УДК 621. 3. 011: 621. 314

В.О. Беженар, А.В. Мороз, Т.О. Терещенко, д-р техн. наук.

Цифрова система захисту від атак за струмом споживання

В статье предложена новая система защиты микроконтроллера по току потребления, проведено моделирование системы и показана ее эффективность при детектировании фрагментов алгоритмов по базе данных.

The article presents the new protection system for microcontroller by the supply current. The modeling was provided, and the effectiveness of the system while detecting the parts of algorithms is prooved.

Вступ

Тенденцією сьогодення є покращення зручності життя людини за рахунок перенесення різноманітних сервісів на електронну платформу. В період світової інформатизації, основним об'єктом промислової власності все більше стає саме інтелектуальна власність. Важливим є захист програм від несанкціонованого копіювання, тиражування, використання не за призначенням. Часто фінансовий успіх компанії залежить від надійності захисту мікропроцесорних систем від зчитування та несанкціонованого доступу. Наприклад, успіх компаній платного телебачення напряму залежить від надійності захисту абонентських смарт-карт. В сучасних електронних платіжних картках також використовуються мікроконтролери для зберігання інформації про рахунок клієнта. Бодай один випадок несанкціонованого доступу до такої інформації може коштувати мільйони доларів. Сучасні інтегральні мікросхеми виконані з мільйонів транзисторів, що виконують роль ключів, які комутують сигнали керування та енергію від джерела живлення. Виконання будь-якої інструкції викликає переключення деякої кількості транзисторів, що супроводжується перерозподілом електричного заряду і споживанням струму від зовнішнього джерела та електромагнітним випромінюванням. Таким чином, робота мікроконтролера супроводжується витоком інформації в два зовнішні канали. В той час як електромагнітне випромінення піддається екрануванню, виключити канал зв'язку з джерелом живлення практично неможливо. Для визначення конфіденційної інформації, якою оперує мікроконтролер застосовують простий аналіз струму споживання (SPA), диференційний аналіз (DPA), та диференційний аналіз високого порядку (HO-DPA) [1,2,3]. Кожен наступний тип атаки за струмом споживання потребує більш тривалого дослідження та використання складних статистичних розрахунків однак його ефективність значно зростає відносно попереднього. В той час як простий аналіз струму споживання дозволяє визначити алгоритм програмного забезпечення та аналізувати його на вразливість до інших типів атак, диференційний аналіз високого порядку дає можливість визначити значну кількість мікрокоманд та проводити безпосередній аналіз криптографічних алгоритмів. Головними перевагами атак за струмом споживання є їх низька вартість та гнучкість. Проведений аналіз показав[1], що тільки 10% команд є команди не-операндного типу. І відповідно можливо було б визначити відповідний відсоток команд алгоритму загальної програми, у разі рівномірності використання всіх команд в алгоритмі. Окрім цього на струми споживання впливає також послідовність виконання команд, тому що в мікроконтролерах AVR є конвеєр, який здійснює вибірку та декодування наступної команди при виконанні поточної. Оскільки у реальних програмах асемблерні команди містять операнди, команди розгалуження та переривання, один тільки аналіз струму споживання у системі з реальним складним алгоритмом у загальному випадку не може бути використаний для отримання цілком усієї програми мікроконтролера, однак даний метод може бути використаний для дослідження алгоритму програми на наявність певних шаблонів програмування - деякої послідовності команд, що відповідають відомому алгоритму. Наприклад, більшість програмних реалізацій таких алгоритмів як DES, AES, RSA та ін. мають схожу структуру. Якщо створити базу даних шаблонів реалізацій таких алгоритмів шифрування, можливо визначити, який алгоритм шифрування використовується у досліджуваній системі, щоб надалі використовувати слабкі місця даного алгоритму.

