Дослідження методів протидії аналізу криптосистем при апаратній реалізації RSA

Студентка групи ДА-51м
Казаченко Ольга Дмитрівна
Керівник роботи:
Доцент, к.т.н., Капшук О. О.

Мета роботи. Дослідження існуючих методів протидії аналізу криптосистем, за інформацією, що несуть сторонні канали, а також дослідження цієї інформації за допомогою розробленого приладу, на тестовій апаратній реалізації RSA.

Об'єкт дослідження. Сторонні канали та інформація, яку вони несуть при роботі криптосистеми.

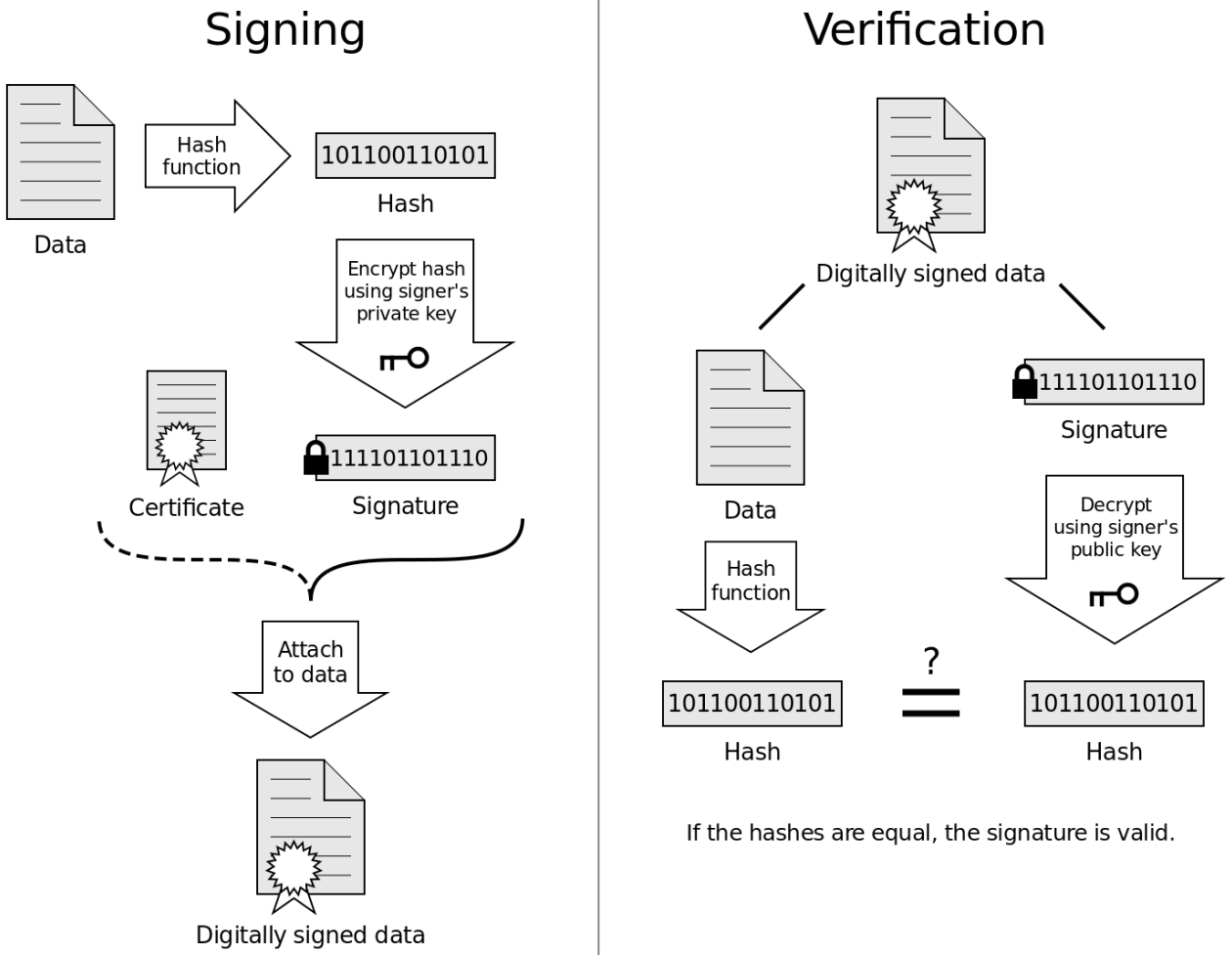
Предмет дослідження. Протидії аналізу інформації по стороннім канали, їх вплив на реалізацію алгоритму, його швидкодію та надійність.

Завдання

- Провести огляд аналізу сигналів, що будуть отримані;
- Провести огляд криптосистеми RSA;
- Дослідити існуючі атаки, що базуються на інформації, отриманої по стороннім каналам;
- Проаналізувати основні, існуючі методи протидії аналізу сторонніх каналів;
- Розробити пристрій, що допомагає збирати інформацію для аналізу;
- Запропонувати результативний метод протидій аналізу криптосистем по стороннім каналам;

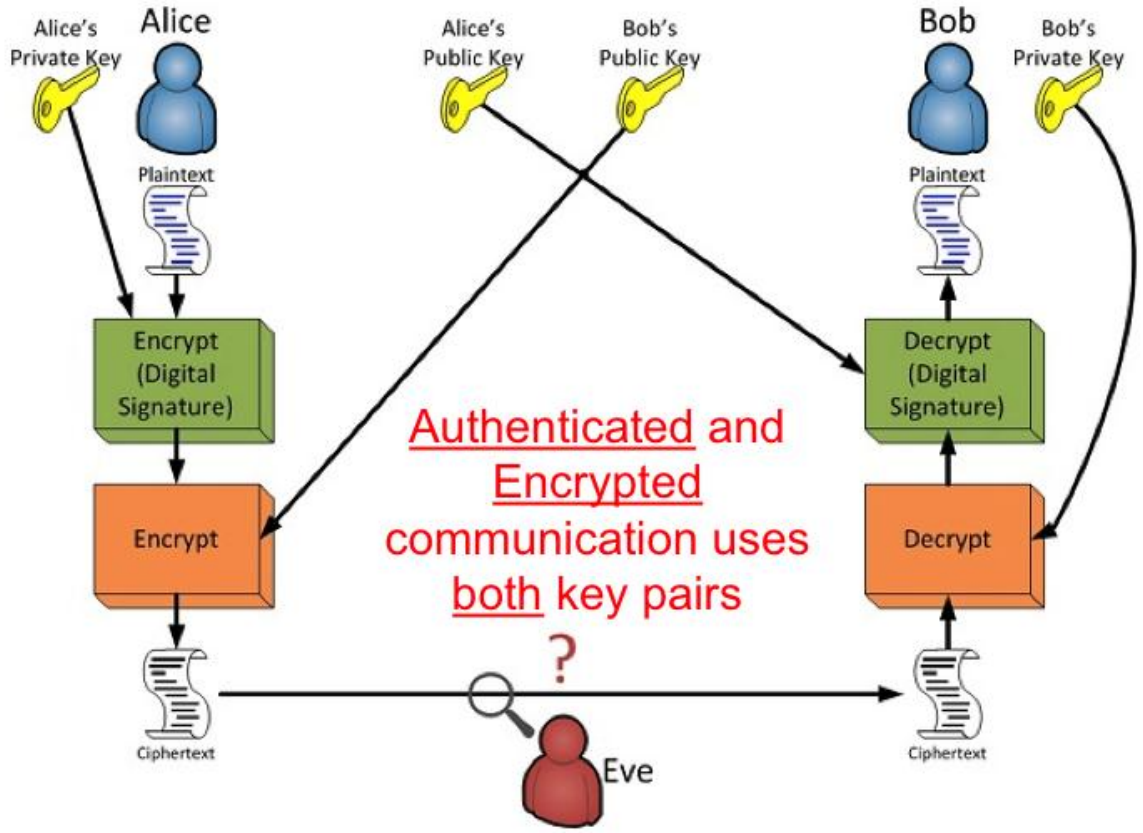
Сфера використання

1. Для підпису даних, для збереження їх цілісності.

