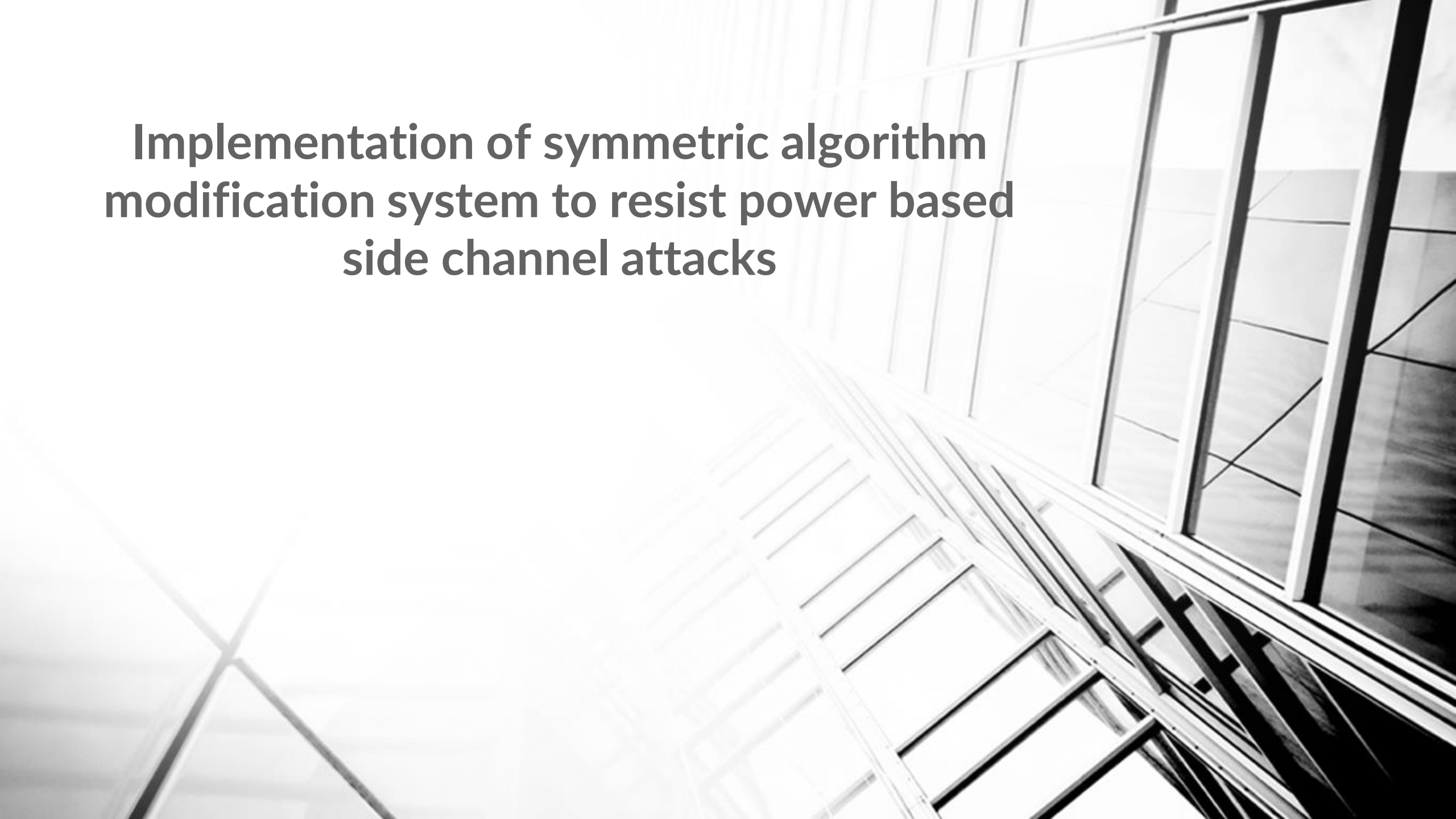
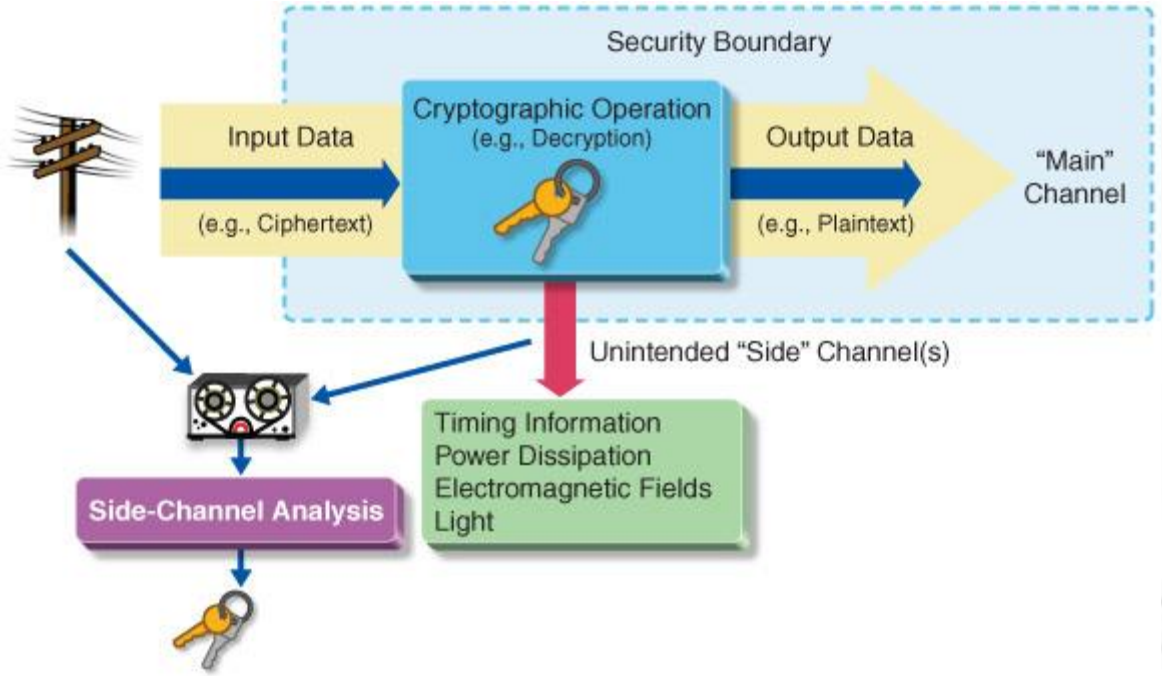
Implementation of symmetric algorithm modification system to resist power based side channel attacks



