Leveraging Electromagnetic Side-Channel Analysis for the Investigation of IoT Devices

Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon

UCD DUBLIN

UCD Forensics and Security Research Group

Status of Digital Forensics

- Acquiring data from computing devices that can help to progress investigations.
- Increasing usage of computing devices adding up to more forensic data sources.
- More and more computing devices are employing encryption to store data.
- Most digital forensic literature assumes either that,
  - Cryptography is not employed
  - Cryptography is bypassed somehow as a part of the legal process.
- It is not possible to ignore the threat posed by encrypted devices.

Forensics of Internet of Things

- IoT opens up new evidence sources from unexpected places.

  ...health implants, sports wearables, smart burglar alarms, smart thermostats...

- Highly heterogeneous device designs.

- Application of encryption worsen the usability of IoT in forensics.

Overcoming the Encryption Barrier

- Logical drive image acquisition.
- Live forensic analysis without turning the device off.
- Temporary plaintext copies saved in other locations in the disk that are produced when applications access encrypted files.
- None of these workarounds are applicable to IoT.

What alternatives do we have?

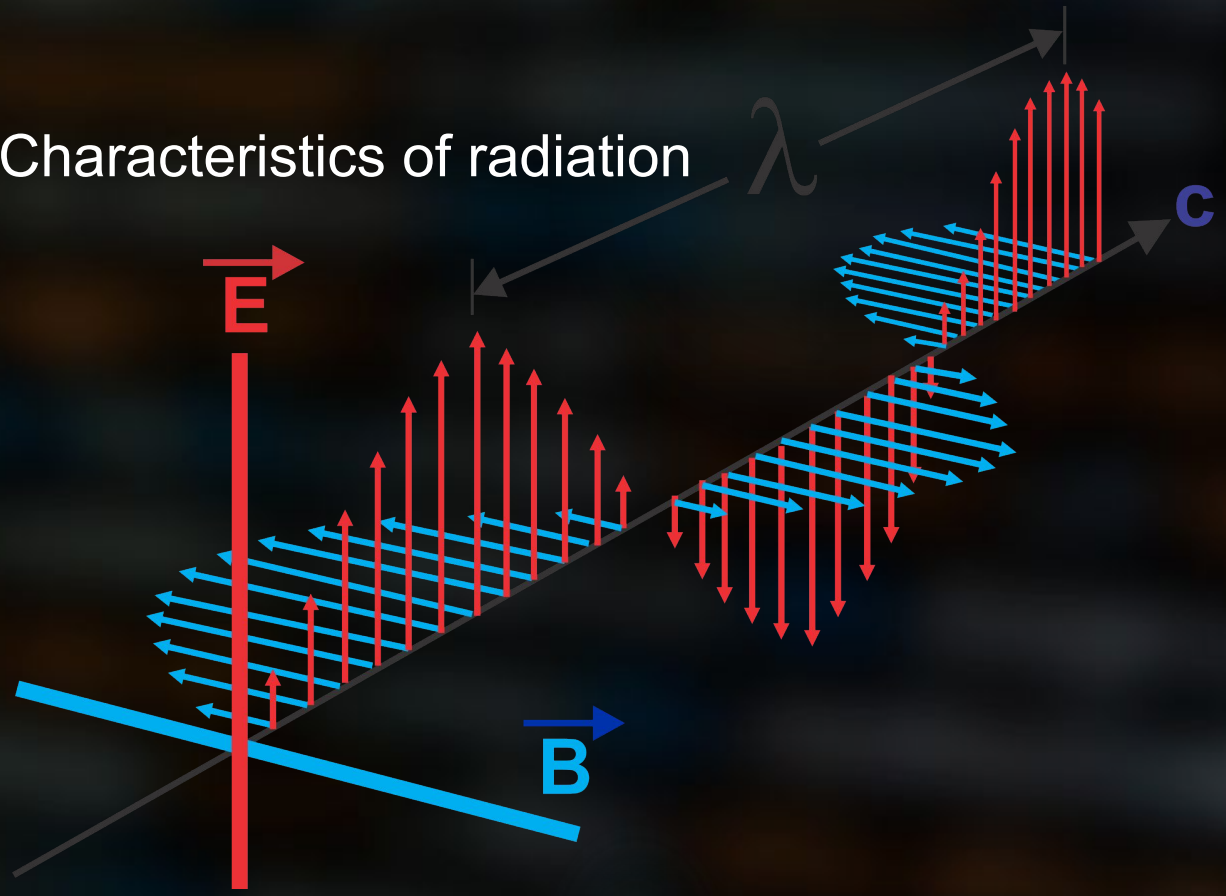
Electromagnetic Side-Channel Analysis

Time-varying electrical currents ⇒ Electromagnetic radiation

Nature of the time-varying current ⇐ Characteristics of radiation

EM radiation from computer processors leak information

EM side-channel analysis (EM-SCA)



Electromagnetic Side-Channel Analysis

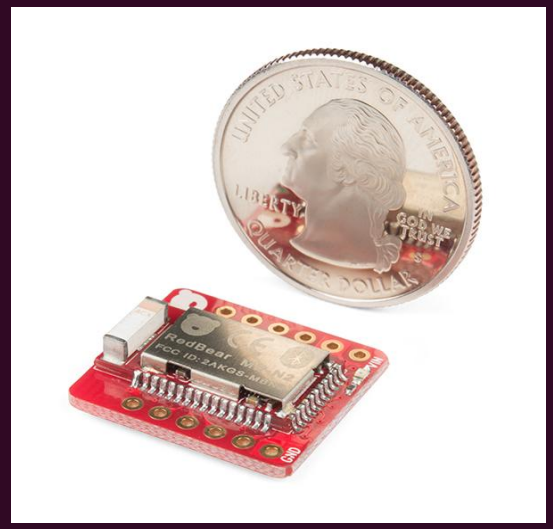
- EM-SCA has been applied to recover cryptographic keys,

  e.g., Camurati et al. (2018)
- Target device: BLE-Nano running AES-128 encryptions.
- ~ 8000 EM trace samples.
- Correlation electromagnetic

