DALHOUSIE UNIVERSITY
FACULTY OF ENGINEERING

LINUX SoC HARDWARE SECURITY INVESTIGATION

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
GROUP 15 - ARIA MURRAY, CHARLEMAGNE TREMBLAY, EMRAN BILLAH, JEFF WESTWOOD

NewAE Technology

1. INTRODUCTION

When a computer processes data or executes instructions, its physical elements exhibit minor variations in power consumption, according to the data being processed or instruction being executed. For example, numbers with higher hamming weight (more "1" bits in binary representation) may require more power to process. This information, which is "leaked" through the device's power signal, can be used to recover data pertaining to the device's operations. Specifically, it is possible to recover a device's secret cryptographic key from power signals traced over the periods during which the device encrypts using the key. This technique - a type of side channel attack - is known as Side Channel Power Analysis (SCPA) [1]. The goal of this project was to apply SCPA to the LinkIt Smart 7688 System on Chip.

2. DESIGN PROCESS

Fig. 1: LinkIt Smart 7688 [2]

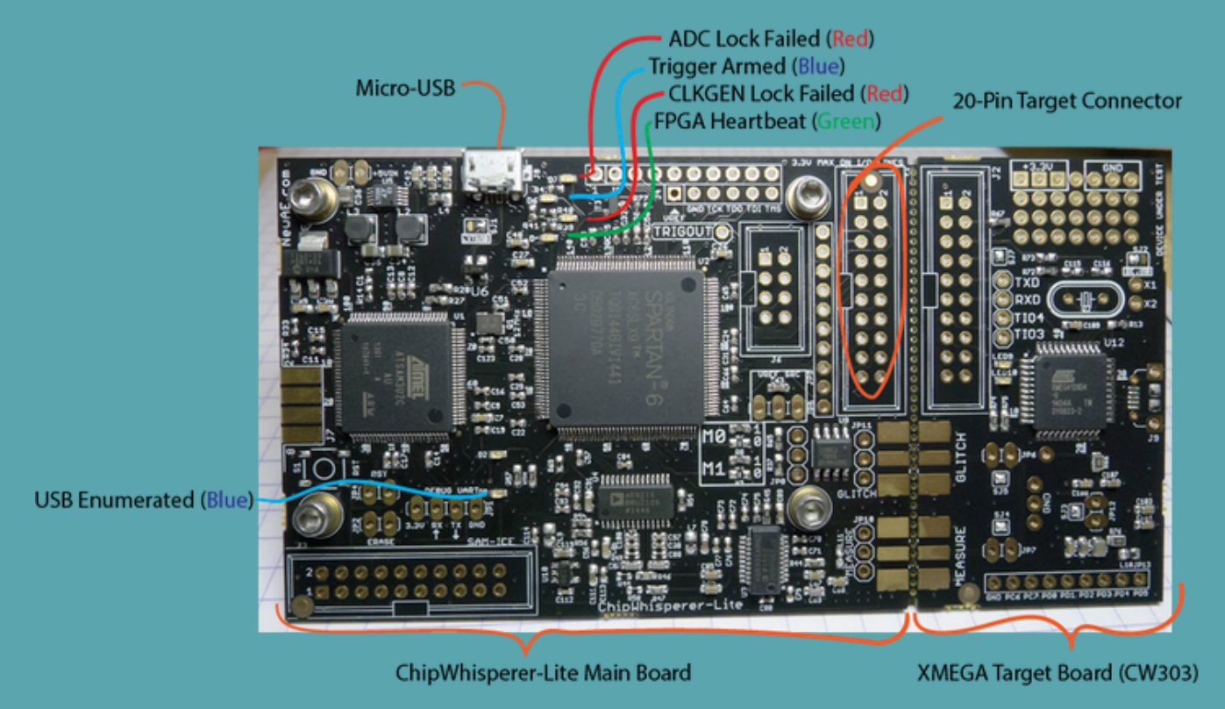


Fig. 2 : ChipWhisperer [3]

In order to prepare the Linkit target for SCPA attack, it was necessary to:

