

Галузь: Електроніка та телекомунікації
Спеціальність: Електроніка
Науковий напрям: Електронні пристрої та системи

Конкурсна робота на тему:

КЛЮЧ ЕЛЕКТРОННИЙ З ФРАКТАЛЬНИМ КОДОМ ДОСТУПУ

Шифр роботи: stone

2020 р.

Анотація

Актуальність роботи: Радіочастотна ідентифікація набула широкого поширення в різних галузях діяльності людини. Враховуючи велику кількість і доступність мікросхем популярних протоколів RFID і дешевих рідерів, широкого поширення устаткування типу цифрових осцилографів, сніферів і спектроаналізаторів, питання підвищення рівня захисту від несанкціонованого отримання даних ключа є актуальним.

Мета роботи: Метою роботи є розроблення трансмітера та транспондера (ключа, мітки) в системі доступу до приміщення з новим способом кодування даних ключа.

Завдання наукової роботи: Запропонувати новий спосіб формування кодів електронного ключа (транспондера).

Методика дослідження: Аналітичний опис кодів, математичне моделювання в програмному середовищі MatLab, практична реалізація макета приладу.

Робота складається з вступу, чотирьох пунктів, висновку та переліку використаної літератури загальним обсягом 17 сторінок. Містить 11 рисунків та 19 джерел літератури.

Передбачувані наукові результати: Нова система доступу із підвищеною захищеністю від зловмисних втручань із фрактальним кодом генерування кодів ключа та способом їх розпізнавання.

Ключові слова: транспондер, трансівер, ключ, кодування, ідентифікація.

Зміст

Вступ

- 1. Принципи роботи радіоміток.**
- 2. Формування фрактального коду доступу в системі доступу.**
- 3. Практична реалізація транспондера.**
- 4. Практична реалізація схеми керування електронного замка.**

Висновок.

Перелік використаної літератури.

Вступ

Радіочастотна ідентифікація (Radio-frequency identification – RFID) використовується, щоб автоматично ідентифікувати і відслідковувати мітки прикріплені до різноманітних об'єктів [1] та будується з використанням RFID читача (трансівера) і мітки (транспондера). Мітка RFID складається з котушки і малих розмірів прийомовідповідача виготовленого у вигляді мікросхеми. Від RFID читача мітка запускається електромагнітним імпульсом запиту, тоді мітка передає назад цифрові дані, які зазвичай являють собою номер або код. На відміну від штрихового коду, мітці не треба бути в межах дії зчитувача. RFID – один з методів автоматичної ідентифікації і отримання даних.

Є два типи міток: пасивні та активні. Пасивні мітки отримують живлення від RFID читача шляхом перетворення енергії електромагнітної хвилі. Оскільки таким чином не можливо передати велику потужність для живлення мітки, їх відстань зчитування обмежена одиницями (в деяких випадках десятках) сантиметрів. Активні мітки живляться від батареї і отже можуть бути прочитані на більшій відстані від RFID читача (до сотень метрів).

Мітки RFID використовуються для обліку, контролю, переміщення у багатьох галузях промисловості, торгівлі, банківській сфері, системах доступу до об'єктів, тваринництві, природоохоронній діяльності та ін [2 - 6]. В певних випадках питання захищеності даних міток має важливе значення [7 - 9].

Метою роботи є розробити транспондер та трансмітер із новою системою генерування кодів ключа та способом їх розпізнавання для підвищення захищеності системи в цілому від зловмисних втручань.

1. Принципи роботи радіоміток.

Існує багато моделей RFID транспондерів популярних стандартів типу Mifare, EMMARINE, TIRIS і т.д. Під них розроблено різного роду емулятори з підтриманням популярних протоколів та різноманітні копіювальники ключів (транспондерів) [10]. Враховуючи велику кількість доступних мікросхем популярних протоколів RFID і дешевих рідерів, широкого поширення

устаткування типу цифрових осцилографів, сніферів і спектроаналізаторів, питання підвищення рівня захисту від несанкціонованого отримання даних ключа є актуальним.

Хорошим плюсом в питанні безпеки серед інших подібних безпроводних систем є сама технологія низькочастотних RFID – вона не дозволяє зчитати код мітки на великій відстані. Пасивні мітки досить малопотужні і мають потребу для свого живлення в досить потужному генераторі зчитувача (трансмітера), особливості поширення радіохвиль на цих частотах також обмежують межі роботи цієї системи. Реальна дальність зчитування транспондерів рідко перевищує 20см для 125 КГц стандартів типу EmMarine (стандартів EM4001, EM4095, EM4097, EM4102, та ін.), для інших протоколів типу Mifare (13,56МГц) може бути більше (1,5 метра для iso15693). Можна досягнути більшої відстані зчитування для низькочастотних рідерів, якщо збільшити розміри котушки і напругу живлення, відповідно і потужність рідера. Проте такі системи громіздкі і як правило їх важко зробити портативними. Беручи до уваги вище сказане приймемо робочу частоту нашої системи 130 КГц, що також спрощує розроблення системи – на низьких частотах знімається багато проблем при проектуванні притаманних високим частотам.

