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

ГОЛЕМБЙОВСЬКИЙ Михайло Петрович

Алгоритми протидії атакам диференційного аналізу енергоспоживання / Algorithms for Defense Against Differential Power Analysis Attacks

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
М.П. Голембйовський

Науковий керівник
к.т.н., доцент Б.О.Маслияк

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2023 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2023

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

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ГОЛЕМБЙОВСЬКИЙ МИХАЙЛО ПЕТРОВИЧ

1. Тема кваліфікаційної роботи:
Алгоритми протидії атакам диференційного аналізу енергоспоживання / Algorithms for Defense Against Differential Power Analysis Attacks
керівник роботи: к.т.н., доцент Б.О. Маслияк

затверджені наказом по університету від 1 грудня 2022 року № _____

2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 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 атак диференціального аналізу потужності та методів захисту від них;
– класифікація атак за побічними каналами електроживлення;
– розробка узагальненого алгоритму атаки DPA;
– реалізація табличного перетворення «читання зі зміщенням» для S-box на мікроконтролерах Atmel;
– дослідження залежності енергоспоживання від операції запису в ОЗП.

5. Перелік графічного матеріалу у роботі:
– типи атак через побічний канал;
– перетворення на здвоєному S-box;
– форма сигналу, що характеризує енергоспоживання мікроконтролера;
– гістограми розподілу значень;
– дев'ять усереднених форм сигналу для різних ваг Хеммінга.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Огляд атак диференціального аналізу потужності та методів захисту від них	12.2022 р. – 03.2023 р.	
2	Алгоритм протидії атакам диференціального аналізу потужності	03.2023 р. – 05.2023 р.	
3	Дослідження залежності енергоспоживання від операції запису в ОЗП	05.2023 р. – 11.2023 р.	

Студент _____ Голембйовський М.П.
(підпис)

Керівник роботи _____ к.т.н., доцент Б.О. Маслияк

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Алгоритми протидії атакам диференційного аналізу енергоспоживання” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека” освітньо-професійної програми «Кібербезпека» написана обсягом 79 сторінок і містить 19 ілюстрацій, 4 таблиці, 1 додаток та 30 джерел за переліком посилань.

Метою випускної кваліфікаційної роботи є розробка алгоритмів протидії атакам диференційного аналізу енергоспоживання.

Методи дослідження. Математичні методи моделювання, методи алгоритмізації, методи апаратно-програмної реалізації.

Результати дослідження: Здійснено класифікацію атак за побічними каналами електроживлення, що дозволило обгрунтувати вибір методів захисту від атак кожного класу. Розроблено узагальнене алгоритмічне забезпечення атаки DPA, що дозволило реалізувати табличне перетворення «читання зі зміщенням» для S-box на мікроконтролерах Atmel. На основі реалізації табличного перетворення проведено дослідження залежності енергоспоживання при виконанні операції запису в ОЗП. На мікроконтролерах Atmel реалізоване табличне перетворення «читання зі зміщенням» для S-box при шифруванні та проведено оцінку якості вимірювальної установки..

Результати роботи можуть успішно застосовуватися для протидії атакам.

Ключові слова: ПРОТИДІЯ АТАКАМ, ПОБІЧНІ КАНАЛИ, ЕНЕРГОСПОЖИВАННЯ, МІКРОКОНТРОЛЕР, ДИФЕРЕНЦІЙНИЙ АНАЛІЗ.

ABSTRACT

The graduate work on the topic „Algorithms for Defense Against Differential Power Analysis Attacks” for Master’s degree on speciality 125 "Cybersecurity " is written on 79 pages and contains 19 illustrations, 4 tables, 1 suplement and 30 references.

The aim of graduate work is to develop algorithms for countering attacks of differential analysis of energy consumption.

Research methods. Mathematical modeling methods, algorithmization methods, hardware and software implementation methods.

Results of the study. The classification of attacks by side channels of power supply was made, which made it possible to justify the choice of methods of protection against attacks of each class. A generalized algorithmic support of the DPA attack was described, which allowed to implement the "read with offset" tabular transformation for S-box on Atmel microcontrollers. Based on the implementation of the tabular transformation, a study of the dependence of energy consumption during the write operation in the RAM was carried out. On Atmel microcontrollers, a tabular transformation of "reading with an offset" for S-box during encryption was implemented, and the quality of the measuring setup was evaluated.

The results of the work can be successfully applied to counter attacks.

Keywords: ANTI-ATTACKS, SIDE CHANNELS, ENERGY CONSUMPTION, MICROCONTROLLER, DIFFERENTIAL ANALYSIS.

ЗМІСТ

ВСТУП

Одним з головних аспектів аудиту безпеки інформаційних систем являється оцінка надійності використаних криптографічних алгоритмів [1-2]. Вибір необхідного ступеня захисту інформації та засобів її забезпечення [3-5] є важливим завданням і має враховувати низку параметрів: рівень секретності інформації; її вартість; час, протягом якого вона має залишатися в таємниці тощо.

Проблема захисту інформаційних ресурсів нині набуває дедалі більш важливого значення [6-7]. Однак далеко не всі присутні на ринку криптографічні засоби забезпечують обіцяний рівень захисту [8-10]. Важливість цієї проблеми важко переоцінити. Системи та засоби захисту інформації (СЗІ) характеризуються тим, що для них не існує простих та однозначних тестів, що дозволяють переконатися у надійному захисті інформації. Наприклад, для перевірки працездатності системи зв'язку достатньо провести її випробування [11-12]. Однак успішне завершення цих випробувань не дозволяє зробити висновок про те, що вбудована у неї підсистема захисту також працездатна. Завдання визначення ефективності СЗІ при використанні криптографічних методів захисту часто більш трудомістка, ніж розробка СЗІ, потребує наявності спеціальних знань і більш високої кваліфікації, ніж завдання розробки. Часто аналіз нового шифру є новим науковим, а не інженерним завданням [13].

Ці обставини призводять до того, що на ринку з'являються засоби криптографічного захисту інформації, про які ніхто не може сказати нічого певного. При цьому часто розробники тримають криптоалгоритм (як показує практика, що часто легко зламується) в секреті. Проте завдання точного визначення використовуваного криптоалгоритму не може бути гарантовано складною хоча б тому, що він відомий розробникам. Крім того, якщо порушник знайшов спосіб подолання захисту, то не в його інтересах про це заявляти. В результаті користувачі таких СЗІ потрапляють у залежність як

мінімум від розробника. Тому суспільству має бути вигідно відкрите обговорення безпеки СЗІ масового застосування, а приховування розробниками криптоалгоритму має бути неприпустимим.

Останнім часом одним із найактуальніших напрямів криптоаналізу стало здійснення атак, що використовують особливості реалізації та робочого середовища [14-15]. Атаки по сторонніх або побічних каналах - це вид криптографічних атак, які використовують опосередковану інформацію, отриману сторонніми або побічними каналами [16-17]. Під інформацією з побічних каналів розуміється інформація, яка може бути отримана з фізичних характеристик пристрою шифрування і при цьому вона не є ні відкритим текстом, ні шифртекстом [18]. Все вище сказане і визначає актуальність даної тематики.

Мета роботи. Метою даної роботи є розробка алгоритмів протидії атакам диференційного аналізу енергоспоживання.

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

– огляд та аналіз атак диференціального аналізу потужності та методів захисту від них;

– класифікація атак за побічними каналами електроживлення;

– розробка узагальненого алгоритму атаки DPA;

– реалізація табличного перетворення «читання зі зміщенням» для S-box на мікроконтролерах Atmel;

– дослідження залежності енергоспоживання від операції запису в ОЗП.

Об’єкт дослідження. Процес протидії атакам диференційного аналізу енергоспоживання.

Предмет дослідження. Методи і засоби протидії атакам диференційного аналізу енергоспоживання.

Методи дослідження. Математичні методи моделювання, методи алгоритмізації, методи апаратно-програмної реалізації.

Наукова новизна одержаних результатів.

1. Здійснено класифікацію атак за побічними каналами електроживлення, що дозволило обгрунтувати вибір методів захисту від атак кожного класу.

2. Розроблено узагальнене алгоритмічне забезпечення атаки DPA, що дозволило реалізувати табличне перетворення «читання зі зміщенням» для S-box на мікроконтролерах Atmel.

3. На основі реалізації табличного перетворення проведено дослідження залежності енергоспоживання при виконанні операції запису в ОЗП.

Практичне значення отриманих результатів. На мікроконтролерах Atmel реалізоване табличне перетворення «читання зі зміщенням» для S-box при шифруванні та проведено оцінку якості вимірювальної установки.

Публікації та апробація КР.

1. Голембйовський М.П., Лисик М.А., Гончарик Г.Я. Класифікація криптоаналітичних атак за побічними каналами. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.139-141 [19].

2. Голембйовський М.П., Голембйовський П.М. Реалізація табличного перетворення «Читання зі зміщенням» для S-box на мікроконтролерах Atmel. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.36-38 [20].

1 ОГЛЯД АТАК ЗА ДИФЕРЕНЦІАЛЬНИМ АНАЛІЗОМ ПОТУЖНОСТІ ТА МЕТОДІВ ЗАХИСТУ ВІД НИХ

1.1 Класифікація атак за побічними каналами електроживлення

Майже всі здійснені на практиці вдалі атаки на криптосистеми використовують слабкості у реалізації та розміщенні механізмів криптоалгоритму [21-22]. Такі атаки засновані на кореляції між значеннями фізичних параметрів, що вимірюються в різні моменти під час обчислень (споживання енергії, час обчислень, електромагнітне випромінювання тощо), і внутрішнім станом обчислювального пристрою, що стосуються секретного ключа. На практиці атаки по побічних каналах на багато порядків ефективніші, ніж традиційні атаки, засновані лише на математичному аналізі. При цьому атаки побічними каналами використовують особливості реалізації (тому їх іноді називають також називають атаками на реалізацію - implementation attacks) для отримання секретних параметрів, задіяних у обчисленнях. Такий підхід менш узагальнений, оскільки прив'язаний до конкретної реалізації, але найчастіше потужніший, ніж класичний криптоаналіз.

В останні роки різко зросла кількість криптографічних атак, що використовують особливості реалізації та робочого середовища. Наприклад, противник може відстежувати енергію, що споживається смарт-картою, коли вона виконує операції з закритим ключем, такі як розшифрування або генерація підпису. Противник може також заміряти час, що витрачається на виконання криптографічної операції, або аналізувати поведінку криптографічного пристрою у разі виникнення певних помилок. Побічну інформацію на практиці зібрати інколи нескладно, тому потрібно обов'язково враховувати таку загрозу в оцінці захищеності системи [23].

Атаки по побічних каналах класифікуються за такими трьома типами:

- за контролем над обчислювальним процесом: пасивні та активні;

- за способом доступу до модуля: агресивні (invasive), напівагресивні (semiinvasive) та неагресивні (non-invasive);

- за методом, який застосовується в процесі аналізу: прості – simple side channel attack (SSCA) і різницеві - різні side channel attack (DSCA).

На сьогоднішній день виділено понад десять побічних каналів. Атаки розрізняються за видом побічного каналу (рисунок 1.1):

- атаки за часом виконання (Timing Attacks);

- атаки з енергоспоживання (Power Analysis Attacks);

- атаки за помилками обчислень (Fault Attacks);

- атаки за електромагнітним випромінюванням (ElectroMagnetic Analysis);

- атаки помилок у каналі зв'язку (Error Message Attacks).

Рисунок 1.1 – Типи атак через побічний канал

Існують і більш витончені види атак:

- атаки по кеш-пам'яті (Cache-based Attacks);

- акустичні атаки (Acoustic Attacks);

- атаки світлового випромінювання (Visible Light Attacks).

Атака за часом – спосіб отримання будь-якої прихованої інформації шляхом точного виміру часу, який потрібен користувачеві для виконання криптографічних операцій. Це перша з атак по побічних каналах, що з'явилася у цивільній криптографії. Найчастіше час обробки даних у криптосистемах трохи змінюється залежно від вхідних значень (наприклад, відкритого тексту чи шифртексту). Це є наслідком оптимізації продуктивності та широкого кола інших причин. Атака за часом заснована на вимірюваннях часу, необхідного модулю шифрування для виконання операції шифрування. Ця інформація може призвести до розкриття інформації про секретний ключ.

Наприклад, ретельно вимірюючи час, необхідний для виконання операцій із секретним ключем, атакуючий може знайти точне значення експоненти в алгоритмі Diffie-Hellman.

Атаки за часом наробили багато галасу у пресі: закриті ключі RSA можуть бути відновлені вимірюванням відносних інтервалів часу, витрачених на виконання криптографічних операцій. Ці атаки були успішно застосовані до карток з мікропроцесорами та інших засобів надійної ідентифікації, а також до серверів електронної комерції у мережі.

Атака з аналізу потужності придатні переважно для апаратної реалізації криптографічних засобів та успішно застосовується при зломі смарт-карт та інших систем, у яких зберігається секретний ключ [24. Щоб виміряти споживану схемою потужність, необхідно послідовно з ланцюгом живлення або заземлення підключити резистор малого опору (наприклад, 50 Ом). Падіння напруги, поділене на опір, дасть силу струму. Сучасні лабораторії мають обладнання, здатне проводити цифрові вимірювання напруги на виключно високих частотах (понад 1 ГГц) і з чудовою точністю (помилка менше 1%).

Атака за потужністю може бути поділена на просту (Simple Power Analysis, SPA) [25] та різницеву (Differential Power Analysis, DPA) [26-27]. Метою SPA є отримання інформації про конкретно виконувані інструкції в системі та про конкретні оброблювані дані. У загальному випадку SPA може

дати як відомості про роботу пристроїв, так і інформацію про ключ. Для здійснення цієї атаки криптоаналітик повинен мати точні дані про реалізацію пристрою. Цей метод використовує безпосередні дані вимірювань, зібрані під час виконання криптографічних операцій [28]. Проста атака по потужності для смарт-карт зазвичай займає кілька секунд, у той час як різницева атака по потужності може зайняти кілька годин.

На відміну від простих атак, різницеві атаки, які засновані на аналізі споживаної потужності, мають на увазі не тільки візуальне уявлення споживаної потужності, але і також статистичний аналіз та статистичні методи виправлення помилок для отримання інформації про ключі. Більше того, DPA часто не потребує даних про конкретну реалізацію і як альтернативу використовує статистичні методи аналізу. Різницевий аналіз потужності – це є один з найпотужніших засобів для проведення криптографічних атак, які використовують побічні канали, причому ця атака вимагає дуже невеликих витрат.

Помилки апаратного забезпечення, що з'являються під час роботи відповідного криптографічного модуля, або помилкові вихідні дані можуть стати важливими побічними каналами і іноді суттєво збільшують уразливість шифру до криптоаналізу [29]. Криптоаналіз на основі формування випадкових апаратних помилок - це вид нападу на шифри у разі, коли передбачуваний порушник має можливість надати на шифратор зовнішній фізичний вплив та викликати поодинокі помилки у процесі шифрування одного блоку даних. Атаки по помилках на криптографічні алгоритми вивчаються з 1996 року, і з того часу майже всі криптографічні алгоритми були піддані атакам такого виду.

Здійсненність атаки за помилками (або, принаймні, її ефективність) залежить від можливостей зловмисника викликати помилки в системі спеціально або користуватися збоями природного походження. Помилки найчастіше відбуваються через стрибки напруги, збої годинника або через випромінювання різних типів.

Розгляд питання стійкості до цього методу особливо актуальний для шифраторів, що застосовуються в інтелектуальних електронних картках. Здебільшого помилки класифікуються за такими аспектами:

- точність, яку порушник може досягти при виборі часу та місця, де з'являється помилка під час роботи криптографічного модуля;

- довжина даних, на які впливає помилка, наприклад, лише один біт;

- постійність помилки, тобто чи є помилка короткочасною чи постійною;

- типи помилок, такі як зміна одного біта або зміна одного біта, але тільки в одному напрямку (наприклад, з 1 на 0), зміна біта на випадкове значення тощо.

Загалом, успішна атака помилок на криптографічні модулі або пристрої вимагає двох кроків: крок створення помилки та крок використання помилки.