  analysis (CEMA)
- 18 minutes to recover the key

We explores the possibility of adapting EM-SCA for digital forensic evidence gathering from IoT devices.

```
Subkey 15, hyp = ed:  0.012530354407226786
Subkey 15, hyp = ee:  0.017266581888572823
Subkey 15, hyp = ef:  0.010556395126552152
Subkey 15, hyp = f0:  0.02396490987572155
Subkey 15, hyp = f1:  0.012949217484922705
Subkey 15, hyp = f2:  0.014502574032304778
Subkey 15, hyp = f3:  0.014963314285949247
Subkey 15, hyp = f4:  0.012954752080796888
Subkey 15, hyp = f5:  0.0130315561783500 3
Subkey 15, hyp = f6:  0.013772034631913068
Subkey 15, hyp = f7:  0.019364248397445407
Subkey 15, hyp = f8:  0.010932180008903168
Subkey 15, hyp = f9:  0.013027691526298332
Subkey 15, hyp = fa:  0.01665869128411864
Subkey 15, hyp = fb:  0.015427833690631214
Subkey 15, hyp = fc:  0.011935004419024819
Subkey 15, hyp = fd:  0.014665594979696694
Subkey 15, hyp = fe:  0.018540794601137632
Subkey 15, hyp = ff:  0.018274501184871804
Best Key Guess:   56   89   ed   be   4c   65   db   f2   aa   2c   bd   c9   26   42   e6   e1
Known Key:        56   89   ed   be   4c   65   db   f2   aa   2c   bd   c9   26   42   e6   e1
PGE:             000  000  000  000  000  000  000  000  000  000  000  000  000  000  000  000
SUCCESS:           1    1    1    1    1    1    1    1    1    1    1    1    1    1    1    1
NUMBER OF CORRECT BYTES: 16
```



Hardware for EM-SCA

Oscilloscopes / spectrum analyzers / traditional radio receivers

Difficult to handle in in digital forensic investigation settings.

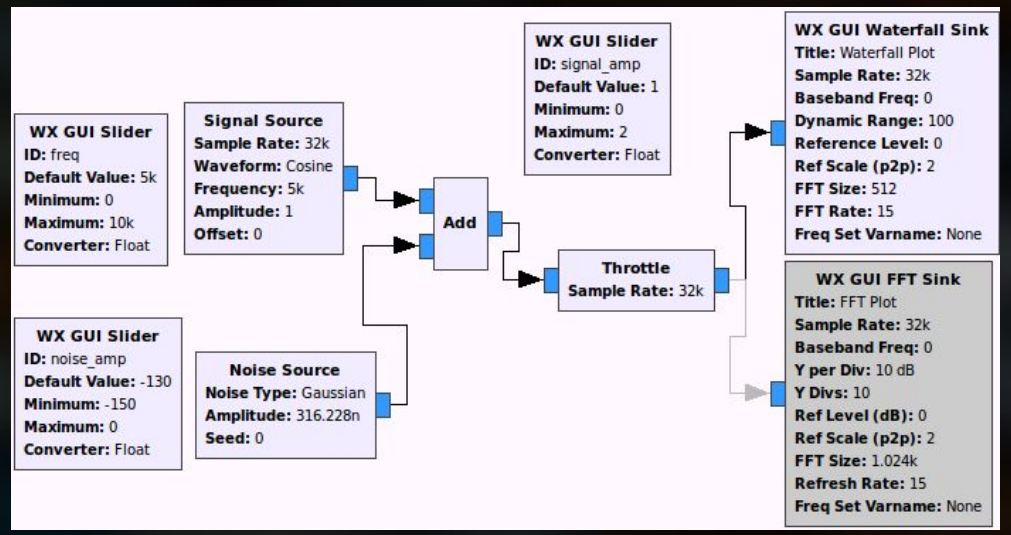
Software-defined radios (SDR)

Easily configurable with software.

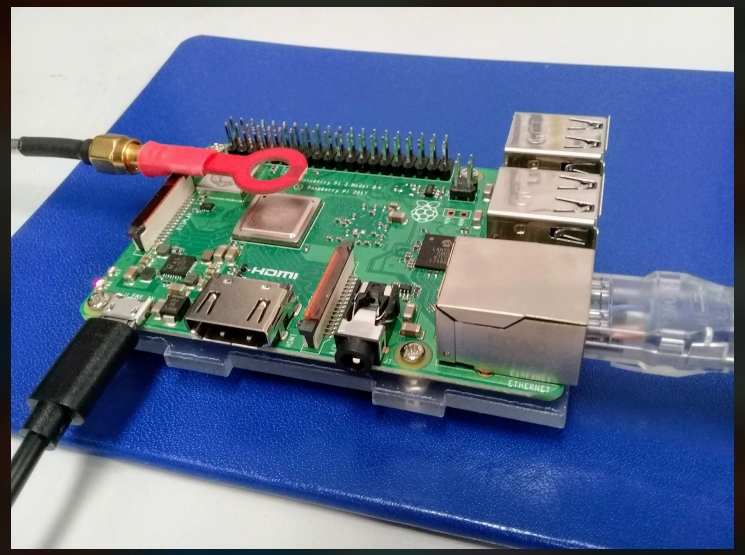
Software Defined Radio (SDR)

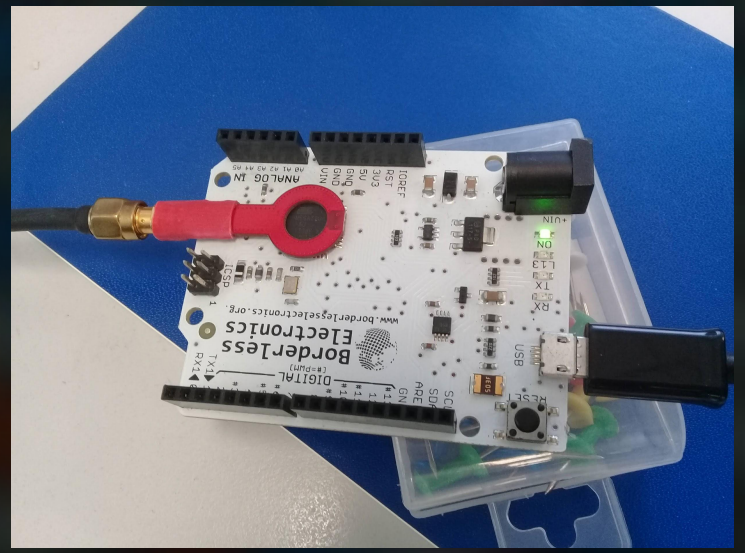
- A fast analog-to-digital converter (ADC).
- RTL-SDR, HackRF, USRP
- Generates digitized samples in Inphase-Quadrature (I-Q) format.
- Open source libraries to process streams of I-Q data samples.
- Can program for a task using Python or using a visual flowgraph editor, GRC.