Блок-схема взаємодії між трансмітером та пасивним транспондером показана на рис.1 [10]. Трансмівер генерує в передаючій котушці магнітне поле, яке наводить в котушці транспондера е.р.с., яка випрямляється, фільтрується і застосовується для живлення схеми. Модуляція добротності коливального контуру транспондера призводить до зміни добротності системи зв'язаних коливальних контурів і як наслідок зміни амплітуди генерованих коливань трансмітером. Останній проводить демодуляцію і декодування отриманих даних.

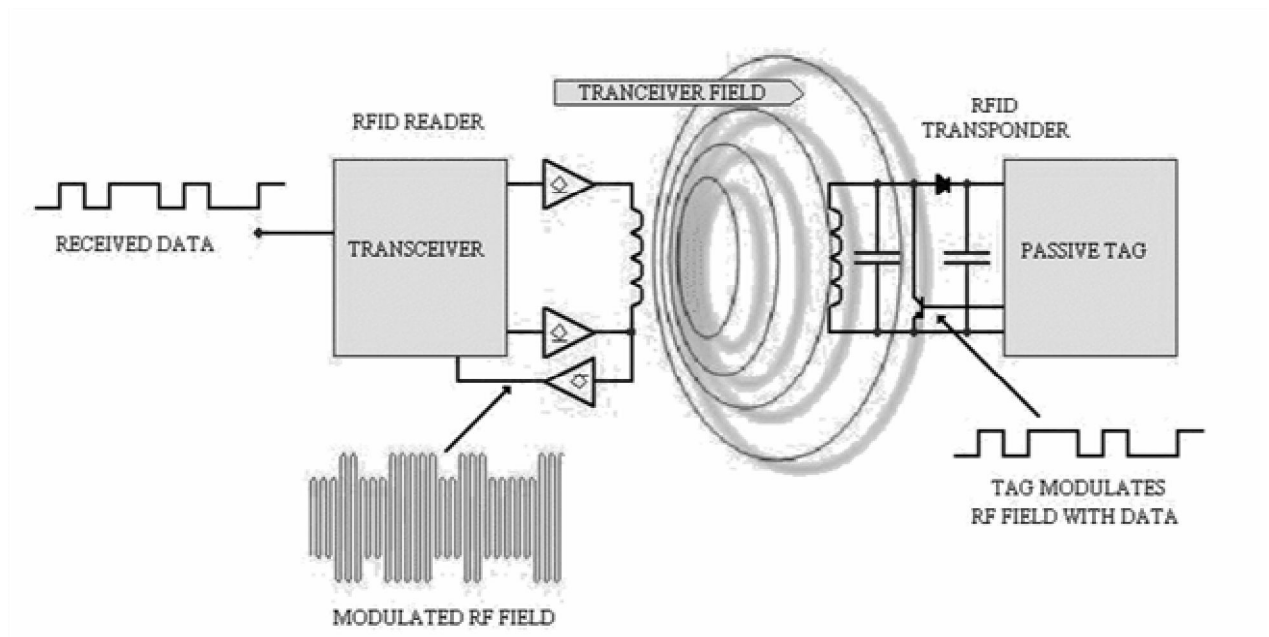


Рис.1 Блок-схема взаємодії між трансмітером та транспондером.

Блок-схема пасивних міток показана на рис.2 [11]. Вона містить наступні блоки: двопівперіодний випрямляч, виділення тактового сигналу, генерації адреси зчитування даних, пам'яті даних, енкодера, модулятора.

