Data Confidentiality for IoT Networks: Cryptographic Gaps and Physical-Layer Opportunities

Marcus de Ree*, Georgios Mantas*†, Jonathan Rodriguez*‡, Saud Althunibat§, Marwa K. Qaraqe¶, Abdullah Alhasanat§, Saif M. Al-Kuwari¶, Moath Alsafasfeh§, Gabriele Oligeri¶, Seda Tusha¶, Muhammad Usman¶, Fatima Abu Taha§, Samiha Alfalahat§, Tasneem Alshamaseen§, and Malak Qaisi§

*Mobile Systems Group, Instituto de Telecomunicações, Aveiro, Portugal
†Faculty of Engineering and Science, University of Greenwich, Chatham Maritime, UK
‡Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd, UK
§Faculty of Engineering, Al-Hussein Bin Talal University, Ma'an, Jordan
¶College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar
Email: mderee@av.it.pt, gimantas@av.it.pt, jonathan@av.it.pt, saud.althunibat@ahu.edu.jo, mqaraqe@hbku.edu.qa

***Abstract*—The conventional solution for providing data confidentiality is by means of encryption (a branch of cryptography). However, encryption schemes are generally designed to provide a certain level of security without necessarily taking resource consumption into account. This poses an issue for Internet of Things (IoT) devices which are limited in terms of storage capacity and computational capabilities. In this paper, we discuss the capabilities of cryptographic solutions for providing data confidentiality and we evaluate whether these solutions are appropriate for IoT networks in terms of resource consumption. Based on the identified drawbacks of cryptographic solutions, we discuss opportunities within the area of physical-layer security (PLS). Finally, we provide an overview of PLS schemes which aim to enhance data confidentiality in IoT networks.**

***Index Terms*—Cryptography, Data Confidentiality, Information Security, Internet of Things, Physical-Layer Security**

I. Introduction

The Internet of Things (IoT) represents the idea of connecting physical objects with the internet. The aim is to enhance the quality of lives by embedding perception abilities in physical objects to sight, hear, touch, talk together and share information, hence transforming them to smart objects. IoT has proven their significance in many domains such as healthcare, transportation, industrial automation, agriculture, military applications, and public safety [1]. In the near future, it is expected that IoT will significantly contribute to the overall quality of life and global economy, which will open the doors for many businesses and applications. Namely, 45% of the internet traffic is estimated to come from machine-to-machine (M2M)-type communication by as early as 2022 [2]. It is estimated that there will be 30.9 billion active connections of IoT devices, with an overall economic impact in the range of $2.7 to $6.2 trillion, by 2025 [3].

Internet connected IoT devices are limited in terms of energy and hardware resources but sometimes deployed in very sensitive locations and scenarios. This puts stringest requirements on the security and privacy of deployed devices and the collected data. Unfortunately, the resource scarcity coupled with profit-driven businesses have stimulated manufacturers to potentially design vulnerable devices. This has opened the doors for adversaries to exploit those devices and access sensitive information with little to no effort [4]. One examples relates to the incident where the wireless interface of the pacemaker on US Vice President Dick Cheney got disabled [5]. The Domain Name System (DNS) provider Dyn suffered from an attack from IoT-specific malware, called Mirai, which caused the company to lose 8% of its customer base [6]. Such security incidents can potentially limit confidence over the huge deployment of IoT networks.

In general, security is a broad term that encompasses several properties that must be provided in order to achieve end-to-end security in any information network. One important security property is data confidentiality. To achieve data confidentiality, the contents of the data must only be exposed to personnel which has been authenticated by some mechanism prior to accessing the data. The confidentiality of the data must be ensured at rest (i.e., storage) and in transit (i.e., during transmission). Generally, confidentiality is achieved through encryption; however, in the context of IoT, ensuring confidentiality becomes a challenge due to the large number of devices and their resource constraints. On the one hand scalability becomes a challenge, while on the other hand devices' resources hinders to directly apply conventional encryption schemes in the IoT.