Помилки можуть бути викликані в смарт-картах шляхом зовнішнього впливу на неї та розміщення її у неправильні умови. Деякі з них – аномальне та раптове зниження або підвищення напруги, частоти, температури, випромінювання, освітлення та ін.

Різницевий аналіз помилок полягає у вивченні результату роботи алгоритму шифрування в нормальних і ненормальних умовах при тому самому вході (відкритому тексті). Ненормальні умови зазвичай виходять створенням помилки в процесі (короткочасна помилка) або перед процесом (постійна помилка) роботи.

Різницевий аналіз помилок широко вивчено з теоретичної точки зору і може бути застосований до майже усіх симетричних криптосистемам.

Зокрема, DES, RC5 та інші шифри є вразливими щодо цього виду криптоаналізу, тому при їх використанні необхідно забезпечити захист апаратури від нав'язування збоїв.

Атаки за електромагнітним випромінюванням можливі, тому що виконання обчислювальних операцій на комп'ютері пов'язане з виділенням електромагнітного випромінювання Вимірюючи та аналізуючи це випромінювання, порушник може отримати значну інформацію про

обчислення та використовувані дані. Атаки з електромагнітного аналізу можуть бути розділені на дві великі категорії: прості (SEMA) та диференціальні (DEMA).

1.2 Теоретичні основи побудови побічних атак за ланцюгами електроживлення (диференціальний аналіз потужності)

Якщо атака SPA передбачає безпосередній, візуальний аналіз коливань енергоспоживання на знятих формах сигналу, інтерпретуючи які зловмисник робить висновок про те, які операції, з якими даними виконуються на чіпі, то атака DPA передбачає статистичний метод аналізу енергоспоживання чіпа, що робить її значно більш ефективною, ніж SPA, в тому випадку, якщо зловмиснику доступна велика кількість даних про енергоспоживання чипа [30]. За останні 20 років, з моменту перших публікацій, які описують принципи реалізації DPA та його застосування, була доведена його придатність щодо будь-яких скільки-небудь відомих алгоритмів захисних перетворень, серед яких, насамперед, блокові шифри, такі як DES, AES, ГОСТ, також алгоритми з відкритим ключем, наприклад, RSA.

Крім опису відомих підходів до реалізації DPA, проілюстрована також універсальність цієї атаки. Зокрема вона не має важливих відмінностей від відомих реалізацій щодо інших блокових шифрів. Узагальнений алгоритм DPA складається з таких основних кроків:

- знімаються дані про енергоспоживання чіпа під час перетворення відомих повідомлень на невідомому ключі;

- проводяться оцінки енергоспоживання чіпа при перетворенні тих самих повідомлень на всіх можливих варіантах невеликої (перебірної) частини ключа (підблок ключа);

- отримані оцінки порівнюються (статистичними методами) зі знятими даними про енергоспоживання чіпа. На істинний підблок ключа вказуватиме

оцінка, яка виявиться найбільш наближеною до виміряного реального енергоспоживання;

- алгоритм повторюється для інших підблоків ключа – ключ відновлюється послідовно, невеликими частинами, з використанням додаткової інформації, чіпа, що витікає по ланцюгу електроживлення.

Тобто побічна атака DPA, на відміну від теоретичних атак (тобто криптографічних методів злому), має поліноміальну (а не експоненційну) складність залежно від довжини захисного ключа перетворення.

1.3 Коротка характеристика основних методів захисту від DPA

DPA є дуже ефективною побічною атакою, за допомогою якої можна відновити ключ шифрів, які вважаються стійкими до всіх відомих криптографічних атак. Безумовний інтерес представляють пропоновані методи захисту від атак цього типу. Аналіз дозволяє розділити існуючі методи захисту від DPA на три групи:

- захист лише на рівні програмного забезпечення;
- захист на апаратному рівні;
- захист на логічному рівні.

Захист на рівні ПЗ можна вважати найдешевшим, тому що його реалізація не вимагає перепроектування чіпа (зміни архітектури, периферійного обладнання тощо), а передбачає внесення змін лише у програмний алгоритм. Цей підхід має лише один недолік – збільшення вимог до ресурсів чіпа (обчислювальна потужність, обсяг ОЗП, ПЗП). Основна ідея полягає у модифікації реалізації алгоритму захисного перетворення таким чином, щоб усунути залежність енергоспоживання від секретної інформації, що обробляється чіпом у процесі виконання захисних перетворень. Існують різні спеціалізовані програмні рішення, що дозволяють досягти цього (для конкретних архітектур чипів або алгоритмів захисних перетворень). Відомі три найбільш ефективні, відомі та універсальні методи:

- маскування;

- балансування;

- рандомізації виконуваних чіпом команд.

Метод маскування передбачає додавання проміжних даних, що з'являються у процесі виконання захисного перетворення, з деякою випадковою комбінацією (маскою), що виробляється вбудованим генератором випадкових чисел, та зняттям даної маски після проведення всіх раундів перетворення (при цьому існують такі модифікації методу маскування, які передбачають зміну маски на кожному раунді). Для розрахунку будь-яких проміжних біт захисного перетворення зловмиснику, крім постійної (і перебірної) частини секретного ключа доведеться вгадувати ще випадкову маску. З тієї причини, що маска генерується випадково і змінюється з кожним повідомленням, що перетворюється, її вгадування чи перебір безглузді. Таким чином без знання маски нападник перестає мати можливість з необхідною точністю розраховувати будь-які проміжні значення захисного перетворення, а, отже, виключається можливість зіставлення їх із відповідними відліками на формах сигналу.

Метод програмного балансування є відносно новим і досить перспективним підходом. Пропонується модифікація програмної реалізації захисного перетворення таким чином, щоб комбінації роботи чіпа, що оброблялися на кожному такті, складалися з однакової кількості нулів та одиниць (мали однакову вагу Хеммінга). Це досягається за рахунок одночасної обробки разом із «корисною» комбінацією, комбінації, інвертованої до неї.

Рандомізація виконуваних процесором команд ґрунтується на ідеї, що в процесі виконання чіпом програми практично завжди існує набір інструкцій, які можуть бути виконані незалежно одна від одної. Інструкцію можна вважати здійсненною, якщо вона не вимагає результату виконання інших інструкцій, що ще не отримані. Вона не змінює даних, що використовуються іншими інструкціями, які поки що не виконані. Щоразу з цього набору інструкцій випадково вибирається одна, яка й виконується. Цей крок робить

марним зіставлення розрахованих на ключі проміжних біт захисного перетворення, що перебирається, з відповідними відліками на формах сигналу, тому що на різних формах сигналу ці відліки випадковим чином змінюватимуть своє становище. Таким чином стає неможливо вгадати, в якому місці на конкретній формі сигналу знаходиться відлік, який характеризує вироблення проміжного значення, що розраховується.

Основна ідея методів захисту на апаратному рівні полягає в тому, щоб додати у фізичну реалізацію чіпа деякі компоненти, що впливають на форми сигналу, та які роблять вкрай скрутним їх зіставлення з даними, що розраховуються на ключах, які перебирається. До цієї групи можна віднести мінімум три методи захисту:

- зашумлення;
- додаткова стабілізація напруги;
- десинхронізація та підроблені такти.

Зашумлення – найбільш тривіальна ідея, полягає в тому, щоб включити до складу чіпа пристрій, що вводить зашумлення ланцюгів живлення. Шум, що додається, повинен мати амплітуду, що значно перевищує коливання корисного сигналу. Цей метод захисту лише ускладнює реалізацію DPA, не забезпечуючи абсолютної захищеності. Незважаючи на це, за вмілої реалізації, він може призвести до необхідності обробки нереалізовано великої кількості форм сигналу для здійснення успішного злому чіпа.

Додаткова стабілізація напруги також є досить тривіальним методом захисту чіпів від аналізу енергоспоживання Ідея полягає в тому, щоб помістити в структуру чіпа стабілізатор напруги, наприклад, виконаний у вигляді зворотного ланцюга зв'язку. Даний пристрій в ідеальному випадку зможе забезпечити один і той самий рівень енергоспоживання незалежно від даних, що обробляються, проте на практиці абсолютної незалежності здобути неможливо. Даний метод, за аналогією із зашумленням, лише зменшує амплітуду сигнальної компоненти, порівняно з шумовою.

За своєю суттю метод десинхронізації та вставки підроблених тактів аналогічний методу рандомізації виконуваних процесором команд. Більше того, він може бути реалізований як на апаратному рівні, так і програмному. Ідея полягає в тому, щоб у процесі виконання захисного перетворення обробляти підроблені такти чи вставляти випадкові переривання. Дані кроки дозволять випадковим чином змінювати місце розташування відліку, що цікавить, на різних формах сигналу, що очевидно призведе до неможливості реалізації DPA. Проте існують методи (так звана пересинхронізація), які дозволяють у деяких випадках «обійти» цей метод захисту.

Основна ідея методів захисту на логічному рівні полягає в усуненні причини витоку інформації з ланцюга електроживлення - різної потужності, споживаної логічними вентилями залежно від біт, що обробляються. В даному випадку можна виділити три основні напрями захисту:

- зниження енергоспоживання;
- зміна структури логічних вентилів;
- апаратне балансування оброблюваних чіпом даних.

Зниження енергоспоживання передбачає використання при розробці та виробництві чіпа технологій, що дозволяють значно зменшити його енергоспоживання. В якості прикладу можна навести технологію «Кремній на ізоляторі». Вона передбачає виробництво транзисторів, які використовують підкладку, виконану за принципом "бутерброду", де замість чисто кремнієвої підкладки використовується кремній-ізолятор-кремнієва. Цей крок дозволяє багаторазово зменшити (але не усунути повністю) паразитну ємність транзисторів (отже, і її час зарядки), забезпечивши таким чином помітне зниження енергоспоживання логічного вентиля під час перемикання, та зростання швидкості перемикання транзисторів (що тягне збільшення швидкості роботи чіпа). Головні недоліки цієї технології: висока вартість та неможливість повного усунення залежності енергоспоживання від оброблюваних даних.

- зміна структури логічних вентилів передбачає модифікацію логічних вентилів з метою внесення додаткових паразитних ємностей, які провокували б сплески енергоспоживання (приблизно однакові) на будь-яких чотирьох переходах: $0\rightarrow0$, $0\rightarrow1$, $1\rightarrow0$, $1\rightarrow1$. На практиці цей метод захисту значно знижує відмінності енергоспоживання під час перемикань між різними станами, але не усуває їх повністю. Однак цього кроку може бути достатньо, щоб утруднити реалізацію DPA настільки, щоб чіп, захищений даним методом, можна було б вважати стійким до аналізу.

Метод апаратного балансування за своєю суттю аналогічний програмному балансування. Найбільш досконала модифікація передбачає реалізацію захисного перетворення на багатопроцесорній (зокрема, двопроцесорній) обчислювальній системі. При цьому один процесор у звичайному режимі виконує операції, передбачені алгоритмом захисного перетворення, тоді як другий процесор паралельно виконує інший алгоритм, побудований таким чином, щоб підтримувати однакове енергоспоживання чипа на кожному такті роботи. Це реалізується шляхом обробки двійкових комбінацій, інвертованих щодо комбінацій, оброблюваних під час виконання алгоритму захисного перетворення. Таким чином, у будь-який момент часу обчислювальна система обробляє комбінації, що складаються з однакової кількості нулів та одиниць.

Можна запропонувати ще один, радикальніший, напрямок щодо захисту від побічних атак за ланцюгами електроживлення - використання безключових захисних перетворень (які не вимагають розподілу ключів) на кшталт системи Діна-Голдсміта. По причині того, що така система заснована на новому підході до побудови захисних перетворень, що вимагає зберігання в пам'яті ключа, реалізація щодо побічних атак по ланцюгах електроживлення виявляється принципово неможливою. Однак було виявлено значні вразливості запропонованої системи. Також її особливістю є те, що вона призначена лише для виконання функції захищеної передачі інформації, але не для її зберігання. Тому подібну систему поки що можна розглядати лише як перспективну

альтернативу «класичним» захисним перетворенням, захищеним описаними вище методами.

З наведеної короткої характеристики методів захисту від DPA видно, що лише методи маскування, програмного балансування та апаратного балансування здатні забезпечити суворо доведений рівень захисту. При цьому метод маскування може бути реалізований порівняно просто і з мінімальними витратами лише для невеликої кількості шифрів (зокрема, AES). Адаптація маскування до шифру «Магма» виявляється надзвичайно складною і потребує значних обчислювальних ресурсів (аналогічна ситуація буде спостерігатися і для інших шифрів). Реалізація методу програмного балансування поки що існує лише для шифру AES (і то з низкою застережень), а питання можливості її адаптації до інших симетричних шифрів (наприклад, DES) ще не вирішені і з високою ймовірністю вирішені не будуть.

Реалізацію методу апаратного балансування можна вважати затратною та незастосовною до дешевих масових продуктів через значне ускладнення архітектури чіпа. Інші, більш прості та дешеві для кінцевого користувача методи, лише ускладнюють аналіз чіпа і ґрунтуються на наступних дуже ризикованих припущеннях:

- доступне зловмиснику вимірювальне обладнання, що має дуже обмежену чутливість;

- зловмисник не здатний значно знизити шумову компоненту на тих формах сигналу, що знімаються;

- зловмисник не здатний компенсувати розсинхронізацію відліків на тих формах сигналу, що знімаються.

Ці методи захисту зазвичай можуть застосовуватися на практиці щодо дешевих чіпів, у різних комбінаціях, але зрозуміло, що вкрай ризиковано покладатися на відсутність у зловмисника дорогого вимірювального обладнання або його низьку кваліфікацію. Наприклад, можна продемонструвати успішну реалізацію атаки на досить популярну смарт-картку Mifare DESFire MF3ICD40. Після цього стало зрозуміло, що

висококваліфікований зловмисник, який має навіть дуже середнє вимірювальне обладнання (більше того, не знає, які саме методи захисту застосовуються в аналізованому чіпі), здатний обійти наведені припущення та відновити ключ захисного перетворення за невеликий проміжок часу. Більше того, відомі ще як мінімум три успішні атаки на комерційні чіпи.

1.4 Обґрунтування вибору та опис пристрою збору даних

При описі відомих атак використовувалися дуже дорогі вимірювальні установки, в основі яких лежав осцилограф з активним диференціальним пробником. Вартість подібної установки, що становить $10 000-15 000, можна вважати цілком прийнятною порівняно з вартістю обладнання, що потрібне для реалізації інших типів побічних атак (наприклад, агресивних атак). Але як наукові дослідження цих атак, так і їх практичне застосування, мали б значно більше поширення, якби вдалося значно скоротити необхідні витрати на вимірювальне обладнання (наприклад, до цілком розумної, за будь-якими мірками, суми в $1 000-2 000). В контексті реалізації атаки вимірювальна установка повинна отримувати аналогові дані від ланцюгів електроживлення чіпа (зокрема, падіння напруги на резисторі, включеному у розрив лінії живлення або землі), перетворювати їх на цифровий вигляд, а потім відправляти на ПК. При цьому необхідно забезпечити відповідну смугу пропускання та чутливість. Сфера застосування сучасних осцилографів дуже широка і вони не найкращим чином підходять для виміру малих сигналів. Осцилограф у поєднанні з активним диференціальним пробником можна вважати дуже надлишковим обладнанням для реалізації такого вузького завдання, а витрати на нього – невиправданими. Тому в поточному експерименті було ухвалено рішення використовувати значно більш дешеву вимірювальну установку, основою якої є плата з аналого-цифровим перетворювачем (АЦП).

АЦП - пристрій, що перетворює безперервний аналоговий сигнал (як правило - напругу) в дискретний (як правило, двійковий цифровий) код, тобто послідовність чисел, віднесених до деяких фіксованих моментів часу. Для перетворення аналогового сигналу на цифровий вигляд АЦП виконують дві операції: дискретизацію та квантування.

Дискретизація - це подання безперервного аналогового сигналу у вигляді послідовності відліків. Значення безперервного в часі сигналу вибираються через проміжки часу Δt (періоди дискретизації). В результаті виходить послідовність значень сигналу через інтервал Δt. Період дискретизації очевидно визначає такий параметр вимірювальної установки, як смуга пропускання, та характеризує здатність достовірно виміряти високочастотні компоненти сигналу.

