МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

КОНЦЕВИЧ Олег Олегович

Алгоритми протидії атакам на побічні канали електроживлення / Countering attacks algorithm for secondary power supply channels

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
О.О. Концевич

Науковий керівник
к.т.н., доцент Н.Г.Яцків

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2022 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2022

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь "магістр"
спеціальність:125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
"____"_____20__ р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
КОНЦЕВИЧ Олег Олегович

(прізвище, ім'я по-батькові)

1. Тема кваліфікаційної роботи
Алгоритми протидії атакам на побічні канали електроживлення / Countering attacks algorithm for secondary power supply channels
керівник роботи: к.т.н., доц. Н.Г.Яцків

затверджені наказом по університету 31 грудня 2021 року № 606

2. Строк подання студентом закінченої кваліфікаційної роботи
16 листопада 2022 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити

– огляд та аналіз інтегральних схем як основного програмно-апаратного засобу для захисту інформації;

– коротка характеристика атак по побічним каналам;

– розробка математичної моделі «витоку» інформації з ланцюга електроживлення та загальної будови вимірювальної установки;

– обгрунтувати вибір апаратного забезпечення;

– реалізувати табличне перетворення S-box на мікроконтролерах Atmel з використанням підходу «читання зі зміщенням»..

5. Перелік графічного матеріалу у роботі.

Діаграма математичних сподівань і СКВ значень відліку для різних ваг Хеммінга.

Блок-схема АЦП конвеєрного типу.

Етапи виконання інструкції для «простої команди» мікроконтролером Atmel ATmega 16.

Форма сигналу, що характеризує енергоспоживання мікроконтролера Atmel при виконання операцій «nop».

Форми сигналу до та після вирівнювання флуктуацій.

Гістограми розподілу значень 1938-го відліку.

Дві форми сигналу, на яких 1938-й відлік має максимальне (суцільна лінія) та мінімальне (пунктирна лінія) значення.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання: 11 жовтня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Огляд фізичних та теоретичних основ побічних атак по каналах електроживлення	12.2021 р. – 03.2022 р.	
2	Математичні моделі побудови побічних атак за ланцюгами електроживлення	03.2022 р. – 05.2022 р.	
3	Розробка і дослідження моделі побічних атак на основі енергоспоживання	05.2022 р. – 11.2022 р.	

Студент _____ Концевич О.О.
(підпис)

Керівник роботи _____ к.т.н., доц. Яцків Н.Г.
(підпис)

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Алгоритми протидії атакам на побічні канали електроживлення” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека” освітньо-професійної програми «Кібербезпека» написана обсягом 76 сторінок і містить 22 ілюстрації, 3 таблиці, 1 додаток та 34 джерела за переліком посилань.

Метою випускної кваліфікаційної роботи є розробка алгоритмів протидії атакам на побічні канали електроживлення.

Методи дослідження. Математичні методи моделювання, методи розрахунку електричних кіл, методи ідентифікації, методи програмно-апаратної реалізації.

Результати дослідження: Здійснено аналіз існуючих інтегральних схем як основного програмно-апаратного засобу для захисту інформації, що дало змогу охарактеризувати фізичні основи побічних атак по ланцюгах електроживлення. Розроблено математичні моделі «витоку» інформації з ланцюга електроживлення, що дозволило встановити загальну будову вимірювальної установки та обґрунтувати варіанти вибору апаратного забезпечення. Досліджено та проаналізовано характеристики основних форм сигналу, що дозволило розробити відповідні рекомендації для захисту від атак на побічні канали електроживлення. Розроблено схему загальної будови вимірювальної установки та реалізовано табличне перетворення S-box на мікроконтролерах Atmel з використанням підходу «читання зі зміщенням».

Результати роботи можуть успішно застосовуватися для протидії атакам на побічні канали електроживлення.

Ключові слова: ПРОТИДІЯ АТАКАМ, ПОБІЧНІ КАНАЛИ, ЕЛЕКТРОЖИВЛЕННЯ, МІКРОКОНТРОЛЕР, ТАБЛИЧНЕ ПЕРЕТВОРЕННЯ.

ABSTRACT

The graduate work on the topic „Countering attacks algorithm for secondary power supply channels” for Master’s degree on speciality 125 "Cybersecurity " is written on 76 pages and contains 2 illustrations, 3 tables, 1 suplement and 34 references.

The aim of graduate work is to develop algorithms for countering attacks on side channels of power supply.

Research methods. Mathematical modeling methods, electrical circuit calculation methods, identification methods, hardware and software implementation methods.

Results of the study: An analysis of existing integrated circuits as the main software and hardware means for information protection was made, which made it possible to characterize the physical basis of side attacks on power supply chains. Mathematical models of "leakage" of information from the power supply chain were explained, which made it possible to establish the general structure of the measuring installation and justify options for choosing hardware. The characteristics of the main signal forms were studied and analyzed, which made it possible to develop appropriate recommendations for protection against attacks on the side channels of the power supply. The scheme of the general structure of the measuring installation was developed and the S-box tabular transformation was implemented on Atmel microcontrollers using the "reading with offset" approach.

The results of the work can be successfully used to counter attacks on side channels of power supply.

Keywords: ANTI-ATTACKS, SIDE CHANNELS, POWER SUPPLY, MICROCONTROLLER, TABLE CONVERSION.

ЗМІСТ

ВСТУП

Безпека сучасних інформаційно-комунікаційних систем нерозривно пов'язана з алгоритмами, що забезпечують конфіденційність і цілісність інформації, яка зберігається і передається, а також функції ідентифікації та аутентифікації [1-5]. Стійкость цих алгоритмів базується на обчислювальній складності рішення деяких задач. Причому до недавнього часу розробники оцінювали їх безпеку у відриві від практичної реалізації на конкретному пристрої – інтегральній схемі [6-7]. Однак у 1999 році в [8] вперше було показано, що, до прикладу, такий параметр, як енергоспоживання інтегральної схеми, має явну залежність від даних, що обробляються. Тому, знявши форму сигналів, які характеризують енергоспоживання чипа в процесі виконання алгоритма деякого захисного перетворення (точніше, криптоалгоритму), і задіявши відносно нескладний математичний апарат простого або диференціального аналізу енергоспоживання (відповідно, атаки SPA або DPA [9-10]), виявляється можливим відновити секретну інформацію, яка обробляється чипом (в конкретному секретному ключі шифру). Даний клас атак називають атаками по побічних каналах (або побічними атаками) [11-12] на відміну від криптографічних атак, які використовують вразливості самих алгоритмів захисних перетворень [13]. Побічні атаки ґрунтуються на ідеї використання «витоку» інформації про секретні дані, які містяться в чипі, від його фізичних параметрів [14-15].

Інтегральні чіпи, які реалізують захисні перетворення, можуть застосовуватися в кінцевих пристроях, які мають різне призначення, найбільш розповсюдженими і чутливими до побічних атак по колах електроживлення, можна порахувати оригінальні витратні матеріали та запасні частини для широкого кола електронних пристроїв, смарт-карти і біометричні документи [16-17]. Останні в нинішній час отримують все більше поширення. Обладнання, здатне забезпечити високоякісний захист інформації [18-19], доступно не тільки державним структурам і великим

приватним підприємствам, але і звичайним людям. Чип, вмонтований в одну із сторінок документа, (наприклад, водійських прав, карточки медичного страхування або паспорта), виконує функцію додаткового захисту від підробок, в біометричних документах, помимо підробки поліграфії, потрібна підробка даних, які зберігаються в чипі (які, як мінімум дублюють нанесену поліграфічним способом інформацію). Ці дані захищаються при допомозі комплексу алгоритмічних засобів (захисних перетворень), серед яких можуть використовуватись алгоритми хешування, асиметричного, симетричного шифрування та інші подібні методи [20-21]. Причому алгоритми симетричного шифрування використовуються значно інтенсивніше за інших, оскільки вони пред'являють менші вимоги до, як правило, дуже сильно обмежених апаратних ресурсів чипа. Звідси успішний злом виконуваного на чіпі захисного перетворення дозволяє зробити копію чіпа (або навіть помістити в нього інші дані). Це дозволяє зробити копію біометричного документа або смарткарти. Для біометричних документів це нівелює додатковий рівень захищеності, що забезпечується використанням такого чіпа [22]. Для смарт-картки, яка застосовується, наприклад, як ключ доступу, це також нівелює головну її перевагу в плані безпеки в порівнянні з класичним (металевим) ключем, тому неможливо зробити її повну копію. Аналогічна ситуація спостерігається з оригінальними запасними частинами та витратними матеріалами. Як найпростіший приклад можна навести картридж для принтера. Можливість виготовлення копії чіпа, вмонтованого в оригінальний картридж, дозволить виготовити коректно працюючий сумісний витратний матеріал, що призведе до збитків фірми-виробника пристрою.

Отже, дана тема має значну актуальність у плані збільшення надійності ідентифікаційних документів.

Мета роботи. Метою даної роботи є розробка алгоритмів протидії атакам на побічні канали електроживлення.

Для вирішення поставленої мети вирішуються наступні **завдання**:

– огляд та аналіз інтегральних схем як основного програмно-апаратного засобу для захисту інформації;

– коротка характеристика атак по побічним каналам;

– розробка математичної моделі «витоку» інформації з ланцюга електроживлення та загальної будови вимірювальної установки;

– обгрунтувати вибір апаратного забезпечення;

– реалізувати табличне перетворення S-box на мікроконтролерах Atmel з використанням підходу «читання зі зміщенням».

Об’єкт дослідження. Процес протидії атакам на побічні канали електроживлення.

Предмет дослідження. Методи і засоби протидії атакам на побічні канали електроживлення.

Методи дослідження. Математичні методи моделювання, методи розрахунку електричних кіл, методи ідентифікації, методи програмно-апаратної реалізації.

Наукова новизна одержаних результатів.

1. Здійснено аналіз існуючих інтегральних схем як основного програмно-апаратного засобу для захисту інформації, що дало змогу охарактеризувати фізичні основи побічних атак по ланцюгах електроживлення.

2. Розроблено математичні моделі «витоку» інформації з ланцюга електроживлення, що дозволило встановити загальну будову вимірювальної установки та обґрунтувати варіанти вибору апаратного забезпечення.

3. Досліджено та проаналізовано характеристики основних форм сигналу, що дозволило розробити відповідні рекомендації для захисту від атак на побічні канали електроживлення.

Практичне значення отриманих результатів. Розроблено схему загальної будови вимірювальної установки та реалізовано табличне

перетворення S-box на мікроконтролерах Atmel з використанням підходу «читання зі зміщенням».

Публікації та апробація КР.

1. Концевич О.О., Бойко Н.З., Савіцький Т.Д. Моделювання та досліження атаки енергоспоживання на основі ваги Хемінга. Збірник матеріалів проблемної наукової міжгалузевої конференції «Автоматизація та комп’ютерно-інтегровані технології» (АКІТ-2022). Тернопіль, 2022. С.94-96 [23].

2. Концевич О.О., Катеринюк С.А., Додь О.А. Експериментальне дослідження атаки енергоспоживання Збірник матеріалів проблемної наукової міжгалузевої конференції «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2022). Тернопіль, 2022. С.108-110 [24].

1 ОГЛЯД ФІЗИЧНИХ ТА ТЕОРЕТИЧНИХ ОСНОВ ПОБІЧНИХ АТАК ПО КАНАЛАХ ЕЛЕКТРОЖИВЛЕННЯ

1.1 Інтегральні схеми як основний програмно-апаратний засіб для захисту інформації

Питання безпеки сучасних інформаційних систем нерозривно пов'язане з надійністю алгоритмів і протоколів [25-27], які використовуються в них, що дозволяють забезпечити конфіденційність інформації, а також функції ідентифікації та автентифікації [28]. Математичним базисом у даному разі виступають методи захисного перетворення інформації, такі як алгоритми шифрування (симетричні чи асиметричні) та хеш-функції (ключові чи безключові).

Реалізація таких захисних алгоритмів у програмному вигляді з використанням засобів операційної системи (ОС) персонального комп'ютера (ПК), сервера чи мобільного телефону можна вважати дуже ризикованою. Сучасні ОС є надзвичайно складними і небезпечними середовищами для обробки чутливої інформації. Тому нині виконання цих операцій, як правило, виносять в окремі інтегральні схеми – нерозкривні чіпи. Такі чіпи використовуються в електронних пристроях найширшого профілю, наприклад:

- ПК та серверне обладнання (у вигляді чіпа TPM, смарт-карти або USB-ключа);
- системи доступу до приміщень (у вигляді смарт-картки);
- електронні ідентифікаційні документи державного зразка, наприклад паспорти, посвідчення водія, медичні картки (у вигляді окремої смарт-картки або NFC чіпа, що вбудовується в одну зі сторінок відповідного документа);
- пристрої для здійснення електронних платежів (у вигляді смарт-картки або телефону використовує технологію NFC);
- пристрої для доступу до систем платного телебачення;
- принтери (для ідентифікації оригінальних витратних матеріалів);

- широкий спектр цивільного та військового обладнання.

У цій роботі буде зроблено акцент на чіпах, в основі яких лежать такі захисні перетворення, як алгоритми симетричного шифрування, зокрема блокові шифри. Функцією останніх є перетворення інформації (деяких вхідних даних, попередньо розбитих на блоки фіксованої довжини у вихідні) з використанням деякого секрету, що називається секретним ключем [29]:

$$E=f(M, k), \tag{1.1}$$

де M і E відповідно блоки вхідних та вихідних даних, зазвичай мають двійковий вигляд;

k – секретний ключ;

$f(*)$– функція шифрування.

Блокові симетричні шифри [30] знайшли широке застосування в чіпах, що не розкриваються, за рахунок значно менших вимог, що висуваються до обчислювальних ресурсів, на відміну від систем із відкритим ключем. Зокрема, такі шифри, як 3DES та AES, активно використовуються у всіх перерахованих вище видах електронних пристроїв.

Відповідно до принципу, сформованого в 19-му столітті Огюстом Керхгоффом, такі системи будуються з розрахунку, що зловмиснику виявляться відомі всі деталі їх реалізації, крім використовуваного ними секретного ключа. При цьому без знання ключа розрахунок невідомого M за відомим E або навпаки виявляється обчислювально складним завданням (тобто неможливим з використанням будь-яких існуючих обчислювальних ресурсів за розумний час) [31]. Настільки ж складним завданням виявляється і розрахунок нової пари (E', M'), де $M' \neq M$.

Під нерозкривними чіпами маються на увазі інтегральні схеми, виготовлені як правило на одному кристалі (тобто інтегральна схема в єдиному корпусі для поверхневого монтажу, що виконує функції цілого пристрою – як правило, має у своєму складі процесор, пам'ять, інтерфейси

введення-виводу, лічильники, таймери тощо). Функцією таких пристроїв є як захищене виконання процедур ідентифікації та аутентифікації, так і надійне зберігання секретного ключа. Вони приймають команди та дані від зовнішнього пристрою, виконують закладені алгоритми (у тому числі із застосуванням секретного ключа), результат виконання надсилається назад. Такі чіпи є закритими платформами зі своєю, дуже простою ОС, при цьому, на відміну від ПК, у них немає інтерфейсу підключення до інтернету і на них зазвичай неможливо встановити інше програмне забезпечення. Секретний ключ зберігається у спеціальній, захищеній області пам'яті, до якої можуть звертатися лише певні програми, що виконуються на чіпі, при цьому ні прямими, ні опосередкованими способами читання ключа ззовні виявляється неможливим.

При аналізі захищеності перетворень, що виробляються нерозкривним чіпом, очевидно слід розглядати стійкість всього апаратно-програмного комплексу загалом, а не тільки закладених у ньому алгоритмів у плані їх стійкості до криптографічних методів злому.

Далі, для спрощення, чіпи, що не розкриваються, будуть називатися просто чіпами, під атаками на чіпи буде матися на увазі несанкціонована спроба вилучення секретного ключа, що зберігається в ньому. А в оцінці безпеки чіпів, згідно з принципом Керхгоффа, буде аналізуватися найгірший варіант – коли зловмиснику відома детальна інформація як про технічні характеристики чіпа, так і про реалізовані на ньому програмні алгоритми, невідомим для нього є лише секретний ключ.

1.2 Коротка характеристика атак по побічним каналам

Алгоритми ідентифікації та аутентифікації, що використовуються в сучасних чіпах, вважаються захищеними від відомих криптографічних атак, тому з математичної Більшість сучасних чіпів є абсолютно захищеними. Однак існує клас атак, які називаються атаками побічними (або сторонніми)

каналами [32] і використовують додаткову інформацію (так званий витік) при фізичній реалізації алгоритму. Такі атаки умовно можна розділити на два класи:

- пасивні – атаки, що не передбачають втручання зловмисника у виконувані чіпом операції. Витік інформації виходить від аналізу фізичних параметрів чіпа, які, як правило, залежать від оброблюваних даних (енергоспоживання, електромагнітне випромінювання, час виконання операцій тощо);

- активні – атаки, що передбачають вплив на обчислювальний процес у чіпі з метою перевести пристрій у вразливий стан. У цьому випадку до витоку інформації наводять помилки, які з'являються при виконанні операцій, що становлять алгоритм.

Кожен із цих двох класів атак, у свою чергу, може бути поділений на три підкласи:

- агресивні атаки – підклас вельми ефективних атак, які передбачають отримання прямого доступу до внутрішніх компонентів чіпа, з повним або частковим руйнуванням його корпусу. Найбільш тривіальний приклад агресивної атаки - створення отвору в корпусі чіпа (механічним або хімічним способом) та пряме електричне підключення до шини даних. Надалі, залежно від того, застосовується пасивна атака або активна, дані можуть просто зчитуватися, або будь-яким чином модифікуватись. Цей тип побічних атак дуже складний, потрібні висококваліфіковані фахівці, дороге лабораторне обладнання та тривалий час на реалізацію щодо кожного пристрою, що зламується;

- напівагресивні атаки – зазвичай потрібне руйнування корпусу чіпа, проте даний клас атак не передбачає встановлення електричних з'єднань із внутрішніми вузлами чіпа - надається вплив на різні області пам'яті за допомогою лазера, УФ-випромінювання або рентгенівського випромінювання (в останньому випадку фізична руйнація корпусу може не знадобитися) з метою зміни програмного коду чипа або провокування

помилок у обчисленнях. Цей тип побічних атак вимагає значно більше дешевого обладнання, ніж агресивні атаки, також їх реалізація займає менше часу;

- неруйнівні атаки – не вимагають пошкодження корпусу чипа чи надання будь-яких інших впливів на чіп, які можна виявити після реалізації атаки. Вони можуть бути активними: наприклад, зміна тактової частоти генератора, що задає напруги живлення або температури чіпа від стандартних значень з метою провокування помилок у операціях. Як пасивні неруйнівні атаки можна виділити аналіз звукових коливань чіпа, часу виконання операцій, електромагнітного випромінювання, енергоспоживання – ці параметри роботи чіпа залежать від виконуваних ним операцій та оброблюваних даних. Застосовуючи спеціалізовані алгоритми аналізу зазначених параметрів, у граничному випадку стає можливим визначення секретного ключа чипа. Цей тип побічних атак є найнебезпечнішим з двох причин: власник скомпрометованого чіпа не зможе визначити факт реалізації атаки; ці атаки, хоч і вимагають тривалого та детального вивчення аналізованого чіпа, але після цього вони дуже просто і дешево масштабуються у відношенні аналогічних чіпів, в результаті вартість атаки в перерахунку на кожний зламаний пристрій може виявитися нікчемним.

