Analysis of Correlation Power Analysis Attacks in Context to the Internet of Things

Andy Nguyen, Aaron Nguyen, Computer Engineering Program

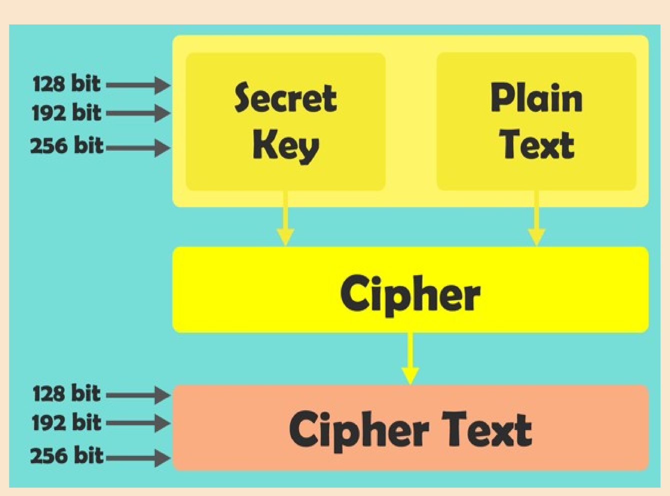
Adviser: Dr. Jaya Dofe

Background

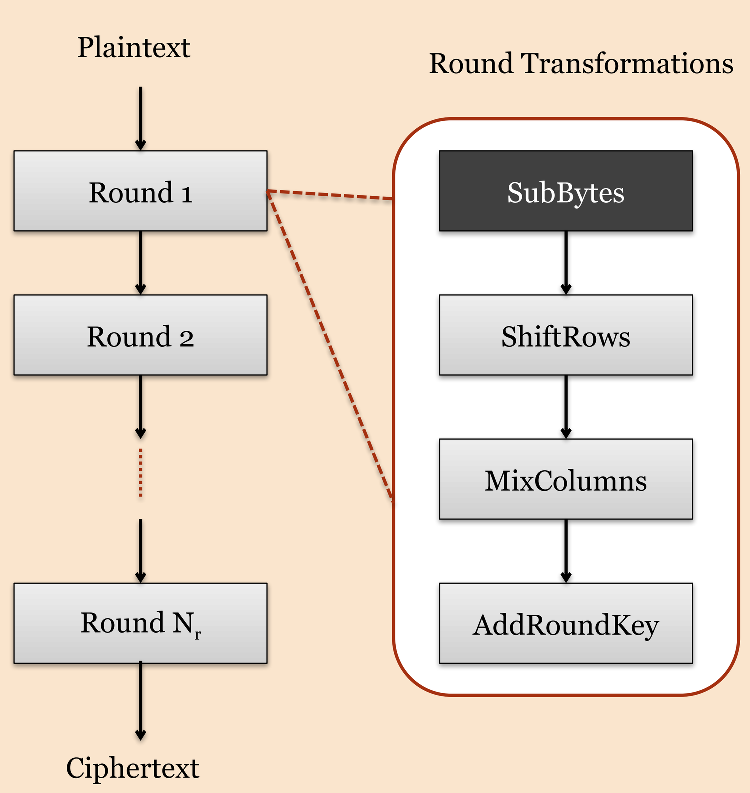
- Internet of Things (IoT) — emerging technology paradigm of various types of machines and devices able to communicate with each other via the Internet
- IoT bring extraordinary possibilities for improvements in various domains like smart cities and grids, healthcare, wearable devices, robotic systems and many other numerous systems
- Challenge to balance IoT device design to be cost effective and secure
- Advancing technology requires IoT security to be more capable of addressing growing malicious attacks
- Widespread availability of IoT devices, make them vulnerable to especially physical attacks, also known as side channel attacks, aimed at reading physical implementations
- Advanced Encryption Standard (AES) is used in industry and military encryption for secure communication and is used in our research as a case study subject

Advanced Encryption Standard

- AES is a symmetric block cipher that encrypt (encipher) and decrypt (decipher) information
- Although AES is a secure algorithm, the hardware implementation of AES can leak secret through the analysis of its hardware's physical properties called a side-channel attack.



