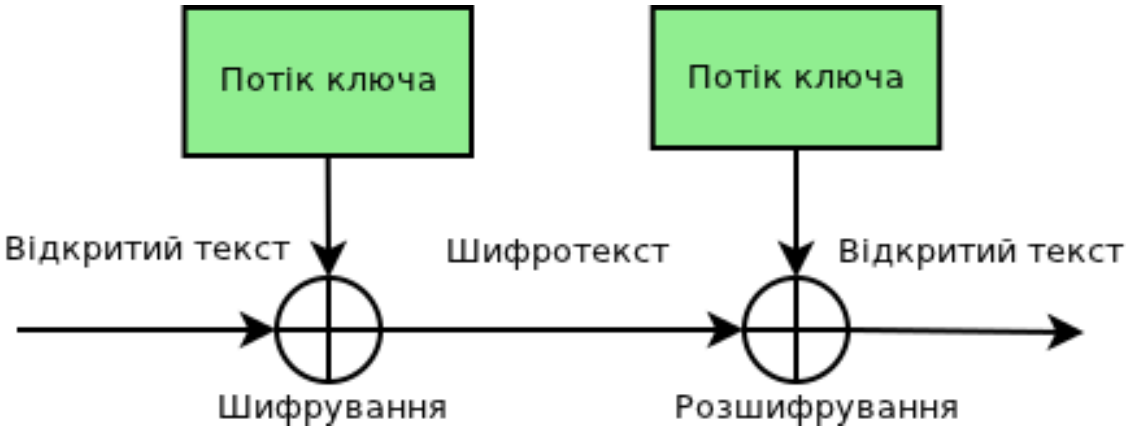

Рисунок 5.2 – Робота потокового шифру

Блочний шифр здатний зашифрувати одним ключем одне чи навіть декілька повідомлень, які в загальній сумі їх довжин будуть більшими, аніж довжина ключа шифрування. Однак постає питання про надійність такого шифрування. Ще одним з мінусів блочного шифрування є мала швидкість шифрування, в порівнянні з потоковим шифруванням.

Різновид симетричного шифрування, який полягає в тому, що кожен символ вихідного тексту під дією алгоритму шифрування перетворюється на символ зашифрованого тексту в залежності не лише від використовуваного ключа шифрування, але й від місця в потоці відкритого тексту. Потоковий шифр реалізовує інший підхід до шифрування, аніж в блочному шифруванні.

ПРИНЦИП РОБОТИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

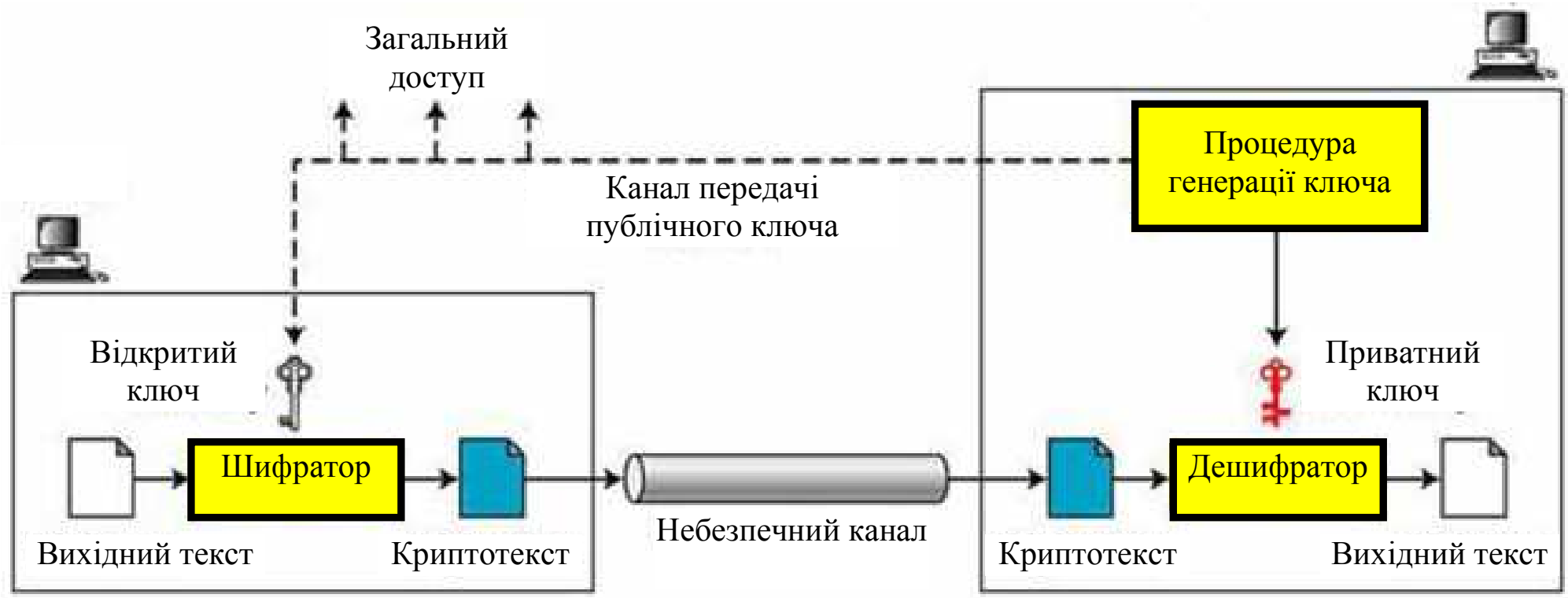

Рисунок 6.1 – Загальна схема асиметричної криптографії

В асиметричній криптографії використовується два ключі:

- публічний ключ;
- приватний ключ.

Відправник використовує публічний ключ для шифрування відкритого тексту для Отримувача, якщо знати вміст відкритого тексту має знати лише він. Дане зашифроване повідомлення відправляється будь-яким способом. Приватний ключ є таємним ключем, і не розголошується. Для того що виконати дешифрування такого повідомлення, необхідно використати приватний ключ.

(MEDIA ACCESS CONTROL) MAC–РІВЕНЬ ЗАСТОСУВАННЯ МЕТОДІВ КРИПТОГРАФІЇ ДЛЯ ЗАДАЧ ТЕЛЕКОМУНІКАЦІЙ

Додатки верхніх рівнів	**VoIP**	**IP**	**E1**	
MAC-рівень	**Підрівень перетворення CS**			
	Основний підрівеь			
	Підрівень безпеки			
Фізичний рівень	Кадр n-1	Кадр n	Кадр n+1	Кадр n+2
Схема передачі				

Рисунок 7.1 – MAC-рівні стандарту IEEE 802.16

Структурно MAC-рівень IEEE 802.16 розділений на три підрівні:

- підрівень перетворення сервісів CS (Convergence Sublayer);
- основний підрівень CPS (Common Part Sublayer);
- підрівень захисту PS (Privacy Sublayer).

У одному каналі можуть працювати сотні різних одиниць термінального обладнання великого числа кінцевих користувачів.

Цим користувачам потрібний доступ до різних сервісів (додатки):

- передача голосу і даних з часовим розділенням;
- з'єднання по протоколу IP;
- пакетна передача мови через IP (VoIP) і тому подібне.

ШИФРУВАННЯ ТА ІСНУЮЧИ ВРАЗЛИВОСТІ БЕЗДРОТОВИХ СИСТЕМ

Головним завданням, які були зроблені альянсом WiFi Alliance для технології IEEE 802.11 WLAN є:

- визначення і **гармонізація стандартів**;
- **сертифікація взаємодії** телекомунікаційного устаткування різних постачальників;
- **просування технології WiMAX** (IEEE 802.16 WMAN (Wireless Metropolitan Area Networks).

Робочою групою IEEE 802.16 за стандартами широкосмугового доступу (BWA, Broadband Wireless Access) були **розроблені наступні стандарти серії 802.16**:

- **IEEE 802.16** або IEEE 802.16-2001 – орієнтований на роботу в спектрі від 10 до 65 ГГц. Вимагає знаходження передавача і приймача в зоні видимості (LOS, Line of Sight).
- **IEEE 802.16a -** пониження робочої частоти та функціонування в зоні непрямої видимості
- **IEEE 802.16e** – розвиток ідей попередніх стандартів з фокусом на мобільності крайового користувача.

