A Cryptographic Perspective to Achieve Practical Physical Layer Security

Marcus de Ree*, Georgios Mantas*†, Jonathan Rodriguez*‡
*Mobile Systems Group, Instituto de Telecomunicações, 3810-193 Aveiro, Portugal
†Faculty of Engineering and Science, University of Greenwich, Chatham Maritime ME4 4TB, U.K.
‡Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd CF37 1DL, U.K.
Email: {mderee, gimantas, jonathan}@av.it.pt

***Abstract*—Communications, wired and wireless, have integrated various cryptographic techniques to ensure privacy and counter surveillance. These techniques have been integrated in most of the network layers, except for the physical layer. This physical layer has, thus far, dealt with schemes such as source coding, channel coding, and (de)modulation, to enable the transmission of data in a reliable and efficient manner. The emergence of physical layer security extends the functionalities at the physical layer to include secure communication, aiming at the transmission of a signal that can only be correctly retrieved by the intended receiver. Therefore, the goals of physical layer security align with cryptographic schemes utilized at the other network layers. From the extensive study of physical layer security schemes, we have observed that there is a knowledge gap regarding certain security principles practiced by cryptographers and the experts within physical layer security, causing many physical layer security schemes to be impractical for standardization and the wide-scale integration into information and communication technologies. This paper describes a variety of security principles and concepts, practiced by cryptographers, and of importance to physical layer security experts. We aim to raise the awareness of these security principles and concepts to experts within the field of physical layer security to improve the practicality, standardization, and integration potential of the design of future physical layer security schemes.**

***Index Terms*—Cryptography, Information Leakage, Physical Layer Security, Standardization**

I. Introduction

Claude Elwood Shannon, known as "the father of information theory", laid the foundation for the branch of information-theoretic security [1], [2] while employed at Bell Labs. Information-theoretic security offers a framework in which the security of information flows can be measured with quantitative information-theoretic metrics and enforced using a combination of signaling and coding mechanisms [3]. Information-theoretic security offers an alternative from cryptographic means, but was largely overlooked during the time following the discovery of public-key cryptography [4].

The last decade has seen the re-emergence of research in the area of information-theoretic security with the goal to secure communication at the lower layers of the communication protocols, the physical layer. Physical layer security is notably important to provide secure communication with resource-constrained devices that do not have the energy capacity and/or computational capabilities to perform more elaborate cryptographic operations [5]. Therefore, physical layer security is an important research area to enable secure communication for networks such as wireless sensor networks (WSNs) and the Internet of Things (IoT). Unfortunately, many physical layer security solutions are unsuitable for these networks since they either rely on resources that are not available (i.e., multi-antenna-based solutions such as multiple-input multiple-output (MIMO) [6] and beamforming), resources that are scarce (i.e., energy consumption associated with artificial-noise-based solutions), or rely on impractical assumptions on the adversary (e.g., awareness of an adversary) [7], [8]. Furthermore, there appears to be a knowledge gap regarding certain security principles practiced by cryptographers and experts within physical layer security, causing schemes to be impractical for standardization and the wide-scale integration into information and communication technologies. This paper intends to provide insight about security principles and concepts exercised within the field of cryptography with the aim to further enforce the design of practical physical layer security schemes with standardization potential.

In section II, we cover the security principle known as Kerckhoffs' principle and how it affects the standardization potential of physical layer security schemes. In section III, we cover the concepts of key space, bit security, one-time pad, and plaintext indistinguishability and how they are related to information leakage in physical layer security schemes and the security strength evaluation. In section IV, we conclude with a summary of our findings.

II. Obstructions for Standardization

A. Kerckhoffs' Principle

In 1883, Auguste Kerckhoffs proposed six principles that should be applied to any cryptographic scheme [9]:

- The scheme must be substantially, if not mathematically, undecipherable;
- The scheme must not require secrecy and can be stolen by the enemy without causing trouble;
- It must be easy to communicate and retain the key without the aid of written notes, it must also be easy to change or modify the key at the discretion of the correspondents;
- The scheme ought to be compatible with telegraph communication;

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

- The scheme must be portable, and its use must not require more than one person;
- Finally, given the circumstances in which such scheme is applied, it must be easy to use and must neither stress the mind or require the knowledge of a long series of rules.

