Physical Layer Security: Authentication, Integrity and Confidentiality

Mahdi Shakiba-Herfeh
ETIS, Université Paris Seine, ENSEA
Université Cergy-Pontoise, CNRS
Cergy-Pontoise, France
mahdi.shakiba-herfeh@ensea.fr

Arsenia Chorti
ETIS, Université Paris Seine, ENSEA
Université Cergy-Pontoise, CNRS
Cergy-Pontoise, France
arsenia.chorti@ensea.fr

H. Vincent Poor
Department of Electrical Engineering
Princeton University
Princeton, NJ
poor@princeton.edu

Abstract*—The goal of physical layer security (PLS) is to make use of the properties of the physical layer – including the wireless communication medium and / or the transceiver hardware – to enable critical aspects of secure communications. In particular, PLS can be employed to provide i) node authentication, ii) message authentication, and, iii) message confidentiality. Unlike the corresponding classical cryptographic approaches which are all based on computational security, PLS's added strength is that it is based on information theoretic security, in which no limitation with respect to the opponent's computational power is assumed and is therefore inherently quantum resistant. In this survey, we review the aforementioned fundamental aspects of PLS, starting with node authentication, moving to the information theoretic characterization of message integrity, and finally, discussing message confidentiality both in the secret key generation from shared randomness and from the wiretap channel point of view. The aim of this review is to provide a comprehensive roadmap on important relevant results by the authors and other contributors and discuss open issues on the applicability of PLS in sixth generation systems.

***Index Terms*—Physical layer security, physical unclonable function, RF fingerprinting, node authentication, message integrity, secrecy encoder, shared randomness, key generation, confidentiality.**

I. Introduction

The increasing deployment of wireless systems poses security challenges in next generation dynamic and decentralized networks, consisting of low cost and complexity devices. Over the last two decades alternative / complementary means to secure data exchange in wireless settings have been investigated in the framework of physical layer security (PLS), addressing jointly the issues of reliability and secrecy. PLS takes advantage of the inherent randomness of wireless communication channels and / or the unclonability of hardware fabrication processes, to harvest entropy and deliver authentication, confidentiality, message integrity and privacy in demanding scenarios. In this chapter, we revisit all aforementioned aspects from an information theoretic security perspective.

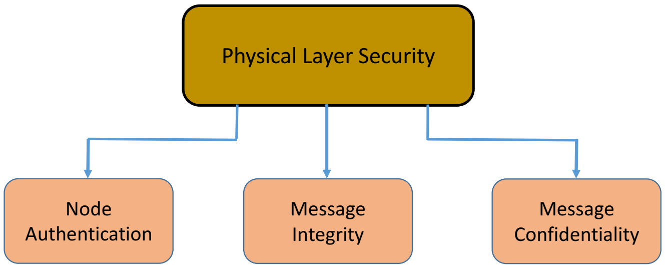

Figure 1: The three main operations of PLS.

PLS relies on information theoretic proofs of (weak or strong) perfect secrecy, a notion first introduced by Shannon in 1949 [1]. As such, PLS systems cannot be "broken" irrespective of the adversarial computational power, i.e., the proofs do not rely on any assumptions regarding the hardness of particular families of algebraic problems. There are some fundamental differences between information theoretic security and classical cryptography based security. In the following, we illustrate some of the pros and cons for each.

Classical cryptography based security: standard cryptosystems as those in employed in the fifth generation (5G) security protocols have notable strengths:

- There are no known feasible attacks on symmetric key cryptosystems such as the advanced encryption system (AES) or elliptic curve Diffie Hellman (ECDH) asymmetric key encryption, and hence they are trustworthy in any conceivable scenario as they are thought of achieving semantic security;
- Only a few assumptions are made about the messages to be encrypted or the trusted third parties in authentication protocols (e.g., regarding the trustworthiness of certificate authorities);
- These systems have been widely employed and tested over decades, the technology is mature, ready-to-use and nowadays inexpensive.

However, crypto based security has indeed certain disadvantages, some of which are pointed out below:

- Generally the semantic security proofs of traditional crypto systems are built around unproven assumptions about the hardness of certain "one-way" functions. As a result, some of these schemes, notably in the realm of asymmetric key encryption, are considered vulnerable to quantum attacks;
- Standard crypto is typically employed in upper layers of the OSI protocol stack, assuming that the PHY connection has already been established. As a result,

they are inherently “inflexible” with respect to wireless connectivity issues and will fail in attacks at the physical layer, e.g., jamming attacks on the control plane;

- State-of-the art key distribution schemes for wireless networks based on the classic cryptography model require a trusted third party and are typically computationally intensive. Therefore, their application in machine-to-machine or low latency applications can be challenging [reference urllc 3 gpp security];
- These security approaches are not tailored to the wireless communication properties and are typically not lightweight. With respect to the latter aspect, as an example, the level of sophistication of Google’s take on a lightweight implementation of AES is rather a proof of the difficulty in rendering these schemes lightweight, rather than the opposite.

Information theoretic security: Notable advantages of PLS based security are as follows:

- No computational limitations are placed on the opponent, PLS schemes that are properly implemented are quantum secure;
- The achievable secrecy rate is a function of the channel quality and the block length of the secrecy encoders and as a result the security is naturally tied to the communication properties;
- Unlike “distributing” keys, PLS can be used to generate on-the-fly secret keys, exploiting channel estimation operations that are customarily performed to establish the PHY connection.
- PLS implementations can be lightweight and related schemes can be advantageous in Internet of things (IoT) or low latency constrained scenarios.

Also the disadvantages of this class of security are as follows

- Some PLS schemes are based on stringent assumptions about the adversarial channel quality, e.g., the wiretap channel scenario, that are impractical in the general case;
- PLS technologies have not been tested “in the field” and it is therefore expected that there will be erroneous implementations before reaching a satisfactory level of maturity;
- The performance bounds of the related encoders have not been characterized in the finite blocklength regime, so the achievable rates back-off from the information theoretic infinite blocklenth capacity is yet unknown.

Despite these issues, PLS is currently studied as a possible second layer of security for particular use cases, e.g., when implementation issues in the 5G security protocols have identifiable shortcomings such as vulnerabilities to false base station attacks [2]. Notably, it is explicitly mentioned as a sixth generation (6G) enabling technology in the first white paper on 6G: “The strongest security protection may be achieved at the physical layer”. In this work, we review how it is possible to move some of the security core functions down to the physical layer, exploiting both the communication radio channel and the hardware as unique entropy sources.