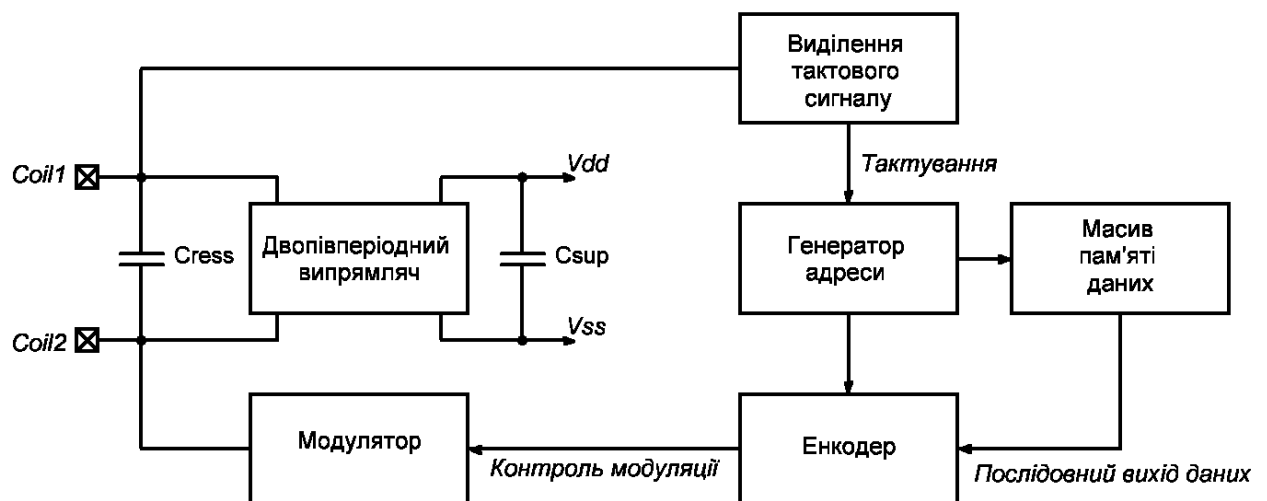


Рис.2 Блок-схема пасивної мітки.

Будується схема мітки у вигляді інтегральної мікросхеми виготовленої за CMOS технологією. Схема живиться від зовнішньої котушки індуктивності в присутності електромагнітного поля. Сигнал для цього випрямляється двопівперіодним випрямлячем. Задаючий генератор адреси зчитування даних

тактується від того ж сигналу через один з виводів котушки. Енкодер проводить кодування бітів зчитаних з пам'яті даних. В залежності від моделі мітки дані можуть передаватися у вигляді манчестерського, двофазного або PSK коду. Здійснюючи модуляцію електромагнітного сигналу модулятором, мікросхема відповідає назад 64 біти інформації які містяться в масиві пам'яті даних. Доступні швидкості передачі одного розряду даних за 64, 32 і 16 періодів носійної частоти.

Підключення зовнішнього фільтрувального конденсатора не вимагається бо схема мітки споживає малий струм. Для функціонування мітки достатньо підключити тільки зовнішню котушку індуктивності. Резонансний конденсатор 78 пФ також інтегральний.

2. Формування фрактального коду доступу в системі доступу.

Достатньо простим в реалізації у вигляді гібридного цифро-аналогового пристрою, що здатний генерувати сигнали зі змінними властивостями є генератор фрактального сигналу показаного на рис.3 [12, 13].

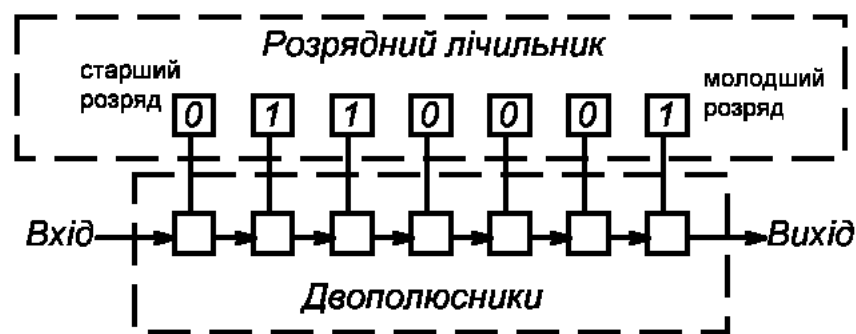


Рис.3 Генератор фрактального сигналу.

Отже це генератор фрактального сигналу з програмованими властивостями, який містить двійковий N - розрядний лічильник. В результаті роботи генератора формується послідовність чисел з періодом повторення 2^N . Працює генератор таким чином. Нехай кожен елемент такого лічильника пов'язаний з двополюсником, який може знаходитися в двох станах. Якщо у відповідному розряді лічильника знаходиться "0", то на виході двополюсника

сигнал рівний $b(1+x)$, де x - вхідний сигнал. Якщо в цьому розряді знаходиться "1", то на виході двополюсника сигнал рівний $-a(1+x)$. Тут " a " і " b " деякі регульовані параметри.

$$x_m = \begin{cases} b(1+x), & C_m = 0 \\ -a(1+x), & C_m = 1 \end{cases} \quad (1)$$

де x_m - сигнал на виході двополюсника, x - сигнал на вході двополюсника, C_m - стан відповідного розряду лічильника.

Усі двополюсники пов'язані в ланцюжок, як показано на малюнку. На вхід цього ланцюжка подається сигнал $x_{in} = b/(1-b)$. На виході такого ланцюжка генеруватиметься сигнал, що описується рекурентним співвідношенням: $x_{2n} = b(1+x_n)$, $x_{2n+1} = -a(1+x_n)$. Тут " n " - дискретний час, відлічуваний лічильником.

Описаний генератор видає сигнал з відомими характеристиками, зокрема, величина розмірності Хаусдорфа $-D$, генерованої послідовності, обчислюється з простого співвідношення: $a^D + b^D = 1$.