Для шифрування даних в 802.16 **використовується алгоритм DES** (Data Enscryption Standart).

Для шифрування ZigBee використовуються протоколи AES. Проте при експорті в країни Європи та Азії діє обмеження щодо довжини ключа. Ключ обмежується до 64 біт. За таких умов, передані внутрішні дані можуть бути розкриті із застосуванням потужних процесорних систем.

ЛЕГКОВІСНА КРИПТОГРАФІЯ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

На сьогодні є близько 50 низкоресурсних алгоритмів, але в більшості, вони абсолютно непридатні для використання. Розробники часто не мають змоги обрати алгоритм і чи зможе він працювати на певному пристрої. На Рисунок 3.4 показано деякі алгоритми та їх застосування.

SPONGENT	176-bit, на основі AES	алгоритми хешування	**Симетричні шифри**
PHOTON	64-bit, на основі AES		
LESAMNTA - LW	128-bit, на основі AES		
PRESENT	80, 128-bit	алгоритми блокового шифрування	
SPECK	64-256-bit		
CLEFIA	128-bit		
TRIVIUM	64-128-bit	алгоритм потокового шифрування	
Еліптичні криві	128-bit	алгоритм потокового шифрування	**Асиметричний шифр**

Рисунок 9.1 – Алгоритми для легковісної криптографії (Light Weight Cryptography, LWC)

У асиметричній криптографії використовуються наступні операції алгебри і алгоритми:

- алгоритми перевірки числа на простоту;
- операції алгебри над великими числами: модульне множення, модульне піднесення до степеня, знаходження залишку від ділення, обчислення зворотного числа по модулю.

Найбільш трудомісткими операціями в асиметричній криптографії є операції модульного множення великих чисел і модульного піднесення до степеня великих чисел.

МАТЕМЕТИЧНА ОСНОВА АЛГОРИТМУ ЕЛІПТИЧНОЇ КРИВОЇ

Еліптичну криву E над певним полем F можна визначити як безліч пар точок $(x, y) \in F^2$, що задовольняють рівнянню:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in F\ . \qquad (10.1)$$

На безлічі $E(F)$, що складається з точок еліптичної кривої і ще одного елементу – нескінченно видаленої точки кривої *O*, можна визначити операцію, що має властивості операції абелевої групи. Групу, що виходить, розглядають як адитивну групу, операцію називають операцією складання і означають знаком плюс. Нескінченно видалена точка кривої О виконує роль нейтрального елементу (нуля) групи .

Еліптичні криві, визначені над полем дійсних чисел та над полем Z_{23}, зображені на Рис.10.10,2, відповідно

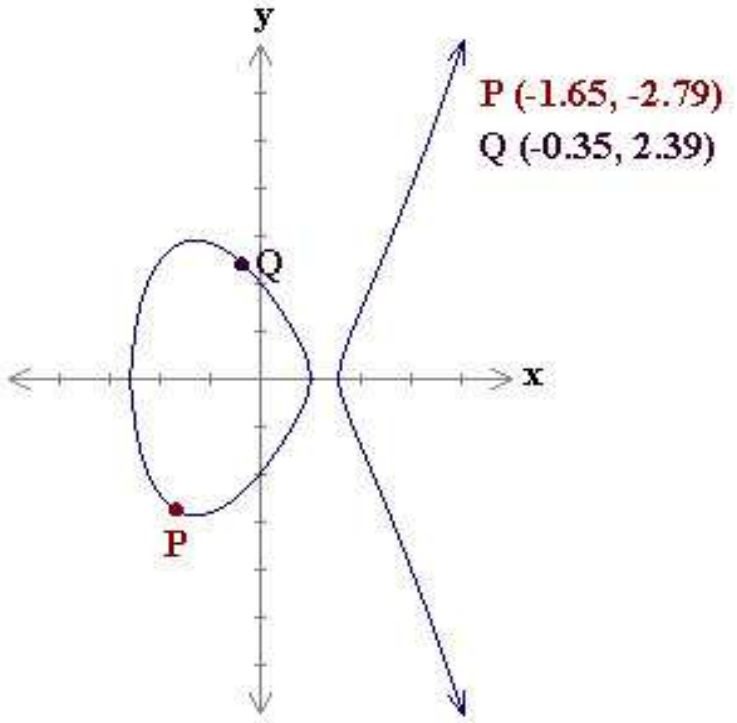

Рисунок 10.1 $y^2 = x^3 - 5x + 4$

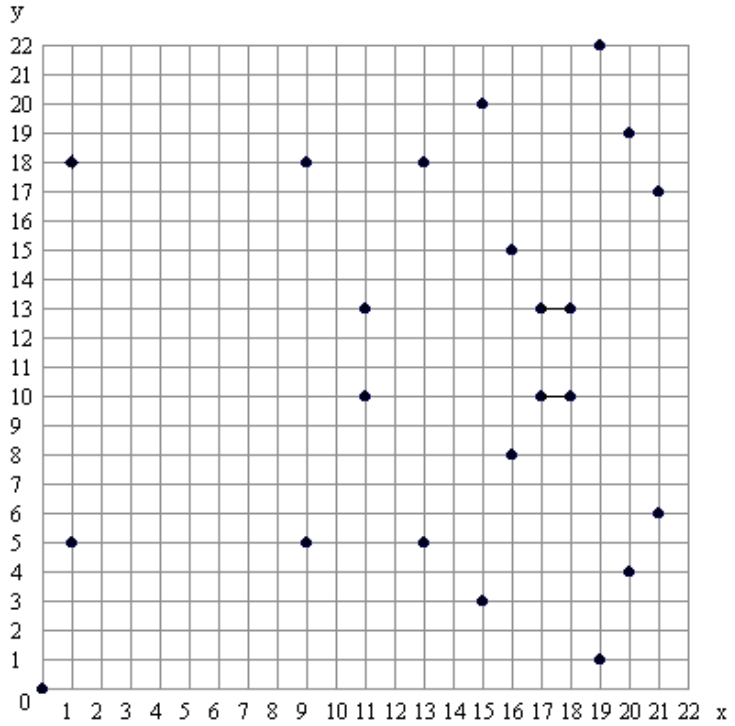

Рисунок 10.2 $y^2 \pmod n = x^3 + x \pmod n, n = 23$

ВИЗНАЧЕННЯ ШВИДКОДІЇ СИСТЕМИ

Потокова швидкість обробки даних – це один з основних параметрів, по яких оцінюють реалізації криптографічного перетворення даних. Найпростіше оцінити швидкість по формулі

$$V = \frac{F \cdot K}{n},$$

де F - тактова частота;

K - розмір блоку, що підлягає криптографічному перетворенню;

n - число тактів, що вимагається на виконання циклу перетворення цього блоку.

Або за більш зручною формулою:

$$V = \frac{D_R + D_W + D_{CR}}{T_{CLK}},$$

де D_R – обсяг даних, що зчитується;

D_W – обсяг даних, що записується;

D_{CR} – обсяг даних, що обробляється за один такт криптографічного перетворення;

T_{CLK} – час одного такту криптографічного перетворення.

Наприклад, такий відомий алгоритм як ГОСТ 28147-89 (або просто "ГОСТ") має швидкодію 32 такти на 8-байтовий блок для криптографічного процесору, тобто теоретична швидкість криптографічного перетворення повинна сягнути 270 Мбайт/с при тактовій частоті в 1000 Мгц. Проте реальна швидкість апаратної реалізації алгоритму – 8-9 Мбайт/с. Обмеження є чисто технологічним: через відсутність необхідного рівня розробок або елементної бази.

ЕКСПЕРИМЕНТАЛЬНА ОЦІНКА ШВИДКОДІЇ

Таблиця 12.1 – Операційні витрати на обрахунок одної математичної операції, для 32 бітного блоку даних

Тип процесора	τ_b, такти	τ_k ,такти	f_{CPU}, МГц
	Ключ 32 біта		
8-біт, AVR RISC	24	140	24
32-біт, ARM RISC	7	42	200
	Ключ 64 біта		
8-біт, AVR RISC	180	2270	24
32-біт, ARM RISC	33	320	200

Фізичний час для обрахунку алфавітів визначається як:

$$T_A(n) = \frac{n \cdot \tau_b + n^2 \cdot \tau_k}{f_{CPU}}, \text{ секунд,}$$

де n – розмірність очикуваного алфавіту; τ_b – операційна складність обрахунку одної букви алфавіту; τ_k – кількість операцій для виконання математичної операцій пошуку; f_{CPU} – швидкодія процесора.