GNU Radio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

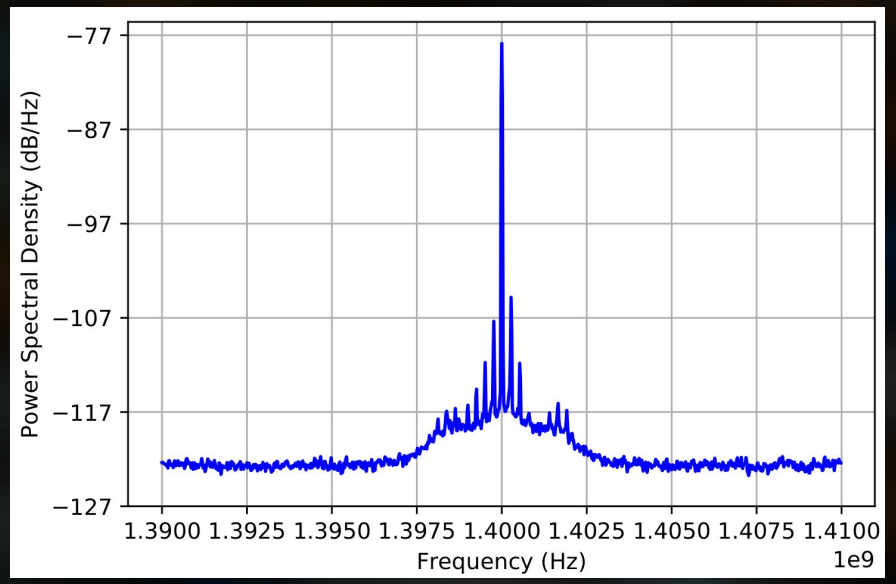


Observation of EM Side-channel



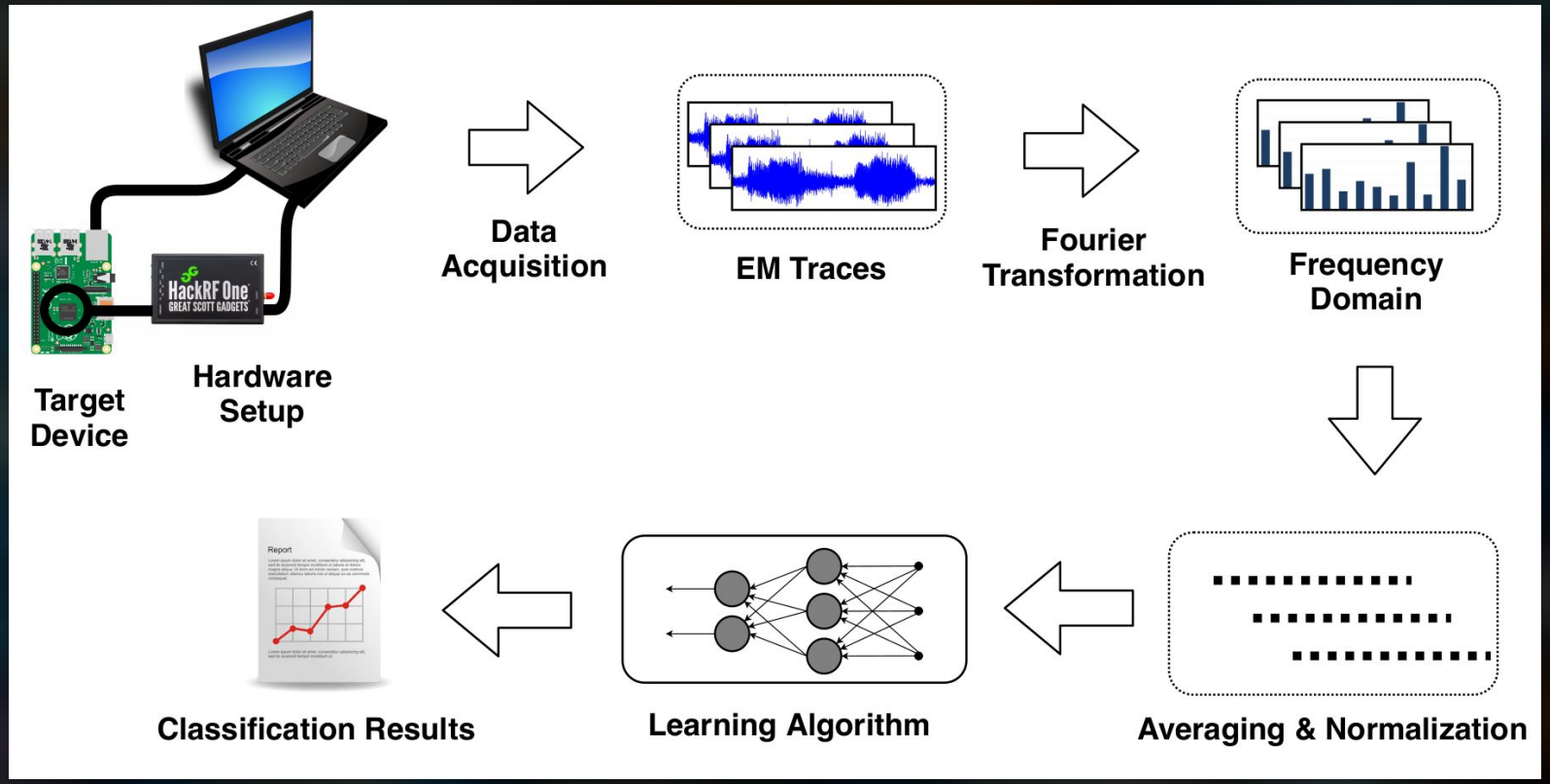


- CPU clock/oscillator is the main source of EM noise.
- EM emissions can be observed at clock frequency and its harmonics.
- Signal attenuates rapidly with distance from the CPU.
- H-loop antennas placed closer to the CPU can pick up strong signals.
- When the fundamental frequency is noisy due to external sources, harmonics can be used.

