Zoli *et al. EURASIP Journal on Wireless Communications and Networking* (2020) 2020:114
https://doi.org/10.1186/s13638-020-01712-6

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Physical-Layer-Security Box: a concept for time-frequency channel-reciprocity key generation

Marco Zoli*, André Noll Barreto, Stefan Köpsell, Padmanava Sen and Gerhard Fettweis

*Correspondence:
Marco.Zoli@barkhauseninstitut.org
Barkhausen Institut gGmbH,
Würzburger Str. 46, 01187 Dresden,
Germany

Abstract
The motivation for this study about Physical Layer Security comes from bridging the gap between the vast theory and a feasible implementation. We propose a Physical-Layer-Security Box as a system-level Box is a system-level solution, named PLS-Box, to solve the key exchange between two wireless communicating parties. The PLS-Box performs a novel key generation method named time-frequency filter-bank. The entropy of the radio channel is harvested via a filter-bank processing, and then turned into a reciprocal security key, at both ends. In this concept work, we also focus on several PLS open issues, such as radio-frequency imperfections and accessibility to the baseband communication modem. The goal is to show a wide applicability of our PLS-Box to actual wireless systems, paving the way for an evolution of existing schemes.

Keywords: Physical-Layer Security, Key generation, Wireless communications, Cryptography, Internet of Things, Time-frequency analysis, UWB, OFDM, 5 G, 6 G

1 Introduction

Every year cybercrime and hacking cause a significant damage to citizens, institutions, and companies worldwide. The total value at risk is assessed to be $5.2 trillion over the next 5 years [1]. As confirmed by future projections [2], security and privacy are becoming crucial for the Internet of Things (IoT) [3, 4] and 5 G [5, 6], e.g., in verticals such as e-Health [7] or Industry 4.0 [8, 9]. The 5 G rollout [10] is also attracting more and more attention today regarding its security [11]; especially considering the additional features, such as reliable and mission-critical networks or Mobile-Edge Computing (MEC) [12, 13], which are particularly vulnerable.

As shown in recent reports [14, 15], new hacking threats are always on the horizon: Internet of Things botnets (e.g., Mirai 2016 and its variants, Brickerbot 2017, Hajim 2016); ransomware attacks (e.g., WannaCry 2017, SamSam 2016, CryptoLocker 2013), CPU side-channel attacks (e.g., Spectre 2018, Meltdown 2018, SWAPGSAttack 2019) and even subscriber-identification-module (SIM)-card attacks (e.g. Simjacker 2019 [16]). The importance of raising security awareness globally is clear. It is worth reminding that most vulnerabilities and breaches are likely caused by lack of basic security awareness by employees or citizens themselves (e.g., the usage of weak passwords or clicking phishing e-mails [17]). This motivates the urgent need of developing new fool-proof solutions today for the security landscape of tomorrow. The conventional approach to design secure communications is based on the computational intractability of cryptography primitives [18], usually implemented in software. Symmetric algorithms, such as Advanced Encryption Standard (AES), assure confidentiality between two parties, but require that a pre-shared key is known as secret information in order to perform encryption and decryption. On the other hand, asymmetric algorithms (such as Diffie-Hellman (DHE)) solve this key exchange problem, thanks to the mathematical intractability of factorization and discrete logarithms. Modern elliptic-curve cryptography (ECC) belongs to this category [19]. Generally, asymmetric algorithms are computationally expensive, slow, and have a high energy consumption [20]. Cryptography asymmetric primitives tend to consume three times more energy than symmetric primitives [21]. Moreover, a trusted centralized unit, known as Public-Key-Infrastructure (PKI), is necessary to manage the asymmetric keys.

Although cryptographic methods are constantly enhanced, they may not be applicable in all modern mobile contexts. Because of additional device requirements, such as long battery life, low complexity, low computing power, and small memory [22, 23], there is in fact a whole research field dedicated to the so-called lightweight cryptography [24]. This is considered more suitable for IoT, with security schemes specifically designed for resource-constrained devices [25].

To complete the picture, it is worth mentioning that asymmetric cryptography will be no longer secure with the advent of quantum computers [26]. In line with the emerging paradigm of post-quantum-cryptography (PQC) [27, 28], today there is an increasing demand for longer security keys in conventional security schemes [29]. The consequences are likely more overhead and latency in the actual communications and databases.

Generally, across the protocol stack from application layer (APP) to the physical layer (PHY), layers are ideally modular and independent. In practice, security functionalities instead might be redundant and inefficiently integrated. Therefore, cross-layer security solutions come into play [30, 31], alternatively to conventional cryptography.

Within this evolving context, new solutions, such as Physical-Layer Security (PLS), are currently under investigation as potential technologies to provide a complementary and flexible layer of security. Among different methods, we can cite channel-reciprocity key generation (CRKG), wiretap coding [32], and physical-unclonable function (PUF) [33–36].

Originally, PLS dates back to the late 1940s [37–39]. Over the years, the PLS paradigm has been emerging from different complementary fields, and more recently, it has been investigated for many applications: TV/radio systems [40], ultra-wideband (UWB) systems [41], WiFi [42], Bluetooth [43, 44], power-line-communication [45], optical fibers [46], satellite links [47], vehicular communication [48], visible light communication [49], and underwater communication [50]. However, to the best of our knowledge, it has not been fully commercially developed and exploited yet. In a nutshell, PLS implements some security functionalities down at the PHY, to achieve improvements in speed, energy, resilience, and isolation. The innovative strength of PLS relies upon the exploitation of the inherent randomness in the communication channel, electronic circuits [51, 52], and radio-frequency (RF) systems [53]. PLS can in fact leverage on unpredictable entropy sources, such as the radio wave propagation, which varies due to mobility and environmental changes.

In conclusion, PLS offers interesting opportunities today, but it is not completely clear how it could be efficiently integrated in existing security frameworks. As far as we know, so far, only few research projects (e.g., Phylaws [54], WiPhyLoc8, and Prophylaxe [55]), and laboratory prototypes have been dedicated to PLS. All of this demands the need of further research for practical solutions.

Our contributions in this work about PLS are:

- Addressing the open issues for implementation of PLS Key Generation, bridging the gap between literature and practice;
- Presenting a new PLS system-level solution named PLS-Box to solve the key exchange between two wireless communicating parties, different from conventional cryptography algorithm;
- Presenting a novel key generation quantization method named time-frequency filter-bank with some examples;
- Proposing a preliminary unified framework for Physical-Layer-Security Key Generation for easy comparison and future development in the research community.

The rest of the paper is organized as follows: Section 2 describes the PLS state of the art. In Section 3, our PLS-Box concept is presented, with implementation issues discussed in Section 4. A novel time-frequency analysis for CRKG is described in Section 5. This leads to Sections 6 and 7, where the filter-bank quantization method is described and some examples are provided in line with actual wireless systems. Finally, in Section 8, a framework to assess the PLS-Box CRKG performance is provided.

2 State of the art

In the IoT era, a mobile device is equipped with many sensors and intelligence, within an heterogeneous architecture. Given that, it is reasonable to expect that PLS will be influenced also by other fields [56], such as hardware security or biometrics [59], along its evolution path. Potentially, CRKG and RF fingerprinting [60] techniques can be revolutionary for key-exchange and authentication problems, but they still have limited and contradicting performances, as reported in current literature. For example in [61], 1 min is necessary to generate 128 bit of security key, whereas in [62], in theory, only 16 ms are estimated for 256 bit of security key.

Traditionally, three entities are considered to investigate the security of a communication channel: Alice, Bob, and Eve. Alice wants to privately send messages to Bob and vice versa. Eve is instead a malicious entity, who wants to eavesdrop on the Alice/Bob messages or interfere with them [31, 63].

In literature, works on PLS are numerous [64]. For the sake of simplicity, we hereby divide them into two branches, according to [65].

2.1 Key-less

Key-less PLS is based on information theory, leveraging on the secrecy capacity concept, given by the pioneering works of Shannon [37] and Wyner [38]. As explained in [62], the key-less PLS consists of building codes for secrecy, without using security keys: Alice and Bob encode the data to communicate in such a way that Eve cannot be able to decode [66], thanks to the performance gap between the legitimate channel and the eavesdropper's channel. The so-called secrecy capacity characterizes the maximal rate at which this successful coding between Alice and Bob may work. Today, the literature is vast [67, 68], including multi-antenna and multi-user PLS schemes, developed in parallel to Multiple-Input-Multiple-Output (MIMO) communications over the last decades. For example, artificial noise techniques [69–71] or wiretap coding [72] fall into this branch.

In a nutshell, key-less PLS has some advantages:

- Bit-stream security, with no key generation;
- Suitability for time division duplex (TDD) and frequency division duplex (FDD).

and disadvantages:

- Partial reduction of communication capacity (i.e., data rate);
- Assumptions on channel state information (CSI) and/or radio channel statistics;
- Required knowledge about eavesdropper capabilities, such as number of antennas and noise level.