У роботі [3] було показано, що при зчитуванні струму споживання мікроконтролера, можна дізнатися вагу Хеммінга бітів на шині даних, що переключаються. Також було показано, що при виконанні алгоритму шифрування DES можна значно зменшити діапазон пошуку секретного ключа шифрування. Цей напрям дослідження передбачає вивчення реакцій мікропроцесорної системи на певний зовнішній вплив для отримання додаткових відомостей, що дозволяють аналізувати конфіденційні дані системи, такі як

паролі, коди доступу, ПІН-коди. Але у більшості сучасних систем при переборі паролю при декількох неправильних спробах система блокується. Це, звичайно, дещо звужує діапазон використання даного методу дослідження, але все-ж таки він може бути використаний при аналізі струму споживання в тих системах, де введення неправильного паролю не приводить до блокування. Наприклад, у бездротових мережах, введення неправильного паролю доступу не призводить до блокування відправника, а отже метод аналізу струму споживання може бути використаний для прискорення перебору паролю у таких системах. Наприклад, у статті [4] наведено практичну реалізацію зчитування секретного ключа з мікросхеми шифрування даних MicroChip KeeLoq. Даний чіп використовується у різних захисних системах, наприклад у системах авто-сигналізації, у системах радіочастотної ідентифікації та контролю доступу. За допомогою атаки за струмом споживання вдалося зчитати секретний ключ системи контролю доступу та створити дублікат такого ключа.

Таким чином, аналіз струму споживання мікроконтролера може використовуватися для комбінованого дослідження, що об'єднує наведені напрямки.

З огляду на вищенаведене, важливим стає захист інформації від зчитування за струмом споживання. Запропонована система захисту дозволяє значно ускладнити зчитування інформації за струмом споживання у мікропроцесорних системах.

1. Огляд існуючих систем захисту мікроконтролерів від зчитування за струмом споживання

Системи захисту від атак за струмом споживання призначені для ускладнення та унеможливлення отримання корисної інформації зі струму споживання. Існуючі системи мають різні параметри та характеристики і можуть бути використані в мікропроцесорних системах в залежності від потреби забезпечення необхідного ступеня захисту при відповідності наявним технологічним вимогам. Основною проблемою більшості високоякісних систем захисту є складність їхньої інтеграції в мікроконтролери з обмеженим розміром кристалу.

Всі системи захисту від атак за струмом споживання можна розподілити на три типи:

- такі, що зменшують корисний сигнал, який може бути доступним через виводи живлення.
- системи, що вносять додатковий струм споживання спотворюючи при цьому корисний сигнал
- непрямі методи живлення мікроконтролерів, що поділяються на:

а) тимчасові (працюють на певному етапі роботи мікроконтролера, або відповідно до потреб програмного забезпеченя)

б) неперервні (працюють протягом всього часу роботи мікроконтролера)

Перший тип систем захисту реалізується як апаратно так і програмно. При програмній реалізації алгоритм програми будується таким чином, щоб обробка захищених даних виконувалась з розподілом в часі або супроводжувалась хибними розрахунками. Також програмним методом є реалізація генератора шуму, однак такі системи суттєво знижують ефективність програмного забезпечення зменшуючи його швидкодію та збільшуючи об'єм пам'яті, що воно займає.

Апаратні системи першого типу базуються на згладжуванні струму споживання за рахунок використання нелінійних елементів та фільтрів. Найпростіша система захисту [4] першого типу складається зі згладжуючого фільтра, що може відключатися від джерела живлення. Вдосконаленням такої системи є використання послідовного та паралельного з'єднань фільтрів, а також матричного включення та введення зворотних зв'язків між фільтрами. При цьому керування такою структурою здійснюється від таймера або генератора випадкових чисел. Таке виконання системи захисту забезпечує не тільки згладження струму споживання, а й внесення в нього додаткових флуктуацій за рахунок перехідних процесів при переключенні фільтрів. Складність реалізації цієї системи полягає у проблемах інтегрального виконання індуктивностей та ємностей, для забезпечення заданих частотних характеристик.

Система захисту, що використана в пристрої [5] поєднує в собі програмний та апаратний захист. Вхідний конденсатор великої ємності забезпечує фільтрацію струму споживання та дозволяє підтримувати роботу процесора деякий час після відключення живлення щоб виконати операцію стирання пам'яті, у випадку виникнення збою при виконанні обчислення з захищеними даними. Як було зазначено раніше існує складність інтегрального виконання реактивних елементів, тому застосування систем захисту, що мають в своєму складі індуктивності та ємності досить обмежене.