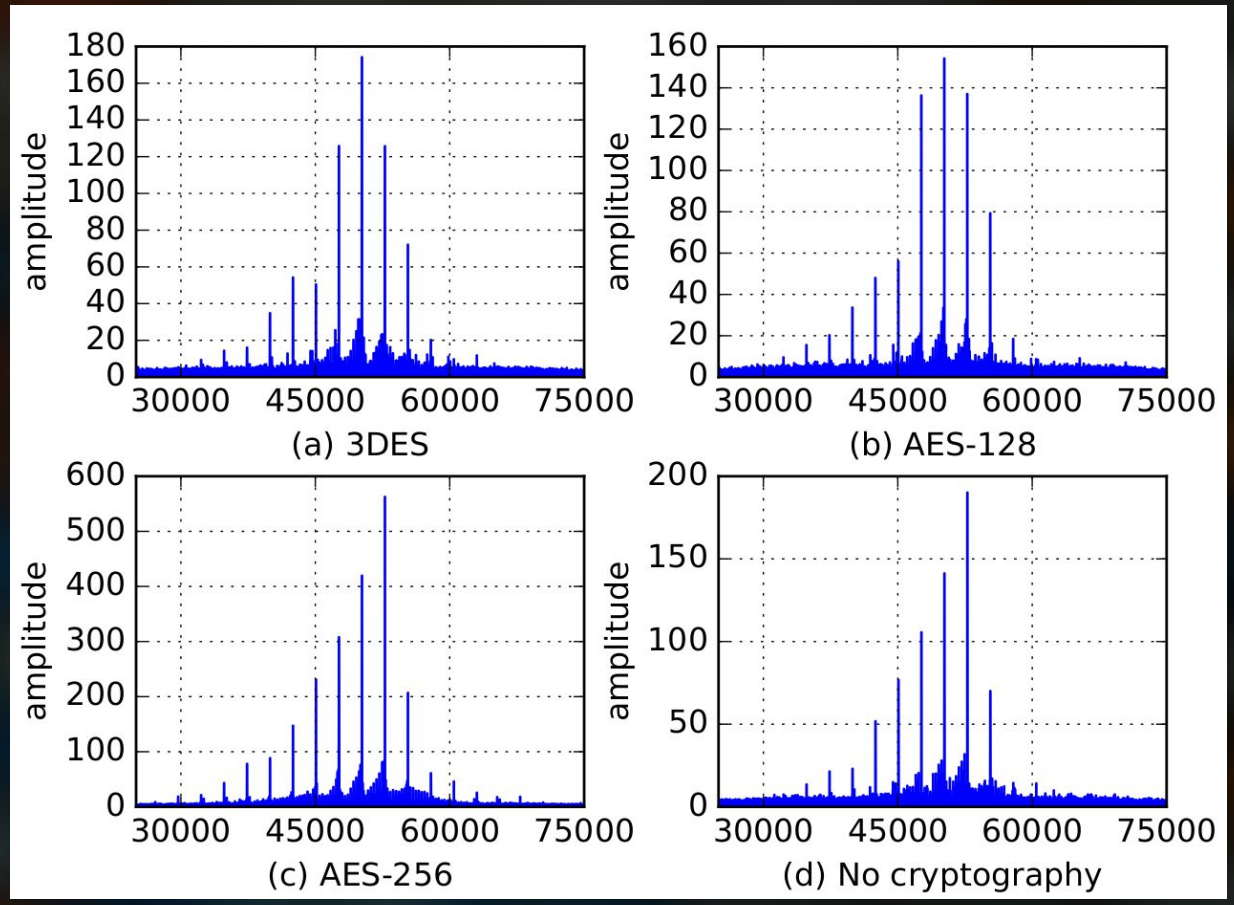


Machine Learning with EM Data

1. Discriminating cryptographic activities
2. Detection of software behaviour
3. Detecting modifications to firmware



Discriminating Cryptographic Activities



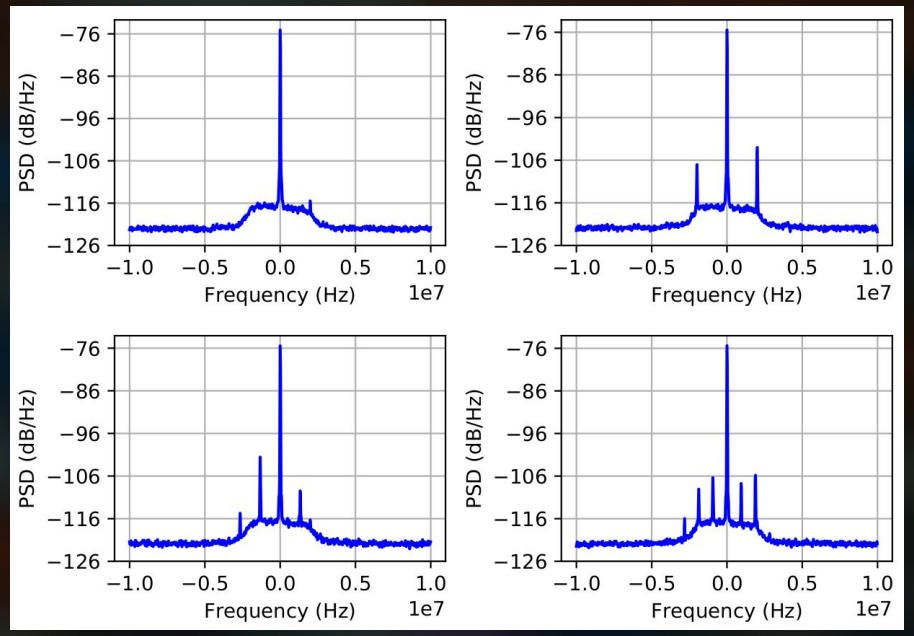
- Raspberry Pi as the target device.
- Three cryptographic classes and a ``no cryptography" class.
- From FFT to 500 features by averaging.
- 4 layer NN (2 hidden - 10x5)
- 600 samples per class.