- Prepare the SDK (Software Development Kit) and development environment
- Enable userspace access to the hardware accelerator
- Reduce the system clock speed to accommodate the ChipWhiperer sampling rate

To enable the ChipWhisperer to be used with a new target, it required:

- Setup of the ChipWhisperer environment
- Testing and validation with provided XMega target board
- Adaptation for use with LinkIt

3. DESIGN DETAILS

SOFTWARE SETUP

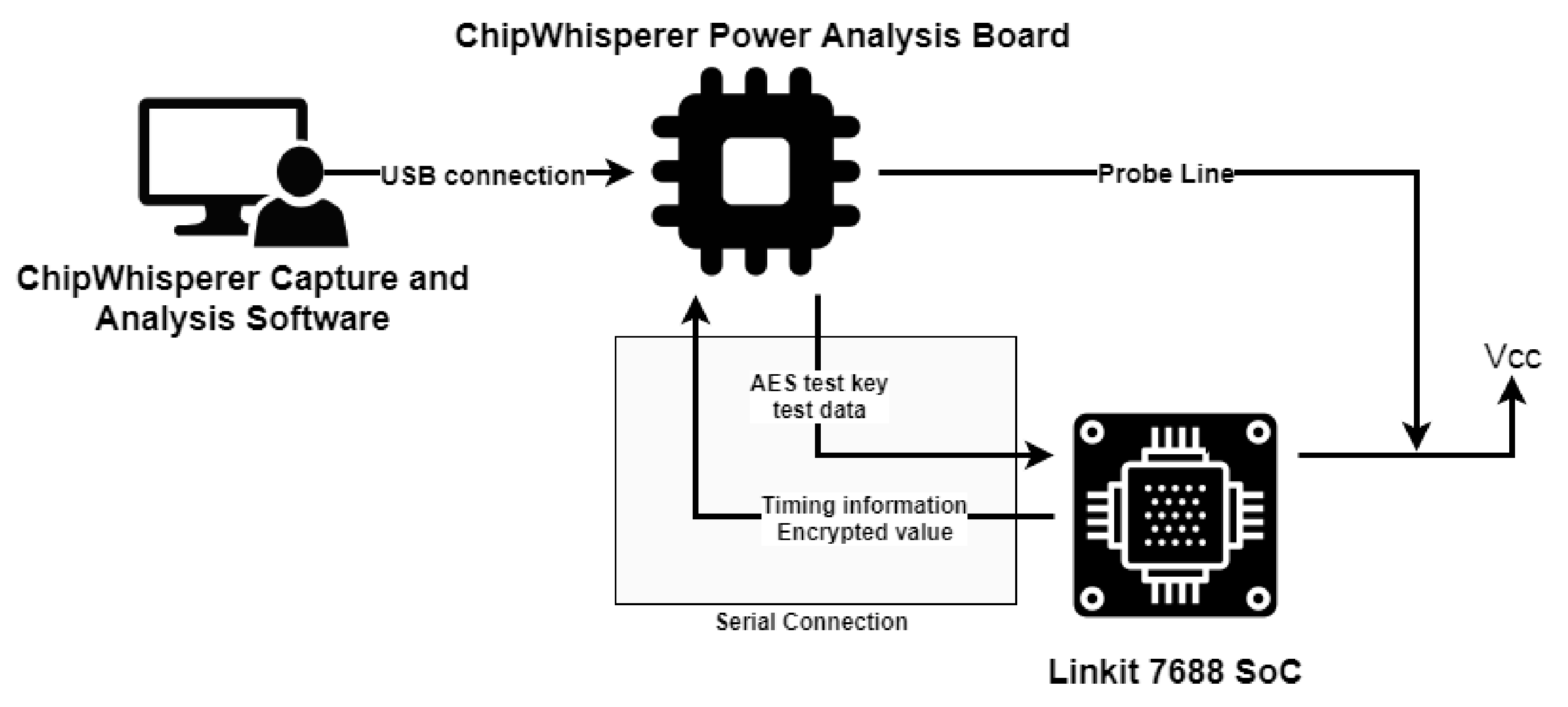


Fig. 3: Overall software setup

The LinkIt Smart 7688:

- To enable userspace access of the hardware accelerator, a third-party crypto driver (mt7628-aes [4]) was installed to route all crypto operations through the hardware accelerator, allowing it to be directly targeted by the power analysis attack.
- This required the use of a newer, unofficial firmware, based on the current version of OpenWRT.
- The LinkIt's base clock speed, being higher than the ChipWhisperer's sampling rate, needed to be reduced using the LinkIt's configuration registers. This lower clock speed required the OpenWRT Watchdog to be disabled.
- The MRAA library [5] was installed on the LinkIt device, to simplify serial communication and control the GPIO 'Trigger' pin.
- To enable a Power Analysis attack, special encryption software is required for the LinkIt to accept a known key from the ChipWhisperer and perform an encryption operation using the key, while maintaining timing information for the ChipWhisperer.

The ChipWhisperer Power Analysis Board:

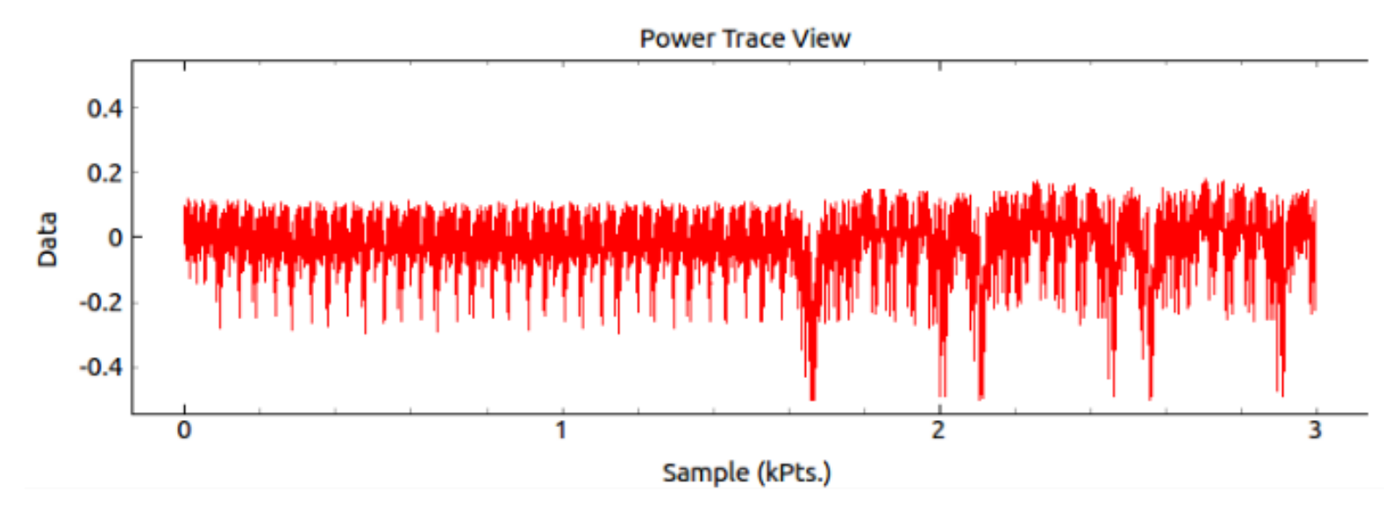
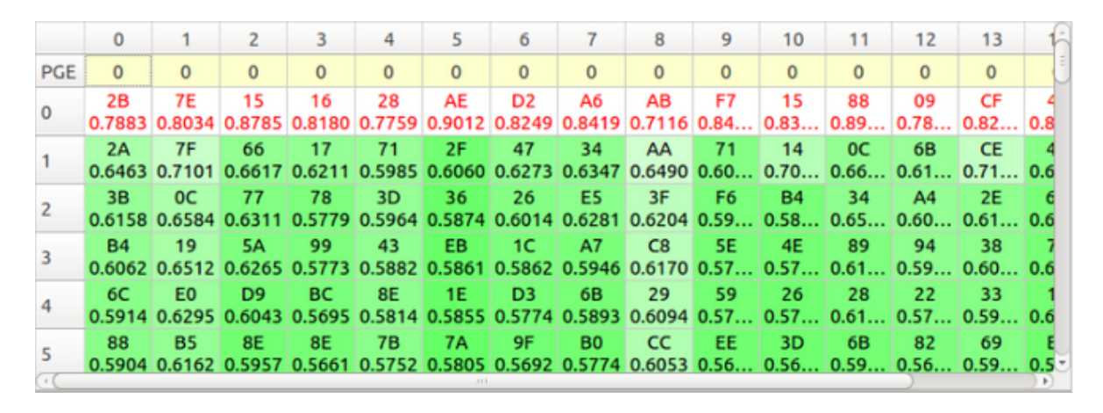