The second principle, stating that a cryptographic scheme must remain secure even when everything about the scheme itself is public knowledge, is known as *Kerckhoffs' principle*. Kerckhoffs theorised that only the secret parts contribute to the security of a scheme, and for practical purposes, should be limited in terms of complexity. In 1949, this principle was rephrased by Claude Shannon as "the adversary knows the scheme", also known as *Shannon's maxim* [1]. Professionals within the field of cybersecurity also know Kerckhoffs' principle as the *open design* principle [10]. Abiding by these principles brings fourth additional advantages, namely (i) public scrutiny allows for the identification of weaknesses within the scheme and to exert confidence in the scheme when no weaknesses can be found after elaborate evaluation, and (ii) the ease of standardization and integration of the scheme into information and communication technologies. The design of the Advanced Encryption Standard (AES), also known as *Rijndael* [11], is a notable example of a cryptographic scheme that abides by Kerckhoffs' principle. From a public competition that consisted of 15 contestents, organized by the National Institute of Standards and Technology (NIST), it was selected as the most suitable scheme and has since been integrated as a security standard into information and communication technologies worldwide.

B. Kerckhoffs' Principle for Physical Layer Security

Kerckhoffs' principle is a guideline for the adversarial model that any security scheme should consider, namely, the adversary knows the scheme. Unfortunately, there appears to be a noticable difference between the adversarial models used for the security evaluation of physical layer security schemes and that of cryptographic schemes. Namely, physical layer security schemes often consider a naive adversary which has either no or limited knowledge about the scheme. From the perspective of the adversary, the scheme is assumed to be at least partially secret. Achieving security through the secrecy of the scheme, known as *secrecy through obscurity*, has historically been shown to be a poor practice to establish and, more importantly, maintain secure communications [12]. Instead, secrecy through obscurity should only be used as an additional security barrier. Transport for New South Wales experienced this first-hand when four students cracked the secret algorithm of Sydney's public transport tickets for busses, trains and ferries, allowing them to print their own valid tickets [13].

Experts within the field of physical layer security should therefore, by default, consider adversaries that possess complete knowledge of the proposed scheme (i.e., abide by Kerckhoffs' principle) and evaluate the level of security that the scheme provides under this assumption. This will be necessary if physical layer security schemes want to be considered for standardization and the wide-scale integration into information and communication technologies. In the following sections, we assume that an adversary has complete knowledge of any scheme used against it.

III. Information Leakage

The concept of *leakage* refers to the leaking of information of a data transmission. Leakage is not necessarily a design flaw, but it does have to be considered when evaluating the level of security or secrecy that a scheme achieves. Information leakage, depending on the information that is being transmitted, can cause severe issues and has to be countered in their own specific ways. In the following subsections, we cover the concepts of key space, bit security, message indistinguishability, and the one-time pad, and we describe how these concepts are related to physical layer security.

A. Key Space

The *key space* determines the number of possible keys that are used in a cryptographic scheme [14]. The key space also determines, to a large extent, the security of the scheme since it dictates the number of possible keys that an adversary would have to check in an *exhaustive key search attack*. The larger the key space is, the more possibilities an adversary would have to check, and the higher the level of security.

The practice of increasing the key space to resist malicious attacks is very noticable when registering your password for an online account, having to abide by rules such as "must contain at least one number", "must contain at least one symbol", and "must be at least x characters long". The more randomness your password contains, the harder it is to crack. An 8-character password that consists of only numbers has a key space of $10^8 (= 1.0 \times 10^8)$ combinations, whereas a 16-character password that consists of both numbers and letters has a key space of $36^{16} (\approx 8.0 \times 10^{24})$ combinations.

B. Bit Security

The security of a cryptographic scheme is often measured in terms of *bit security*. Even though there is no universally accepted, general, formal definition of bit security, many cryptographers seem to have an intuitive common understanding of what "n bits of security" means: an adversary that successfully breaks the cryptographic scheme must incur a cost of at least 2^n, or, alternatively, any efficient attack achieves at most a success probability of 2^{-n} [15].