Другий тип систем захисту характеризується наявністю інтегрованого блоку, що дає можливість накладання на реальний струм споживання додаткового зазвичай хаотичного шуму. Типовою є система захисту на основі блоку

ключів [6]. Система керування на основі генератора випадкових чисел, що виконується на основі „шумлячого" діода представляє його вихідний шум бінарною послідовністю. Ваона надходить на виводи керування ключами та забезпечує їхнє ввімкнення-вимкнення. Комутація блоку ключів супроводжується споживанням струму при перехідних процесах та додає певний рівень постійної складової струму. В залежності від системи керування блок ключів може виконуватися з ідентичним опором або з певною залежністю, що дає можливість змінювати додатковий струм споживання в широкому діапазоні. Реалізація такої системи захисту супроводжується суттєвим зменшенням корисної площі кристалу, яка є критичним параметром для багатьох мікроконтролерів.

Найпоширенішими є системи захисту *третього типу*, що додатково можуть містити попередньо розглянуті структури. Найпростіші системи такого типу [7,8,9] призначені для тимчасового від'єднання внутрішніх елементів мікроконтролера від зовнішнього джерела живлення, функціонування яких підтримується за рахунок накопиченої енергії. Типовою системою захисту, що забезпечує тимчасову захисну дію є система [8]. Вона має вхідний ключ, що перемикає живлення мікроконтролера між накопичуючим конденсатором та зовнішнім джерелом. Перемикання здійснюється або з певним періодом, або в залежності від підпрограми, що виконується. Тобто ця система дозволяє виконувати обчислення з використанням криптографічних даних від заряду накопиченого в конденсаторі, в той час як без необхідності пристрій споживає енергію від зовнішнього джерела. Пристрої захисту [8,9] є вдосконаленнями попереднього і характеризуються ускладненням структури ключів та конденсаторів та алгоритму їхньої роботи. Це дозволяє суттєво зменшити час протягом якого можливе проведення атаки. Однак збільшення ефективності подібних схем супроводжується значним збільшенням їх розміру.

Найкращим прикладом неперервної системи захисту третього типу є незалежне джерело живлення на основі двох конденсаторів [10]. Виводи живлення мікроконтролера через ключі під'єднано до вхідних конденсаторів достатньої з ємністю достатньою для тимчасової роботи мікроконтролера (виконання підпрограми). Через ключі, що працюють в протифазі з вхідними конденсатори з'єднані з внутрішніми ланцюгами. За рахунок періодичного переключення ключів живлення центрального процесора та периферійних пристроїв постійно відбувається від одного з конденсаторів в той час як інший заряджається від зовнішнього джерела.

2. Запропонована система захисту мікроконтролера від зчитування за струмом споживання

З огляду на наведені недоліки існуючих систем захисту мікроконтролерів від зчитування за струмом споживання, була розроблена нова система захисту, в якій запропоновано покращення характеристик захищеності від зчитування за струмом споживання.

Систему захисту виконано на основі додаткового процесорного ядра, яке виконує команди з пам'яті мікроконтролера. Це дозволяє замінити два блоки: аналоговий ГВЧ та цифровий блок ключів одним цифровим пристроєм та виключити з топографії мікроконтролера аналогову схему ГВЧ. Додаткове ядро є програмованим пристроєм, і тому дозволяє використовувати алгоритми ГВЧ різної складності в залежності від потрібного ступеня захищеності, що дає можливість оптимізувати швидкодію мікроконтролера. Зв'язок основного ядра з допоміжним дозволяє використовувати динамічні дані, якими оперує мікроконтролер та використовувати їх в алгоритмі ГВЧ, що значно поліпшує характеристики алгоритму. Так, використання лише одного байту динамічних даних дає можливість збільшити період програмного алгоритму ГВЧ в 2^8 = 256 разів, або використовувати більш прості швидкодіючі алгоритми ГВЧ, а отже і більшу тактову частоту центрального процесора (ЦП).

На рис.1 зображено структурну схему мікроконтролера із запропонованою системою захисту.

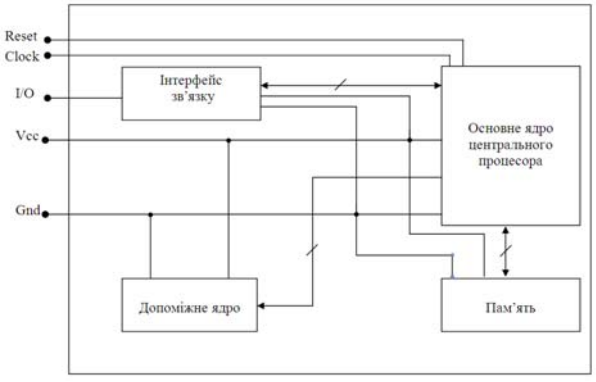

Рис.1. Мікроконтролер з системою захисту

Мікроконтролер містить інтерфейс зв'язку, що забезпечує обмін даними ЦП із зовнішніми пристроями, та пам'ять, в якій зберігаються конфіденційні дані. Зв'язок мікроконтролера із зовнішніми пристроями здійснюється через порти інтерфейсу зв'язку „I/O", сигнали синхронізації „clock", „reset", виводи живлення „Vcc" і „Gnd".