Fig. 4: CW Power Trace Capture

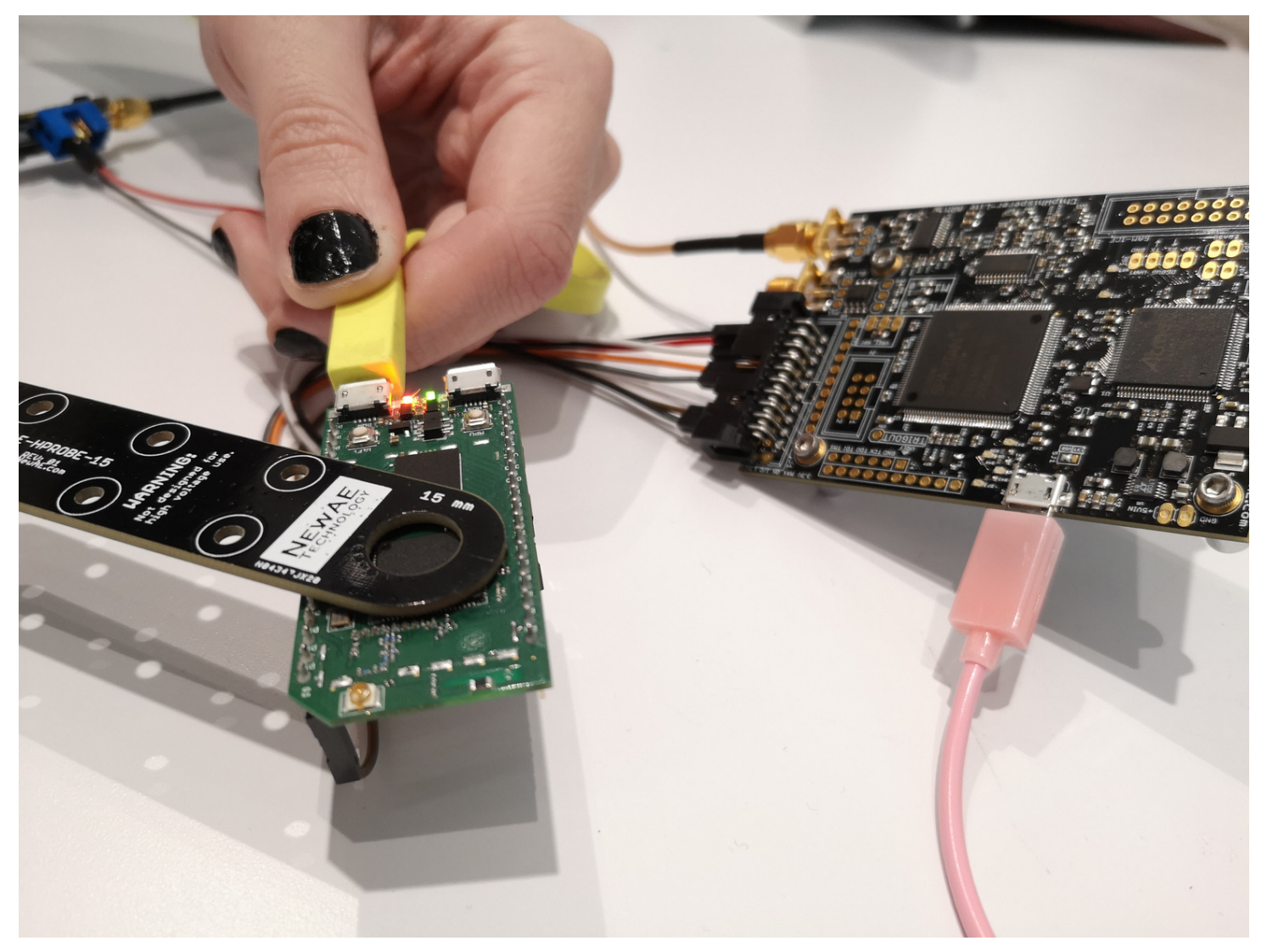


	0	1	2	3	4	5	6	7	8	9	10	11	12	13	1
PGE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
0	2B 0.7883	7E 0.8034	15 0.8785	16 0.8180	28 0.7759	AE 0.9012	D2 0.8249	A6 0.8419	AB 0.7116	F7 0.84...	15 0.83...	88 0.89...	09 0.78...	CF 0.82...	4 0.8
1	2A 0.6463	7F 0.7101	66 0.6617	17 0.6211	71 0.5985	2F 0.6060	47 0.6273	34 0.6347	AA 0.6490	71 0.60...	14 0.70...	0C 0.66...	6B 0.61...	CE 0.71...	4 0.6
2	3B 0.6158	0C 0.6584	77 0.6311	78 0.5779	3D 0.5964	36 0.5874	26 0.6014	E5 0.6281	3F 0.6204	F6 0.59...	B4 0.58...	34 0.65...	A4 0.60...	2E 0.61...	6 0.6
3	B4 0.6062	19 0.6512	5A 0.6265	99 0.5773	43 0.5882	EB 0.5861	1C 0.5862	A7 0.5946	C8 0.6170	5E 0.57...	4E 0.57...	89 0.61...	94 0.59...	38 0.60...	7 0.6
4	6C 0.5914	E0 0.6295	D9 0.6043	BC 0.5695	8E 0.5814	1E 0.5855	D3 0.5774	6B 0.5893	29 0.6094	59 0.57...	26 0.57...	28 0.61...	22 0.57...	33 0.59...	1 0.6
5	88 0.5904	B5 0.6162	8E 0.5957	8E 0.5661	7B 0.5752	7A 0.5805	9F 0.5692	B0 0.5774	CC 0.6053	EE 0.56...	3D 0.56...	6B 0.59...	82 0.56...	69 0.59...	E 0.5

Fig. 4: CW Analyzer Results Table

- To confirm the functionality of the ChipWhisperer as well as to demonstrate a Power Analysis attack, the ChipWhisperer was used to break AES encryption on the included target XMega.
- Generic Python scripts for the Power Analysis attack are provided with the ChipWhisperer software. These scripts were modified for the LinkIt board by specifying appropriate baud rate, I/O pins, and the use of an external clock.

HARDWARE SETUP



- The LinkIt and ChipWhisperer were connected together over serial. The LinkIt provided an external clock and a trigger signal to the ChipWhisperer. Finally, a power trace was used for the power measurements.
- To measure the power line, a direct connection was originally used. However, the resulting signal was far too weak for any analysis to take place. A shunt resistor was deemed infeasible, so an H-field probe was instead used for measurement.

4. CONCLUSION AND RECOMMENDATIONS

- Created the Power Analysis environment for the LinkIt chip
- Successfully gathered power traces during encryption and confirmed correct cyphertext on the LinkIt side
- A more accurate way of capturing power traces to isolate the crypto operations.
- Improving userspace control over the LinkIt to reduce noise

5. REFERENCES

- https://wiki.newae.com/Correlation_Power_Analysis [1]
- https://labs.mediatek.com/en/chipset/MT7688 [2]
- https://newae.com/tools/chipwhisperer/ [3]
- https://github.com/vschagen/mt7628-aes [4]
- https://github.com/intel-iot-devkit/mraa [5]