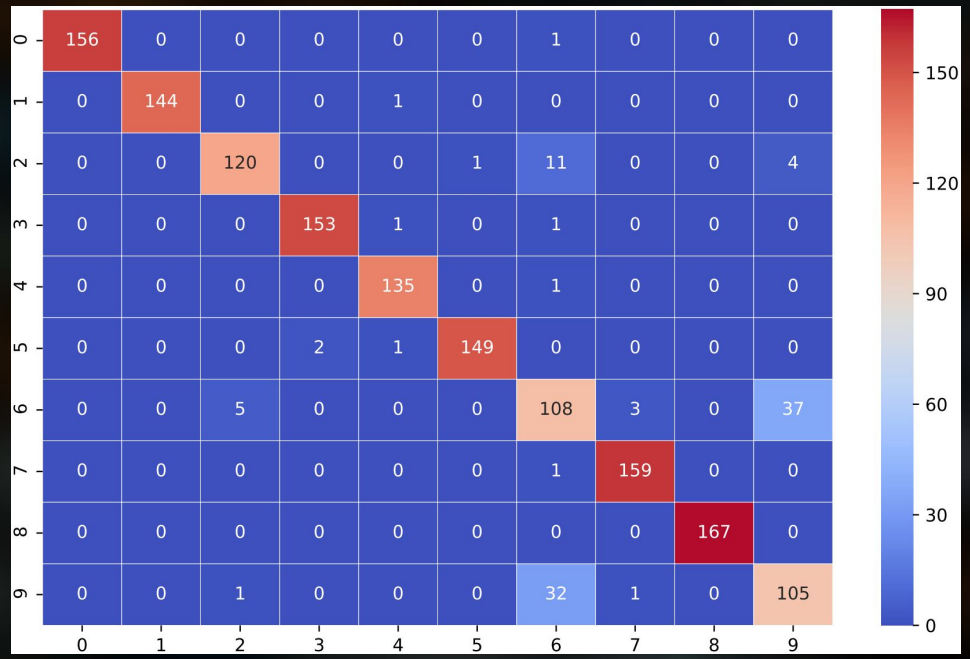
Activity	Precision	Recall	F1-Score
Other	0.93	0.85	0.89
AES-256	0.78	0.86	0.82
AES-128	0.99	0.92	0.95
3DES	0.81	0.85	0.83

Detection of Software Behaviour

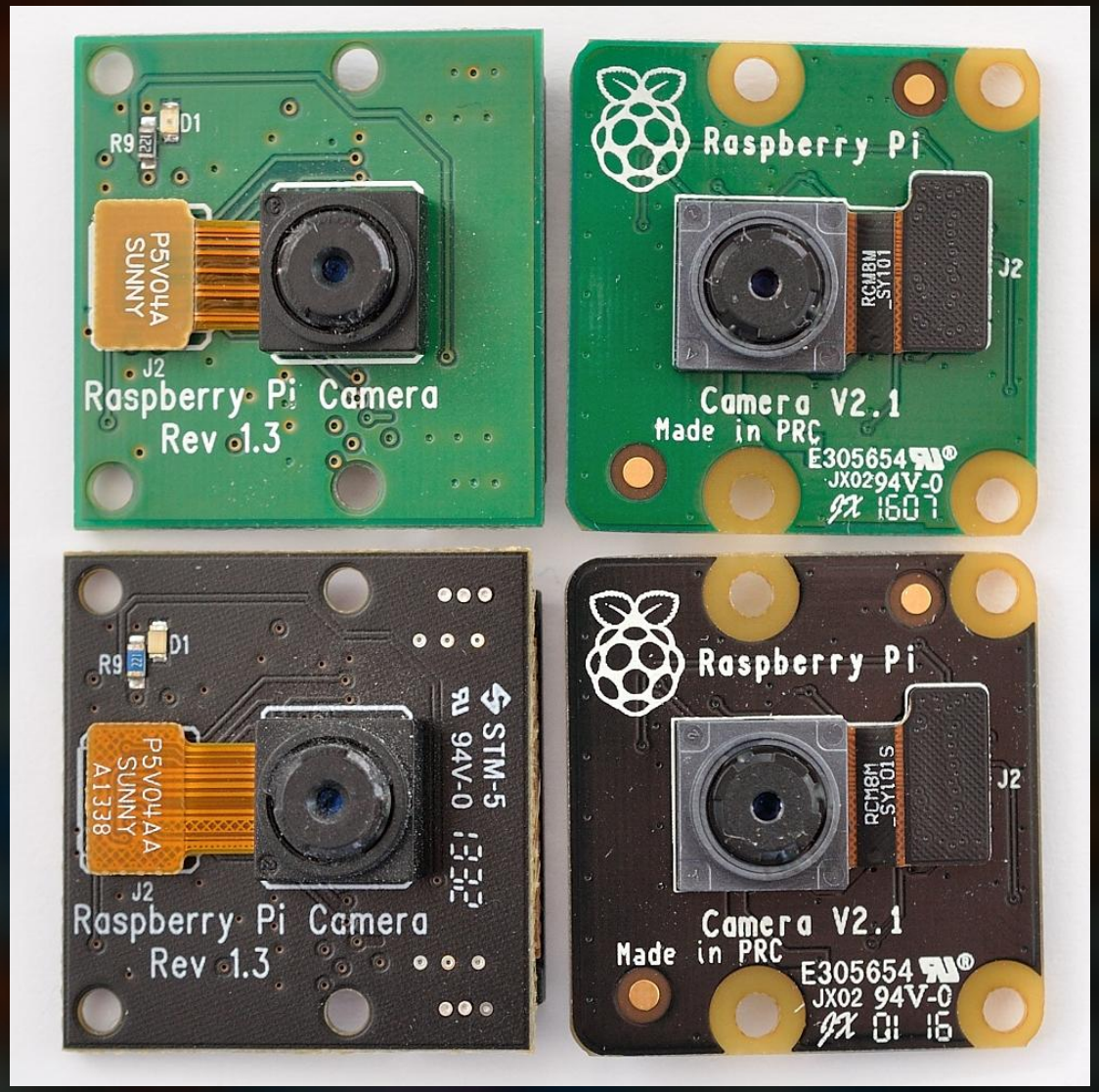

```
/* Arduino test program */
void setup(){
}
void loop(){
    for(int i=0, i<20, i++) { delay(10); }
    for(int i=0, i<20, i++) { delay(10); }
    /* further loops */
}
```