2.2 Key-based

Key-based PLS (named CRKG in the following) extracts keys from a common source of randomness, as suggested initially in [39, 73]. In wireless communication systems, the channel itself is the source, as it varies randomly in time, space, and frequency. Basically, there are two fundamental assumptions:

1. The radio channel is reciprocal, such that Alice and Bob experience the same wireless medium and so can share the same secret. Unfortunately, this is not practically true for frequency-division duplex (FDD) systems, where uplink (UL) and downlink (DL) occur in separated bands. This is possible however in TDD, which is increasingly the duplexing scheme of choice for wireless systems.
2. The scenario offers a spatial protection (i.e., spatial decorrelation) against attackers. Eve's radio channel is probably very different from Alice's and Bob's, because Eve cannot be superimposed to Alice's or Bob's positions. However, the well-known assumption of a correlation distance equal to half-wavelength (i.e., $\lambda/2$) [40] may not hold in reality, as demonstrated by [61, 74, 75].

One way to accomplish key-based PLS is by processing the received-signal-strength indicator (RSSI) [75–77]. RSSI is a PHY metric computed as an average received power over a certain time of the communication signal. Since it depends on the RF chain as well as the analog-digital conversion (ADC) and so is vendor-dependent. Since it is generally available in most wireless modems/interfaces, RSSI has been widely adopted for key-based PLS experimental works. RSSI-based CRKG primarily benefits from a time-variant scenario: since the terminals are moving (or there are significant mobile objects/people in the surrounding), the security key is generated from received power fluctuations (i.e., fading). In general, the acquisition rate of RSSI limits the key quality and size. For instance, in a scenario with limited mobility, the fading has little temporal variation, and so, RSSI methods become generally very slow and inefficient. For example, in [76] 8 min are necessary to generate 256 bit of secret key. Moreover, in [78], the RSSI key-based scheme [79] is demonstrated to suffer from sabotaging of key generation that reveals up to 47% of the generated secret bits.

Differently, the CSI CRKG methods generate secret keys from wideband observations of the channel, such as channel impulse response (CIR) or channel transfer function (CTF) (e.g., OFDM sub-carriers) [80]. This is the approach we follow in this work.

In a nutshell, key-based PLS has some advantages:

- Easy experimental set-up [43, 76], for instance using software-defined-radio (SDR), Zigbee or WiFi cards;
- Compatibility with modern encryption methods, since only the key distribution method is addressed;
- Peer-to-peer key exchange without a centralized control.

and disadvantages:

- Suitability only for TDD systems, as it requires a reciprocal channel;
- Constraints from the radio channel characteristics.

2.3 Key-less vs key-based comparison

Practically, key-less PLS addresses confidentiality directly encoding the data thought the channel. Then, the performance directly depends on the knowledge of the channel characteristics, such as signal-to-noise ratio (SNR), and Eve's capabilities. However, the profile of an attacker is usually difficult to estimate a priori. If Eve is more powerful than expected, (e.g., by having a very large number of antennas or a low-noise receiver), then, the effective security capacity may be effectively lower than the employed data rate. The system might become intrinsically insecure.

Key-based PLS, on the other hand, may rely on existing and well-established symmetric encryption schemes to ensure confidentiality, addressing only the CRKG key generation. This decoupling aspect allows to flexibly renovate the encryption key on demand or to change the key strength if necessary.

Because of these considerations, we argue that key-based PLS is more likely to be integrated more easily into a realistic overall security concept.

3 PLS Box

We present hereby the PLS-Box with a high-level description of its functionalities. The PLS-Box is conceptually similar to hardware-security-module (HSM) [81] or Trusted-Platform-Module [82, 83]. The goal of the PLS-Box is to perform CRKG from the received communication data, as depicted by the block diagram in Fig. 1.

The important point here is the interaction between our PLS-Box and the wireless baseband communication modem. In reality, as shown by [84], it is hard to claim if a given modem is trustable or not, since is the only point of access to the radio channel. Therefore, we define 3 ideal configurations:

- The box is implemented as part of the modem and so has low-level access to all PHY features. This is the usual assumption in literature. This way is called "modem-aided" in the following;
- The box bypasses the modem and operates independently (Fig. 1). In this case, the box needs only a minimum amount of information from the modem, such as a trigger signal of incoming received frame, for example. This way is called "blind" in the following.

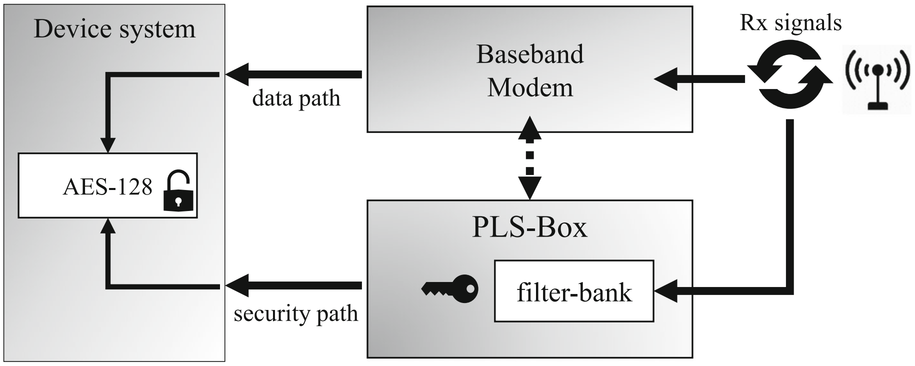

Fig. 1 System-level description of the PLS-Box at receiver side. The PLS-Box is independent form the baseband modem, providing a security path for the key generation. The data decryption is performed externally with AES-128, for example

However, there is a general trade-off between security and efficiency: the modem needs the box to encrypt and decrypt the data, whereas the box needs the modem to access the radio channel or the received signal. Practically, replicating all the modem functionalities (such as synchronization, mixing, sampling and channel estimation) in the box is costly and redundant, while adding the PLS blocks in the modem requires its full re-design. However, considering the overall security on a device, it is worth adopting a principle of isolation among the chips preventing the spread of a malicious attack, even at PHY.

Finally, in terms of cross-layer security, the PLS-Box could pass the generated key to perform conventional encryption (see Fig. 1). Alternatively, the PLS-Box itself can perform decryption (and encryption) of the communication data already at PHY.

Before describing the novelties of the PLS-Box in details, it is necessary to define the CRKG protocol which the PLS-Box is supposed to perform, in line with [31, 67, 68, 85, 86].

3.1 CRKG protocol

- Authentication: Alice and Bob must trust each other before performing CRKG. This preliminary stage could be achieved in a conventional way [85], by exploiting, for example, secret keys stored by the devices manufacturer and challenge-response authentication methods. Alternatively, there are PLS techniques, such as PUF [87], vicinity-solution [61], or radio-signature authentication [85, 88, 89]. RF fingerprinting can be implemented today with good results [60, 90–95], thanks to the power of classification and clustering of machine and deep learning [96–98]. At this stage, Eve can try to impersonate Bob or Alice, playing a man-in-the-middle attack [85]. Authentication is out of scope of this work.
- Channel probing: While Alice and Bob exchange frames for communication, their PLS-Boxes work for security. If the modem access is granted to the PLS-Box, the focus could be on the frame preamble of the received signal. Such preamble contains sounding sequence (e.g., Zadoff-Chu) which are commonly available for communication tasks (e.g., channel estimation [99], carrier recovery, and synchronization) and therefore suitable to probe the radio channel for CRKG. Differently with no modem support, the PLS-Box can acquire the received full frame

and process it for CRKG. During this stage of the protocol, Eve can perform several attacks [100]. For example, in [74], a stalking attack is performed by Eve in proximity of Bob, obtaining successfully up to 97% of the CRKG key. In IoT scenarios, Eve can be represented by a multitude of nodes (e.g., botnet), which can cooperate passively to wiretap the Alice-Bob link in multiple positions, even simultaneously at both ends. Being part of the network, Eve is likely to be similar to Alice and Bob. Anyway, it can also have more powerful hardware, and with that, it can produce intentional interference, namely jamming [40, 85]. The negative consequences of this attack could be unbalanced-reciprocity in Alice and Bob signals, or a forced repetition of the CRKG scheme, as sort of denial-of-service. This could be harmful, because Eve might attempt to trigger multiple CRKG sessions and crack the key.

- Quantization: After gathering enough frames, the PLS-Box must transform signals into security keys. This is the crucial stage called quantization. It is of course a lossy operation. PLS key-based methods commonly use thresholding or level-crossing algorithms [79, 101]. The ideal goals are:
  - Alice and Bob agree on the same key, regardless of additive white Gaussian noise (AWGN), interference, RF impairments and TDD delays, and Eve's attacks;
  - The quantized-generated key is random;
  - Quantization is fast and adaptive to radio channel conditions.

  In this work, we propose a filter-bank processing as basis for quantization in Section 6.
- Reconciliation: Even though Alice and Bob experience the same channel, they may end up with different keys, as aforementioned. The reconciliation stage corrects these mismatching errors. For example, forward error correction (FEC) schemes, such as Bose Chaudhuri Hocquenghem (BCH) codes or Secure-Sketch [102, 103] can be set to refine the quantized key and fix up to 20% of the bits [61]. Unfortunately, the reconciliation imposes an additional data exchange between Alice and Bob, and so, Eve can perform other attacks. It is worth reminding that reconciliation is a delicate stage, because the whole PLS CRKG scheme collapses if Alice and Bob do not match the generated key perfectly. Reconciliation is out of scope of this work.
- Privacy amplification: Privacy amplification is usually included as the last stage in order to maximize the entropy of the reconciled key, thanks to one-way cryptography, such as hash functions. Amplification is out of scope of this work.
- Symmetric encryption: Once the Alice/Bob key is ready, any symmetric encryption scheme (e.g., AES) can provide confidentiality. It can be implemented by hardware or software, by the PLS-Box or externally.