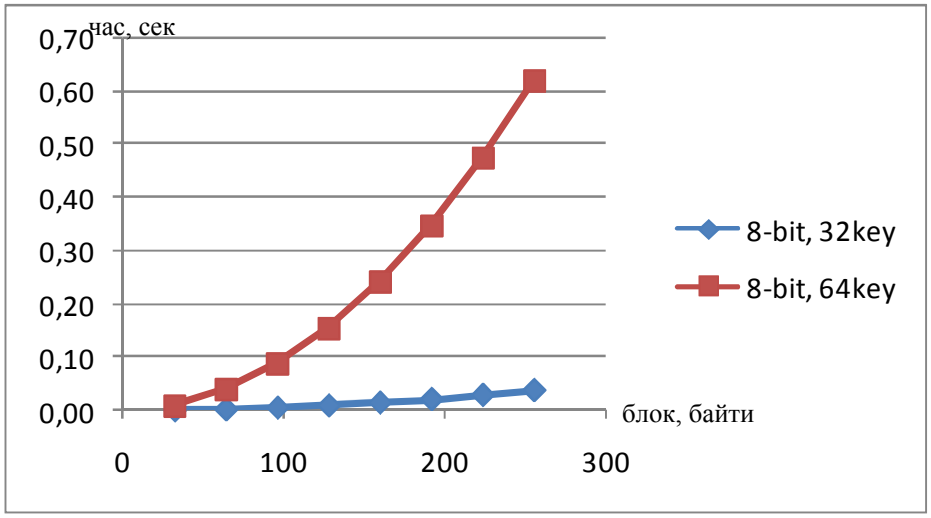

Рисунок 12.1 – Обчисленння алфавітів для 8-бітного контролера

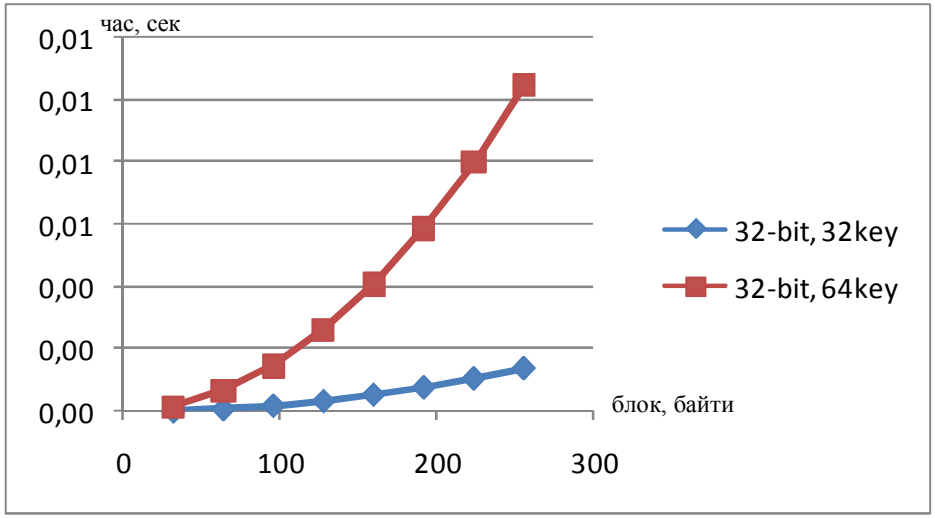

Рисунок 12.2 – Обчисленння алфавітів для 32-бітного контролера

ЕКСПЕРИМЕНТАЛЬНА ОЦІНКА ШВИДКОДІЇ

Таблиця 4.3 – шифрування та підготовка даних для передачі згідно стандартів 802.15.4b та 802.15.4a

Розмір блоку шифрування, біти	Час на 1 байт	802.15.4b		802.15.4a	
		Час підготовки блоку, 63 байт	Кількість блоків за 1 сек	Час підготовки блоку, 127 байт	Кількість блоків за 1 сек
	8 бітний контролер, ключ 32 біти				
32	0,00033	0,020808	48,05733	0,041947	23,83946
96	0,002962	0,186611	5,35874	0,376184	2,658272
192	0,011838	0,745779	1,34088	1,503396	**0,665161**
256	0,02104	1,325533	0,754413	2,672107	**0,374236**
	8 бітний контролер, ключ 64 біти				
32	0,00534	0,336428	2,972401	0,678197	1,474498
96	0,047982	3,022866	0,330812	6,093714	**0,164104**
192	0,191849	12,08647	0,082737	24,3648	**0,041043**
256	0,341029	21,48485	0,046544	43,31073	**0,023089**
	32 бітний контролер, ключ 32 біти				
32	1,19E-05	0,000749	1335,123	0,00151	662,3053
96	0,000107	0,006718	148,8613	0,013542	73,84456
192	0,000426	0,026847	37,24759	0,054121	18,47715
256	0,000757	0,047718	20,95631	0,096194	10,39565
	32 бітний контролер, ключ 64 біти				
32	$9{,}04 \times 10^{-5}$	0,005695	175,5818	0,011481	87,09963
96	0,000812	0,051148	19,55096	0,103109	9,698507
192	0,003246	0,204484	4,890363	0,412213	2,425928
256	0,005769	0,363478	2,751199	0,732725	1,364768

В загальному видно, що застосування 32 бітної архітектури дозволяє отримати більш ніж 70 разову перевагу.

ОЦІНКА ЧАСУ РОБОТИ СЕНСОРНИХ МЕРЕЖ

Таблиця 14.1 – Енергоспоживання модулі за стандартом 802.15.4 фірми Digi

Режим	**Споживання струму, мА**
Активний	10
Режим сну	0,003
Передача	125
Прийом	40

Рисунок 14.1 – Зовнішній вигляд модулів XBee (https://www.digi.com)

Таблиця 14.2. Часові втрати згідно стандарту 802.15.4 ZigBee

Дія	**Час (у мс)**
CSMA/CA	2,368 мс
Передача кадру	4,256 мс
Затримка після передачі	0,192 мс
Передача підтвердження	0,352 мс
Загальний час (T_Σ)	7,168 мс

Час активності пристрою за один раз складає 16мс.

Час в 3мс – передача зібраних даних і стільки ж витрачається на їх прийом.

Час підготовки до передачі даних – 2мс. Таким чином, один цикл складає **24мс**., отже швидкість:

$$\frac{1000}{24} = 41\,(\text{пакет/с})$$

ВИСНОВКИ

1. Визначені проблеми застосування криптографічних процесів у цілому та в ракурсі забезпечення надійності від втручання третьою стороною зокрема. Показано як прості алгоритми, симетричні, так і сучасні алгоритми – асиметричні.

2. Встановлено, що більшість нових алгоритмів базується на основі симетричного алгоритму AES. Визначено, що асиметричні алгоритми є найбільш надійними, оскільки вони забезпечують захист інформації, шляхом використання публічного ключа для шифрування, а приватного ключа для дешифрування інформації. В такому випадку, при втручанні в пристрій передачі, приватний ключ все ще є захищеним, оскільки в самому пристрої не зберігається.

3. Розглянуто алгоритми шифрування в розрізі застосування для обчислювальних систем малої обчислювальної потужності. Представлено порівняння математичного базису. Для асиметричних алгоритмів відносять різні моделі, але для легковісних алгоритмів відносяться алгоритми на основі роботи з модульною арифметикою. Складність виконання цих обчислень і обумовлює складність підтримки асиметричних протоколів в системах обмеженої потужності. Один з таких алгоритмів є алгоритм на основі еліптичних кривих. Цей алгоритм характеризується зменшеною обчислювальною потужністю.