We consider three important security operations: node authentication, message integrity and message confidentiality as depicted in Fig. 1. In node authentication, the goal is for nodes to identify uniquely the other side of the communication. With respect to message integrity, the goal is to be able to identify tampering attacks on the exchanged messaged, i.e., verify the integrity of the received information in the presence of active attackers. Finally, in message confidentiality, users want to “hide” the content of their transmissions from a passive opponent (eavesdropper).

The rest of the paper is organized as follows. In Section II three different PLS methods of node authentication are reviewed: i) physical unclonable functions (PUFs), ii) biometric based authentication, and iii) RF fingerprinting. Next, in Section III, the information theoretic bounds on the achievable rates when message integrity is required are reviewed, both for noiseless and noisy transmission channels. Furthermore, in Section IV we consider message confidentiality. Two alternative approaches to achieve message confidentiality are reviewed: i) keyless secrecy encoding in wiretap channels and, ii) channel based secret key generation (SKG), used in conjunction with symmetric encryption in hybrid schemes.

II. Node authentication

In all communication networks, users utilize authentication protocols to prove their identity. In standard crypto protocols, asymmetric key encryption is typically used in the authentication phase. However, the standard cryptographic schemes in the realm of public key encryption (PKE), are computationally intensive, incurring considerable overhead and can rapidly drain the battery of energy constrained devices [3], [4]. Additionally, traditional public key generation schemes are not *quantum secure* – in that when sufficiently capable quantum computers will be available they will be able to break current known public key encryption schemes – unless the key sizes increase to impractical lengths.

As a result, in 6G, PLS based authentication arises as a possible alternative. PLS authentication protocols usually consist of two stages, namely an enrollment stage and a release (authentication) stage. The enrollment stage occurs offline. In this stage, unique characteristics of the node or user to be authenticated are measured. Hashed versions of these measurements along with related helper (side) information are stored at the verifier side in a database. In the release stage, new measurements are taken and sent to the verifier; the latter uses the helper information to regenerate the hash of the initial measurement, in which case the authentication is successful. The role of the helper information is critical as it allows to correct for discrepancies between different measurements due to noise (in any actual system, deriving the same exact outcome from two consecutive measurements is impossible). Error correcting codes from the family of Slepian Wolf encoders are typically used in these systems; as an example, if the implementation is based on linear block

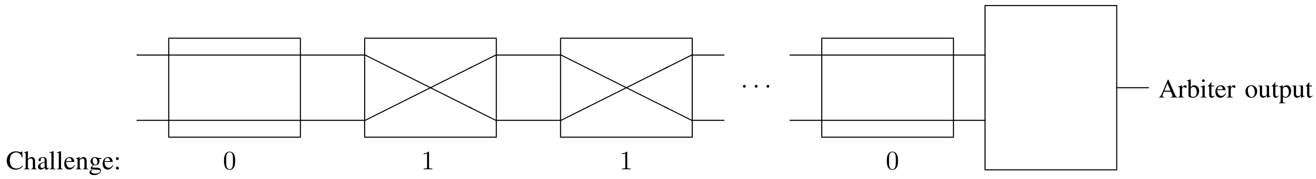

Figure 2: Arbiter PUF

codes, the helper information is typically in the form of the syndrome of the initial measurement.

From an information theoretic point of view, the basic idea is to generate a hashed version of the initial measurement, similarly to regenerating a unique secret key used for authentication, derived during the enrollment stage. As the rate of the secret key generation increases, the attacker has a harder task to guess it correctly. In other words, the level of security increases, while a lower bound on the length of the authentication key is imposed by the size of the brute force attack that can be mounted by an adversary. In following, we describe three different PLS approaches employed for node authentication. We note that a combination of these can also be employed, in order to increase the authentication vector size.

A. Physical unclonable functions (PUFs)

The concept a physical unclonable function was first introduced in [5]. The idea is that integrated circuits (ICs) have uniquenesses in their physical microstructure which is inherited from inevitable variations during the fabrication process. These unique characteristics are *unpredictable* before the end of the manufacturing and can be considered as digital signatures or identities of the ICs. A PUF should be *unclonable*, which means that given the exact fabrication procedure, it is infeasible to reproduce the same physical microstructure. The security of PUFs stems from these properties. An example of an arbiter based PUF is depicted in Fig. 2.

PUFs operate based on challenge-response pairs (CRPs). In the enrollment stage, a set of challenges are applied to a PUF (e.g., in the form of input voltages to a chain of logical gates) and the response of the PUF to each challenge, i.e., a hash of the PUF measurement, are stored in a database at the verifier. The responses for different challenges are different and each PUF has a unique response. Due to noise in measurements, in this stage some helper data is also stored in the database to enable the re-generation of the registered CRPs in the release stage. The collected sets of CRPs are considered as the IDs of the devices to be authenticated.

In the release stage, the verifier presents a particular challenge to the PUF. After running the challenge, the PUF releases the corresponding response (PUF measurement). If the response collected from the PUF in the release stage along with the helper information can reproduce the stored authentication key in the enrollment stage, the user is authenticated. A PUF that has an exponential number of CRPs is considered “strong” [6], i.e., it has a higher entropy and is a better option for security purposes as opposed to weak PUFs with polynomial numbers of CRPs. In [7], the authors consider an information theoretic perspective on PUFs and derive the entropy in a particular type of PUFs based on their physical properties.

In the CRP scheme, the attacker may acquire a software model of the PUF by using information extracted from exchanged CRPs in the clear. Intrinsically, a PUF hides a “random” function, and learning such functions from input-output pairs falls within the context of machine learning (ML). The authors in [8] show their proposed PUF is secure against the strongest known classical and reliability-based ML attack. Different PUF-based authentication protocols for wireless sensor networks have recently been proposed in the literature [9]–[14].

B. Biometrics

Biometric authentication is used for user (as opposed to device) authentication. The security of the method comes from the uniqueness and consistency of biometric characteristics of each person. Similar to PUF based authentication, the fundamental scheme consists of two stages. In the enrollment stage the biometric characteristics of users are sampled and in plain form or through a transformation are stored in the database of the verifier. Due to noisy measurement and possible changes in biometric characteristics over time or damages, helper data is also stored in this stage. In the release stage, the verifier demands a new biometric sample from the user and if the new measurement with the assist of the helper information can reproduce the same data stored during the enrollment stage, the user is authenticated.

