

# Electromagnetic Side-Channel Attack Resilience against PRESENT Lightweight Block Cipher

Nilupulee A. Gunathilake, Ahmed Al-Dubai, William J. Buchanan and Owen Lo  
Blockpass ID Lab, School of Computing, Edinburgh Napier University, United Kingdom

**Abstract**—Lightweight cryptography is a novel diversion from conventional cryptography that targets internet-of-things (IoT) platform due to resource constraints. In comparison, it offers smaller cryptographic primitives such as shorter key sizes, block sizes and lesser energy drainage. The main focus can be seen in algorithm developments in this emerging subject. Thus, verification is carried out based upon theoretical (mathematical) proofs mostly. Among the few available side-channel analysis studies found in literature, the highest percentage is taken by power attacks. PRESENT is a promising lightweight block cipher to be included in IoT devices in the near future. Thus, the emphasis of this paper is on lightweight cryptography, and our investigation shows unavailability of a correlation electromagnetic analysis (CEMA) of it. Hence, in an effort to fill in this research gap, we opted to investigate the capabilities of CEMA against the PRESENT algorithm. This work aims to determine the probability of secret key leakage with a minimum number of electromagnetic (EM) waveforms possible. The process initially started from a simple EM analysis (SEMA) and gradually enhanced up to a CEMA. This paper presents our methodology in attack modelling, current results that indicate a probability of leaking seven bytes of the key and upcoming plans for optimisation. In addition, introductions to lightweight cryptanalysis and theories of EMA are also included.

**Index Terms**—Lightweight cryptology, PRESENT cipher, electromagnetic side-channel analysis

## I. INTRODUCTION

Internet-of-things (IoT) is a communication infrastructure that is being spread widely, increasing the number of connected devices exponentially. Estimates predict that there would be more than 200 billion connected devices by 2025 [1]. The ecosystem of IoT is constrained in terms of resource adaptability, because it is operated on low data rates (kbps), contains small onboard memories and is usually battery-powered. Nevertheless, its data flow is known to be dense, opaque and supposed to have low latency. Power consumption of these devices is greatly reduced in comparison with standard computing devices. Hence, green networking is an added advantage of IoT. An overall review of IoT is accessible in [2] and [3]. However, IoT is struggling to adopt adequate security features because conventional cryptography requires high processing capabilities, large capacities as well as faster data rates. As a result, a specific approach just targeting IoT data and privacy protection was introduced recently to build cryptographic methods in lightweight. Those techniques expect to offer shorter key lengths/initialisation vector (IV),

smaller block sizes/internal state (IS) and lower memory requirements. A complete literature review about lightweight cryptology can be referred in [4].

In cryptology, cryptanalysis is vital to verify the strengths and weaknesses of proposed cryptographic algorithms. In cryptanalysis, non-cryptographic primitives such as internal power variations, external electromagnetic (EM) radiation, acoustic changes, data remanence on devices pose a substantial threat in securing a device. Therefore, side-channel analysis of recommended ciphers is a must in parallel with other types of cryptanalysis such as mathematical validations, use-case simulations and brute-force analysis. The basics of physical security phenomena are accessible in [5]. Study [6] demonstrates that KLEIN is a side-channel resistant cipher regarding first-order attacks, but it may still be vulnerable to higher-order attacks. Recently, an option of re-keying which helps prevent side-channel attacks, has been introduced to lightweight cryptography as well [7]. On the other hand, physical leakage analysis remains to be thoroughly researched. The majority of existing work belongs to power analysis (PA) [8]. In this context, [9], [10] and [11] are about differential PA (DPA) and a correlation PA (CPA) of PRESENT respectively. A DPA of Simon and LED is available in [12] and a CPA of Fantomas, LBlock, Piccolo, PRINCE, Simon and Speck is accessible in [13]. However, other crucial characteristics such as EM emission, cache monitoring, optical changes, cold boot remain to be fully observed. [14] evaluates results against a differential EM analysis (DEMA) of PRESENT. [15] and [16] are about correlation EMA (CEMA) of PRINCE and Twine respectively. According to the available literature, a research outcome regarding CEMA of PRESENT by another research group is still unavailable.