AES Encryption



Encryption Structure of AES Algorithm

Scope of the Work

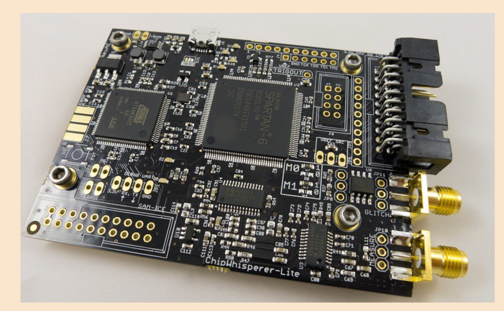
- Using side-channel technology, namely NewAE ChipWhisperer, simulation of a real-world situation to replicate an actual attack
- Analysis of AES baseline design against power analysis attack
- Investigation of a lightweight masking countermeasure to counteract the power-based side-channel analysis
- Such countermeasures are crucial for preventing harmful attacks in the advancing world we live in today

Experimental Setup

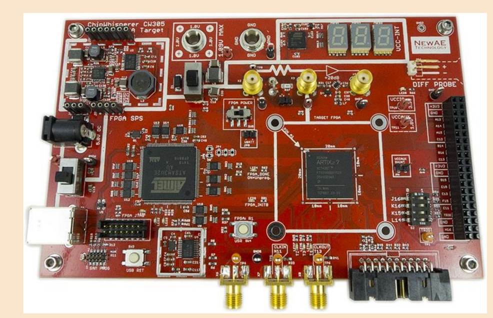
Capture Boards and Target Board

- Side-channel Attacks are performed using the CW1200 and the CWLITE capture boards
- Target simulation is performed using the CW305
- The CW305 can implement countermeasure defenses using hardware besides software by using an FPGA