Через інтерфейс зв'язку ЦП отримує інструкції для виконання певних дій щодо оперування даними. Результат виконання повертається через інтерфейс зв'язку до зовнішніх пристроїв. До виводів живлення мікроконтролера „Vcc" і „Gnd" паралельно під'єднано допоміжне процесорне ядро, що виконує функцію системи захисту від аналізу струму споживання. Використовуючи дані з пам'яті, додаткове ядро виконує команди, забезпечуючи при цьому внесення додаткових флуктуацій у струм споживання мікроконтролера в цілому. За рахунок зв'язку між основним та допоміжним ядром та пам'яттю досягається також вибір „зерна" (числа, що є основою програмних алгоритмів ГВЧ) алгоритму генерації ГВЧ з динамічно змінних даних пам'яті, що можуть змінюватися під час обчислень, суттєво збільшуючи період алгоритму, а отже, і ступінь захищеності мікроконтролера.

3. Математичне моделювання системи захисту та дослідження її ефективності

Для дослідження ефективності запропонованої системи захисту проведено математичне моделювання. На попередньому етапі отримують оцифровані за допомогою цифрового осцилографа струми споживання мікроконтролера при виконанні заздалегідь відомих команд, та зберігають їх у базі даних. Електрична принципова схема експериментальної установки наведена на рис.2. Установка містить мікроконтролер ATTiny12, датчик струму на резисторі, допоміжний світлодіод для індикації поточного номеру програми, та кнопку скидання.

Блок-схему алгоритму програмного забезпечення мікроконтролера наведено на рис.3. Алгоритм складається з 16 підпрограм, при чому перехід на наступну підпрограму виконується при натисканні кнопки RESET. Кожна підпрограма являє собою цикл, в якому виконуються спочатку команди встановлення та скидання біту порта (цей сигнал використовується для синхронізації), та досліджуваної команди.

У лістингу 1 наведений асемблерний код тестових програм для мікроконтролера. Для прикладу узято підпрограми, що циклічно виконують команди BREQ та SUB.

Лістинг 1

```
prog_7:
    Sez
l_prog_7:
    cbi PORTB,2
    sbi PORTB,2
    breq    l_prog_7
    rjmp    l_prog_7

prog_12:
    ldi  r25,0xFF
    ldi  r26,0x01
l_prog_12:
    cbi PORTB,2
    sbi PORTB,2
    subr25,r26
    rjmp    l_prog_12
```