Найбільш відомою, універсальною та небезпечною побічною атакою можна вважати пасивну неруйнівну атаку, що використовує аналіз енергоспоживання, який був уперше запропонований Полом Кьохером в 1999 [33]. Ідея цього підходу заснована на фізичних особливостях роботи сучасних чіпів, що призводять до того, що їх енергоспоживання залежить від виконуваної операції та оброблюваних у ній даних. Ця робота присвячена саме цьому типу побічних атак.

1.3 Фізичні основи побічних атак по ланцюгах електроживлення

Сучасні інтегральні схеми (ІС) можна поділити на три великі групи:

- ASIC [34] – інтегральні схеми спеціального призначення, вони є чіпами з наперед визначеною логікою і є вузько спеціалізованими. Використовуються для вирішення конкретної задачі в конкретному пристрої масового виробництва (мобільні телефони, комп'ютери, телевізори тощо). Внаслідок того, що такі чіпи виготовляються для виконання строго обмежених функцій, характерних лише для даного пристрою, то ASIC виконують їх дуже швидко, а самі схеми (через відсутність непотрібних компонентів) мають мінімальний розмір. ASIC найчастіше виготовляються під замовлення і мають низьку собівартість - від декількох центів, до декількох доларів, тільки за масового виробництва (сотнями тисяч і навіть мільйонними тиражами). При дрібносерійному та одиничному виробництві ASIC мікросхеми обходяться дуже дорого (у такому разі їх виробництво виявляється нерентабельним);

- мікроконтролери - пристрої, що поєднують на одному кристалі функції процесора та периферійних пристроїв, у тому числі ОЗУ, ПЗУ (є мініатюрними, однокристальними ЕОМ). Мікроконтролери більш універсальні, ніж ASIC, оскільки логіка їх роботи не визначається на заводі-виробнику – вони можуть бути сконфігуровані програмістом до виконання широкого спектра завдань. В цьому випадку використовується масове виробництво (мільйонними тиражами) і як наслідок забезпечується низька вартість, а широкий спектр характеристик мікроконтролерів дозволяє підібрати оптимальний для вирішення конкретного завдання. На відміну від ASIC, внаслідок своєї універсальності, мають більший розмір, по причині програмного способу реалізації алгоритмів вони значно поступаються по продуктивності, а за масового виробництва обходяться дорожче. Сфера використання дуже широка, охоплює практично всю споживчу електроніку та промисловість.

- ПЛІС [7] – пристрої, що дозволяють створити на одному кристалі будь-яку цифрову інтегральну схему На відміну від ASIC, логіка роботи ПЛІС не визначається при виготовленні, а задається програмуванням. На

відміну від мікроконтролера, програмування якого передбачає введення в його ПЗУ набору інструкцій, згідно яким вбудований процесор виконує необхідні операції (функції реалізуються програмним способом з використанням вже наявної внутрішньої електричної схеми), при програмуванні ПЛІС на апаратному рівні створюється схема з'єднання між його внутрішніми елементами На одному кристалі ПЛІС може бути запрограмована будь-яка інтегральна схема до процесора. Найбільш потужні ПЛІС еквівалентні ASIC схемам, а їх тактова частота може досягати гігагерца - продуктивність ПЛІС лежить десь посередині між мікроконтролерами та ASIC, а їхня вартість при масовому виробництві значно перевищує вартість мікроконтролерів, а тим більше ASIC.

Примітивним елементом ІС будь-якого типу є електронні ключі, які в переважній більшості випадків фізично виконуються у вигляді польових МОП (метал-оксид-напівпровідник) транзисторів *p*-типу та *n*-типу (рисунок 1.1), технологія виробництва ІС з їх використанням називається КМОП (комплементарна структура металоксид-напівпровідник). Транзистори *n*-типу проводять струм від витоку до стоку в тому випадку, якщо до керуючого електрода - затвору прикладено позитивну (щодо витоку) напругу, *p*-типу - якщо негативну.

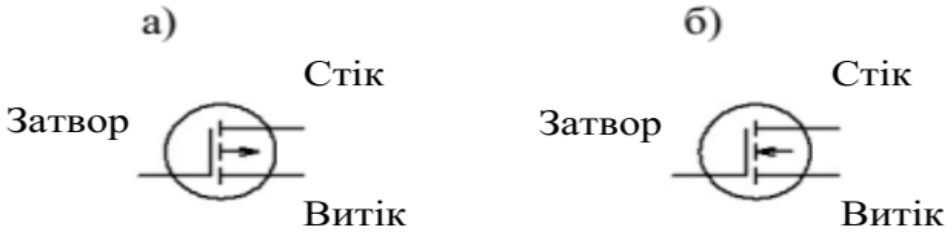


Рисунок 1.1 – Польові транзистори: а) *p*-типу; б) *n*-типу

Транзистори, з'єднані у певній послідовності, утворюють так звані логічні вентилі (ЛВ) – базові логічні елементи ІС, що виконують елементарну логічну операцію, перетворюючи один або кілька вхідних логічних значень, у

вихідні. У свою чергу, ЛВ утворюють вузли більшої агрегації, такі як суматори, лічильники, тригери, дешифратори тощо.

Основною перевагою технології КМОП є низьке енергоспоживання. Причиною цього є використання польових транзисторів, які, на відміну від біполярних, керуються напругою, а не струмом.

Цей приклад є дуже показовим для пояснення причин витоку інформації з ланцюга електроживлення і може бути вельми просто екстрапольований на інші типи ЛВ, які відрізняються один від одного кількістю транзисторів та схемою їх взаємного з’єднання.

Принципова схема інвертора наведена рисунку 1.2, він склаається з двох послідовно з'єднаних транзисторів *p*-типу (згори) та *n*-типу (знизу). Вхід інвертора з'єднаний із затворами обох транзисторів, а в якості виходу вибирається точка з'єднання стоку нижнього транзистора із витоком верхнього. Якщо на вхід інвертора подати "0" (рисунок 1.2), то транзистор *p*-типу (верхній) відкриється, а *n*-типу (нижній) закриється – вихід виявиться від'єднаним від землі та приєднаним до живлення, на ньому буде логічна «1». При подачі на вхід інвертора логічної "1" - верхній транзистор закриється, а нижній вихід відкриється і виявиться з'єднаним із землею – на ньому буде логічний «0».

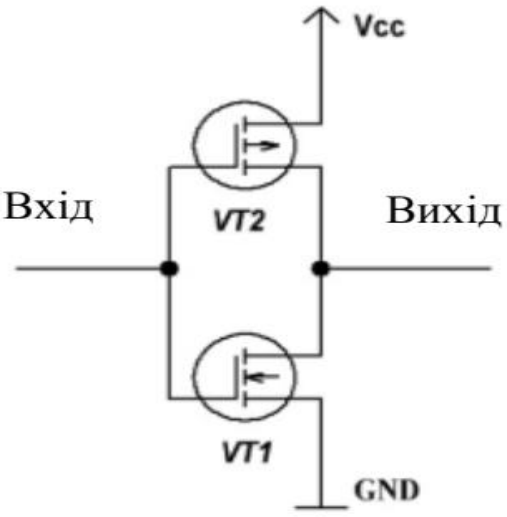


Рисунок 1.2 – Принципова схема інвертора

З опису зрозуміло, що верхній транзистор (*p*-типу, розташований між контактом живлення та логічним виходом), відповідає за формування логічної «1». А нижній транзистор (*n*-типу, розташований між землею та логічним виходом), відповідає за формування логічного "0". Подібний підхід до проектування ЛВ дозволяє досягти того, що за будь-яких логічних рівнів на вході, обидва транзистори не виявляться одночасно відкритими. Цей приклад характеризує одну з основних переваг КМОП-технології – в статичному режимі (інтервал часу, протягом якого логічні рівні подаються на вхід логічного вентиля, не змінюються) струм I_{CTAT} між ланцюгом живлення та землі, що утворюється виключно струмами витоку, виявляється мізерно малий - близько 1 пА на один вентиль [10,]. Отже, статична споживана потужність усіх можливих переходів може бути розрахована за наступною формулою:

$$P_{CTAT}=I_{CTAT}\times V_{DD}, \qquad (1.2)$$

що для напруги живлення в 5В становить зневажливо малі $P_{CTAT}=5\cdot10^{-12}$ В=5 пВт.

Однак вхідний сигнал може здійснювати всього різних чотири типи переходів, і якщо при (умовних) переходах 0→0 або 1→1 споживана з мережі живлення потужність $P_{0\to0}$ та $P_{1\to1}$ буде практично відсутня, то при переходах 0→1 або 1→0 вона буде досить значною (пов’язано з роботою логічного вентиля; якщо під час її виконання логічний рівень на вході ЛВ змінюється, то це називають динамічним режимом). Потужність, що споживається логічним вентилем у динамічному режимі, крім статичної складової, визначається ще й динамічною (таблиця 1.1), яка, у свою чергу, обумовлена двома причинами: струмом короткого замикання та струмом заряду паразитних ємностей.

Таблиця 1.1 - Переходи логічних рівнів інвертора

Перехід	Споживана потужність	Тип споживаної потужності
0→0	$P_{0\to0}$	Статична
0→1	$P_{0\to1}$	Статична+динамічна
1→0	$P_{1\to0}$	Статична+динамічна
1→1	$P_{1\to1}$	Статична

Струм короткого замикання виникає через те, що в моменти зміни вхідного логічного рівня 0→1, 1→0 одні транзистори вентиля відкриваються, інші закриваються, при цьому перемикання відбувається не одночасно і моментально - існує дуже короткий проміжок часу, коли обидва транзистори виявляються відкритими, що обумовлює короткочасний сплеск споживаної потужності за рахунок протікання струму короткого замикання через відкриті транзистори (від VDD до GND). Споживану в даному разі потужність можна оцінити за наступною формулою:

$$P_{КЗ}=V_{DD}\cdot I_{СЕРЕД}\cdot p_{0\to1}\cdot f\cdot t_{КЗ}, \qquad (1.3)$$

де $t_{КЗ}$ - інтервал часу, протягом якого обидва транзистори виявляються відкритими;

f – тактова частота мікросхеми;

$I_{СРЕД}$ - середній струм, що протікає через транзистори;

$p_{0\to1}$ – ймовірність виникнення переходів 0→1, 1→0.

За оцінкою, струмом короткого замикання обумовлено не більше 20% від усієї споживаної потужності вентиля. Найбільшу потужність вентиль споживає під час заряду своєї ємнісної складової (що являє собою сукупність власних паразитних ємностей транзисторів і ліній живлення, що їх з'єднують, вони умовно позначені на рисунках 1.3 у вигляді одного конденсатора $C_{ЗАГ}$). Коли після логічної "1" на вхід інвертора подається логічний «0» (рисунок

1.3а), транзистор з *n*-каналом (VT1) закривається, з *p*-каналом (VT2) відкривається. У цей момент ємнісна складова ЛВ заряджається, що зумовлює значний сплеск енергоспоживання, який може бути виявлений шляхом вимірювання падіння напруги на резисторі $R_{ВИМ}$, вставленому в розрив лінії живлення чіпа. При подачі на вхід інвертора логічної «1» відбувається розряд $C_{ЗАГ}$ через відкритий транзистор *n*-типу в землю (рисунок 1.3б), що також можна виявити виміром падіння напруги на резисторі, вставленому вже у розрив лінії землі чіпа.

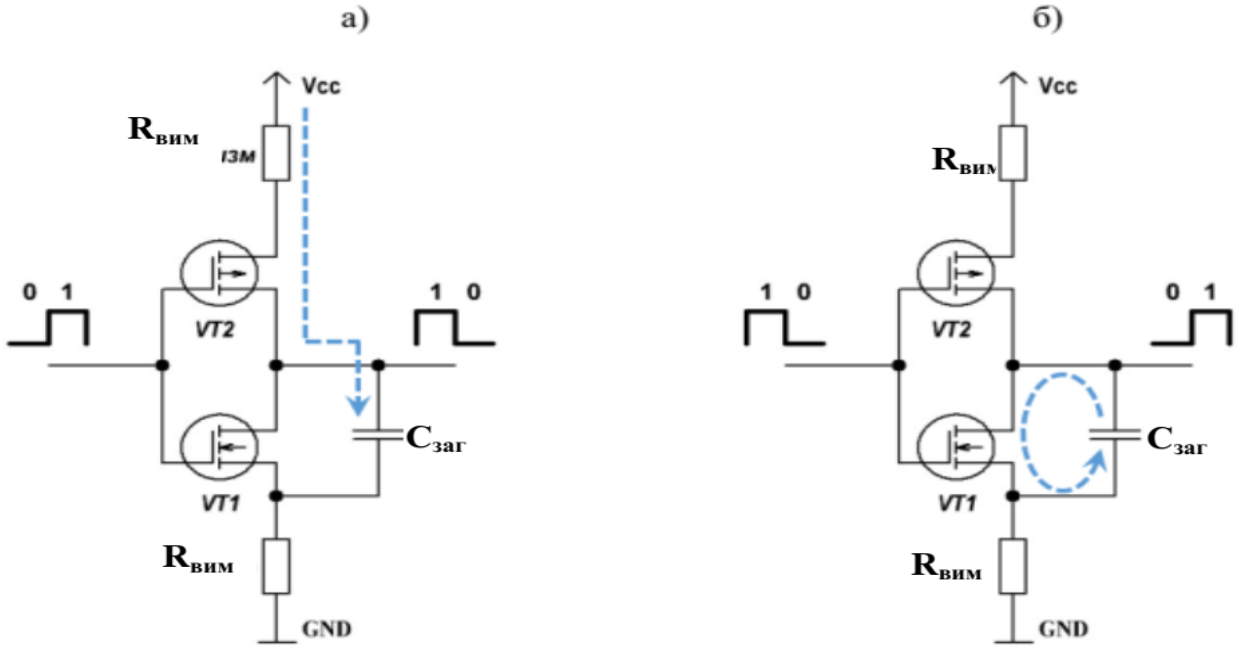


Рисунок 1.3 - Схема протікання струму в інверторі при: а) подачі логічного нуля; б) подачі логічної одиниці

Споживану потужність, обумовлену цим ефектом, можна оцінити за наступною формулою [10]:

$$P=C_L \cdot V^2_{DD} \cdot p_{0\to1} \cdot f, \qquad (1.4)$$

де C_L - величина паразитної ємності (ємність «конденсатора» $C_{ЗАГ}$);

V_{DD} – напруга живлення;

$p_{0\to1}$ – ймовірність того, що логічний сигнал на виході інвертора зробить перехід 0→1;

f – тактова частота роботи пристрою.

Експериментально було підтверджено, що у КМОП мікросхемах найбільша частка енергоспоживання припадає на описаний вище, заряд паразитної ємності (коли на вхід інвертора на зміну логічній одиниці приходить логічний нуль). Коли ж на зміну логічному нулю приходить логічна одиниця (паразитна ємність перестає заряджатися і починає розряджатися), також спостерігається сплеск енергоспоживання, але значно менший. Він обумовлений лише описаним вище короткочасним відкриттям одразу двох транзисторів.

Величина паразитної ємності визначається насамперед типом вентиля та технологічним процесом виробництва транзисторів, у тому числі довжиною ліній живлення, які зв'язують ЛХ, а також числом зв'язаних вентилів (сучасний технологічний процес виробництва інтегральних схем не дозволяє повністю усунути паразитні ємності ЛВ).

Типові значення ємності C_L становлять порядку $10^{-15}\div10^{-12}$Ф=1фФ÷1пФ. Таким чином, для напруги живлення 5 В, частоти задаючого генератора чіпа 4 МГц, ймовірності переходу 0→1, що дорівнює 0.25, споживана логічним вентилем потужність, обумовлена зарядом паразитної ємності, складе $P=10^{-12}$ Ф·25 В·0.25·4·10^6 Гц= 25·10^{-6} Вт=10 мкВт на один вентиль.

З груп логічних вентилів формують той чи інший функціональний блок чіпа з більшою функціональністю та складністю (суматори, лічильники та інші), а ті, у свою чергу, з'єднуючись шинами (збільшуючи рівень агрегації), утворюють інтегральні схеми.

Отже, енергоспоживання КМОП мікросхеми загалом визначається сукупним енергоспоживання всіх ЛВ чіпа, тому воно залежить від даних, які оброблюються в будь-якій момент часу окремими збираннями ЛВ.

1.4 Загальна будова аналізованих чіпів

Розглядатимемо атаку побічними каналами стосовно мікроконтролерів. Мікроконтролери дуже схожі за своєю будовою на чіпи, що не розкриваються. Більше того, при дрібносерійному виробництві як чіпи, що здійснюють процедури ідентифікації та аутентифікації, часто використовуються саме мікроконтролери, тому що замовляти виробництво ASIC чіпів виявляється абсолютно невигідно. З іншого боку, мікроконтролери значно більш універсальні, а особливості їх будови не становлять секрету – їх з легкістю можна запрограмувати на виконання будь-яких доступних операцій та досліджувати витік інформації з ланцюга живлення при виконанні цих операцій. Також мікроконтролери є більш доступними для придбання, тому отримані результати можуть бути легко відтворені, а при необхідності уточнено та доопрацьовано іншими дослідниками.

У відомих публікаціях при експериментальній демонстрації реалізацій атак по ланцюгах електроживлення, а також тестуванні пропонованих методів захисту часто використовувалися мікроконтролери фірм Atmel (родина ATmega) та Microchip (Родина PIC). Нижче буде коротко розглянуто основні особливості будови мікроконтролерів цих двох сімейств, зокрема двох восьмирозрядних моделей: Atmel ATmega16-8PU та Microchip PIC16F877A.

Центральним вузлом будь-якого мікроконтролера є арифметико-логічний пристрій (АЛП), що служить для виконання всіх логічних та арифметичних операцій (Обробка даних). Узагальнена блок-схема АЛП показана на рисунку 1.4. На його вхід надходять:

- два операнди (дані);

- код операції – двійкова послідовність, що перемикає АЛП в режим, відповідний операції, яку потрібно здійснити над операндами (наприклад: додавання по mod2, арифметичне додавання тощо);

- прапори – інформація про результат виконання попередньої команди (наприклад, про перенесення біта у старшому розряді при виконанні попередньої операції арифметичного складання, який необхідно врахувати під час виконання поточної операції).