This method of authentication has been widely used over decades for different applications. However, privacy concerns pose a major challenge. The biometric characteristics of a human cannot be changed. If the stored data are compromised by attackers, they can be used to imitate legitimate users. Different approaches have been proposed to protect the stored data from such attacks. For example, in [15], [16] a type of cryptographic primitive called secure sketch is considered. In this approach, a hash of the biometric information is stored in the database along with the helper data. In [17], [18], the authors study a cancelable biometric scheme in which an irreversible transformation of the biometric data is stored.

Information theoretic analyses of these schemes have been performed [19], [20] and the largest rate of the authentication key has been characterized [21] in absence of privacy requirements. In all of the aforementioned works and in the basic proposed scheme, the helper data can contain information about the biometric characteristics. The two part paper [22], [23] studies the privacy-security trade off in biometric security and considers two scenarios with perfect key protection and perfect privacy model, that address two different perspectives of the problem.

a) Perfect key protection system: In this model the helper data (V) does not contain any information about the secret key (K). The privacy of the biometric measurement is measured as the normalized equivocation rate $H(X^n|V)/H(X^n)$, where $H(\cdot)$ denotes entropy. The greater normalized equivocation means the higher level of privacy which can be arbitrarily close to unity when the mutual information of V and X goes to zero ($I(V;X) \rightarrow 0$). In perfect key protection system, there is a trade off between the rate of secret key generation R and the level of the biometric measurement privacy Δ_P. For a perfect key protection biometric authentication system, a privacy-security pair (Δ_P, R) is said to be achievable if for any $\epsilon > 0$, there exists an integer n, that satisfies the following conditions:

$$H(K)/n \geq R, \tag{1}$$

$$H(X^n|V)/H(X^n) \geq \Delta_P, \tag{2}$$

$$I(V;K)/n \leq \epsilon, \tag{3}$$

$$Pr(K \neq \hat{K}) \leq \epsilon, \tag{4}$$

where X and $\hat{K}$ represent the measurement in the enrollment stage and the estimated secret key, respectively. It has been shown that the capacity region $\mathbb{C}$ contains the set of all privacy-security pairs (Δ_P, R) such that [22]

$$\Delta_P \leq 1 - \frac{I(U;X) - I(U;Y)}{H(X)}, \tag{5}$$

$$R \leq I(U;Y), \tag{6}$$

where Y denotes the measurement in the release stage and U is an auxiliary random variable such that (U, X, Y) forms a Markov chain $U \rightarrow X \rightarrow Y$.

b) Perfect privacy system: In this model the helper data (V) does not contain any information about the biometric measurement (X). The performance of perfect privacy system can be measured by the rate of secret key generation and the normalized equivocation of the generated key $H(K|V)/H(K)$. In this system, a rate-equivocation (R, Δ_s) is achievable if for any $\epsilon > 0$, there exists an integer n, that satisfies the following conditions:

$$H(K)/n \geq R, \tag{7}$$

$$I(X^n;K)/n \leq \epsilon, \tag{8}$$

$$H(K|V)/H(K) \geq \Delta_s, \tag{9}$$

$$Pr(K \neq \hat{K}) \leq \epsilon. \tag{10}$$

It has been shown that a privacy-rate pair (R, Δ_s) is achievable if and only if, for the random processes X^n and Y^n for each $\epsilon > 0$ there exist an n and functions Ψ_n of X^n and Φ_n of Y^n such that [22]

$$Pr[\Psi_n(X^n) \neq \Phi_n(Y^n)] \leq \epsilon, \tag{11}$$

$$H(\Psi_n(X^n))/n \geq R\Delta_s - \epsilon. \tag{12}$$

Note that if K is a function of X^n, perfect privacy means perfect key protection.

C. Wireless identification using RF fingerprinting

Utilizing wireless channel characteristics is another approach to authenticate the nodes. In this approach, the wireless channel characteristics such as the user / device localization, e.g., using the received signal strength indicator (RSSI) or the link quality indicator (LQI) and the angle of arrival are used to verify the "expected location" of the users / devices. Wireless identification is commonly used in scenarios in which localization also needs to be verified e.g., in IoT sensors monitoring temperature and pressure at various equipment. Different variants of wireless identification have been studied for different applications [14], [24]–[26].

III. Message Integrity

A second major requirement of secure communications is that the legitimate receiver should be able to ensure the integrity of received messages. In many applications, this operation is considered even more important than that of confidentiality, given that many messages might not be "secret" but should be "authentic". In this scenario, the opponent is active and can sketch different attacks to deceive the receiver, typically by tampering with the message in transit. As an example, in substitution attacks, the attacker changes content of the message transmitted by the legitimate source. In impersonation attacks, the attacker sends a fake message while the source is idle. The receiver should be able to detect the fake and modified messages from the authentic ones [27], [28].

Message integrity requires a secret key shared by the two communicating parties and unknown by the attacker. The rest of the system design, such as the encoding / decoding schemes, are publicly available. The receiver considers the received signal as authenticated / verified (i.e., the integrity test is successful), if there exists a valid "tag" that can uniquely relate the received message to the secret key k, while the attacker cannot produce a valid (tag, message) pair despite intercepting a large number of related exchanges; proofs along this line of reasoning fall into the category of chosen ciphertext semantic security. The entropy of the shared key should be high enough to not allow the attacker to mount brute force attacks on the system.

The information theoretic limits of the message authentication problem was first considered by Simmons [29]. In Simmons's model, a noiseless channel between the terminals has been assumed (Fig. 3). In this model, the transmitter transmits w which is a function of the secret key k and

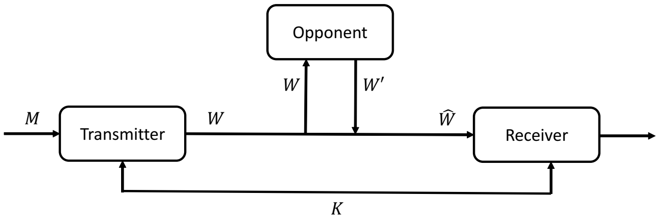

Figure 3: The message authentication model for noiseless channel.

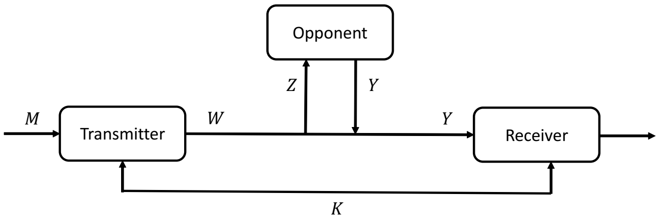

Figure 4: The message authentication model for noisy channel.

the message m ($w = f(k, m)$). The opponent observes the signal transmitted in the clear. However, the receiver observes $\hat{w}$, which can be different from the original signal and modified by the opponent. It has been shown that the success probability of impersonation and substitution attacks in message authentication can be lower bounded by $2^{-I(K,W)}$ and $2^{-H(K|W)}$, respectively. Therefore the success probability of the attacks by the opponent is lower bounded by $\frac{1}{\sqrt{|\mathcal{K}|}}$, where $|\mathcal{K}|$ is the size of the key space.