### A. Our Contribution

PRESENT is a promising block cipher recognised to be an alternative for Advanced Encryption Standard (AES) in lightweight applications. According to the developers of the cipher, it is more prone to side-channel and invasive hardware attacks [17]. Thus, our contribution involves modelling a white-box, but non-invasive CEMA attack to evaluate the vulnerability of the PRESENT against its firmware robustness. This is still ongoing research, and this paper structures over:

- An EMA classification and its relevant theories
- A description of our attack model implementation
- Our latest results and observations
- Discussion over the progress achieved so far

\*This work is supported by the research grants from the School of Computing, Edinburgh Napier University, UK. Any correspondence related to this article can be sent to nilupulee.gunathilake@napier.ac.uk

- Plans for optimisation and finalisation of the work

## II. ELECTROMAGNETIC SIDE-CHANNEL ANALYSIS

Electronic circuitries emit EM radiation as they operate. The radiated EM emanation can be detected using near-field (NF) EM compatibility (EMC) probes. According to Faraday's law of induction, changes of magnetic flux in a magnetic field generate a voltage in the probe's loop (equation 1). In EMA, excess EM radiation round a device resulted by an encryption is measured to observe if there is any correspondent relationship between secret information and EM field variations. However, the task is more difficult from the attacker's perspective where prerequisite knowledge of the encryption key is unavailable. Although oscilloscope has been the typical device used to monitor and collect EM waveforms, software-defined radio (SDR) has become an interesting low-cost alternative nowadays.

$$V = 2\pi BA \quad (1)$$

where,

$V$  - Voltage

$\pi$  - The constant Pi, equal to 3.14159

$B$  - Average magnetic field

$A$  - Area perpendicular to the magnetic field

If a possibility of any EM attack is indicated in preliminary studies, necessary countermeasures can be enabled in prior to manufacturing devices for commercial use, such as:

- Proper EM shielding made of suitable materials, *e.g.*, inclusion of Faraday cages
- Addition of EM noise to hide or misguide the leakage
- Asynchronism of device clock correspondent to critical cryptographic functions
- Cryptographic operation obfuscating firmware application [18]
- Randomisation of cryptographic function sequences and or lookup tables
- Use of pointers in data structures instead of values

There are several attack models used in EMA, known as simple EMA (SEMA), DEMA, CEMA and template EMA (TEMA). Since our work is based on SEMA and CEMA, those two types are briefly described under the following subsections. Despite the type, Hamming calculations are an essential procedure to obtain hypothesised values to compare with actual data [19]. Hamming results indicate the maximum number of bit changes within the registers of the device. For obtaining the values, either Hamming distance (HD) or Hamming weight (HW) method is used. In this study, the HW (equation 2) has been used due to its higher efficiency. This counts all numbers of non-zero elements in a binary number at once, *e.g.*, HW of 10110010 is 4.

$$E = a.HW(D) + b \quad (2)$$

where,

$E$  - Hypothesised EM emission energy

$D$  - Intermediate value

$a$  - Gain

$b$  - Noise

Performing EMA has been conducted in the time domain for a known period of time. On the contrary, new efforts were introduced in the frequency domain recently as an improved step. According to the literature, frequency domain work tends to avoid trace misalignment issues where time-domain results may be affected by frequently.

### A. Simple EMA (SEMA)

This is simply a visual inspection of EM traces to identify its leakage points or encryption behaviour. Generally, the process may not involve breaking into secret data, but it might become possible to extract encryption keys by contemplating clock information as well as presumable HW changes of the device [20].