На виході АЛП з'являється результат виконання операції, а також відповідні йому прапори.

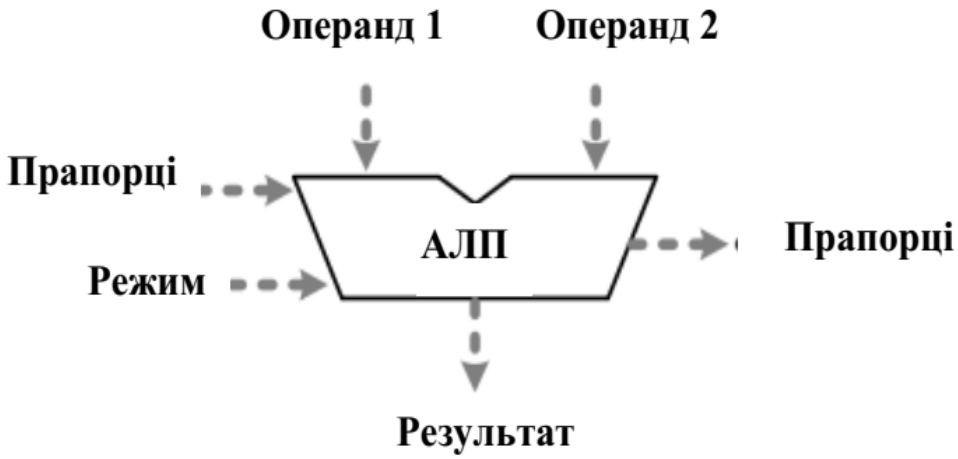


Рисунок 1.4 - Узагальнена блок-схема АЛУ

Спрощено структуру АЛУ можна подати у вигляді кількох збірок ЛВ, кожна з яких реалізує ту чи іншу арифметичну, логічну функцію чи функцію передачі даних (наприклад, переміщення даних між регістрами, ОЗП, ПЗП). При цьому АЛУ сучасних чіпів є багаторозрядним, тобто воно здатне за один машинний цикл здійснювати операції з операндами, кожен із яких складається з кількох біт. Зараз широке поширення має восьми-розрядна архітектура – такі чіпи випускаються вже кілька десятиліть, вони є дешевими та надзвичайно надійними, а саме ці фактори і є найважливішими при виготовленні чіпів, що не розкриваються.

Крім АЛУ, в мікроконтролерах присутні два типи пам'яті: енергозалежна та енергонезалежна. У першому випадку для зберігання даних потрібна постійна наявність електричного живлення, а у другому випадку дані зберігаються навіть після його вимкнення. Також, як і АЛУ, кожен

осередок пам'яті являє собою транзисторний блок. Наприклад, один із способів побудови осередків енергозалежної пам'яті полягає у паралельному з'єднанні двох D-тригерів, побудованих на базі розглянутих вище ЛВ типу інвертор.

Енергозалежна пам'ять може бути поділена на дві області:

- робочі регістри;

- ОЗУ.

У мікроконтролері ATmega16 є 32 восьми-розрядних робочих регістри, велика частина операцій (логічні, арифметичні) можуть бути виконані лише з даними, завантаженими в робочі регістри, причому ці операції виконуються найбільш швидко (більшість за один машинний цикл). ОЗУ, як правило, використовується для зберігання проміжних даних під час виконання чіпом програми, оскільки щодо ОЗУ доступні лише команди читання/запису, а його обсяг значно перевищує обсяг робочих регістрів.

Будова восьми-розрядних мікроконтролерів PIC має низку принципових відмінностей від мікроконтролерів ATmega. Зокрема, PIC мають всього один робочий регістр і чотири так званих банки (bank) оперативної пам'яті. Частина осередків цієї пам'яті використовується для управління мікроконтролером, але більшість – для зберігання даних. Для виконання переважної більшості операцій з однією змінною вона має бути попередньо завантажена в робочий регістр (наприклад, логічні операції змінної з константою, пересилання даних між двома осередками ОЗУ тощо). При виконанні операцій з двома змінними (наприклад, логічні або арифметичні операції між двома) одна з них також неодмінно повинна утримуватися в робочому регістрі. Враховуючи той факт, що робочий регістр у мікроконтролерах PIC один – програмування його на асемблері є дуже нетривіальним процесом, а швидкість виконання програми виявляється у 8-10 разів повільнішою, ніж на мікроконтролерах ATmega.

Окремо варто виділити регістр статусу, реалізований в обох мікроконтролерах. Він виконаний у вигляді восьми розрядного регістру,

безпосередньо з'єднаного з АЛУ. Функціональність цього регістру в мікроконтролерах PIC та ATmega дещо відрізняється, однак вони мають як мінімум два біти однакового функціонального призначення:

- біт, що називається прапором перенесення. Він встановлюється в одиницю в тому випадку, якщо при виконанні попередньої операції у старшому розряді відбулося перенесення/позика біта;

- біт, що називається прапором нуля. Він встановлюється в одиницю, якщо результат виконання попередньої операції виявився нульовим (байт, що складається з восьми нулів).

Енергонезалежну пам'ять також можна розділити на дві області:

- Flash-пам'ять (пам'ять програм);

- EEPROM.

У Flash-пам'яті зберігається виконувана чіпом програма, також туди можуть бути записані додаткові «користувацькі» дані (наприклад, таблиці перетворення) і ці дані можуть бути використані під час виконання програми (хоча процедура читання з Flash-пам'яті займає набагато більше часу, ніж із ОЗУ). Однак модифікувати дані, що зберігаються в Flash-пам'яті, можливо лише при програмуванні чіпа, на відміну EEPROM пам'яті, основна функціональна відмінність якої полягає в тому, що дані, що зберігаються в ній можуть бути змінені в процесі виконання програми (в асемблері чіпа, крім команд читання даних, доступні також команди запису), причому швидкість читання/запису для EEPROM пам'яті також дуже низька.

Усі області пам'яті пов'язані з АЛУ шиною даних – лінією зв'язку, фізично виконаною у вигляді струмопровідних доріжок. Під час виконання коду програми з відповідної області пам'яті дані надходять по шині в АЛУ, результат також по шині пересилається у вибрану область пам'яті. Очевидно, що розрядність шини даних (кількість паралельних доріжок) повинна бути не менше розрядності АЛУ - для мікроконтролерів, що розглядаються, - це вісім біт. Шина даних через свою відносно велику протяжність має суттєву ємнісну складову. Стверджується, що енергоспоживання, яке витрачається на

передачу даних по шині, займає дуже велику частку від загального споживання чіпа.

Виконувана чіпом програма, як правило, створюється мовою високого рівня (наприклад, мовою С), а в тому випадку, коли необхідно забезпечити максимальну швидкість роботи програми за мінімальних вимог до апаратних ресурсів, використовується мова низького рівня – асемблер (створення складних програм на ньому є дуже трудомістким завданням). Потім вона компілюється, в результаті чого перетворюється на так званий машинний код, де кожна команда програми представлена у вигляді двійкового числа – слова. Наприклад, довжина слова в мікроконтролерах PIC, що розглядаються, дорівнює 14-ти бітам. Слова, своєю чергою, записуються у Flash-пам'ять чіпа. В процесі виконання програми вони послідовно зчитуються та виконуються в АЛУ. Кожне слово містить всю необхідну інформацію для виконання конкретної операції, зокрема код операції (двійкова послідовність, що визначає виконувану чіпом команду), а також, залежно від команди, інформацію про операнди та місце збереження результату виконання операції. Таким чином, будь-який алгоритм, що виконується чіпом, подається у вигляді набору простих операцій, які послідовно виконуються. У процесі виконання цих операцій задіяні описані вище вузли чіпа. При цьому логічно припустити, що енергоспоживання чіпа при виконанні різних операцій може значно відрізнятися, так як різні операції виконуються в АЛУ, що відрізняються конструктивно збиранням ЛВ, а також при цьому використовуються різні області пам'яті.

2 МАТЕМАТИЧНІ МОДЕЛІ ПОБУДОВИ ПОБІЧНИХ АТАК ЗА ЛАНЦЮГАМИ ЕЛЕКТРОЖИВЛЕННЯ

2.1 Математичні моделі «витоку» інформації з ланцюга електроживлення

Для того, щоб зв'язати енергоспоживання чіпа з оброблюваними даними, необхідно подати його математичну модель. Ця модель може мати різні рівні точності. Чим вищий рівень точності, тим більше потрібно обчислювальних ресурсів та інформації про чип. Отже, застосування тієї чи іншої моделі визначається наявними у зловмисника обчислювальними ресурсами та ресурсами, які він готовий витратити на отримання інформації про технічні особливості аналізованого чіпа. Моделі енергоспоживання чіпа можна розділити як мінімум на дві групи в залежності від рівня абстракції: моделі, що розглядають роботу чіпа на аналоговому рівні та на логічному.

Моделювання роботи чіпа на аналоговому рівні є найбільш докладним, повним та точним. У цьому випадку передбачається наявність найповнішої інформації про будову чіпа аж до перерахування складових його транзисторів, доріжок, що їх з'єднують, а також розміри всіх паразитних ємностей. На основі цих даних будується математична модель, яка шляхом розв'язання диференціальних рівнянь (наприклад, з використанням популярного програмного пакета SPICE або його аналогів) дозволяє розрахувати напруги та струми у будь-якій частині чіпа. Для атак на чіпи ця модель практично не може бути використана в основному через причини відсутності у зловмисника настільки детальної інформації про аналізований чіп.

Моделювання на логічному рівні передбачає наявність інформації про логічні вентилі чіпа, порядок їх з'єднання, часто додається інформація про затримки сигналу, що проходить від вентиля до вентиля. Моделі, що описують енергоспоживання чіпа на логічному рівні, вимагають значно менших обчислювальних ресурсів, ніж аналогове моделювання, а також

менших знань про чип. Недоліком таких моделей очевидно є їхня менша точність. На першому етапі для кожного ЛВ визначається, які переходи та з якою затримкою здійснять пов'язані з ним вентилі при всіх можливих варіантах вхідних значень (0→0, 0→1, 1→0, 1→1). На другому етапі для сукупності всіх логічних вентилів чіпа розраховуються передбачувані рівні енергоспоживання чіпа при вчиненні тих чи інших логічних переходів на окремих вентилях (тобто при появі певних даних у певному вузлі чипа). Цей крок передбачає наявність моделей, що зв'язують логічні переходи на окремих вентилях із витраченою на них (на ці переходи) потужністю. Дані моделі в основному ґрунтуються на інформації про потужність, яка споживається різними типами ЛВ у статичному та динамічному режимах.

Модель, що описує енергоспоживання чіпа на логічному рівні, на практиці також вимагає таких знань про будову аналізованого чіпа, які, як правило, відсутні у зловмисника. Тому практичну застосовність мають більш універсальні моделі: так звана модель ваги Хеммінга та модель відстані Хеммінга. Як було показано вище, ЛВ, на основі яких виготовляються чіпи, споживають потужність переважно у моменти перемикання. Ідея моделі відстані Хеммінга полягає в тому, щоб обчислювати кількість переходів 0→1, 1→0, що відбуваються в чіпі в певний інтервал часу, що згодом дасть можливість побудувати подібність форми сигналу, з тією лише відмінністю, що замість значень споживаної потужності вона міститиме кількість ЛВ, які переключилися.

Припустимо, що у момент часу i (наприклад у робочому регістрі) є комбінація M_i, а в наступний момент часу i+1 в даний регістр з ОЗУ була завантажена комбінація M_{i+1}. Тоді потужність, що витрачається на дану зміну, буде пропорційна $HW(M_i \oplus M_{i+1})$, де $HW(*)$ – це вага Хеммінга. Наприклад, якщо восьмибітова двійкова комбінація «1111 1111» змінилася на комбінацію «1111 0000», то відстань Хеммінга між цими двома комбінаціями дорівнюватиме чотири – простіше кажучи у чотирьох з восьми розрядів значення біт зміняться (рисунок 2.1), отже, з мережі живлення, крім

статичної потужності (що споживається всіма ЛВ чіпа), буде споживатися динамічна потужність, обумовлена перемиканням чотирьох ЛВ, що становлять чотири осередки розглянутого регістру. Якщо розглядати чіпи з восьмирозрядною архітектурою, то всі можливі комбінації, що з'являються в регістрах, ОЗП, EEPROM або на шині даних, можуть давати лише дев'ять рівнів енергоспоживання: наприклад, мінімальний нульовий рівень спостерігатиметься у тому випадку, якщо комбінація не зміниться в жодному розряді. Перший рівень – при зміні значення одного біта, тощо аж до максимального восьмого рівня – за зміни значень всіх восьми біт. Отже, використовуючи цю модель, можна оцінити енергоспоживання чіпа, яке буде пропорційне до кількості переходів (0→1 або 1→0).

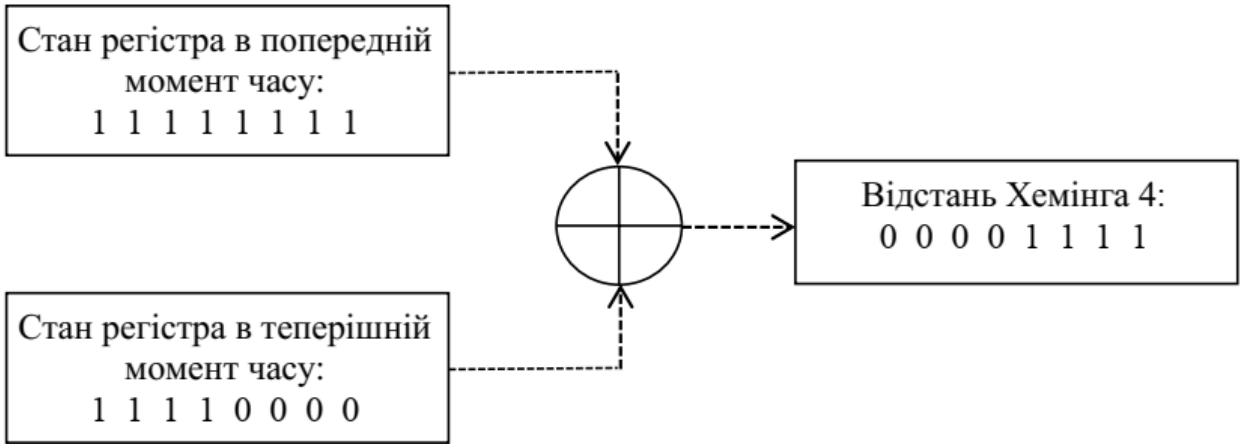


Рисунок 2.1 - Модель енергоспоживання на відстані Хеммінга

При використанні моделі відстані Хеммінга зазвичай робиться ряд припущень:

- у статичному режимі енергоспоживання вентилів відсутнє (модель її не враховує);

- на перехід 0→1 та на перехід 1→0 витрачається однакова потужність (в принципі, цей недолік можна нівелювати, окремо підраховуючи переходи 0→1 та 1→0);

- немає різниці в енергоспоживання між різними типами логічних вентилів.

Описані припущення сильно спрощують процес складання моделі енергоспоживання, вимоги до обчислювальних ресурсів та обсяг необхідної інформації про особливості будови чіпа. Очевидна складність цієї моделі полягає в тому, що потрібно знати попередні бітові значення розрядів, для визначення кількості розрядів, які змінили своє значення.

У ряді випадків попередня модель може бути спрощена тим припущенням, що в деяких частинах схеми перед виробленням нової комбінації, біти розрядів, що розглядаються, можуть обнулятися. У цьому випадку, очевидно, відпаде необхідність розрахунку значень розглянутих біт у попередній момент часу, тому що приймається, що попередні значення біт дорівнювали нулям. Тому споживана потужність буде пропорційна кількості одиниць (вазі Хеммінга) в *n*-бітовій комбінації, що з'являється. Наприклад (рисунок 2.2), якщо на восьмирозрядній шині даних з'являється комбінація "00000010", то це означає, що комбінація, яка в попередній момент часу дорівнює восьми нулям, змінилася в одному розряді. Таким чином, споживатиметься потужність, потрібна для зміни стану одного розряду. Якщо на шині даних з'являється комбінація із восьми одиниць, то це означає, що зміняться всі вісім розрядів. Отже, споживатиметься потужність, потрібна для зміни стану восьми розрядів.

Рисунок 2.2 - Модель енергоспоживання за вагою Хеммінгу

Дана модель вкрай проста, практично не вимагає знання конструктивних особливостей аналізованого чіпа і в багатьох випадках може

виявитися дуже ефективною. У тих випадках, коли ця модель виявляється неефективною, рекомендується застосовувати модель відстані Хеммінга.

2.2 Загальна будова вимірювальної установки

Класична блок-схема вимірювальної установки представлена рисунку 2.3. Вона складається із чотирьох основних компонентів:

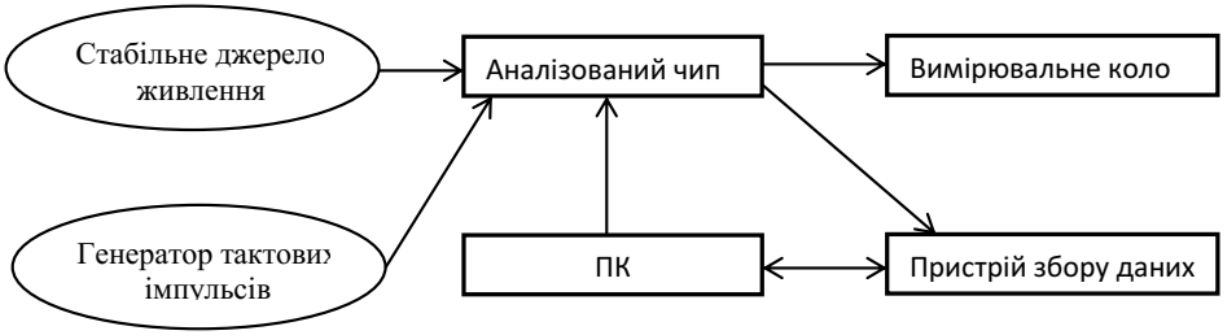


Рисунок 2.3 – Блок-схема вимірювальної установки

1) аналізований чіп – фізичний пристрій, з якого потрібно витягти секретний ключ. Аналізований чіп має інтерфейс зв'язку із зовнішніми пристроями (зазвичай через універсальний асинхронний приймач), він використовується для отримання команд (у тому числа ініціюючих виконання захисних перетворень), а також надсилання відповідей з результатом виконання цих команд. Важливою особливістю є те, що чіп зазвичай тактується зовнішнім кварцовим резонатором або генератором, тому що стабільність вбудованого LC-ланцюжка, як правило, занадто погана для виконання відповідальних завдань, що може призводити до помилок у процесі обміну інформацією між чіпом та зовнішніми пристроями, а також може збільшити джиттер на формах сигналу, що знімаються. Також необхідно враховувати те, що в процесі реалізації атаки необхідно розрізняти найменші коливання енергоспоживання, таким чином, нестабільність або зайва зашумленість ланцюга живлення можуть призвести до неможливості

проведення атаки або надмірного збільшення потрібної кількості даних про енергоспоживання. Тому чіп необхідно заживлювати від дуже стабільного джерела живлення лабораторного рівня. На додаток до цього рекомендується безпосередньо перед його контактами живлення встановлювати кілька конденсаторів для додаткової стабілізації напруги;

2) вимірювальне коло – комплекс елементів, функція яких полягає в тому, щоб забезпечувати електричне з'єднання між аналізованим чіпом та пристроєм збору даних. При цьому він повинен надавати мінімальний вплив на чіп і передавати сигнал з максимально можливою достовірністю. Зазвичай у вимірювальному колі використовується резистор (рисунок 2.4), вставлений у розрив контакту живлення чи землі чіпа, до якого приєднується осцилографічний пробник - він знімає падіння напруги на резисторі, яке, за законом Ома, прямо пропорційне струму, споживаному чіпом під час своєї роботи. Якщо роздільна здатність використовуваного пристрою збирання даних або підсилювача пробника недостатньо для розпізнавання коливань напруги між резистором і пробником, то може бути додатково встановлений широкосмуговий підсилювач.