На етапі квантування діапазон значень сигналу розбивається на відрізки з кроком квантування δ, після чого кожне значення відліків сигналу, взяте з інтервалом дискретизації Δt, наводиться («притягується») до ряду дискретних рівнів. Кількість рівнів, що характеризує один з основних параметрів будь-якого АЦП – розрядність, яка вочевидь визначає його чутливість. Крок квантування визначає непереборну похибка, властиву всім АЦП - помилку квантування, яка полягає в тому, що значення сигналу, що знаходиться між двома рівнями, округляється до одного з них.

Також велике значення для побічних атак по ланцюгах електроживлення має джиттер. В ідеальному випадку квантовані відліки повинні братися через рівні проміжки часу, однак генератор, що тактує АЦП, не ідеальний. Отже, через тремтіння фронту тактового сигналу інтервал дискретизації Δt схильний до флуктуацій. У найпростішому випадку джиттер веде до спотворення форми оцифрованого сигналу.

Існує безліч типів АЦП, найпростіший з них – паралельні АЦП (АЦП прямого перетворення). Вони застосовуються в більшості високошвидкісних осцилографів. Паралельні АЦП, як правило, мають роздільну здатність 8-10

розрядів (2^8-2^{10} рівнів квантування). АЦП даного типу здійснюють квантування сигналу одночасно за допомогою набору компараторів, включених паралельно джерелу вхідного сигналу. Головна перевага паралельних АЦП у тому, що за рахунок паралельної роботи всіх його компараторів, час, потрібний на квантування кожного відліку, дорівнює часу затримки в одному компараторі і часу затримки в перетворювачі кодів. Таким чином, цей тип АЦП здатний оцифровувати сигнал із частотою до одиниць (деякі навіть до десятка) ГГц. Недоліком даних АЦП є чутливість – для отримання N розрядів, необхідно 2^N-1 компараторів, а отже для отримання восьми розрядного АЦП (256 рівнів квантування) необхідно 255 компараторів, а для 16-ти розрядів - вже 65535 компараторів.

На основі паралельних АЦП будуються одні з найпопулярніших на сьогоднішній день АЦП конвеєрного типу, які спрощено являють собою складання з двох і більше послідовно підключених секцій паралельних АЦП. Частота квантування таких АЦП виявляється нижчою, ніж паралельних, проте на момент проведення дослідження лише АЦП конвеєрного типу мали частоту дискретизації вище 100 МГц при роздільній здатності 14-16 біт, тобто це єдиний тип АЦП, що підходив під завдання аналізу споживаної чіпами потужності.

Блок АЦП є основою будь-якого сучасного осцилографа, оскільки саме цей пристрій дискретизує аналоговий сигнал, переводячи його в цифровий вигляд, який далі виводиться на дисплей осцилографа і може бути збережений на ПК. Але через те, що вимір сигналів з рівнем десятків мікровольт є вкрай специфічним і незатребуваним переважною більшістю користувачів завданням, в осцилографи встановлюються «класичні» восьмирозрядні АЦП, що забезпечують необхідну більшості користувачів широку смугу пропускання (існують дуже рідкісні моделі осцилографів «високої роздільної здатності» з АЦП на 10 або 12 розрядів, проте їх вартість виявляється надзвичайно високою). У контексті вирішення завдання аналізу енергоспоживання чіпа, АЦП на 16 розрядів забезпечить чутливість значно

вище будь-якого осцилографа, побудованого на основі 8-12-розрядного АЦП. Причому не потрібно буде посилення сигналу, що позбавляє від додаткових спотворень, які вносяться підсилювачем. При цьому забезпечується прийнятна смуга пропускання. АЦП AD9652 фірми Analog Devices на момент проведення дослідження мав унікальне співвідношення роздільної здатності та частоти дискретизації, він володіє 16-ма рівнями квантування (у динамічному діапазоні від -1.8 до 1.8. Теоретично, його роздільна здатність за напругою становить $U_{КРОК} = \frac{3,6}{2^{16}} = \frac{3,6}{65536} = 0,0000549 = 54,9$ мкВ.

При цьому забезпечується частота дискретизації до 310 МГц. Фізично АЦП є інтегральною схемою в корпусі для поверхневого монтажу розміром 1х1 см (рисунок 1.2).

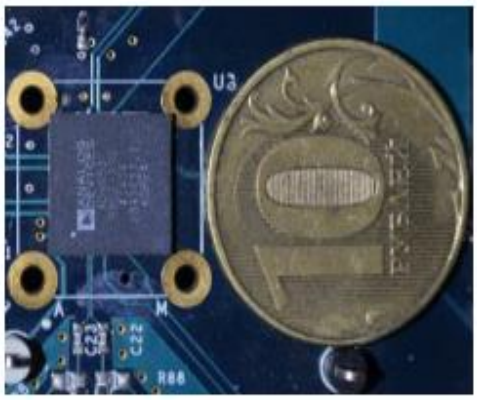


Рисунок 1.2 – Фото АЦП AD9652

Для використання АЦП як високоточної системи збору даних його необхідно змонтувати на плату і провести розведення кожного контакту відповідно до технічної інструкції, що є дуже нетривіальним завданням, тому було використано АЦП, змонтоване на фірмовій оцінювальній платі AD9652-310EBZ Evaluation Board, вартістю $420, а також плата поєднання з ПК HSC-ADC-EVALCZ FPGA-Based Data Capture Kit, вартістю $620, яка має буферну пам'ять на 64 536 відліків, реалізацію функції тригера та інтерфейс зв'язку з ПК (USB). У комплекті з обладнанням виробник постачає програмне

забезпечення «VisualAnalog», що надає різні функції обробки даних, одержуваних від узгодження. Для роботи АЦП потрібне підключення зовнішнього джерела тактового сигналу. Виробник рекомендує використовувати генератор з ультранизьким джиттером Rohde & Schwarz SMA 100 вартістю $25 000. Через його високу ціну був використаний значно менш стабільний кварцовий генератор EPSON з частотою 100 МГц, вартість такого генератора виявляється меншою за $20.

2 АЛГОРИТМ ПРОТИДІЇ АТАКАМ ДИФЕРЕНЦІАЛЬНОГО АНАЛІЗУ ПОТУЖНОСТІ

2.1 Узагальнений алгоритм атаки DPA

З моменту свого виникнення принципи реалізації DPA не зазнали суттєвих змін. В узагальненому вигляді його алгоритм складається з наступних п'яти етапів.

На першому етапі реалізації DPA зловмисник обирає деяке проміжне значення алгоритму захисного перетворення $a_l(i)=f(m_l(i),k_l)$, що залежить від деяких відомих даних (зазвичай це підблок повідомлення $m_l(i)$), та відповідного підблоку невідомого секретного ключа k_l. Часто в якості таких проміжних значень вибираються виходи S-box шифру, які, для прикладу залежать від восьми біт раундового ключа).

На другому етапі зловмисник проводить зняття форм сигналу, що характеризують енергоспоживання чіпа у процесі виконання захисного перетворення. При цьому зловмисник повинен знати, при перетворенні якого повідомлення $m_l(i)$ отримана відповідна форма сигналу (зазвичай форми сигналу зберігаються на ПК у вигляді окремих файлів, у назву кожного з яких записується відповідне повідомлення). Загальну сукупність таких повідомлень можна подати у вигляді вектора:

$$\vec{m}_l = (m_l(1),...,m_l(i),...,m_l(N)), \tag{2.1}$$

де N – загальна кількість повідомлень, що обробляються, та відповідно знятих форм сигналу.

У свою чергу, кожну зняту форму сигналу можна представити у вигляді такого вектора:

$$\vec{S} = (S(i,1),...,S(i,j),...,S(i,T)), \tag{2.2}$$

де $S(i, j)$ значення j-го відліку i-ої форми сигналу;

T – кількість відліків i-ої форми сигналу.

Загальну сукупність форм сигналу можна подати у вигляді матриці А розмірністю NxT (таблиця 2.1). Також дуже важливо, щоб значення енергоспоживання для кожного стовпця отриманої матриці були обумовлені виконанням тих самих операцій, тобто необхідно щоб вони були «вирівняні».

Таблиця 2.1 – Матриця значень відліків масиву N форм сигналу, кожна з яких складається з T відліків

Номер форми сигналу	Відлік форми сигналу			
	1	2	…	T
1	$S(1,1)$	$S(1,2)$	…	$S(1,T)$
2	$S(2,1)$	$S(2,2)$	…	$S(2,T)$
…	…	…	…	…
N	$S(N,1)$	$S(N,2)$	…	$S(N,T)$

На третьому етапі складається вектор варіантів підблоку ключа, що перебирається:

$$\vec{k}_l^{'} = \left(k_l^{'}(1),...,k_l^{'}(d),...,k_l^{'}(K)\right), \tag{2.3}$$

де K – загальна кількість можливих варіантів ключа, що перебирається.

Наприклад, якщо зловмисник проводитиме атаку на шифр з використанням виходів S-box, то враховуючи, що вхід S-box визначається сумою восьми біт повідомлення та восьми біт раундового ключа, тобто $\vec{k}_l^{'} = (0,1,...,255)$. Після цього на кожному варіанті ключа $k_l^{'}(d)$ з використанням відомого вектора $\vec{m}_l$ (тобто сукупності повідомлень), обчислюється вектор

передбачуваних проміжних значень (вибраних на першому кроці) – сукупність таких векторів для *K* варіантів підблоку ключа, що перебирається, утворює матрицю B (таблиця 2.2) розмірністю *N*x*K*, де кожен елемент матриці визначається наступним чином:

$$a_l^{'}\left(i, k_l^{'}(d)\right) = f\left(m_l(i), k_l^{'}(d)\right), \tag{2.4}$$

де d=1, …, K; i=1, …, N.

Таблиця 2.2 – Матриця проміжних значень $a_l^{'}\left(i, k_l^{'}(d)\right)$

Номер форми сигналу	Розраховане проміжне значення			
	1	2	…	K
1	$a_l^{'}(1,1)$	$a_l^{'}(1,2)$	…	$a_l^{'}(1,K)$
2	$a_l^{'}(2,1)$	$a_l^{'}(2,2)$	…	$a_l^{'}(2,K)$
…	…	…	…	…
N	$a_l^{'}(N,1)$	$a_l^{'}(N,2)$	…	$a_l^{'}(N,K)$

Кожен стовпець матриці *B* міститиме проміжні значення $a_l^{'}\left(i, k_l^{'}(d)\right)$, обчислені на певному варіанті підблоку ключа *k'*(*d*) для всіх оброблюваних повідомлень. З цього моменту метою атаки DPA є дізнатися значення, з якого стовпця отриманої матриці оброблялися чіпом. Знаючи це, моментально визначається істинний варіант підблоку ключа, що перебирається.

На четвертому кроці, ґрунтуючись на своїх знаннях про аналізований чіп, зловмисник вибирає модель витоку, за допомогою якої кожному розрахованому проміжному значенню $a_l^{'}\left(i, k_l^{'}(d)\right)$ буде зіставлено коефіцієнт, що характеризує передбачувану величину енергоспоживання - з таких величин утворюється матриця C (яка має таку ж розмірність, як і матриця B).

Наприклад, якщо була обрана найпростіша модель ваги Хеммінга, то кожному значенню $a_l^{'}\left(i,k_l^{'}(d)\right)$ буде зіставлена його вага Хеммінга. Якщо припустимо, що $a_l^{'}(3,4)=34=00100010$, то в матриці C елемент з такими самими координатами $h_l^{'}(3,4)=2$, оскільки HW(00100010)=2, а якщо $a_l^{'}(3,14)=63=11111111$, то це значення буде відповідати $h_l^{'}(3,14)=8$. Необхідно розуміти, що ідеальна модель витоку - це та модель, яка кожному розрахованому проміжному значенню $a_l^{'}\left(i,k_l^{'}(d)\right)$ зіставляла б фактичну величину енергоспоживання, проте такі моделі надто складні, і потребують всебічних знань технічних характеристик аналізованого чіпа, які, як правило, недоступні. Тому зазвичай використовують модель витоку, яка зіставляє кожному відліку на знятій формі сигналу якийсь коефіцієнт (наприклад вага Хеммінга значення $a_l^{'}\left(i,k_l^{'}(d)\right)$ або відстань Хеммінга), що є числом, що лише побічно характеризує кількість логічних вентилів, що переключилися (а отже і енергоспоживання чіпа під час обробки відповідної комбінації).

На п'ятому етапі зловмисник здійснює порівняння кожного окремого стовпця матриці C з кожним стовпцем матриці A, тобто спочатку береться перший стовпець матриці C (для першого варіанта підблоку ключа, що перебирається), порівнюється з першим стовпцем матриці A (що містить перші відліки *N* форм сигналу), потім з другим стовпцем матриці A (характеризує другі відліки *N* форм сигналу), і так далі аж до *T*-го стовпця матриці A.

Найчастіше при порівнянні елементів двох матриць застосовують коефіцієнт лінійної кореляції (у зарубіжних джерелах зазвичай застосовують назву "Кореляція Пірсона"):

$$c\left(k_l^{'}(d),j\right)=\frac{\sum_{i=1}^{N}\left[\left(h_l^{'}\left(i,k_l^{'}(d)\right)-h_l^{'}(k_l^{'}(d))\right)\cdot\left(S(i,j)-S(j)\right)\right]}{\sqrt{\sum_{i=1}^{N}\left[\left(h_l^{'}\left(i,k_l^{'}(d)\right)-h_l^{'}\left(k_l^{'}(d)\right)\right)^2\cdot\sum_{i=1}^{N}\left(S(i,j)-S(j)\right)^2\right]}}, \qquad (2.5)$$

де $h_l^{'}\left(k_l^{'}(d)\right)$ - вибірка з ваг Хеммінга проміжних значень $a_l^{'}\left(i,k_l^{'}(d)\right)$, розрахованих на d - му варіанті підблоку ключа, що перебирається, за N повідомленнями;

$S(j)$ – вибірка із значень j-го відліку за N формами сигналу;

X – середнє значення вибірки X.

У результаті утворюється вектор з T коефіцієнтів кореляції $\vec{c}\left(k_l^{'}(d)\right)=\left(c\left(k_l^{'}(d),1\right),c\left(k_l^{'}(d),2\right),...,c\left(k_l^{'}(d),T\right)\right)$, спочатку для першого варіанту ключа, що перебирається. Тобто визначається кореляція між оцінками значень енергоспоживання, розрахованими на варіанті ключа, що перебирається, і реальними значеннями відліків енергоспоживання на усіх формах сигналу. Потім знаходяться такі самі вектори для інших K-1 варіантів підблоку ключа.

При виборі істинного варіанта $k_l^{'}(d)=k_l$ підблоку ключа, що перебирається значення ваг Хеммінга будуть розраховані правильно: $h_l^{'}\left(i,k_l^{'}(d)\right)=h_l(i)$, де $h_l(i)$ – вага Хеммінгу обраного проміжного значення $a_l(i)$. Так як між вагою Хеммінга $h_l(i)$ даних, що обробляються чіпом, та амплітудою сплеску відповідних відліків форм сигналу $S(i, j)$ існує прямо пропорційна залежність, то на кореляційному векторі виникатимуть сплески в районі цих відліків. У районі інших відліків настільки значних сплесків виникати не буде оскільки вони не мають (або мають значно меншу) залежність від $h_l(i)$. На інших варіантах підблоку ключа, що перебирається, $k_l^{'}(d)\neq k_l$ вага Хеммінга $h_l^{'}\left(i,k_l^{'}(d)\right)$ для більшої частини повідомлень буде розрахована невірно, тому значних сплесків на інших кореляційних векторах не виникатиме.

Таким же чином, використовуючи ті ж форми сигналу, відновлюються інші підблоки раундового ключа (задіяні під час обчислення входів інших S-box). Знаючи раундовий ключ першого раунду, для всіх повідомлень, що

перетворюються, зловмисник зможе розрахувати вхід другого раунду, атака на раундовий ключ якого здійснюється аналогічно. Таким

Таким чином, поетапно можна відновити раундові ключі всіх раундів, а, отже, і секретний ключ захисного перетворення.