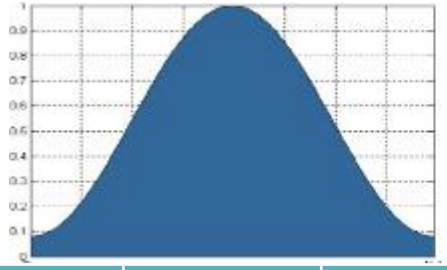


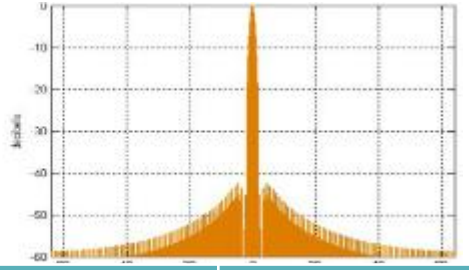
Сфера використання

2. Для збереження конфіденційності даних користувачів.



Огляд аналізу сигналів





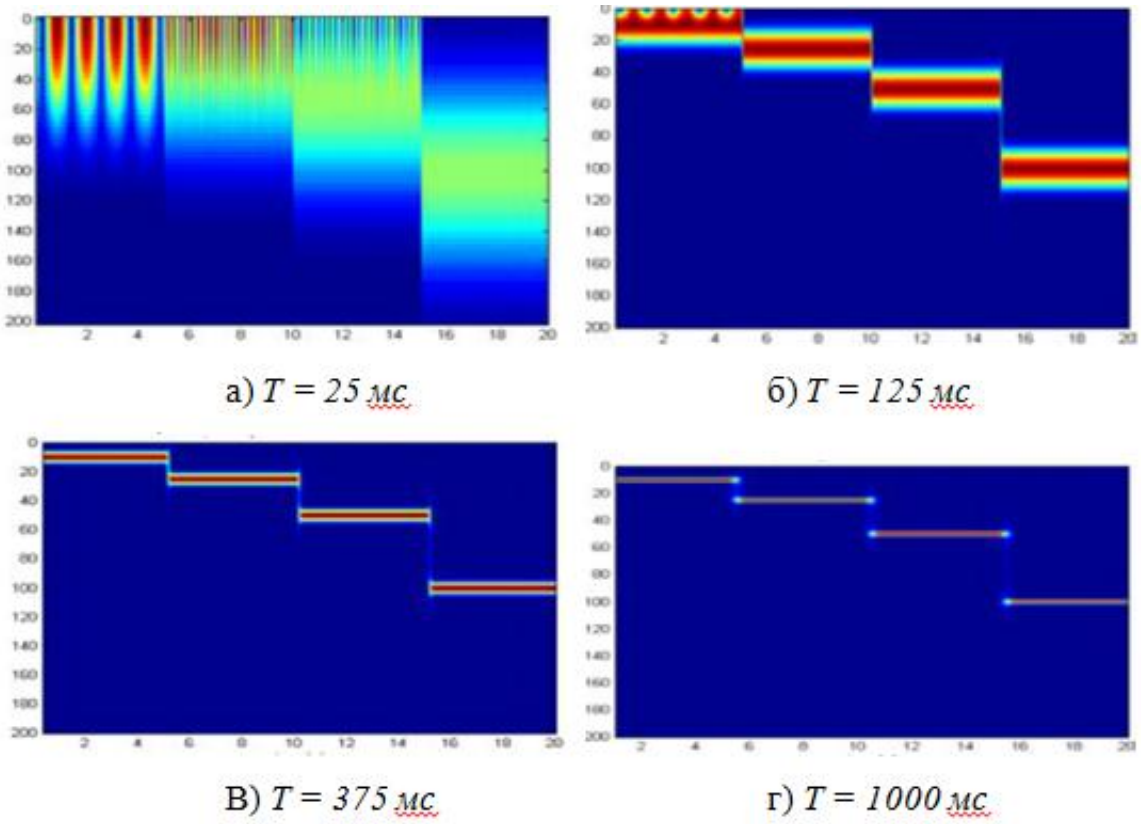
Обробка неперіодичного сигналу виконується віконним перетворенням Фур'є.

В аналізі використовується віконне перетворення Хеммінга, як компромісне по збереженню відношення сигнал/шуму та для точного виділення близьких по частоті спектральних компонент.

Функція вікна	Рівень бокових пелюсток, дБ	Швидкість затухання бокових пелюсток, дБ/октаву	Еквівалентна ширина частотної смуги бокових пелюсток, відліки	Погіршення відношення сигнал/шум порівняно з вхідним сигналом, дБ
Хеммінга	-43	-6	1.36	3.10
Ханна	-32	-18	1.50	3.18
Бартлетта	-27	-12	1.33	3.07
Блекмана (α = 0.16)	-58	-18	1.73	3.01
Кайзера (α = 3.0)	-69	-6	1.80	3.56
Кайзера (α = 3.5)	-82	-6	1.93	3.74
Прямокутне	-13	-6	1.00	3.92

Огляд аналізу сигналів

Ширина вікна при дослідженні буде варіюватись через принцип невизначеності.