Рисунок 2.4 - Вимірювальне коло установки

Замість установки резистора може бути використаний безконтактний спосіб вимірювання при допомозі електромагнітного зонда, що розташовується над чіпом, який вловлює електромагнітне випромінювання під час виконання захисних перетворень;

3) пристрій збору даних – це прилад, що перетворює аналоговий сигнал, отриманий від вимірювального кола, у цифровий вигляд для його подальшого збереження на носії інформації, роль якого грає жорсткий диск ПК. Як правило, як пристрій збору даних використовується широкосмуговий осцилограф, причому вартість такого приладу може перевищувати навіть суму в $10000;

4) персональний комп'ютер. Він направляє на аналізований чіп команди, що ініціюють виконання захисних операцій, крім того ПК приймає та зберігає дані про енергоспоживання, які отримують від пристрою збору даних.

Описана експериментальна вимірювальна установка функціонує за таким алгоритмом:

1) ПК переводить пристрій збору даних в режим очікування тригерного сигналу;

2) ПК відправляє на чіп дані, за потреби супроводжуючи їх службовими командами, що ініціюють операції захисного перетворення, а також відправляє тригерний сигнал на пристрій збирання даних;

3) аналізований чіп, отримавши від ПК необхідні дані, виконує закладений алгоритм, після чого повертається до режиму очікування наступної команди від ПК;

4) визначення збору даних, отримавши, тригерний сигнал, оцифровує і записує у внутрішній буфер дані від вимірювального ланцюга, ці дані характеризують енергоспоживання чіпа під час проведення захисних перетворень;

5) пристрій збору даних надсилає записані дані з буфера до ПК;

6) ПК записує прийняті дані у файл;

7) кроки 1-6 повторюються стільки разів, скільки форм сигналу в результаті необхідно отримати.

2.3 Теоретичні основи побудови побічних атак за ланцюгами електроживлення

Оскільки енергоспоживання чіпа залежить від виконуваних ним операцій та даних, які він на цих операціях обробляє, то найбільш тривіальною атакою, що дозволяє використовувати цю особливість роботи сучасних чіпів, простий аналіз потужності (simple power analysis - SPA).

Атака SPA передбачає пряму інтерпретацію даних про енергоспоживання чіпа з метою визначення як виконуваних ним операцій, так і оброблюваних даних. Будь-який алгоритм, що виконується чіпом (у тому числі і алгоритм захисного перетворення), представляється у вигляді набору елементарних операцій з певними даними, які він послідовно обробляє.

При виконанні різних операцій задіяні різні вузли чіпа, отже, кожен вид операції, що виконується чіпом, залишає свій унікальний відбиток на знятій формі сигналу.

В якості прикладу можна навести графіки на рисунках 2.5, де зображено форму сигналу, що характеризує енергоспоживання мікроконтролера при виконання шифру AES.

За формою сигналу, зображеного на рисунку 2.5а, можна розрізнити дев'ять ділянок, які характеризують перші дев'ять раундів шифру AES (обробці першого раунду відповідає ділянка між 0.06 та 0.73 мс, другого – між 0.84 та 1.52 мс і т. д.), а також ще одна ділянка меншої тривалості (в районі четвертої мс), що характеризує обробку десятого раунду AES, який, згідно зі стандартом, є скороченим (в ньому відсутнє перетворення MixColumns). Збільшення масштабу області, що відповідає першому раунду (рисунок 2.6а) дозволяє визначити окремі частини алгоритму, виконуваного чіпом.

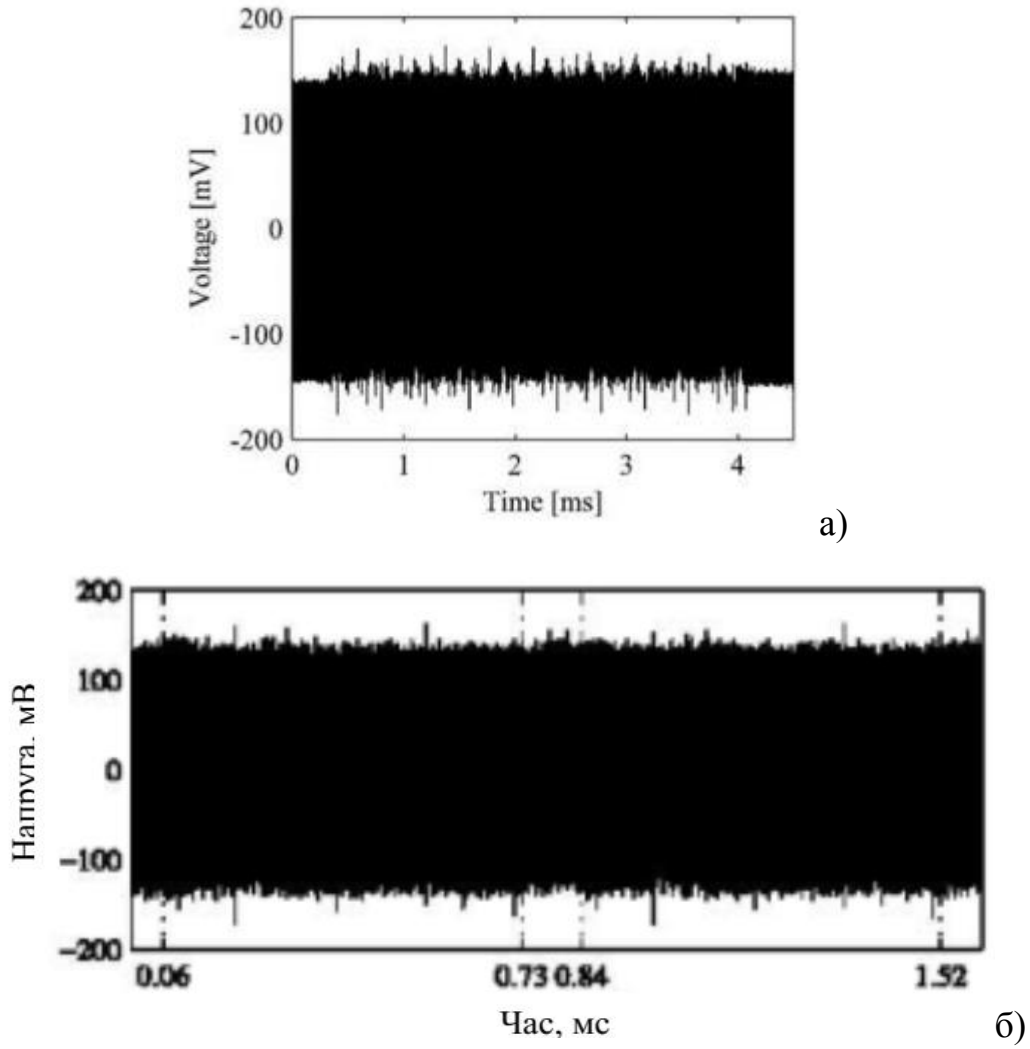


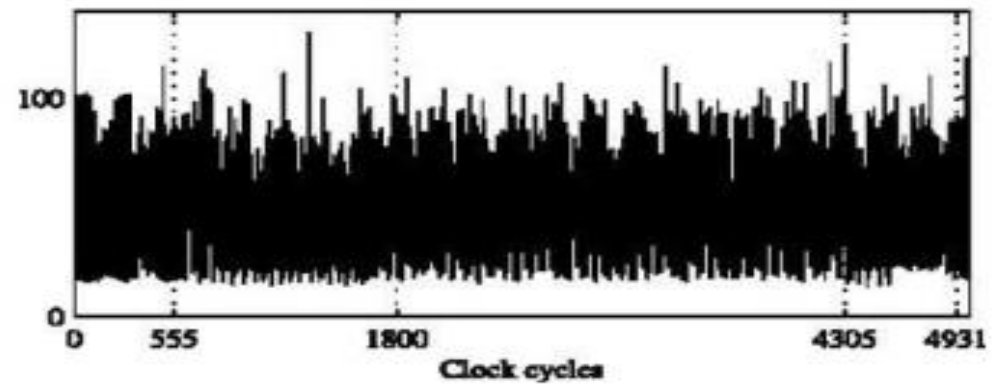
Рисунок 2.5 - Форма сигналу, що характеризує енергоспоживання мікроконтролера під час виконання шифру AES: а) повна форма сигналу; б) ділянка, що відповідає обробці перших двох раундів

Детальне знання алгоритму AES, а також зіставлення програмного коду мікроконтролера з отриманою формою сигналу, дозволяє розбити її на три області відповідно до операцій, що складають шифр:

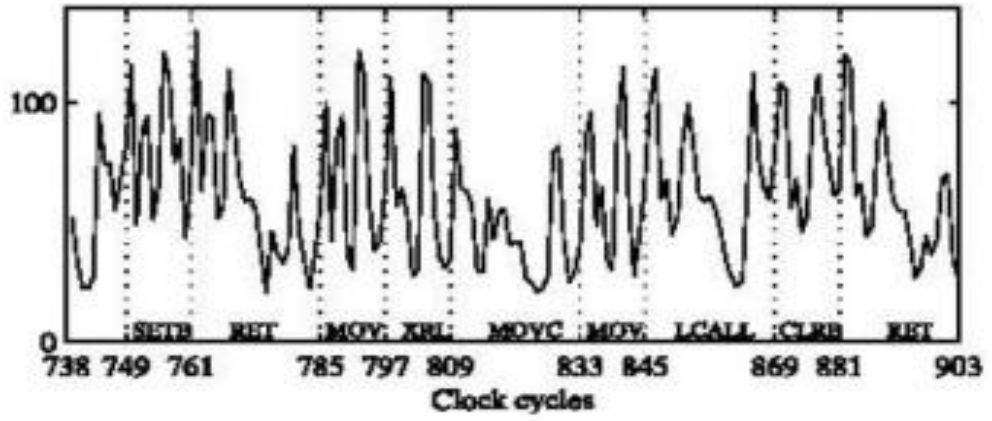
- ділянка між 555 та 1800 відліками відповідає виконанню перетворень AddRoundKey, SubBytes та ShiftRows;

- між 1800 та 4305: виконання перетворення MixColumns;

- між 4305 та 4931: вироблення ключа першого раунду.



а)



б)

Рисунок 2.6 - Частина форми сигналу, яка характеризує енергоспоживання чіпа при виконанні шифру DES: а) перший раунд (від 555-го до 4305-й відліки); б) перший раунд, ділянка від 738-го до 903-ого відліку

Подальше збільшення масштабу отриманої форми сигналу дозволяє порівняти стрибки енергоспоживання з конкретними операціями, що виконуються (рисунок 2.6б).

Після визначення стрибків напруги, що відповідають виконанню конкретної операції захисного алгоритму, здійснюється перехід до наступного кроку – визначення значення оброблюваної комбінації. Як приклад припустимо, що отримані форми сигналу, що характеризують енергоспоживання чіпа під час виконання алгоритму шифру AES. На першому раунді цього алгоритму i-й блок повідомлення $m(i)$ складається по mod2 з блоком раундового ключа першого раунду $k(1)$ (обидва блоки у двійковому вигляді мають довжину 128 біт). При виконанні даного

перетворення на восьмирозрядному чіпі додавання цих комбінацій здійснюється частинами (підблоками) по вісім біт за 16 підходів:

$$t_l(i, r)=m_l(i)\oplus k_l(r), \qquad (2.1)$$

де l=1, ..., 16 – оброблюваний підблок;

r=1, ..., 10 – номер раунду;

$t_l(i, r)$ – результат виконання операції додавання по mod2, що подається потім на вхід S-box.

Також припустимо, що після здійснення операції додавання по mod2 її результат пересилається на тимчасове зберігання з робочого регістру в осередок ОЗП. На рисунку 2.7 зображені сплески енергоспоживання, характерні для виконання цієї операції на аналізованому мікроконтролері Atmel. При цьому дано дев'ять форм сигналу, по одній для кожної з ваг Хеммінга пересланої комбінації (з метою зменшення шумової компоненти для кожної ваги Хеммінга було зроблено статистичне усереднення по 1 000 вимірів).

З рисунка 2.7б видно, що амплітуда сплеску енергоспоживання в діапазоні від 140-го до 143-го відліку змінюється пропорційно вазі Хеммінга пересланої комбінації. Звідси стає очевидною практична можливість визначення ваги Хеммінга комбінації, що є результатом виконання проміжної операції виконуваного захисного алгоритму (зокрема комбінації, щозалежить від секретного ключа). Найбільш тривіальний підхід до визначення ваги Хеммінга оброблюваної комбінації називається шаблонною атакою (Template Attack). Вона найбільш відома для апаратних реалізацій шифрів AES та DES [9]. Шаблонна атака передбачає наявність у зловмисника тестового чіпа, аналогічного тому, на який передбачається реалізація атаки. При цьому вкрай бажана можливість його вільного програмування, а також багаторазового ініціювання операції захисного перетворення з різними вхідними даними. Далі такий чіп називатиметься тестовим, а чіп, на який

передбачається зробити практичну атаку - аналізованим чипом або просто чипом.

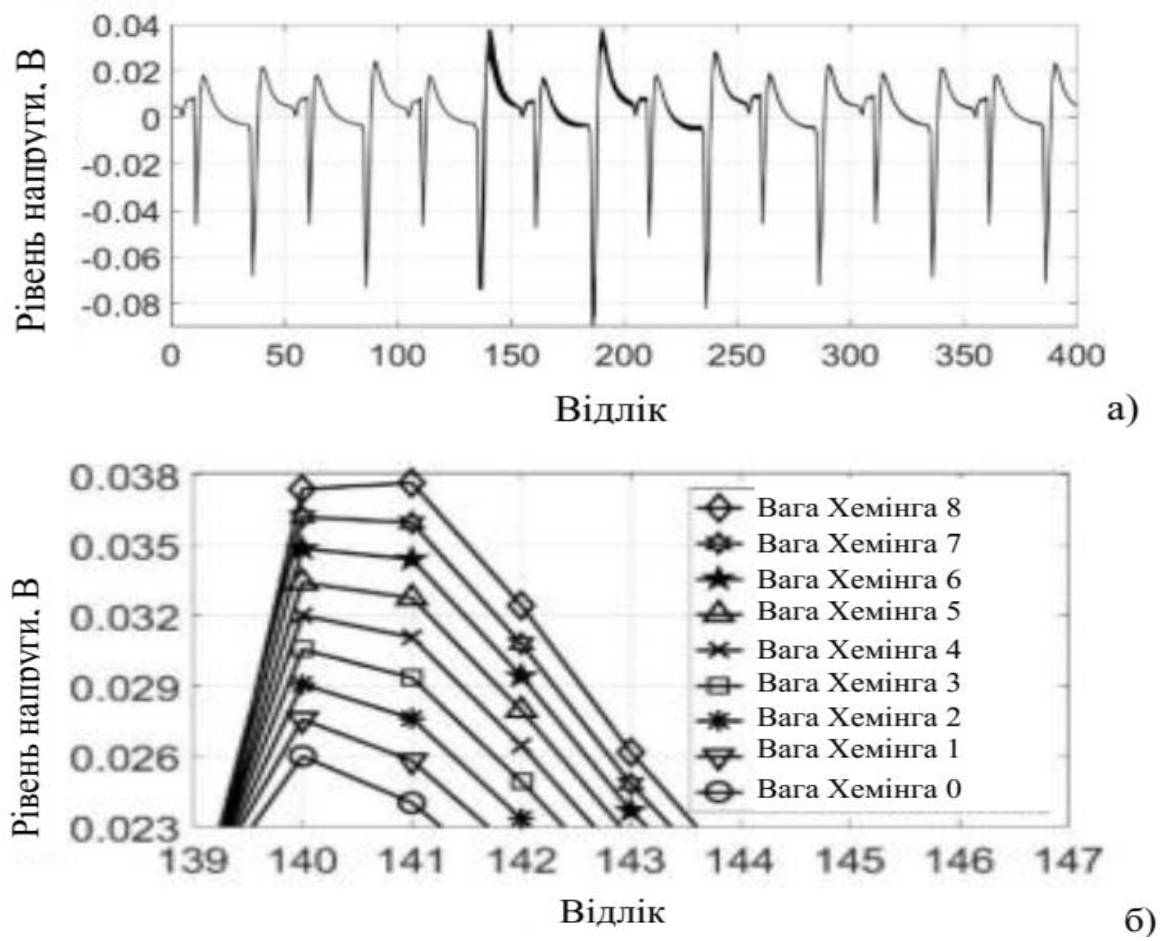


Рисунок 2.7 - Дев'ять усереднених (для мінімізації шуму) форм сигналу, отриманих під час пересилання байт з різними вагами Хеммінга, з регістру до чистої комірки ОЗУ: а) повна форма сигналу; б) збільшена ділянка з максимальним сплеском

На попередньому етапі реалізації шаблонної атаки визначаються стрибки енергоспоживання, характерні для виконання окремих операцій – ця інформація дозволить локалізувати області форми сигналу аналізованого чіпа, що характеризують енергоспоживання під час обробки даних, що залежать від ключа. Потім у цих областях форм сигналу вибираються відліки, на яких їх значення найбільшим чином відрізняються для різних ваг Хеммінга оброблюваних даних (наприклад, для форм сигналу, зображених на

рисунку 2.7б, це 140-141-й відлік – на них різниця між сплесками для різних ваг Хеммінга досягає 2.6 мВ). Через наявність шумової складової на формах сигналу значення амплітуд сплесків енергоспоживання під час виконання тієї чи іншої операції можна вважати випадковою величиною із нормальним розподілом. Тому за кожною вагою Хеммінгу оброблюваних комбінацій розраховуються середні значення вибраних відліків та середньоквадратичні відхилення (створюється шаблон). Отриманий шаблон можна подати у вигляді матриці або діаграми (рисунок 2.8), де пунктирна лінія відповідає середньому значенню 140-го відліку для відповідної ваги Хеммінга пересланої комбінації (μ(140, *hw*), де *hw* – вага Хеммінга, μ(•) – математичне очікування), а сіра область вище та нижче лінії вказує на область можливих значень відліку відповідно з правилом трьох сигм (3·σ(140, *hw*), де σ (•) – середньоквадратичне відхилення). Очевидно, що коли ці області не перекриваються, то за сплеском енергоспоживання на окремо взятій формі сигналу з ймовірністю понад 99% можна буде однозначно визначити вагу Хеммінга оброблюваної комбінації. Найчастіше через наявність великої шумової складової на формах сигналу області значень відліків перекриваються, тоді однозначне визначення ваги Хеммінга за шаблоном виявиться неможливим – у цьому випадку можна зробити висновок лише про ймовірності обробки комбінації з певною вагою Хеммінга.