2.2 Аспекти реалізації атаки DPA з розрахунком векторів кореляції

При реалізації DPA важливим питанням є вибір проміжного розрахованого значення алгоритму захисного перетворення. Зловмисник має обирати таке проміжне значення $a_l(i)$, яке при переборі варіантів підблоку ключа давало б найбільші відмінності у сплесках для істинного та хибних ключів. Наприклад, як проміжне значення, що розраховується, можна вибрати деяку частину результату складання повідомлення з раундовим ключем: $m(i) \oplus k$. Розглянемо представлений на рисунку 2.1 молодший восьмибітовий підблок шифру AES: $m_{0\text{-}7}(i) \oplus k_{0\text{-}7}$. В цьому випадку на істинному варіанті підблоку ключа, що перебирається, $k'_{0-7}(d) = k_{0-7}$, комбінація $a'_{0-7}\left(i, k'_{0-7}(d)\right) = m_{0-7}(i) \oplus k'_{0-7}(d)$ буде розрахована вірно для будь-яких підблоків повідомлення $m_{0\text{-}7}(i)$, що приведе до значного сплеску на кореляційному векторі. Якщо варіант підблоку ключа буде вгаданий неправильно: $k'_{0-7}(d) \neq k_{0-7}$, то значення $a'_{0-7}\left(i, k'_{0-7}(d)\right) = m_{0-7}(i) \oplus k'_{0-7}(d)$ для будь-яких повідомлень $m_{0\text{-}7}(i)$ будет відрізнятися від істинного минимум в одному розряді (враховуючи однозначність операції додавання за mod2).

В цьому випадку доцільно використати формулу для оцінки зниження кореляційного сплеску:

$$c\left(h_l(k_l), h'_l\left(k'_l(d)\right)\right) = \frac{COV\left(h_l(k_l), h'_l\left(k'_l(d)\right)\right)}{\sigma\left(h_l(k_l)\right) \cdot \sigma\left(h'_l\left(k'_l(d)\right)\right)} = \frac{n-2e}{n}, \qquad (2.6)$$

де $h_l(k_l)$ і $h_l^{'}\left(k_l^{'}(d)\right)$ - масиви з N ваг Хемінга проміжних значень $a_l^{'}\left(i,k_l^{'}(d)\right)$, розрахованих відповідно на істинному та хибному варіантах підблоку ключа, що перебирається;

n – довжина комбінації $a_l^{'}\left(i,k_l^{'}(d)\right)$;

e – кількість біт, в яких відрізняється істинний та хибний підблоки ключа.

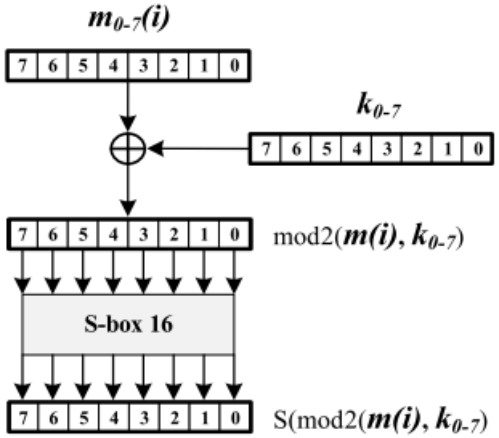


Рисунок 2.1 – Частина першого раунду шифру

З формули (2.6) видно, що у найгіршому для зловмисника разі, коли було обрано помилковий варіант підблоку ключа, який відрізняється від істинного одним розрядом, розрахований в процесі реалізації DPA сплеск на кореляційному векторі виявиться на 25% нижче, ніж на справжньому ключі. На інших варіантах ключа сплеск виявиться ще нижче.

Якщо в якості проміжного значення, що розраховується, вибрати комбінацію виходу S-box, то у цьому випадку аналітична оцінка зниження кореляційного сплеску виявляється надзвичайно складною. Однак, моделювання показує, що за рахунок нелінійності перетворень на S-box помилка навіть в одному розряді підблоку ключа, що перебирається, може призвести до помилки обчислення від одного до всіх восьми бітів виходу S-box. Хоча теоретично ваги Хеммінга отриманих комбінацій можуть збігатися з вагами Хеммінгу комбінацій, отриманих на істинному варіанті підблоку

ключа, що перебирається. Проте моделювання з використанням всіх можливих пар повідомлення/ключ дає ймовірність такого збігу не більше 30%. У той час, як сплеск на кореляційному векторі при найгіршому для зловмисника неправильному варіанті підблоку ключа не перевищить 20.3% (при використанні восьмирозрядної архітектури чіпа), що безумовно значно краще для зловмисника, ніж 75%-й сплеск, у разі використання входів S-box. З цієї причини, при реалізації атаки DPA як розраховане проміжне значення захисного перетворення $a_l(i)$ зазвичай вибирають не результат додавання по mod2, а результат нелінійного перетворення.

Однією з ключових переваг DPA в порівнянні з SPA є можливість придушення практично будь-якої шумової компоненти на формах сигналу за рахунок використання статистичного усереднення.

Одним із центральних понять математичної статистики у контексті розглянутої задачі є поняття кореляційної залежності – це статистичний зв'язок кількох (далі будуть розглядатися лише дві) випадкових величин, при якій зміна однієї з них приводить до закономірної зміни іншої. Мірою кореляційної залежності є коваріація

$$COV(A,B)=\frac{1}{N}\sum_{i=1}^{N}\left(A(i)-\overline{A}\right)\left(B(i)-\overline{B}\right), \qquad (2.7)$$

де A, B – вибірки двох випадкових величин, наявність залежності між якими необхідно визначити (обсяг кожної вибірки дорівнює N);

$A(i)$, $B(i)$ – i-те значення випадкових величин, i=1, 2, …, N;

$\overline{A}$, $\overline{B}$ - середні значення (математичні сподівання) випадкових величин $A(i)$, $B(i)$.

Розраховане за (2.7) значення коваріації буде числом, що характеризує силу лінійної залежності між вибірками A та B . Це число може приймати як позитивні, так і негативні значення. У першому випадку говорять про пряму залежність, у другому – про зворотну. З (2.7) видно, що значення коваріації

визначається не тільки силою залежності випадкових величин, але й розмірністю значень цих величин (тобто одиницями вимірювання). Це значення буде лежати в межах $\mathrm{COV}(A, B) \leq \pm\sigma(A)\cdot\sigma(B)$. При цьому, у разі відсутності лінійної залежності, воно виявляється рівним нулю.

Для усунення залежності значення коефіцієнта коваріації від розмірності значень аргументів використовується його нормування, тобто розподіл коефіцієнта коваріації на добуток СКВ відповідних вибірок – результат є коефіцієнтом кореляції:

$$c\left(k_l^{'}(r), j\right) = \frac{COV\left(h_l^{'}\left(k_l^{'}(d)\right), S(j)\right)}{\sigma\left(h_l^{'}\left(k_l^{'}(d)\right)\right)\cdot\sigma\left(S(j)\right)}, \tag{2.8}$$

де $c\left(k_l^{'}(r), j\right)$ - коефіцієнт кореляції для j-го відліку на $k_l^{'}(d)$ варіанті підблоку ключів, які перебираються;

$\sigma(*)$ – середньоквадратичне відхилення;

$h_l^{'}\left(k_l^{'}(r)\right)$ - вибірка значень ваг Хемінга виходу S-box, розрахована на $k_l^{'}(d)$ варіанті підблоку ключа, що перебирається;

$S(j)$ – вибірка значень j-го відліку по N формах сигналу.

В підсумку кожен відлік коваріаційного вектора зводиться до єдиної розмірності. Таким чином, сплески кореляційного вектора не залежатимуть від розмірностей вибірок, а визначаються лише ступенем залежності їх значень. Значення коефіцієнта кореляції завжди буде в інтервалі від −1 (для ідеальної зворотної залежності) до 1 (для ідеальної прямої залежності). У разі відсутності залежності, так само, як і для коефіцієнта коваріації, значення кореляції прямує до нуля.

Зауважимо, що історично перший алгоритм DPA передбачав, що в якості проміжного значення захисного перетворення вибирається лише один біт виходу S-box. Такий підхід нині зветься «1-Bit DPA». Він обчислював деяку цільову функцію, кінцевий зміст якої зводився до розрахунку коваріації між

розрахованим бітом та відліками на формах сигналу. Очевидно, що при виборі варіанта підблоку ключа, що перебирається, кожен біт виходу S-box буде розрахований вірно, а, отже, спостерігатиметься сильна залежність розрахованого значення з відповідним відліком на формах сигналу. З таблиці 2.1 видно, що при виборі помилкового варіанту ключа ймовірність збігу будь-якого біта виходу S-box з істинним значенням буде помітно нижча. Отже, відповідні сплески на коварійному або кореляційному векторі також виявляться значно меншими.

Таблиця 2.1 - Можливості збігу біт виходу S-box, розрахованих на хибних варіантах підблоку ключа, що перебирається, з відповідними бітами, розрахованими на істинному

	Ймовірність збігу з істинним значенням	
Розряд виходу S-box	Від, %	До, %
0	39,0625	62,5000
1	35,9375	62,5000
2	37,5000	60,9375
3	40,6250	59,3750
4	37,5000	60,9375
5	45,3125	53,1250
6	39,0625	59,3750
7	37,5000	62,5000

Недолік 1-bit DPA полягає в тому, що чіп обробляє комбінації не побітово, а підблоками, довжина яких рівна відповідній розрядності чіпа. Отже, стрибок енергоспоживання, викликаний обробкою, наприклад, виходу S-box на восьми-розрядному чіпі характеризуватиме значення восьми біт виходу S-box загалом. Отже, частина цього стрибка, що характеризує енергоспоживання, яке витрачається на обробку решти (семи неврахованих)

біт буде представляти для зловмисника додатковий (так званий алгоритмічний) шум.

Цей шум у поєднанні з електронним шумом призводить до значного зниження співвідношення сигнал/шум, що дуже негативно впливає на успішність реалізації атаки, приводячи до значних сплесків на помилкових варіантах ключа. Тому на даний час використовується модель Multiple Bit DPA, що передбачає в якості проміжного значення вибирати комбінацію, рівну розрядності чіпа.

2.3 Табличне перетворення «читання зі зміщенням» для S-box на мікроконтролерах Atmel

Реалізація перетворення S-box за допомогою підходу «читання зі зміщенням» на мікроконтролерах Atmel є актуальною темою. Цей метод використовується для обробки восьмирозрядної архітектури чіпа, що передбачає операції над байтами, використовуючи восьмирозрядні шини, регістри та арифметико-логічні пристрої.

Для початку вхідний блок повідомлення $m(i)$, який буде шифруватися, розділяється на восьмибітові частини. Ці частини зберігаються в восьмибітових регістрах або оперативній пам'яті (ОЗП), займаючи вісім байт. Секретний ключ також підлягає перетворенню у раундові ключі $k(r)$, де r - номер раунда, і зберігається в постійній запам'ятовуючій пристрої (ПЗП), щоб уникнути обчислення ключів для кожної ітерації шифрування.

Для виконання операції додавання правої частини повідомлення та раундового ключа за mod2 відповідні байти повідомлення та ключа зчитуються в регістри. Після цього вони піддаються операції арифметичного додавання, результат якої перезаписується в один з регістрів. Отриманий результат може бути скопійований до ОЗП, замінюючи відповідний байт повідомлення $m(i)$. Аналогічні дії виконуються для трьох інших восьмибітових блоків повідомлення та раундового ключа.

Після проведення операцій додавання отримані чотири восьмибітові блоки піддаються перетворенню з використанням S-box. Це перетворення оптимальніше виконувати побайтно. Проте спочатку слід розглянути реалізацію перетворення на S-box, де кожен S-box обробляється окремо, щоб продемонструвати неефективність використання чотирьох бітових операцій на восьмибітовій архітектурі чіпа.

Важливим етапом є програмування комірок ПЗП, яке виконується послідовно для кожного вихідного значення S-box. Комбінації від "0000" до "1111" записуються у вигляді байтів, заносячи в пам'ять програм номер першої комірки. Такі дії повторюються для всіх восьми S-box, при цьому вихідні значення записуються у вигляді байтів, де старші чотири біта нульові.

Хоча використання підходу "читання зі зміщенням" для табличного перетворення S-box на мікроконтролерах Atmel є потенційно ефективним, варто врахувати його обмеження на восьмибітовій архітектурі чіпа.

На рисунку 2.2 представлена схема процесу запису виходів S-box в ПЗУ.

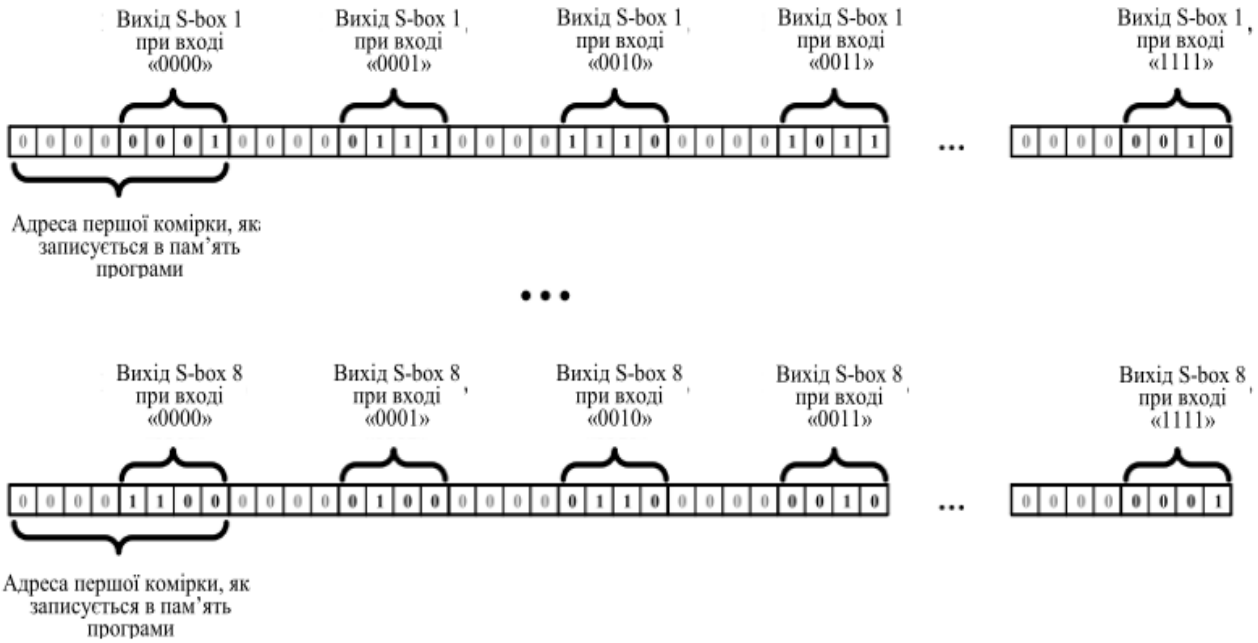


Рисунок 2.2 - Схема процесу запису виходів S-box в ПЗУ

Потім чотири (спочатку молодших) біти 32-х бітової послідовності $m(i)+k(r)$ необхідно скласти з адресою першого осередку восьмого S-box, та за отриманою адресою (тобто за адресою першого осередку восьмого S-box зі зміщенням на величину вхідного значення), здійснити читання з комірки ПЗУ. Її вміст очевидно виявиться виходом восьмого S-box, відповідним його вхідному значенню. Наведемо приклад. Припустимо, що адресою першого осередку восьмого S-box (див. рис. 2.2) є: «0001 1111». Тоді якщо чотири молодші біти суми $m(i)+k(r)$ дорівнюватимуть «0000», то очевидно, що відбудеться читання з першого осередку і зчитється комбінація: "0000 1100". Якщо чотири молодші біти суми $m(i)+k(r)$ дорівнюють «0001», то відбудеться читання з наступного осередку за адресою 0001 1111 + 0001 = 0010 0000. Буде зчитано комбінацію «0000 0100» і так далі. Описану операцію необхідно повторити сім разів для S-box, що залишилися. З наведеного прикладу відразу видно слабкість описаної реалізації табличного перетворення - очевидно, що восьмирозрядні шини, регістри та АЛУ чіпа будуть використовуватися не ефективно (наполовину пропускної можливості). До того ж, у більшості асемблерів виникнуть складності із вичленуванням чотирьох біт із суми $m(i)+k(r)$, записаної в чотирьох регістрах (або осередках ОЗП) побайтно. В асемблерах восьмирозрядних чіпів зазвичай відсутні команди, що дозволяють оперувати чотирма бітами. У цьому випадку чотири біти суми $m(i)+k(r)$ буде необхідно вирізати побітово (побітові операції зазвичай присутні) в деякий проміжний регістр, який потім складатиметься з адресою комірки S-box. На виконання цих операцій піде значний час, що є абсолютно недоцільно (рисунок 2.3).