Сигнали для передачі "0" і "1" (рис.4, рис.5) формуються в дискретній лінії зв'язку таким чином. Взятий лічильник з розрядністю $N=10$, "0" відповідатиме сигнал з наступними значеннями параметрів $a=0,85$ і $b=0,55$. При передачі "1" $a=0,55$ і $b=0,85$. При цьому розмірність Хаусдорфа D обох сигналів однакова і складає 2,085.

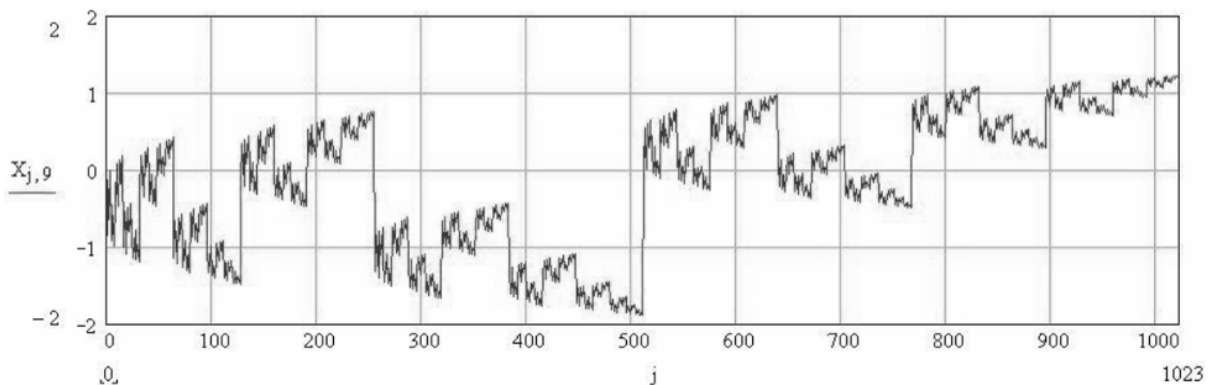


Рис.4 Вихідний фрактальний сигнал "0".

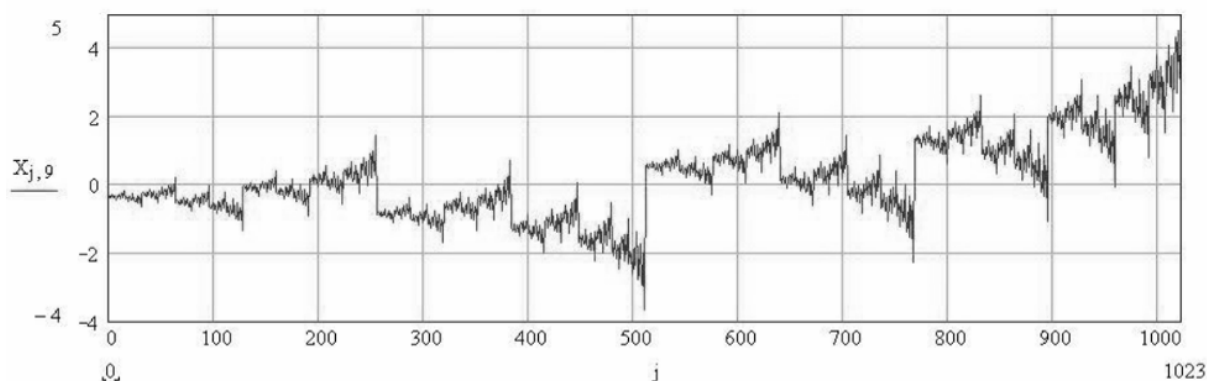


Рис.5 Вихідний фрактальний сигнал "1".

Далі отримані відліки сигналу ми нормуємо та перетворюємо в цифровий код від 0 до 255. Кількість відліків, як видно вище, залежить від розрядності лічильника в генераторі. Маніпулюючи параметрами a та b і розрядністю лічильника N можна формувати множину фрактального коду $X(n)$ розміром від 0 до $2^N - 1$. Мітка (ключ) генерує послідовність $K(n)$ кодів певної довжини l_k (5 байтів). Ця послідовність $K(n)$ фактично є вибіркою з множини $X(n)$ починаючи з позиції p_k (рис.6).

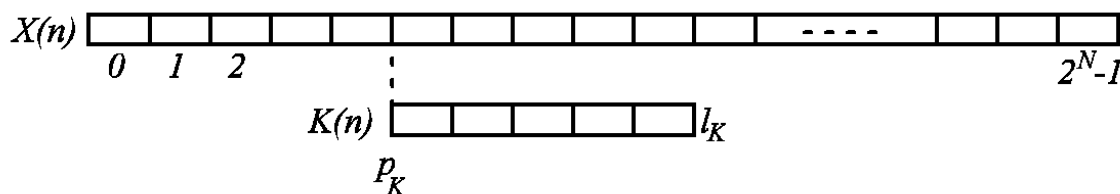


Рис.6 Вибірка коду ключа $K(n)$ з множини $X(n)$.