Do you know What is Side Channel attack ?

Side Channel Attack is ..

Any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms.



Side Channel Attack is .. (Cont..)

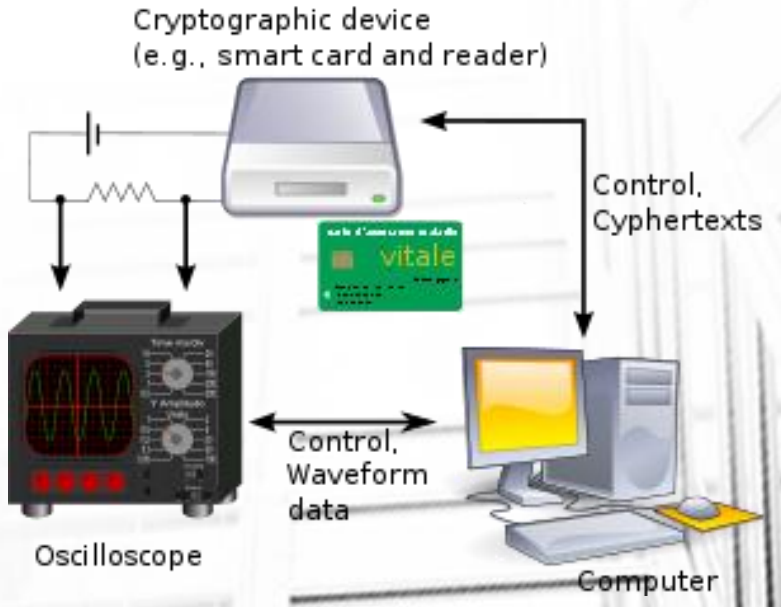
These attacks based on “Side Channel Information “. Side channel information is information that can be retrieved from the encryption device that is neither the plaintext to be encrypted nor the ciphertext resulting from the encryption process.

That Side Information can be ,

- Timing Information
- Electromagnetic Radiation
- Power consumption
- Thermal Radiation
- Acoustic Emanation

Why this Research Based On Power Consumption ?

- Power consumption analysis is one of the **most effective and powerful** methods.
- **Most frequently used method** to collect side-channel-information by attacker and intruders
- Power consumption analysis is also considered as one of the **most reliable side-channel-information sources**
- power consumption is the most cost effective when compared with other methods of information gathering



Up to Now..

- There are devices that are design to gather side-channel-information.
- Can analyze side channel information to perform an attack.
- Have the capability to derive the key through the attack.

Up to Now.. (Cont….)

- SASEBO (Side channel Attack Standard Evaluation Board)
- CHIP WHISPERER
- SAKURA-G FPGA

Problems Identified ..