Аналогічні проблеми виникнуть з виходами S-box, зчитаними з ПЗП. Їх чотири старші біти не нестимуть жодної інформації, тобто виявляться нульовими. Звичайно існують інші підходи до перетворення на чотирьох-розрядних S-box, але їхня ефективність виявиться не кращою.

Враховуючи описані недоліки чотирьох-розрядних перетворень, реалізацію операції S-box очевидно логічніше здійснювати побайтно з

використанням здвоєних S-box. Дана методика передбачає, що в запам’ятовуючий пристрій будуть записуватися виходи пари сусідніх S-box: S-box 1-2, S-box 3-4, S-box 5-6, S-box 7-8 для кожного з 256-ти можливих варіантів входу (рисунок 2.4).

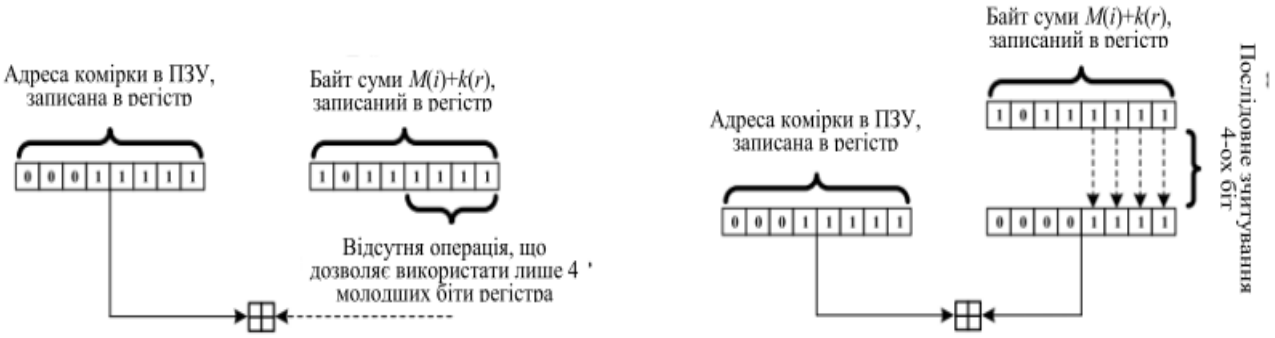


Рисунок 2.3 – Процес додавання адреси першої комірки S-box з комбінацією, яка представляє його вхід

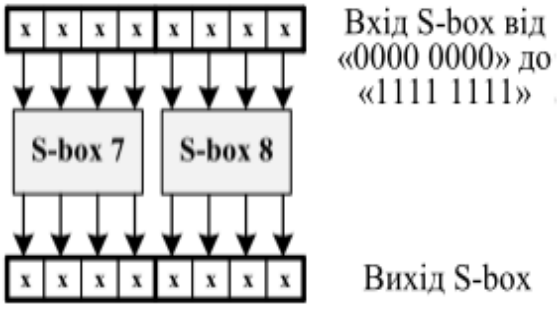


Рисунок 2.4 – Демонстрація роботи здвоєних S-box

В результаті кожний записаний в ПЗП байт буде використаний повністю (рисунок 2.5).

Отже, результат додавання m(i)+k(r) може зчитуватися побайтно однією командою, цей байт додається до адреси першого осередку відповідного S-box, і по знайденою адресою ПЗП зчитується байт - вихід відповідної пари S-box (рисунок 2.6).

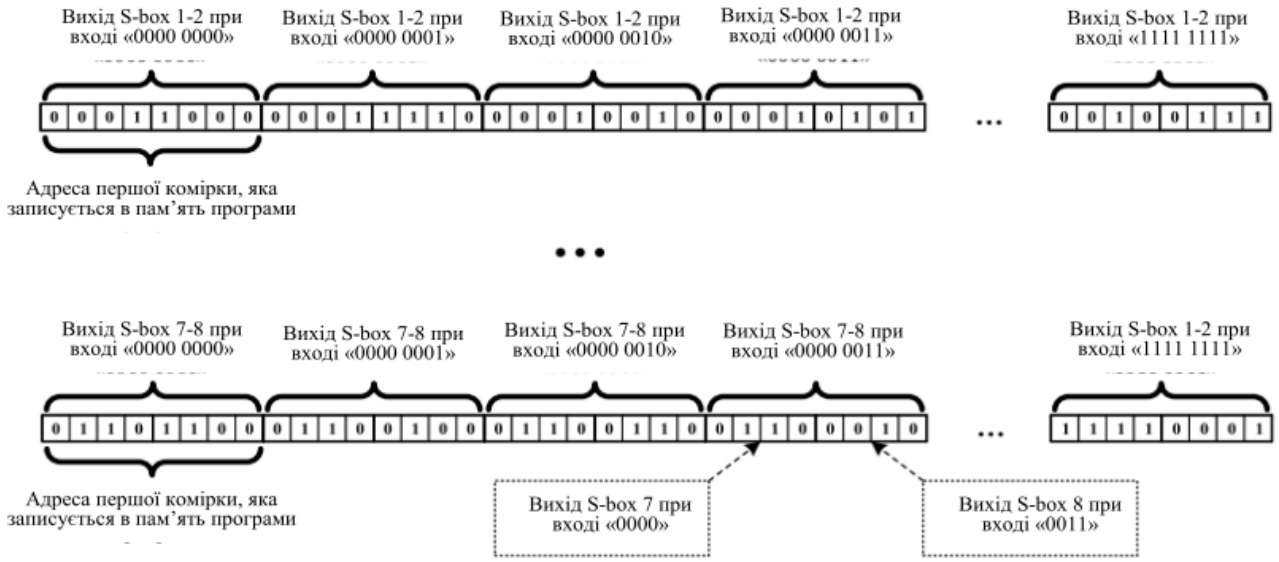


Рисунок 2.5 - Процес запису виходів здвоєних S-box в ПЗП

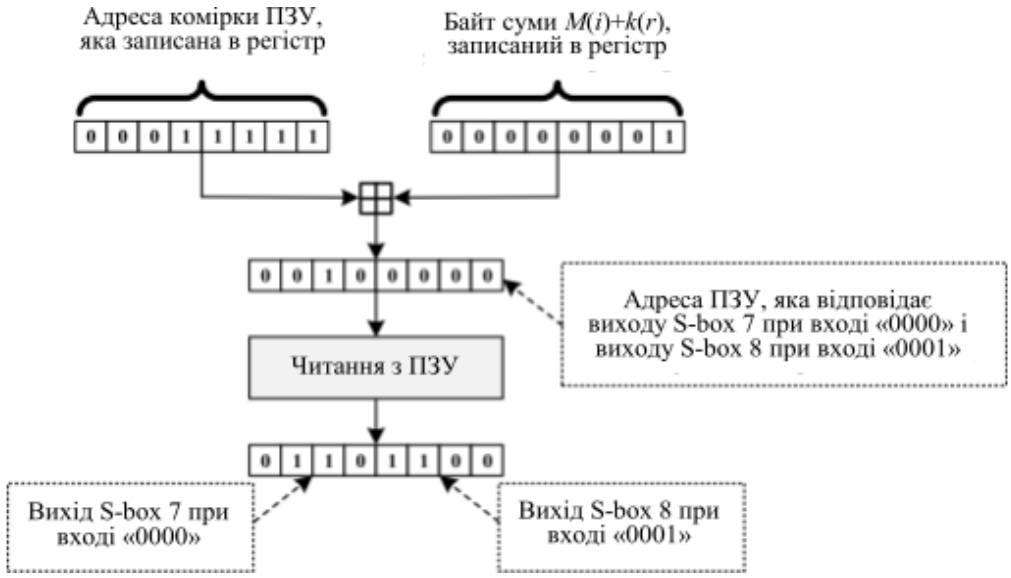


Рисунок 2.6 – Перетворення на здвоєному S-box

Дані операції буде потрібно повторити вже не вісім, а чотири рази. Цей підхід збільшить швидкість виконання перетворення на S-box не менше, ніж у 5 разів, але для зберігання таблиць перетворення чотирьох здвоєних S-box замість 128-ми байт ПЗУ потрібно 1024 байти, що, враховуючи виграш у швидкості перетворення та менший обсяг коду, можна вважати цілком виправданим.

2.4 Оцінка якості вимірювальної установки

Маючи у розпорядженні вимірювальну установку, що має достатню чутливість та смугу пропускання, зловмисник отримує можливість аналізувати стрибки енергоспоживання чіпа та за їх амплітудою робити висновки про оброблювані дані. Однак за будь-яких реальних вимірів на знятих формах сигналу завжди будуть присутні шуми, які можуть значно ускладнювати аналіз. Їх можна розділити на дві великі групи електронні та алгоритмічні.

Нехай при проведенні деяких логічних операцій вимірюється енергоспоживання чіпа. В результаті буде отримана деяка форма сигналу з певною постійною складовою та присутніми на ній стрибками напруги, що характеризують енергоспоживання логічних вентилів за кожний такт роботи чіпа. Якщо, не змінюючи дані, що обробляються чіпом, повторити експеримент і зняти другу форму сигналу, то вона трохи відрізнятиметься від першої – дані відмінності є наслідком впливу електронного шуму. При проведенні реальних вимірювань позбавитися електронного шуму неможливо, проте можна мінімізувати вплив деяких причин виникнення.

Можна виділити такі основні види електронних шумів:

- шум джерела живлення – найбільш очевидний вид шуму, що полягає в нестабільності напруги, яка подається на аналізований чіп, що прямо відбивається на зашумленості форм, що знімаються сигналу. Якщо заживлювати чіп, наприклад, від USB порту ПК, то стандартні для нього шумові коливання напруги в діапазоні 10-50 мВ не дозволять розрізнити невеликі коливання "корисного" сигналу в сотні мікровольт або одиниці мілівольт. Такий рівень шуму буде дуже складно знизити до прийнятних значень навіть після обробки дуже великої кількості форм сигналу. Для мінімізації цього ефекту необхідно використовувати стабільне джерело живлення, та додатково, перед контактами живлення чіпа встановлювати

конденсаторний фільтр. Вимірювальну установку, крім того, доцільно доповнити стабілізатором напруги;

- шум генератора тактового сигналу – тобто нестабільність тактової частоти та зашумлення тактових імпульсів. Приводить до того, що навіть при обробці тих самих даних, від вимірювання до вимірювання значення сигналу зміщуватимуться на часовій шкалі, що призведе до спотворення сплесків напруги. Для мінімізації цих ефектів рекомендується застосовувати якісні кварцові генератори, або значно більш дорогі високоточні генератори довільної сигнальної форми. В принципі погане «вирівнювання» форм сигналу, як правило, не може призвести до неможливості проведення атаки, але здатне значно збільшити необхідну кількість оброблюваних форм сигналу;

- шум живлення периферійних пристроїв – якщо від лінії живлення мікроконтролера заживлюються інші, змонтовані на плату пристрої (генератор тактового сигналу, перетворювач рівнів інтерфейсу RS232 і подібні вузли), то всі ці компоненти можуть впливати на форму сигналу, що знімається, яка крім операцій, що виконуються безпосередньо мікроконтролером, залежатиме від операцій, що виконуються іншими пристроями. Для мінімізації цього ефекту рекомендується використовувати дві лінії живлення – одна безпосередньо для аналізованого чіпа, друга - для периферійних пристроїв. В ідеальному випадку ці дві лінії повинні бути гальванічно розв'язані. У експерименті замість гальванічної розв'язки використовувалися два стабілізатори з фіксованою вихідною напругою та кілька конденсаторних фільтрів, що мало звести до незначного рівня вплив двох ліній живлення одна на одну;

- шум електромагнітного випромінювання – шум викликаний Е/М наведеннями на чіп як від периферійних пристроїв, змонтованих на ту ж плату, так і від сторонніх електричних приладів, включаючи ПК та пристрій збору даних. Даний вид шуму може бути мінімізованим екрануванням чіпа та його ланцюгів живлення, а також проведенням вимірювань у спокійному Е/М середовищі.

У процесі виконання на аналізованому чіпі будь-яких операцій, що становлять захисний алгоритм, зловмисника цікавить енергоспоживання лише тих логічних вентилів, які перемикаються під час обробки даних, які залежать від секретного ключа. Однак на кожному такті одночасно з ними відбувається перемикання великої кількості вентилів, що утворюють різні «системні» вузли. Найбільш тривіальні з них:

- регістр лічильника команд є адресою наступної команди, його значення збільшується після кожної виконаної команди);

- регістр команд (в нього завантажується кодове позначення наступної по порядку команди);

- регістр статусу (змінює своє значення залежно від ряду параметрів результату, отриманого при виконанні чергової команди).

При виконанні реальних вимірів стрибки енергоспоживання чіпа, обумовлені перемиканням безлічі логічних вентилів в рамках одного такту його роботи, як правило, зливаються в один-два «загальні» сплески. Їх амплітуда, крім частини, обумовленої перемиканням цікавлячих зловмисника ЛВ, складатиметься і з енергоспоживання, що витрачається на перемикання «системних» вентилів. Потужність, що споживається такими ЛВ, не представляє для зловмисника жодного інтересу - навіть вона по суті є для нього шумом. Цей шум визначається архітектурою аналізованого чіпа, тому боротися з ним дуже складно. Частину таких алгоритмічних шумових складових, яка не залежить від оброблюваних даних, можна мінімізувати збільшенням кількості оброблюваних форм сигналу (наприклад, від даних, що обробляються, не залежить стан регістру команд та лічильника команд). Іншу частину алгоритмічного шуму, що залежить від оброблюваних даних (наприклад, частина вмісту регістру статусу), на жаль, мінімізувати не можна, що може в результаті призводити до помилок при відновлення секретного ключа чіпа.

3 ДОСЛІДЖЕННЯ ЗАЛЕЖНОСТІ ЕНЕРГОСПОЖИВАННЯ ВІД ОПЕРАЦІЇ ЗАПИСУ В ОЗП

3.1 Опис принципів монтажу аналізованого чіпа

Як аналізований чіп був обраний дуже популярний мікроконтролер Atmel ATmega16L-8AU у корпусі типорозміру DIP-40. Цей чіп має досить високе енергоспоживання, крім того він має широкий діапазон робочих напруг і частот. Як і більшість захищених чіпів, він заснований на восьмирозрядній архітектурі, а формат корпусу DIP-40 спрощує модифікацію схеми та забезпечує високу доступність окремих ніжок.

Для того, щоб знизити ймовірність виникнення електромагнітних наведень та перешкод, на ланцюгу електроживлення мікроконтролера при його монтажі на макетну плату було витримано принцип мінімальної достатності - монтувалися виключно необхідні елементи (рисунок 3.1).

