Side Channel Power Analysis of SPARX Block Cipher

Mark Elkommos — supervised by Dr Elisabeth Oswald, Department of Computer Science

Side Channels and SPARX cipher

Side Channels

A side channel is information that is gained through execution of a cryptographic algorithm, by measuring its physical attributes.

Devices leak information about intermediate variables they process.

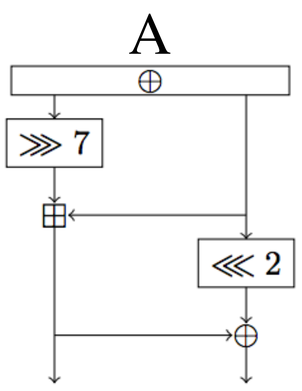
Power analysis involves using the power consumption of the device to derive secret information.

Differential power analysis uses knowledge of inputs and sub-key guesses to deduce the key.

SPARX Cipher

A Lightweight block cipher based on modular addition, rotations and XOR operations.

Based on the round function below.



Algorithm 1 SPARX encryption
Inputs plaintext $(x_0, ..., x_{w-1})$; key $(k_0, ..., k_{v-1})$
Output ciphertext $(y_0, ..., y_{w-1})$

Let $y_i \leftarrow x_i$ for all $i \in [0, ..., w-1]$
for all $s \in [0, n_s - 1]$ **do**
  for all $i \in [0, w-1]$ **do**
    for all $r \in [0, r_a - 1]$ **do**
      $y_i \leftarrow y_i \oplus k_r$
      $y_i \leftarrow A(y_i)$
    end for
    $(k_0, ..., k_{v-1}) \leftarrow K_v((k_0, ..., k_{v-1}))$
  end for
  $(y_0, ..., y_{w-1}) \leftarrow \lambda_w((y_0, ..., y_{w-1}))$
end for
Let $y_i \leftarrow y_i \oplus k_i$ for all $i \in [0, ..., w-1]$
return $(y_0, ..., y_{w-1})$

Progress and Todo

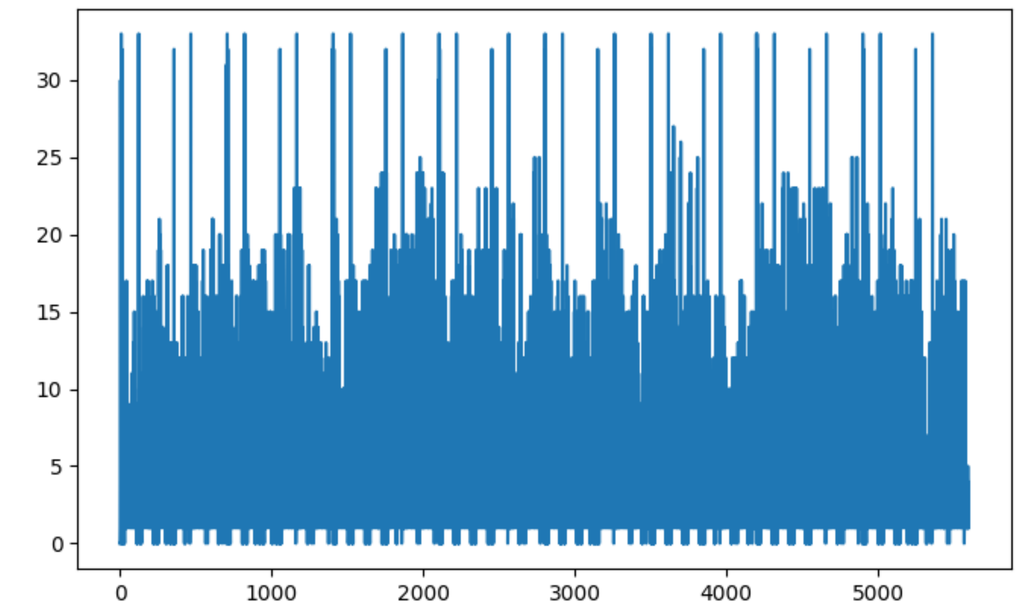
Project So Far

- Created ARM implementation of the SPARX cipher for the ARM cortex M0.
- Created power model simulation for the ARM assembly based on Hamming Weight and Hamming Distance metrics.
- Implemented two attacks against the simulation in C++ and Python.

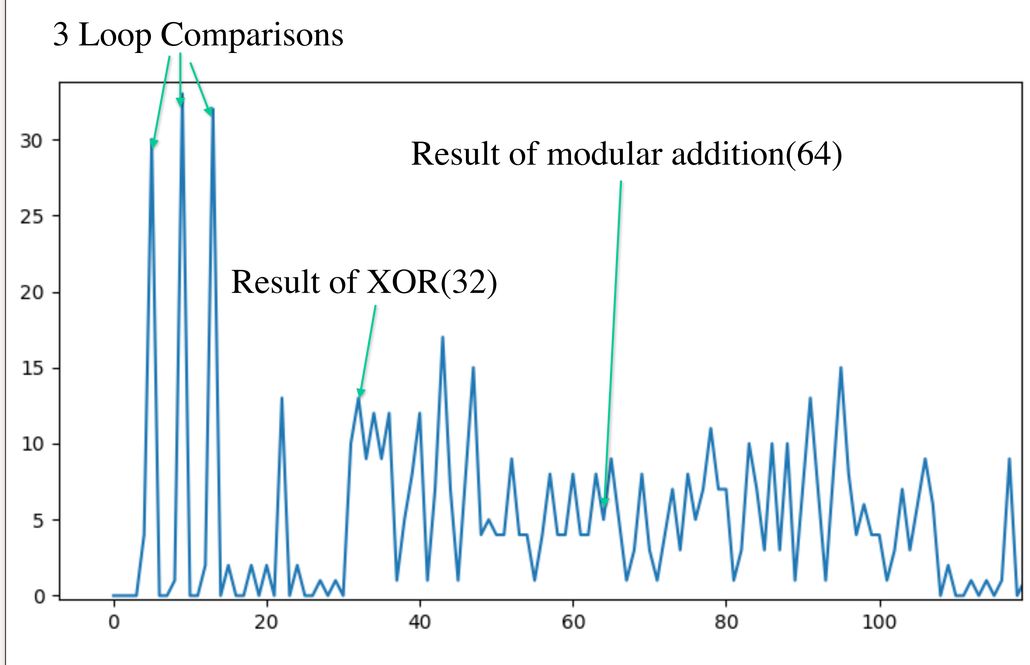
To do

- Test attacks against a more realistic simulator.
- Collect power traces from actual device using oscilloscope and apply attacks on the device
- Develop suitable countermeasures against the attacks.

Simulation Results



Trace of entire encryption



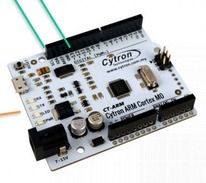
Zooming in on first round

Leakages of hamming weights and hamming distances used to deduce the key

Experimental Setup

Oscilloscope to collect power traces

Computer to send commands to device and analyse traces



ARM cortex M0 running SPARX encryption