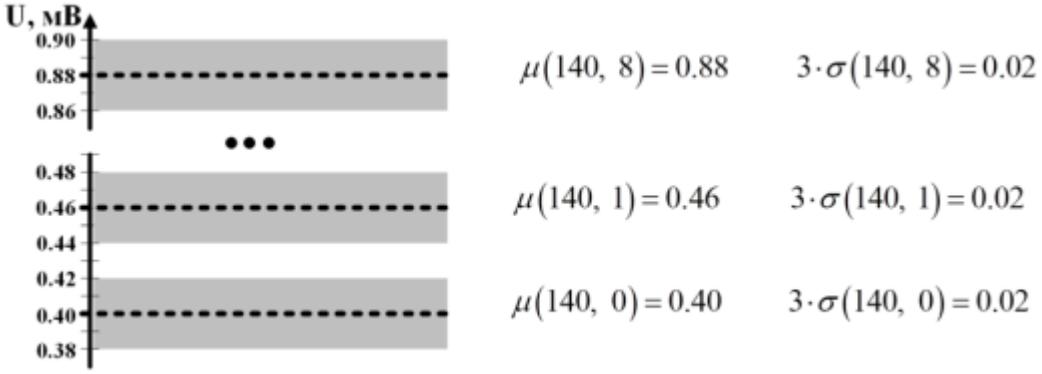


Рисунок 2.8 - Діаграма математичних сподівань і СКВ значень відліку для різних ваг Хеммінга

Визначення ваги Хеммінга деякої проміжної захисної операції перетворення не призводить до однозначного визначення секретного ключа, проте дозволяє суттєво скоротити кількість можливих ключів. Припустимо, що у (1.5) відомий підблок повідомлення $m_l(i)$ і визначена вага Хеммінга $t_l(i, r)$ – результат його складання за mod2 з ключем $k_l(r)$. Вага Хеммінга $HW(t_l(i, r))$ може набувати дев'ять значень від 0 до 8 залежно від того, в скількох розрядах відрізняються комбінації $m_l(i)$ і $k_l(r)$. Нульова вага Хеммінга говорить про ідентичність цих комбінацій. Вага Хеммінга, рівна вісім, говорить про те, що комбінації відрізняються у всіх розрядах, тобто комбінація $k_l(r)$ є інвертованою по відношенню до $m_l(i)$. У цих випадках підблок ключа може бути визначений однозначно.

Однак, якщо наприклад значення $HW(t_l(i, r))$ дорівнює одиниці, то кількість можливих варіантів підблокування ключа збільшується до восьми, оскільки невідомо, в якому саме розряді відрізняються комбінації $m_l(i)$ і $k_l(r)$. Строго аналогічна ситуація спостерігається при $HW(t_l(i, r))=7$. Кількість можливих варіантів ключа $k_l(r)$ залежно від ваги Хеммінга результату додавання $t_l(i, r)$ наведено в таблиці 2.1. З неї видно, що навіть у найгіршому випадку при вазі Хеммінга, рівній чотири, кількість можливих варіантів ключа буде скорочено більш, ніж у 3,6 рази.

Таблиця 2.1 – Кількість можливих варіантів підблоків ключа залежно від значення $HW(t_l(i, r))$

Вага Хемінга	0	1	2	3	4	5	6	7	8
К-сть варіантів ключа	1	8	28	56	70	56	28	8	1

Таким чином, для кожного з 16 підблоків раундового ключа першого раунду можна отримати масив можливих значень, який має значно менший обсяг порівняно з усіма 256-ма можливими значеннями підблоку ключа. Кількість значень у масиві очевидно можна ще скоротити, якщо аналізується не одна форма сигналу, а кілька, які отримані під час перетворення різних

повідомлень. Також кількість значень можна скоротити, аналізуючи ваги Хеммінга наступних перетворень алгоритму. Припустимо, що $m_l(i)$=00001111, $k_l(r)$=00001110. Отримаємо, що $t_l(i, r)$=00000001. Звідси $HW(t_l(i, r))$=1. Зловмиснику відомі значення $m_l(i)$ і $HW(t_l(i, r))$. Звідси він робить висновок, що ключ $k_l(r)$ відрізняється від $m_l(i)$ всього в одному розряді, тобто існує лише вісім таких ключів. Однак після перетворення комбінації $t_l(i, r)$=00000001 на S-box отримається комбінація $p_l(i, r)$=11101110 – її вага Хеммінга дорівнює шести. З восьми відібраних раніше варіантів підблоку ключа всього шість дають таку ж вагу Хеммінгу виходу S-box на повідомленні $m_l(i)$=00001111. Також необхідно зазначити, що при використанні додаткового аналізу виходів S-box вже не два, а десять із 256-ти можливих варіантів підблоку ключа можуть бути визначені однозначно. При цьому по решті ключів кількість можливих варіантів значно скоротиться, наприклад (таблиця 2.2) існує 12 варіантів підблоку ключа $k_l(r)$ при використанні в чипі яких зловмисник (у разі реалізації двоетапної атаки) отримає всього два кандидати на справжній варіант ключа.

Кількість можливих варіантів ключа може бути зменшено ще сильніше під час аналізу енергоспоживання на наступних операціях, зокрема наступних раундах.

Підсумовуючи наведене вище, можна сформувати ряд базових умов, потрібних для реалізації атаки SPA:

1) можливість підключення до ланцюгів електроживлення аналізованого чіпа;

2) можливість здійснення мінімум одного захисного перетворення на аналізованому чипі з використанням невідомого секретного ключа та відомого вхідного повідомлення;

3) наявність апаратури, що дозволяє вимірювати енергоспоживання чіпа, з високою точністю;

4) наявність у зловмисника того ж (або подібного до нього) чіпа, як чіп, на який передбачається реалізація атаки;

5) знання особливостей реалізації алгоритму захисного перетворення, що використовується чіпом.

Таблиця 2.2 – Кількість варіантів підблоків істинного ключа $k_l(r)$ (у першому рядку), відповідне кількості кандидатів на справжній варіант ключа, який отримує зловмисник при двоетапній атаці (у другому рядку)

К-сть істинних варіантів підблоку ключа	Отримана зловмисником к-сть варіантів підблоку ключа
12	2
6	3
8	4
25	5
36	6
16	8
18	9
24	12
13	13
15	15
32	32
20	20
21	21

Перші три умови, як правило є цілком здійсненними на практиці. Виконання четвертої умови звичайно може бути скрутним, але його також можна вважати обов'язковим. В ідеальному випадку необхідна наявність можливості вільного програмування тестового чіпа або хоча б можливість виконання захисного перетворення для вхідних повідомлень, що задаються зловмисником, на відомому ключі – це дозволить сформувати шаблон, який використовуватиметься для злому реального чіпа.

У разі відсутності можливості вільного програмування чипа можуть виникнути складнощі з ідентифікацією окремих операцій, що виконуються чипом. Для визначення на формі сигналу сплесків енергоспоживання, обумовлених виконанням певної операції з відомими даними, можна робити розрахунок кореляційного вектора. Останній являє собою набір коефіцієнтів кореляції між даними, оброблюваними чіпом на певному етапі виконання алгоритму, та відліками форм сигнал. У областях, що відповідають обробці даних, що розглядаються, на кореляційному векторі спостерігатимуться значні сплески. На практиці п'ята умова також є обов'язковою – без знання асемблерного коду, як правило, може бути зроблено визначення окремих раундів захисного перетворення. Проте визначення окремих операцій, що виконуються на цьому раунді, можна вважати дуже складним завданням, особливо враховуючи зашумленість форм сигналу, що знімається. Можна вважати, що основна складність реалізації атаки SPA на незахищені чіпи полягає у необхідності виконання останніх двох умов, що, стосовно реального чіпа, може виявитися дуже важкореалізованим. Необхідно відзначити, що атака SPA є безальтернативною у випадку, якщо зловмиснику доступна вкрай обмежена кількість форм сигналу від аналізованого чіпа - в граничному випадку атака може бути реалізована всього за однією формою сигналу.

Існує досить простий метод захисту від атак SPA – зменшення співвідношення сигнал-шум на формах сигналу, що знімаються. Це можна зробити двома способами, прийнятими окремо або спільно: зменшенням енергоспоживання чіпа та зашумленням ланцюгів електроживлення чіпа. В результаті значення відліку для всіх ваг Хеммінга взаємно перекриватимуться.

Отже, маючи невелику кількість форм сигналу (недостатню для усереднення шумової компоненти), зловмисник не зможе з необхідною достовірністю визначити вагу Хеммінга оброблюваних комбінацій за відповідними сплесками. З цієї причини SPA як окрему атаку можна вважати

незастосовною до сучасних чіпів, її частіше використовують як допоміжний інструмент при реалізації значно потужнішої побічної атаки диференціального (різницевого) аналізу потужності (DPA). Головною перевагою атаки DPA над SPA є відсутність необхідності наявності тестового чіпа, а також детальні знання про особливості реалізації алгоритму захисного перетворення (зазначимо, що хоч ці знання не є обов'язковими, проте їх наявність може збільшити ймовірність успішної реалізації DPA). Недолік DPA у порівнянні зі SPA – необхідність отримання більшого масиву даних про енергоспоживання чіпа (від сотень до тисяч форм сигналу).

3 РОЗРОБКА І ДОСЛІДЖЕННЯ МОДЕЛІ ПОБІЧНИХ АТАК НА ОСНОВІ ЕНЕРГОСПОЖИВАННЯ

3.1 Обгрунтування вибору апаратного забезпечення

На рисунку 3.1 показано принципову схему паралельного АЦП з вісьмома рівнями квантування. Принцип дії таких АЦП простий: на вхід подається опорна напруга $V_{ОП}$ та аналоговий сигнал $V_{СИГН}$, який необхідно перетворити на цифровий код. Опорна напруга за допомогою резистивного дільника, що складається з резисторів однакового номіналу, поділяється на сім однакових рівнів. Перетворюваний сигнал надходить на неінвертуючі входи компараторів. Опорний сигнал через дільники напруги подається на інвертуючи входи компараторів. Компаратори порівнюють вхідний сигнал АЦП з опорною напругою - якщо напруга на неінвертуючому вході компаратора перевищує напругу на інвертуючому, то на виході компаратора формується напруга логічної одиниці, інакше – логічного нуля.

Якщо напруга перетворюваного сигналу на неінвертуючому вході АЦП виявиться меншою від всіх опорних напруг, що подаються на інвертуючи входи компараторів, то на виходах всіх компараторів будуть нульові логічні рівні сигналу. Підвищуючи рівень вхідного сигналу до напруги, що перевищує напругу на інвертуючому вході нижнього компаратора, на виході останнього сформується рівень логічної одиниці, а на виході АЦП сформується код 001. При подальшому збільшенні рівня вимірюваного сигналу код прийматиме значення: 010, 011, і так далі. Максимальне значення 111 на виході АЦП сформується при перевищенні вхідним сигналом значення опорного сигналу верхнього компаратора.

АЦП, представлений рисунку 3.1, складається з восьми компараторів, він дозволяє представити в двійковому коді (цифровому вигляді) напругу від 0 до $V_{ОП}$ вісьмома рівнями з кроком $\frac{1}{7}V_{ОП}$: 0, $\frac{1}{7}V_{ОП}$, $\frac{2}{7}V_{ОП}$, $\frac{3}{7}V_{ОП}$, $\frac{4}{7}V_{ОП}$,

$\frac{5}{7}V_{ОП}$, $\frac{6}{7}V_{ОП}$, $\frac{7}{7}V_{ОП}=V_{ОП}$. Напруга буде описуватись тризначною двійковою комбінацією від 000 до 111 – це трирозрядний АЦП.

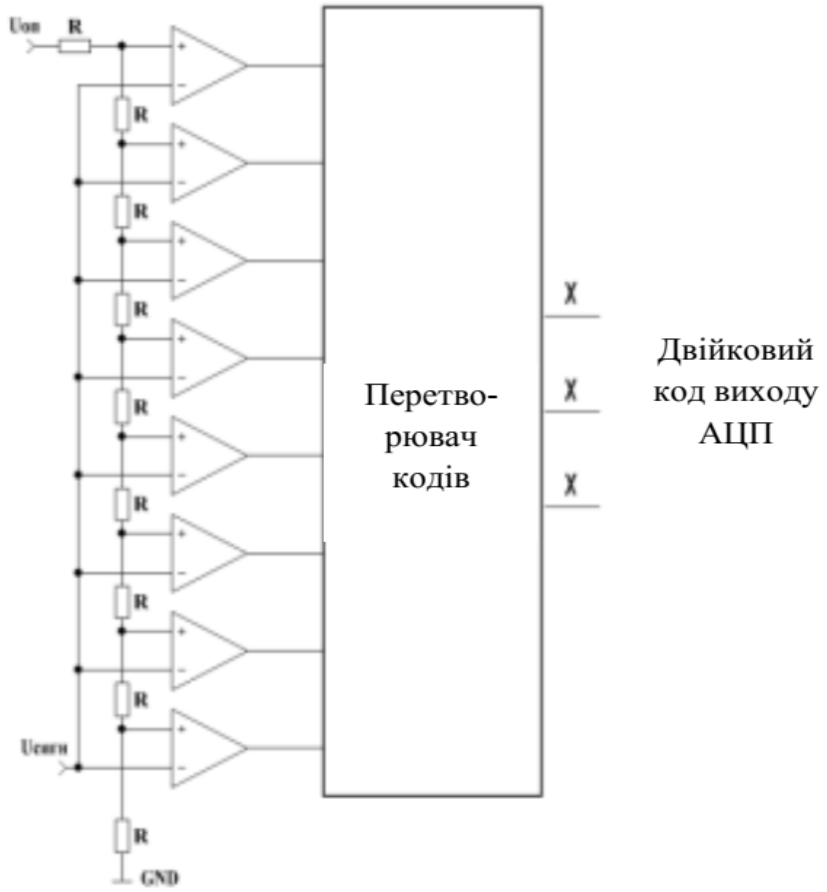


Рисунок 3.1 – Принципова схема паралельного АЦП

Наведений приклад добре ілюструє похибку АЦП, яку називають помилкою квантування. Квантований сигнал описується всього вісьмома рівнями напруги, тому значення сигналу, що знаходяться між двома рівнями, округляються до одного з них. Ця помилка визначається кроком квантування, у наведеному прикладі він становить $\frac{1}{7}V_{ОП}$. Помилки квантування є наслідком обмеженої роздільної здатності АЦП, вони властиві всім АЦП та принципово не усувні.

На рисунку 3.2 наведено блок-схему АЦП конвеєрного типу. Дискретне значення сигналу запам'ятовується у пристрої вибірки-зберігання

(ПВЗ), потім воно перетворюється на код за допомогою паралельного АЦП першої секції, при цьому дане АЦП має відносно малу розрядність N_1. Після цього отриманий код за допомогою цифро-аналогового перетворювача перетворюється назад у напругу, що представляє дуже грубе наближення до реального сигналу. Воно віднімається з точного значення напруги з ПВЗ, що надходить на суматор. Отримана різниця підсилюється і запам'ятовується в ПВЗ другої секції, потім за допомогою АЦП другої секції з розрядністю N_2 перетворюється на код.

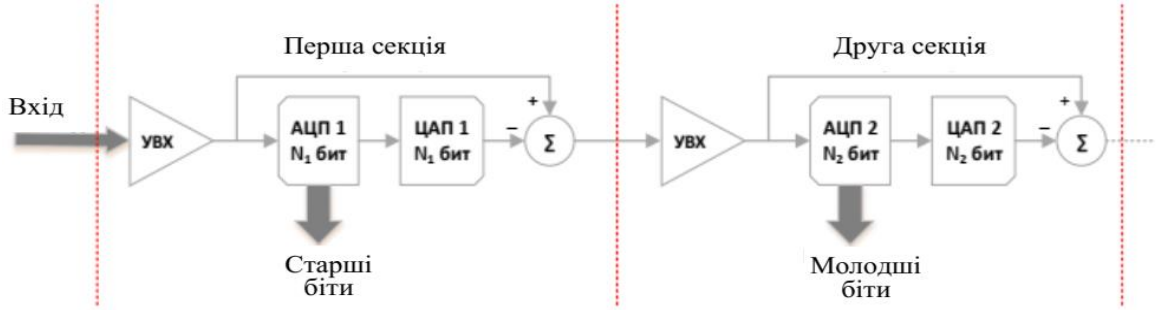


Рисунок 3.2 - Блок-схема АЦП конвеєрного типу

Таким чином, маючи дві восьмирозрядні секції (по 255 компараторів у кожній), можна отримати 16-ти розрядний АЦП. Звідси АЦП конвеєрного типу, що складається з 510 компараторів, забезпечує ту ж саму роздільну здатність, що і паралельний АЦП, який складається з 65535 компараторів. Частота квантування таких АЦП зазвичай буде нижчою, ніж паралельних, проте на сьогоднішній день для 16-тибітових АЦП конвеєрного типу можлива робота на частотах 200-400 МГц. Варто зауважити, що кількість компараторів може бути знижена ще сильніше за рахунок збільшення числа секцій, проте це неминуче призведе до зниження частоти квантування.

З технічної документації мікроконтролера Atmel ATmega16 відомо, що він має Гарвардську архітектуру, тобто є окрема пам'ять та шина адреси для програм і для даних. Отже, за кожен такт (починаючи з приходу

наростаючого фронту тактового сигналу) здійснюється виконання поточної інструкції та вибірка з пам'яті програм наступною (рисунок 3.3).