Генерування починається з 0-го по 5 байтів при кожному наступному опитуванні. Замок сканує ключ на всій множині можливих значень кодів – при співпадині видає сигнал дозволу на відкривання дверей. Також замок запам'ятовує позицію ключа на множині відліків фрактального коду. Якщо позиція не співпадає – то видати попередження. Якщо позиція ключа випереджає позицію записану в замку – є підозра, що проводили маніпуляції з ключем, якщо випереджає позиція замка – проводилися маніпуляції із замком.

Якщо різниця в позиціях велика (наприклад 5 – можна встановлювати програмно) заборонити відкривання і видати сигнал "тривога". Позиція ключа змінюється як в замку так і в ключі під час опитування ключа синхронно.

3. Практична реалізація транспондера.

Схему ключа (транспондера) спроектовано на мікроконтролері [14] (рис.7). Застосовано мікроконтролер молодшого сімейства, RISC архітектури, оскільки схема має бути якомога простішою і містити мінімум радіокомпонентів. Швидкодії при тактовій частоті внутрішнього генератора, ресурсів пам'яті програм та даних цілком достатньо для поставленої задачі. Широкий діапазон напруг живлення (від 2 до 5,5 В) та малий споживаний струм (менше 1 мА) дозволяють його застосувати в розроблюваній схемі.

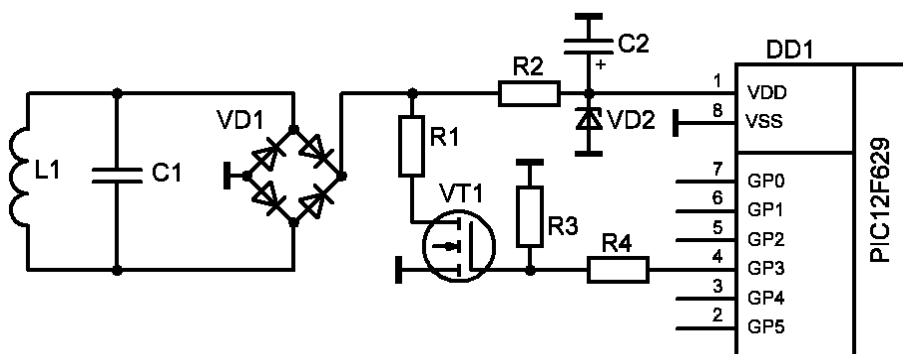


Рис.7 Схема електрична принципова ключа.

Магнітне поле, яке створене прийомопередавачем (трансівером), наводить е.р.с. в котушці індуктивності (L1) коливального контуру (L1,C1). Ця напруга випрямляється діодним мостом (VD1) і через резистор (R2) подається на виводи живлення мікроконтролера (DD1). Ланка R2,VD2 забезпечує стабілізацію напруги на рівні не вище 5 В, оскільки напруга на котушці може сягати більшої величини (до 15 В, залежно від напруги живлення схеми трансмітера). Конденсатором (C2) згладжуються пульсації по шині живлення. Амплітудна модуляція здійснюється транзистором VT1. Для забезпечення модуляції на заданому рівні послідовно з транзистором увімкнений резистор (R1). Керування транзистором здійснюється через резистори R3,R4.

Зменшити кількість елементів в схемі можна за рахунок особливостей схеми самого мікроконтролера [11]. В сучасних мікроконтролерах на кожній ніжці порта введення/виведення присутні обмежувальні діоди, які запобігають перевищенню напруги сигналу на ніжці більше за напругу живлення або нижче рівня напруги загального провідника (рис.8). Ці діоди можуть слугувати як випрямні (рис.9). Отже від випрямного моста можна відмовитися і під'єднати коливальний контур на пряму до ніжок порта мікроконтролера.

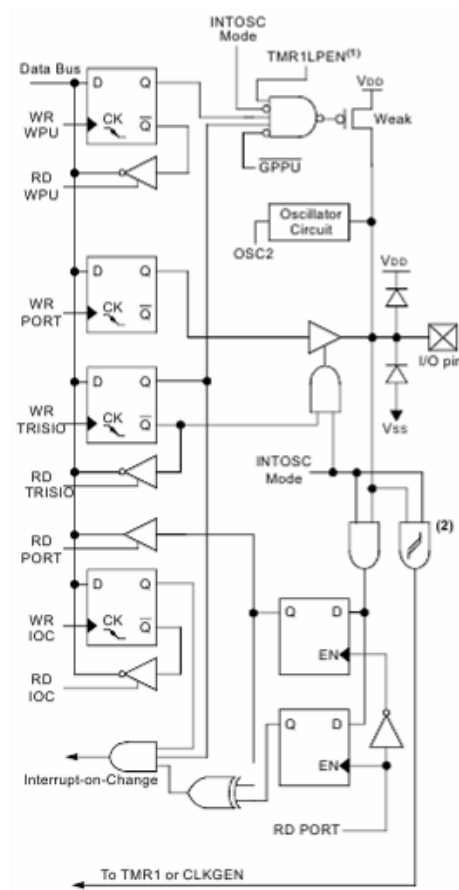


Рис.8 Блок-схема виводів порта мікроконтролера.