4 PLS-Box implementation issues

Figure 2 represent the first step towards a broad PLS implementation inside a wireless transceiver. In details, the PLS authentication methods might acquire unique RF fingerprints (i.e., signatures) from the transmission path, such as local oscillator (LO), mixer, and power amplifier (PA) blocks. Instead, the key-less PLS might operate digitally beyond the ADC, as part of the channel coding.

On the other hand, the key-based PLS works on the data obtained from the receiver path. Considering practical implementation, it is not defined yet at which section would be better to operate: ideally, the best option is the modem-aided way, where the PLS-Box

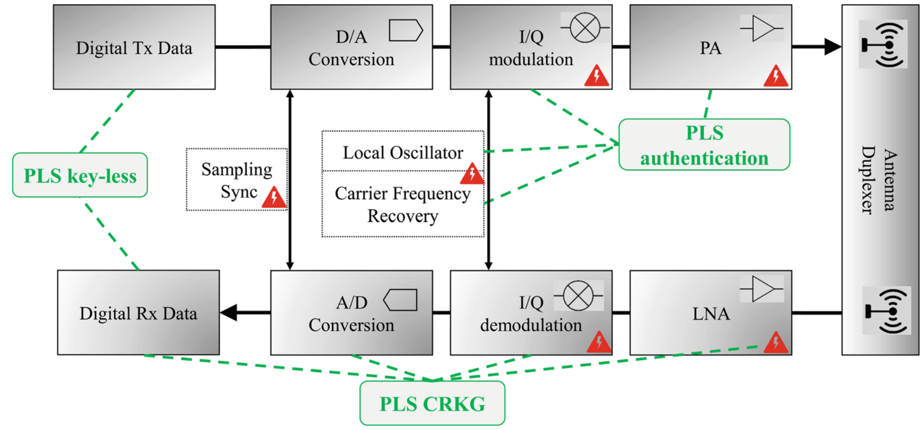

Fig. 2 Block diagram of RF transceiver with PLS extensions: PLS blocks in green and RF impairments in red

has at disposal the full received frame at baseband, with RF impairments compensated and the data payload decoded. On the other hand, in a blind way, a possible solution is to perform only down-conversion and sampling on the received signals, without any intent of data demodulation or decoding.

In the end, the compensation of RF impairments remains a big open issue, because they represent, in fact, the constraints to Alice-Bob reciprocity and key matching. For instance, a base station (BS) has better equipment than any user equipment (UE) (e.g., number of antennas, better LNA, and better ADC). The differences in RF transceivers are hence reflected in signal imperfections, asymmetrically. The same frame in UL and in DL is differently influenced by the diverse RF hardware [104], even in TDD systems, although the radio channel has not changed at all.

We list here several hardware non-idealities that should be taken into account for PLS CRKG realistic results:

- PA distortion: Caused by the non-linearities present in the transmission PA [105–107]. The distortion consequences are represented by the growth of undesired harmonics (out-of-band and in-band), named inter-modulation effects;
- Phase noise: Caused by imperfections in the LO [105, 106, 108]-generating small phase drifts in the mixing stage, during up/down-conversion;
- Carrier frequency offset (CFO): The CFO are frequency shifts of the incoming signals, with respect to expected carrier frequency [105, 108], due to LO skew (i.e., thousands of Hz) and Doppler effect (i.e., hundreds of Hz at most);
- I/Q imbalance: Caused by differences between the in-phase and quadrature components and by non-idealities of the LO [105, 106, 108, 109];
- ADC non-idealities: ADC imperfections, such as clipping, bias, and jitter, may negatively contribute to alter synchronization and sampling between Alice and Bob [105, 107];
- Noise: AWGN thermal noise power level can differ between Alice and Bob, due to different receiver temperatures and different hardware.

In conclusion, there are several open issues: where to allocate the PLS blocks along the RF chain, whether to trust or not the baseband modem, and how to account for the impact of non-reciprocal hardware impairments.

5 Time-frequency CRKG

Regarding the channel probing and the quantization stages of the CRKG protocol, we introduce here the considerations which lead to the idea of the filter-bank. Table 1 shows important radio channel parameters for a time and frequency analysis, as explained in the following.

5.1 Time-domain

Wireless links are often quasi-static. Channel fluctuations in time (i.e., time-selectivity) in communications are a secondary issue in many scenarios, such as home, office, shopping mall, restaurants, and city center. To assess such channel time variations, the well-known coherence time T_{coh} [110, 111] is used to describe a time window where two channel realizations (i.e., frames) are correlated along time. In reality, apart from high-speed trains, satellite, or flying objects, T_{coh} ranges from 1 ms up to 250 ms. With reference to Table 1, the T_{coh} is inversely proportional to the Doppler spread (ν_{DPS}), which is the dispersion metric that accounts for the frequency shifts in the communication bandwidth, due to the mobility of terminals. We define t_p as the PLS-Box probing time, defined as the time interval between two received frames (Fig. 3). T_{coh} can be many orders of magnitude larger than the channel probing interval t_p, depending on the PHY specifications. This means that Alice and Bob are likely to sound the channel in a reciprocal way before it changes irreversibly and so extract the same key.

With this in mind, it is possible to make important considerations on the limits of RSSI-based CRKG. Generally, at the baseband, a narrowband radio channel is modeled as a complex Gaussian stochastic process (with Rayleigh amplitude and uniform phase distribution), representing a model for NLOS small-scale fading. Given the received signal envelope and a threshold set for its level crossing, the well-known level-crossing ratio (LCR) and the average fade duration (AFD) are expressed by the following Eqs. (1 ,2), as fading parameters:

$$\mathrm{LCR} = \sqrt{2\pi} f_D \rho e^{-\rho^2} \tag{1}$$

$$\mathrm{AFD} = e^{(\rho^2)-1} \; / \; (\sqrt{2\pi} f_D \rho), \tag{2}$$

where f_D is the maximum Doppler shift and ρ is the ratio between the LCR threshold and the root-mean-squared level of the signal envelope [110]. The ideal situation is given by the scenario where the channel fading has large LCR and short AFD, meaning, respectively, that the keys are likely to have 0s and 1s uniformly distributed (i.e., no long consecutive sequence of 0s or 1s). According to the above equations, this can be achieved by increasing the parameter f_D. This can be experienced only with fast moving terminals (or at very high carrier frequency), as confirmed experimentally by [44]. f_D is not a design parameter, and, essentially, it limits the RSSI methods. The same conclusions are supported by [112], where the RSSI CRKG upper bound is computed with Nakagami fading. For an extension of the above equations with non-Rayleigh fading see [113, 114]. For sake

Table 1 Time-frequency parameters

Domain	Dual	CRKG	Channel
Time, t	$\xrightarrow{\mathscr{F}}$ ν Doppler	t_p	$T_{\mathrm{coh}} \propto 1/\nu_{DPS}$
Frequency, f	$\xleftarrow{\mathscr{F}}$ τ Delay	f_p	$B_{\mathrm{coh}} \propto 1/\tau_{DS}$

$\mathscr{F}$ indicates Fourier transform of brevity, we focus in the following on our novel filter-bank approach which is by-design independent on the kind of fading. It is worth stressing that Rayleigh-fading assumption across literature [100] might not be found in real systems, where the radio channel statistics are usually not known, must be estimated and are likely to be ruled by Rice-fading (e.g., in indoor environments). As well as for communications, it is worth recommending realistic channel models as shown in [115].

5.2 Frequency-domain

Differently from time-domain variations, the channel multipath is instead nearly always present, independently from terminal movements. In some situations, such as point-to-point links, strong LOS, beamforming-based, or narrowband signals, the multipath components (MPC) may not be noticeable. However, in most cases, particularly with broadband communications, the channel multipath can be used for the generation of keys (i.e., CSI-based CRKG).

Depending on the antennas, a received signal is generally composed by a multitude of attenuated and delayed replicas of the transmitted signal, because of the propagation interactions among the emitted electromagnetic radio waves and the surrounding environment (e.g., buildings or walls). The channel distortion (i.e., frequency selectivity) can be exploited for our CRKG purposes, considering to have enough bandwidth to resolve the multipath components. This is why we deem the multipath as a more reliable feature of the wireless communications for PLS, rather than fading. In other words, the multipath can be considered a signature of the channel, dependent on the environment, the antennas, and the terminal positions.

Similarly to the previous consideration on T_{coh}, the well-known coherence bandwidth B_{coh} (see Table 1) [110], describes the bandwidth at which two frequencies are likely to be correlated. It ranges from tens of kHz up to hundreds of MHz, depending on antennas, propagation scenario (i.e., urban, suburban, and rural) and carrier frequency, and it is inversely proportional to the delay spread τ_{DS}. Then, we define f_p as the frequency interval at which the PLS-Box samples the bandwidth of the received signal (see Fig. 4).