In [30], [31], the authors consider noisy channels and demonstrate that introducing noise in the model can make the receiver reject some valid messages. They conclude that channel noise is detrimental to message authentication. Coversely, in [32], [33], the authors study the message authentication problem via noisy channels from a new perspective. The authors propose a scheme in which the transmitter exploits the noise in the channel to "hide" the key information from the opponent. In their scheme, the transmitter performs joint channel coding and message authentication coding. The channel code is designed such that the conditional probability distribution after observing the channel output at the opponent side is very close to a uniform distribution. In [32], a discrete memoryless channel (DMC) model is considered and it is assumed that the opponent observes Z with a particular conditional probability distribution given the message w has been sent (Fig. 4). If the opponent does not perform any attack, the receiver observes Y with a particular conditional probability distribution given w. However, if the opponent performs an attack, it can modify Y according to its attack policy.

The receiver may make two possible types of error, which are to wrongly reject an authentic message (false negative)) or to accept a modified or fake message (false positive). The proposed scheme in [32] utilizes a wiretap channel model to protect the secret key. Basically, the transmitter chooses an input distribution P_W such that $I(W;Y) - I(W;Z) > 0$. Then, the source generates a codebook for the wiretap channel with $2^{nI(X;Y)}$ codewords, where n is the blocklength and we assume it is large enough to satisfy a low decoding error probability requirement at the receiver. The source then partitions the codewords into $|\mathcal{K}|$ subsets, i.e., $|\mathcal{K}| < 2^{n[I(W,Y)-I(W,Z)]}$. Each subset is associated with each key.

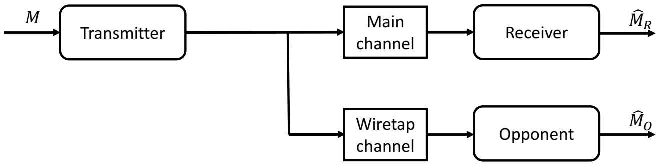

Figure 5: The wiretap channel.

Assume, the codeword length be large enough that there be more than $|M|$ codewords in each subset. The source then divides each subset into $|M|$ bins, each corresponding to a message. There are multiple codewords in each bin. In the transmission, if the intended message is m, and the key is k, the source then randomly chooses a codeword w from the mth bin of the kth subset using a uniform distribution. As the coding rate is $I(X;Y)$ the receiver can decode the message with high probability if n is large enough. On the other hand, according to the fundamental wiretap channel result, the opponent cannot gather a significant amount of information about the secret key in this scheme. It is shown that the success cheating probability is upper bonded by $\frac{1}{|\mathcal{K}|}$, which is significantly higher than the bound for the noiseless channel; as this scheme the transmitter uses the noise of the channel an an added entropy source to "hide" the key, the same approach cannot be applied for the noiseless scenario.

IV. Message Confidentiality Using Secrecy Encoders

Next, we study two distinct approaches to keep the messages confidential from third parties: i) the wiretap channel model, which exploits an advantage in terms of channel quality at the legitimate receiver in this Section, and, ii) secret key generation from shared randomness which exploits a common alea shared by the legitimate pair and at least partially unobserved by the opponent to generate a secret key (e.g., to be used with some appropriate encryption scheme) [34], in the next Section.

Wyner in [35] introduced the discrete memoryless wiretap channel model. In this model the transmitter communicates with a legitimate receiver and they want to keep the message confidential from a third party who is eavesdropping (passively intercepting the channel as in Fig. 5). In this scheme, no secret key is shared between the legitimate nodes. Wyner showed that the maximum achievable rate at which both reliable communication between the legitimate parties and weak secrecy with respect to the eavesdropper can be established, referred to as the channel's secrecy capacity C_s, can be expressed as follows:

$$C_s = \max_{V \to X \to YZ} I(U;Y) - I(U;Z), \quad (13)$$

where Y is the observation of the legitimate receiver, Z denotes the observation of the eavesdropper, X is the transmitted codeword and U is an auxiliary random variable such that (U, X, YZ) is a Markov chain $U \to X \to YZ$. According to (13), the secrecy capacity is the difference maximization between two values of mutual information which is taken over all possible input distributions $p(x)$. Hence both the legitimate receiver and the opponent channel conditions are essential to wiretap code designs. As it is mentioned before, in this model, the legitimate nodes do not need to share any secret key for their communication. One of the main drawbacks of using wiretap channel encoders in practice is that in this model the secrecy of the communication can only be established when there exists a particular input distribution $p(x)$ such that the mutual information of the main channel is higher than that of the wiretap channel, which is not guaranteed. Importantly, the transmitter needs to know the channel state of the opponent, an assumption that is impractical in many scenarios.

As a solution to the latter concern, the wiretap channel model with partial channel state information have been studied [36], [37], using an appropriate model where the uncertainty of practical CSI is taken into account. In the related model, the wiretap channel coefficient is divided to two parts. The first part is assumed to be known by the transmitter while the second one is unknown. As the weight of the second part becomes higher, the transmitter has lower information of the wiretap channel coefficient. In the case that the wiretap channel state is not available, the secrecy outage probability of is alternatively used as the security performance metric, in lieu of the secrecy capacity. The secrecy outage probability indicates the probability that the instantaneous secrecy capacity C'_s is lower than a target value C_s.

Furthermore, a plethora of alternative techniques have also been proposed in the literature to mitigate the need for full adversarial CSI, such as transmitting in the adversary's null signal space by leveraging the potential of multiple-input multiple-output (MIMO) transmission, injecting artificial noise to the adversarial signal space [38], [39], adaptive power allocation [40]–[42], exploitation of relay channels, faster than Nyquist assisted secrecy [43], [44], network coding [45], [46], and cognitive radio systems [47], [48].

V. Secret Key Generation (SKG) from Wireless Fading Coefficients

In this Section, we review the generation of secret keys from common randomness in the form of the wireless channel coefficient observed by a transmitter / receiver pair. This approach exploits the reciprocity of the wireless channel during the channel coherence time. The reciprocity refers to the property that the channel responses at both sides are the same (Fig 6). Therefore, the two endpoints of the channel observe a noisy form of a shared randomness from which they can distil a secret key. In a multipath rich environment, a third party should be only a few wavelengths away from the transmitter or the receiver so that their observed channel coefficients are independent from that in the direct channel between the transmitter and the receiver; this is a practical assumption in many actual wireless scenarios. Such generated keys can be secure with information-theoretic guarantees when the generation scheme is carefully applied, as opposed to keys generated from pseudorandom number generators.