### B. Correlation EMA (CEMA)

This is an efficient version of DEMA which processes several bits at a time where device details are not required. The computations focus on the correlation between a hypothesised intermediate value obtained via either the HD or the HW method and actual data captured in EM traces. The highest correlation of accurately aligned traces may indicate a possibility of a leakage point. Equation 3 is used to calculate correlation coefficient for the task.

$$\rho = \frac{Cov(X, Y)}{\sigma_X \sigma_Y} \quad (3)$$

where,

$\rho$  - Pearson correlation coefficient

$Cov(X, Y)$  - Covariance between X and Y

$\sigma_X$  - Standard deviation of X

$\sigma_Y$  - Standard deviation of Y

## III. ATTACK MODELLING

### A. PRESENT Block Cipher

PRESENT is a block cipher introduced by the authors of [17] in 2007. It is recognised to be an ultra-lightweight<sup>1</sup> cipher that has been approved by the ISO/IET [21]. In addition, the NIST has mentioned it under lightweight block cipher listing in their NISTIR 8114 report [22]. Its architecture is a substitution-permutation network (SPN), and the block size is 64-bit. Although there are two versions with a 80-bit key and a 128-bit key, the 80-bit one is recommended for lighter weight encryption. The energy consumption is around  $5\mu W$  over 32 clock cycles. It computes through 31 rounds as in Fig. 1. This cipher aims hardware optimisation owning small footprints of 1570 gate equivalent (GE) for the 80-bit version and 1886 GE for the 128-bit version. The substitution box (S-box) is a 4-bit to 4-bit which results in 28 GE. The numerical mapping of it as in Table I.

<sup>1</sup>Ultra-lightweight cryptography targets specific areas of algorithms for selective hardware types and or selected cipher sections

TABLE I  
S-BOX MAPPING OF PRESENT BLOCK CIPHER

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

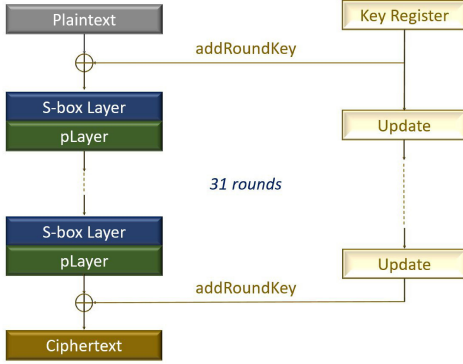


Fig. 1. PRESENT encryption process

## B. Methodology

Initially, a SEMA of data distribution differences was performed for both encryption and non-encryption statuses. The primary resources used here are an oscilloscope (Keysight InfiniiVision MSOX4101A) with 5GSa/s (5 billion samples per second) and NF EMC probes (TekBox H20, H10 and H5) with a 9kHz to 6GHz frequency range. The signals were amplified using a 40dB wide-band amplifier (TekBox TBWA2) before being fetched to the oscilloscope. The encryption was run on an Arduino UNO board. Two probe positions were examined that are in parallel and perpendicular to the chip. MATLAB(r) 2020b software was used for postprocessing data. Regarding the choices of functionalities of the PRESENT:

- 80-bit version is chosen
- The first round of the encryption is considered
- S-box was targeted due to its non-linearity. Thus, it would be easier to identify impacts on waveforms
- The encryption key used is AC DE FB 21 F9 23 75 C0 E6 as same as in [11]

A trigger signal was used to locate the S-box operational area of the waveform by connecting the LED port of the Arduino UNO board to a separate channel of the oscilloscope. Consequently, the usable sampling rate for EM traces was reduced to 2.5GSa/s. The Arduino IDE code used for PRESENT encryption was derived from [23], and its accuracy was verified using test vectors given in [17]. In contrast, MATLAB codes created for trace collection, reconstruction and attack performance were validated using known test data values. Some precautions were taken to enhance the performance by reducing possible system noises and ambient EM interferences. For that:

- A resultant averaged waveform for five encryption cycles was taken per ciphertext

- The setup was lightly covered using Faraday fabrics (low-cost alternative instead of expensive Faraday cages)
- The computer was operated in flight mode
- New frequency components generated as a result of the encryption were filtered