There are already evidence confirming that the frequency domain offers superior performance and more flexibility for PLS: in [42], a key generation of 90 bits per packet is obtained between Alice and Bob, with only $5 \sim 10\%$ of key mismatch, whereas, approximately, only tens of bit per second are generated via RSSI methods.

6 PLS-Box filter-bank model

A combined time-frequency analysis benefits from multipath and mobility to harvest entropy for CRKG. The validity of this approach is additionally confirmed by how efficiently the radio resources are commonly scheduled in a time-frequency grid (e.g., time slots and sub-carriers) in actual wireless networks (e.g., LTE, 5 G).

Considering a general model for the filter-bank, the starting point is represented by the following:

$$y(t) = h(t) * x(t) + n(t); \tag{3}$$

where x is the transmitted signal, n is the AWGN component, h is the baseband radio channel transfer function, y is the received signal, and * denotes the convolution operator.

The channel h can be characterized by a time-variant complex impulse response [61, 116]:

$$h(t,\tau) = \sum^{N_p} \alpha(t) \cdot e^{-j\phi(t)} \delta(t - \tau(t)), \tag{4}$$

where N_p is the number of multipath components (MPC), the set of $[\alpha, \phi, \tau]$ are, respectively, the random amplitude, phase, and propagation delay and $\delta(t)$ is the Dirac delta function.

Alternatively, Eq. (4) can be rewritten with an explicit time-frequency representation of the channel:

$$h(t,f) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} S(\tau, \nu) \cdot e^{j2\pi(t\cdot\nu - f\cdot\tau)} d\tau d\nu, \tag{5}$$

whose parameters are summarized in Table 1. The function $S(\tau, \nu)$ is the delay-Doppler spread function [117, 118]. This describes how the energy transmitted is dispersed in delays (τ) and Doppler (ν) shifts through the channel, which is, in fact, the unpredictable chaotic nature of the radio channel.

In our PLS context, the signal $x(t)$ is the transmitted frame by Alice to Bob and vice versa, as sketched in Fig. 3 (we assume $h_{AB} = h_{BA}$). In practice, the PHY characteristics of the signal are constant in a short term, but the content of the frame (e.g., payload) might change. Alice and Bob are primarily communicating and not sounding the radio channel. So, in a modem-aided CRKG, we can assume that the PLS-Box has perfect knowledge of $x(t)$, being capable to detect, demodulate, and decode $y(t)$. In a blind CRKG, the PLS-Box operates on $y(t)$ with limited knowledge of $x(t)$. For example, the box knows only when a frame starts and ends or which bandwidth is used. In the following, we assume a blind CRKG with $x(t)$ as a $\delta(t)$ of Dirac, negligible AWGN noise $n(t)$ and $y(t)$ available at baseband.

Then, we define a filter-bank block Fb as a set of M filters which process N received frames, sampled at intervals f_p and t_p, respectively. The goal is to project the received frame y over M parallel filters in the frequency domain, providing at the end $M \cdot N$ outputs to the quantization stage of CRKG. This not only increases the key generation rate, but also adds more degrees of freedom to the key generation.

Figure 4 depicts the filter-bank outputs, represented by the matrix $\underline{C}$ in a time-frequency plane, derived according to the following equations:

$$C_{(m,n)} = \frac{1}{\gamma} \int_{(n-1)t_p}^{nt_p} y(t) * Fb_m(t) dt, \qquad \forall n, m \tag{6}$$

$$Key = \text{Quant}\left(\begin{bmatrix} C_{(1,1)} & \dots & C_{(1,N)} \\ \vdots & \ddots & \vdots \\ C_{(M,1)} & \dots & C_{(M,N)}, \end{bmatrix} \right), \tag{7}$$

where n is the frame index, $1 \leq n \leq N$, m is the filter index within the filter bank, $1 \leq m \leq M$, $1/\gamma$ is an arbitrary normalization factor, and $Fb_m(t)$ is the impulse response of the mth filter. The functional Quant$(\cdot)$ in Eq. (7) represents the quantization process, which can be done in different manners [31], and is out of the scope of the work.

In other words, the received signal $y(t)$ is filtered by different band-pass filters, such that the filter outputs $C(m, n)$ reflect an estimate of the magnitude of the channel frequency response $h(t)$.

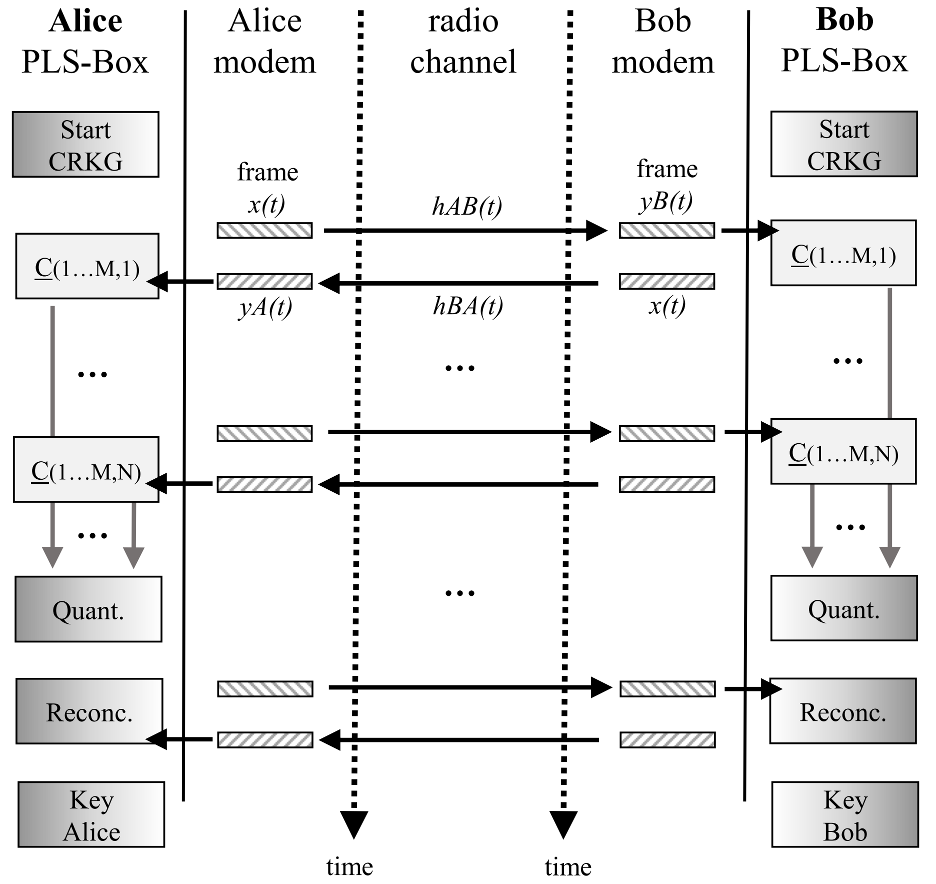

Fig. 3 Sequence of messages between Alice and Bob to perform time-frequency filter-bank CRKG. The $x(t)$, $yA(t)$, $yB(t)$, $hAB(t)$, and $hBA(t)$ are described in Eq. (3), where A means Alice and B means Bob. The C is the set of M filter-bank outputs described in Eqs. (6) and (7)

According to the data processing inequality theorem, the filter-bank can only obtain equal or minor entropy with respect to what is initially available from the radio channel. However, in principle, by observing the radio channel both in time and in frequency, we can operate over two dimensions, and so extracting more entropy, rather than by means of solely temporal fading, e.g. RSSI-based CRKG. The filters can be a uniform grid of finite-impulse response (FIR) filters, but they can be also implemented using fast Fourier transform (FFT) or even wavelet transform. The big advantage of the proposed filtering approach is flexibility, as shown in Section 7. It works with any chosen communication waveform, as long as t_p and f_p are given. It allows us to choose both M, N, depending if the received frames are correlated in time, i.e., T_{coh} is larger than t_p, or in frequency, i.e., B_{coh} is larger than the f_p, (see Table 1). Depending on the channel conditions, an additional step of whitening [119] may be performed on the filter-bank outputs $\underline{C}$ in order to remove time-frequency correlations among filters.