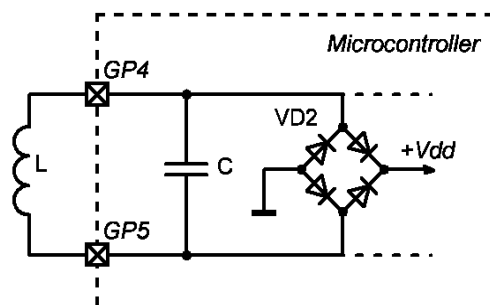


Рис.9 Використання обмежувальних діодів ніжок порта мікроконтролера як випрямних.

На виході порти на ніжках можуть комутувати струми до 20 мА, мають досить потужні як для таких цифрових мікросхем ключові транзистори на виході. Тому можна не застосовувати зовнішній ключовий транзистор. Роль балансного опору для стабілітрона і опором навантаження для ключів ніжок порта виконує активний опір котушки індуктивності. Котушка містить велику кількість витків тонким провідником (намотана на оправі діаметром 50 мм дротом діаметру менше 0,22мм і налічує більше 50 витків). Для тактування використаний внутрішній генератор мікроконтролера на 4 МГц. Остаточна схема транспондера наведена на рис.10.

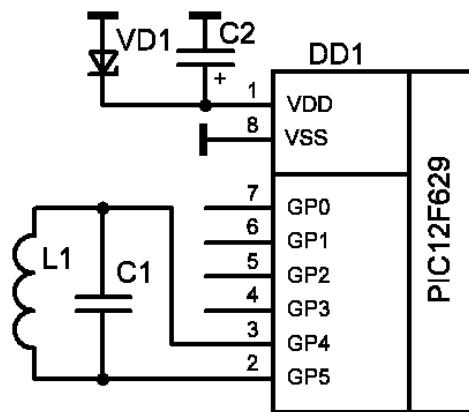


Рис.10 Схема електрична принципова ключа з меншою кількістю радіоелементів.

Алгоритм роботи програми можна побудувати двома способами: проводити обчислення множини кодів ключа $X(n)$ згідно вище описаних формул і вибирати послідовність $K(n)$ коду ключа залежно від позиції ключа p_k ; згенерувати необхідну множину кодів $X(n)$ і записати її в пам'ять мікроконтролера (розмір множини обмежена об'ємом пам'яті мікроконтролера) і потім проводити вибірку послідовності $K(n)$ коду ключа залежно від позиції ключа p_k . Ми вибрали перший спосіб, який дозволить проводити подальші дослідження і змінювати параметри ключів.

Алгоритм роботи програми ключа для мікроконтролера має таку послідовність дій:

1. Зчитуємо позицію ключа p_k та миттєві значення двополюсників з флеш-пам'яті мікроконтролера;
2. Генеруємо сигнал $K(n)$ з кількістю відліків l_k ;
3. Нормуємо відліки сигналу та перетворюємо в двійкові коди з розрядністю 8;
4. Запам'ятовуємо позицію ключа p_k та миттєві значення двополюсників у перезаписувану флеш-пам'ять мікроконтролера;
5. Видаємо код на вихід з передачею бітів манчестерським кодом;

4. Практична реалізація схеми керування електронного замка.

Схема електронного замка для розробленого транспондера спроектована з використанням поширених схемотехнічних рішень [15, 16] і адаптована для нашої розробки. Схема (рис.11) має максимально можливу простоту і дозволяє прочитувати дані транспондера на відстані 2 – 5 см при добре налагоджених контурах.

Трансівер побудований на спеціалізованій мікросхемі EM4095 [17], яка містить в собі необхідні блоки для обміну даними з транспондером. Робоча частота визначається індуктивністю $L1$ та конденсаторами $C6 \div C8, C10$ (в нашій схемі 130 КГц).

Схема виконавчої частини пристрою зібрана на мікроконтролері PIC16F73 [18]. Він проводить обробку даних (вхід "RF") зчитування ключів, взаємодію з клавіатурою, обмін даними через USART протокол (сигнали "RX", "TX") з швидкістю 9600 біт/с (наприклад для підключення до комп'ютера через узгоджувач USB-TTL), видає сигнал на пристрій керування електрозамком (сигнал "TM", вивід інформації на дисплей (OPEN – відкрито, ATEN – увага, ALRT – тривога, номер ключа, та ін.), звуковий сигнал виводиться на ніжку RA5. Дисплей та клавіатура підключені за стандартним загальноприйнятими

схемами. Тактується мікроконтролер від вбудованого тактового генератора, частоту якого задає кварцовий резонатор на 8 МГц. Параметри фрактального коду ключа містяться в флеш-пам'яті (EEPROM) мікроконтролера.