At our current stage, 256 waveforms were collected for 256 different plaintext values, each byte of the plaintext value incrementing from 0x00 to 0xFF in hexadecimal. Firstly, the encryption code was set for the first round, compiled and uploaded on the board. The output of the previous AddRoundKey has to be taken into attention when the S-box function is defined in encryption (Arduino IDE) as well as postprocessing of actual data (MATLAB). Regarding the CEMA, hypothesised calculations for ciphertexts were obtained in MATLAB considering each key byte value from 00 to FF for each plaintext used during encryption. Then, the HW of the ciphertexts were gained as follows.

---

### Algorithm HW calculation of the ciphertexts

---

```

for  $k = 0, 1, 2, \dots, 255$  do
  for  $p = 0, 1, 2, \dots, 255$  do
    Output of AddRound key set input to S-box
    Look up the S-box value
    Calculate HW and save
  end for
end for

```

---

Next, the highest correlation coefficient ( $\rho$ ) values between the HW results and actual data points were calculated per plaintext. Using a graph of the data points versus  $\rho$ , correspondence key values for the highest correlation points were checked. Apart from just the highest correlation branches, the key-value distribution over the graph was analysed to identify potential leakage areas. The pseudo-code for calculation correlation values is shown below.

---

### Algorithm Correlation coefficient calculation

---

```

for  $k = 1, 2, \dots, \text{last data point of waveform}$  do
  Calculate  $\rho$  between arrays of actual data and HW
  if empty then
    Save key value and its  $\rho$  value
  else
    if  $\rho \geq \text{previous}$  then
      Overwrite key value and update  $\rho$  value
    end if
  end if
  Plot graph of data points vs.  $\rho$ 
end for

```

---

## IV. RESULTS AND OBSERVATIONS

### A. SEMA

The parallel position data was often noisy, and it did not reflect any substantial difference between encryption and non-encryption statuses. Regarding the perpendicular position of all magnetic probes, appearing of new frequency elements could be observed at 11.25MHz, 22.5MHz, 45.08MHz, 56.33MHz, 78.83MHz, 90.08MHz and 112.66MHz. Among those, the 45.08MHz component has the highest amplitude and the 56.33MHz owns the second highest. However, increased amplitude of already existing elements during the non-encryption status could be seen at 33.75MHz, 50.62MHz, 67.58MHz, 135.16MHz, 151.87 and 168.98MHz. Histogram plots revealed a slight voltage increase during the encryption.

### B. CEMA

Even though around eight noticeable trough areas appeared in the correlation graphs similar to the power analysis results in [11], a sharpened shape could be gained after filter application. At this phase, bandpass filters were tried regarding all new elements together and the first two highest components individually. The 45.08MHz element illustrated better shapes, and the 56.33MHz one did not show any promising pattern. Correlation graph comparison for some sample data as in Fig. 2. Most of the time, the lowest point of the troughs did not reveal the exact key byte, but the correct key leakage was able to be found somewhere in the lower part of the relevant trough, up to seven bytes which are FB, 21, F9, 23, 75, C0 and E6. A summary of key byte indication as in Table II. In addition, the same method was run on the non-encryption data in order to verify that the notable troughs are due to the encryption impact. No significant correlation difference was there in non-encryption data.