- Arduino Leonardo running 10 programs
- FFT (20,000,000) to a vector of 1000 features.
- 1000 buckets with max values.
- Over 90% classification accuracy





Detecting Modifications to Firmware

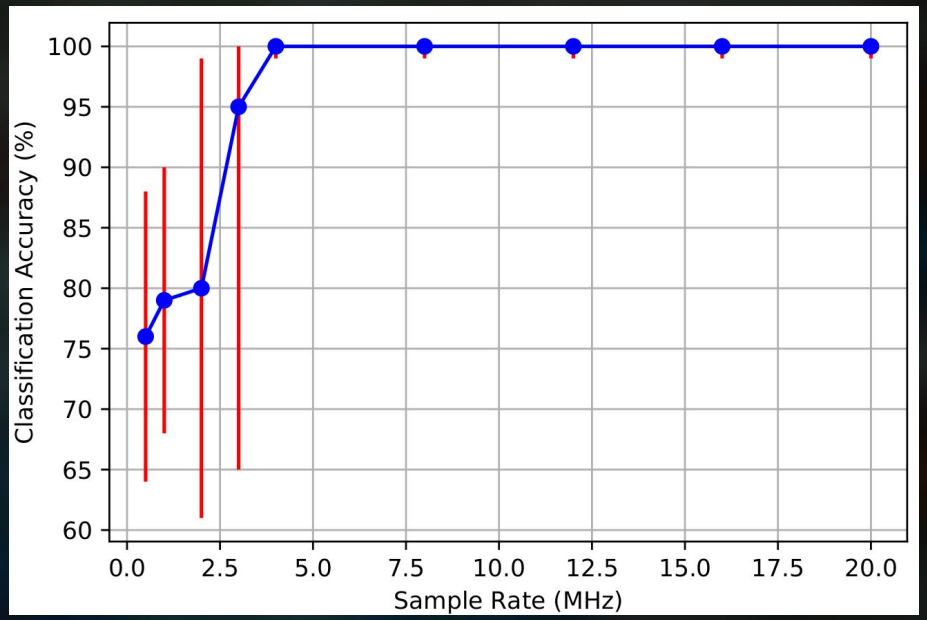


- Arduino Leonardo as the target device.
- FFT to 1000 features using max values.
- One-class SVM with a non-linear kernel (RBF).
- 1 legitimate program and 20 slightly modified programs for testing.
- 100% detection accuracy for all the tested programs.

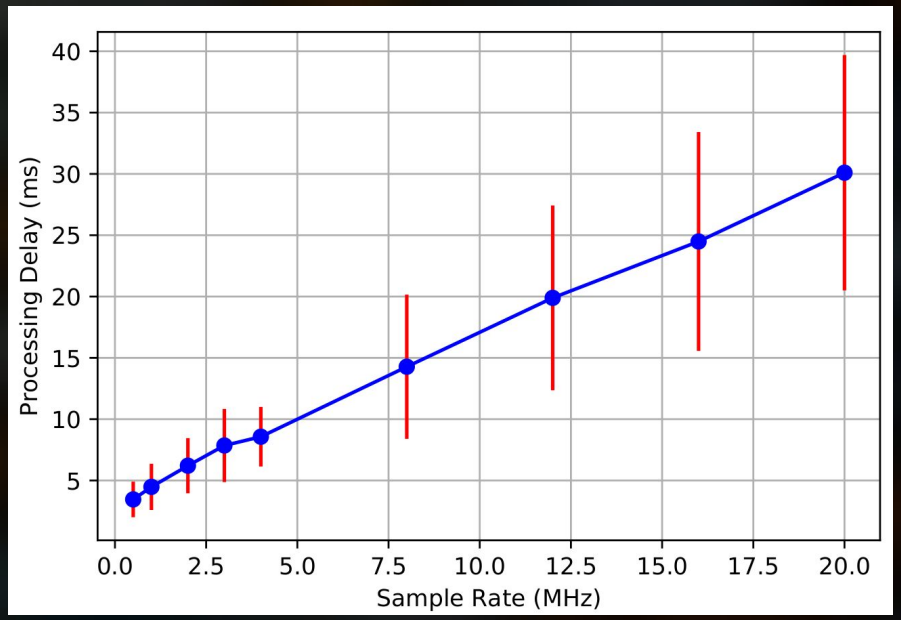
Storage and Real-time Requirements

- Each I-Q sample = 8 bytes
- Highest sampling rate = 20 MHz
- Size of the 1 minute signal capture ≈ 9 GB

  (8 bytes × 20 MHz × 60 seconds = 8.94 GB).