4. Виходячи із специфікацій цього стандарту була емпірично обраховано часові показники, що показують витрати на сам процес передачі інформації (на прикладі стандартів 802.15.4a та 802.15.4b), визначена ефективна швидкість передачі даних при застосуванні алгоритму шифрування за допомогою гамування в програмі для 8- та 32-бітного контролера загального призначення. Виконано обрахунок для 32 та 64 бітного ключа для блоків від 32 до 256 байт. Показано, що навіть 8-бітний контролер здатний забезпечити шифрування. Проте особливістю є те, що розмір блоку шифрування не співпадає з блоками даних, що передається через модулі ZigBee. Також розраховано теоретичне споживання струму і час роботи пристроїв при заявленій швидкості передачі даних.

ISSN 2307-5732
DOI 10.31891/2307-5732

НАУКОВИЙ ЖУРНАЛ

4.2020

ВІСНИК

Хмельницького національного університету

Том 1

Технічні науки

Technical sciences

SCIENTIFIC JOURNAL
HERALD OF KHMELNYTSKYI NATIONAL UNIVERSITY

2020, Issue 4, Volume 287, Part 1

Хмельницький

ВІСНИК
ХМЕЛЬНИЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
серія: Технічні науки

Затверджений як фахове видання (перереєстрація)
Категорія «Б», РІШЕННЯ АТЕСТАЦІЙНОЇ КОЛЕГІЇ № 1643 ВІД 28.12.2019

Засновано в липні 1997 р. ***Виходить 6 разів на рік***

Хмельницький, 2020, № 4, Том 1 (287)

Засновник і видавець: Хмельницький національний університет
(до 2005 р. – Технологічний університет Поділля, м. Хмельницький)

Включено до науково-метричних баз:

Google Scholar	http://scholar.google.com.ua/citations?hl=uk&user=aIUP9OYAAAAJ
Index Copernicus	http://jml2012.indexcopernicus.com/passport.php?id=4538&id_lang=3
Polish Scholarly Bibliography	https://pbn.nauka.gov.pl/journals/46221

Технічний редактор Горященко К. Л., к.т.н.
Редактор-коректор Броженко В. О.

Рекомендовано до друку рішенням вченої ради Хмельницького національного університету, протокол № 3 від 29.10.2020 р.

Адреса редакції: редакція журналу "Вісник Хмельницького національного університету"
Хмельницький національний університет
вул. Інститутська, 11, м. Хмельницький, Україна, 29016

☎ (038-2) 67-51-08 **web:** http://journals.khnu.km.ua/vestnik
http://lib.khnu.km.ua/visnyk_tup.htm

e-mail: visnyk.khnu@gmail.com

Зареєстровано Міністерством України у справах преси та інформації.
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 9722 від 29 березня 2005 року

МАШИНОБУДУВАННЯ, МЕХАНІКА ТА МАТЕРІАЛОЗНАВСТВО

ЕЛЕКТРОМЕХАНІКА, ЕЛЕКТРОТЕХНІКА ТА ЕНЕРГЕТИКА

АВТОМАТИЗАЦІЯ, ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

ЕЛЕКТРОМЕХАНІКА, ЕЛЕКТРОТЕХНІКА ТА ЕНЕРГЕТИКА

DOI 10.31891/2307-5732-2020-287-4-143-148
УДК 621

К.Л. ГОРЯЩЕНКО, А.А. ТАРАНЧУК, Я.В. СУПРУНЮК
Хмельницький національний університет
О.В. ЦИРА
Одеська національна академія зв'язку ім. О.С. Попова

ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ В СИСТЕМАХ ОБМЕЖЕНОЇ ПРОЦЕСОРНОЇ ПОТУЖНОСТІ

Один з напрямків розвитку безпроводових систем передачі інформації ґрунтується на впровадженні мереж на базі простих вузлів, що використовуються в таких стандартах, як ZigBee, Bluetooth, Wibree. Інформація, що передається мережею, може бути перехоплена та використана третьою стороною. Простота конструкції, мінімальне енергоспоживання та мінімальний обсяг пам'яті не дозволяють впровадити складні алгоритми криптографічного захисту інформації. Складність алгоритму захисту обумовлена розрядністю процесора (8, 16 або 32 біти), наявним обсягом пам'яті ПЗП та ОЗП, а також енергоспоживанням в процесі виконання криптографічного перетворення. Обсяг пам'яті також є важливим для прийняття, обробки та передачі інформації між вузлами мережі.

Ключові слова: безпроводова мережа, вузол, криптографія.

K.L. HORIASHCHENKO, A.A. TARANCHUK, Y.V. SUPRONYUK
Khmelnitsky national university, Ukraine
O. TSYRA
Odessa national academy of communication named by O. Popov

APPLICATION OF CRYPTOGRAPHIC ALGORITHMS IN SYSTEMS WITH LIMITED PROCESSING POWER

One of the directions of development of wireless information transmission systems is based on the introduction of networks based on simple nodes used in such standards as ZigBee, Bluetooth, Wibree. Information transmitted over the network may be intercepted and used by a third party. Simplicity of design, minimum power consumption and minimum amount of memory do not allow to implement complex algorithms of cryptographic protection of information. The complexity of the protection algorithm is due to the bit size of the processor (8, 16 or 32 bits), the available amount of RAM and RAM, as well as power consumption during cryptographic conversion. The amount of memory is also important for receiving, processing and transmitting information between network nodes.

One of the possible ways to increase the efficiency of cryptographic operations in hardware is to build them on the principle of "master - slave". The method involves the use of a general-purpose processor as the central head of the device module ("master"), and a specialized arithmetic coprocessor ("master"), which performs all time-consuming operations under the control of the master.

Keywords: wireless network, node, cryptography.

Вступ

Сьогодні у світовій практиці послуг у сфері контролю стану розподілених в просторі вузлів визначилася стійка тенденція на посилення ролі технічних засобів. Тенденція ця не випадкова: численні дослідження в області особистої і майнової безпеки показали, що широке використання технічних засобів дозволяє виключити або звести до мінімуму негативний вплив самої ненадійної ланки в системі - людини, якій властиві стомлюваність, неуважність, халатність і т. п. При цьому, організація розподіленої мережі контролю і передачі за допомогою технічних засобів обходиться споживачеві значно дешевше, а надійність її вища [1, 5].

По факту, в середині 90-х років, такими вузлами мережі контролю і передачі ставали системи безпеки для охоронних систем.

У завданнях 2020-х років - розподілені системи контролю за станом здоров'я людей в приміщеннях, на вулиці, в транспорті і так далі. Глобальна пандемія вірусу COVID - 19 веде до усвідомленої необхідності створення медичних мереж контролю.

Історично, при створенні систем розподіленого контролю основна увага приділялася таким аспектам, як [1]:

- автоматизація, яка дозволяє до мінімуму спростити процеси введення об'єктів під охорону, скоротити обслуговуючий персонал; істотно скоротити кількість неправдивих тривог через втручання в роботу системи;
- контроль каналу зв'язку, що забезпечує високу достовірність передачі і виключає втрату тривожної інформації;
- розробка широкої гамми об'єктових пристроїв з різними функціональними і сервісними можливостями, що дозволяють задовольнити потреби найширших верств населення.

З точки зору організації захисту об'єктів від несанкціонованого проникнення, як по устаткуванню технічними засобами охорони, так і по тактиці дій чергових служб, існуючі системи не мають яких-небудь істотних відмінностей.

Передача інформації з використанням безпроводових технологій

Питання про достовірне та безпечне надсилання інформації від приймача до отримувача відоме ще з давніх часів. Основним завданням криптографії в давні часи було забезпечення конфіденційності, або простіше кажучи шифрування – інформація, що містилася, мала бути змінена таким чином, щоб прочитати та зрозуміти міг лише той, кому дійсно назначено [1], а не будь-яка інша стороння особа, без відомостей про спосіб, яким було зашифрована відповідна інформація.

Криптографічним алгоритмом (шифром) називається така математична функція, що дозволяє виконати над інформацією дію шифрування та дешифрування.

Найпопулярнішим способом в давні часи був так званий шифр Цезаря (або інша назва – шифр зсуву) – шифрування інформації, що передавалася на папері, в якому кожна буква тексту, що був написаний, замінювалась на ту, яка була віддалена (зсунута) на три позиції в буквенному алфавіті. Простий для нинішньої техніки шифр, став основою для складніших способів, до прикладу шифр Віженера чи ROT13 [1, 1, 6].