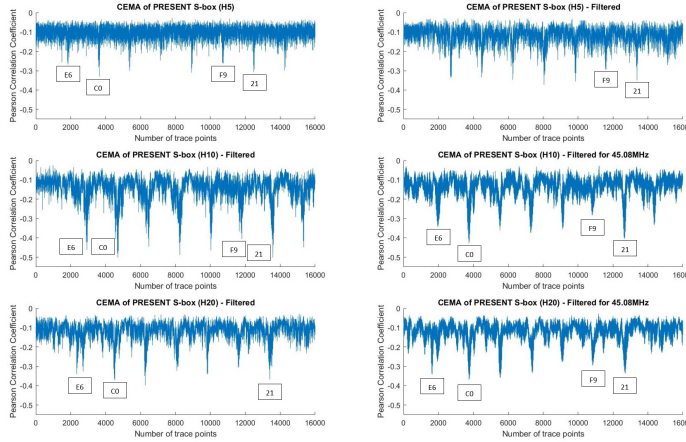


Fig. 2. Result comparison of the CEMA of PRESENT

## V. DISCUSSION

The summary of the results confirms that the encryption has affected the EM emission of the device, and it illustrates a high probability of leaking at least two bytes at once up to seven

bytes. Not having significant troughs regarding non-encryption data verifies the above fact further. In contrast, the potential of the first (E6), the sixth (F9) and the seventh (21) byte leakage is greater as the probability exceeds 50%. The H5 (5mm diameter) probe revealed four bytes, the H10 (10mm diameter) did six bytes and the H20 (20mm diameter) leaked seven bytes. The H5 was able to gain the maximum number of bytes at once (four bytes) without even needing to be filtered, but it could not leak all seven bytes. What is more, the H20 was able to offer all seven bytes, but in individual attempts. This may be due to the fact that probes with larger loops are more sensitive, but have lower frequency resolution. However, extracting the exact bytes correctly is quite challenging because external noise interference cannot be avoided completely in EMA. Nevertheless, changes of frequency selection and filter orders in bandpass filtering caused the location change of indicated bytes most of the time. Therefore, a choice of the most suitable filter type along with its order, as well as the position must be made for optimised results.

According to Fig. 7 of [14], the accuracy of leakage increases when the number of waveforms are increased. However, the possible maximum number of waveform collections may depend on the design of the attack model. [18] mentions that filtering frequencies closer to harmonics of the device clock frequency may increase exactness. Hence, our further steps to enhance the performance by:

- Analysing all affected frequencies individually (newly appearing and amplitude changed ones) and clock frequency harmonics in filtering
- Verifying over the results via the most suitable probe type, filter type, order and frequency range
- Increasing the number of waveforms if possible (up to 2048)
- Increasing the sampling rate up to 5GSa/s if possible
- Calculating the success rate for different key values

At least one-byte leakage of the key reduces processing time considerably in brute force analysis to derive the rest of the bytes. On the other hand, it is extremely difficult for an attacker to locate the functional area when the encryption runs in all 31 rounds with all dependable steps such as addRoundKey, S-box and Player in a black-box environment. This study further verifies that the optimum position of Arduino UNO for EM attack is perpendicular between +5V and GND pins as in [24].

## VI. CONCLUSIONS

IoT devices are struggling to have sufficient security due to their constraints regarding resource adaptability. Also, this smart technology introduces smarter threats and hazards. Thus, the integration of sufficient security mechanisms is challenging. Consequently, lightweight cryptography comes to the rescue. However, lightweight ciphers are emerging and need careful verification over proper analyses before their use in commercial applications. Side-channel attacks are of the utmost importance in physical security because it is a different scenario from algorithmic strength. Our research focuses on EM side-channel resilience against PRESENT

TABLE II  
KEY BYTE LEAKAGE PROBABILITIES

Probability of Leakage								
Key Byte	FB	21	F9	23	43	75	C0	E6
H5	0	33%	60%	6.67%	0	0	20%	46.67%
H10	13.33%	53.33%	66.67%	0	0	6.67%	20%	80%
H20	6.67%	53.33%	46.67%	6.67%	0	13.33%	20%	40%
Probability of Leakage at a Time								
H5	Four bytes: 6.67%		Three bytes: 13.33%		Two bytes: 46.67%		One byte: 13.33%	
H10	Four bytes: 20%		Three bytes: 40%		Two bytes: 13.33%		One byte: 13.33%	
H20	Four bytes: 6.67%		Three bytes: 26.67%		Two bytes: 33.33%		One byte: 20%	

lightweight block cipher. The work initially started from a SEMA and was then enhanced up to a CEMA. There is no other CEMA of the PRESENT existing in the literature. The current results illustrate eight leakage locations with a probability of encryption key leakage up to seven bytes out of ten. This work still continues towards optimisation.