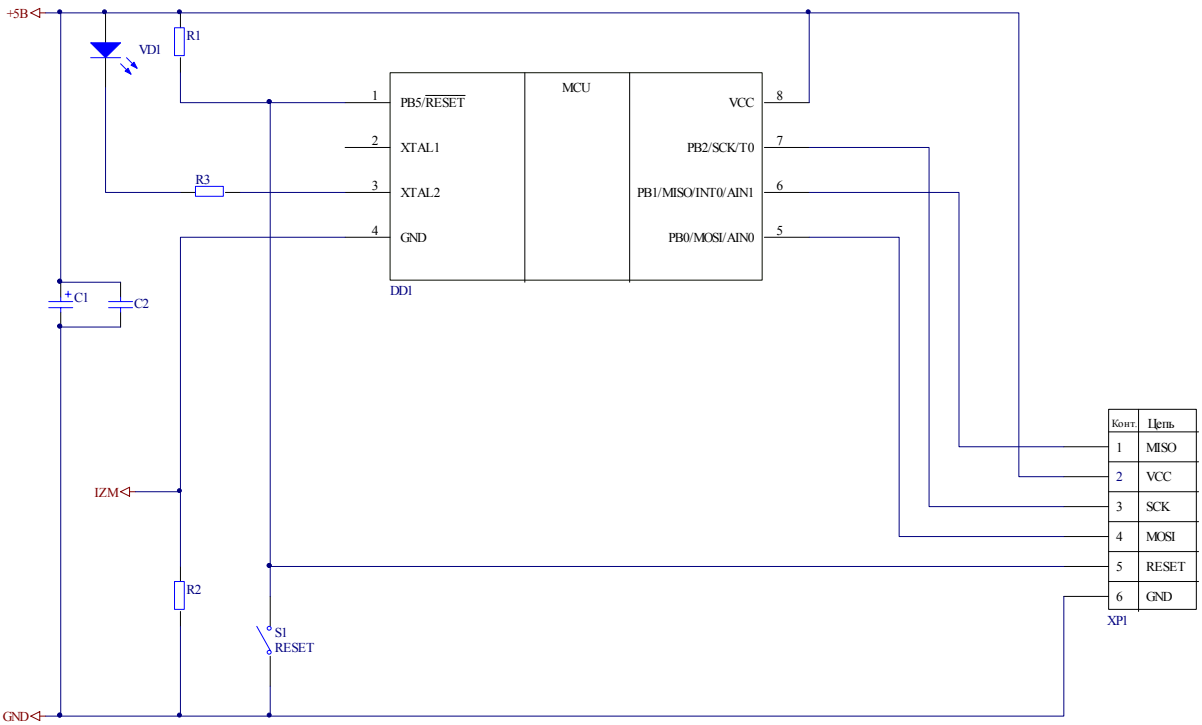

Рис.2. Схема електрична принципова експериментальної установки

На наступному етапі дослідження, струми команд з бази даних порівнюють між собою за допомогою коефіцієнта взаємної кореляції. В тому випадку, якщо коефіцієнт кореляції лежить в діапазоні 0.9..1.0, вважається що два струми схожі між собою. Таким чином, вдалося показати, що при зчитуванні струму споживання мікроконтролера можливо виділити до 62% команд із загального потоку команд у програмі. Детальна методика отримання оцифрованих струмів споживання мікроконтролера описана окремо [1,2,3].

