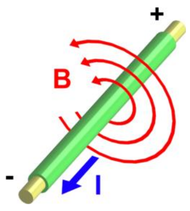
TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

EM Side Channel Analysis on Complex SoC Architectures

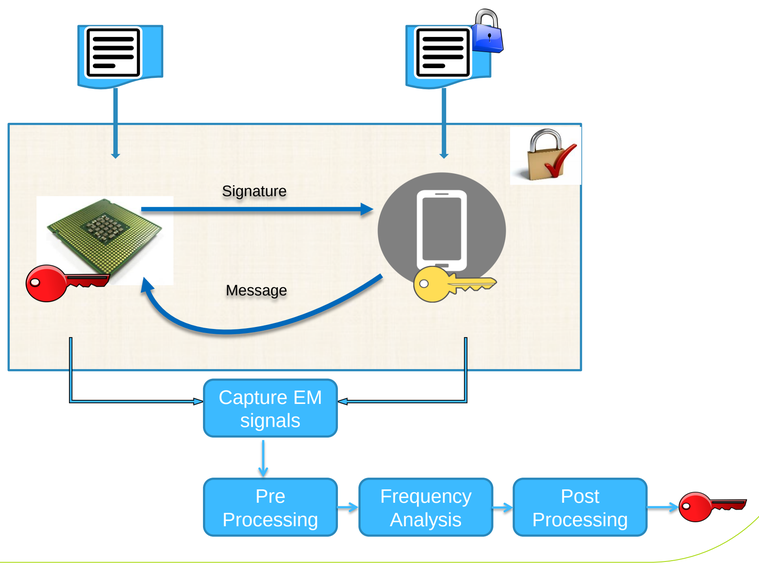
Sohaib ul Hassan, Billy Bob Brumley

EM Side Channel

- **EM side channels are caused due to processor/memory activity modulated on some carrier (usually clock signals and its harmonics)**



- **These channels contain several compromising frequencies, that can be targeted to break cryptographic implementations**



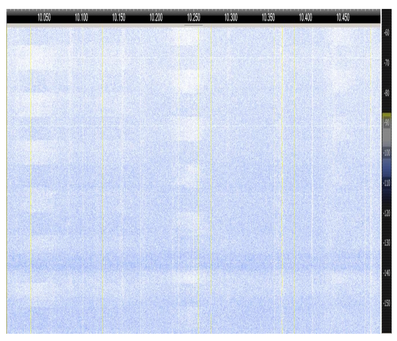
OpenSSL Elliptic Curve Cryptography

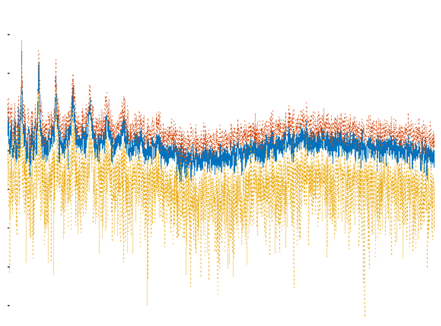
- **OpenSSL uses Elliptic Curve crypto in Diffie-Hellman Key Exchange and Digital Signature schemes**
- **It is particularly attractive to use in low power embedded devices**

- **The Elliptic Curve point multiplication operation generates a sequence of Double and Add operations dependent on the scalar *K***

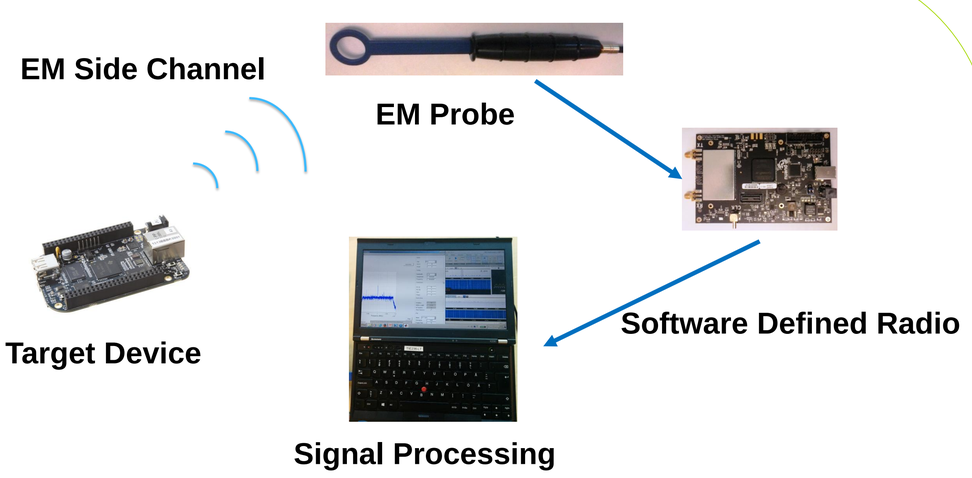
```
Q := 0
for i = k ... 0:
    Q := double(Q)
    if(d_i = 1)
        Q := add(Q, P)
return Q
```

- **EM side channel showing Double and Add operations falling on different parts of the frequency spectrum**





EM Acquisition and Key Extraction



Results

- **OpenSSL EC secp256k1** curve running on **ARM® Cortex-A8**
- Low Cost Setup using **Software Defined Radio**
- **Single EM trace** used to recover key
- **Non-Invasive** and **Passive** Attack model
- Key extraction possible at **lower frequencies and sampling rates**
- **Signal Denoising** techniques can recover full or partial key in EM signals with low SNR

Department of Pervasive Computing, Tampere University of Technology

Tekes