In this paper, we take a closer look into the capabilities and limitations of cryptographic solutions as well as physical-layer solutions for providing data confidentiality in IoT networks. In section II, we examine the capabilities and limitations of cryptographic solutions. In section III, we examine the capabilities and limitations of physical-layer security (PLS) solutions. Finally, we conclude this paper in section IV.

This research was sponsored [in part] by the NATO Science for Peace and Security Programme under grant [SPS G5797].

II. Data Confidentiality through Cryptography

The conventional solution for providing data confidentiality in wireless communication is by means of cryptography. Cryptographic solutions can be separated as symmetric key cryptography and asymmetric key cryptography (i.e., public key cryptography). Table I presents a comparison between these two types.

TABLE I
A comparison between symmetric and asymmetric key cryptography.

Attribute	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key	The same key is used for encryption and decryption	A pair of keys is used (i.e., a public and private key)
Key Exchange	Out-of-band	In-band
Algorithm Complexity	Less complex and faster	Complex and slower
Size of the Ciphertext	Equal to the plaintext	Equal or larger than the plaintext
Examples of Encryption Algorithms	AES	ECC, McEliece, NTRU

A. Symmetric Key Cryptography

Symmetric key cryptography, the cryptographic infrastructure in which both communicating parties share a unique key that can be used for encryption and decryption, is well-known for its ability to provide data confidentiality with a relatively low consumption footprint. However, it suffers from limitations in terms of key distribution and management, especially for large-scale networks [7].

Authenticated Key Exchange. Authentication and key establishment are fundamental pre-requisites in setting up secure communication between two or more users. However, these two steps are generally intertwined. There are two kinds of schemes that arrange an authenticated exchange of symmetric keys:

- *Key pre-distribution* relies on an in-band key exchange to securely, and in an authenticated manner, distribute long-lived symmetric keys to any pair of users. The use of a particular symmetric key informs both users who they are communicating with.
- *Session key distribution* relies on a key distribution center (KDC) which every user shares a pre-distributed long-lived symmetric key with. This key enables secure communication between a user and the KDC and it allows any user to request the KDC for the secure distribution of a short-lived symmetric key (i.e., session key) with any other user on-demand.

Both schemes require some physical (i.e., out-of-band) process that involves both authentication along with a pre-distribution of long-lived symmetric keys. This requirement is known as the *key distribution problem*. Both schemes also suffer from scalability and interoperability issues [8], and are therefore mainly used in closed environments. These solutions may still be suitable for smart homes or industrial IoT (IIoT) networks, but not for general IoT applications in which devices have no initial knowledge of each other nor can they establish a pre-distributed key.

Lightweight Symmetric Encryption Algorithms. The main advantage of symmetric encryption algorithms over asymmetric encryption algorithms is their computational efficiency. These algorithms (i.e., ciphers) can be designed for implementation in software (i.e., code running on a specific processor or micro-controller), in hardware (i.e., full-custom chip-design, generally using application specific integrated circuits (ASIC) or a field programmable gate array (FPGA) technology), or in both [9]. The variety of implementation platforms complicates the efficiency comparison [10]. The design of lightweight ciphers has been an active area of research since 2005 [11], composed of block ciphers and stream ciphers.

- *Block ciphers* operate on fixed-length strings (i.e., blocks) of plaintext bits that are encrypted using the same key. The advanced encryption standard (AES) [12] is perhaps the most well-known block cipher. Novel variants of AES, presented in [13] and [14], made improvements for implementation in resource constrained devices.
- *Stream ciphers* operate on individual plaintext bits that are encrypted with a so-called keystream. This keystream can be constructed from the key itself or by combining the key with plaintext bits. Some noteworthy stream ciphers resulted from the eSTREAM project [15] that targeted to deliver a small portfolio of promising stream ciphers with a better performance than AES in CTR (stream cipher) mode.