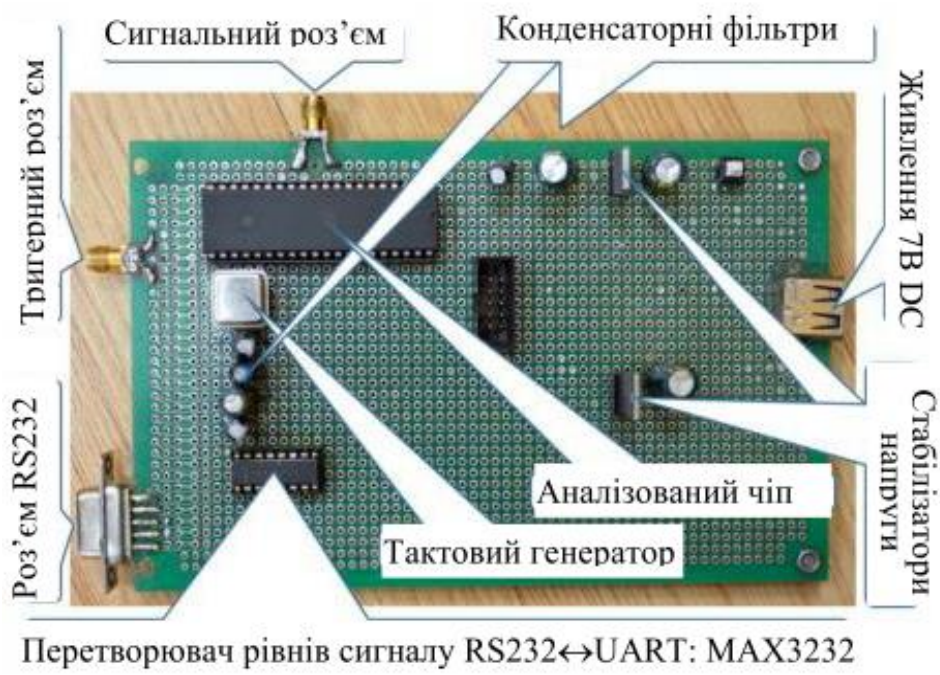


Рисунок 3.1 – Макетна плата з аналізованим мікроконтролером

Живлення плати (7.5 В) здійснювалося від стабілізованого джерела живлення Robiton SN1000S через USB роз'єм (рисунок 3.1, права сторона плати). Між ним та контактами живлення мікроконтролера були змонтовані два конденсаторні фільтри (при цьому останній конденсатор ставиться лише у півсантиметрі від контакту живлення V_{DD} мікроконтролера). У проміжку між фільтрами встановлений стабілізатор напруги LM7805CV, на якому напруга знижується до 5 вольт (стабілізатор застосовується для додаткового захисту від просадок напруги у разі нестабільної роботи побутової мережі). Окремий стабілізатор напруги і два конденсаторні фільтри були встановлені також перед контактами живлення кварцового генератора тактового сигналу та перетворювача рівнів сигналу RS232↔UART. У представленій схемі для тактування мікроконтролера застосовується зовнішній кварцовий генератор, так як вбудований в чіп LC ланцюжок має значно гіршу стабільність. У свою чергу, ПК пов'язаний з мікроконтролером через інтерфейс RS-232 з боку ПК та блок універсального асинхронного приймача (UART) з боку мікроконтролера. Ці інтерфейси електрично не сумісні, тому для узгодження сигналів використовувався перетворювач рівнів сигналу MAX3232.)

Крім цього, на платі змонтовано:

- тригерний роз'єм («SMA») – він з'єднаний з ніжкою мікроконтролера, на яку перед початком виконання захисного перетворення виставляється логічна одиниця. Цей роз'єм, що з'єднується з тригерним входом плати погодження АЦП з ПК, необхідний для запуску збору даних точно у той момент, коли мікроконтролер виконує досліджувані операції. Такий прийом дуже спрощує аналіз енергоспоживання мікроконтролера, оскільки одна з основних вимог, що зумовлюють можливість реалізації побічних атак по ланцюгах електроживлення полягає в тому, що на отримуваних формах сигналу стрибки напруги, що відповідають виконанню будь-якої операції, повинні розташовуватися в тому самому місці на тимчасовій шкалі. Таке спрощення зазвичай можливе лише при використанні пристроїв, запрограмованих зловмисником. При реалізації атаки на пристрій, програма

якого не піддається зміні, може застосовуватися підхід, що передбачає запуск пристрою збору даних через певний інтервал після відправки від ПК на чіп команди, який ініціалізує операцію захисного перетворення. Однак цей інтервал може бути не постійним. У цьому випадку форми сигналу, зняті вручну або за допомогою програмного алгоритму, вирівнюються зловмисником «на око». Така операція займає великий обсяг часу та не завжди можлива;

- сигнальний роз'єм (SMA) – він з'єднаний з контактом землі мікроконтролера через резистор 10 Ом (рисунок 3.2). Саме через цей роз'єм на плату з АЦП надходить сигнал, що характеризує енергоспоживання чіпа. Від його якості прямо залежить успішність атаки, що проводиться. Сигнальний роз'єм через перехідник безпосередньо підключається до входу сигналу плати АЦП. Цей підхід виключає використання довгих з'єднувальних проводів, які, за рахунок ємнісної складової, звужували б смугу пропускання. Така схема включення передбачає, що на АЦП надходитиме сигнал, що характеризує падіння напруги на резисторі, включеному у розрив лінії землі чіпа. За законом Ома воно буде пропорційне силі струму, що протікає по ніжці GND мікроконтролера: $U=R \cdot I=10$ Ом$\cdot I$. Сила струму, в свою чергу, визначатиметься енергоспоживанням мікроконтролера у двох режимах: статичному (струми витоку в транзисторах) та динамічному (струм короткого замикання, струм зарядки паразитних ємностей).

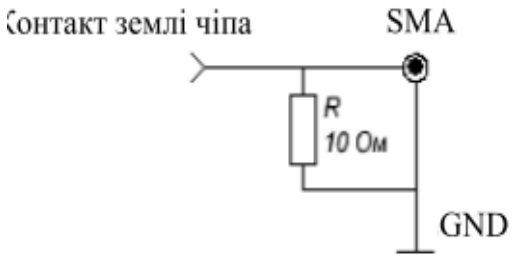


Рисунок 3.2 – Схема підключення сигнального SMA роз'єму до контакту землі чіпа

3.2 Залежність енергоспоживання при виконанні операції запису в ОЗП

На першому етапі мікроконтролер був запрограмований на запис випадкової восьмибітової комбінації (що надійшла в його робочий регістр від ПК) в чисту комірку внутрішнього ОЗП. Для кожного можливого варіанта восьмибітової двійкової комбінації було знято близько 200 форм сигналу, що характеризують енергоспоживання чіпа (тобто 256·200=51200 форм сигналу). Зняті форми сигналу виявляються дуже схожими на форми сигналу, отримані під час виконання команд «nop», крім однієї особливості – на всіх формах сигналу в районі 1300-го відліку (рисунок 3.3) помітний стрибок напруги (сплеск напруги від 0-го до 300-го відліку викликаний енергоспоживанням, що витрачається на посилку тригерного сигналу і від даних не залежить, тому тут і надалі він не враховуватиметься).

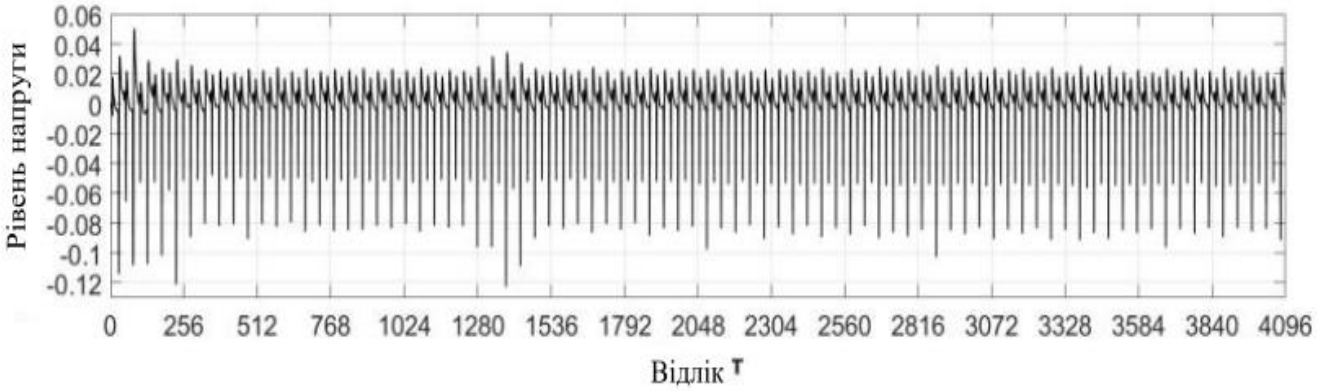


Рисунок 3.3 – Форма сигналу, що характеризує енергоспоживання мікроконтролера при виконання операції запису в чисту комірку ОЗП

Збільшення масштабу ділянки, де відбувається стрибок напруги (рисунок 3.4), дозволяє зробити висновок, що його тривалість складає близько 3 тактів або 150 відліків (з 1328-го по 1478-й відліки). Разом з цим із технічної документації на мікроконтролер відомо, що операція запису байта даних в ОЗП займає 2 такти. Виходить, що стрибок енергоспоживання, обумовлений виконанням аналізованої операції, відбувається не тільки на тих тактах, на

яких ця операція виконується, а й зачіпає сусідні такти. Можна припустити, що причиною цього явища є затримки поширення сигналу і ємнісні складові контактних доріжок, яким необхідно деякий час на розряд. Факт того, що даний часовий інтервал насправді відповідає операції запису в ОЗП, що підтверджується і аналізом програмного коду мікроконтролера – затримка між посилкою тригерного сигналу та операцією запису в ОЗП становить 25 тактів, що відповідає приблизно 1250 відлікам на формі сигналу.

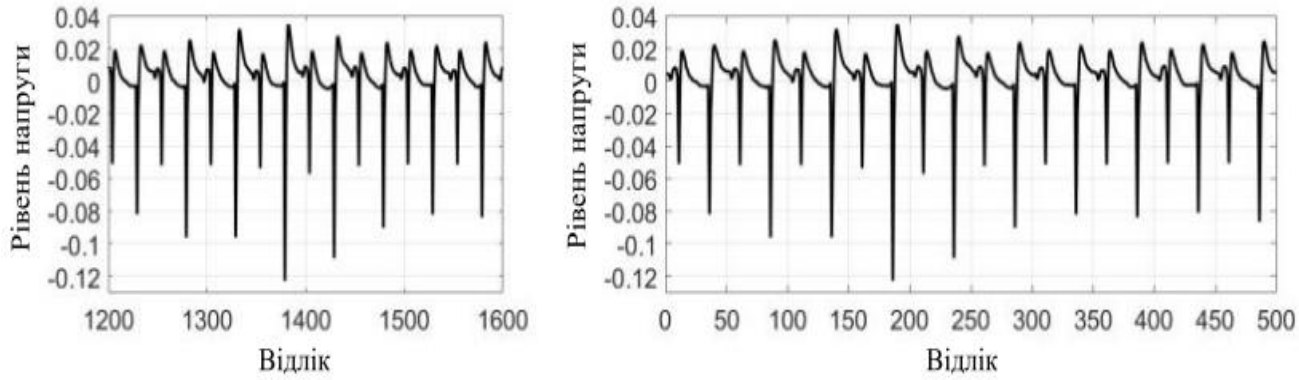


Рисунок 3.4 – Збільшена ділянка форми сигналу, яка характеризує енергоспоживання мікроконтролера при виконанні операції запису в чисту комірку ОЗП: а) до вирівнювання; б) після вирівнювання форм сигналу та вирізання розглянутої ділянки

Зняті форми сигналу очікувано виявилися розсинхронізованими і потребували вирівнювання. Емпірично було з'ясовано, що найбільш надійна прив'язка здійснюється за максимальним значенням, що знаходиться у вікні між 1360-м і 1410-м відліками. При виконання операції вирівнювання з форм сигналу вирізався інтервал в 500 відліків (включаючи 2.5 такти до виконання аналізованої операції та п'ять тактів після), що дозволило скоротити час їхньої подальшої машинної обробки (рисунок 3.4б).

Найбільший інтерес представляють такти, яким відповідають два максимальні сплески на 140-му та 190-му відліках форм сигналу (приклад однієї з них зображений на рисунку 3.4б). На рисунках 3.5 збудовано

гістограми розподілу їх значень (далі аналізований на формі сигналу відлік називатиметься цільовим). При їх порівнянні з гістограмою видно, що для 140-го відліку математичне очікування змістилося у бік великих значень приблизно на 0.0085 рівня напруги (що еквівалентно 16.5 мВ): з 0.0226 (41 мВ) до 0.0311 (57.5 мВ), а для 190-го відліку - на 22.9 мВ, тобто до 0.0355 (63.9 мВ). СКВ також збільшилося більш, ніж у 2 рази, з 0.00094 (1.7 мВ) до 0.00246 (4.4 мВ) для 140-го відліку та до 0.00199 (3.6 мВ) для 190-го відліку.

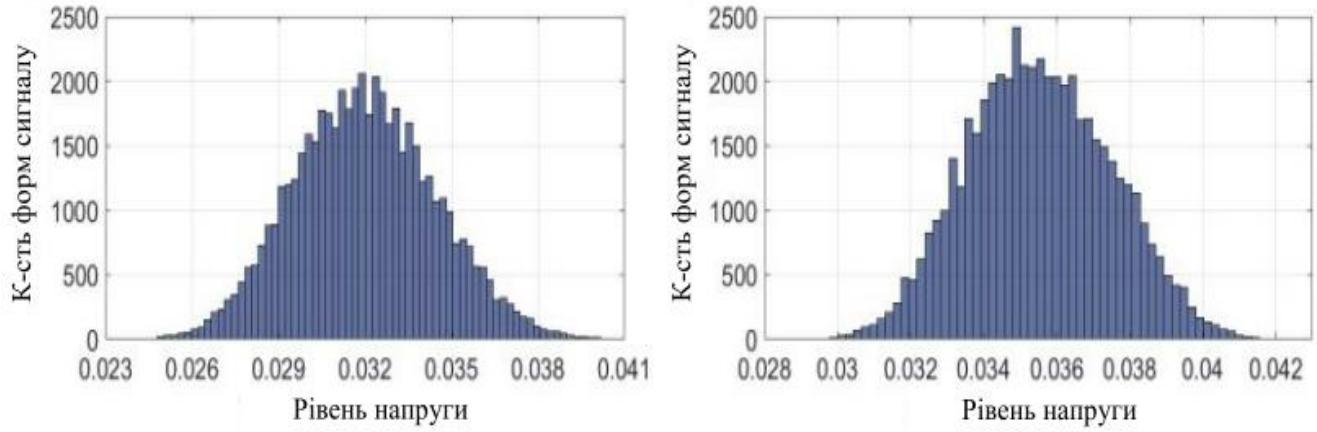


Рисунок 3.5 - Гістограми розподілу значень: а) 140-го; б) 190-го відліків

Логічно припустити, що зміщення математичного очікування було викликане виконуваною операцією з оброблюваними даними. Для перевірки цієї гіпотези було побудовано окремі гістограми розподілу значень 140-го відліку для масивів форм сигналу, відповідних обробці кожного з дев'яти можливих ваг Хеммінгу. Спочатку були відібрані форми сигналу, отримані при збереженні в ОЗП комбінацій з вагою Хеммінга, рівною "0", потім з вагою Хеммінга "1" і так далі, аж до ваги Хеммінга, що дорівнює восьми.

Після цього для кожного складеного масиву форм сигналу була побудована окрема гістограма розподілу значень 140-го відліку, і такі ж дії були реалізовані щодо 190-го відліку. Огинаючі гістограми для всіх дев'яти ваг Хеммінга зведені в єдиному масштабі на рисунках 3.6, з чого виразно видно, що для кожної ваги Хеммінга значення цільового відліку мають нормальний розподіл із приблизно однаковим СКВ та різним середнім значенням (тобто

математичним сподіванням). Дані гістограми є експериментальним підтвердженням висунутої раніше гіпотези, згідно якої енергоспоживання мікроконтролера пропорційно залежить від кількості логічних вентилів, які перемикалися, а, отже, від ваги Хемінга комбінацій, які обробляються.