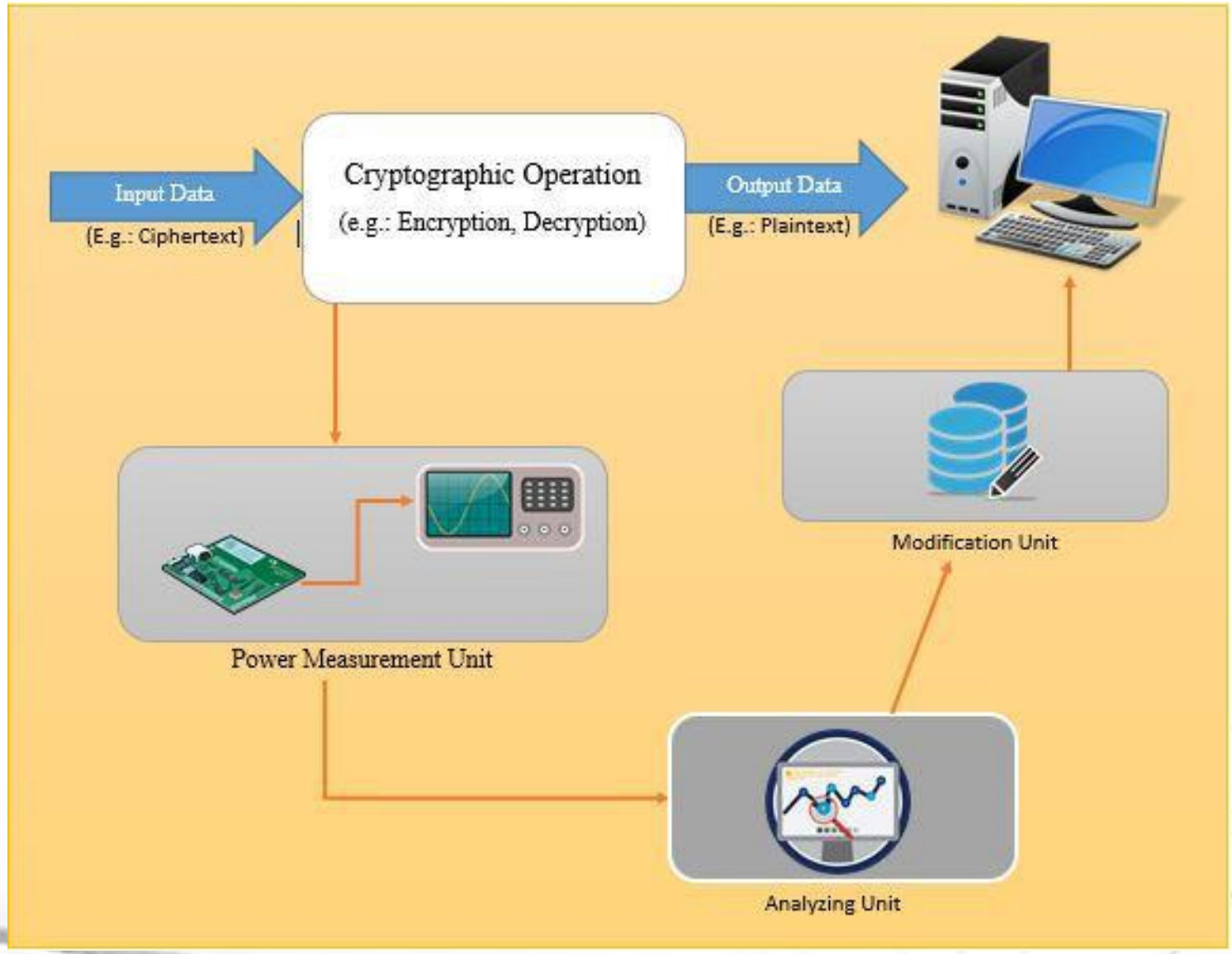
- There is no any product to find the vulnerable points in algorithm by analyzing power spike patterns.
- There is no process to patch it automatically without altering the algorithm in order to mitigate side channel attacks.

How we mitigate side channel patterns?

Solution

Adding “RANDOMNESS” to the algorithm

Overall Idea



Extracting power consumption measurements

- Implementing a device to extract power consumption information
- Based on Arduino and FPGA board.
- Implementing an algorithm to take power consumption information into digital format and input to PC.

Data classification, analysis and module training

- Classifying extracted data by selecting the subset of all available data in a linear manner procedure.
- Data Preparation
- Transforming preprocessed data into appropriate machine learning styles using techniques
- Training fluently to obtain the most accurate and reliable solution for the he performance of vulnerability
- Utilizing performance of the applied process

Automate Code embedding mechanism

- Adding suitable modification to analyze algorithms
- Uses machine learning techniques.
- Modification are done in the code level of the algorithm

Benefits

- Cost Effective
- Less complexity – can be use by any person who doesn’t have knowledge in cryptology
- Cryptographic algorithm can be strengthen against side channel attack.

Capturing the Market

- Free and open source at the initial stage
- Use social media to promote


THANK
YOU

Questions ?