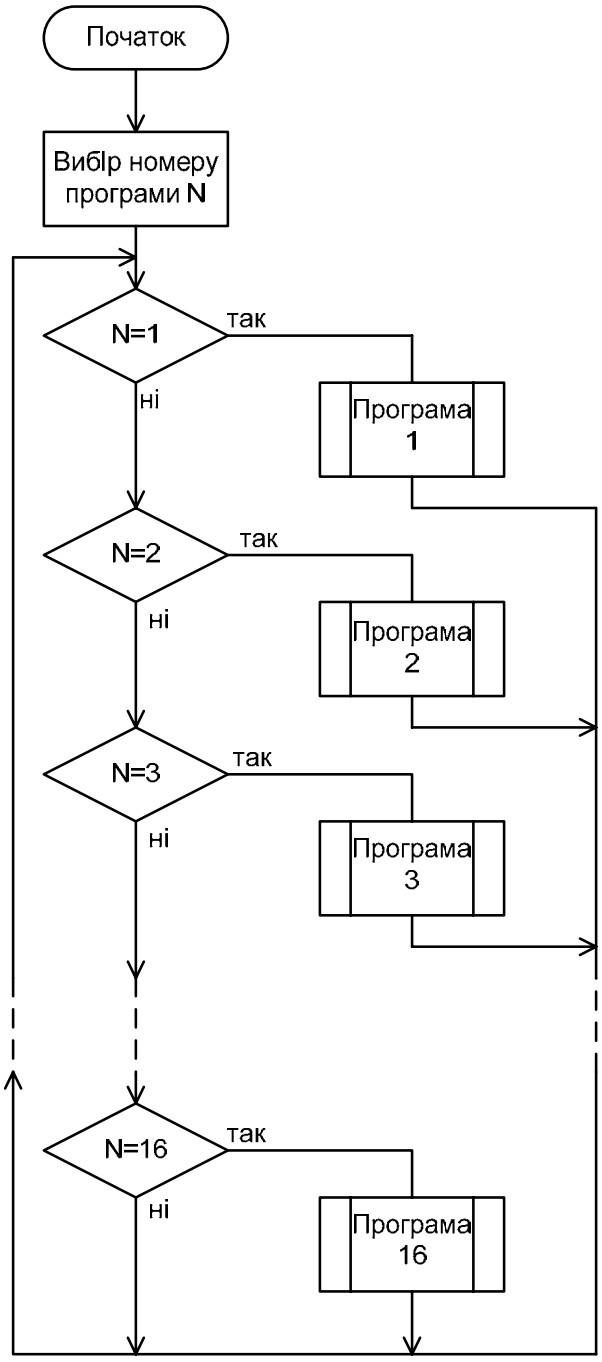

Рис.3. Алгоритм тестового програмного забезпечення мікроконтролера

Для дослідження перспективності покращення захисту мікроконтролера за допомогою системи, що генерує додаткові хибні команди, була використана наступна методика: З бази даних узято два струми споживання (для прикладу, струми споживання команд BREQ та SUB) та накладені між собою. У результаті отримуємо сумарний струм споживання двох команд, так, якби ці команди у мікроконтролері виконувалися паралельно. Далі цей сумарний струм споживання порівнювався за допомогою коефіцієнта взаємної кореляції зі струмами інших команд, зокрема зі струмами вихідних команд, з яких він був складений. Результати порівняння зведені в Таблицю 1. У верхньому рядку та у правому стовпчику наведено назви асемблерних команд, запис про струм споживання яких міститься у базі даних струмів. На перетині рядків та стовпчиків міститься значення коефіцієнта взаємної кореляції при порівнянні даних двох команд.

Таблиця 1

BREQ	SUB	BREQ+SUB	
0,909	-0,320	0,768	**CPI**
0,986	-0,653	0,501	**BREQ**
0,992	-0,719	0,416	**BRNE**
0,922	-0,326	0,777	**CP(Z=1)**
-0,712	0,988	0,241	**CP(Z=0)**
-0,676	0,991	0,289	**BRCC**
0,965	-0,508	0,623	**BRCS**
0,145	0,566	0,827	**CPSE**
-0,693	0,980	0,255	**MOV**
0,992	-0,677	0,463	**LDI**
0,984	-0,711	0,414	**CLZ**
0,990	-0,679	0,458	**ROL**
0,991	-0,681	0,457	**ROR**
0,905	-0,305	0,779	**SWAP**
-0,279	0,349	0,051	**ADD**
-0,653	0,984	0,329	**SUB**
0,950	-0,444	0,677	**CLR**
-0,513	0,973	0,473	**SER**
0,984	-0,553	0,594	**COM**
-0,477	0,969	0,513	**NEG**
0,552	0,236	0,957	**BRMI**
0,348	0,447	0,944	**BRPL**
0,213	0,527	0,868	**NOP**
0,977	-0,515	0,629	**SEC**
0,968	-0,488	0,648	**CLC**
0,975	-0,526	0,614	**SEZ**
0,501	0,329	0,914	**BREQ+SUB**

Коефіцієнт автокореляції (порівняння команди з собою) для однієї і тієї самої команди менше за 1, оскільки при обчисленні, для отримання більш достовірного результату, були використані значення струмів споживання, рознесені у часі. Так, коефіцієнти автокореляції для команд BREQ та SUB складають відповідно 0.986 та 0.984, що означає високу імовірність виділення даних команд з потоку при детектуванні у реальній системі. За рахунок накладання команд BREQ та SUB між собою, моделюється поведінка системи захисту, у якій струм споживання мікроконтролера, що виконує основну програму, буде накладатися на струм споживання додаткового захисного мікроконтролера. Обчислення коефіцієнту взаємної кореляції між отриманою сумарною послідовністю BREQ+SUB та струмами вихідних команд BREQ та SUB, дає числові значення 0.501 та 0.329 відповідно, що означає зменшення імовірності детектування вищенаведених команд у пристрої з системою захисту. Таким чином, система захисту із паралельним підключенням захисного мікроконтролера до шини живлення, дозволяє реально зменшити імовірність детектування команд, і тим самим покращити захист мікроконтролера від зчитування за струмом споживання. Реалізація додаткового захисного мікроконтролера може бути різною, в залежності від наявних ресурсів. Одним з варіантів реалізації може бути підключення зовнішнього мікроконтролера до шини живлення основного. Однак у даному випадку необхідно передбачити неможливість фізичного відключення захисного мікроконтролера. Це можливо досягти при використанні спеціальних корпусів із захисними пристроями, що знищують секретну інформацію при відкритті корпуса. Можливо також розподіляти основний алгоритм програми між основним та допоміжним ядром, і налаштувати обмін інформацією між ними, а у разі несанкціонованого доступу забезпечити знищення програмного пакету. Іншим варіантом виконання запропонованої системи захисту може бути використання двохядерних мікрокопроцесорів та мікроконтролерів. При цьому одне ядро буде використовуватись для виконання корисної програми, а інше ядро буде задіяне для виконання програми захисту. Ще одним з можливих варіантів реалізації системи захисту при реалізації пристрою на платформі ASIC є реалізація захисного мікроконтролера за допомогою вбудованої PLD-області. Слід також зазначити, що сьогодні можливе виготовлення фірмами-виробниками мікроконтролерів на замовлення, з необхідною конфігурацією вбудованих пристроїв та програмним забезпеченням. Тому, у пристроях із захистом інформації, коли собівартість даного пристрою відходить на другий план перед його захищеністю, реалізація додаткового захисного ядра процесора на одному кристалі є цілком можливою і оправданою. Ще одним можливим варіантом реалізації системи захисту від атак за струмом споживання є використання одноядерного мікроконтролера з програмою, що випадково маніпулює внутрішніми ресурсами – наприклад, включення та відключення АЦП, компаратора, підтягуючих резисторів на портах. Це призводить до введення додаткового випадкового шуму до струму споживання мікроконтролера, а отже значно ускладнює аналіз струму споживання.