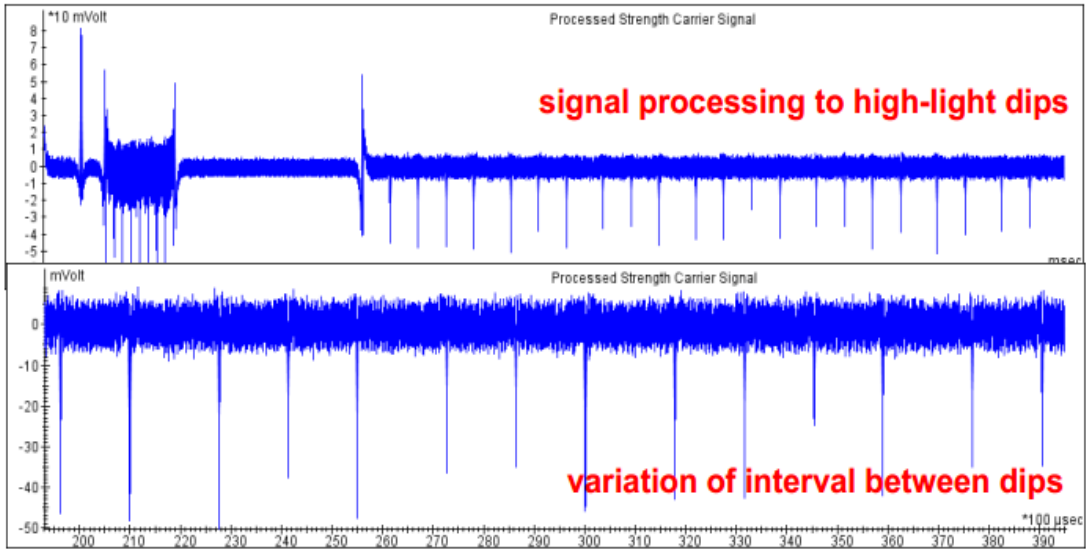
а) $T = 25$ мс

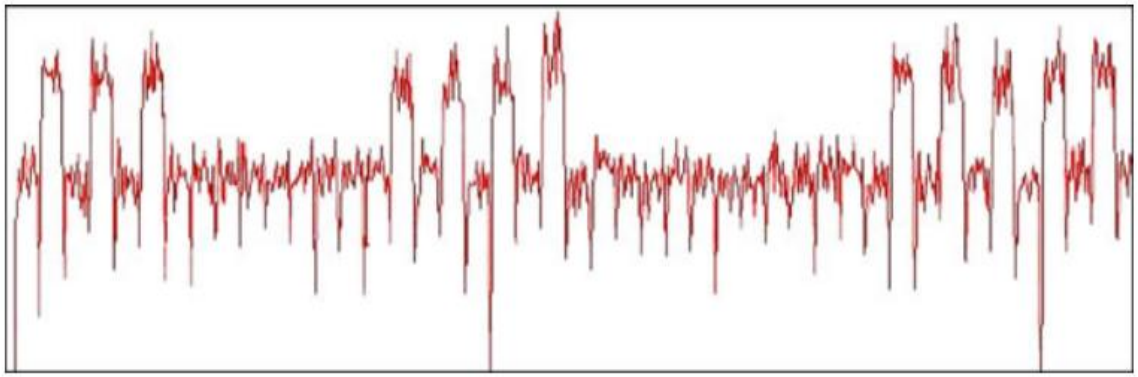
б) $T = 125$ мс

В) $T = 375$ мс

г) $T = 1000$ мс

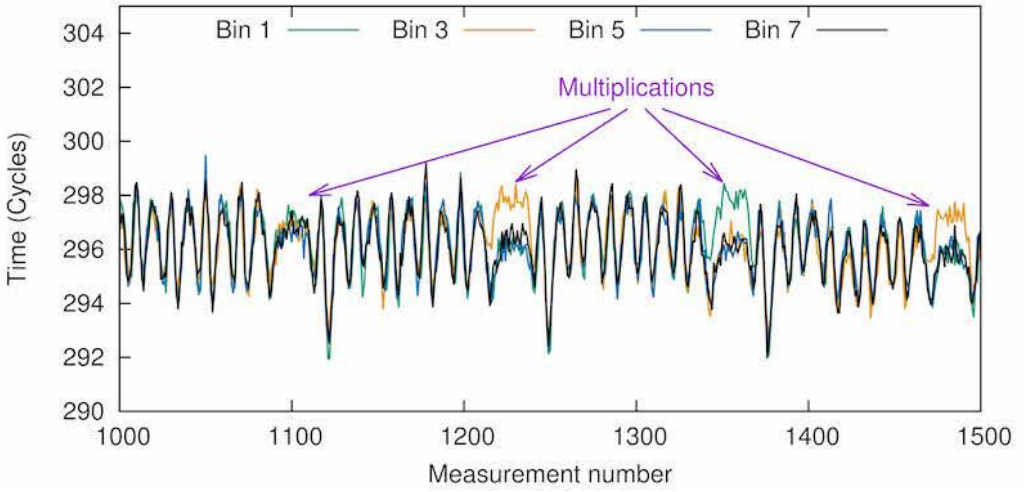
Огляд криптосистеми RSA

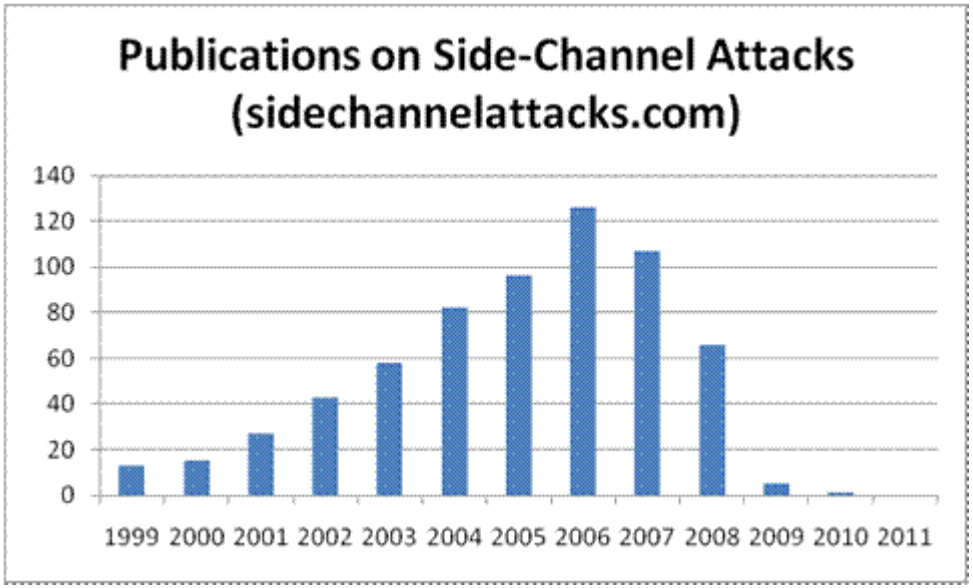




SCA

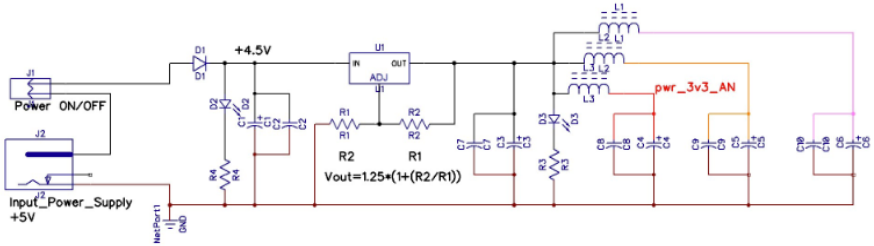
Цілю аналізу стають операції піднесення у степінь та множення, через їх залежність від вхідних даних та явна помітність на діаграмі сигналу. Також часто використовувана CRT для покращення швидкодії алгоритму, негативно впливає на сторонні канали видаючи багато інформації про виконувані операції, таким чином не рекомендується до використання алгоритму без прийнятних протидій до SCA.