Stream ciphers were thought to offer substantial advantages in resource constrained applications, but this claim was rejected in [16]. Even more, [17] stated that stream ciphers are often considered inferior to block ciphers. Despite the continuous development of lightweight ciphers, [18] concluded that AES remains the preferred choice for provisioning security.

Standardization Efforts. A variety of standardized encryption schemes that are deployed today, such as AES, were developed as part of international competitions initiated by the National Institute of Standards and Technology (NIST). Unfortunately, the competition which led to the development of AES did not consider the strict requirements of resource constrained devices in IoT networks. Therefore, NIST launched a competition in 2015 for the development of lightweight cryptographic solutions that are suitable for securing sensor networks, healthcare, distributed control systems, as well as the IoT [19]. As of March 29, 2021, the competition reached the final round with ten candidates remaining of which the winners are expected to be announced in early 2022. It is worth mentioning that the proposals for lightweight encryption schemes are all based on symmetric key cryptography and most of these are block ciphers.

B. Asymmetric Key Cryptography

The concept of asymmetric key cryptography was first proposed by Diffie and Hellman in 1976 [20]. This approach of cryptography was presented as a solution to the key distribution problem. As discussed previously, securely sharing a key is often problematic as it usually requires physical interaction. Asymmetric key cryptography solves this problem by allowing every user to generate a pair of mathematically linked keys, a private key, and a corresponding public key. The private key is kept secret whereas the public key can be openly shared.

Authenticated Key Exchange. Asymmetric key cryptography and its key exchange schemes are known for its scalability properties. These schemes are therefore adopted in the Internet, as they allow two or more users to establish secure communication without requiring them to have any initial knowledge of each other.

- *Key transport schemes* utilizes a trusted third party (TTP) (e.g., certification authority, private key generator) to establish a pair of mathematically linked keys, the public key and the private key. In an authenticated manner (e.g., through signature verification on public key certificates in PKI), the public key can be disseminated and used by any other user that wishes to securely communicate with the owner of that public key. Any user can use the public key to encrypt and transmit the encrypted data whereas only the owner of the corresponding private key can decrypt the message [21].
- *Key agreement schemes* are similar to key transport schemes in the sense of utilizing a TTP to establish a public and private key pair. However, instead of utilizing the public key in encryption algorithms to secure communication, the public key are used in a key agreement protocol. This protocol results in the establishment of a unique key that will only be known by the participating users. This key is symmetric, and can therefore be used in lightweight symmetric encryption algorithms [21].

Due to the mathematical structure that the key pairs are based on, both schemes involve heavy computations [7]. Providing data confidentiality through key transport schemes is considered resource intensive due to the constant use of asymmetric encryption and decryption algorithms. The main advantage of key agreement schemes is its ability to enable key distribution in large-scale IoT networks while simultaneously allowing data confidentiality to be provided through lightweight symmetric ciphers.

Lightweight Asymmetric Encryption Schemes. The performance of asymmetric encryption (and decryption) algorithms is closely related to the underlying intractable computational problem (e.g., integer factorization, discrete logarithm problem) since it specifies the size of the domain, key parameters, and arithmetic operations (e.g., addition, multiplication, exponentiation, bilinear pairings) [21]. The following asymmetric cryptosystems have been proposed for constrained devices [7].

- *Rabin's Cryptosystem* [22] is known for its efficient encryption algorithm compared to its decryption counterpart. This asymmetry could be beneficial for IoT networks where resource constrained devices encrypt the data while decryption is performed by a more powerful device [23]. Schemes were proposed for wireless sensor networks (WSNs) [24], but has not been promoted in more recent literature.
- *Elliptic Curve Cryptosystem* [25] is known for its performance for achieving higher levels of bit-security. It was demonstrated in [16] that ECC allows for compact implementations and claimed that optimized software algorithms enable ECC operations below one second for 80-bit security on resource constrained devices. ECC is the most suitable asymmetric cryptosystem for constrained devices according to [18].
- *McEliece's Cryptosystem* [26] is notorious for its large key sizes. Its encryption and decryption algorithms are very fast [27], even for large key sizes, but received little attention for network with constrained devices due to its memory storage requirement.
- *NTRU Cryptosystem* [28] relies on lattice-based operations which are considered relatively efficient. In comparison to RSA or ECC, evaluations from [23], [29] show that NTRU is quite fast and involve less consumption on different devices including FPGAs and microcontrollers. Its main drawback is message expansion, causing additional power consumption for data transmission [23].