In the end, the time-frequency filter-bank key generation comes with some challenges. It is necessary to have enough bandwidth to capture the multipath. For example, LoRa [120] or Bluetooth [43] are too narrowband, whereas in 5 G, WiFi or UWB [121], the available bandwidth ranges from tens to hundreds of MHz, enabling the frequency-domain filter-bank (e.g., 5 G has 800 MHz of maximum available bandwidth [122]). This

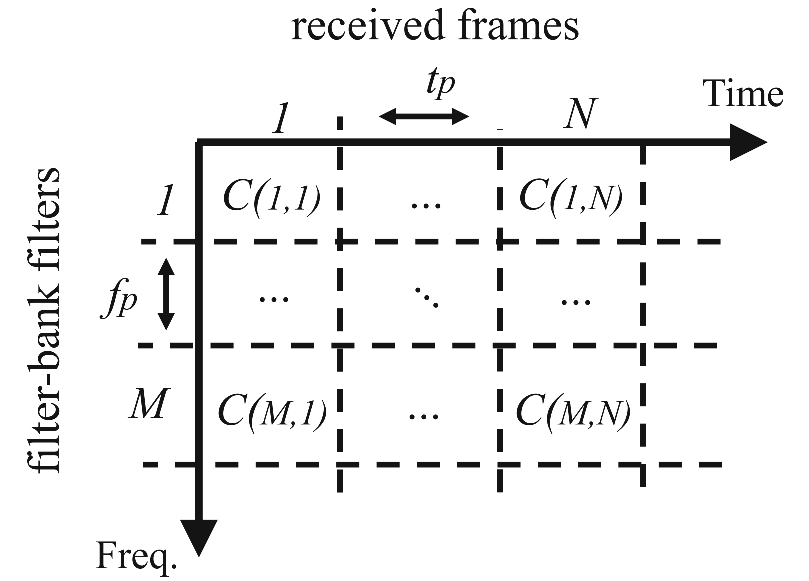

Fig. 4 Abstract representation of the filter-bank time-frequency plane. The $C_{(m,n)}$ is the filterbank output of the *n*th frame and *m*th filter

positive trend is also supported by current research on mm-wave [123, 124] and THz bands [22, 125], pushing for Gbps data rate.

6.1 Example of filter-bank input-output correlation

To demonstrate the potential of the filter-bank, we performed a simple simulation. Thanks to the property of the channel model QuaDRiGa (QUAsi Deterministic RadIo channel GenerAtor version 2.2.0) [126], we investigate the performance of the filter-bank CRKG in the urban 3GPP TR38.901 UMi [127] scenario. A micro base-station (Alice) is located at a 10-m height, in the middle of an ideal circular cell of 500 m^2. It serves 100 UEs (i.e., Bobs) randomly dropped in the area, with 50% indoor probability and uniformly distributed, with 0.5 to 3 m of height. For each UE (Bob), an eavesdropper UE (Eve) is located at 1 m of distance along a random direction on the horizontal plane. The frequency carrier is set to 2 GHz, all the UEs are static, and, for the sake of simplicity, the radio channel is assumed perfectly reciprocal, noiseless, and interference free. Therefore, the simulation is not meant to be representative of all scenarios, but to provide preliminary hints of the filter-bank potential.

As shown in Table 2, the Pearson coefficients are calculated on inputs-outputs of the *Fb* in order to evaluate the correlation between Bob and Eve. The simulation includes 6 different bandwidths and 2 different filter-bank settings with M=32 and M=512 filters.

Ideally, the Pearson coefficient between Bob and Eve should be 0.0, showing a perfect isolation between Alice/Bob and Eve. As confirmed also experimental work by [61], in reality, the correlation might vary significantly due to the radio channel. However, several results are interesting:

- Firstly, before the filter-bank, the Pearson coefficients computed on the received signal in time, i.e., $y(t)$, are higher than the same signal in frequency, i.e., $Y(f) = FFT(y(t))$ (see columns 2 and 3 in Table 2).

Table 2 Example of correlation between Bob and Eve in the simulated 3GPP TR38.901 UMi scenario

Pearson coefficients (average on 100 UEs)				
Bandwidth	Before *Fb*		After *Fb* on $\underline{C}$	
MHz	On $y(t)$	On $Y(f)$	$M = 32$	$M = 512$
10	0.85	0.48	0.59	0.47
20	0.82	0.45	0.50	0.42
40	0.75	0.35	0.48	0.33
80	0.68	0.33	0.45	0.24
160	0.62	0.30	0.36	0.20
250	0.60	0.32	0.31	0.19

- Secondly, with larger bandwidth, more multipath components can be resolved by the filter-bank. So, correlation is decreasing proportionally with bandwidth (along rows in table). The propagation differences are more pronounced between Bob and Eve.
- Thirdly, after the filter-bank (see columns 4 and 5 in table), the correlation on $\underline{C}$ is less than before the filter-bank (see columns 2 and 3 in table) on y or Y.
- Finally, after the filter-bank, it is evident that with M=512 (column 5 in table), the filter-bank $\underline{C}$ is less correlated with respect to M=32 (column 4 in table). Because the frequency-domain resolution is increased (i.e., f_p is smaller), Bob and Eve differences can be easier spotted out.

7 PLS-Box filter-bank examples

In the following, two examples of PLS-Box CRKG are given: a OFDM example, compliant to actual system as 5 G or WiFi [128] (Fig. 5), and an UWB example, as an emerging technology for indoor localization [129] (Fig. 6). Both examples follow the general diagram depicted by Fig. 3, but differentiating between a case of modem-aided PLS-Box and a case of blind PLS-Box, respectively

7.1 Modem-aided filter-bank

PLS in OFDM systems is not new, as shown by [99, 130–134]. All the essential structures for our time-frequency CRKG processing are ready: RF impairments are compensated [106], radio channel is estimated [99, 135], and the bandwidth spans from tens to hundreds of MHz.

In this example, the filter-bank is directly implemented via FFT/IFFT, inside the PHY OFDM modem. Ideally, all the sub-carriers should be used to sound the channel at once, over the full bandwidth. In practice, the PLS-Box might use the CSI collected from the sub-carrier pilots for key generation, according to the pilot allocation of the OFDM system. In terms of signal acquisition for PLS, this solution is somehow equivalent to well-known channel sounding technique based on Vector-Network-Analyzer (VNA) [136].

Assuming independent sub-carriers and 1 bit quantization for each sub-carrier, the resulting key generation rate is increased by a factor proportional to the FFT size, e.g., in the range of 64–6400, with respect to RSSI schemes. Approximately, considering 15 KHz as sub-carrier spacing and 100 MHz of bandwidth, at least 6666 sub-carriers/-bands are available for the filter-bank, for example.

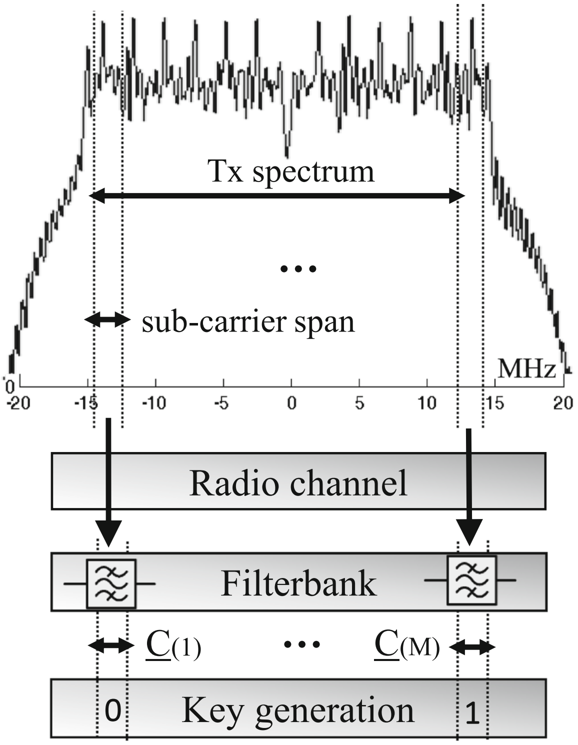

Fig. 5 Qualitative representation of modem-aided PLS-Box filter-bank with an OFDM waveform

Of course, dedicating radio resources to PLS-Box security reduces the communication performance. However, the pilot tones and the preamble are already part of the OFDM PHY, so in principle, the PLS-Box is only re-using information available in the modem, with negligible overhead.

In terms of security, the proposed OFDM CRKG solution is even supported by the literature [42]. In [137], Eve attacks Alice/Bob introducing controlled movements of an object in a static indoor environment, causing intentionally predictable changes in Alice/Bob received power, (i.e., LOS/NLOS switching). So dictating the RSSI oscillations, the key generated has predictable periodic bit sequences. Then, [42] proposes a PLS scheme in a OFDM systems against such channel attack, showing that the LOS/NLOS strikes are not present in all the OFDM sub-carriers, and so, a high-entropy key can be anyway extracted, thanks to frequency diversity.