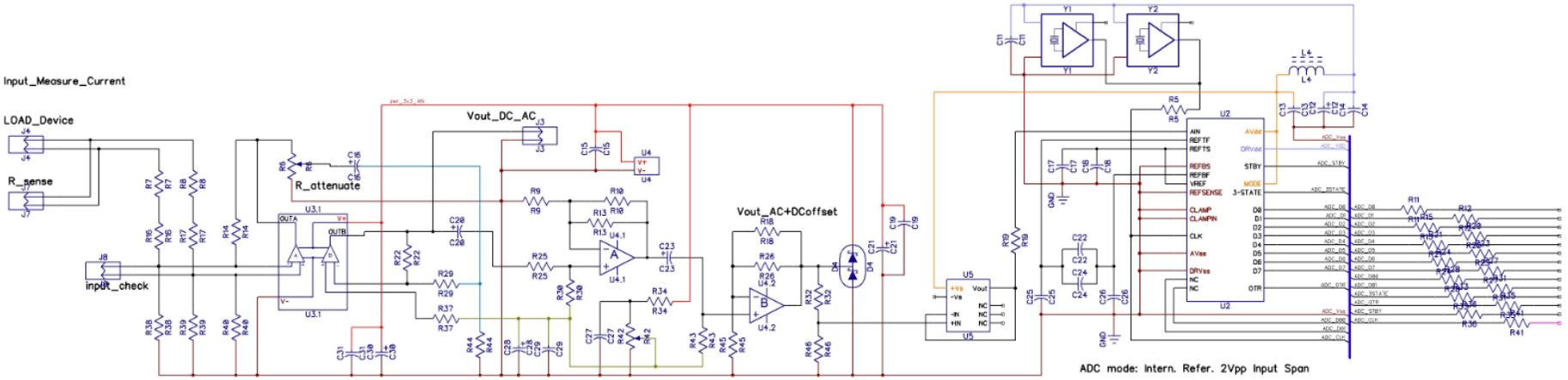




SCA

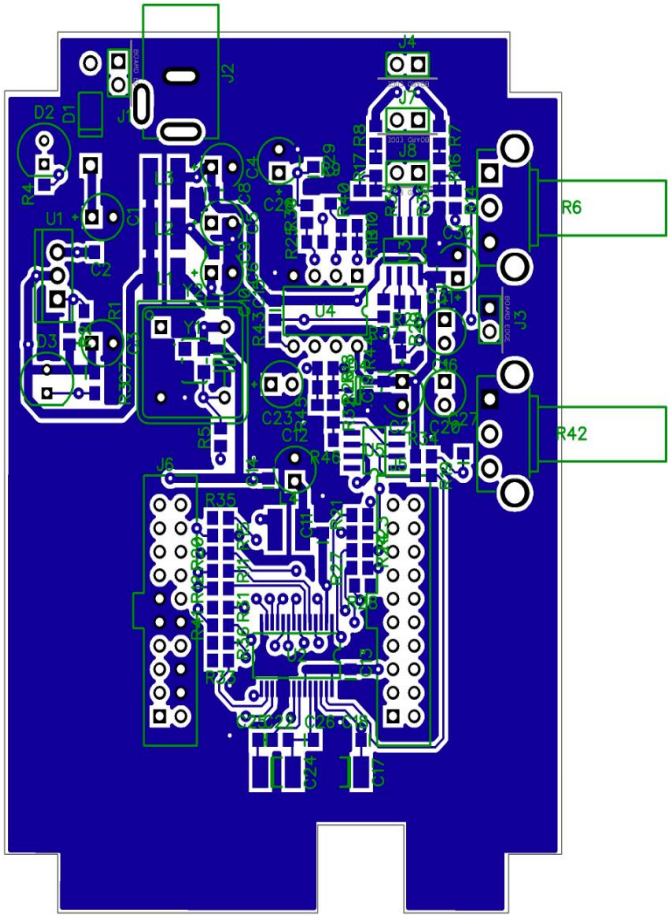
Збирання інформації.

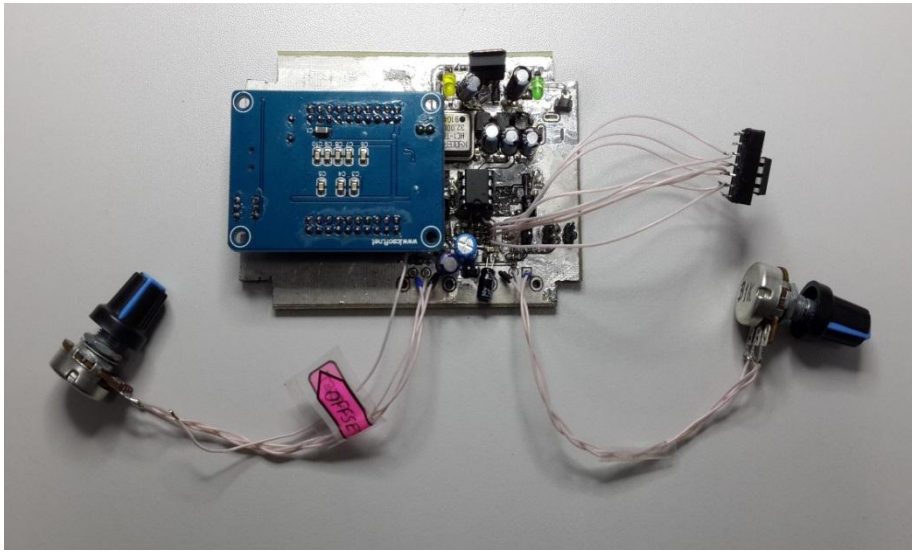




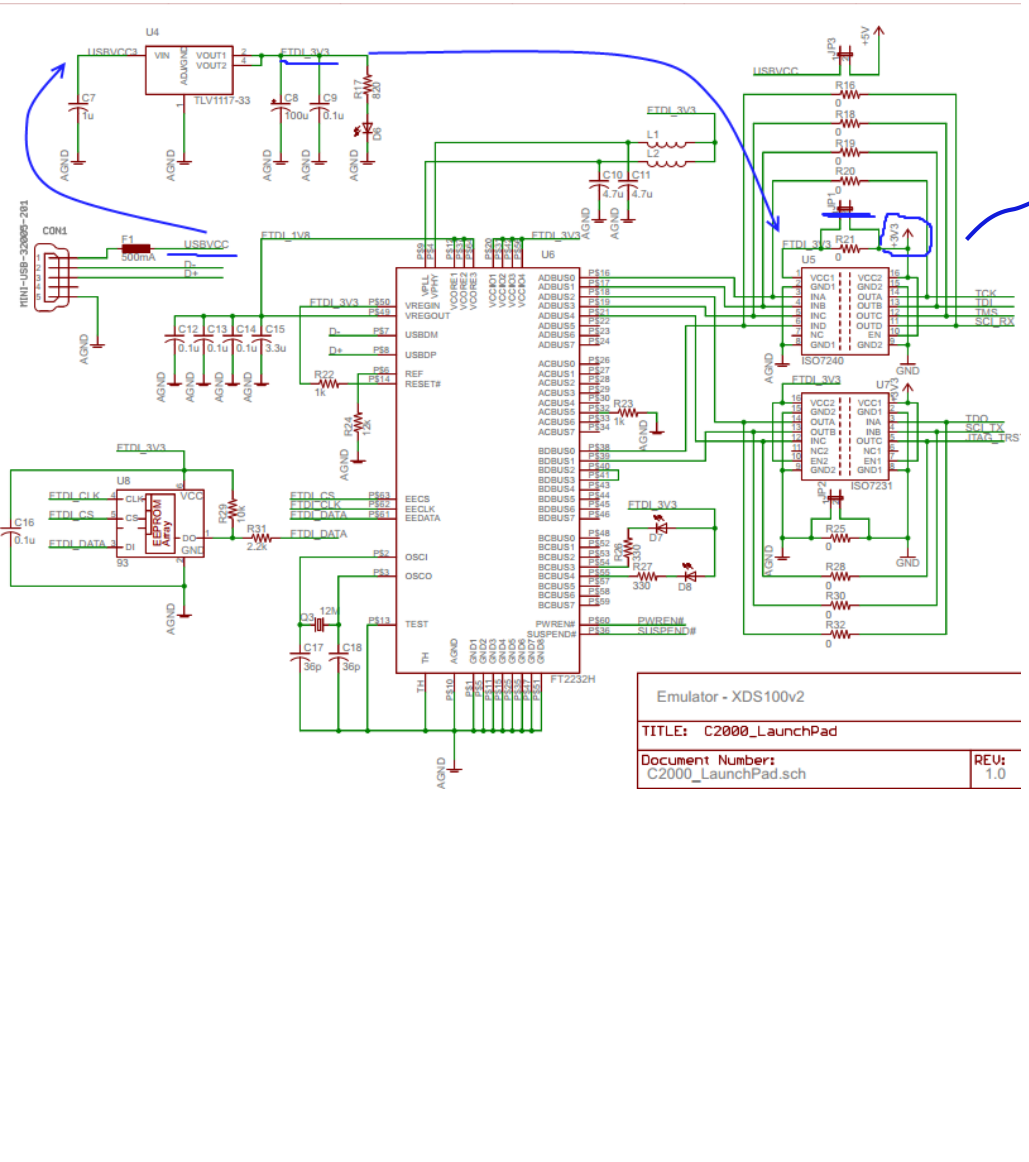
SCA

Збирання інформації.