Suppose that the selected passwords, mentioned above, are completely random and that the most efficient attack from an adversary to crack the password is to simply check every possible combination. The 8-character password requires the adversary to check $10^8 (\approx 2^{26})$ possibilities whereas the 16-character password requires the adversary to check $36^{16} (\approx 2^{82})$ possibilities, corresponding to 26- and 82-bit security, respectively. To put the strength of these passwords into perspective, the Bitcoin network – argueably the largest modern use of computational power for cryptography – recently peaked at checking $215 \times$

$10^{18} (\approx 2^{67})$ "passwords" (i.e., hashes) per second [16]. The Bitcoin network can therefore crack the 8-character password instantly and the 16-character password within about 10 hours. Much of the current day information and communication technologies are protected with 128-bit security, sufficient to withstand the Bitcoin network for the next 50 billion years.

C. Key Space & Bit Security for Physical Layer Security

The research area of physical layer-based key generation utilizes the randomness of the time-varying communications channel such that any two devices, within each other's transmission range, can generate one or more secret bits. The secret bits can then be used in a (physical layer-based) encryption or authentication scheme to provide security. Both devices would initially engage in a channel estimation protocol to obtain their channel state information (CSI). Parameters such as the channel frequency or phase, the received signal strength indicator (RSSI), and the channel impulse response (CIR) are popular choices for extracting secret bits and to establish a shared secret key [17]. Each of these properties has their benefits and drawbacks and must be considered properly depending on the deployment scenario. For example, a drawback of the utilization of RSSI for key generation is that this parameter is distance-dependent and may therefore be vulnerable to information leakage. Suppose that a physical layer-based key generation scheme utilizes RSSI and the scheme defines the secret bit (or bits) according to whether the observed RSSI satisfies a certain threshold (or interval). An adversary may not be able to determine the RSSI or the corresponding secret bit as accurately as the intended transceivers, but the observation may provide the adversary with enough information to make an educated guess, as illustrated in Figure 1.

If we assume that an adversary, due to information leakage from an RSSI estimation, can guess the correct bit with a probability that is greater than 50%, then the keys within the key space no longer follows a uniform probability distribution (i.e., certain keys are more probable than others). This affects the likeliness and success probability of the adversary finding the correct key and thus lowers the level of bit security. Therefore, such a key generation scheme would have to genereate a key larger than 128 bits in order to achieve 128-bit security. To provide insight regarding the severity of information leakage and its impact of the achieve bit security level, we estimated the bit security levels for keys of various sizes under the following adversarial assumptions:

1) The adversary obtains no knowledge about the individual secret bits, thus has a bit estimation probability of 50%. This is generally assumed in cryptographic literature and is included as a baseline.
2) The adversary observes leaked information, allowing it to estimate the secret bit with 60% accuracy.
3) The adversary observes leaked information, allowing it to estimate the secret bit with 70% accuracy.
4) The adversary observes leaked information, allowing it to estimate the secret bit with 80% accuracy.

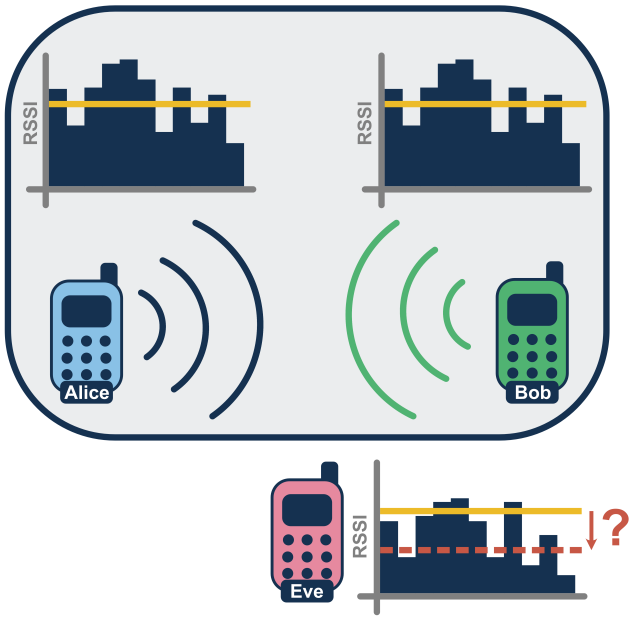

Fig. 1. Illustration of an RSSI-based secret key generation process between Alice and Bob, where secret bits are determined by the satisfaction of a preset threshold (i.e., the yellow line). The eavesdropper Eve may still recognize stronger from weaker signals, leaking information about the secret bits.