Moreover, assuming that complex CSI is attainable at OFDM PHY and reciprocal [138–140], the CSI phase domain represent a CRKG opportunity to be further explored for several reasons. In line-of-sight (LOS)-dominant scenario, the channel is flat (i.e., non-selective) inhibiting the filter-bank method. Therefore, the channel phases represent the last resort to harvest entropy. In fact, as shown in [141] by means of ray-tracing Eve's attack, the CSI phases cannot be predicted accurately as good as the CSI magnitude. In addition, analyzing the signal phases over multi-antenna ports allows to estimate angle-of-arrival (AoA) spectrum (e.g., using MUltiple SIgnal Classification (MUSIC) algorithms), opening the opportunity to use also the angle domain for PLS [142]. In the end, taking into account the aforementioned RF impairments and practical non-reciprocity issues, it is not completely clear if the CSI phase is an effective reliable parameter for

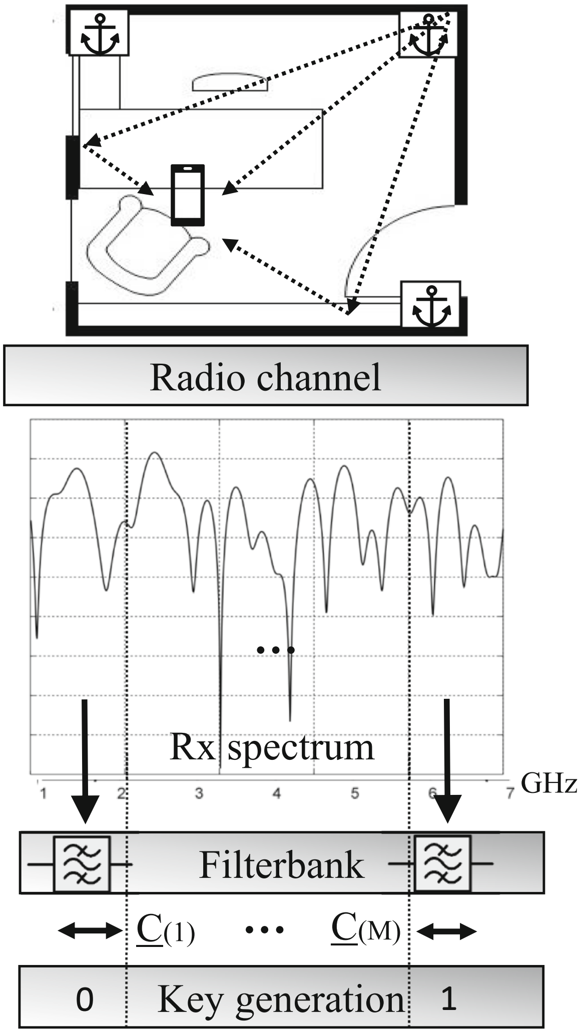

Fig. 6 Qualitative representation of blind PLS-Box filter-bank with an UWB waveform

practical CRKG. Actually, there is no sufficient evidence in literature to be confident that phase CRKG could work in practical systems. Moreover, radio channel phase estimation is definitively more challenging rather than RSSI or scalar CSI. Further research is necessary.

7.2 Blind filter-bank

UWB systems perform indoor localization and communication, in line with IEEE 802.15.4 [143–146]. Several works [147–151] have already performed investigations on PLS in UWB systems: [152] obtains a key generation rate of 18 bps and [41] shows that Eve correlation can reach 50%. However, to our knowledge, no investigation has been published so far regarding a time-frequency approach for UWB PLS key generation, such as the filter-bank here presented. In order to do so, we can in fact take advantage of the natural GH span of bandwidth of the UWB waveform [121].

We assume to have a blind PLS-Box which is filtering the received UWB frame, independently from the UWB modem. The processing is described as shown in Fig. 6: a localization anchor of the UWB system placed in a corner of an office scenario is communicating with a portable device. The goal is to locate the position of the device in the room. Even though the UWB link range is a few meters and LOS, the frequency selectivity is expected to be significant, thanks to the impulsive nature of the UWB waveform. In terms of signal acquisition, this solution is indeed equivalent to well-known channel sounding technique [153].

Moreover, there is an interesting synergy between UWB and PLS [154]. The localization information about the terminal positions (attained by the UWB system) represents a threat for the PLS schemes, due to ray-tracing attacks [155]. This means that if the UWB modem is compromised, the positions of Alice and Bob might be spoiled. Then, Eve might simulate correctly the radio channel and try to predict the CRKG key. For example, in [141], a ray-tracing attack is investigated in a common office scenario at 2.4 and 5 GHz: the mean absolute error is less than 2 dB, between the narrowband received power predicted by the ray tracing and the measurements (i.e., comparable to real-life case). It is hard to forecast the impact of this attack on real mobile wideband system. With the increasing trend of environment digitization and virtual/augmented reality, indoor/outdoor digital maps be easily available online. Furthermore, with increasing computational power of devices, the time required for a complete ray-tracing simulation may be in the same order of magnitude as that of CRKG protocol (i.e., msec). Further research is necessary.

8 PLS-Box CRKG optimization

Recalling all the previous sections, the PLS-Box performance can be optimized in time and frequency and throughout the CRKG protocol. The optimization parameters are collected in Table 3.

- kT is the key generation *time* required for CRKG. Ideally, an exchange of frames (or packets) would be the minimum number: one for authentication, one for channel probing and one for reconciliation. In literature, kT is in the order of tens/hundreds of milliseconds, depending on the channel conditions;
- kS is the *size* of the final key, in number of bits (i.e., 128 bit). The key size can be shortened after reconciliation, discarding erroneous bits, and even more, after privacy amplification to maximize its randomness [61];
- $kR = kS/kT$ is the key generation *rate*, in terms of *bps* or, alternatively, bits-per-frame. For example, in [44], a $kS = 256$ bit key is obtained in $kT = 5$ s of CRKG, achieving a rate $kR = 51$ bps. Generally, in literature $kR = 10 \sim 100$.

Table 3 CRKG optimization parameters

Symbol	Description
kT	Key generation time
kS	Key size
kR	Key generation rate
kH	Key entropy
kM	Alice/Bob's key mismatch
kL	Eve's key leakage
kC	Key generation consumption

Clearly dependent on the PHY and hardware

- *kM* is the key generation *mismatch*, indicating the number of bits which are not corresponding at Alice and Bob sides. It is equivalently to the bit-error-rate for communications. Generally, in literature $kM = 2 \sim 20\%$.
- *kL* is the key *leakage* to Eve, expressing how capable Eve is to wiretap Alice and Bob. It can given directly by the number of key bits sniffed correctly or can be characterized by the mutual information among Alice, Bob, and Eve [61].
- *kH* is the key *entropy*. In literature, the quality of the key is usually addressed by means of the National Institute of Standards and Technology (NIST) tests, specifically tackling randomness [156] and entropy [157]. It is worth noticing that not all NIST randomness tests are suitable for short keys. For example, the FFT test seems to be unreliable [99, 158]. Even flaws in the NIST entropy estimators have been debated [159, 160], leaving the entropy estimation an open issue [61].
- *kC* is the key generation *energy consumption*. Equivalently in communications, the energy efficiency of CRKG can be computed as kS/kC in terms of bit/J. It is naturally hardware-dependent and useful to benchmark CRKG schemes versus conventional cryptography methods [44]. For instance, a comparison of energy consumption by [61], shows that the RSSI scheme proposed in [137] consumes 2.4 mJ versus the 101.2 mJ of ECC-DHE, implementing both algorithms in an ARM Cortex M3 processor. These are very good results, but further energy consumption comparisons are necessary to outline the advantages of PLS in practical systems.

In conclusion, the optimization of PLS-Box faces a trade-off in the CRKG: *kM* and *kL* must be minimized, that is minimum key mismatching errors and Eve's leakage; but *kS* and *kH* must be maximized, that is long keys with high entropy. The problem is that Alice and Bob have no knowledge about Eve and cannot communicating anything clear-text over the the radio channel. Moreover, their PLS-Boxes are not likely to be able to jointly cooperate to optimize the CRKG filter-bank.

However, we envision that machine learning algorithms can be utilized for this task [161–163], in order to handle the variations of the radio channel and the key quality.

For example, in case of classification of the radio channel LOS and time-invariant, the entropy is very limited. So, the PLS-Box might adaptively reduce the filter-bank number of filters entropy (i.e., LOS and time-invariant), the PLS-Box might adaptively drive the filter-bank reducing the number of filters to limit the correlation in the key bits, or fall back to RSSI-methods, or even use the phase information. Eventually, it might notify the upper layers about the inconvenient channel conditions at PHY, advising to rely on conventional schemes for key generation. This cross-layer feedback needs further investigation.

9 Conclusions and future work

After an initial overview of the security landscape of today, we have outlined the motivations of Physical-Layer Security, providing a summary of the state of the art of this promising field. In this regard, we have presented the PLS-Box as a new flexible paradigm towards an effective PLS implementation. We have discussed the open issues and challenges of this concept, such as RF impairments, accessibility to the PHY baseband modem, and attacker capabilities. In details, we have focused on channel-reciprocity-key-generation, presenting a novel strategy for time-frequency key-generation, based on filter-bank processing. This new approach aims at improving the performance of key generation, thanks to a dynamic time-frequency wideband signal processing. We have shown the general model of the filer-bank and its benefits, by means of a simple simulation in a usually 3GPP and not 3 GPP. 3rd Generation Partnership Project scenario. Additionally, two PLS-Box filter-bank examples have been described, in line with today's OFDM and UWB systems, showing the suitability and flexibility of our solutions. Our future work will be oriented to model the filter-bank, and test its performance in a real-life prototype.