The performance gap between symmetric encryption algorithms and asymmetric encryption algorithms was quantified in [16] and [18]. It was stated that an optimized ECC algorithm may still perform 100 to 1,000 times slower than a standard symmetric cipher such as AES. This correlates to a two- to three orders of magnitude higher power consumption [16].

C. Concluding Remarks

The limited hardware, low-complexity, and energy constraints of IoT devices along with the scalability of IoT networks presents unique challenges to the development of lightweight solutions. The most lightweight cryptographic solution would be to utilize asymmetric key cryptography for the purpose of key distribution, a key agreement protocol to enable the establishment of pairwise symmetric keys, and then take advantage of the performance benefits of symmetric encryption algorithm to provide data confidentiality. This "lightweight" solution would still suffers from having to utilize complex and energy inefficient procedures. Instead, physical-layer solutions may be able to provide data confidentiality with a reduced complexity requirement. For example, physical-layer techniques may enable the establishment of a symmetric key for any pair of devices, effectively replacing the establishment of asymmetric keys, the exchange and verification of the legitimacy of the public keys, and the execution of a key agreement protocol. Therefore, robust PLS methods may supplement or replace cryptographic solutions to enhance data confidentiality at minimal expense.

III. Data Confidentiality through Physical-Layer Security

PLS schemes present an alternative for providing data confidentiality by exploiting the random, unique, and natural fingerprints in wireless fading channels between the transmitter and the intended receiver [30]. Encoding and decoding schemes are based on physical-layer parameters such as modulation type, channel coding, and symbol mapping. Providing data confidentiality via PLS has become more and more popular, especially for securing IoT network scenarios, but still requires significant research efforts prior to its adoption [31]. It it worth mentioning that not all available PLS solutions comply with IoT systems. As an example, many modern communication systems possess multiple antennas and can therefore benefit from the inherent degrees-of-freedom, whereas IoT devices are generally limited to a single antenna.

We identified four main categories to provide data confidentiality in IoT systems through PLS: (i) signal source indistinguishability, (ii) channel coding, (iii) artificial noise, and (iv) unique signal design. In this section, we explore the significant PLS solutions proposed for each category.

A. Signal Source Indistinguishability Approaches

The signal source indistinguishability approaches rely on the intrinsic challenge of mapping an over-the-air radio signal to the actual transducer. If we assume an anonymous transmission (i.e., no local identifiers have been used to link the message to the transmitter), mapping the radio signal to its transmitter is a challenging task. This approach is also interesting for its ability to generate shared secret keys, thus enforcing confidentiality.

A preliminary scheme was presented in [32] where each radio signal is adopted to probabilistically establish one secret bit. The bit value is complemented as a function of the transmitted identity, thus allowing only the transmitter and receiver to correctly decode (complement) its value. If the eavesdropper cannot associate the signal to the source, it does not know whether to complement the bit value. This scheme was designed for pairs of users and has been extended in [33] to suit a network-wide environment.

Another scheme [34] uses a full duplex transducer to transmit and receive on two randomly chosen frequencies. The pair of users experience one of two possible scenarios: a collision when both the transmitter and receiver are on the same frequency, or a successful exchange. In the second case, only the two users are aware of the allocation of the two frequencies, i.e., the one is used for transmitting and the one for receiving, and therefore they can exploit this uncertainty to generate one secret bit.