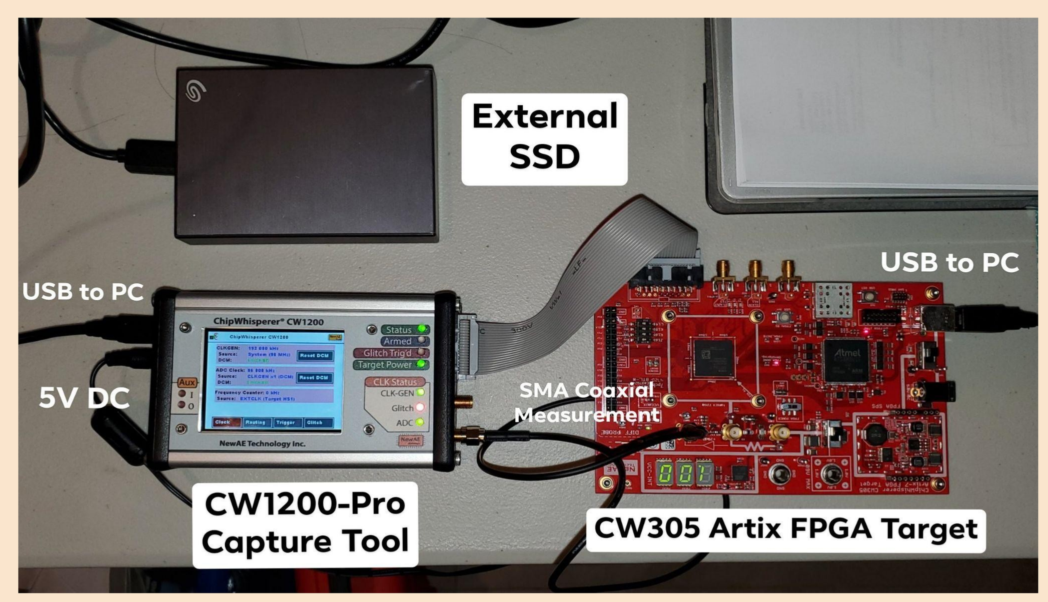
CW1200



CWLite



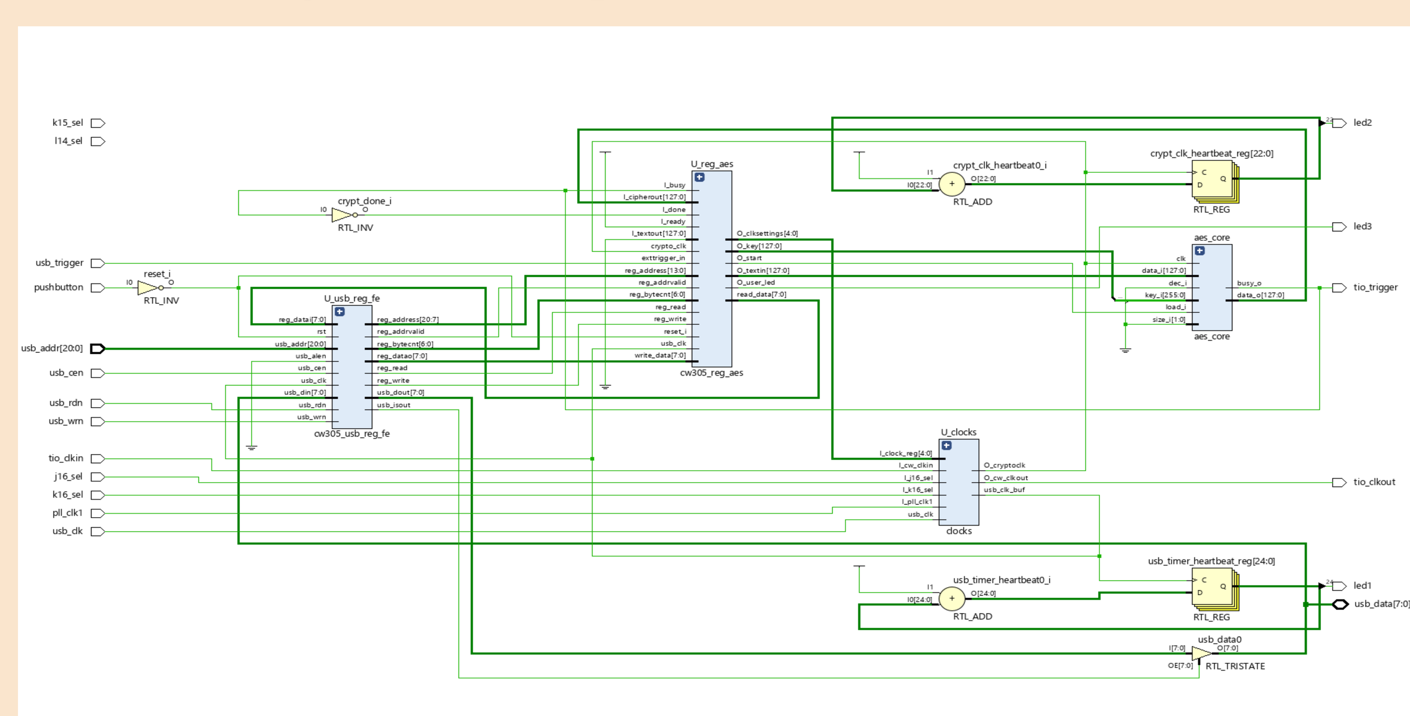
CW305



Complete Experimental Setup

Jupyter and Vivado

- The boards are programmed using Jupyter and bitstreams are created using the Vivado platform



RTL Schematic of AES

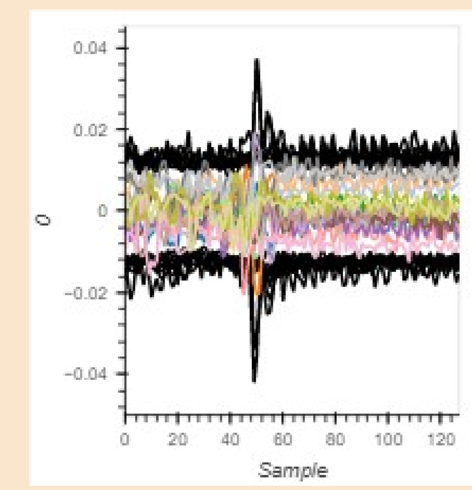
Leakage Models

- There are several points in the AES operation where leaked data can be exploited
- Chipwhisperer provides 15 CPA leakage models which can be used to derive the secret key from AES implementations
- 50k power traces from a standard hardware AES implementation are captured and then analyzed using the 15 leakage models

Results

Attack Information

- The time each leakage model took to analyze the 50k power traces and how many keys were retrieved were recorded
- Last_state_diff was the most effective leakage model for this hardware AES implementation, being the only one to derive the key in 50k power traces
- Last_state_diff attacks the hamming weight between round 9 and round 10 of the AES operations



Power vs Time of 50k Traces

Model #	Leakage Models	Keys Retreived	Time Taken (sec)
1	after_key_mix	0	1725.566
2	inverse_sbox_output	0	1756.588
3	last_round_state	2	1777.565
4	last_round_state_diff	16	2217.719
5	last_round_state_diff_alternate	4	2235.516
6	mix_columns_output	0	3916.158
7	plaintext_key_xor	0	1746.129
8	round_1_2_state_diff_key_mix	4	14130.898
9	round_1_2_state_diff_sbox	1	14614.175
10	round_1_2_state_diff_text	3	4526.853
11	sbox_in_out_diff	0	1873.616
12	sbox_input_successive	0	1839.024
13	sbox_output	1	1814.954
14	sbox_output_successive	0	1891.839
15	shift_rows_output	0	3070.302