Abbreviations

ADC: Analog-digital conversion; AES: Advanced encryption standard; AFD: Average fade duration; APP: Application layer; AoA: Angle-of-arrival; AWGN: Additive white Gaussian noise; BCH: Bose Chaudhuri Hocquenghem; BS: Base station; CFO: Carrier frequency offset; CIR: Channel impulse response; CRKG: Channel-reciprocity key generation; CSI: Channel state information; CTF: Channel transfer function; DHE: Diffie–Hellman; DL: Downlink; PLS-Box: Encryption box; ECC: Elliptic-curve cryptography; FDD: Frequency-division duplex; FEC: Forward error correction; FFT: Fast Fourier transform; GNSS: Global navigation satellite system; HSM: Hardware-software module; IoT: Internet of Things; KPI: Key performance indicator; LCR: Level-crossing ratio; LO: Local oscillator; LOS: Line-of-sight; MEC: Mobile-edge computing; MIMO: Multiple-Input-Multiple-Output; MUSIC: MUltiple SIgnal Classification; NIST: National Institute of Standards and Technology; NLO: Non-line-of-sight; OFDM: Orthogonal frequency-division multiplexing; PA: Power amplifier; PHY: Physical layer; PLC: Power-line communications; PLS: Physical-Layer Security; PQC: Post-quantum-cryptography; PUF: Physical-unclonable function; RF: Radio-frequency; RSA: Rivest–Shamir–Adleman; RSSI: Received-signal-strength indicator; SDR: Software-defined-radio; SHA: Secure hash algorithm; SNDR: Signal-to-noise-and-distortion ratio; SNR: Signal-to-noise ratio; TDD: Time-division duplex; TLS: Transport-layer security; UL: Uplink; UWB: Ultra-wide-band; VNA: Vector network analyzer; WBAN: Wireless body-area network; 3GPP: 3rd Generation Partnership Project; UE: User Equipment

Acknowledgements

The authors declare that they have no acknowledgements.

Authors' contributions

The authors have contributed equally to the paper. The authors read and approved the final manuscript.

Funding

This research was co-financed by public funding of the state of Saxony, Germany.

Availability of data and materials

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Received: 6 November 2019 Accepted: 15 April 2020
Published online: 05 June 2020

References

1. Accenture: Ninth Annual Cost of Cybercrime Study. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study. Online; Accessed 2019
2. IDC: Worldwide Internet of Things Spending Guide. https://www.idc.com/getdoc.jsp?containerId=IDCP29475. Online; Accessed 2019
3. L. Chen, et al., Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey. IEEE Access. **5** (2017). https://doi.org/10.1109/ACCESS.2017.2695525
4. I. Andrea, C. Chrysostomou, G. Hadjichristofi, Internet of Things: security vulnerabilities and challenges. IEEE Symp. Comput. Commun., 180–187 (2015). https://doi.org/10.1109/ISCC.2015.7405513
5. M. Liyanage, et al., *A Comprehensive Guide to 5G Security*. (Wiley, 2018). isbn:9781119293071
6. M. La Polla, F. Martinelli, D. Sgandurra, A survey on security for mobile devices. IEEE Commun. Surv. Tutor. **15**(1), 446–471 (2013). https://doi.org/10.1109/SURV.2012.013012.00028
7. (2019). https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation. Accessed 2019
8. V. Alcácer, V. Cruz-Machado, Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing Systems. Eng. Sci. Technol. Int. J. **22**(3), 899–919 (2019). https://doi.org/10.1016/j.jestch.2019.01.006
9. K. Huang, C. Zhou, Y. Qin, W. Tu, A Game-Theoretic Approach to Cross-Layer Security Decision-Making in Industrial Cyber-Physical Systems. IEEE Trans. Ind. Electron. **PP**(XX), 1–1 (2019). https://doi.org/10.1109/TIE.2019.2907451
10. A. Al-Dulaimi, et al., *5G Networks: fundamental requirements, enabling technologies and operations management*. (Wiley, 2018). isbn:978-1-119-33273-2
11. D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, V. Stettler, in *Proc. 2018 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS '18*, A Formal Analysis of 5G Authentication, (2018), pp. 1383–1396. https://doi.org/10.1145/3243734.3243846. arXiv:1806.10360v3

12. European Telecommunications Standards Institute ETSI, *Mobile Edge Computing Introductory Technical White Paper*. https://portal.etsi.org/TBSiteMap/MEC/MECWhitePapers.aspx. Online 2018; Accessed 2019
13. D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, Z. Han, Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City. IEEE Access. **7**, 54508–54521 (2019). https://doi.org/10.1109/ACCESS.2019.2913438
14. Symantec, *Internet Security Threat Report (ISTR)*, (2019). https://www.symantec.com/security-center/threat-report. Accessed 2019
15. Cisco, *2018 Annual Cybersecurity Report*, (2018). https://www.cisco.com/c/m/enau/products/security/offers/annual-cybersecurity-report-2018.html. Accessed 2019
16. WIRED, *Security News This Week: 'Simjacker' Attack Can Track Phones Just by Sending a Text*, (2019). https://www.wired.com/story/simjacker-attack-north-korea-security-news/. Online; Accessed 2019
17. Cisco, *Cybersecurity Series 2019, Email Security*, (2019). https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf. Online 2019; Accessed 2019
18. R. K. M. J. Chakraborty, *Hand Book on Hardware Cryptography - Algorithms and Analysis*. (LAP LAMBERT Academic Publishing, 2018). isbn:978-6139841653
19. I. Setiadi, A. I. Kistijantoro, A. Miyaji, Elliptic curve cryptography: algorithms and implementation analysis over coordinate systems. 2015 2nd Int. Conf. Adv. Inform. Concepts, Theory Appl. **16**, 1–6 (2015). https://doi.org/10.1109/ICAICTA.2015.7335349
20. K. Piotrowski, P. Langendoerfer, S. Peter, in *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks - SASN '06*, How public key cryptography influences wireless sensor node lifetime, (2007), p. 169. https://doi.org/10.1145/1180345.1180366
21. T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, L. Uhsadel, A Survey of Lightweight-Cryptography Implementations. IEEE Des. Test Comput. **24**(6), 522–533 (2007). https://doi.org/10.1109/MDT.2007.178
22. K. L. Matti Latva-aho, *Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence, 6G Flaship*. (Technical Report September, University of Oulu, Finland, 2019)
23. R. Roman, C. Alcaraz, J. Lopez, A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes. Mob. Netw. Appl. **12**(4), 231–244 (2007). https://doi.org/10.1007/s11036-007-0024-2
24. S. B. Sadkhan, A. O. Salman, *A survey on lightweight-cryptography status and future challenges*, (2018), pp. 105–108. https://doi.org/10.1109/ICASEA.2018.8370965
25. A. Biryukov, L. P. Perrin, *State of the Art in Lightweight Symmetric Cryptography, University of Luxemburg*. (University of Luxemburg, 2017)
26. L. Chen, et al., *NIST: Report on Post-Quantum Cryptography NIST*. https://csrc.nist.gov/publications/detail/nistir/8105/final. Online 2016; Accessed 2019
27. Quantamagazine, *Does nevens law describe quantum computings rise*, (2019). https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618. Accessed 2019
28. IEEE Spectrum, *What Google's Quantum Supremacy Claim Means for Quantum Computing*, (2019). https://spectrum.ieee.org/tech-talk/computing/hardware/how-googles-quantum-supremacy-plays-into-quantum-computings-long-game. Accessed 2019
29. ECRYPT CSA, *D5.4: Algorithms, Key Size and Protocols Report*, (2018). https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf. Accessed 2019
30. K. Zeng, K. Govindan, P. Mohapatra, Non-cryptographic authentication and identification in wireless networks [Security and Privacy in Emerging Wireless Networks. IEEE Wirel. Commun. **17**(5), 56–62 (2010). https://doi.org/10.1109/mwc.2010.5601959
31. J. Zhang, T. Q. Duong, A. Marshall, R. Woods, Key Generation From Wireless Channels: A Review. IEEE Access. **4**, 614–626 (2016). https://doi.org/10.1109/ACCESS.2016.2521718
32. Li G., C. Sun, J. Zhang, E. Jorswieck, B. Xiao, A. Hu, Physical layer key generation in 5G and beyond wireless communications: challenges and opportunities. Entropy. **21**(5) (2019). https://doi.org/10.3390/e21050497
33. C. H. Chang, Y. Zheng, L. Zhang, A Retrospective and a Look Forward: Fifteen Years of Physical Unclonable Function Advancement. IEEE Circ. Syst. Mag. **17**(3), 32–62 (2017). https://doi.org/10.1109/MCAS.2017.2713305
34. J. Delvaux, D. Gu, D. Schellekens, I. Verbauwhede, Secure Lightweight Entity Authentication with Strong PUFs: Mission Impossible? IEEE Trans. Inf. Forensic. Secur., 451–475 (2014). https://doi.org/10.1007/978-3-662-44709-3
35. B. Gassend, D. Clarke, M. van Dijk, S. Devadas, in *Proc. 9th ACM Conf. Comput. Commun. Secur. - CCS '02*, Silicon physical random functions, (2002), p. 148. https://doi.org/10.1145/586110.586132
36. R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications, PhD Thesis, Technische Universität Darmstadt*. https://doi.org/10.1007/978-3-642-41395-7_2
37. C. E. Shannon, Communication Theory of Secrecy Systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949). https://doi.org/10.1002/j.1538-7305.1949.tb00928.x
38. A. D. Wyner, The Wire-Tap Channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975). https://doi.org/10.1002/j.1538-7305.1975.tb02040.x
39. R. Ahlswede, I. Csiszar, Common randomness in information theory and cryptography—Part I: Secret sharing. IEEE Trans. Inf. Theory. **39**(4), 1121–1132 (1993)
40. S. Mathur, R. Miller, A. Varshavsky, W. Trappe, N. Mandayam, in *Proc. 9th Int. Conf. Mob. Syst. Appl. Serv. - MobiSys '11*, ProxiMate, (2011), p. 211. https://doi.org/10.1145/1999995.2000016
41. F. Marino, E. Paolini, M. Chiani, in *Proc. - IEEE Int. Conf.*, Secret key extraction from a UWB channel: analysis in a real environment (Ultra-Wideband, 2014), pp. 80–85. https://doi.org/10.1109/ICUWB.2014.6958955
42. H. Liu, Y. Wang, J. Yang, Y. Chen, in *Proc. IEEE INFOCOM*, Fast and practical secret key extraction by exploiting channel response, (2013), pp. 3048–3056. https://doi.org/10.1109/INFCOM.2013.6567117
43. S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, R. Ricci, Secret key extraction using Bluetooth wireless signal strength measurements. Elev. Annu. IEEE Int. Conf. Sensing, Commun. Netw., 293–301 (2014). https://doi.org/10.1109/SAHCN.2014.6990365