All source indistinguishability-based schemes suffer from attacks that attempt to locate one or more users involved in the protocol. As soon as localization of a user leaks its identity, i.e., identification via localization, the generation of the bit is no longer secret. This attack can be deployed with classical localization techniques such as triangulation and trilateration, but requires an adversary to deploy multiple sensors in the area.

B. Channel Coding Approaches

Channel coding schemes play a key role in PLS-based approaches, especially in case the channel of the intended user is more powerful than that of an eavesdropper. In channel coding-based approaches, the data is encoded by the transmitter using a unique error-correcting code in such a way that the intended receiver is capable of decoding. Any eavesdropper, generally suffering from a degraded channel, would be unable to correctly decode the data.

The authors of [35] investigated the fundamental limits and coding methods of the wiretap channel from an information-theoretic perspective. The authors presented a way of exploiting the capacity achieving codes to achieve secrecy capacity. This is achieved using the codes capable of achieving the eavesdropper's capacity. In particular, the authors verified the feasibility of designing linear time decodable secrecy codes exploiting low density parity check (LDPC) codes. The main channel is assumed to be noiseless while the wiretap channel is considered as a binary erasure channel (BEC). This work was extended in [36], proposing a secure coding scheme for a type II wiretap channel where the wiretap channel is a memoryless binary-input output-symmetric (MBIOS) channel.

The work presented in [37] proposes an LDPC code-based coding scheme for the Gaussian wiretap channel and exhibits certain practical features. Namely, the scheme is applicable to finite block length, encodable in linear time, and can be combined with existing cryptographic protocols to minimize the security gap. The authors define the security gap as a measure of separation between thresholds of reliability and security of error-correcting codes. The authors presented the security gap as low as a few dB, which seems to be an improvement over conventional error-correcting codes.

The authors in [38] proposed a polar code-based coding scheme that works for a wide range of wiretap channels achieving secrecy capacity, provided that both the main and wiretap channels are symmetric and binary input and that the wiretap channel is degraded with respect to the main channel. In addition, the authors provide a modified version of the proposal which has stronger security and achieves secrecy capacity. However, the main channel must be noiseless to ensure reliability. This work was extended in [39] with the aim to provide strong security and reliability. To solve this problem, the authors considered multi-block polar codes that guarantee strong reliability and security under the assumption of a symmetric and degraded wiretap channel.

C. Artificial Noise Approaches

In this category, artificial noise (AN) is added to the transmitted data symbols by the transmitter [40] or by a third cooperative party [41] with the aim of degrading the channel quality of the eavesdropper. The added AN will be in the null space of the intended receiver's channel to prevent its channel from degrading.

In [42], the secrecy outage probability (SOP), (i.e., the probability that secret data is successfully decoded by an eavesdropper) is investigated for a two-hop IoT network in

the presence passive eavesdroppers. Two types of eavesdroppers are considered, colluding and non-colluding. It has been shown that collusion can significantly increase the SOP, while cooperative jamming can enhance the confidentiality of the transmitted data.

Authors in [43] considered the SOP minimization problem in a two-node IoT system in the presence of a cooperative jammer and an eavesdropper. The cooperative jammer is placed to help secure the transmission link by generating jamming signals to confuse the eavesdropper. The secrecy outage is minimized by optimizing the power allocation and secrecy rate thresholds. This scheme is limited in the sense that the eavesdroppers' channel state information (CSI) is assumed to be available.

In [44], the secrecy performance of a download IoT system is investigated where IoT nodes support simultaneous wireless information and power transfer (SWIPT). Unlike other cooperative jamming techniques, this work assumes that each node supports full duplex, and hence, it uses the harvested energy to emit a jamming signal to confuse eavesdroppers. Two multiple access schemes have been considered; orthogonal frequency division multiple access (OFDMA) and time division multiple access (TDMA), and the problem of resource allocation has been formulated to maximize the sum secrecy rate. Suboptimal mathematical solutions have been presented for scenarios with and without CSI at the transmitter. The main finding of this work is represented by the superior performance of OFDMA as compared to TDMA in terms of the sum secrecy rate.