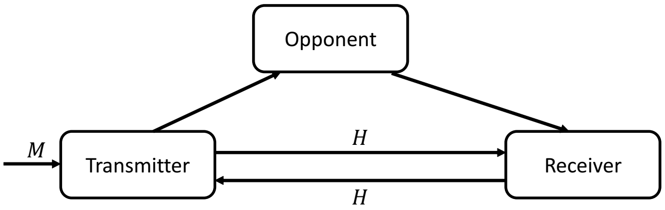

Figure 6: The channel based secret key generation system model.

The SKG standard procedure typically encompasses three phases [49]:

Advantage distillation: the legitimate nodes exchange probe signals to obtain estimates of their reciprocal channel state information (CSI) and pass them through a suitable quantizer [50]. Commonly, the received signal strength (RSS) has been used as the CSI parameter for generating the shared key [51], while in [52], [53] the CSI phase has been proposed.

Information reconciliation: discrepancies in the quantizer local outputs due to imperfect channel estimation are reconciled through public discussion using Slepian Wolf decoders. In this phase, with the aid of public discussion, the nodes should reconcile to a common key while avoiding to reveal any information about it. Numerous practical information reconciliation approaches using standard forward error correction (FEC) codes such as low density parity check codes (LDPC) have been proposed [54], [55], while in [52] the possibility of employing short Bose, Chaudhuri, Hocquenghem (BCH) FEC codes has also been explored.

Privacy amplification: applying universal hash functions to the reconciled information ensures that the generated keys are uniformly distributed (i.e., have maximum entropy) and are completely unpredictable by an adversary [56]. More importantly, it ensures that even if an adversary has access to (even a large) part of the decoder output, the final secret key can be unpredictable [57]. However, in this case, the genuinely random input space to the hash function needs to be large enough in order to avoid brute force attacks. When part of the reconciled information is known to the adversary, the corresponding amount of entropy needs to be "supressed" by the privacy amplifier.

Employing the standard SKG system model, let us assume that the transmitter and the receiver exchange a probe signal X in two consecutive slots and that their respective observations Z_A and Z_B, can be expressed as

$$Z_A = XH + N_A, \quad (14)$$

$$Z_B = XH + N_B, \quad (15)$$

where X denotes the channel input and H is the channel gain between the legitimate nodes, modeled as a circularly symmetric complex Gaussian random variable with zero mean and variance σ_H^2. N_A and N_B denote accordingly circularly symmetric complex Gaussian zero mean random variables that model the impact of additive white Gaussian noise with variances σ_A^2 and σ_B^2, respectively (typically $\sigma_A^2 = \sigma_B^2$).

A. Secret key rate

At first, let us assume that the attacker is a passive eavesdropper that only tries to obtain an estimate of H by interception. The case of an active attacker will be considered next. The information theoretic limits regarding the rate for generating secret keys has been established in [Mauer Ciszar]. From an information theoretic perspective, a secret key with rate R is achievable if for any $\epsilon > 0$ and sufficiently large blocklength n, there exists a public discussion strategy such that

$$Pr(K_A \neq K_B) < \epsilon, \tag{16}$$

$$\frac{1}{n} I(\Phi, \Psi; K_1) < \epsilon, \tag{17}$$

$$\frac{1}{n} H(K_1) > R - \epsilon, \tag{18}$$

$$\frac{1}{n}\log(|\mathcal{K}|) < \frac{1}{n} H(K) + \epsilon, \tag{19}$$

where Φ and Ψ denote the public messages sent by the transmitter and receiver in the information reconciliation subprocess, respectively, and K_A and K_B denote the distilled keys by the transmitter and receiver, respectively.

Theorem 1: The secret key capacity C_s assuming unlimited public discussion case is given as [49]

$$C_s = I(Z_A; Z_B). \tag{20}$$

However, in some scenario, there may be some limitations on public channel discussion. The capacity of secret key in public channel with limited rate is discussed in the following theorem.

Theorem 2: The secret key capacity C_s when the public channel rate constraint is R, is given by [58]

$$C_s = \max_U I(U; Z_B), \tag{21}$$

$$s.t. \quad U \rightarrow Z_A \rightarrow Z_B, \tag{22}$$

$$I(U; Z_A) - I(U; Z_B) \leq R, \tag{23}$$

where U is an auxiliary random variable.

Furthermore, it is possible that the evesdropper observes a sequence Z_E correlated to the the common randomness source. In this case, the security constraint in (16) should be transformed to

$$\frac{1}{n} I(\Phi, \Psi, Z_E; K_1) < \epsilon. \tag{24}$$

The secret key capacity C_s when the opponent has side information Z_E and the public channel rate constraint is R, is in the following theorem.

Theorem 3: The secret key rate R_s is achievable when the opponent has side information Z_E and the public channel rate constraint is R, is [58]

$$R_s = [I(U; Z_B) - I(U; Z_E)]^+, \tag{25}$$

$$s.t. \quad U \rightarrow Z_A \rightarrow Z_B, \tag{26}$$

$$I(U; Z_A) - I(U; Z_B) \leq R, \tag{27}$$

where U is an auxiliary random variable and $[x]^+ = \max\{x, 0\}$.

B. Authenticated encryption using SKG

Under the system model in Fig. 6 and normalizing to unity the noise variances, i.e., $\sigma_A^2 = \sigma_B^2 = 1$) for simplicity, the SKG rate can expressed as [59]–[61]:

$$R_k = \log_2\left(1 + \frac{P\sigma^2}{2 + \frac{1}{P\sigma^2}}\right), \tag{28}$$

while the corresponding *minimum* necessary reconciliation rate has been shown to be $h(H_B|H_A)$ [62], where $h(\cdot)$ denotes differential entropy. To develop a hybrid cryptosystem that can withstand active attacks [63], [64], the SKG can be used in conjunction with standard block ciphers, e.g., AES in Galois counter mode (GCM), to build hybrid authenticated encryption schemes.