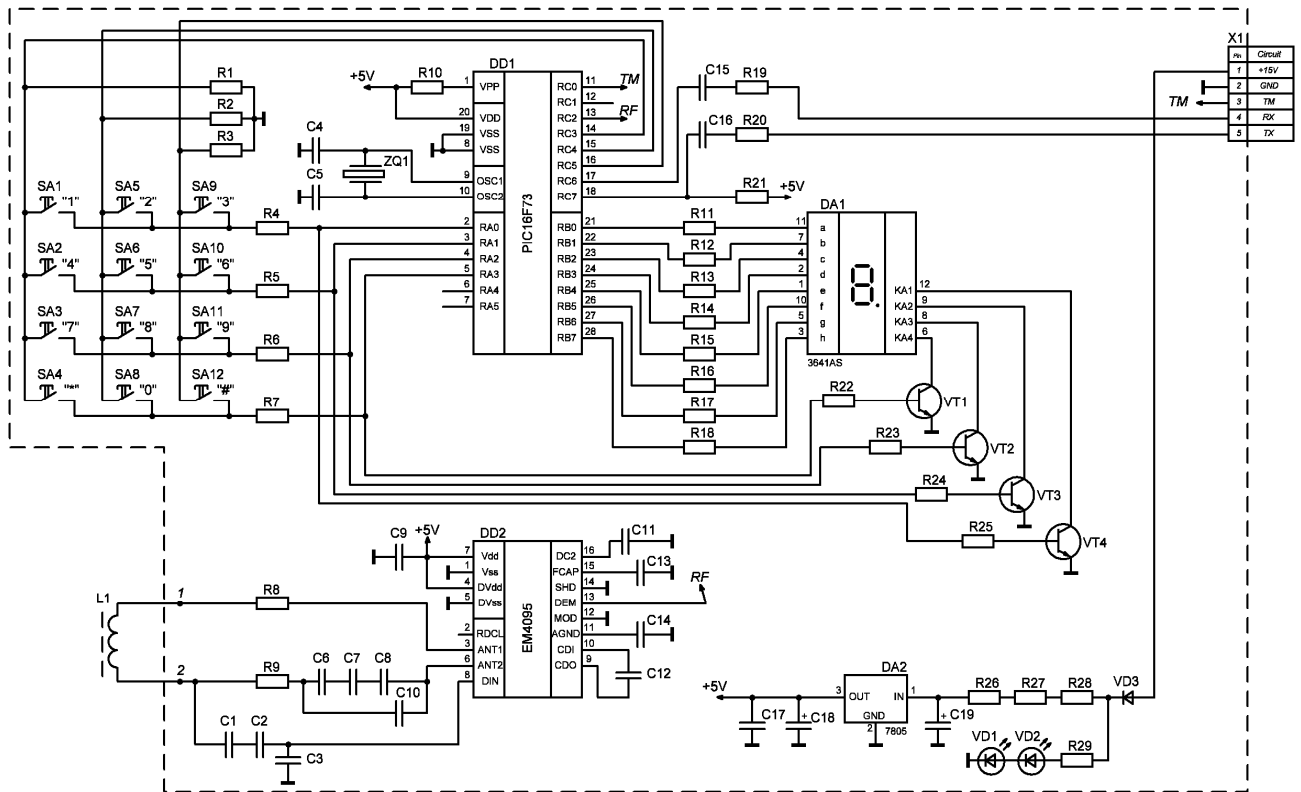


Рис.11 Схема електрична принципова трансівера з виконавчими елементами.

Живлення схеми (+5 В) забезпечується стабілізатором 7805 [19]. Індикація увімкненого пристрою та підсвічування клавіатури здійснюється світлодіодами VD1, VD2. Діод VD3 запобігає виходу з ладу схеми при випадковому підключенні входу живлення за не правильною полярністю.

Схему можна спростити наприклад замінивши мікроконтролер на PIC12F629, і прибрати клавіатуру та дисплей. Основна функція (розпізнавання коду ключа і подавання керуючих сигналів на виконавчі пристрої) залишиться без змін. При цьому необхідно відкорегувати програму мікроконтролера.

Алгоритм роботи програми схеми керування електронного замка:

1. Скануємо ключ (приймаємо біти повідомлення у вигляді манчестерського коду та декодуємо його).