D. Unique Signal Design

This category is based on the used methodology for performing modulation and symbol mapping at the transmitter side. Symbol constellation rotation at the transmitter side is one fundamental technique for providing data confidentiality. The legitimate receiver can reverse the constellation rotation and then perform symbol detection. The index modulation (IM) concept can also be considered under this category from the perspective of symbol mapping.

The authors of [45] proposed a choatic compressed sensing (CS) mechanism to ensure low-cost sampling while preserving data confidentiality in Internet of Multimedia Things networks. Firstly, multiple images are sampled based on the measurement matrix generated chaos. The multiple measurements are rearranged into a master image. Then, the master image is permuted using an Arnold transform to produce the encrypted image. Finally, the encrypted result is diffused using single value diffusion. In this way, batch processing of multimedia big data is allowed while confidentiality is preserved through a permutation-diffusion procedure.

In [46], the authors propose a relay-aided vectorized (RAV) scheme to protect downlink communication in IoT networks under pilot contamination attacks. In this attack, an adversary is able to emulate the channel estimation pilot signals and send them back in reverse link to emulate a legitimate receiver. The proposed approach is based on scrambling data symbols among multiple transmit antennas and multiple transmission times. It also relies on a relay to enhance signal reconstruction, and hence, the secrecy performance at the legitimate receiver while limiting interception at the eavesdropper.

Authors in [47] studied the secure transmission with diverse communication requirements in IoT networks using non-orthogonal multiple access (NOMA). Specifically, one considered user is a delay-sensitive user (DSU) while a second is a security-required user (SRU). According to the NOMA principle, the DSU is viewed as a weak user (i.e., bad channel condition) and should be allocated with more power. To evaluate the performance, authors derived the SOP and the effective secrecy throughput (EST) of the SRU. They showed that the performance of their NOMA scheme performed better than the orthogonal multiple access schemes in terms of the EST and SOP.

E. Concluding Remarks

The applicability of many covered PLS schemes is questionable in terms of practical deployments in general purpose IoT networks due to the induced overhead or assumptions about the eavesdropper's location, the number of eavesdroppers, instantaneous channel characteristics, channel statistics, or node mobility.

IV. Conclusions

The confidence in cryptographic security solutions and the maturity of the field will likely make encryption the default solution for providing data confidentiality, even for IoT networks. This claim can be supported by the current standardization efforts from bodies such as NIST. Even though these efforts are useful and potentially applicable for resource constrained devices in IoT networks, the main performance bottleneck (i.e., the secure and authenticated distribution of cryptographic keys) remains problematic. This bottleneck may not have a lightweight cryptographic solution and thus leaves a gap which may be filled by a lightweight physical-layer solution. Thus, a hybrid solution which combines the strengths of cryptography and unique physical-layer parameters has the potential to provide data confidentiality with reduced resource consumption for general purpose IoT networks.

The examined literature proposes a variety of PLS approaches for providing data confidentiality in IoT networks. Many of these approaches would even be able to achieve data confidentiality independent of cryptographic solutions. However, many of the proposed PLS schemes still suffer from (i) significant overhead requirements, (ii) impractical assumptions related to the eavesdropper, or (iii) impractical assumptions related to the network model (e.g., the assumption of a static network even though many IoT networks have a dynamic topology), limiting their practicality. Novel and practical PLS schemes, aligning with the resources and capabilities of IoT nodes, must be designed which limits the overhead requirement and are based on more appropriate assumptions.

References

[1] A. Al-Faqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commum. Surveys Tuts.*, vol. 17, no. 4, pp. 2347-2376, 2015.

[2] S. Taylor, "The Next Generation of the Internet Revolutionizing the Way We Work, Live, Play, and Learn," CISCO, San Francisco, CA, USA, 2013.