#### REFERENCES

- [1] K. Gremban, "Editorial and Introduction to the Issue: Risk and Rewards of the Internet of Things," *IEEE Internet of Things Magazine (IoTM)*, vol. 1 September, no. 1, p. 2, Sep. 2018. [Online]. Available: <https://www.comsoc.org/publications/magazines/ieee-internet-things-magazine>
- [2] N. A. Gunathilake, A. Al-Dubai, and W. J. Buchanan, "Internet of Things: Concept, Implementation and Challenges," in *International Conference on IoT and its Applications (ICIA)*. Jamshedpur, India: Springer, Dec. 2020, due to be published by Springer. [Online]. Available: [https://www.researchgate.net/publication/347987943\\_Internet\\_of\\_Things\\_Concept\\_Implementation\\_and\\_Challenges](https://www.researchgate.net/publication/347987943_Internet_of_Things_Concept_Implementation_and_Challenges)
- [3] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications," in *IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Republic of Ireland, Apr. 2019, pp. 707–710, doi: 10.1109/WF-IoT.2019.8767250.
- [4] N. A. Gunathilake, A. Al-Dubai and William J. Buchanan, "Recent Advances and Trends in Lightweight Cryptography for IoT Security," in *16th International Conference on Network and Service Management (CNSM)*, Izmir, Turkey, Nov. 2020, pp. 1–5, doi: 10.23919/CNSM50824.2020.9269083.
- [5] N. A. Gunathilake, A. Al-Dubai, W. J. Buchanan, and O. Lo, "Electromagnetic Analysis of an Ultra-lightweight Cipher: PRESENT," in *10th International Conference on Cryptography and Information Security (CRYPIS) - ACCEPTED*, Sydney, Australia, Jun. 2021.
- [6] W. Li, "An Ultra-Lightweight Side-Channel Resistant Crypto for Pervasive Devices," in *International Journal of Multimedia and Ubiquitous Engineering*, vol. 10, no. 11, 2015, pp. 173–186, doi: 10.14257/ijmue.2015.10.11.17.
- [7] "On Implementation Security and ISAP v2.0." [Online]. Available: <https://csrc.nist.gov/CSRC/media/Presentations/updates-on-the-implementation-security-of-isap/images-media/session-5-primas-implementation-security-ISAP.pdf>
- [8] A. Heuser, S. Picek, S. Guilley, and N. Mentens, "Side-Channel Analysis of Lightweight Ciphers: Does Lightweight Equal Easy?" in *Radio Frequency Identification and IoT Security*, G. P. Hancke and K. Markantonakis, Eds., 2017, pp. 91–104, doi: 10.1007/978-3-319-62024-4\_7.
- [9] X. Duan, Q. Cui, S. Wang, H. Fang, and G. She, "Differential Power Analysis Attack and Efficient Countermeasures on PRESENT," in *8th IEEE International Conference on Communication Software and Networks (ICCSN)*, 2016, pp. 8–12, doi: 10.1109/ICCSN.2016.7586627.
- [10] J. Zhang, D. Gu, Z. Guo, and L. Zhang, "Differential Power Cryptanalysis Attacks against PRESENT Implementation," in *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, vol. 6, 2010, pp. V6–61–V6–65, doi: 10.1109/ICACTE.2010.5579367.
- [11] O. Lo, W. J. Buchanan, and D. Carson, "Correlation Power Analysis on the PRESENT Block Cipher on an Embedded Device," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*. Hamburg, Germany: Association for Computing Machinery, 2018, doi: 10.1145/3230833.3232801.
- [12] D. Shanmugam, R. Selvam, and S. Annadurai, "Differential Power Analysis Attack on SIMON and LED Block Ciphers," in *Security, Privacy and Applied Cryptography Engineering (SPACE)*, R. S. Chakraborty, V. Matyas, and P. Schaumont, Eds., vol. 8804. Springer International Publishing, 2014, doi: 10.1007/978-3-319-12060-7.