З розвитком людства і науки, такі способи шифрування інформації ставали все більш неефективними. Наступним кроком стали машини, які виконували шифрування та дешифрування інформації, найвідомішою з яких є Енігма. Та з появою комп'ютерних систем, можна було зашифрувати будь-які дані, представивши їх у двійковому вигляді, а не лише у текстовому вигляді, як це відбувалося доволі довгий період людства.

В наш час це питання так і залишилось актуальним, тільки тепер інформацією обмінюються не лише люди, а й пристрої, які оточують нас. І чим більше є таких пристроїв, тим гостріше стає це питання.

Перед криптографічними методами завжди висувають наступні вимоги [4]:

1. Зашифроване повідомлення можливо прочитати лише при наявності ключа.
2. Кількість операцій, що потрібні для визначення використаного ключа шифрування по фрагменту зашифрованого повідомлення й відповідного відкритого тексту, повинно бути не менше загального числа можливих ключів.
3. Кількість операцій, які необхідні для розшифрування повідомлення способом перебору ключів, повинно мати строгу нижню порогову оцінку й виходити за межі можливостей сучасного обладнання, або вимагати високі витрати на обчислення.
4. На надійність захисту шифрованої інформації не впливає знання сторонніми алгоритму шифрування.
5. Маленька зміна ключа шифрування призводить до істотних змін самої зашифрованої інформації, навіть при шифруванні вихідного тексту, який був зашифрований.
6. Незначна зміна вихідного тексу призводить до істотних змін зашифрованої інформації, при використанні того ж ключа шифрування.
7. Структурні елементи алгоритму шифрування завжди залишаються без змін.
8. Додаткові біти, що вводяться в інформацію, в процесі її шифрування, повинні бути надійно сховані в зашифрованій інформації.
9. Довжина зашифрованої інформації не повинна перевищувати загальну довжину вихідної інформації.
10. Мають бути виключені прості та легкі залежності, які використовуються для формування ключа шифрування.
11. Будь-який ключ з множини ключів має забезпечувати надійний захист інформації.
12. Реалізація алгоритму повинна бути як на програмному та апаратному рівні.

Тому в цілях подальшого розвитку і вдосконалення систем збору та передачі інформації до нових розробок останнім часом пред'являються додаткові вимоги:

- імітостійкість і криптозахист, системи, що забезпечують стійкість, до несанкціонованого «обходу» і обумовлені появою «кваліфікованих» крадіжок;
- висока інформативність, що забезпечує розділення сигналів про проникнення і пожежу, аварію або зміну параметрів лінії зв'язку і т. д.;
- можливість сполучення системи з оптоволоконними каналами зв'язку, обумовлена впровадженням підприємствами зв'язку нових цифрових технологій передачі інформації;
- уніфікація створюваних технічних засобів, тобто можливість об'єднання різних пристроїв в єдиний програмно-апаратний комплекс збору та передачі інформації.

Пріоритетним завданням технічної політики в області розвитку таких систем є розробка відсутніх на сьогодні єдиних вимог, що в умовах різноманіття існуючих і нових, дозволить уніфікувати стики систем передачі сповіщень.

Передача інформації з використанням бездротових технологій

Разом з ростом технологій та розвитком мобільних пристроїв, стало зрозуміло, що дріт використовувати можна на невеликих відстанях, і для пристроїв, що в більшості випадків використовуються стаціонарно, без переміщення по великих площах. Постало питання про впровадження бездротового з'єднання, для передачі інформації між пристроями на відкритій місцевості. Таким чином, почався розвиток бездротового підключення. В залежності від відстані, на якій буде передаватись інформація, бездротові мережі можна поділити на три класи: WPA, WLAN, WMAN.

За дальністю дії, бездротові мережі, можна поділити наступним чином [7]:

WPAN – бездротова мережа, що охоплює невелику частину території, невелику швидкість передачі інформації, а також передача інформації відбувається лише між декількома пристроями. Прикладом такої технології є Bluetooth, ZigBee.

WLAN – бездротова мережа, що охоплює середню за розміром ділянку (відстанню до 100 метрів), в залежності від використання стандарту передачі та частоти розміщення, швидкість передачі може сягати до 3,4 Гбіт/с. Прикладом такої технології є Wi-Fi.

WMAN – бездротова мережа, що охоплює велику територію (область покриття до 50 кілометрів). В залежності від використання стандарту, швидкість передачі може варіюватись, максимальним значенням є 1 Гбіт/с. Прикладом такої технології є WiMax.

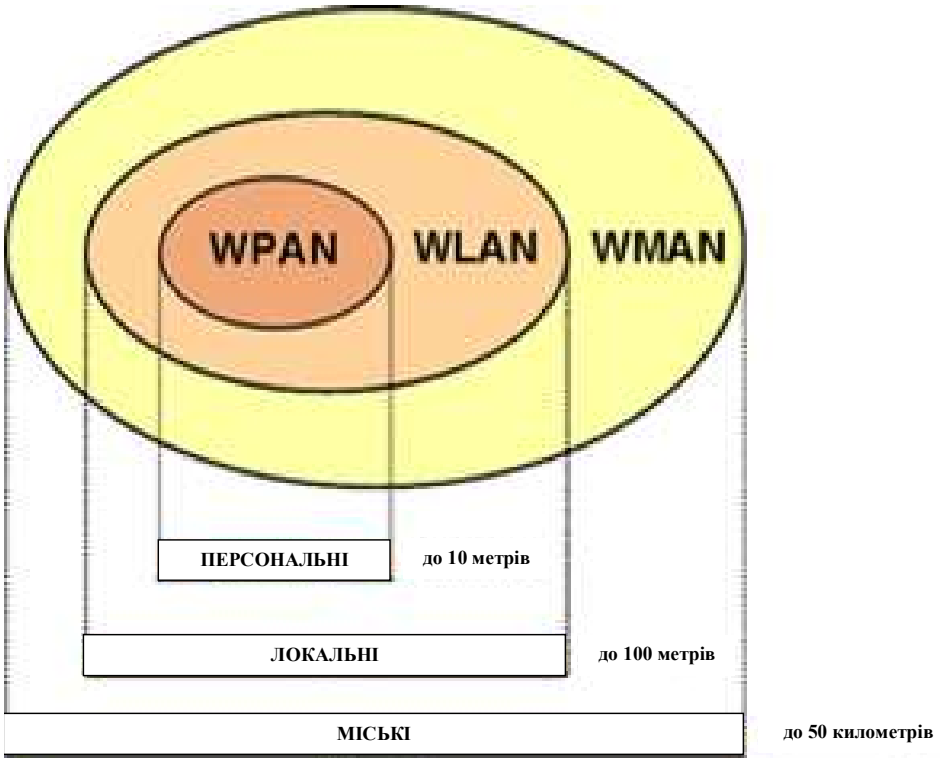

Рис. 1. Класифікація безпроводових технологій в залежності від дальності дії [7]

Безпровідні сенсорні мережі - це розподілені мережі, що мають здатність до реорганізації власної структури. Характеризуються стійкістю до відмови окремих елементів цієї мережі, а також обмінюються інформацією по безпровідному зв'язку. Кожен елемент мережі має автономне джерело живлення, мікрокомп'ютер, приймач/передавач.

Виділяють наступні основні стандарти для малопотужних безпровідних мереж:

- IEEE 802.15.4;
- ZigBee;
- Bluetooth;
- Wibree.

Область покриття мережі може складати від декількох метрів до декількох кілометрів, залежно від типу модуля і антени, а також за рахунок здатності ретрансляції повідомлень від одного елементу до іншого. Обмін даними між двома кінцевими пристроями може здійснюватися через ретранслятор, у тому випадку, якщо дальність роботи цих пристроїв не дозволяє їх взаємне виявлення. Таким чином, пристрою з малим радіусом дії за допомогою системи ретрансляторів можуть спілкуватися один з одним.

