Correlation Electromagnetic Attack on PRESENT Lightweight Block Cipher

Nilupulee A. Gunathilake, Ahmed Al-Dubai, William J. Buchanan and Owen Lo

Research Problem

- Not enough studies regarding side-channel analysis of lightweight ciphers exis
- Unavailability of a correlation electromagnetic analysis (CEMA) of PRESENT

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Table 1: S-box of PRESENT

Figure 1: Locating S-box area

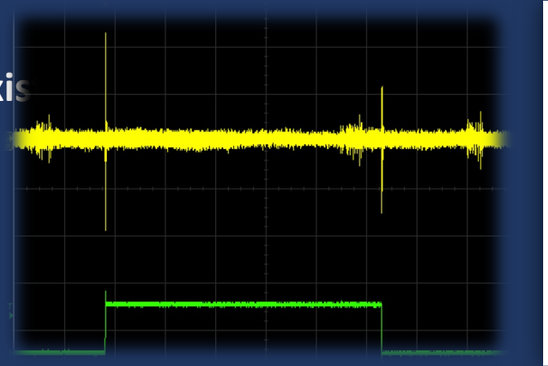
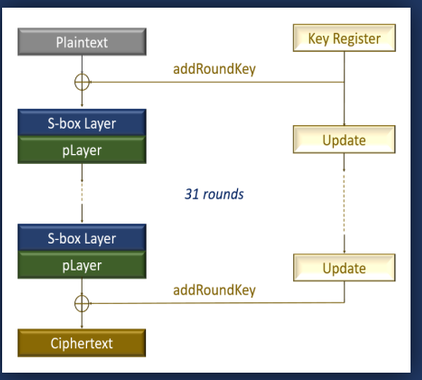


Figure 2: Process of PRESENT encryption



Key Features of the Research

- A simple EMA to find the encryption behaviour and frequencies affected by the encryption
- A CEMA of PRESENT's substitution box (S-box) for the first round

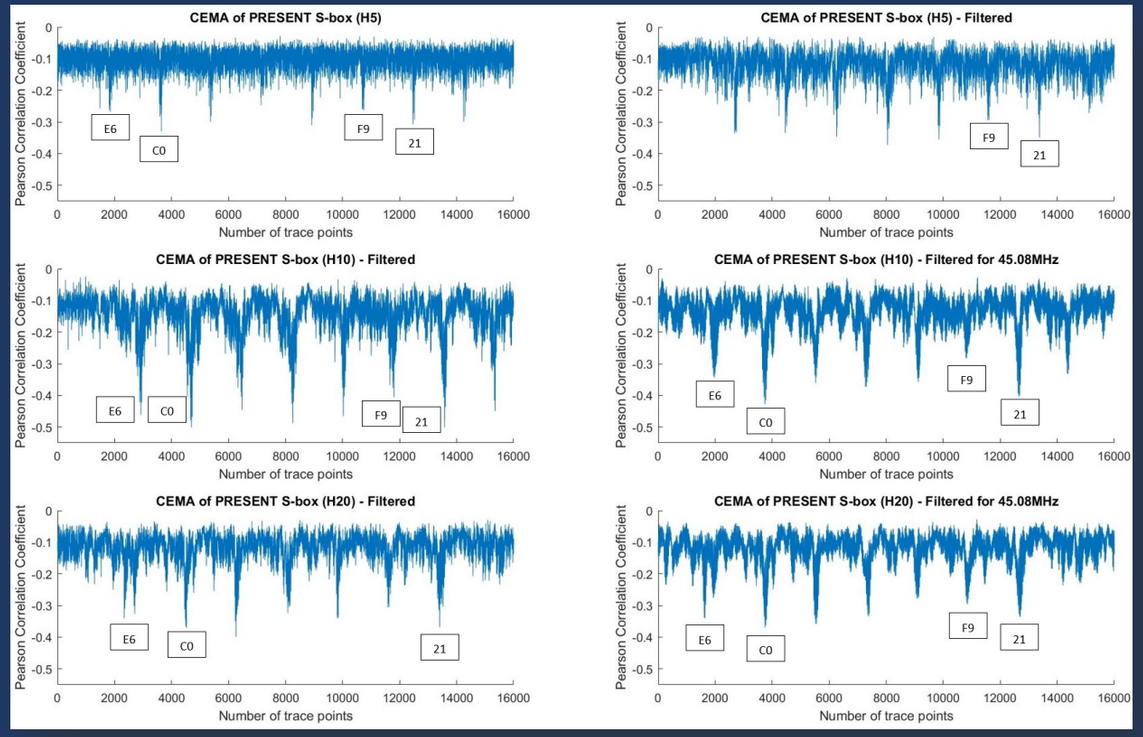


Figure 3: Resultant correlation graphs

Probability of Leakage								
Key Byte	1st **E6**	2nd **C0**	3rd **75**	4th **43**	5th **23**	6th **F9**	7th **21**	8th **FB**
H5	46.67%	20%	0	0	6.67%	60%	33%	0
H10	80%	20%	6.67%	0	0	66.67%	53.33%	13.33%
H20	40%	20%	13.33%	0	6.67%	46.67%	53.33%	6.67%

Probability of Leakage at a Time				
H5	Four: 6.67%	Three: 13.33%	Two: 46.67%	One: 13.33%
H10	Four: 20%	Three: 40%	Two: 13.33%	One: 13.33%
H20	Four: 6.67%	Three: 26.67%	Two: 33.33%	One: 20%

Table 2: Results summary

Progress

- ✓ Eight troughs in resultant correlation graphs that indicate eight major leakage areas
- ✓ Seven bytes of the secret key were derived

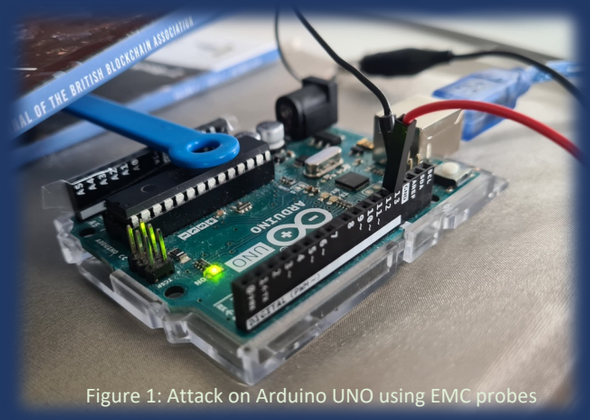


Figure 1: Attack on Arduino UNO using EMC probes