Analysis of 15 Leakage Models for 50k Traces

Finished traces 49975 to 50000

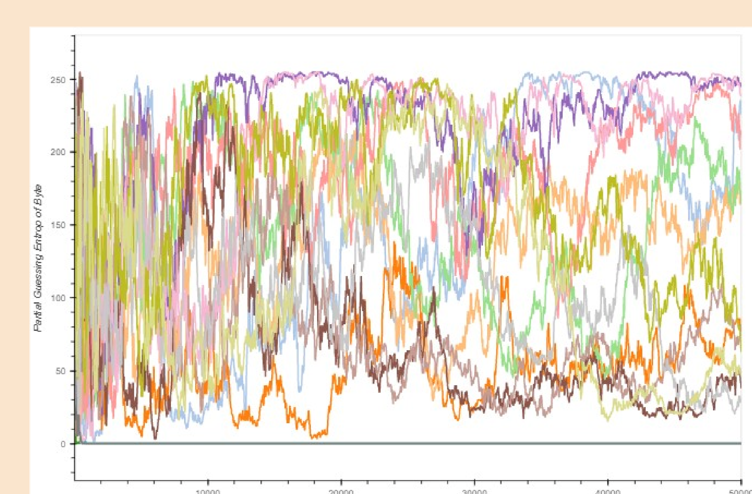
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PGE=	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	D0 0.174	14 0.217	F9 0.215	A8 0.185	C9 0.190	EE 0.204	25 0.204	89 0.186	E1 0.150	3F 0.207	0C 0.216	C8 0.187	B6 0.193	63 0.192	0C 0.186	A6 0.198
1	7C 0.042	B5 0.020	D1 0.020	34 0.020	B6 0.047	40 0.021	18 0.020	00 0.019	FA 0.036	CC 0.020	31 0.019	F5 0.019	C9 0.050	CD 0.019	B4 0.021	85 0.019
2	17 0.037	29 0.019	40 0.020	64 0.018	22 0.037	35 0.018	86 0.018	D2 0.017	A1 0.032	80 0.020	6C 0.019	1C 0.018	8E 0.039	FF 0.018	90 0.018	A3 0.019
3	AE 0.033	F0 0.018	4F 0.018	8F 0.017	F4 0.036	4E 0.018	0A 0.017	1E 0.017	33 0.029	55 0.018	1E 0.017	D3 0.017	DC 0.037	15 0.018	08 0.017	8E 0.017
4	8D 0.031	95 0.018	EA 0.018	26 0.017	4C 0.035	D3 0.017	94 0.016	9D 0.017	2A 0.027	4D 0.017	83 0.017	CE 0.017	33 0.037	70 0.018	02 0.017	5A 0.017

Time for Model 4 Attack: 2217.718965768814

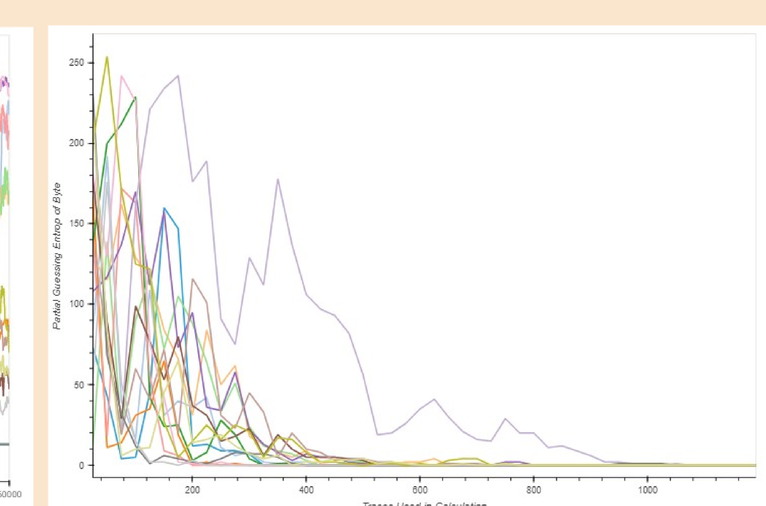
Last_state_diff Leakage Model

Partial Guessing Entropy Comparison

- In PGE vs Traces graph, PGE of 0 indicates the key is correctly retrieved
- A comparison is shown between unsuccessful key retrieval and a successful key retrieval



PGE vs Traces Graph (Key Not Found)



PGE vs Traces Graph (Key Found)

Summary

- Last_state_diff leakage model retrieving the secret key successfully for the given hardware implementation does not mean it will be successful for other hardware implementations.
- Same with the other leakage models, some that were not successful in retrieving the secret key may find success in retrieving the key from other hardware implementations
- Further testing will be done on other hardware AES implementations once we fully port to the Chipwhisperer environment