Постановка проблеми дослідження на прикладі пристроїв мережі ZigBee

Пристрої безпроводової системи забезпечують можливість швидкого створення мережі. Як було показано вище, пристрої володіють власним джерелом живлення. Це джерело часто є простою батареєю з невеликою ємністю та призначеною для одноразового використання. Сам датчик-вузел мережі не підлягає ремонту або заміні в процесі експлуатації. Основна причина такого ставлення – відносна простота конструкції, мінімальний розмір та низька ціна. Наприклад, на рис. 2 наведено приклад включення модуля ZigBee (тип RC2300) для обміну даними по послідовному порту. Як видно з рисунку, модуль забезпечує функціонал зчитування, обробки, зв’язку та передачі.

У технології ZigBee використовується два типи модулів зв’зку різної складності. Повністю функціональний пристрій (FFD — Full Function Device) здатний приймати і передавати дані, у тому числі і чужі (по ланцюжку). При об'єднанні FFD -устройств можуть бути реалізовані топології «зірка», «кожен з кожним» і «кластерне дерево».

Пристрій з обмеженим набором функції (RFD — Reduced Function Device) — це найпростіший тип, який може тільки переговорюватися з координуючим пристроєм. При об'єднанні в мережу RFD може використовуватися тільки в топології «зірка». Окрім ділення на FFD і RFD в специфікації ZigBee визначені три типи логічних пристроїв — координатор мережі, маршрутизатор і крайовий пристрій.

Координатор ініціалізував мережу, управляє мережевими вузлами, зберігає інформацію про налаштування кожного мережевого вузла, задає номер частотного каналу і ідентифікатор мережі PAN ID.

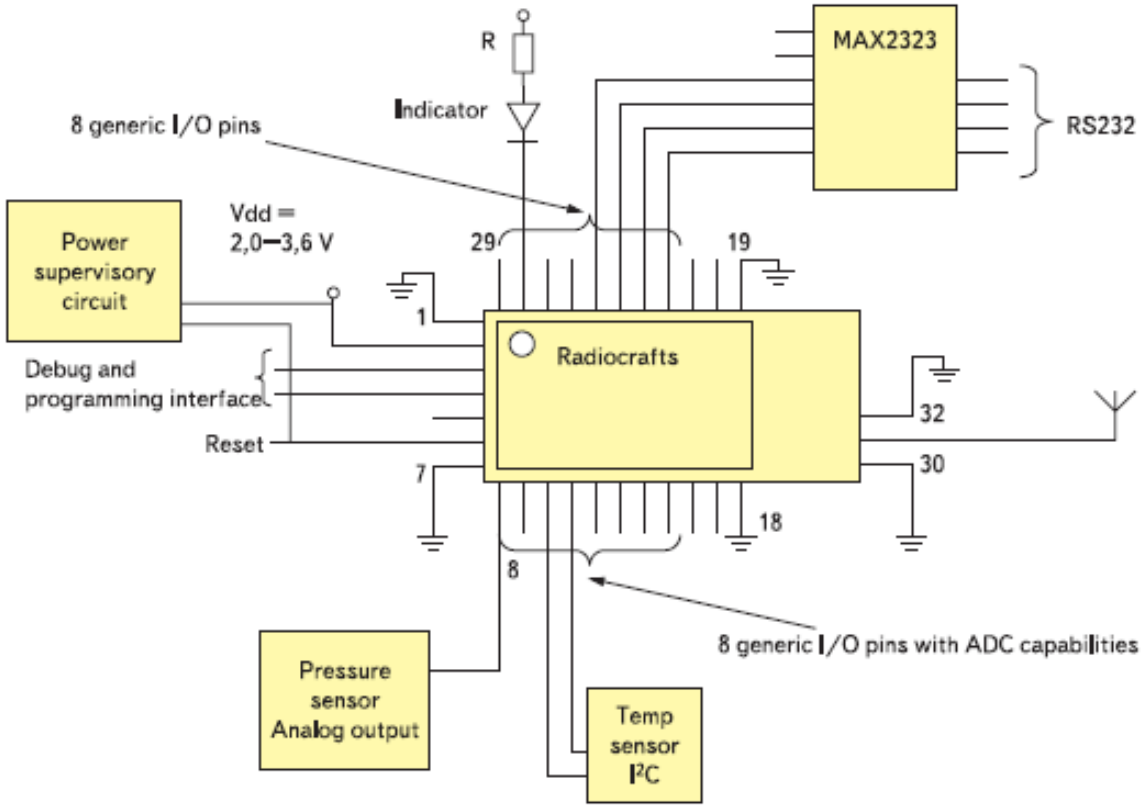

Рис. 2. Приклад включення модуля ZigBee (тип RC2300) для обміну даними по послідовному порту

Проблема апаратної реалізації вузлів розподіленої мережі з підтримкою криптографії

В залежності від пристрою, який використовується кінцевим користувачем, визначається той чи інший клас бездротової передачі інформації.

Взаємодію між відправником і отримувачем з урахуванням криптографічної системи описується наступним чином [1]:

1. Відправник отримує з джерела генерування ключів, ключ К1, яким буде зашифрована інформація – повідомлення М.

2. Відправник зашифровує за допомогою ключа К1 необхідну для передачі інформацію М, та передає криптограму Е відкритими каналами зв'язку в напрямку до одержувача (або одержувачів).

3. Отримувач, за допомогою джерела генерування ключів, отримує необхідний ключ К2, для розшифрування зашифрованої інформації. В залежності від схеми шифрування, ключі К1 та К2 можуть бути однаковими або різними.

4. Отримувач розшифровує за допомогою згенерованого ключа К2 зашифровану інформацію Е, та отримує її в звичайному вигляді для ознайомлення – повідомленні М.

На рис.3 показано також і шифрувальника супротивника. Супротивник намагається досягнути як мінімум дві мети:

1) встановлення ключа розшифрування К2 для можливості зчитування повідомлення М з криптограми Е.

2) встановлення ключа шифрування К1 для можливості зміни повідомлення М або введення в мережу спотворених повідомлень.

3) Отже можна зробити висновок, що криптографічні протоколи, що використовуються в протоколі передачі інформації мають забезпечити надійність від втручення інших сторін не менше певного часу.

Рис. 3. Загальна структурна схема передачі інформації із застосуванням криптографії

Процес розробки апаратних або апаратно-програмних засобів криптографічного захисту інформації на основі сучасних асиметричних криптографічних алгоритмів, у тому числі і національних асиметричних криптографічних алгоритмів [1], безпосередньо пов'язаний з необхідністю реалізації арифметичних операцій, що лежать в основі алгоритмів. Так, стандарт ГОСТ 34.10-2018 використовує числа розмірністю не менше 256 біт, що в десятковому уявленні складає $\approx 10^{77}$:

- великі габарити, що робить неможливим їх застосування в малогабаритних і ношених пристроях, як наприклад в USB - ключах;
- велике споживання електроенергії, що знижує ефективність їх використання в пристроях з батарейним живленням;
- велика кількість виводів : більшість високопродуктивних процесорів мають кількість виводів від 300 і вище, що призводить до небажаних ускладнень схемотехніки проектованих пристроїв. Крім того, конструктивне розташування виводів в сучасних корпусах спричиняє за собою необхідність в дорогому спеціалізованому устаткуванні, що унеможливлює широкий розвиток розробок такого роду (як правило, усі процесори з числом виводів ≥ 200 випускаються в корпусах з кульковими виводами BGA);
- неоптимізована система команд під конкретне завдання: ефективність програмного коду (а значить і швидкість виконання програми) безпосередньо залежить від фіксованої системи команд конкретного процесора;
- обмежена розрядність даних : сучасні процесори мають фіксовану розрядність даних (8, 16 або 32 розряди), що призводить до збільшення програмного коду при виконанні криптографічних операцій, і як наслідок - до зниження продуктивності пристрою в цілому;
- лінійність програмного коду: в процесорах відсутні можливості незалежного і паралельного виконання декількох трудомістких операцій одночасно;
- висока вартість, яка росте пропорційно збільшенню продуктивності.

Висновки

Виходячи з вищенаведеного наведеного, можна зробити висновок, що використання високопродуктивних процесорів для виконання криптографічних операцій в апаратних засобах є малоефективним і недоцільним за рахунок великого енергоспоживання.