5) The adversary observes leaked information, allowing it to estimate the secret bit with 90% accuracy.

We used Python to compute the levels of bit security achieved by keys ranging between 1 and 36 bits in length under the aforementioned adversarial assumptions[1]. Due to the computational complexity involved, we were unable to compute the bit security for keys of larger sizes. We found that, for 36-bit keys, the computational workload of an adversary is reduced by a factor of about 2.5 when it is able to estimate the secret bits with a 60% accuracy (i.e., achieves 34-bit security), a factor of about 12 at a 70% accurate secret bit estimation (i.e., achieves 32-bit security), a factor of about 164 at an 80% accurate secret bit estimation (i.e., achieves 28-bit security), and a factor of about 14.910 at a 90% accurate secret bit estimation (i.e., achieves 22-bit security). The results are presented in full in Figure 2.

To determine the impact of information leakage during the secret key agreement process for larger keys, we computed both an upper bound and a lower bound for the achieved bit security per key length, up to keys of 128 bits. Our preliminary results show that, for 128-bit keys, the achieved levels of bit security assuming an adversarial bit estimation accuracy of 60%, 70%, 80%, and 90% are approximately 125 bits, 118 bits, 106 bits, and 84 bits, respectively. The results are presented in full in Figure 3.

In the case that the (physical layer-based) encryption or authentication scheme requires a 128-bit key and would not accept a longer key, the generated key can be fed into an appropriate hash function to reduce its length to 128 bits without compromising its 128-bit security level.

[1]The Python code is made publicly available at [18].

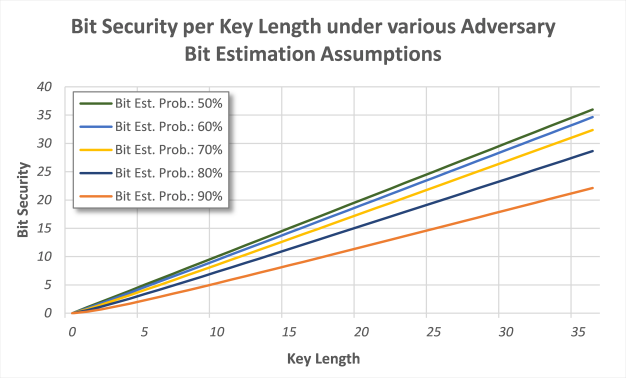

Fig. 2. The computed levels of bit security that are achieved for keys of 1 to 36 bits under various adversary bit estimation probability assumptions.

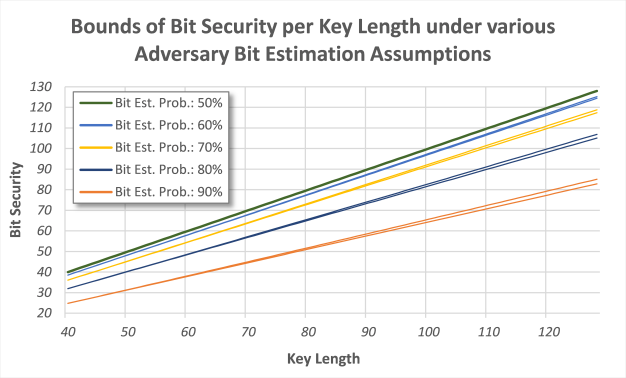

Fig. 3. The estimated upper and lower bounds of bit security that are achieved for keys of 40 to 128 bits under various adversary bit estimation probability assumptions.

To summarize, it is adamant for physical layer-based key generation schemes to consider an appropriate adversarial model (i.e., following Kerckhoffs' principle) and the amount of information leakage that may occur for the presented key generation technique. The estimated leakage impacts the level of bit security achieved against an exhaustive key search attack and determines the number of extra bits that a secret key should have in order to guarantee a sufficient security level. The study of information leakage for different CSI parameters in physical layer-based key generation is a current knowledge gap worth of additional study.