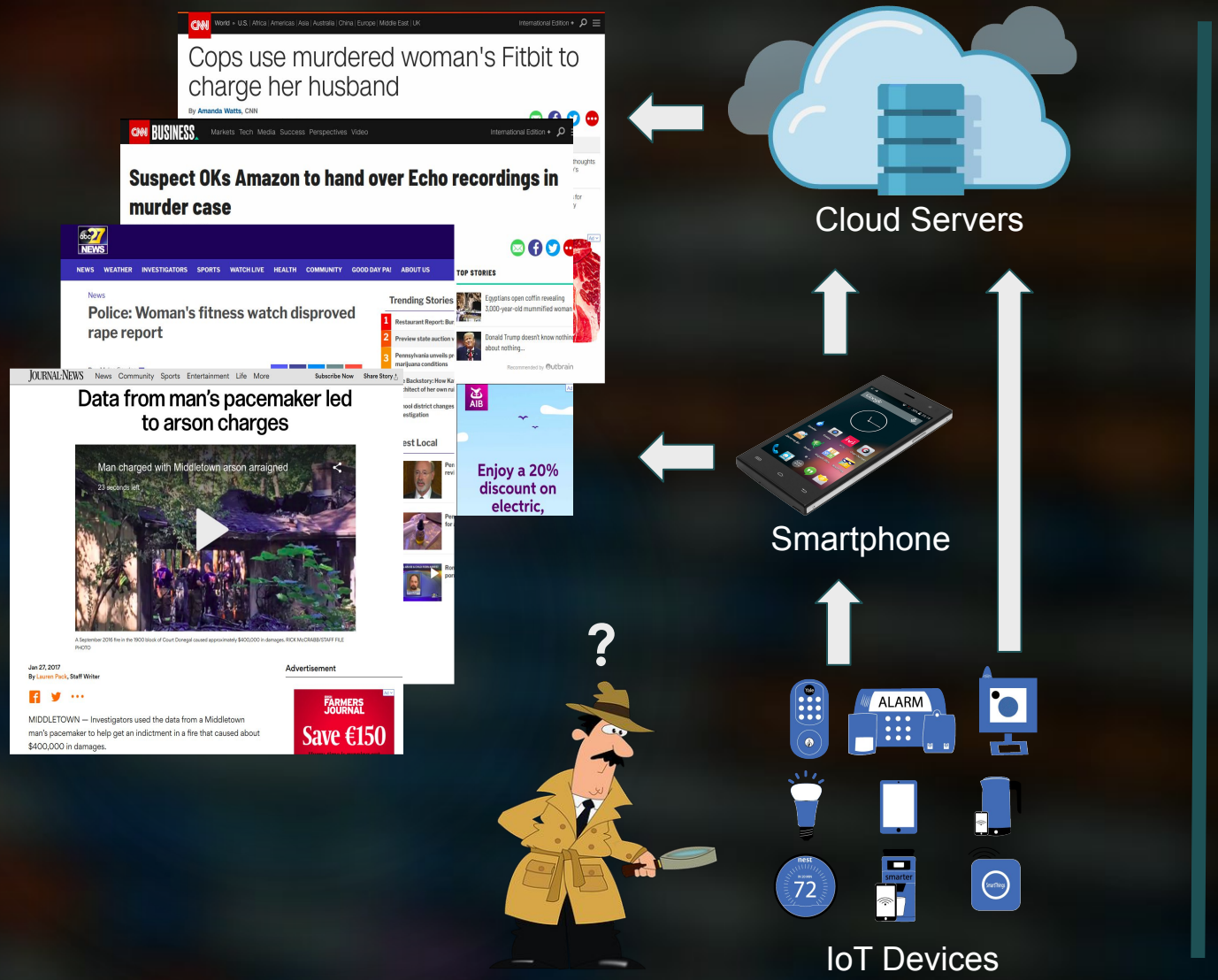
It's OK to have lower sampling rates to cope with storage requirements.



Even the highest sample rate does not exceed our capability to process data in real-time

Hence, live forensic analysis is possible!

Application of EM-SCA



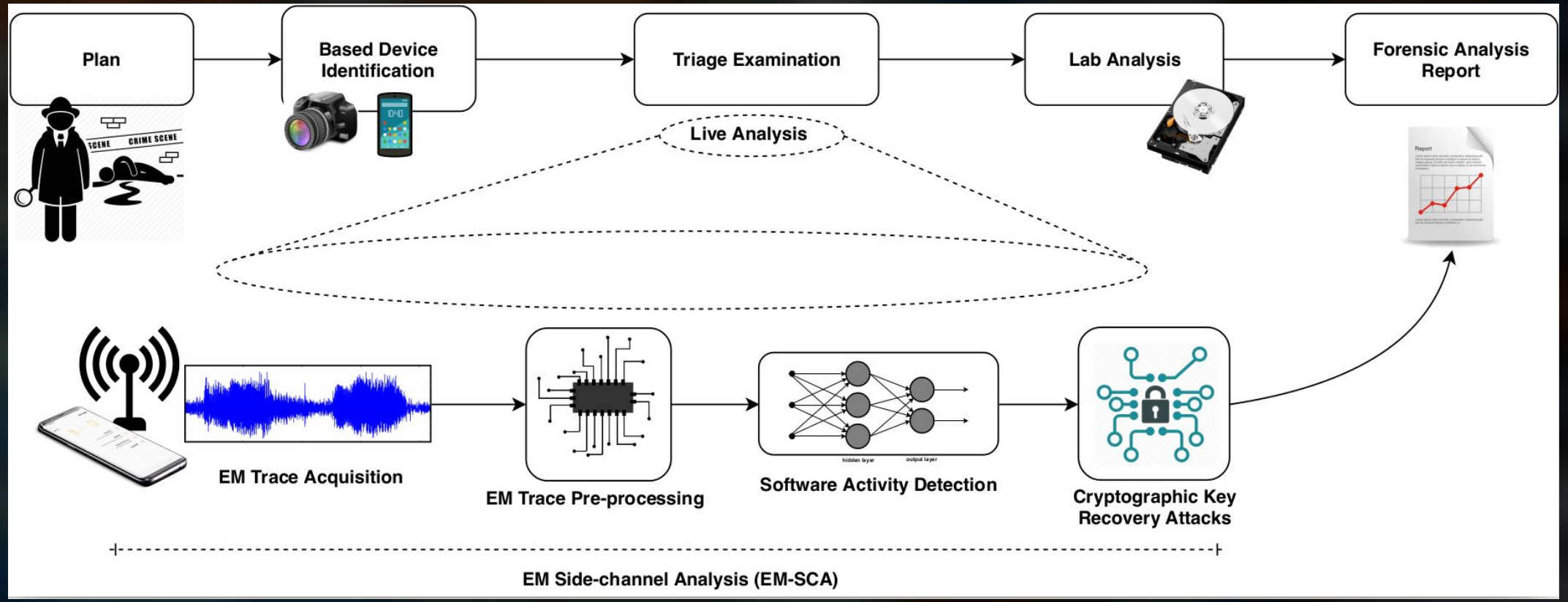
- Smartphone apps and cloud servers are the window to most IoT devices.
- IoT devices are mostly black boxes due to,
  a. lack of standard forensic data gathering interfaces
  b. high heterogeneity of devices
  c. employment of encryption
- EM-SCA opens up a window to gather insights directly from the IoT devices.