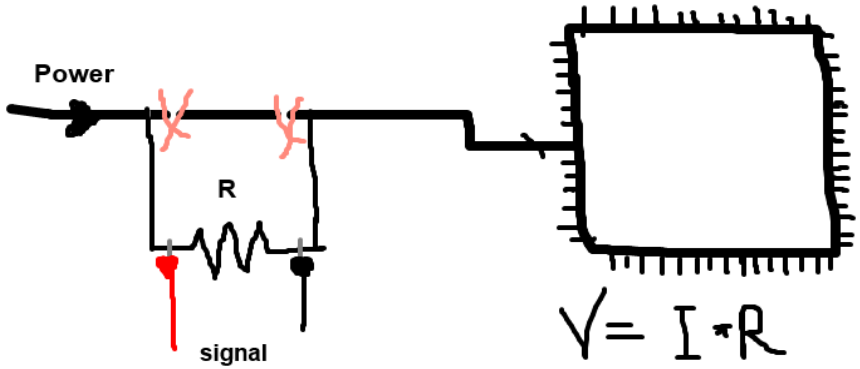
SCA

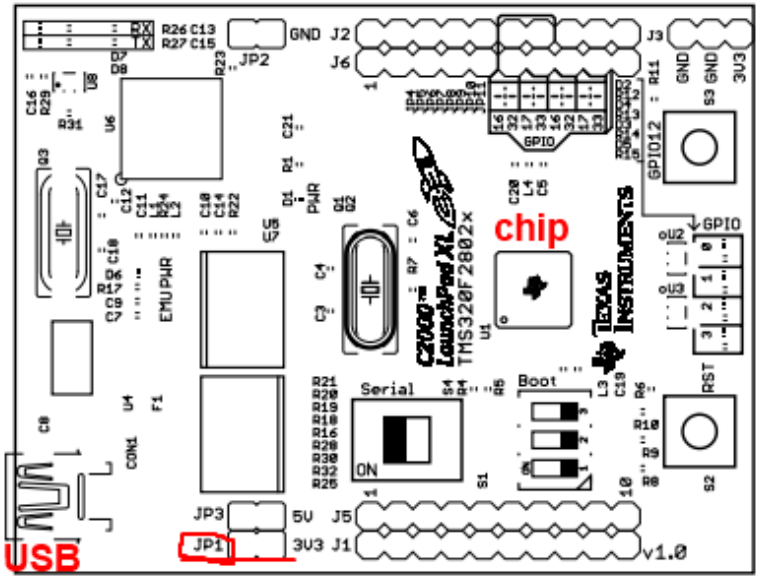


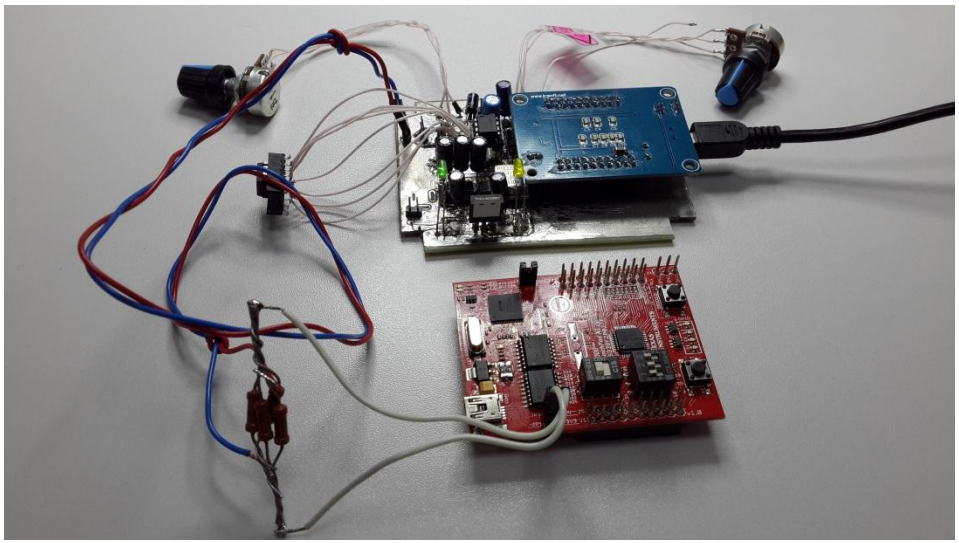
Пошук місця заміру споживання.

SCA

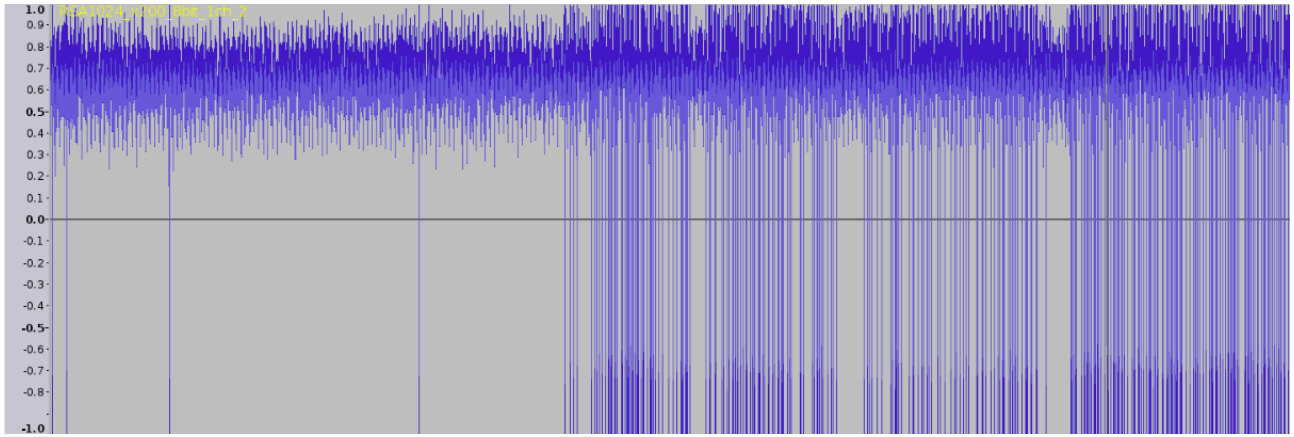
Збирання інформації.