D. One-Time Pad

The *one-time pad*, also known as *Vernam's cipher*, was invented by Frank Miller in 1882 and re-invented by Gilbert Vernam in 1917 [19]. The one-time pad encrypts a plaintext by adding the first element of the plaintext with the first element of the key, the second element of the plaintext with the second element of the key, and so on. This scheme achieves perfect security under the following assumptions:

- The key must be at least as long as the plaintext.
- The key must have been generated at random.
- The key must never be reused.
- The key must only be shared between the transmitter and the inteded receiver.

The information that a one-time pad can leak is the length of the plaintext, since the corresponding ciphertext will be equally long. This is also the only piece of information that a one-time pad will leak. Even though this seems harmless, certain situations in which a receiver would acknowledge receiving a message by responding "yes" or "no" could leak sufficient information to infer the plaintext. These situations would require *padding*, a technique in which additional random characters are transmitted to prevent any leakage. In the case where as "yes" or "no" response is required, an additional random character would be appended to the "no" response to prevent leakage.

In the context of physical layer security, the concept of leaking information through leaking the message length may generally not be of much concern since the size and format of data packets are standardized. Although it is still worth mentioning to raise awareness of this vulnerability.

E. Plaintext Indistinguishability

The concept *plaintext indistinguishability* means that an adversary is unable to distinguish the correct plaintext from a partially deciphered ciphertext. Essentially, when an adversary guesses a part of the key correctly, it would still be unable to distinguish the partially deciphered ciphertext from a random ciphertext. Thus, it prevents an adversary from reconstructing the key piece-by-piece.

The plaintext indistinguishability problem may occur when keys are not appropriately used in an encryption scheme. Take, for example, the one-time pad. This scheme is perfectly secure under the assumptions stated in the previous section but the amount of keying material to be generated and distributed is impractical when large amounts of data are exchanged between two transceivers. Suppose that the rate at which data has to be transmitted is ten times larger than the rate at which keying material can be generated and distributed. For pratical purposes, we prefer not to reduce the data rate to $1/10$. A trivial solution may be to encrypt the first ten consecutive pieces of data with the generated secret key, then encrypt the following ten consecutive pieces of data with the newly generated secret key, and so on. Due to the relative small key size, an adversary may be able to execute an exhaustive key search attack without much issue. If the adversary is able to distinguish which attempted key is the secret key, since it would be able to identify which plaintext looks like an actual message, then the encryption method is broken. The regular updating of the (relatively small) key would not add sufficient security. It is easy to see that fewer blocks of data, encrypted with the same key, are better capable of providing plaintext indistinguishability and thus increase the level of security of the encryption method. The extreme case is the one-time pad where every block of data (i.e., bit) is encrypted with a unique key, eliminating any possibility of plaintext distinguishability and thus achieving perfect security.

F. Plaintext Indistinguishability for Physical Layer Security

The problem of *plaintext distinguishability* can also be related to physical layer security schemes. Recall that physical layer-based key generation schemes can utilize different parameters from the CSI and is shared between any two transceivers (see section III-C). These parameters include the channel phase. Suppose that a physical layer-based key generation scheme utilizes the channel phase and the scheme defines the secret bit (or bits) according to whether the observed phase satisfies a certain threshold (or interval). An advantage of the utilization of the channel phase is that this parameter is distance-independent. This prevents an adversary from using a location-dependent technique to extract partial information about the generated bit(s). However, a drawback is that the re-estimation of the shared channel may not result in the establishment of secret bits that are statistically uncorrelated from its previous value. The *coherence time*, a measure for the minimum amount of time required for the phase to become uncorrelated from its previous state, dictates how frequently the channel can be re-estimated for key generation. The amount of *channel fading* (i.e., the rate at which channel characteristics, such as the channel phase, change) is therefore directly related to the amount of time that it will take to generate a key with sufficient bits. The use of the channel phase for key generation may therefore not be the most suitable option in static networks with slow fading channels. A phase-based key generation scheme can achieve both practicality (i.e., decent throughput) and security (i.e., based on the discussion regarding plaintext indistinguishability), but seemingly at the cost of a longer initialization process for the generation of appropriate sized keys.