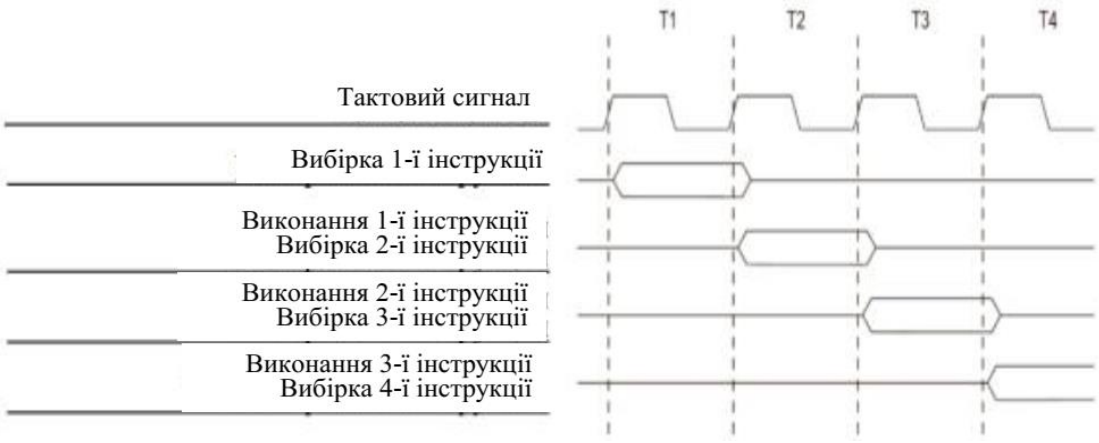


Рисунок 3.3 - Етапи виконання інструкцій мікроконтролером Atmel ATmega 16

Пам'ять програм (Flash пам'ять) мікроконтролера призначена для зберігання послідовності команд, що керують його функціонуванням, та має 16-ти бітову організацію. Число циклів стирання/запис - не менше 10 тис. Пам'ять даних розділена на три області: реєстрова пам'ять, ОЗП та EEPROM. Регістрова пам'ять включає 32 робочі регістри, і службові регістри портів вводу/виводу. Всі вони розташовані в адресному просторі ОЗП, але не є його частиною, вони мають байтовий формат. В області регістрів вводу/виводу розташовані різні службові регістри (регістри управління мікроконтролером, регістри статусу тощо), а також регістри управління периферійними пристроями, що входять до складу мікроконтролера. По суті, управління мікроконтролером полягає в управлінні цими регістрами.

Для довготривалого зберігання різної інформації, яка може змінюватися в процесі функціонування мікроконтролера, використовується EEPROM-пам'ять. Цей тип пам'яті зручний для зберігання проміжних даних, різних констант, коефіцієнтів, серійних номерів, ключів тощо. EEPROM може бути записана як при програмуванні мікроконтролера, так і у процесі

його функціонування. Кількість циклів стирання/запису – щонайменше 100 тис.

ОЗП використовується для оперативного зберігання даних. Число циклів читання та запису в ОЗП не обмежене, але при відключенні напруги живлення вся інформація втрачається. Відмінність між робочими регістрами та оперативною пам'яттю у тому, що з регістрами можна проводити будь-які операції, а щодо оперативної пам'яті доступні лише операції читання/запису даних з/в регістри.

Всі команди обробляють дані (операнди) у вигляді байтів, що містяться в будь-якому з 32-ох робочих регістрів мікроконтролера, в які вони можуть бути завантажені і з яких вони можуть бути вивантажені в ОЗП та EEPROM. Безпосереднє виконання команд здійснюється в АЛУ. Після завантаження програми мікроконтролера в пам'ять програм в спеціальний регістр, що називається лічильником команд, записується адреса комірки пам'яті програм, що містить першу команду. У процесі виконання програми на першому такті АЛУ зчитує з лічильника команд адресу комірки пам'яті програм (вибірка першої інструкції), та інкремент лічильника команд, а на другому такті проводиться виконання першої команди і водночас виконується читання другої команди за адресою, на який вказує лічильник команд, також виробляється інкремент лічильника команд тощо. Більшість команд виконується мікроконтролерами Atmel за один такт звернення до ОЗП, ПЗП. Команди передачі управління, як правило, виконуються за 2-3 такти. У документації до мікроконтролера ATmega16 наведено приклад виконання "простої" команди, що виконується за один такт (рисунок 3.4).

Таким чином реалізується, наприклад, операція додавання по mod2 (XOR). Вона може бути здійснена тільки з байтами, що знаходяться у двох робочих регістрах (у робочі регістри дані попередньо можуть бути завантажені з ОЗП або ПЗУ за допомогою відповідних команд). Підкреслимо, що паралельно з виконанням команди, схематично показаною на рисунку 3.4, здійснюється читання з пам'яті програм наступної команди (дана особливість

гарвардської архітектури призведе до накладання алгоритмічного шуму на аналізовані відліки, оскільки на значення напруги, що характеризують енергоспоживання в процесі виконання команди, будуть накладатися значення напруги, що відносяться до наступної команди).

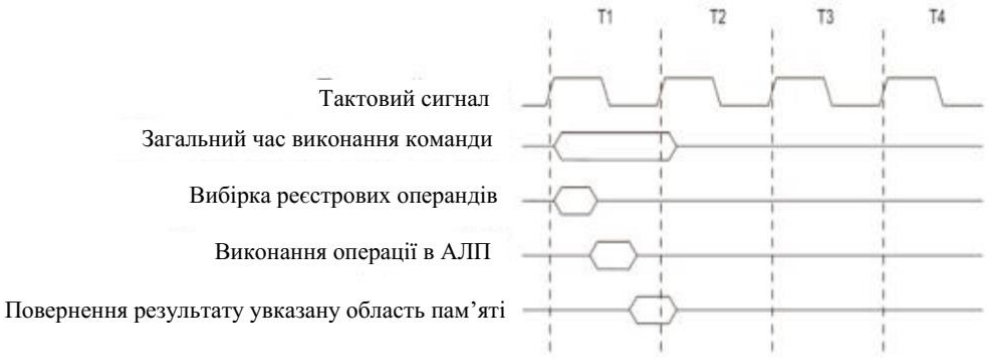


Рисунок 3.4 - Етапи виконання інструкції для «простої команди» мікроконтролером Atmel ATmega 16

Отже, на першому етапі з двох регістрів проводиться вибірка байт, які необхідно скласти по mod2 - вони подаються на АЛП. На другому етапі АЛП здійснює операцію додавання по mod2, а на третьому етапі результат надходить з АЛП в один із робочих регістрів, що беруть участь в операції, перезаписуючи один із доданків (надалі результат може бути залишений у регістрі або скопійований в ОЗП/ПЗП за допомогою відповідних команд).

3.2 Реалізація табличного перетворення S-box на мікроконтролерах Atmel з використанням підходу «читання зі зміщенням»

Восьмирозрядна архітектура чіпа передбачає, що в будь-яких перетвореннях чіп оперує як мінімум байтами (маючи відповідно восьмирозрядні шини, регістри, АЛП). Поступаючий для шифрування блок повідомлення $m(i)$ розбивається на восьмибітові частини і зберігається в регістрах або ОЗП (займаючи вісім байт), секретний ключ логічно спочатку перетворити в раундові ключі $k(r)$, де r – номер раунда, і зберігати в ПЗП

(замість того, щоб для кожної ітерації шифрування виробляти заново). Для того, щоб скласти праву частину повідомлення з раундовим ключем, байт повідомлення і ключа потрібно зчитати в регістри, після чого виконати операцію арифметичного додавання цих двох регістрів. При цьому результат буде записаний в один з них (перезаписуючи один з доданків). Потім результат може бути скопійований в ОЗП, замінюючи для прикладу відповідний байт повідомлення *m(i)*. Ця операція повторюється для решти трьох восьмибітових блоків повідомлення і раундового ключа. Аналогічно відбувається операція додавання по mod2.

Таким образом, операція додавання по $\mathrm{mod}2^{32}$ $m(i)+k(r)$ буде здійснюватися побайтно – від молодших байт до старших (це дозволить врахувати перенос біт в сусідній розряд). Після цього отримані чотири восьмибітові блоки повинні бути перетворені на восьми S-box. Очевидно, що перетворення на S-box ефективніше реалізовувати побайтно, але спочатку необхідно пояснити, як ці перетворення реалізуються на практиці. Спочатку опишемо реалізацію перетворень на S-box, які передбачають обробку кожного S-box окремо для того, щоб проілюструвати неефективність чотирьох бітових перетворень на восьмибітовій архітектурі чипа. Будь-яке табличне перетворення на типовому асемблері реалізується з використанням підходу, який називається «читанням зі зміщенням». При програмуванні чипа в комірки його ПЗП (під ПЗП розуміється Flash або EEPROM-пам’ять – їх використання зумовлено тим, що записані в них дані зберігаються навіть після відключення живлення від чіпа) послідовно один за одним записуються всі вихідні значення S-box, починаючи із значення, яке отримується у випадку приходу на вхід комбінації 0: «0000», потім 1: «0001» і т. д., до вихідного значення, отриманого по приходу комбінації 15: «1111». При цьому адрес першої комірки заноситься в пам’ять програм, дана операція повторюється для всіх восьми S-box. При цьому кожне вихідне значение S-box записується у вигляді байта, чотири старших біта якого будуть нульовими, значущими є тільки чотири молодших біти.

3.3 Аналіз характеристик форм сигналу

Форми сигналу, зняті вимірювальною установкою, характеризують падіння напруги на резисторі, вставленому в розрив лінії землі мікроконтролера. Це падіння напруги пропорційне споживаній мікроконтролером потужності. Значення кожного відліку форми сигналу можна охарактеризувати п'ятьма складовими:

- постійна складова, обумовлена струмами витоку: $U_{\text{ПОСТ. ШУМ}}$;
- постійна складова, обумовлена алгоритмічним шумом: $U_{\text{АЛГ. ШУМ}}$;
- постійна складова, обумовлена виконуваною операцією (командою) $U_{\text{ОП}}$;
- шумова складова обумовлена електронним шумом (вона змінюється на кожній формі сигналу): $U_{\text{ЕЛ. ШУМ}}$;
- складова, що залежить від даних $U_{\text{ДАН}}$, що обробляються.

Всі перелічені складові сигналу є унікальними для кожної конкретної моделі чіпа, а шумова складова $U_{\text{ЕЛ.ШУМ}}$ додатково визначається характеристиками вимірювальної установки, а також електромагнітною зашумленістю навколишнього середовища.

Корисною для зловмисника є складова $U_{\text{ДАН}}$, оскільки вона безпосередньо залежить від даних, що обробляються. Складова $U_{\text{ОП}}$ може використовуватися для ідентифікації окремих операцій, що виконуються чіпом, у разі відсутності в зловмисника докладної інформації про виконуваний аналізований чіп алгоритм. При статистичному аналізі $U_{\text{ОП}}$ не впливає на успішність атаки, тому що для конкретної операції вона є константою. Постійна складова $U_{\text{ПОСТ.ШУМ}}$ ніяк не впливає на успішність проведеної атаки, так як не залежить від даних, що обробляються, і на кожному такті роботи чіпа буде приблизно однаковою: $Var\ (U_{\text{ПОСТ.ШУМ}})=0$, $E\ (U_{\text{ПОСТ. ШУМ}})=\text{const}$, де $Var\ (\bullet)$ – дисперсія; $E(\bullet)$ – математичне очікування. Постійна складова $U_{\text{АЛГ. ШУМ}}$ впливає на успішність проведеної атаки, так як, по-перше, є додатковою шумовою компонентою (для її мінімізації потрібна

обробка більшої кількості форм сигналу); по-друге, окремі її компоненти можуть мати залежність від оброблюваних даних. В цьому випадку її повне усунення усередненням буде неможливо. Шумова складова $U_{\text{ЕЛ. ШУМ}}$ також очевидно впливає на успішність атаки, що проводиться. Вона, як правило, має гауссівський розподіл з нульовим середнім. Її вплив на результат атаки може бути мінімізований шляхом усереднення форм сигналу. Для перевірки цієї гіпотези мікроконтролер було запрограмовано на багаторазове виконання команди «nop» –порожня команда. Вона виконується за один такт роботи, при цьому вміст регістрів даних, ОЗП, ПЗП, шини даних не змінюються. Перед виконанням цих операцій мікроконтролер відсилав на АЦП тригерний сигнал (логічну «1»), який запускав збір даних, та подальше вивантаження отриманої форми сигналу. Усього було знято 102 400 форм сигналу. Приклад однієї з них представлений рисунку 3.5.

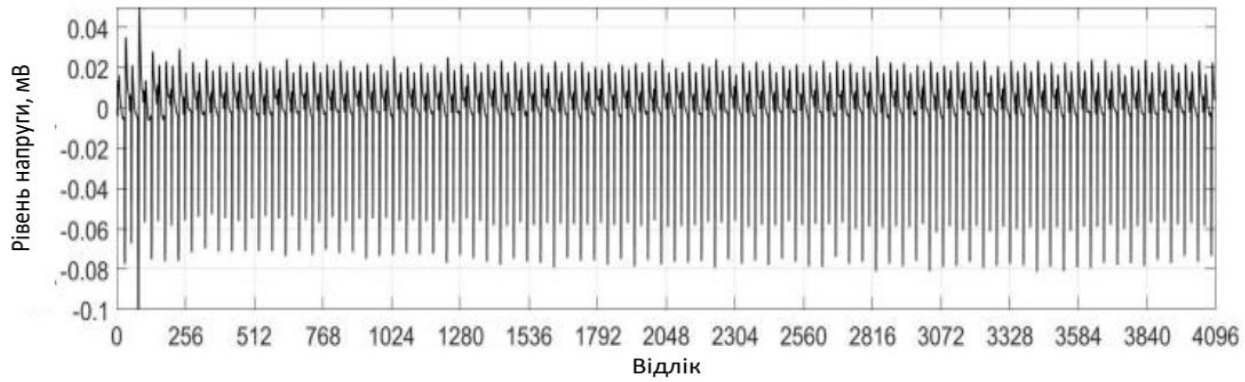


Рисунок 3.5 - Форма сигналу, що характеризує енергоспоживання мікроконтролера Atmel при виконання операцій «nop»

Необхідно пояснити деякі особливості одержуваних від АЦП форм сигналу:

- вхідний тракт АЦП видаляє постійну низькочастотну складову сигналу, однак на ефективність реалізації побічних атак по ланцюгах електроживлення ця особливість вплине, оскільки для них важливі лише відносні високочастотні зміни сигналу;

- на осі ординат та осі абсцис відкладаються не абсолютні значення напруги та часу, а відносні. По осі ординат відкладено рівні напруги (привести їх до абсолютних значень можна, співвідносячи з динамічним діапазоном АЦП від -1,8 В до 1,8 В. Наприклад, значення на осі ординат, що дорівнює одному рівню напруги, буде еквівалентне 1,8, значення -0,5 буде еквівалентне -0.9 В.). По осі абсцис відкладені відліки. Інтервал між двома сусідніми відліками еквівалентний часовому інтервалу, зворотному частоті дискретизації тактового генератора АЦП, тобто 1/(100 МГц)=10 нс. Також необхідно помітити, що за стрибками напруги можна дуже просто визначити струм, що протікає, і споживану потужність. Враховуючи, що форми сигналу характеризують падіння напруги на резисторі, опір якого складає $R_{ВИМ}$=10 Ом, то за законом Ома миттєве значення протікаючого через нього струму визначається так:

$$I_{ЗАГ}(t) = \frac{U_{ЗАГ}(t)}{R_{ВИМ}} = \frac{U_{ЗАГ}(t)}{10\ \ Ом}, \qquad (3.1)$$

де $U_{ЗАГ}(t)$ - падіння напруги на резисторі, зняте в момент часу t;

$I_{ЗАГ}$ - сила струму, що протікає по ланцюгу електроживлення мікроконтролера в той же момент часу.

Споживана потужність визначається так:

$$P_{ЗАГ}(t) = I_{ЗАГ}(t) \cdot U_{ЖИВЛ} = \frac{U_{ЗАГ}(t)}{R_{ВИМ}} \cdot U_{ЖИВЛ} = \frac{U_{ЗАГ}(t)}{10\ \ Ом} \cdot 5B, \qquad (3.2)$$

де $U_{ЖИВЛ}$=5 В – напруга живлення чіпа.

Таким чином, миттєве значення споживаної чіпом потужності можна отримати діленням відповідного значення напруги (визначеного за знятими формами сигналу) на коефіцієнт 0,5.

В даному експерименті для тактування мікроконтролера використовувався кварцовий генератор із частотою 2 МГц, тому тривалість одного такту роботи мікроконтролера складає близько 1/(2000000 Гц)=500 нс, що відповідає 50 відлікам на знятих формах сигналу. На рисунку 3.6 кожні 2 сплески (наприклад, з 1933 по 1983 р. відліки) якраз мають тривалість 50 відліків. Звідси логічно припустити, що кожна пара сплесків характеризує енергоспоживання мікроконтролера на одному такті роботи.

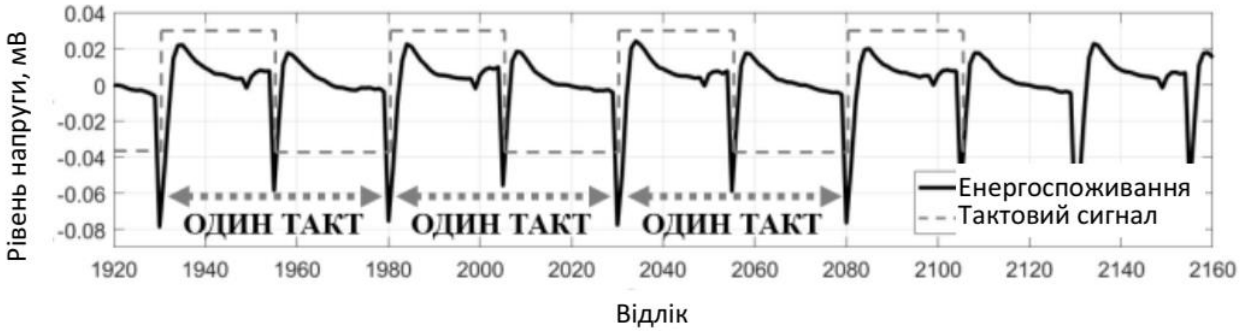


Рисунок 3.6 – Ділянка форми сигналу, отримана при виконанні команди «nop»

Можна передбачити, що від'ємний сплеск в середині такту (рисунок 3.7) і пропорційні його амплітуді частини сплесків на кінцях такту зумовлені струмом короткого замикання $I_{КЗ}$. Струмами зарядки паразитних ємностей I_C зумовлені невеликі частини сплесків на кінцях такту. Необхідно підкреслити, що наведені на рисунку 3.7 сплески характеризують енергоспоживання усіх ЛВ, які формують чіп, у відповідний момент часу. Серед них знаходяться ЛВ, які обробляють інформацію, що представляє інтерес для зловмисника.