[3] J. Manyika *et al.*, "Disruptive Technologies: Advances that will Transform Life, Business, and the Global Economy," McKinsey Global Institute, 2013.

[4] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghabi, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Imperical Look on Internet-Scale IoT Exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702-2733, 2019.

[5] G. Kolata. "Of Fact, Fiction and Cheney's Defibrillator". The New York Times. https://www.nytimes.com/2013/10/29/science/of-fact-fiction-and-defibrillators.html (accessed May 17, 2021).

[6] S. Weagle. "Financial Impact of Mirai DDoS Attack on Dyn Revealed in New Data". Corero. https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html (accessed Apr. 28, 2021).

[7] H. Hellaoui, M. Koudil, and A. Bouabdallah, "Energy-Efficient Mechanisms in Security of the Internet of Things: A Survey," *Comput. Netw.*, vol. 127, pp. 173-189, 2017.

[8] A. F. Skarmeta, J. L. Hernández-Ramos, and M. V. Moreno, "A Decentralized Approach for Security and Privacy Challenges in the Internet of Things," in *IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, South Korea, pp. 67-72, Mar. 2014.

[9] B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, "A Survey on Lightweight Block Ciphers for Low-Resource Devices: Comparative Study and Open Issues," *J. Netw. Comput. Appl.*, vol. 58, pp. 73-93, 2015.

[10] S. Kerckhof, F. Durvaux, C. Hocquet, D. Bol, and F.-X. Standaert, "Towards Green Cryptography: A Comparison of Lightweight Ciphers from the Energy Viewpoint," in *Int. Wksp. Cryptographic Hardware and Embedded Systems (CHES)*, Leuven, Belgium, pp. 390-407, Sep. 2012.

[11] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A Review of Lightweight Block Ciphers," *Journal of Cryptographic Engineering*, vol. 8, pp. 141-184, 2018.

[12] National Institute of Standards and Technology (NIST), "Announcing the Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, 2001.

[13] M. Feldhofer, J. Wolkenstorfer and V. Rijmen, "AES Implementation on a Grain of Sand," *IEE Proceedings - Information Security*, vol. 152, no. 1, pp. 13-20, 2005.

[14] A. Moradi, A. Poschman, S. Ling, C. Paar, and H. Wang, "Pushing the Limits: A Very Compact and a Threshold Implementation of AES," in *Int. Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, Tallinn, Estonia, pp. 69-88, May 2011.

[15] eCRYPT. "The eSTREAM Portfolio". https://www.ecrypt.eu.org/stream/ (accessed, May 23, 2021).

[16] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A Survey of Lightweight-Cryptography Implementations," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522-533, 2007.

[17] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos, "Lightweight Cryptography for Embedded Systems - A Comparative Analysis," in *Int. Wksp. Data Privacy Management (DPM), Autonomous and Spontaneous Security (SETOP)*, Egham, UK, pp. 333-349, Sep. 2013.

[18] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT," *Wireless Personal Communications*, vol. 112, pp. 1947-1980, 2020.

[19] L. Bassham *et al.*. "Lightweight Cryptography". https://csrc.nist.gov/projects/lightweight-cryptography (accessed May 19, 2021).

[20] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[21] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001.

[22] M. O. Rabin, "Digitalized Signatures and Public Key Functions as Intractable as Factorization," Massachusetts Institute of Technology, Cambridge, MA, USA, pp. 1-16, Jan. 1979.

[23] G. Gaubatz, J.-P. Kaps, E. Öztürk, and B. Sunar, "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," in *Int. Conf. Pervasive Computing and Communications Wksp. (PerCom)*, Kauai, HI, USA, pp. 146-150, Mar. 2005.

[24] Y. Oren, and M. Feldhofer, "A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes," in *ACM Conf. Wireless Network Security (WiSec)*, Zurich, Switzerland, pp. 59-68, Mar. 2009.

[25] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987.