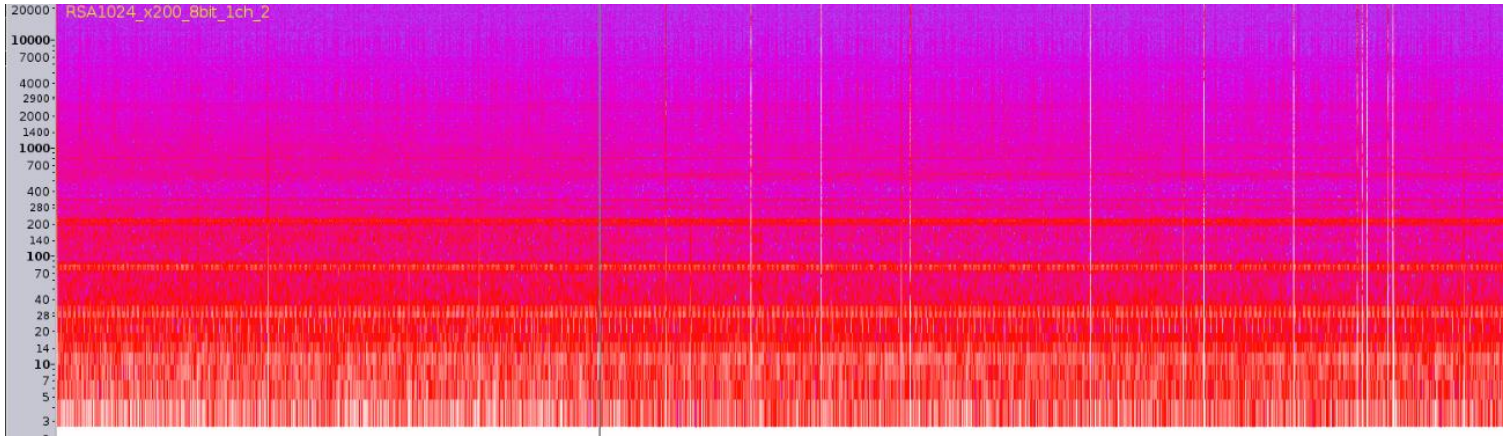




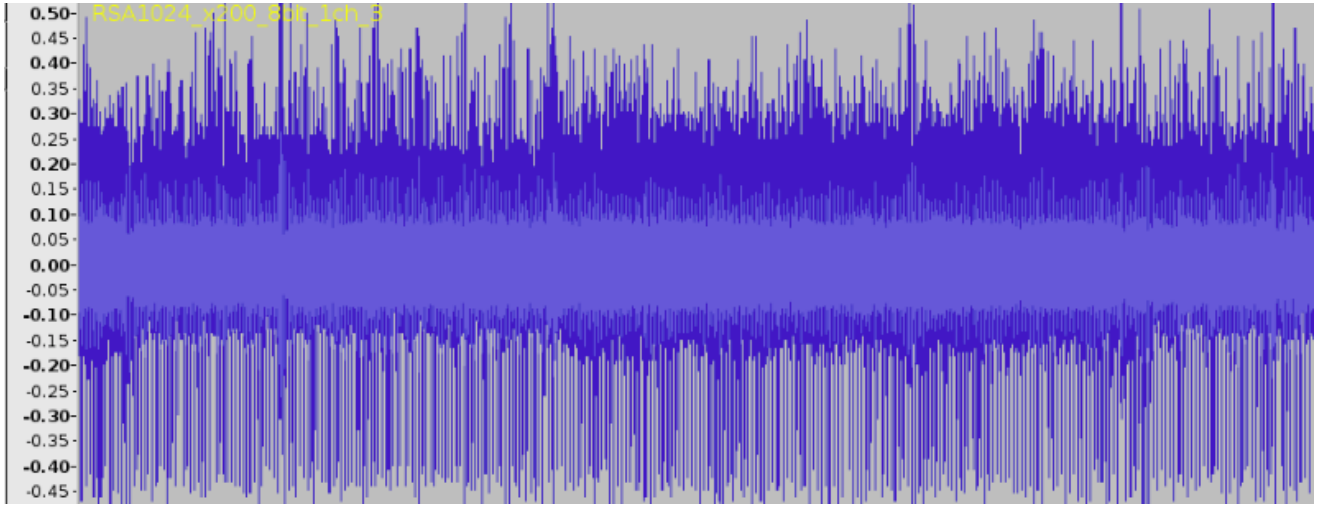
Дослідження сигналу



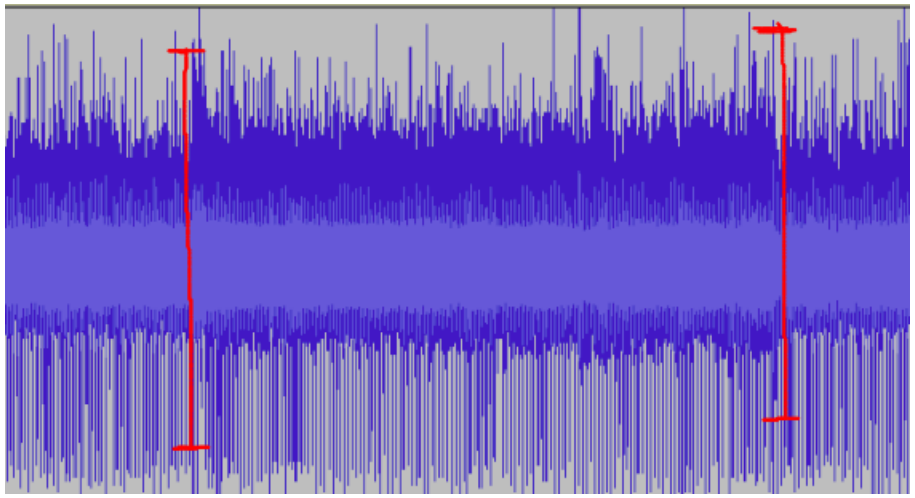
Вибір робочої точки



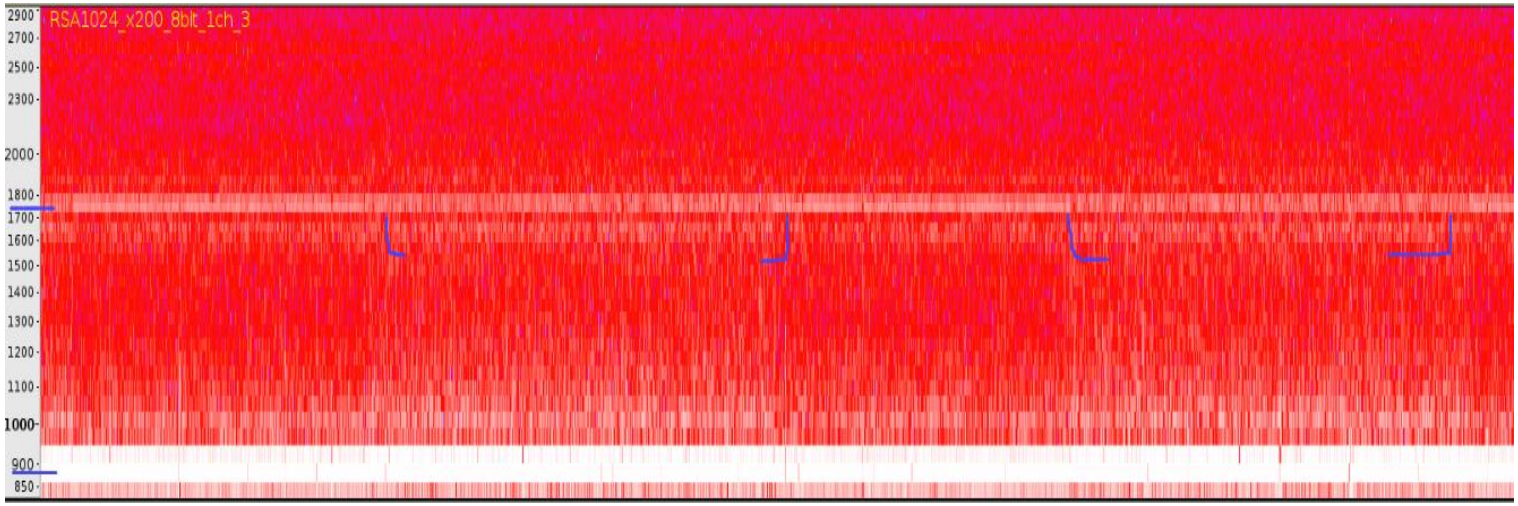
Дослідження сигналу



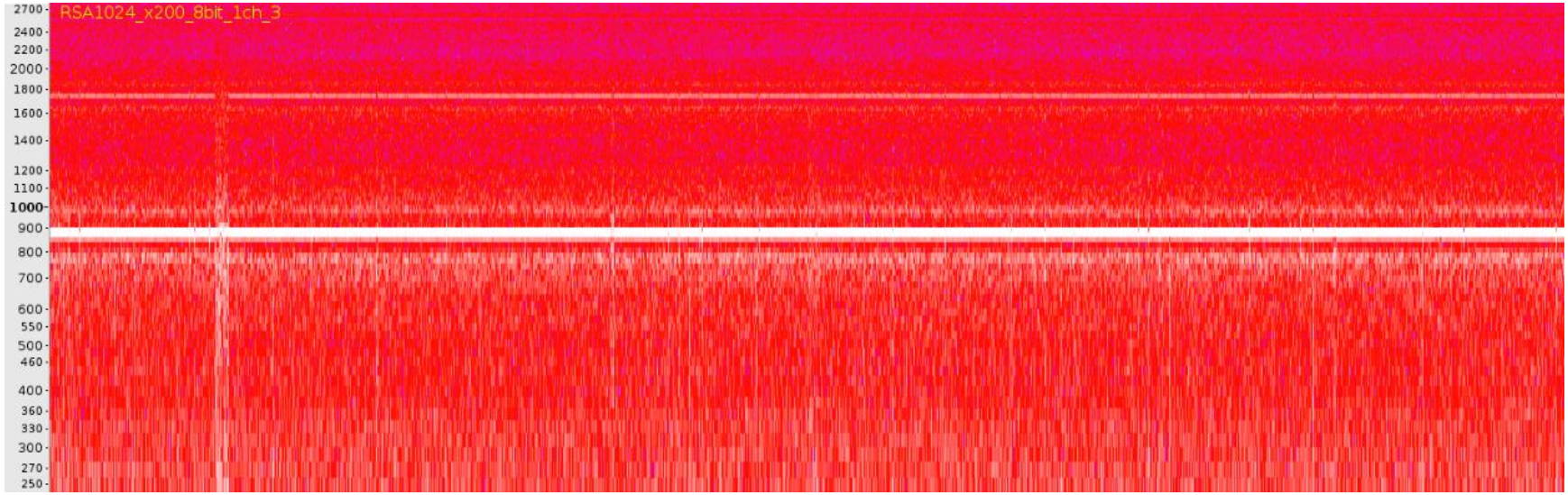
Виділення інформативних зон



Дослідження сигналу

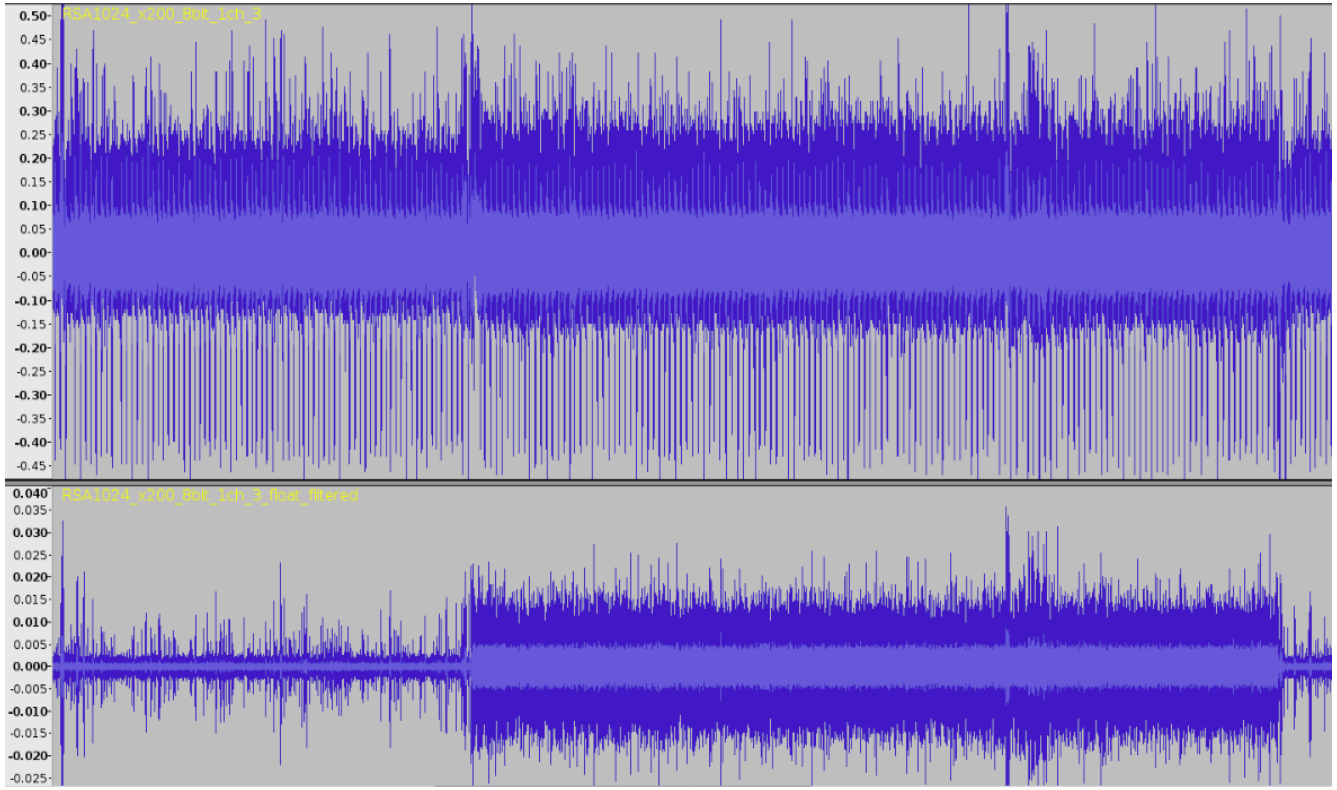


Локалізація частоти сигналу



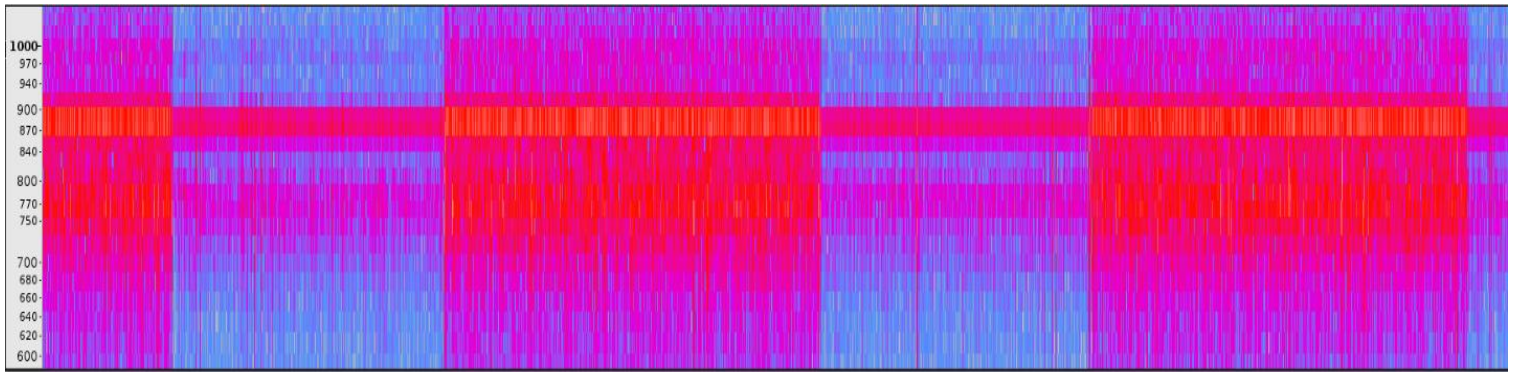
Дослідження сигналу

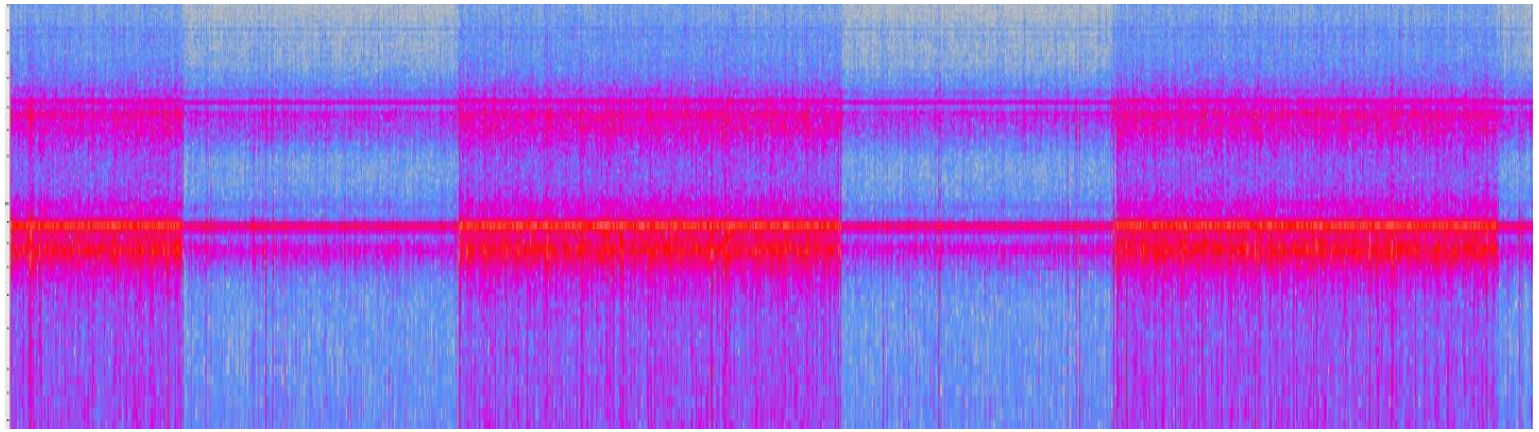
Фільтрація сигналу за обраними частотами.



Дослідження сигналу

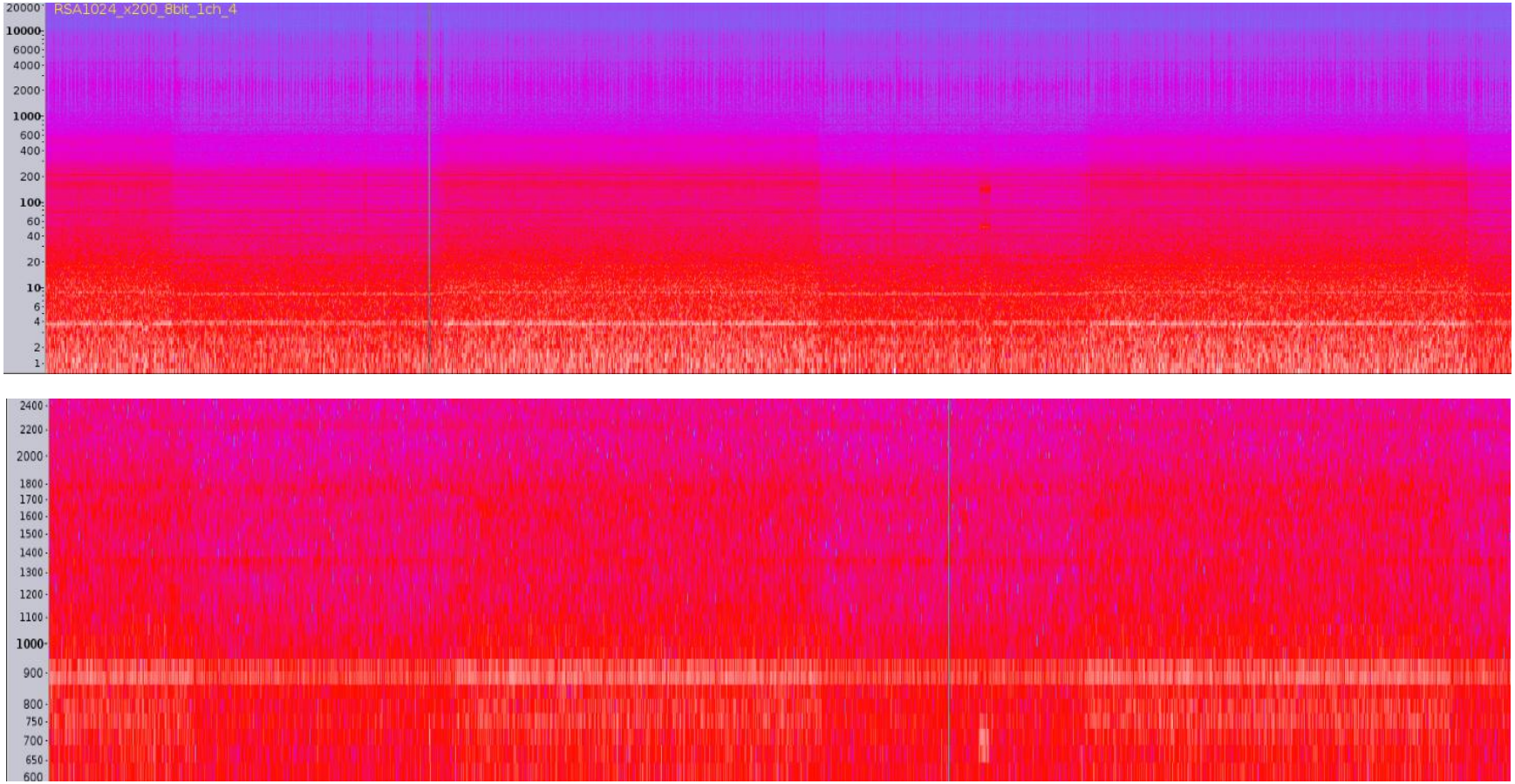
Спектр відфільтрованого сигналу.





Дослідження сигналу

Локалізація інформативних частот.



Висновки

- SCA – серйозна загроза надійності RSA алгоритму;
- Для попередження можливих атак, необхідно впроваджувати протидії SCA;
- Для кожної системи набір необхідних контрзаходів визначається вимогами до системи та особливістю її побудови;
- Одною з найбільш універсальних протидії є апаратне приховання, що застосовує архітектурні можливості системи;
- Реалізовуючи алгоритм треба завжди брати до увагу, як змінюється інформації, яку несе система, враховувати виконання яких інструкції може привести до витоку інформації;

Старт-ап проекту

- Проект важко комерціалізується, адже він не є універсальним рішенням, а тому може зацікавити лише як підхід до вирішення проблем зі сторонніми каналами, а не як готовий товар.
- На ринку наявна монополістична конкуренція;
- Існує декілька фірм-конкурентів, тому вихід на нього не буде легким.
- Проект є конкурентоспроможним лише завдяки своїй високій надійності.
- Для впровадження ринкової реалізації проекту слід обрати альтернативу, яка передбачає розробку програмного продукту, а потім якісну рекламу та PR, сконцентровану навколо позитивних характеристиках даного програмного продукту, таких як низька ціна, надійність, безпека і т.д.

Дякую за увагу!