За рахунок нестабільності тактових генераторів мікроконтролера і АЦП сплески на отриманих формах сигналу від вимірювання до вимірювання будуть зміщуватися по часовій шкалі на 5-7 відліків, тобто на 50-70 нс. (рисунок 3.8а). Очевидно, що даний ефект буде істотно затрудняти машинний аналіз енергоспоживання при виконанні будь-якої команди. Отже,

потрібне вирівнювання флуктуацій форм сигналу (рисунок 3.8б). Вирівнюванн передбачає суміщення сплесків напруги в межах розглянутого такту.

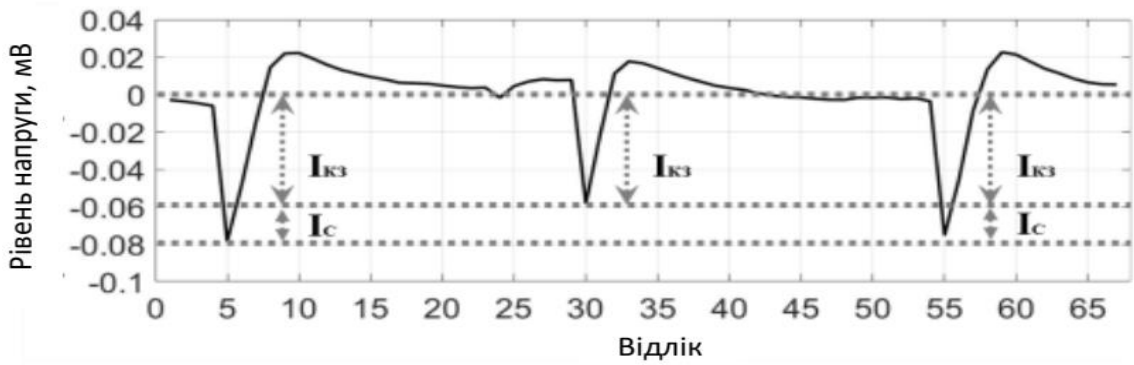


Рисунок 3.7 – Ділянка форми сигналу, яка характеризує енергоспоживання на одному такті роботи чипа

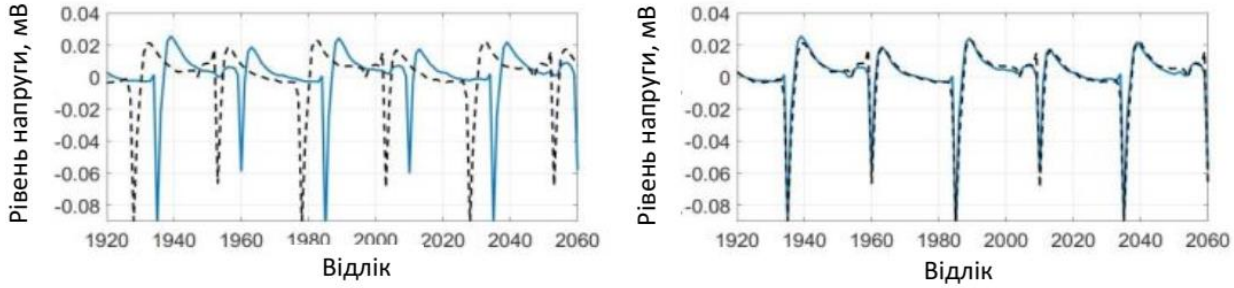


Рисунок 3.8 - Дві форми сигналу: а) до; б) після вирівнювання флуктуацій

Якщо розглядати дві форми сигналу, зображені на рисунку 3.8а, то необхідно сумістити сплеск на 1938-м відліку першої форми сигналу з сплеском на 1934-м відліку другої форми сигналу. Це можна зробити, наприклад, зсунувши другу форму сигналу на 5 відліків праворуч. Вдобавок, для зниження часу обробки і об’єму пам’яті, яка вимагається для зберігання форм сигналу, їх можна обрізати з правої та лівої сторін, залишивши тільки відліки, які характеризують досліджувані такти роботи мікроконтролера.

Технічно процес вирівнювання заключається в заданні «вікна», в якому знаходиться деякий яскраво виражений сплеск. В наведеному прикладі це коливання напруги між 1920-м та 1945-м відліками. В цьому вікні для кожної

форми сигналу відбувається пошук максимального від’ємного сплеску (тобто мінімального значення). Потім зчитується 15 відліків до цього значення і 125 відліків після. Таким чином відбувається деяка «привязка» до від’ємного сплеску, яка дозволяє досить якісно вирівняти усі 102 400 форми сигналу. В цьому випадку гістограма розподілу, для прикладу, 1938-го відліку (максимальний додатній сплеск на першому такті рисунка 3.8б) прийме класичну гаусівську форму дзвона (рисунок 3.9б) на відміну від розподілу того ж відліку до вирівнювання форм сигналу (рисунок 3.9а).

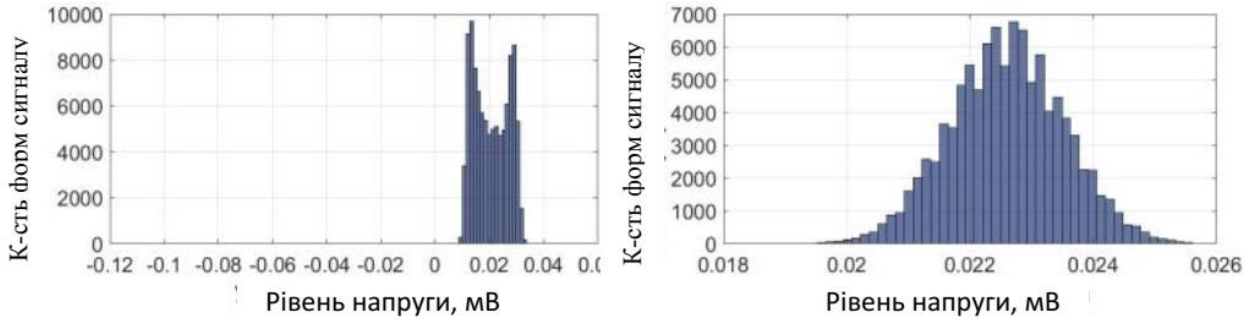


Рисунок 3.9 - Гістограми розподілу значень 1938-го відліку: а) до; б) після вирівнювання форм сигнала

Математичне сподівання розглянутого відліку становить порядку 0.0226 (що еквівалентне 41 мВ). Враховуючи правило трьох сигм, згідно якого 0.9973% значень випадкової величини лежить в діапазоні (x–3σ; x+3σ), де σ – середньоквадратичне відхилення, отримується, що СКВ значень відліку становить порядку 0.00094 (що еквівалентно 1.7 мВ). Значення відліку на приблизно 0,0027% (264) формах сигналу будуть виходити за межі ±3σ (= 0.00282 ~ 5.1 мВ). Мінімальне значення, яке приймається 1938-м відліком, становить порядку 0.004 (7.2 мВ), максимальне – порядку 0.04 (72 мВ). На рисунку 3.10 наведені дві форми сигналу (крайні випадки), на яких 1938-й відлік приймає вказані значення. Звідси видно, що навіть в таких «крайніх» випадках алгоритм вирівнювання виконується коректно.

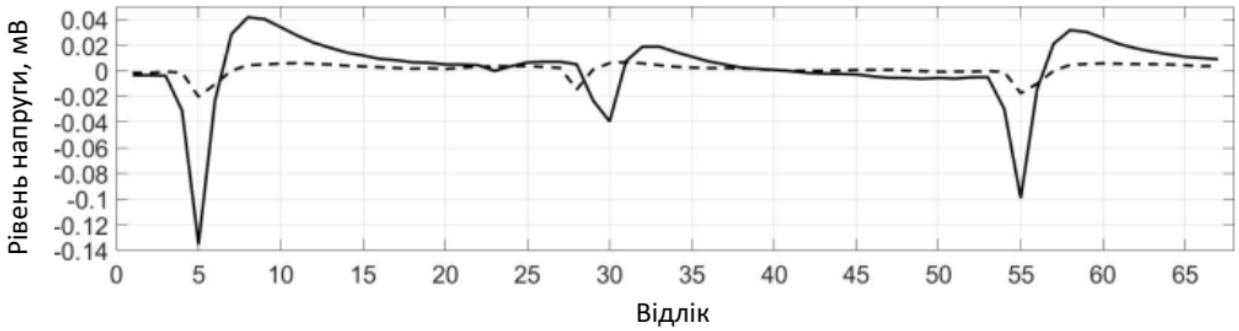


Рисунок 3.10 - Дві форми сигналу, на яких 1938-й відлік має максимальне (суцільна лінія) та мінімальне (пунктирна лінія) значення; форми сигналу є вирівняними і, для оптимізації процесу їх наступної обробки, обрізаними з правої та лівої сторін, в результаті чого 1938-й відлік змістився на місце п’ятого відліку

Так як в даному прикладі мікроконтролер виконав одну і ту ж операцію і спостереження за енергоспоживанням відбувалось в одному і тому ж відліку знятих форм сигналу, то тоді $Var(U_{ПОСТ.\ ШУМ})=Var(U_{АЛГ.\ ШУМ})=$ $=Var(U_{ОП})=Var(U_{ДАН})=0$, $E(U_{ПОСТ.\ ШУМ})=\text{const}$, $E(U_{АЛГ.\ ШУМ})=\text{const}$, $E(U_{ОП})=\text{const}$, $E(U_{ДАН})=\text{const}$.

Це означає, що електронний шум у використаній вимірювальній установці має СКВ порядку 5.1 мВ, при нульовому математичному сподіванні (після виконання процедури мінімізації шуму тактового генератора).

ВИСНОВКИ

1. Здійснено аналіз існуючих інтегральних схем як основного програмно-апаратного засобу для захисту інформації, що дало змогу охарактеризувати фізичні основи побічних атак по ланцюгах електроживлення.

2. Розроблено математичні моделі «витоку» інформації з ланцюга електроживлення, що дозволило встановити загальну будову вимірювальної установки та обґрунтувати варіанти вибору апаратного забезпечення.

3. Досліджено та проаналізовано характеристики основних форм сигналу, що дозволило розробити відповідні рекомендації для захисту від атак на побічні канали електроживлення.

4. Розроблено схему загальної будови вимірювальної установки та реалізовано табличне перетворення S-box на мікроконтролерах Atmel з використанням підходу «читання зі зміщенням».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Волокітін А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Інформаційна безпека державних організацій і комерційних фірм. К.: Юніор, 2012. 303 с.
2. Петраков А.В. Основи практичного захисту інформації. К.: Юніор, 2009. 395 с.
3. Global Internet Phenomena Report – Asia pacific, Africa and the middle-east. Sandvine inc. 2016. URL: https://www.sandvine.com/ resources/global-internet-phenomena/2016/asia pacific-africa-and-the-middle-east.html.
4. Кладій Ю.М., Максим'юк А.І., Осадчук О.Й., Скриник В.Я. Алгоритм ідентифікації мережевого трафіку та його тестування. Збірник матеріалів проблемної наукової міжгалузевої конференції «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2021). Тернопіль, 2021. С.11-12.
5. Інформаційна безпека: навчальний посібник. Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
6. ISO/IEC 15288:2008. Systems and software engineering – System life cycle processes [Електронний ресурс]. Режим доступу: http:\\www.iso.org\ standart\43564.html
7. Moradi A., Barenghi A., Kasper T., Görtz H., Paar C. On the vulnerability of FPGA bitstream encryption against power analysis attacks: extracting keys from xilinx Virtex-II FPGAs. Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS 2011). 2011. P. 111-124.

8. Kocher P., Jaffe J., Jun B., Wiener M. Differential Power Analysis. Advances in Cryptology — CRYPTO’ 99. CRYPTO 1999. Lecture Notes in Computer Science. 1999. Vol. 1666. P. 388-397.

9. Mangard S., Lee P.J., Lim C.H. A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion. Information Security and Cryptology – ICISC 2002. ICISC 2002. Lecture Notes in Computer Science. 2003. Vol 2587. P. 343-358.

10. May D., Muller H.L., Smart N.P., Koç Ç.K., Naccache D., Paar C. Random register renaming to foil DPA. Cryptographic Hardware and Embedded Systems — CHES 2001. CHES 2001. Lecture Notes in Computer Science. 2001. Vol 2162. P. 28-38.

11. Jaffe J. More Differential Power Analysis: Selected DPA Attacks. ECRYPT Summerschool on Cryptographic Hardware, Side Channel and Fault Analysis. 2006.

12. Joye M., Olivier F., van Tilborg H. Side-Channel Analysis. Encyclopedia of Cryptography and Security. 2005. P. 571-576.

13. Hnath W., Pettengill J. Differential Power Analysis Side-Channel Attacks in Cryptography [Електронний ресурс]. 2010. 42 с. Режим доступу: https://pdfs.semanticscholar.org/f6bc/06ad389ccd63614f9e2d882ca1d8b9042cae.pdf.

14. Mangard S., Oswald E., Popp T. Power Analysis Attaks: Revealing the Secrers of Smart Card. [USA]: Springer US, 2017. 338 p.

15. Peeters E. Advanced DPA Theory and Practice: Towards the Security Limits of Secure Embedded Circuits. New York: Springer-Verlag New York, 2013. 139 p.

16. ATmega16A [DATASHEET] [Електронний ресурс]: Atmel Corporation - Microcontrollers, 32-bit, and touch solutions. Режим доступу: http://www.atmel.com/images/atmel-8154-8-bit-avratmega16a_datasheet.pdf.

17. National Supercomputing Center in Wuxi [Електронний ресурс]. Режим доступу: http://demo.wxmax.cn/wxc/ introduction.php?word= introduction&i=34.

18. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. К.: КПІ ім. Ігоря Сікорського, 2018. 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

19. Остапов С. Технології захисту інформації. Посібник. Родовід, 2014. 428 с.

20. Akkar M., Giraud C. Koç Ç.K., Naccache D., Paar C. An implementation of DES and AES secure against some attacks. Cryptographic Hardware and Embedded Systems — CHES 2001. CHES 2001. Lecture Notes in Computer Science. 2001. Vol. 2162. P. 309-318.

21. Mace F., Standaert F.-X., Hassoune I., Legat J.-D., Quisquater J.-J. A dynamic current mode logic to counteract power analysis attacks. Proceedings of DCIS 2004. 2004. P. 186-191.

22. Alshammari R., Zincir-Heywood A.N. An Investigation on the Identification of VoIP traffic: Case study on Gtalk and Skype. International Conference on Network and Service Management (CNSM). 2010. С. 310– 313.

23. Концевич О.О., Бойко Н.З., Савіцький Т.Д. Моделювання та досліження атаки енергоспоживання на основі ваги Хемінга. Збірник матеріалів проблемної наукової міжгалузевої конференції «Автоматизація та комп’ютерно-інтегровані технології» (АКІТ-2022). Тернопіль, 2022. С.94-96.

24. Концевич О.О., Катеринюк С.А., Додь О.А. Експериментальне дослідження атаки енергоспоживання Збірник матеріалів проблемної наукової міжгалузевої конференції «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2022). Тернопіль, 2022. С.108-110.

25. Bhattacharya S. Cryptology and information security - past, present, and future role in society. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.

26. What is Spring Security? August 13, 2018 [Електронний ресурс] URL: https://www.developer.com/java/ent/whatis-spring-security.html.

27. Spring Security authentication. October 30, 2018. [Електронний ресурс] URL: http://shazsterblog.blogspot.com/2018/10/spring-security-authenticationsecurity.html.

28. Advantages and Disadvantages of Certificate Authentication. [Електронний ресурс]. URL: https://www.ssh.com/manuals/server-zosproduct/55/ch06s03s05.html.

29. Masoumi M., Rezayati M.H. Novel Approach to Protect Advanced Encryption Standard Algorithm Implementation Against Differential Electromagnetic and Power Analysis. IEEE Transactions on Information Forensics and Security. 2015. Vol. 10. P. 256-265.

30. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Symmetric Cryptoalgorithms in the Residue Number System. Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.

31. Гапак О.М. Криптоаналіз. Криптографічні протоколи. Навчальний посібник. Ужгород: Ужгородський національний університет, 2021. 93 с.

32. Skorobogatov S.P. Semi-invasive attacks – A new approach to hardware security analysis. Technical Report UCAM-CL-TR-630. University of Cambridge. Computer Laboratory. 2005. 144 p.

33. Kocher P., Jaffe J., Jun B., Wiener M. Differential Power Analysis. (eds) Advances in Cryptology — CRYPTO’ 99. CRYPTO 1999. Lecture Notes in Computer Science. 1999. Vol. 1666. P. 388-397.

34. ASIC basics tutorial [Електронний ресурс]: Radio-Electronics.com: resources, analysis & news for electronics engineers. – Режим доступу: http://www.radioelectronics.com/info/data/semicond/asic/asic.php.


АВТОМАТИЗАЦІЯ
ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ
ТЕХНОЛОГІЇ
проблемно-наукова міжгалузева
конференція молодих науковців
аспірантів та студентів
м. Тернопіль
2022

ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
НАДВІРНЯНСЬКИЙ КОЛЕДЖ НТУ
ГАЛИЦЬКИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

Проблемно-наукова міжгалузева конференція

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (АКІТ – 2022)

21—23 лютого 2022 року

Тернопіль

БЕЗПЕКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 519.7

Концевич О.О.[1], Бойко Н.З.[2], Савіцький Т.Д.[1]

[1]Західноукраїнський національний університет
[2]Тернопільський технічний ліцей Тернопільської міської ради

МОДЕЛЮВАННЯ ТА ДОСЛІЖЕННЯ АТАКИ ЕНЕРГОСПОЖИВАННЯ НА ОСНОВІ ВАГИ ХЕМІНГА

Вступ. Безпека сучасних інформаційно-комунікаційних систем нерозривно пов'язана з алгоритмами, що забезпечують конфіденційність і цілісність інформації, яка зберігається і передається, а також функції ідентифікації та аутентифікації. Стійкість цих алгоритмів базується на обчислювальній складності рішення деяких задач. У 1999 році вперше було показано, що, до прикладу, такий параметр, як енергоспоживання інтегральної схеми, має явну залежність від даних, що обробляються. Тому, знявши форму сигналів, які характеризують енергоспоживання чипа в процесі виконання алгоритма деякого захисного перетворення і задіявши відносно нескладний математичний апарат простого або диференціального аналізу енергоспоживання (відповідно, атаки SPA або DPA), виявляється можливим відновити секретну інформацію, яка обробляється чипом (в конкретному секретному ключі шифру) [1]. Даний клас атак називають атаками по побічних каналах (або побічними атаками). Побічні атаки ґрунтуються на ідеї використання «витоку» інформації про секретні дані, які містяться в чипі, від його фізичних параметрів.