[26] R. J. McEliece, "A Public-Key Cryptosystem based on Algebraic Coding Theory," in *The Deep Space Network: Progress Report 42-44*, National Aeronautircs and Space Administration, Pasadena, CA, USA, pp. 114-116, 1978.

[27] T. Eisenbarth, T. Güneysu, S. Heyse, and C. Paar, "MicroEliece: McEliece for Embedded Devices," in *Int. Wksp. Cryptographic Hardware and Embedded Systems (CHES)*, Lausanne, Switzerland, pp. 49-64, Sep. 2009.

[28] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A Ring-based Public Key Cryptosystem," in *Int. Algorithmic Number Theory Symp. (ANTS)*, Portland, OR, USA, pp. 267-288, Jun. 1998.

[29] G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public Key Cryptography in Sensor Networks - Revisited," in *European Wksp. Security in Ad-Hoc and Sensor Networks (ESAS)*, Heidelberg, Germany, pp. 2-18, Aug. 2004.

[30] A. Chorti, C. Hollanti, J.-C. Belfiore and H. V. Poor, "Physical Layer Security: A Paradigm Shift in Data Confidentiality," in *Physical and Data-Link Security Techniques for Future Communication Systems*, Springer, Cham, pp. 1-15, 2016.

[31] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773-1828, 2019.

[32] G. Di Pietro and G. Oligeri, "COKE Crypto-Less Over-the-Air Key Establishment," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 163-173, 2013.

[33] S. Sciancalepore, G. Oligeri, G. Piro, G. Boggia, and R. Di Pietro, "EXCHANge: Securing IoT via Channel Anonymity," *Computer Communications*, vol. 134, pp. 14-29, 2019.

[34] M. Usman, S. Raponi, M. Qaraqe, and G. Oligeri, "KaFHCa: Key-Establishment via Frequency Hopping Collisions," arXiv:2010.09642 [cs], 2020.

[35] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin and J.-M. Merolla, "Applications of LDPC Codes to the Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933-2945, 2007.

[36] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure Nested Codes for Type II Wiretap Channels," in *IEEE Information Theory Wksp. (ITW)*, Tahoe City, CA, USA, pp. 337-342, Sep. 2007.

[37] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC Codes for the Gaussian Wiretap Channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532-540, 2011.

[38] H. Mahdavifar and A. Vardy, "Achieving the Secrecy Capacity of Wiretap Channels using Polar Codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428-6443, 2011.

[39] E. Sasoglu and A. Vardy, "A New Polar Coding Scheme for Strong Security on Wiretap Channels," in *IEEE Int. Symp. Information Theory (ISIT)*, Istanbul, Turkey, pp. 1117-1121, Jul. 2013.

[40] X. He and A. Yener, "Secure Degrees of Freedom for Gaussian Channels with Interference: Structured Codes outperform Gaussian Signaling," in *IEEE Global Telecommunications Conf. (GLOBECOM)*, Honolulu, HI, USA, pp. 1-6, Nov. 2009.

[41] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019, 2008.

[42] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On Secure Wireless Communications for IoT under Eavesdropper Collusion," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 3, pp. 1281-1293, 2016.

[43] L. Hu *et al.*, "Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219-228, 2018.

[44] D. Xu and H. Zhu, "Secure Transmission for SWIPT IoT Systems with Full-Duplex IoT Devices," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10915-10933, 2019.

[45] Y. Zhang *et al.*, "Low-Cost and Confidentiality-Preserving Data Acquisition for Internet of Multimedia Things," *IEEE Internet Things J.*, vol 5., no. 5, pp. 3442-3451, 2018.

[46] N. Zhang, R. Wu, S. Yuan, and D. Chen, "RAV: Relay Aided Vectorized Secure Transmission in Physical Layer Security for Internet of Things under Active Attacks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8496-8506, 2019.

[47] Z. Xiang *et al.*, "Secure Transmission in a NOMA-Assisted IoT Network with Diversified Communication Requirements," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 11157-11169, 2020.