Application of EM-SCA

- An IP camera that takes photos when a motion is detected.
- Images are stored locally on an SD card with encryption.
- User can remotely initiate a video streaming which uses encryption as well.
- Cryptographic key is securely stored on the camera in a way not easily accessible to third parties.

How can I extract and decrypt a particular encrypted image on the SD card?

Application of EM-SCA



Limitations

- EM-SCA only applicable if the device is giving out sufficient EM radiation.
- Properly shielded devices are difficult to reach without high powered signal amplifiers.
- A firmware update can change the EM signature completely.
- Key recovery requires large number of traces.
  a. encryption should occur frequently
  b. need a sufficient time to observe as many encryption as possible
- Presence of multiple devices within the vicinity that produce EM radiation in similar frequencies can make the isolation of one device difficult.
- A huge variety of manufacturers/configurations for the same device - e.g., Amazon Echo.

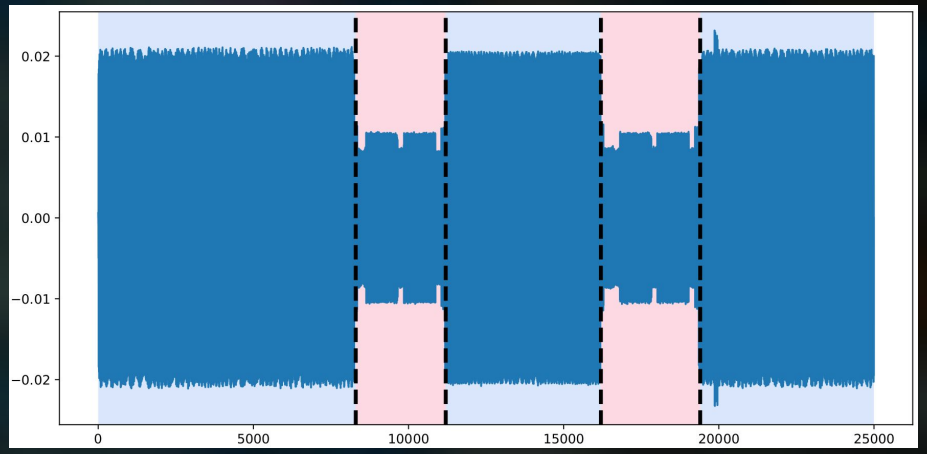
Conclusion

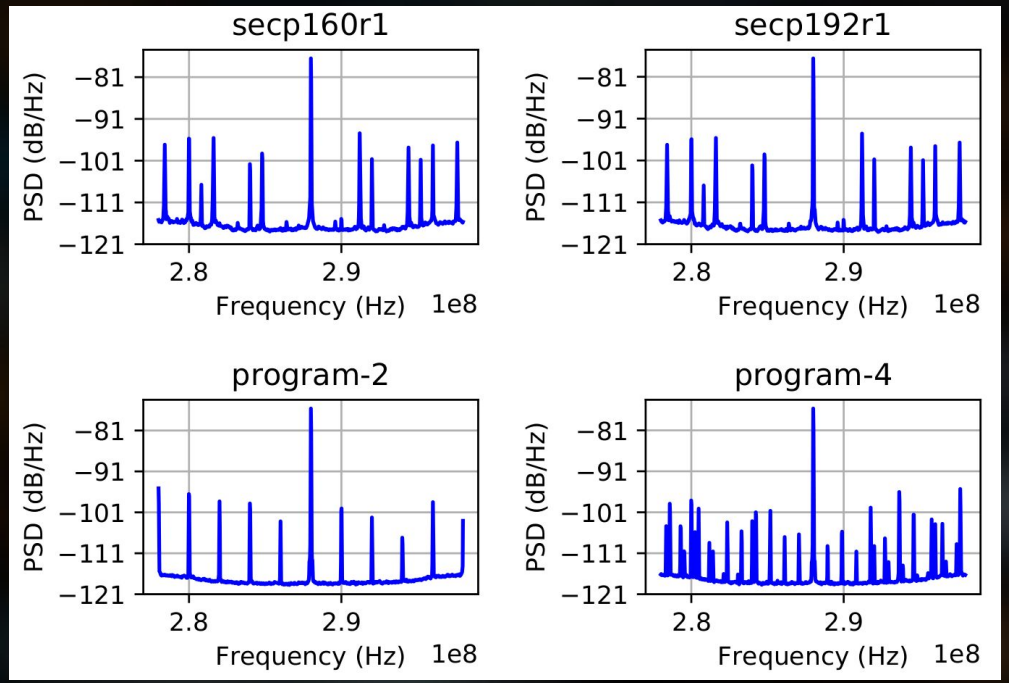
- This work demonstrates the possibility of using EM-SCA as a window to computing devices, in particular to IoT devices, to gather forensically useful information.
- EM-SCA is a potential approach to break the encryption barrier in digital forensics.
- It's possible to detect when an IoT device is performing encryptions or any other important software behavior using machine learning models.
- Detection of cryptographic algorithm through EM-SCA removes the need of prior knowledge about a device to perform key recovery attacks.
- Size of EM signal data is manageable since we can use lower sampling rates without inflicting any harm to the accuracy of automatic software behavior detection.

Ongoing work

- Implementing a ready-to-use, extensible EM-SCA analysis software framework for digital forensic investigators.

- Developing techniques to automatically extract EM traces without hardware/software instrumentation of the target device.





ASANKA.SAYAKKARA@UCDCONNECT.IE

WWW.FORENSICSANDSECURITY.COM

@FORSECRESEARCH

UCD Forensics and
Security Research Group