As a sketch of such a hybrid scheme, let us assume a system with three parties: Alice who wishes to transmit a secret message $\mathbf{m}$ to Bob with confidentiality and integrity, and Eve (the opponent), that can act as a passive and active attacker. The following algorithms are employed:

- The SKG scheme denoted by $\mathtt{G} : \mathcal{H} \rightarrow \mathcal{K} \times \mathcal{S}$, accepting as inputs a vector of complex numbers (the fading coefficients), and generating as output a binary vectors of sizes n and $n-k$, respectively, $n, k \in \mathbb{N}$, (in the key and the syndrome spaces), *i.e.*,

  $$\mathtt{G}(H) = (K, S_A), \tag{29}$$

  where $K \in \mathcal{K}$ denotes the key obtained from H after privacy amplification and $S_A \in \mathcal{S}$ is Alice's syndrome (side information used for reconciliation).
- A symmetric encryption algorithm, e.g., AES GCM, denoted by $\mathtt{Es} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$ where $\mathcal{C}$ denotes the ciphertext space with corresponding decryption $\mathtt{Ds} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$, such that

  $$\mathtt{Es}(K, m) = c, \tag{30}$$

  $$\mathtt{Ds}(K, c) = m, \tag{31}$$

  for $K \in \mathcal{K}$, $m \in \mathcal{M}$, $c \in \mathcal{C}$.
- A pair of message authentication code (MAC) algorithms, e.g., in HMAC mode, denoted by $\mathtt{Sign} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{T}$, with a corresponding verification algorithm $\mathtt{Ver} : \mathcal{K} \times \mathcal{M} \times \mathcal{T} \rightarrow (yes, no)$, such that

  $$\mathtt{Sign}(K, m) = t, \tag{32}$$

  $$\mathtt{Ver}(K, m, t) = \begin{cases} yes, & \text{if integrity verified} \\ no, & \text{if integrity failed} \end{cases} \tag{33}$$

A hybrid crypto-PLS system for AE SKG can be built as follows:

1) The SKG procedure is launched between Alice and Bob generating a key and a syndrome $\mathtt{G}(H)=(K,S_A)$.
2) Alice breaks her key into two parts $K=\{K_e,K_i\}$ and uses the first to encrypt the message as $c=\mathtt{Es}(K_e,m)$. Subsequently, using the second part of the key she signs the ciphertext using the signing algorithm $t=\mathtt{Sign}(K_i,c)$ and transmits to Bob the extended ciphertext $[S_A\|c\|t]$, where $[\cdot\|\cdot]$ denotes concatenation of the corresponding binary vectors.
3) Bob checks first the integrity of the received ciphertext as follows: from $\mathbf{S}_A$ and his own observation he evaluates $K=\{K_e,K_i\}$ and computes $\mathtt{Ver}(K_i,c,t)$. The integrity test will fail if any part of the extended ciphertext was modified, including the syndrome (that is sent as plaintext); for example, if the syndrome was modified during the transmission, then Bob would not have evaluated the correct key and the integrity test would have failed.
4) If the integrity test is successful then Bob decrypts m=$\mathtt{Ds}(K_e,c)$.

C. Shielding SKG from active attacks during pilot exchange

The proposed authenticated encryption scheme using SKG is however vulnerable to man-in-the-middle (MiM) attacks during the pilot exchange phase, a vulnerability that was until recently unexplored. Here, we propose a simple scheme to overcome this issue. We assume a man-in-the-middle (MiM) attack in the form of an injection signal and then move to denial of service attacks in the form of jamming [65]–[67].

MiM attacks: MiM in SKG pilot exchange takes the form of a signal injection. Various possible approaches have so far surfaced on how to launch injection attacks; the attack can consist in controlling the movement of intermediate objects in the wireless medium, thus generating predictable changes in the received RSSI (e.g., by obstructing or not the line of sight), or the opponent can spoof the SKG process by injecting a signal W to Alice and Bob so the opponent will have some information about the secret key, as follows

$$
\begin{aligned}
Z_A &= XH + W + N_A,\\
Z_B &= XH + W + N_B,
\end{aligned}
\tag{34}
$$

where W denotes the injected signal. A simple approach to generate W can be devised as long as the adversary has one more antenna than the legitimate users. An example, let us consider the case in which Alice and Bob have one antenna each and the MiM has two. In this case, the MiM can choose a precoding matrix P so that

$$
W = \mathbf{H_{AE}}^T\mathbf{P}X_J = \mathbf{H_{BE}}^T\mathbf{P}X_J \tag{35}
$$

where, $\mathbf{H_{AE}}$ and $\mathbf{H_{BE}}$ denote the channel matrices between Alice and Eve and Bob and Eve, respectively. The precoding matrix $\mathbf{P}$ can be built as follows:

$$
\mathbf{H_{AE}}^T\mathbf{P}X_J = \mathbf{H_{BE}}^T\mathbf{P}X_J \Rightarrow P_1 = \frac{H_{BE2}-H_{AE2}}{H_{AE1}-H_{BE1}}P_2, \tag{36}
$$

where X_J is a generic transmitted signal by the MiM to satisfy the power constraint.

Under this attack, the secret key rate controlled by the opponent is upper bounded by [65]

$$
L \leq I(Z_A, Z_B; W). \tag{37}
$$

A countermeasure to injection attacks can be built by randomizing the pilot sequence exchanged between Alice and Bob [65]. Here, we propose to randomize the pilots by drawing them from a (scaled) QPSK modulation, as follows: instead of transmitting the same probing signal X, Alice and Bob transmit independent, random QPSK probe signals X and Y, respectively. Alice's observation Z_A is modified accordingly as

$$
Z_A \;=\; YH + W + N_A, \tag{38}
$$

while Bob's observation is given in (34). To establish shared randomness in spite of the pilot randomization, Alice and Bob post-multiply Z_A and Z_B by their randomized pilots, obtaining local observations $\tilde{Z}_A$ and $\tilde{Z}_B$ (unobservable by Mallory), expressed as:

$$
\begin{aligned}
\tilde{Z}_A &= XZ_A = XYH + XW + XN_A, && (39)\\
\tilde{Z}_B &= YZ_B = XYH + YW + YN_B. && (40)
\end{aligned}
$$

The source of shared randomness, when the pilots are randomized QPSK symbols, is a circularly symmetric zero mean Gaussian random variable, $XYH \sim \mathcal{CN}(0, P^2\sigma^2)$.