2. Зчитуємо позицію ключа p_k і також запам'ятовуємо її в тимчасову змінну p_{tk} .
3. Зчитуємо миттєві значення двополюсників з флеш-пам'яті мікроконтролера.
4. Генеруємо сигнал $K(n)$ з кількістю відліків l_k .
5. Нормуємо відліки сигналу та перетворюємо в двійкові коди з розрядністю 8.
6. Порівнюємо отримані двійкові дані ключа з розрахованими.
7. Якщо коди співпадають – перейти до п.8, якщо не співпадають – збільшити позицію ключа p_k та перейти до п.4.
8. Запам'ятовуємо позицію ключа p_k та миттєві значення двополюсників у перезаписувану флеш-пам'ять мікроконтролера.
9. Порівняти позиції ключа тимчасову змінну p_{tk} із поточною змінною p_k :
 - якщо $p_{tk} = p_k$ – перейти до п.11;
 - якщо $p_{tk} < p_k$ або $p_{tk} > p_k$ на 1 хід – видати сигнал "попередження" та перейти до п.11;
 - якщо $p_{tk} < p_k$ або $p_{tk} > p_k$ на 3 ходи – видати сигнал "тревога" та перейти до п.1.
10. Подати сигнал на відкривання дверей, зробити затримку на 2 с та перейти до п.1

Висновки

В даній роботі запропонована апаратна реалізація пристрою системи доступу з ключем, що використовує фрактальний код. Застосований новий спосіб формування коду ключа та алгоритм його розпізнавання, що дозволило покращити захищеність такої системи.

Для протидії підбору ключа в схему можна ввести додаткові запобіжні заходи. Зокрема зробити додатково прив'язку до часового зсуву після кожного

розпізнавання, тоді зловмиснику буде не відомо з якого моменту починається множина відліків ключа.

Застосування поширеної елементної бази та протоколів передавання дозволяє використовувати готові рішення з корекцією або заміною керуючої програми контролера за новим алгоритмом.

Через відносно великий об'єм обчислень система не розрахована на підтримання великої кількості ключів з різними фрактальними кодами, що вимагає вдосконалення.

Перелік використаної літератури

1. Miles, Stephen Bell RFID Technology and Applications// London: Cambridge University Press.— 2011.— pp. 6–8
2. "Radio Frequency Identification: Applications and Implications for Consumers".— Ftc.gov. March.— 2005. Що таке RFID-технології, особливості і переваги їх застосування 2019 .— Режим доступу: <http://vikna.if.ua/cikavo/102674/view>
3. "Locating and Marking Products".— 3M Company.— 2012.
4. Зиборов И.А. Применения RFID технологий в деятельности различных субъектах хозяйствования// Молодой ученый.— 2009.— №12.— С. 17-22.
5. Fisher, Jill A., Monahan, Torin "Evaluation of Real-time Location Systems in their Hospital Contexts"// International Journal of Medical Informatics.— 2012, 81 (10): 705–712.
6. Радіочастотна ідентифікація.— Режим доступу: https://uk.wikipedia.org/wiki/Радіочастотна_ідентифікація
7. Ilyas, edited by Syed Ahson, Mohammad RFID handbook: applications, technology, security, and privacy.— Boca Raton: CRC Press. 2008.— 478.p.— ISBN 9781420054996.
8. Butters, Alan "Radio Frequency Identification: An Introduction for Library Professionals"// Australasian Public Libraries and Information Services.— 2006, vol.19 (№4).— pp.164–74.— ISSN 1030-5033

9. Hancke, Gerhard P "Practical eavesdropping and skimming attacks on high-frequency RFID tokens"// Journal of Computer Security.– vol.19 (№2) .– 2011.– pp.259–288.– doi:10.3233/JCS-2010-0407.
10. RFID Reader.– Режим доступа:
<https://www.cnblogs.com/shangdawei/p/3729375.html>
11. RFID Made Easy.// Copyright © 2005, EM Microelectronic-Marin SA .– Режим доступа: www.emmicroelectronic.com
12. Казимиров А.Н. Генератор сверхширокополосного фрактального сигнала для радиотехнических систем связи// Наука ЮУрГУ: материалы 66-й научной конференции. Секции технических наук.– 2014, С.690-693
13. Казимиров А.Н. Радиочастотные и низкочастотные хаотические колебания в устройствах связи// Наука ЮУрГУ: материалы 67-й научной конференции. Секции технических наук.– 2015, С.709-713
14. DS41190G. PIC12F629/675 8-Pin, Flash-Based 8-Bit CMOS Microcontrollers, 2010 Microchip Technology Inc. .– Режим доступа:
<https://ww1.microchip.com/downloads/en/devicedoc/41190c.pdf>
15. PicNic - emulator/spyware for HF RFID// Режим доступа:
<https://www.cnblogs.com/shangdawei/p/4834188.html>
16. Sound card based RFID sniffer/emulator.– Режим доступа:
<https://www.cnblogs.com/shangdawei/p/4834188.html>
17. EM4095. Read/Write analog front end for 125 kHz RFID Basestation.– Режим доступа:
https://www.emmicroelectronic.com/sites/default/files/products/datasheets/em4095_ds.pdf
18. DS30325B. PIC16F7X 28/40-Pin 8-Bit CMOS FLASH Microcontrollers// 2002 Microchip Technology Inc. .– Режим доступа:
<https://ww1.microchip.com/downloads/en/DeviceDoc/30325b.pdf>
19. LM340, LM340A and LM7805 Family Wide VIN 1.5-A Fixed Voltage Regulators.– Режим доступа: <http://www.ti.com/lit/ds/symlink/lm340.pdf>