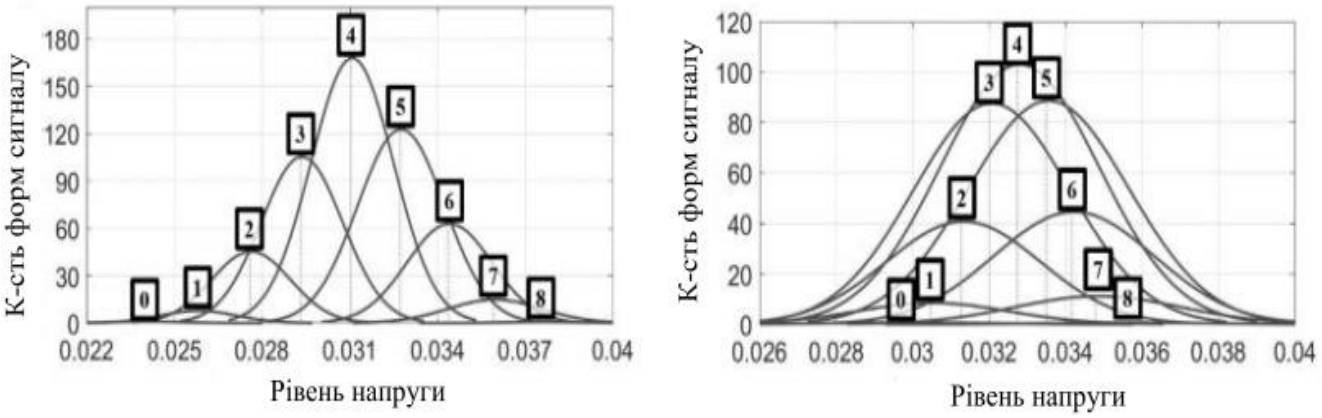


Рисунок 3.6 - Огинальні гістограми розподілу значень: а) 140-го; б) 190-го відліків залежно від ваги Хеммінгу оброблюваних байт (вказаний у квадратах)

Кожне збільшення на одиницю ваги Хеммінгу оброблюваних комбінацій призводить до збільшення середнього значення цільового відліку приблизно на 2.3 мВ для 140-го відліку та на 1.2 мВ для 190-го відліку. СКВ шуму при цьому трохи збільшується зі збільшенням ваги Хеммінга, в середньому на 0.2 мВ для 140-го відліку і на 0.05 мВ для 190-го відліку. Його усереднене значення становить 2.6 мВ для 140-го відліку та 2.9 мВ для 190-го відліку.

З отриманих експериментальних результатів можна дійти невтішного висновку, що у формах сигналу завжди присутній електронний шум $U_{Ел.Шум}$, який залежить від оброблюваних даних. Разом з цим СКВ шуму виявляється порівняним або більшим від відмінностей математичних очікувань цільового відліку для сусідніх ваг Хеммінга. Використовуючи правило трьох сигм, можна визначити, що для 140-го відліку, для порядку 60% форм сигналу

шумова компонента не буде виходити за межі (-2.3, +2,3) мВ. Отже, для цих форм сигналу можливе однозначне визначення ваги Хеммінга за значенням відліку. Для решти 40% форм сигналу визначення ваги Хеммінга, що зберігаються в ОЗП даних, за значеннях відліку на окремій формі сигналу, виявиться практично неможливим, через накладення на даний відлік шумової компоненти, що перевищує відмінності математичних очікувань цільового відліку для сусідніх ваг Хеммінга. Можливість однозначного визначення ваги Хеммінга оброблюваної комбінації за значенням 190-го відліку буде існувати для близько 40% форм сигналу, за рахунок зменшення співвідношення сигнал/шум.

Значення цільового відліку можна описати наступною математичною моделлю:

$$U_{заг} = U_{сигн} + U_{ел.шум}, \quad (3.1)$$

де $U_{сигн}=U_{дан}+U_{оп}+U_{пост.шум}+U_{алг.шум}$ – стрибок напруги, який визначається операцією, що виконується мікроконтролером, і вагою Хеммінга оброблюваних даних, його середнє значення виявиться зсунутим за рахунок постійного і алгоритмічного шуму.

Важливо зауважити, що при розгляді на формах сигналу відліку, що відповідає виконанню однієї і тієї ж операції з одними і тими ж даними, яка відбувається в один і той же час, компоненти $U_{дан}$, $U_{оп}$, $U_{пост.шум}$, $U_{алг.шум}$ будуть постійними.

Для наведених вище даних на 140-му відліку $E(U_{дан})$=2.3 мВ, на 190-му відліку другого такту $E(U_{дан})$=1.2 мВ. Для визначення $E(U_{оп})$ необхідно знати математичне очікування найбільшого сплеску напруги на такті, на якому мікроконтролер не виконує операцій (виконує порожню операцію). Відомо, що воно складає 41 мВ. Отже, враховуючи те, що за збереження в ОЗП комбінації з нульовою вагою Хеммінга (в процесі чого, ймовірно, не відбувається перемикання логічних вентилів ОЗП) математичне очікування

найбільшого сплеску (а саме 190-й відлік на другому такті) становить 52.8 мВ. Тоді $E(U_{оп})$=58.2-41=17.2 мВ і відповідно $E(U_{пост.шум})+E(U_{алг.шум})$=41 мВ.

$U_{ел.шум}$ являє собою шумову складову з нульовим середнім значенням $E(U_{ел.шум})=0$ та гауссівським розподілом, який характеризується деякою дисперсією $Var(U_{ел.шум})=\sigma^2_{ел.шум}$. Для 140-го відліку вона становить 2.6^2=6.76, а для 190-го відліку – 2.9^2=8.41.

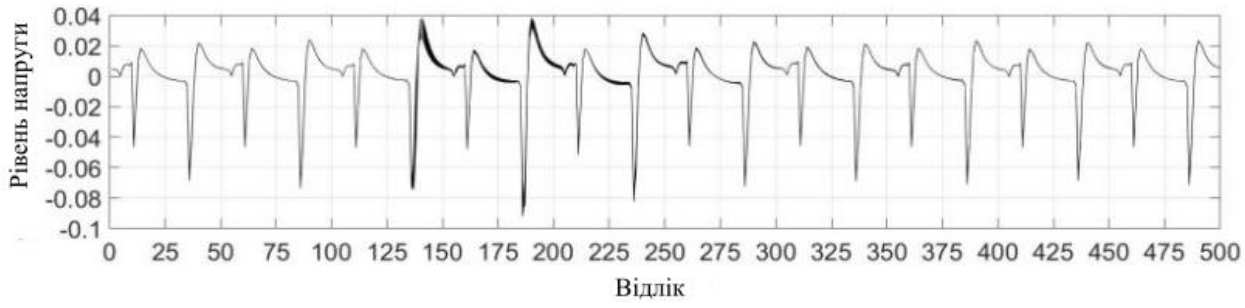
Можна показати, що усереднення великої (в ідеальному випадку нескінченної) кількості форм сигналу для кожної ваги Хеммінга призведе до того, що буде знайдено математичне очікування кожного (у тому числі цільового) відліку.

Тому на усередненій формі сигналу шумова складова цільового відліку буде прямувати до нуля (так як $E(U_{ел.шум})=0$) і значення відліку прямуватиме до $U_{сиг}$ (так як $E(U_{сиг})$=const).

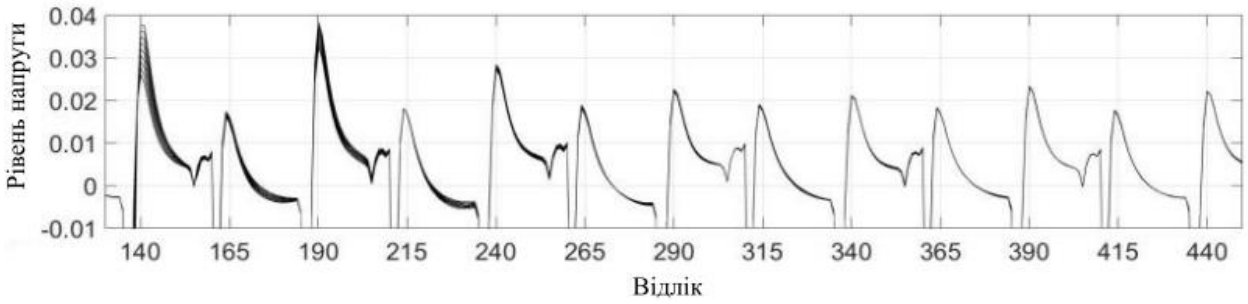
Для перевірки цієї гіпотези на практиці вирівняні 51200 форм сигналу були усереднені для кожної з дев'яти ваг Хеммінга, тобто сукупність форм сигналу була розбита на дев'ять масивів залежно від ваги Хеммінга байта, що обробляється. Після цього по кожному масиву була розрахована усереднена форма сигналу. Дев'ять усереднених форм сигналу для різних ваг Хеммінга представлені на рисунках 3.7.

Збільшення масштабу представленої на рисунку 3.7а форми сигналу дозволяє зробити висновок, що залежність енергоспоживання чіпа від оброблюваних даних існує на шести тактах роботи мікроконтролера (збільшені області усереднених форм сигналу представлені на рисунку 3.7б). При цьому сила залежності зменшується від такту до такту, непостійним є і характер залежності – у деяких випадках вона пряма, в інших – зворотна. На рисунку 3.8 наведена збільшена область форми сигналу, яка характеризує енергоспоживання чіпа на першому такті з 136 по 186 відліки. Залежність від даних проявляється у всій області форми сигналу. Для спрощення характеристики залежностей кожен такт був розбитий на чотири області: перша та третя – максимальні негативні сплески на такті (включаючи область

справа, в якій вони наростають), друга та четверта – максимальні позитивні (включаючи область справа, де вони спадають).



а)



б)

Рисунок 3.7 - Дев'ять усереднених форм сигналу для різних ваг Хеммінга під час виконання операції запису в чисту комірку ОЗП

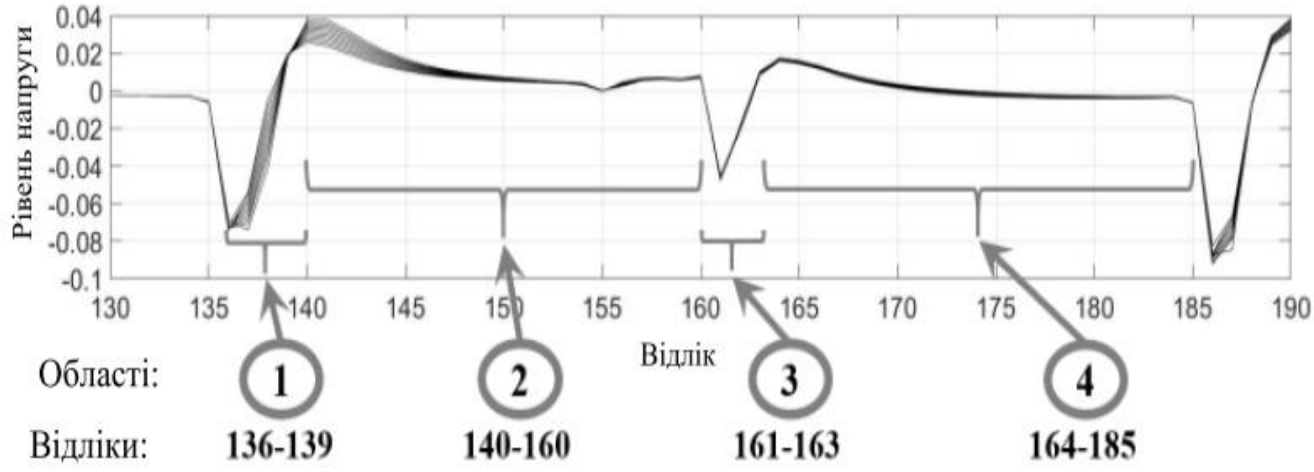


Рисунок 3.8 - Дев'ять усереднених форм сигналу для різних ваг Хеммінга, встановлення кордонів областей аналізованих тактів

Максимальна різниця в енергоспоживанні при обробці даних із різними вагами Хеммінга виникає в першій та другій областях першого такту (відповідно до $U_{дан}$=7.2 мВ і $U_{дан}$=2.7 мВ для кожного збільшення ваги Хеммінга на одиницю). Залежність у третій області набагато слабші (до $U_{дан}$=0.46 мВ), залежність у четвертій області також дуже слабка (до $U_{дан}$=0.44 мВ). Також необхідно звернути увагу на те, що найбільша залежність від оброблюваних даних проявляється не в пікових значеннях форм сигналу, а областях, розташованих правіше (областях наростання та спаду сигналу). Така сама структура залежності спостерігається і в наступних тактах. Також цікаво відзначити, що у різних областях такту напрямок залежності довільним чином змінюється від прямої на зворотну.

Очевидно, що чим більше значення $U_{дан}$ по відношенню до $U_{ел.шум}$ (чим сильніший сигнал, що перевищує шум), тим менше форму сигналу буде необхідно усереднити для однозначного визначення ваги Хеммінга оброблюваної мікроконтролером комбінації на певному такті. Зазвичай для характеристики відношення сигналу до шуму використовують так званий коефіцієнт сигнал/шум (SNR), який визначається за такою формулою:

$$SNR = \frac{Var(Сигнал)}{Var(Шум)}, \tag{3.2}$$

де $Var(Сигнал)$ – це дисперсія $U_{дан}$ для різних ваг Хеммінга;

$Var(Шум)$ – дисперсія шуму.

У контексті побічних атак по ланцюгах електроживлення можна сказати, що чим більше значення SNR, тим більше інформації «витікає» ланцюгом електроживлення.

Значення $U_{дан}$, СКВ і SNR для кожної з чотирьох областей кожного з шести тактів, на яких існує залежність енергоспоживання від ваги Хеммінгу оброблюваних даних наведено в таблиці 3.1. При цьому в межах кожної області вибирався один відлік, на якому значення $U_{дан}$ є максимальним

(максимальна залежність енергоспоживання від даних). Наприклад, у другій області першого такту (140-160-й відліки) максимальне значення $U_{дан}$ досягається на 141-му відліку – у таблиці наведено значення $U_{дан}$, СКВ та SNR для даного відліку, також вказано напрямок залежності – пряма чи зворотна.