Одним із можливих способів підвищення ефективності виконання криптографічних операцій в апаратних засобах є їх побудова за принципом «ведучий - ведений». Спосіб припускає використання процесора загального призначення як центрального керівника модуля пристрою («ведучий»), і спеціалізований арифметичний співпроцесор («ведений»), що виконує усі трудомісткі операції під управлінням ведучого. Це зменшує енергоспоживання в моменти виконання дій прийому інформації та її передачі. Спеціалізований співпроцесор забезпечує швидкість обробки за короткі терміни часу.

Література

1. Горященко К.Л. Формат Adobe PDF как средство распространения защищенной информации / К.Л. Горященко, І.В. Троцишин // Вимірювальна та обчислювальна техніка в технологічних процесах. – Хмельницький. – 2006. – № 1. – С. 132-136.

2. Бабаш А. В. Криптография (аспекты защиты). / А. В. Бабаш, Г. П. Шанкин. — М.: СОЛОН-ПРЕСС, 2007. – 512 с.

3. Панасенко С. П. Аппаратные шифраторы / С. П. Панасенко, В.В. Ракитин // Журнал «Мир ПК». 2002. № 8.

4. Шокало В.М. Концепция создания отечественных специальных цифровых систем передачи информации / В.М. Шокало, А.И. Цопа // Науково-технічний журнал «Захист інформації». – Київ: ДУІКТ,

2006. – Вип. №3. – С. 51-57.

5. Горященко К.Л. Ризики цілісності інформації на переносних носіях інформації / К.Л. Горященко, О.І. Полікаровських, В.Є. Гавронський, Ю.І. Сніжко // Вісник Хмельницького національного університету. – 2008. – № 4. – С. 66-70.

6. Горященко К.Л. Аспекти захисту програмного коду у відкритому апаратному середовищі / К.Л. Горященко // Вісник Хмельницького національного університету. – 2009. – № 2. – С. 208-212

7. Стрельницкий А.Е. Вариант повышения помехозащищенности радиоканала фиксированной связи WiMAX / А.А. Стрельницкий, А.И. Цопа, В.М. Шокало // Труды 8-й Международной научно-практической конференции «Современные информационные технологии» /СИЭТ'2007/. – Одесса, 2007. – С. 173.

References

1. Horiashchenko K.L. Format Adobe PDF kak sredstvo rasprostranenija zashhishhennoj informacii / K.L. Horiashchenko, I.V. Trocishin // Vimirjuvalna ta obchisljuvalna tehnika v tehnologichnih procesah. – Hmelnickij. – 2006. – № 1. – S. 132-136.

2. Panasenko S. P., Rakitin V.V. Apparatnye shifratory // Zhurnal «Mir PK». 2002. № 8.

3. Babash A. V., Shankin G. P. Kriptografija (aspekty zashhity). — M.: SOLON-PRESS, 2007. – 512 s.

4. Shokalo V.M. Koncepcija sozdanija otechestvennyh special'nyh cifrovyh sistem peredachi informacii / V.M. Shokalo, A.I. Copa // Naukovo-tehnichnij zhurnal «Zahist informacii». – Kiïv: DUIKT, 2006. – Vip. №3. – S. 51-57.

5. Horiashchenko K.L. Riski cilisnosti informacii na perenosnih nosijah informacii / K.L. Horiashchenko, O.I. Polikarovskih, V.E. Gavronskij, Ju.I. Snizhko // Visnik Hmelnickogo nacionalnogo universitetu. – 2008. – №4. – S. 66-70.

6. Horiashchenko K.L. Aspekti zahistu programnogo kodu u vidkritomu aparatnomu seredovishhi / K.L. Horiashchenko // Visnik Hmelnickogo nacionalnogo universitetu. – 2009. – №2. – S. 208-212

7. Strelnickij A.E., Copa A.I., Shokalo V.M. Variant povyshenija pomehozashhishhennosti radiokanala fiksirovannoj svjazi WiMAX / // Trudy 8-j Mezhdunarodnoj nauchno-prakticheskoj konferencii «Sovremennye informacionnye tehnologii» /SIJeT'2007/. – Odessa, 2007. – S. 173.

Рецензія/Peer review : 19.10.2020 р. Надрукована/Printed :06.11.2020 р.

Canada. – January/February 2017. – Volume 6. – Number 1. – P. 22–26.

10. Щербань В.Ю. Порівняльний аналіз роботи нитконатягувачів текстильних машин / В.Ю. Щербань, Н.І. Мурза, А.М. Кириченко, М.І. Шолудько // Вісник Хмельницького національного університету. Технічні науки. – 2016. – № 6(243). – С. 18–21.

11. Scherban V. Basic parameters of curvature and torsion of the deformable thread in contact with runner / V. Scherban, N. Murza, A. Kirichenko, O. Kolisko, M. Sholudko // Intellectual Archive, Toronto: Shiny World Corp., Richmond Hill, Ontario, Canada. – Nov/Des – 2016. – Volume 10. Number 2. – P. 18–23.

12. Scherban V. Kinematics of threads cooperates with the guiding surfaces of arbitrary profile / V. Scherban, N. Murza, O. Kolisko, M. Sheludko, I. Semenova // Intellectual Archive, Toronto: Shiny World Corp., Richmond Hill, Ontario, Canada. – May/June – 2016. – Volume 5.– Number 3. – P. 23–27.

References

1. Svidotstvo № 89242 pro reiestratsiiu avtorskoho prava na tvir. Kompiuterna prohrama dlia realizatsii chyselnykh metodiv / Shcherban V.Iu., Kolysko O.Z., Makarenko Yu.V., Melnyk H.V., Petko A.K., Sholudko M.I., Kalashnyk V.Iu. – Data reiestratsii 03.06.2019 r.

2. Svidotstvo № 89243 pro reiestratsiiu avtorskoho prava na tvir. Kompiuterna prohrama «Prohramnyi kompleks dlia vyznachennia optymalnoi traiektorii nytky na trykotazhnykh mashynakh / Shcherban V.Iu., Kolysko O.Z., Makarenko Yu.V., Melnyk H.V., Petko A.K., Sholudko M.I., Kalashnyk V.Iu. – Data reiestratsii 03.06.2019 r.

3. Kompiuterne proektuvannia system: prohramni ta alhorytmichni komponenty / [V.Iu. Shcherban, O.Z. Kolysko, H.V. Melnyk ta in.]. – K. : Osvita Ukrainy, 2019. – 902 s.

4. Shcherban V.Iu. Optymizatsiia protsesu vzaiemodii nytky z napriamnymy z urakhuvanniam anizotropii fryktsiinykh vlastyvostei / V.Iu. Shcherban, M.I. Sholudko, O.Z. Kolysko, V.Iu. Kalashnyk // Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – 2015. – № 225(3). – S. 30–33.

5. Shcherban V.Iu. Doslidzhennia vplyvu materialu nytky i anizotropii tertia na yii natiah i formu osi / V.Iu. Shcherban, V.Iu. Kalashnyk, O.Z. Kolysko, M.I. Sholudko // Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – 2015. – № 223(2). – S. 25–29.

6. Matematychni modeli v SAPR. Obrani rozdily ta pryklady zastosuvannia / V.Iu. Shcherban, S.M. Krasnytskyi, V.H. Rezanova. – K. : KNUTD, 2011. – 220 s.

7. Scherban V.Yu., Kolisko O.Z., Sholudko M.I., Kalashnik V.Yu. Algorithmic, software and mathematical components of CAD in the fashion industry. K.: Education of Ukraine, 2017. 745 p.

8. Shcherban V.Iu. Efektyvnist roboty kompensatoriv natiahu nytky trykotazhnykh mashyn / V.Iu. Shcherban, N.I. Murza, A.M. Kyrychenko, M.I. Sholudko // Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – 2017. – № 1(245). – S. 83–86.

9. Scherban V. Equalizations of dynamics of filament interactive with surface / V. Scherban, G. Melnik, A. Kirichenko, O. Kolisko, M. Sheludko // Intellectual Archive, Toronto: Shiny World Corp., Richmond Hill, Ontario, Canada. – January/February 2017. – Volume 6. – Number 1. – P. 22–26.

10. Shcherban V.Iu. Porivnialnyi analiz roboty nytkonatiahuvachiv tekstylnykh mashyn / V.Iu. Shcherban, N.I. Murza, A.M. Kyrychenko, M.I. Sholudko // Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – 2016. – № 6(243). – S. 18–21.