Мета: моделювання та дослідження атаки енергоспоживання на основі ваги Хемінга.

1. Модель «витоку» інформації з ланцюга електроживлення

Вхідний сигнал може здійснити чотири типи переходів, і якщо при (умовних) переходах 0→0 або 1→1, споживана з мережі живлення потужність $P_{0\to0}$ та $P_{1\to1}$ буде практично відсутня, то при переходах 0→1, 1→0 вона буде значною (робота логічного вентиля, у процесі якої логічний рівень на вході ЛВ змінюється – називають [2] динамічним режимом). Потужність, що споживається логічним вентилем у динамічному режимі, крім статичної складової, визначається ще й динамічною (таблиця 1), яка, у свою чергу, обумовлена двома причинами: струмом короткого замикання та струмом заряду паразитних ємностей.

Таблиця 1 - Переходи логічних рівнів інвертора

Перехід	Споживана потужність	Тип споживаної потужності
0→0	$P_{0\to0}$	Статична
0→1	$P_{0\to1}$	Статична+динамічна
1→0	$P_{1\to0}$	Статична+динамічна
1→1	$P_{1\to1}$	Статична

Для того, щоб зв'язати енергоспоживання чіпа з оброблюваними даними, необхідно подати його математичну модель. Ця модель може мати різні рівні точності. Чим вищий рівень точності, тим більше потрібно обчислювальних

ресурсів та інформації про чип. Припустимо, що у момент часу i (наприклад у робочому регістрі) є комбінація M_i, а в наступний момент часу i+1 в даний регістр з ОЗУ була завантажена комбінація M_{i+1}. Тоді потужність, що витрачається на дану зміну, буде пропорційна $HW(M_i \oplus M_{i+1})$, де $HW(*)$ – це вага Хеммінга. Наприклад, якщо восьмибітова двійкова комбінація «1111 1111» змінилася на комбінацію «1111 0000», то відстань Хеммінга між цими двома комбінаціями дорівнюватиме чотири – простіше кажучи у чотирьох з восьми розрядів значення біт зміняться (рисунок 1), отже, з мережі живлення, крім статичної потужності (що споживається всіма ЛВ чіпа), буде споживатися динамічна потужність, обумовлена перемиканням чотирьох ЛВ, що становлять чотири осередки розглянутого регістру.

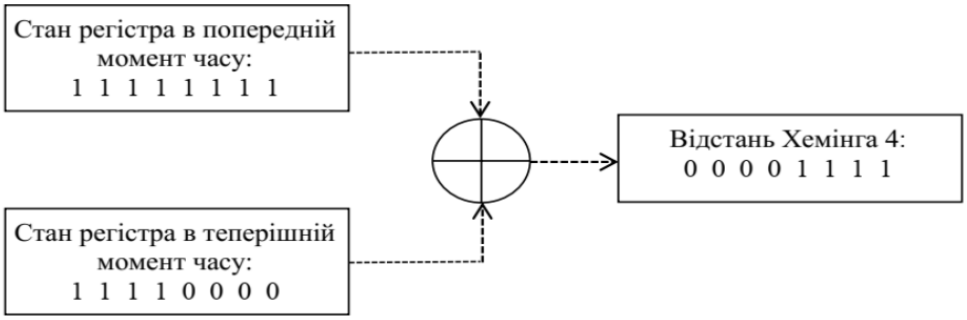


Рисунок 1 - Модель енергоспоживання на основі відстані Хеммінга

2. Дослідження розробленої моделі

На рисунку 2 зображені сплески енергоспоживання, характерні для виконання цієї операції на аналізованому мікроконтролері Atmel. При цьому дано дев'ять форм сигналу, по одній для кожної з ваг Хеммінга пересланої комбінації (з метою зменшення шумової компоненти для кожної ваги Хеммінга було зроблено статистичне усереднення по 1 000 вимірів).

З рисунка 2б видно, що амплітуда сплеску енергоспоживання в діапазоні від 140-го до 143-го відліку змінюється пропорційно вазі Хеммінга пересланої комбінації. Звідси стає очевидною практична можливість визначення ваги Хеммінга комбінації, що є результатом виконання проміжної операції виконуваного захисного алгоритму (зокрема комбінації, щозалежить від секретного ключа). Найбільш тривіальний підхід до визначення ваги Хеммінга оброблюваної комбінації називається шаблонною атакою (Template Attack). Вона найбільш відома для апаратних реалізацій шифрів AES та DES. Шаблонна атака передбачає наявність у зловмисника тестового чіпа, аналогічного тому, на який передбачається реалізація атаки. При цьому вкрай бажана можливість його вільного програмування, а також багаторазового ініціювання операції захисного перетворення з різними вхідними даними. Далі такий чіп називатиметься тестовим, а чіп, на який передбачається зробити практичну атаку - аналізованим чипом або просто чипом.

На попередньому етапі реалізації шаблонної атаки спочатку визначаються стрибки енергоспоживання, які характерні для виконання окремих операцій – ця інформація дозволить локалізувати області форми сигналу аналізованого чіпа, що

характеризують енергоспоживання під час обробки даних, що залежать від ключа.

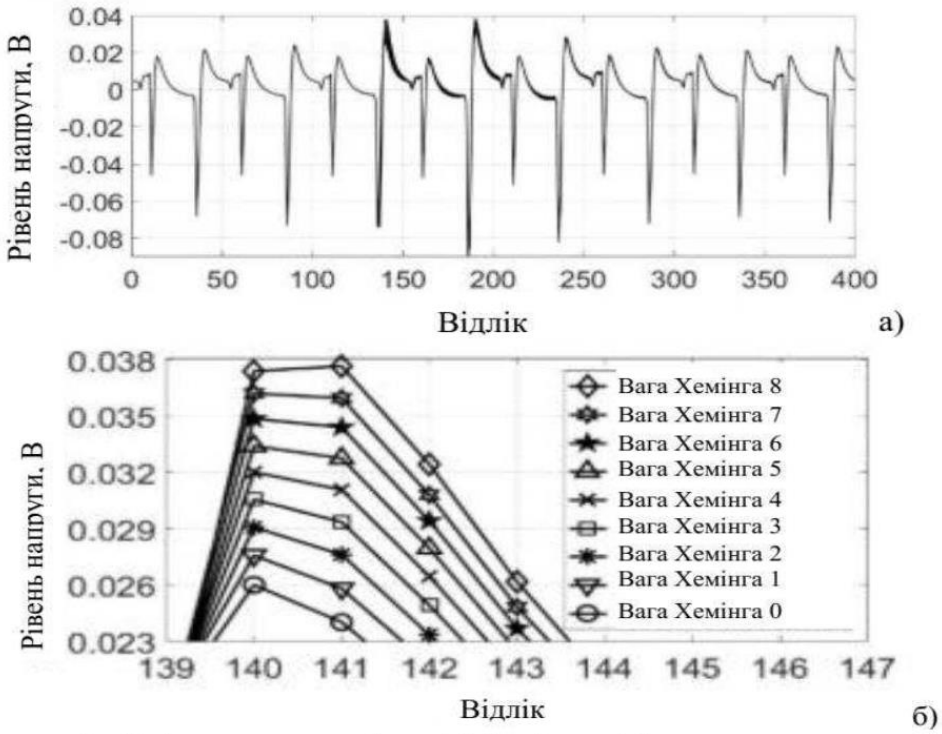


Рисунок 2 - Дев'ять усереднених (для мінімізації шуму) форм сигналу, отриманих під час пересилання байт з різними вагами Хеммінга, з регістру до чистої комірки ОЗУ: а) повна форма сигналу; б) збільшена ділянка з максимальним сплеском

Потім у цих областях форм сигналу вибираються відліки, на яких їх значення найбільшим чином відрізняються для різних ваг Хеммінга оброблюваних даних (наприклад, для форм сигналу, зображених на рисунку 1.11б, це 140-141-й відлік – на них різниця між сплесками для різних ваг Хеммінга досягає 2.6 мВ). Через наявність шумової складової на формах сигналу значення амплітуд сплесків енергоспоживання під час виконання тієї чи іншої операції можна вважати випадковою величиною із нормальним розподілом. Тому за кожною вагою Хеммінгу оброблюваних комбінацій розраховуються середні значення вибраних відліків та середньоквадратичні відхилення (створюється шаблон). Отриманий шаблон можна подати у вигляді матриці або діаграми

Висновки. Проведено моделювання та дослідження атаки енергоспоживання на основі ваги Хемінга. Розроблено схему та представлено усереднені форми сигналу, які отримані під час пересилання байтів з різними вагами Хеммінга

Перелік використаних джерел.

1. Mangard S., Oswald E., Popp T. Power Analysis Attaks: Revealing the Secrers of Smart Card. [USA]: Springer US, 2017. 338 p.

2. Peeters, E. Advanced DPA Theory and Practice: Towards the Security Limits of Secure Embedded Circuits. New York : Springer-Verlag New York, 2013. 139 p.


КІБЕРБЕЗПЕКА ТА
КОМП'ЮТЕРНО-ІНТЕГРОВАНІ
ТЕХНОЛОГІЇ
КБКІТ-2022
науково-практична конференція
молодих вчених
аспірантів та студентів
м.Тернопіль

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2022)

науково-практична конференція
молодих вчених, аспірантів та студентів

29–31 серпня 2022
Тернопіль

УДК 004.9

Концевич О.О.[1], Катеринюк С.А.[2], Додь О.А.[1]

[1]Західноукраїнський національний університет
[2]Збаразький ліцей №3 імені Т.Р. Михальського

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ АТАКИ ЕНЕРГОСПОЖИВАННЯ

Вступ. Алгоритми ідентифікації та аутентифікації, що використовуються в сучасних чіпах, вважаються захищеними від відомих криптографічних атак, тому з математичної Більшість сучасних чіпів є абсолютно захищеними. Однак існує клас атак, які називаються атаками побічними (або сторонніми) каналами [1] і використовують додаткову інформацію (так званий витік) при фізичній реалізації алгоритму. Найбільш відомою, універсальною та небезпечною побічною атакою можна вважати пасивну неруйнівну атаку, що використовує аналіз енергоспоживання. Ідея цього підходу заснована на фізичних особливостях роботи сучасних чіпів, що призводять до того, що їх енергоспоживання залежить від виконуваної операції та оброблюваних у ній даних [2].

Мета: Моделювання та дослідження атаки енергоспоживання на основі ваги Хемінга.

1. Схема експериментальної установки для дослідження атаки енергоспоживання

Блок-схема вимірювальної установки представлена рисунку 1. Вона складається із чотирьох основних компонентів:

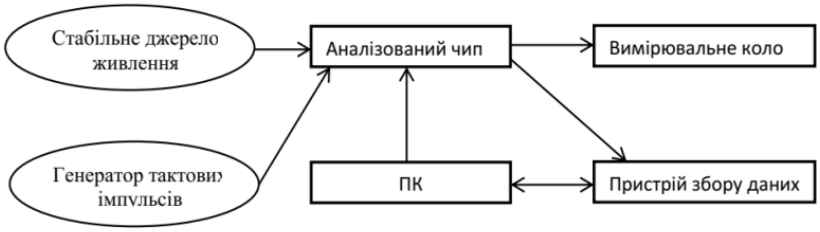


Рисунок 1 – Блок-схема вимірювальної установки

1) аналізований чіп – фізичний пристрій, з якого потрібно витягти секретний ключ;

2) вимірювальне коло – комплекс елементів, функція яких полягає в тому, щоб забезпечувати електричне з'єднання між аналізованим чіпом та пристроєм збору даних. При цьому він повинен надавати мінімальний вплив на чіп і передавати сигнал з максимально можливою достовірністю. Зазвичай у вимірювальному колі використовується резистор, вставлений у розрив контакту живлення чи землі чіпа;

3) пристрій збору даних – це прилад, що перетворює аналоговий сигнал, отриманий від вимірювального кола, у цифровий вигляд для його подальшого збереження на носії інформації, роль якого грає жорсткий диск ПК. Як правило, як пристрій збору даних використовується широкосмуговий осцилограф;

4) персональний комп'ютер. Він направляє на аналізований чіп команди, що

ініціюють виконання захисних операцій, крім того ПК приймає та зберігає дані про енергоспоживання, які отримують від пристрою збору даних.

Описана вимірювальна установка функціонує за таким алгоритмом:

1) ПК переводить пристрій збору даних в режим очікування тригерного сигналу;

2) ПК відправляє на чіп дані, за потреби супроводжуючи їх службовими командами, що ініціюють операції захисного перетворення, а також відправляє тригерний сигнал на пристрій збирання даних;

3) аналізований чіп, отримавши від ПК необхідні дані, виконує закладений алгоритм, після чого повертається до режиму очікування наступної команди від ПК;

4) визначення збору даних, отримавши, тригерний сигнал, оцифровує і записує у внутрішній буфер дані від вимірювального ланцюга, ці дані характеризують енергоспоживання чіпа під час проведення захисних перетворень;

5) пристрій збору даних надсилає записані дані з буфера до ПК;

6) ПК записує прийняті дані у файл;

7) кроки 1-6 повторюються стільки разів, скільки форм сигналу в результаті необхідно отримати.

2. Експериментальні дослідження на основі розробленої схеми

Для проведення експериментальних досліджень мікроконтролер було запрограмовано на багаторазове виконання команди «nop» –порожня команда. Вона виконується за один такт роботи, при цьому вміст регістрів даних, ОЗП, ПЗП, шини даних не змінюються. Перед виконанням цих операцій мікроконтролер відсилав на АЦП тригерний сигнал (логічну «1»), який запускав збір даних, та подальше вивантаження отриманої форми сигналу. Усього було знято 102 400 форм сигналу. Приклад однієї з них представлений рисунку 2.

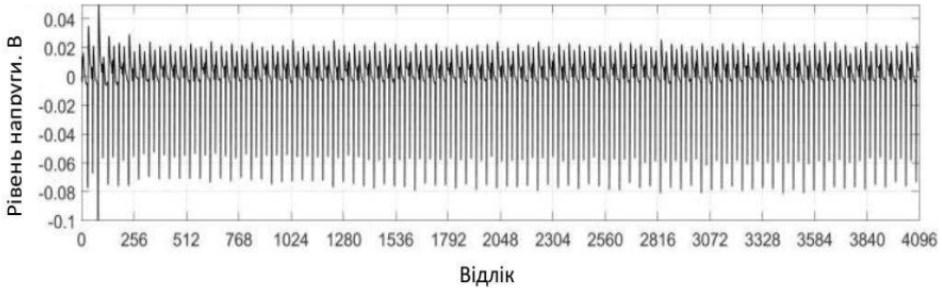


Рисунок 2 - Форма сигналу, що характеризує енергоспоживання мікроконтролера Atmel при виконання операцій «nop»

Необхідно пояснити деякі особливості одержуваних від АЦП форм сигналу:

- вхідний тракт АЦП видаляє постійну низькочастотну складову сигналу, однак на ефективність реалізації побічних атак по ланцюгах електроживлення ця особливість вплине, оскільки для них важливі лише відносні високочастотні зміни сигналу;
- на осі ординат та осі абсцис відкладаються не абсолютні значення напруги та часу, а відносні. По осі ординат відкладено рівні напруги

(привести їх до абсолютних значень можна, співвідносячи з динамічним діапазоном АЦП від -1,8 В до 1,8 В. Наприклад, значення на осі ординат, що дорівнює одному рівню напруги, буде еквівалентне 1,8, значення -0,5 буде еквівалентне -0.9 В.). По осі абсцис відкладені відліки. Інтервал між двома сусідніми відліками еквівалентний часовому інтервалу, зворотному частоті дискретизації тактового генератора АЦП, тобто 1/(100 МГц)=10 нс. Також необхідно помітити, що за стрибками напруги можна дуже просто визначити струм, що протікає, і споживану потужність.

Для тактування мікроконтролера використовувався кварцовий генератор із частотою 2 МГц, тому тривалість одного такту роботи мікроконтролера складає близько 1/(2000000 Гц)=500 нс, що відповідає 50 відлікам на знятих формах сигналу. На рисунку 3 кожні 2 сплески (наприклад, з 1933 по 1983 р. відліки) якраз мають тривалість 50 відліків. Звідси логічно припустити, що кожна пара сплесків характеризує енергоспоживання мікроконтролера на одному такті роботи.

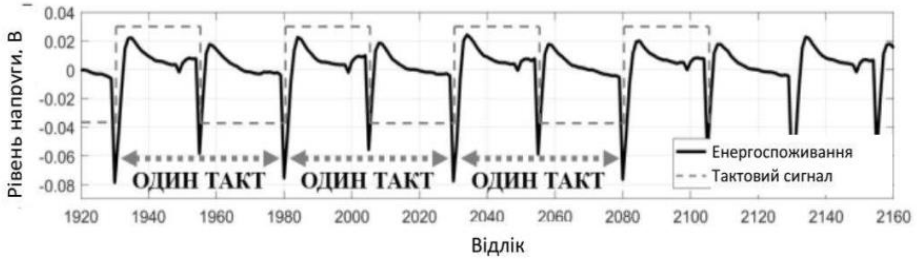


Рисунок 3 – Ділянка форми сигналу, отримана при виконанні команди «nop»

Можна передбачити, що від'ємний сплеск в середині такту і пропорційні його амплітуді частини сплесків на кінцях такту зумовлені струмом короткого замикання $I_{КЗ}$. Струмами зарядки паразитних ємностей I_C зумовлені невеликі частини сплесків на кінцях такту.

Математичне сподівання розглянутого відліку становить порядку 0.0226 (що еквівалентне 41 мВ). Враховуючи правило трьох сигм, згідно якого 0.9973% значень випадкової величини лежить в діапазоні $(x-3\sigma;\ x+3\sigma)$, де σ – середньоквадратичне відхилення, отримується, що СКВ значень відліку становить порядку 0.00094 (що еквівалентно 1.7 мВ).

Висновок. Встановлено, що енергоспоживання чіпа залежить від даних, які обробляються. Показано, що ця залежність має складний характер. Використана вимірювальна установка, яка працює з частотою дискретизації 100 Мвиб/с, дозволяла описати кожний такт роботи мікроконтролера 50-ма відліками, що можна вважати достатнім параметром.

Перелік використаних джерел.

1. Ratanpal G.B., Williams R.D., Blalock T.N. An on-chip signal suppression countermeasure to power analysis attacks. IEEE Transactions on Dependable and Secure Computing. 2014. Vol. 1. Iss. 3. P. 179–189.

2. Mangard S., Oswald E., Popp T. Power Analysis Attaks: Revealing the Secrers of Smart Card. [USA]: Springer US, 2017. 338 p.