Висновки

1. Запропонована система захисту від зчитування за струмом споживання дозволяє покращити захищеність мікропроцесорного пристрою за рахунок введення до струму споживання струмів додаткових команд, яку не несуть інформації про виконувану програму, а лише ускладнють аналіз струму споживання.

2. Збільшення кількості додаткових команд дозволяє підвищити захищеність мікропроцесорної системи, оскільки кожного разу на одну і ту саму команду реальної програми припадають різні команди програми захисту.

3. Введення додаткових команд захисного мікроконтролера зменшує коефіцієнт кореляції при детектуванні команд основного мікроконтролера з 0.986 та 0.984 до 0.501 та 0.329, що суттєво знижує імовірність несанкціонованого зчитування команд за струмом споживання, а отже, покращення захищеності мікрокопроцесорної системи в цілому.

4. Виконання запропонованого пристрою захисту можливо за допомогою двохядерних мікроконтролерів та мікропроцесорів. При цьому одне ядро буде виконувати основну програму, а друге – захисну програму. Реалізація такого пристрою захисту є цілком можливою і оправданою.

Література

1. *Мороз А.В.* Визначення рівня захищеності програмного забезпечення мікроконтролерів за методом аналізу струму споживання // Электроника и связь. Тем. выпуск "Проблемы электроники". ч.1. - 2008. - №1-2. - С.238-241.
2. *Мороз А.В.,* Терещенко Т.О. Дослідження захищеності програмного забезпечення мікроконтролерів за струмом споживання // Технічна електродинаміка. Тем. випуск "Проблеми сучасної електротехніки".ч.2.- 2008.-С.99-102.

3. *P. Kocher*, J. Jaffe, B. Jun, "Differential Power Analysis" Crypto 99 Proceedings, Lecture Notes In Computer Science Vol. 1666, M. Wiener, ed., Springer-Verlag, 1999.
4. *Thomas* Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani. "Physical Cryptanalysis of KeeLoq Code Hopping Applications". Ruhr University of Bochum, Germany. http://eprint.iacr.org/2008/058.pdf.
5. *Пат*. WO 02/09030, 31.01.2002. Data-processing arrangement comprising confidential data. PAUTOT, Fabrice.
6. *Пат.* US 6419159 США, 16.07.2002. Integrated Circuit Device With Power Analysis Protection Circuitry. Odinak G.
7. *Пат*. US 6748535 США,8.01.2004. System and method for suppressing conducted emission by a cryptographic device comprising an integrated circuit. Frederic W. Ryan, Monroe A. Weiant, Edward J. Twarog.
8. *Пат.* US 6848619 США, 1.02.2005. Microcontroller protected against power attack. Robert Leydier.
9. *Пат.* US 2002/0010872 США, 24.01.2002. Data carrier for the adaptation of a consumption time interval to the power consumption of the data carrier. Peter Thueringer, Klaus Ully, Marcus Feuser.
10. *Пат*. EP 1113386 Европа, 23.12.2000.Protecting smart cards from power analysis with detached power supplies. Shamir, Adi Rehovot.