Furthermore, due to the fact that X and Y are independent and have zero mean, the variables XW and YW are uncorrelated, circularly symmetric zero-mean Gaussian random variables, and, therefore independent, while the same holds for XN_A, YN_B, i.e., $(XW, YW) \sim \mathcal{CN}(\mathbf{0}, \sigma_J^2 P\Gamma\mathbf{I}_2)$ and $(XN_A, YN_B) \sim \mathcal{CN}(\mathbf{0}, P\mathbf{I}_2)$. Alice and Bob extract the common key from the modified source of common randomness XYH as opposed to XH. On the other hand, since XW, YW, XN_A, YN_B are i.i.d. complex circularly symmetric Gaussian random variables, the proposed scheme reduces injection attacks to uncorrelated jamming attacks, i.e., we get that

$$
L \leq I\left(\tilde{Z}_A, \tilde{Z}_B; W\right) = 0. \tag{41}
$$

Pilot randomization has in essence reduced injection attacks to jamming attacks.

Jammming attacks: Building on the results of the previous subsection, we next examine in detail the scenario in which the attacker acts as a jammer. Tow major alternatives have been identified to counter jamming:

1) The legitimate nodes harvest energy (EH) from the jamming signal: By harvesting the jamming power in a first phase and exploiting it to boost the pilot power during SKG in a second phase, the jammer's action may in fact increase the SKG capacity; in this case, the jammer should not launch the attack, i.e., it is neutralized. However, it is not always optimal for the legitimate nodes to neutralize the jammer. Indeed, using EH can reduce the SKG capacity since, for a non-trivial fraction of time, there is no secret bits generation; when the jammer is neutralized the penalty in terms of SKG rate might become too high, depending on the system parameters [reference missing].

2) Channel hopping or spreading: If the legitimate nodes do not have EH capabilities, yet there is another way to defend against jamming by assuming that the legitimate nodes can employ channel hopping or spreading over multiple orthogonal subcarriers [paper reference missing].

Here, the idea is to use channel hopping in a random fashion and avoid most of the jammer's interference as opposed to completely neutralizing it. Since potential jammers cannot predict the subcarrier used by the legitimate nodes, they will always spread their powers over the entire spectrum: the larger the number of subcarriers, the smaller the jammer's interference on each subcarrier. However, channel hopping is not always optimal since only a fraction of the entire spectrum is used for SKG. Depending on the system parameters, it can be preferable for the legitimate nodes to spread the available power across the entire spectrum rather than concentrate it on a single subcarrier.

VI. Conclusion

Many standard cryptographic schemes, particularly those in the realm of public key encryption (PKE), are computationally intensive, incurring considerable overhead. For example, a 3GPP report on the security of ultra reliable low latency communication (URLLC) systems notes that "for a URLLC service with higher speed than 65 kbps, the 3GPP Release 15 radio access network (RAN) cannot fulfill the quality of service (QoS) requirement while enforcing user plane integrity protection" [68]. Additionally, traditional public key generation schemes are not *quantum secure* – in that when sufficiently capable quantum computers will be available they will be able to break current known public key encryption schemes – unless the key sizes increase to impractical lengths.

In this chapter, we have reviewed alternative approaches to secure future communication systems by considering PLS. We have presented recent results on PLS with respect to major emerging application areas in authentication, integrity and confidentiality. We have focused on three topics of secure communications, namely node authentication, message integrity, and, secrecy, including secret key generation. We have reviewed some of the information theoretic limits and discussed implementations proposed recently in the literature. Additionally, we have discussed open issues that need to be addressed before the employment of PLS in future generation networks.

VII. Acknowledgments

This work is supported by the ELIOT ANR-18-CE40-0030.

References

[1] C. E. Shannon, "Communication theory of secrecy systems*," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] 3GPP, "Study on 5G security enhancement against false base stations (Release 16)," 3rd Generation Partnership Project (3GPP), Technical Specification (TR) 33.809, Oct. 2019, version 0.7.0. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539

[3] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct 2015.

[4] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct 2015.

[5] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[6] U. Rührmair, H. Busch, and S. Katzenbeisser, "Strong pufs: Models, constructions, and security proofs," in *Towards Hardware-Intrinsic Security: Foundations and Practice*, A.-R. Sadeghi and D. Naccache, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 79–96.

[7] B. Škorić, S. Maubach, T. Kevenaar, and P. Tuyls, "Information-theoretic analysis of capacitive physical unclonable functions," *Journal of Applied Physics*, vol. 100, no. 2, p. 024902, 2006.

[8] P. H. Nguyen, D. P. Sahoo, C. Jin, K. Mahmood, U. Rührmair, and M. van Dijk, "The interpose puf: Secure puf design against state-of-the-art machine learning attacks," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2019, no. 4, pp. 243–290, Aug. 2019.

[9] M. Miroslav, A. Chorti, M. J. Reed, and L. Musavian, "Authenticated secret key generation in delay constrained wireless systems," *Eurasip JWCN*, under review.

[10] M. Miroslav, A. Chorti, and M. J. Reed, "Subcarrier scheduling for joint data transfer and key generation schemes in multicarrier systems," to appear in IEEE Proc. Global Communications Conference (Globecom), Dec. 2019.

[11] M. Mitev, A. Chorti, and M. Reed, "Optimal resource allocation in joint secret key generation and data transfer schemes," in *2019 15th International Wireless Communications Mobile Computing Conference (IWCMC)*, June 2019, pp. 360–365.

[12] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A puf-based secure communication protocol for iot," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 3, pp. 67:1–67:25, Apr. 2017.

[13] M. H. Mahalat, S. Saha, A. Mondal, and B. Sen, "A puf based light weight protocol for secure wifi authentication of iot devices," in *8th International Symposium on Embedded Computing and System Design (ISED)*, Dec 2018, pp. 183–187.

[14] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-factor authentication for iot with location information," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3335–3351, April 2019.

[15] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 503–512, Sep. 2007.

[16] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in *2007 IEEE Conference on Computer Vision and Pattern Recognition*, June 2007, pp. 1–6.

[17] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, April 2007.

[18] J. Bringer, H. Chabanne, and B. Kindarji, "The best of both worlds: Applying secure sketches to cancelable biometrics," *Science of Computer Programming*, vol. 74, no. 1, pp. 43 – 51, 2008, special Issue on Security and Trust.

[19] T. Ignatenko and F. Willems, "On privacy in secure biometric authentication systems," in *2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07*, vol. 2, April 2007, pp. II–121–II–124.

[20] G. Cohen and G. Zemor, "The wiretap channel applied to biometrics," in *ISITA*, Parma, Italy, 2004, pp. 1–5.

[21] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," in *Biometric Authentication*, D. Maltoni and A. K. Jain, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 158–170.

[22] L. Lai, S. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems—part i: Single use case," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 122–139, March 2011.