IV. Conclusions

In this paper, we discussed a variety of security principles and concepts that dictate design methodologies and the security evaluation of cryptographic schemes. Abiding by these security principles and concepts have led to the design of practical designs of cryptographic schemes and awareness of the security principles and concepts within the field of physical layer security may enforce the design of more practical physical layer security schemes. Namely, abiding by Kerckhoffs' principle should lead to a paradigm shift in the considered adversarial model and will strengthen the security argument of physical layer security schemes. Awareness of the key space and bit security as a measure of estimating security levels against computational adversaries should lead to a more thorough investigation of information leakage in physical layer-based key generation schemes and its impact. Finally, awareness of the plaintext indistinguishability concept should provide additional insight into the amount of information leakage that should and should not be acceptable when making a trade-off between the practicality and the security of a physical layer-based encryption scheme. The one-time pad serves as an example of how perfect security affects practicality and vice versa.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The Wire-Tap Channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] M. Bloch *et al.*, "An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.

[4] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[5] M. de Ree, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez and I. E. Otung, "Key Management for Beyond 5G Mobile Small Cells: A Survey," *IEEE Access*, vol. 7, pp. 59200–59236, 2019.

[6] S. Althunibat, V. Sucasas, G. Mantas and J. Rodriguez, "Physical-Layer Entity Authentication Scheme for Mobile MIMO Systems," *IET Communications*, vol. 12, no. 6, pp. 712–718, Apr. 2018.

[7] A. Abushattal, S. Althunibat, M. Qaraqe and H. Arslan, "A Secure Downlink NOMA Scheme Against Unknown Internal Eavesdroppers," *IEEE Wireless Communications Letters*, vol. 10, no. 6, pp. 1281–1285, Jun. 2021.

[8] M. de Ree *et al.*, "Data Confidentiality for IoT Networks: Cryptographic Gaps and Physical-Layer Opportunities," *Proc. Int. Wksp. Computer Aided Modeling and Design of Communication Links and Networks* (CAMAD), Porto, Portugal, pp. 1–6, Oct. 2021.

[9] A. Kerckhoffs, "La Cryptographie Militaire," *Journal des Sciences Militaires*, vol. 9, pp. 5–38, Jan. 1883.

[10] R. E. Smith, "A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles," *IEEE Security & Privacy*, vol. 10, no. 6, pp. 20–25, Nov./Dec. 2012.

[11] J. Daemen and V. Rijmen, "The Design of Rijndael: The Advanced Encryption Standard (AES)," Springer, 2nd edition, 2020.

[12] D. Kahn, "The Codebreakers: The Comprehensive History of Secret Communicaiton from Ancient Times to the Internet," Scribner, 1996.

[13] B. Grubb, "Free Ride: Students Crack Ticket Algorithm," *The Sydney Morning Herald*, Nov. 2012. https://www.smh.com.au/technology/free-ride-students-crack-ticket--algorithm-20121112-2984x.html (accessed Apr. 7, 2022).

[14] D. R. Stinson, "Cryptography: Theory and Practice," CRC Press, 3rd edition, 2006.

[15] D. Micciancio and M. Walter, "On the Bit Security of Cryptographic Primitives," *Proc. Int. Conf. Theory and Applications of Cryptographic Techniques* (EUROCRYT), Tel Aviv, Israel, pp. 3–28, Apr. 2018.

[16] Blockchain Explorer, "Mining Information - Total Hash Rate (TH/s)," *Blockchain.com*, 2022. Available: https://www.blockchain.com/charts/hash-rate (accessed Apr. 13, 2022).

[17] M. Bottarelli, G. Epiphaniou, D. K. B. Ismail, P. Karadimas, and H. Al-Khateeb, "Physical Characteristics of Wireless Communication Channels for Secret Key Establishment: A Survey of the Research," *Computers & Security*, vol. 78, pp. 454–476, Sept. 2018.

[18] M. de Ree, *Bit Security versus Leakage*, GitHub, 2022. [Online]. Available: https://github.com/mderee/Public-Scripts/blob/main/Security-vs-Leakage.

[19] S. M. Bellovin, "Frank Miller: Inventor of the One-Time Pad," *Cryptologia*, vol. 35, no. 3, pp. 203–222, 2011.