- [13] A. Biryukov, D. Dinu, and J. Großschädl, "Correlation Power Analysis of Lightweight Block Ciphers: From Theory to Practice," in *Applied Cryptography and Network Security*, M. Manulis, A.-R. Sadeghi, and S. Schneider, Eds. Springer International Publishing, 2016, pp. 537–557.
- [14] Y. Nozaki, T. Iwase, Y. Ikezaki, and M. Yoshikawa, "Differential Electromagnetic Analysis for PRESENT and its Evaluation with Several Selection Functions," *Journal of International Council on Electrical Engineering*, vol. 7, no. 1, pp. 137–141, Jun. 2017, doi: 10.1080/22348972.2017.1344014.
- [15] M. Yoshikawa and Y. Nozaki, "Electromagnetic analysis attack for a lightweight cipher PRINCE," in *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 2016, pp. 1–6, doi: 10.1109/ICCCF.2016.7740423.
- [16] M. Yoshikawa, Y. Nozaki, and K. Asahi, "Electromagnetic analysis attack for a lightweight block cipher TWINE," in *IEEE/ACIS International Conference on Wireless Information Technology and Systems (ICWITS) and Applied Computational Electromagnetics (ACES)*, 2016, pp. 1–2, doi: 10.1109/ROPACES.2016.7465354.
- [17] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. VIKKELSOE, "PRESENT: An Ultra-Lightweight Block Cipher," in *Cryptographic Hardware and Embedded Systems (CHES)*, P. Paillier and I. Verbauwhede, Eds. Springer, Berlin, Heidelberg, 2007, pp. 450–466, doi: 10.1007/978-3-540-74735-2\_31.
- [18] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "A Survey of Electromagnetic Side-channel Attacks and Discussion on their Sase-Progressing Potential for Digital Forensics," *Digital Investigation*, vol. 29, p. 43–54, Jun. 2019, doi: 10.1016/j.diin.2019.03.002.
- [19] G. L. Ding, J. Chu, L. Yuan, and Q. Zhao, "Correlation Electromagnetic Analysis for Cryptographic Device (PACCS)," in *Pacific-Asia Conference on Circuits, Communications and Systems*, 2009, pp. 388–391, doi: 10.1109/PACCS.2009.144.
- [20] A. Lakshminarasimhan, "Electromagnetic Side-Channel Analysis for Hardware and Software Watermarking," Feb. 2011, masters Thesis 1911 - 02 - 2014.69. [Online]. Available: <https://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1822&context=theses>
- [21] ISO/IEC ICS 35.030 IT Security, "Information Security — Lightweight Cryptography," *ISO/IEC JTC 1/SC 27 Information security, Cybersecurity and Privacy Protection*, Nov. 2019. [Online]. Available: <https://www.iso.org/standard/78477.html>
- [22] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, "Report on Lightweight Cryptography," *National Institute of Standards and Technology*, Mar. 2017, doi: 10.6028/NIST.IR.8114.
- [23] lightweightcrypto.org. (2017) C PRESENT Implementation (8bit). Bochum, Germany. Accessed: 05.09.2020. [Online]. Available: [http://www.lightweightcrypto.org/downloads/implementations/PRESENT08-bit\\_implementation.rar](http://www.lightweightcrypto.org/downloads/implementations/PRESENT08-bit_implementation.rar)
- [24] P. Robyns. (2019, Feb.) Performing Low-cost Electromagnetic Side-Channel Attacks using RTL-SDR and Neural Networks. Brussels, Belgium. Accessed: 10.02.2020. [Online]. Available: <https://youtu.be/cs08QSIbp-A>