11. Scherban V. Basic parameters of curvature and torsion of the deformable thread in contact with runner / V. Scherban, N. Murza, A. Kirichenko, O. Kolisko, M. Sholudko // Intellectual Archive, Toronto: Shiny World Corp., Richmond Hill, Ontario, Canada. – Nov/Des – 2016. – Volume 10. Number 2. – P. 18–23.

12. Scherban V. Kinematics of threads cooperates with the guiding surfaces of arbitrary profile / V. Scherban, N. Murza, O. Kolisko, M. Sheludko, I. Semenova // Intellectual Archive, Toronto: Shiny World Corp., Richmond Hill, Ontario, Canada. – May/June – 2016. – Volume 5.– Number 3. – P. 23–27.

Рецензія/Peer review : 18.09.2020 р. Надрукована/Printed :04.11.2020 р.

Повні вимоги до оформлення рукопису http://vestnik.ho.com.ua/rules/

Рекомендовано до друку рішенням вченої ради Хмельницького національного університету, протокол № 3 від 29.10.2020 р.

Підп. до друку 29.10.2020 р. Ум.друк.арк. 36,51 Обл.-вид.арк. 34,74
Формат 30х42/4, папір офсетний. Друк різографією.
Наклад 100, зам. № _____

Тиражування здійснено з оригінал-макету, виготовленого
редакцією журналу "Вісник Хмельницького національного університету"
редакційно-видавничим центром Хмельницького національного університету
29016, м. Хмельницький, вул. Інститутська, 7/1. тел (0382) 72-83-63

Mon Nov 30 09:15:38 EET 2020, Стецюк Віктор Іванович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 9%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 81593 Название: Метод криптографічного захисту вузлів мережі ZigBee Добавлено в БД: 2020-11-30 Авторы: Супрунюк Ярослав Вікторович Руководители: Горященко Костянтин Леонідович Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	112461	898	2399 (2%)	33 (4%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Имя пользователя:
Kafedra TMIT KhNU

ID проверки:
1005362083

Дата проверки:
04.12.2020 12:21:53 EET

Тип проверки:
Doc vs Internet + Library

Дата отчета:
04.12.2020 12:46:54 EET

ID пользователя:
100005657

Название файла: Супрунюк_ТРм-19-2

Количество страниц: 93 Количество слов: 16839 Количество символов: 122174 Размер файла: 1.10 MB ID файла: 1005654684

1197 слов помечены как "исключенные" и не учитываются в подсчете слов

7.58%
Совпадения

Наибольшее совпадение: 2.34% с Интернет-источником (https://zavantag.com/docs/405/index-1128770.html)

7.28% Источники из Интернета	241	Страница 95
0.54% Источники из Библиотеки	40	Страница 97

0.15% Цитат

Цитаты	3	Страница 98

Не найдено ни одной ссылки

0.01% Исключений

Некоторые источники исключены автоматически (фильтры исключения: количество найденных слов меньш...

0.01% Исключений из Интернета	2	Страница 99

Нет исключенных библиотечных источников

Модификации

Обнаружены модификации текста. Подробная информация доступна в онлайн-отчете.

Замененные символы	41

Завідувачу
кафедри телекомунікацій,
медійних та інтелектуальних
технологій (ТМІТ)
Підченко С.К.
здобувача вищої студента
Супрунюка Ярослава Вікторовича
2 курсу, гр. ТРм-19-2

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

02.12.20 Супрунюк Я. В.

РЕЦЕНЗІЯ

на дипломну роботу студента групи ТРм-19-2

Супрунюка Ярослава Вікторовича

"Метод криптографічного захисту вузлів мережі ZigBee"

Дипломна робота присвячена розгляду питань підвищення криптографічної безпеки передачі інформації між мережі вузлами ZigBee із застосуванням алгоритму еліптичних кривих.

Актуальність теми підтверджується достатньо проробленим питання щодо застосуванням сучасних криптографічних протоколів як симетричних так і асиметричних, існування в галузі криптографічного захисту спеціального напряму криптографії – легковісної криптографії, що направлена на забезпечення обчислювальних задач у системах обмеженої обчислювальної потужності.

В дипломній роботі магістра ставиться та виконується ряд завдань, серед яких:

- розглянуто питання щодо запроваджених криптографічних методів у бездротових телекомунікаційних системах;
- визначено перспективні алгоритми криптографічного захисту інформації, що передаються між вузлами такої мережі;
- розглянуто алгоритми, що використовуються для систем із малою обчислювальною потужністю в ракурсі застосування для обчислювальних систем малої обчислювальної потужності;
- виконано моделювання параметрів модулів передачі із застосуванням криптографічного захисту інформації для модулів мережі ZigBee.

Робота складається з 4-х розділів, загальним обсягом 92 сторінок. В роботі використано 50 посилань на літературні джерела. В роботі 29 рисунків та 7 таблиць.

За змістом робота є цілісною та містить грунтовну кількість посилань на літературні джерела, висновки з отриманих результатів сформовані технічно грамотно.

Викладення матеріалу є послідовним та логічно пов`язаним, застосовується велика кількість ілюстрацій та додатків. Наведені у роботі формули, припущення та висновки мають достатнє обгрунтування та детальне пояснення. Мова викладення роботи є технічно грамотною, зрозумілою та не перенасиченою спеціальними термінами. Оформлення пояснювальної записки знаходиться на належному рівні, граматичних та стилістичних помилок дуже обмежена кількість.

Серед позитивних сторін магістерської роботи слід відмітити наступне:

1. В результаті аналізу, в роботі встановлено, що більшість нових алгоритмів базується на основі симетричного алгоритму AES. Застосування асиметричних алгоритмів є найбільш

надійними, оскільки вони забезпечують захист інформації шляхом використання публічного ключа для шифрування, а приватного ключа для дешифрування інформації. В такому випадку, при втручанні в пристрій передачі, приватний ключ все ще є захищеним, оскільки в самому пристрої не зберігається.

2. Розглянуто алгоритми шифрування в розрізі застосування для обчислювальних систем малої обчислювальної потужності. Для асиметричних алгоритмів основою є виконання алгоритмів на основі роботи з модульною арифметикою. Ці обчислення і обумовлює складність підтримки асиметричних протоколів в системах обмеженої потужності. Один з таких перспективних алгоритмів для легковісної криптографії є алгоритм на основі еліптичних кривих. Виконано обрахунок для 32 та 64 бітного ключа для блоків від 32 до 256 байт. Показано, що навіть 8-бітний контролер здатний забезпечити шифрування.

3. Показано, що виходячи із специфікацій стандартів 802.15.4a та 802.15.4b), визначена ефективна швидкість передачі даних при застосуванні алгоритму шифрування в програмі для 8- та 32-бітного контролера загального призначення. При теоретичній швидкості у 250 кБіт/с, в наслідок неспівпадіння розмірів блоку шифрування та блоку передачі даних, ефективна швидкість буде зменшена.

В цілому дипломна робота магістра Супрунюка Ярослава Вікторовича "Метод криптографічного захисту вузлів мережі ZigBee" повністю відповідає вимогам до кваліфікаційних робіт магістра та заслуговує на оцінку "відмінно", а її автор – на присвоєння кваліфікаційного рівня магістра зі спеціальності 172 – "Телекомунікації та радіотехніка".

Рецензент:
д.т.н., проф., зав.каф. АКІТ Мартинюк В. В.

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ ПО КАФЕДРИ

ТЕЛЕКОМУНІКАЦІЙ, МЕДІЙНИХ ТА ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів ідентичності схожості:

Назва: Методи криптографічного захисту вузлів мережі ZigBee

Автор: Супрунюк Ярослав Вікторович

Спеціальність: 172 Телекомунікації та радіотехніка

Освітня програма Телекомунікації та радіотехніка

Науковий керівник к.т.н., доц. Горященко Костянтин Леонідович

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнуті. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження: Запозичення у розмірі 7.58%, виявлені в роботі містять посилання на відповідні джерела літератури, що використані в роботі. Результати досліджень не містять запозичень. Висновки по роботі є унікальними та також не містять запозичень. Робота приймається до захисту.

02.12.2020 р.

Науковий керівник роботи: К.Л. Горященко

Зав. каф. ТМІТ С.К.Підченко