Таблиця 3.1 - Відліки з найкращими для зловмисника значеннями $U_{дан}$, СКВ і SNR у кожній з чотирьох областей тактів, на яких існує залежність енергоспоживання від ваги Хеммінга оброблюваних даних, при виконанні операції запису в чисту комірку ОЗП

Такт	Область	Залежність	Відлік	$U_{дан}$,мВ	СКВ,мВ	SNR	Особл. відмітки
1	2	3	4	5	6	7	8
1	1	Обернена	138	7,155	26,51	0,17515	
	2	Пряма	141	2,727	2,55	2,87130	
	3	Обернена	162	0,462	25,34	0,00070	*
	3	Обернена	163	0,337	8,5	0,00380	*
	4	Обернена	172	0,438	1,62	0,17858	
2	1	Обернена	187	3,479	56,94	0,00772	
	1	Пряма	189	0,944	11,00	0,02308	*
	2	Пряма	190	1,229	2,92	0,47183	
	3	Залежність сильно порушена					
	4	Обернена	228	0,353	1,56	0,11022	
	4	Обернена	230	0,333	1,52	0,11265	
3	1	Обернена	237	1,782	47,20	0,00269	*
	2	Пряма	240	0,244	1,74	0,05361	
	2	Пряма	242	0,271	2,98	0,01648	
	3	Залежність сильно порушена					
	4	Пряма	264	0,194	1,71	0,01802	
	4	Обернена	284	0,140	1,54	0,01906	

Продовження таблиці 3.1

1	2	3	4	5	6	7	8
4	1	Обернена	289	0,214	9,31	0,00095	*
	2	Обернена	290	0,118	1,97	0,01355	*
	2	Обернена	293	0,146	2,26	0,00873	*
	3	Залежність сильно порушена					
	4	Пряма	316	0,108	2,39	0,00400	*
	4	Пряма	323	0,092	1,64	0,00997	
5	1	Залежність сильно порушена					
	2	Обернена	352	0,084	1,52	0,00781	
	2	Обернена	355	0,106	2,76	0,00266	
	3	Залежність сильно порушена					
	4	Пряма	384	0,063	1,53	0,00387	
6	1	Залежність сильно порушена					
	2	Пряма	390	0,029	1,94	0,00138	*
	2	Пряма	391	0,039	2,47	0,00106	*

У графі «Особливі позначки» проставлявся знак «*» у тому випадку, якщо в зазначеному відліку залежність була порушена для однієї ваги Хеммінга. Якщо у всіх розрахунках відповідної області залежність порушувалася для двох або більше ваг Хеммінга, то навпроти номера відповідної області проставлялася позначка «Залежність сильно порушена». Необхідно відзначити, що максимальне значення $U_{дан}$ у межах аналізованої області не завжди означає, що в даному відліку буде спостерігатися максимальний SNR. Значення СКВ шуму може відрізнятися в 2-3 рази для різних відліків, навіть в областях, на яких не відбувається різких спадів або наростання сигналу (як у першій та третій областях). У свою чергу, в першій та третій областях спостерігаються різкі спади та наростання сигналу (див. рис. 3.8). У цих областях $U_{дан}$ досягають дуже великих значень, але разом з тим спостерігається й значна дисперсія шуму. Це явище можна пояснити

обмеженістю частоти дискретизації використовуваної вимірювальної установки. Воно дуже ясно ілюструється формами сигналу, зображеними на рисунку 3.8 - навіть при обробці тих самих даних на одній і тій же операції деякі зняті форми сигналу можуть дуже сильно спотворюватися, причому не складає труднощів автоматично відбраковувати такі форми сигналу. Для випадків, коли максимальні значення $U_{дан}$ не відповідають максимальним значенням SNR у таблиці 3.1 додані рядки, що мають сірий фон. В них вказані відліки у тій же області відповідного такту, в яких SNR є максимальним. На основі результатів вимірювань, наведених у таблиці 3.1, а також описаного вище, можна зробити наступні основні висновки про особливості енергоспоживання аналізованого чіпа при виконанні операції запису байта даних у чистий осередок ОЗП:

- енергоспоживання мікроконтролера має дуже істотну залежність від оброблюваних даних. При цьому виконанням самої операції обумовлено збільшення амплітуди стрибків напруги на знятих формах сигналу до 17.2 мВ (майже на 42%, або 8.6 мВт) порівняно з виконанням чіпом порожньої команди. Крім того, енергоспоживання визначається вагою Хеммінга оброблюваних даних, причому ця "добавка" може досягати 7.2 мВ (17.6%, або 3.6 мВт) для кожного збільшення ваги Хеммінгу на одиницю;

- залежність енергоспоживання від даних, що обробляються, зачіпає мінімум чотири наступних такти. (Далі це явище називатиметься залишковою кореляцією.) Енергоспоживання на цих тактах також залежатиме від ваги Хеммінгу комбінації, що обробляється. Ця залежність спадає від такту до такту, причому можна вважати, що через п'ять тактів вона сходить нанівець;

- на кожному з шести тактів найбільший SNR спостерігається у другій та четвертій областях, до того не в пікових значеннях, а правіше (областях спаду сигналу);

- характер залежності може змінюватися кілька разів від прямої на зворотну навіть у межах однієї області такту.

3.3 Залежність енергоспоживання від оброблюваних даних при виконання операції запису в попередньо заповнену комірку ОЗП

Описаний експеримент був повторений для операції запису даних у комірку ОЗП, яка містить деяку випадкову комбінацію (ця операція виконується мікроконтролером також за два такти). Проте в даному випадку розраховувалася не вага Хеммінга для байта, що зберігається, а відстань Хеммінга між даними, що записуються в запам’ятовуючий пристрій, і тими даними, які вони перезаписують. Дев'ять усереднених форм сигналу представлені рисунку 3.9.

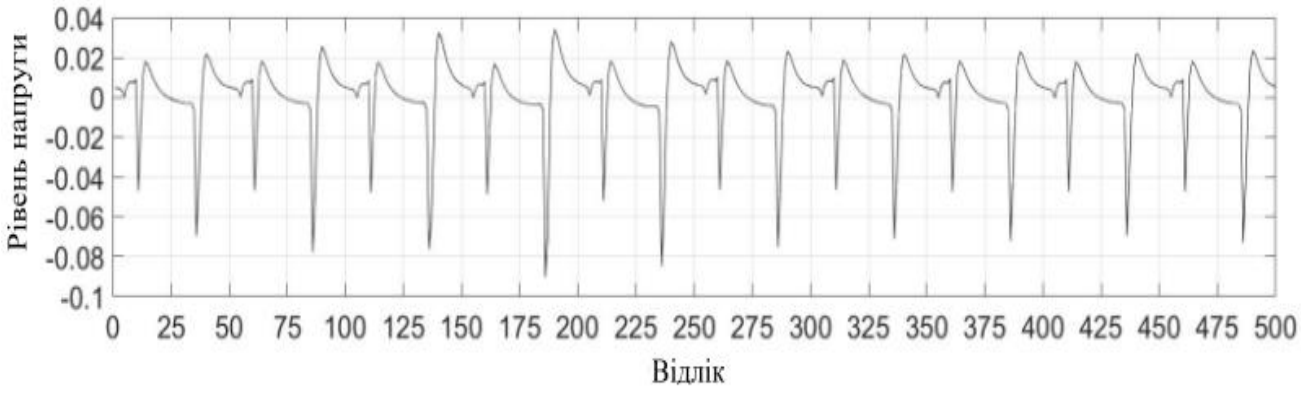


Рисунок 3.9 – Дев'ять усереднених форм сигналу для різних відстаней Хеммінга під час виконання операції запису в попередньо заповнену комірку ОЗП

Збільшення масштабу на рисунку 3.9 показує, що всього лише на двох перших тактах існує відповідна залежність енергоспоживання мікроконтролера від відстані Хеммінга між даними, що записуються і перезаписуються в ОЗП (збільшені області форми сигналу представлені на рисунках 3.10).

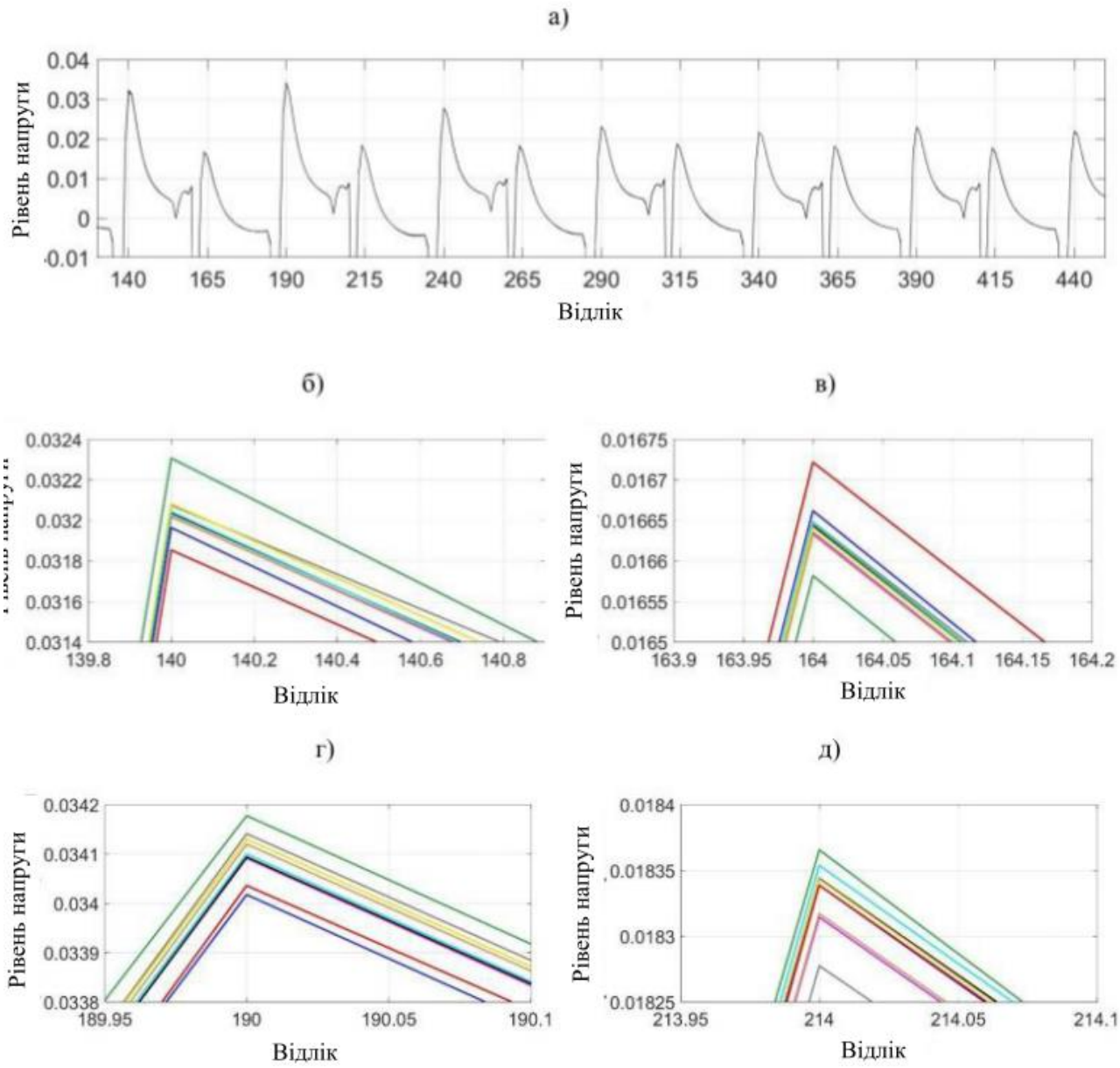


Рисунок 3.10 – Збільшені області усереднених форм сигналу, які характеризують залежність енергоспоживання мікроконтролера ATmega 16 від віддалі Хеммінга між записуючою та перезаписуючою комбінаціями, при виконанні операції запису в попередньо заповнену комірку ОЗП

При цьому залежність є дуже слабкою та для деяких відстаней Хеммінгу порушується. Тому були збудовані (рисунок 3.11) дев'ять усереднених форм сигналу без урахування наявності в осередку ОЗП будь-яких даних (з використанням моделі ваги Хеммінгу).

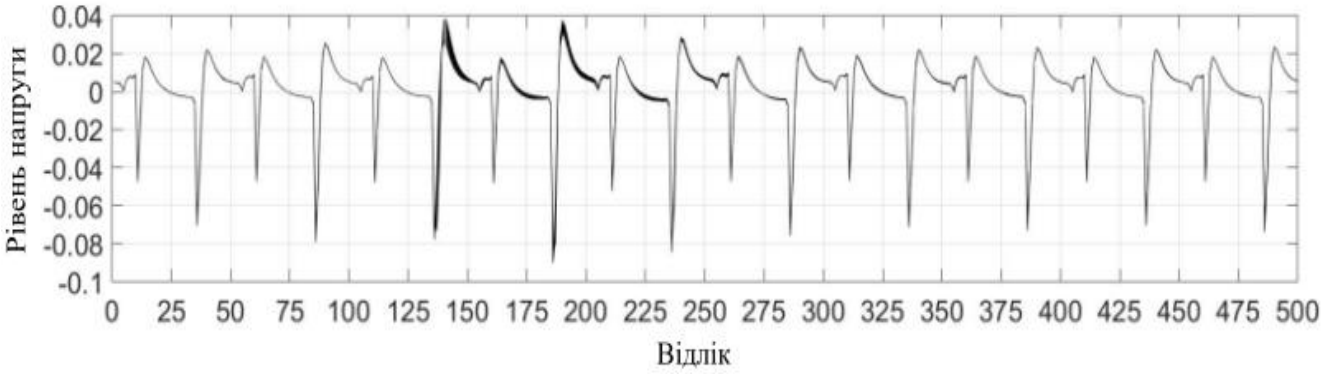


Рисунок 3.11 – Дев'ять усереднених форм сигналу для різних ваг Хеммінга під час виконання операції запису в попередньо заповнену комірку ОЗП

Гістограми, а також характеристики форм сигналу, при використанні моделі ваги Хеммінга практично повністю повторюють описані раніше, для операції запису в чисту окомірку ОЗП (у тому числі і явище залишкової кореляції на чотирьох наступних тактах).

Аналогічно операції запису в чисту комірку ОЗП, для операції запису в попередньо заповнену комірку кожне збільшення на одиницю ваги Хеммінгу оброблюваних комбінацій призводить до збільшення середнього значення 140-го відліку приблизно на 2.29 мВ, а 190-го - на 1.3 мВ. СКВА шуму також трохи збільшується зі збільшенням ваги Хеммінга, і в середньому воно становить 2.44 мВ та 1.76 мВ відповідно. SNR для 140-го відліку складе 2.26, а для 190-го – 1.34, значення $E(U_{On})$=55.3-41=14.3 мВ. Значення $U_{дан}$, СКВ та SNR для ділянок шести тактів, на яких існує залежність енергоспоживання від ваги Хеммінга оброблюваних даних, показує, що відсутні скільки-небудь значні відмінності в енергоспоживанні порівняно з випадком запису даних у чисту комірку ОЗУ.

З даних можна зробити висновок, що енергоспоживання мікроконтролера практично не залежить від кількості біт, що змінилися, в попередньо заповненому осередку ОЗП. Звідси логічно припустити, що осередки ОЗП перед записом нових даних затираються або операція запису в ОЗП вимагає незначних витрат енергії. В цьому випадку отримані при

використанні моделі ваги Хеммінга сплески обумовлені тільки енергією, що витрачається на читання даних з регістру в АЛП та зарядку ліній шини даних для подальшого пересилання в ОЗП. У будь-якому випадку, незалежно від того, чи здійснюється запис в чисту комірку ОЗП, або попередньо заповнену, для визначення записуваної комбінації по знятих формах сигналу необхідно використовувати модель ваги Хеммінга.

ВИСНОВКИ

1. Здійснено класифікацію атак за побічними каналами електроживлення, що дозволило обгрунтувати вибір методів захисту від атак кожного класу.

2. Розроблено узагальнене алгоритмічне забезпечення атаки DPA, що дозволило реалізувати табличне перетворення «читання зі зміщенням» для S-box на мікроконтролерах Atmel.

3. На основі реалізації табличного перетворення проведено дослідження залежності енергоспоживання при виконанні операції запису в ОЗП.

4. На мікроконтролерах Atmel реалізоване табличне перетворення «читання зі зміщенням» для S-box при шифруванні та проведено оцінку якості вимірювальної установки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Akkar M., Giraud 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.

2. Lv J. On Two DES Implementations Secure against Differential Power Analysis in Smart-Cards. Information and Computation. 2006. Vol. 204. Iss. 7. P. 1179–1193.

3. 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.

4. Петраков А.В. Основи практичного захисту інформації. К.: Юніор, 2009. 395 с.

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

7. 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. C. 310– 313.

8. 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.

9. 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.

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

11. 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.

12. 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.

13. 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.

14. Balasch J., Gierlichs B., Verdult R., Batina L., Verbauwhede I. Power Analysis of Atmel CryptoMemory – Recovering Keys from Secure EEPROMs. Topics in Cryptology – CT-RSA 2012. Lecture Notes in Computer Science. 2012. Vol. 7178. P. 19-34. 212

15. Brier E., Clavier C., Olivier F. Correlation Power Analysis with a Leakage Model. Cryptographic Hardware and Embedded Systems - CHES 2004. CHES 2004. Lecture Notes in Computer Science. 2004. Vol. 3156. P. 16-29.

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

17. Messerges T., Dabbish T., Sloan R. Investigations of power analysis attacks on smartcards. Proceedings of the USENIX Workshop on Smartcard Technology. 1999. P. 151-162.

18. 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.

19. Голембйовський М.П., Лисик М.А., Гончарик Г.Я. Класифікація криптоаналітичних атак за побічними каналами. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.139-141.

20. Голембйовський М.П., Голембйовський П.М. Реалізація табличного перетворення «Читання зі зміщенням» для S-box на мікроконтролерах Atmel. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.36-38.

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

22. 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.

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

24. 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.

25. 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.

26. 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.

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

28. 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.

29. 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.

30. 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.

ДОДАТОК А

Копії публікацій