[23] L. Lai, S. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems—part ii: Multiple use case," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 140–151, March 2011.

[24] K. Bonne Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*, Sep. 2007, pp. 331–340.

[25] M. N. Aman, K. C. Chua, and B. Sikdar, "Secure data provenance for the internet of things," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*, ser. IoTPTS '17. New York, NY, USA: ACM, 2017, pp. 11–14.

[26] S. T. Ali, V. Sivaraman, D. Ostry, and S. Jha, "Securing data provenance in body area networks using lightweight wireless link fingerprints," in *Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices*, ser. TrustED '13. New York, NY, USA: ACM, 2013, pp. 65–72.

[27] S. M. Perlaza, A. Chorti, H. V. Poor, and Z. Han, "On the impact of network-state knowledge on the feasibility of secrecy," in *2013 IEEE International Symposium on Information Theory*, July 2013, pp. 2960–2964.

[28] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "Physical layer security in wireless networks with passive and active eavesdroppers," in *2012 IEEE Global Communications Conference (GLOBECOM)*, Dec 2012, pp. 4868–4873.

[29] G. J. Simmons, "Authentication theory/coding theory," in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 411–431.

[30] Y. Liu and C. Boncelet, "The crc-ntmac for noisy message authentication," in *MILCOM 2005 - 2005 IEEE Military Communications Conference*, Oct 2005, pp. 2775–2781 Vol. 5.

[31] C. G. Boncelet, "The ntmac for authentication of noisy messages," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 35–42, March 2006.

[32] L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels," *IEEE Transactions on Information Theory*, vol. 55, no. 2, pp. 906–916, Feb 2009.

[33] L. Lai, H. E. Gamal, and H. V. Poor, "Message authentication: Information theoretic bounds," in *Securing Wireless Communications at the Physical Layer*, R. Liu and W. Trappe, Eds. Boston, MA: Springer US, 2010, pp. 335–353.

[34] A. Chorti, C. Hollanti, J. 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*, M. Baldi and S. Tomasin, Eds. Cham: Springer International Publishing, 2016, pp. 1–15.

[35] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[36] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, Jan 2011.

[37] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1696–1707, April 2012.

[38] A. Chorti, "Helping interferer physical layer security strategies for m-qam and m-psk systems," in *2012 46th Annual Conference on Information Sciences and Systems (CISS)*, March 2012, pp. 1–6.

[39] A. Chorti and H. V. Poor, "Achievable secrecy rates in physical layer secure systems with a helping interferer," in *2012 International Conference on Computing, Networking and Communications (ICNC)*, Jan 2012, pp. 18–22.

[40] A. Chorti, K. Papadaki, and H. V. Poor, "Optimal power allocation in block fading channels with confidential messages," *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 4708–4719, Sep. 2015.

[41] A. Chorti, K. Papadaki, and H. V. Poor, "Optimal power allocation in block fading gaussian channels with causal CSI and secrecy constraints," in *2014 IEEE Global Communications Conference*, Dec 2014, pp. 752–757.

[42] A. Chorti, K. Papadaki, P. Tsakalides, and H. V. Poor, "The secrecy capacity of block fading multiuser wireless networks," in *2013 International Conference on Advanced Technologies for Communications (ATC 2013)*, Oct 2013, pp. 247–251.

[43] A. Chorti and H. V. Poor, "Faster than nyquist interference assisted secret communication for ofdm systems," in *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Nov 2011, pp. 183–187.

[44] A. Chorti, "Masked-ofdm: A physical layer encryption for future ofdm applications," in *2010 IEEE Globecom Workshops*, Dec 2010, pp. 1254–1258.

[45] D. A. Karpuk and A. Chorti, "Perfect secrecy in physical-layer network coding systems from structured interference," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1875–1887, Aug 2016.

[46] A. Chorti, M. M. Molu, D. Karpuk, C. Hollanti, and A. Burr, "Strong secrecy in wireless network coding systems with m-qam modulators," in *2014 IEEE/CIC International Conference on Communications in China (ICCC)*, Oct 2014, pp. 181–186.

[47] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017. [Online]. Available: https://www.pnas.org/content/114/1/19

[48] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1027–1053, Secondquarter 2017.

[49] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[50] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 1422–1430.

[51] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 128–139.

[52] C. Saiki and A. Chorti, "A novel physical layer authenticated encryption protocol exploiting shared randomness," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sep. 2015, pp. 113–118.

[53] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, March 2008, pp. 3013–3016.

[54] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *2006 IEEE International Symposium on Information Theory*, July 2006, pp. 2593–2597.

[55] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, June 2010.

[56] U. Maurer, R. Renner, and S. Wolf, "Unbreakable keys from random noise," in *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, P. Tuyls, B. Skoric, and T. Kevenaar, Eds. London: Springer London, 2007, pp. 21–44.

[57] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, 1st ed. New York, NY, USA: Cambridge University Press, 2011.

[58] I. Csiszar and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, March 2000.

[59] E. V. Belmega and A. Chorti, "Protecting secret key generation systems against jamming: Energy harvesting and channel hopping approaches," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2611–2626, Nov 2017.

[60] E. V. Belmega and A. Chorti, "Energy harvesting in secret key generation systems under jamming attacks," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[61] A. Chorti and E. V. Belmega, "Secret key generation in rayleigh block fading awgn channels under jamming attacks," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[62] R. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography. i. secret sharing,” *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[63] A. Chorti, “Optimal signalling strategies and power allocation for wireless secret key generation systems in the presence of a jammer,” in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[64] A. Chorti, “Overcoming limitations of secret key generation in block fading channels under active attacks,” in *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, July 2016, pp. 1–5.

[65] A. Chorti, “A study of injection and jamming attacks in wireless secret sharing systems,” in *Proceedings of the 2nd Workshop on Communication Security*. Springer International Publishing, 2018, pp. 1–14.

[66] M. Miroslav, A. Chorti, E. Belmega, and M. J. Reed, “Man-in-the-middle and denial of service attacks in wireless secret key generation,” to appear in IEEE Proc. Global Communications Conference (Globecom), Dec. 2019.

[67] S. M. Perlaza, A. Chorti, H. V. Poor, and Z. Han, “On the tradeoffs between network state knowledge and secrecy,” in *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, June 2013, pp. 1–6.

[68] 3GPP, “Study on the security for 5G URLLC (Release 16),” 3rd Generation Partnership Project (3GPP), Technical Specification (TR) 33.825, March 2019, version 0.4.0. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/ SpecificationDetails.aspx?specificationId=3548