44. J. Wan, A. B. Lopez, M. A. Al Faruque, in *ACM/IEEE 7th Int. Conf. Cyber-Physical Syst. ICCPS 2016 - Proc.*, Exploiting Wireless Channel Randomness to Generate Keys for Automotive Cyber-Physical System Security, (2016), pp. 1–10. https://doi.org/10.1109/ICCPS.2016.7479103
45. A. M. Tonello, A. Pittolo, Physical layer security in power line communication networks: an emerging scenario, other than wireless. IET Commun. **8**(8), 1239–1247 (2014). https://doi.org/10.1049/iet-com.2013.0472
46. A. A. E. Hajomer, X. Yang, A. Sultan, W. Sun, W. Hu, Key Generation and Distribution Using Phase Fluctuation in Classical Fiber Channel. Int. Conf. Transparent Opt. Netw. **2018-July**, 1–3 (2018). https://doi.org/10.1109/ICTON.2018.8473760
47. A. Vazquez-Castro, M. Hayashi, Physical Layer Security for RF Satellite Channels in the Finite-Length Regime. IEEE Trans. Inf. Forensics Secur. **14**(4), 981–993 (2019). https://doi.org/10.1109/TIFS.2018.2868538
48. B. M. ElHalawany, A. A. A. El-Banna, K. Wu, Physical-Layer Security and Privacy for Vehicle-to-Everything. IEEE Commun. Mag. **57**(10), 84–90 (2019). https://doi.org/10.1109/MCOM.001.1900141
49. D. Tian, W. Zhang, J. Sun, C.-X. Wang, Physical-Layer Security of Visible Light Communications with Jamming, 512–517 (2019). https://doi.org/10.1109/ICCChina.2019.8855859
50. Y. Luo, L. Pu, Z. Peng, Z. Shi, RSS-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements. IEEE Commun. Mag. **54**(2), 32–38 (2016). https://doi.org/10.1109/MCOM.2016.7402258
51. B. Halak, M. Zwolinski, M. S. Mispan, in *2016 IEEE 59th Int. Midwest Symp. Circuits Syst. (October)*, Overview of PUF-based hardware security solutions for the internet of things, (2016), pp. 1–4. https://doi.org/10.1109/MWSCAS.2016.7870046
52. D. N. Ahmad-Reza Sadeghi, Hardware Intrinsic Security from Physically Unclonable Functions. Inf. Secur. Cryptogr. **9783642143120**, 39–53 (2010). https://doi.org/10.1007/978-3-642-14452-32
53. Q. Xu, R. Zheng, W. Saad, Z. Han, Device fingerprinting in wireless networks: challenges and opportunities. IEEE Commun. Surv. Tutorials (2016). https://doi.org/10.1109/COMST.2015.2476338
54. PHYLAWS Project, *PHYsical LAyer Wireless Security*, (2019), pp. 2012-2016. www.phylaws-ict.org/. Accessed 2019
55. PROPHYLAXE Project 2013-2015, *PROPHYLAXE*, (2019). www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/prophylaxe. Accessed 2019
56. G. Baldini, G. Steri, A Survey of Techniques for the Identification of Mobile Phones Using the Physical Fingerprints of the Built-In Components. IEEE Commun. Surv. Tutor. **19**(3), 1761–1789 (2017). https://doi.org/10.1109/COMST.2017.2694487. Accessed 2020-02-11
57. Q. Xu, Y. Zhou, J. Mao, Configurable secure ECC hardware module for resource constrained device. 1st Asia Pacific Conf. Postgrad. Res. Microelectron. Electron. PrimeAsia. **09706201102**, 424–427 (2009). https://doi.org/10.1109/PRIMEASIA.2009.5397353
58. H. Ju, Y. Jeon, J. Kim, in *Proc. - 2015 Int. Conf. Comput. Sci. Comput. Intell. CSCI*, A study on the hardware-based security solutions for smart devices, (2016), pp. 833–834. https://doi.org/10.1109/CSCI.2015.105
59. S. Vongsingthong, S. Boonkrong, A survey on smartphone authentication. Walailak J. Sci. Technol. **12**(1), 1–19 (2015). https://doi.org/10.2004/wjst.v12i1.864
60. B. Chatterjee, D. Das, S. Sen, *RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning*, (2018), pp. 205–208. https://doi.org/10.1109/HST.2018.8383916
61. C. Zenger, *Physical-layer security for the Internet of Things, PhD Thesis*. (University of Bochum, 2017)
62. M. Bloch, J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. (Cambridge Press, 2011). isbn:978-0521516501
63. A. Badawy, T. Elfouly, T. Khattab, A. Mohamed, M. Guizani, Unleashing the secure potential of the wireless physical layer: secret key generation methods. Phys. Commun. **19**, 1–10 (2016). https://doi.org/10.1016/j.phycom.2015.11.005
64. D. Wang, B. Bai, W. Zhao, Z. Han, A Survey of Optimization Approaches for Wireless Physical Layer Security. IEEE Commun. Surv. Tutor. **21**(2), 1878–1911 (2019). https://doi.org/10.1109/COMST.2018.2883144
65. J. M. Hamamreh, H. M. Furqan, H. Arslan, Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey. IEEE Commun. Surv. Tutor. **21**(2), 1773–1828 (2019). https://doi.org/10.1109/COMST.2018.2878035
66. H. V. Poor, R. F. Schaefer, Wireless physical layer security. Proc. Natl. Acad. Sci. **114**(1), 19–26 (2017). https://doi.org/10.1073/pnas.1618130114
67. A. Mukherjee, S. A. A. Fakoorian, J. Huang, A. L. Swindlehurst, Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. IEEE Commun. Surv. Tutor. **16**(3), 1550–1573 (2014). https://doi.org/10.1109/SURV.2014.012314.00178
68. Y. Liu, H.-H. Chen, L. Wang, Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges. IEEE Commun. Surv. Tutor. **19**(1), 347–376 (2017). https://doi.org/10.1109/COMST.2016.2598968
69. R. Negi, S. Goel, *Secret communication using artificial noise*, vol. 3, (2005), pp. 1906–1910. https://doi.org/10.1109/VETECF.2005.1558439
70. S. Goel, R. Negi, Guaranteeing Secrecy using Artificial Noise. IEEE Trans. Wirel. Commun. **7**(6), 2180–2189 (2008). https://doi.org/10.1109/TWC.2008.060848
71. S. Goekceli, O. Cepheli, S. T. Basaran, G. K. Kurt, G. Dartmann, G. Ascheid, in *2017 IEEE Globecom Work. (GC Wkshps)*, How Effective is the Artificial Noise? Real-Time Analysis of a PHY Security Scenario, (2017), pp. 1–7. https://doi.org/10.1109/GLOCOMW.2017.8269228
72. Y. Z. Xiangyun Zhou, Lingyang Song, *Physical Layer Security in Wireless Communications*. (CRC Press, 2005). isbn:9781466567009
73. U. Maurer, Secret key agreement by public discussion. IEEE Trans. Inf. Theory. **39**(3), 733–742 (1993)
74. X. He, H. Dai, W. Shen, P. Ning, in *2013 Proc. IEEE INFOCOM*, Is link signature dependable for wireless security? (2013), pp. 200–204. https://doi.org/10.1109/INFCOM.2013.6566763
75. J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, Q. Xu, Experimental Study on Key Generation for Physical Layer Security in Wireless Communications. IEEE Access. **4**, 4464–4477 (2016). https://doi.org/10.1109/ACCESS.2016.2604618

76. S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, R. Ricci, Secret key extraction using Bluetooth wireless signal strength measurements. Elev. Annu. IEEE Int. Conf. Sensing, Commun. Netw., 293–301 (2014). https://doi.org/10.1109/SAHCN.2014.6990365
77. G. Revadigar, C. Javali, H. J. Asghar, K. B. Rasmussen, S. Jha, Mobility Independent Secret Key Generation for Wearable Health-care Devices. Proc. 10th EAI Int. Conf. Body Area Netw. (2015). https://doi.org/10.4108/eai.28-9-2015.2261446
78. S. Eberz, M. Strohmeier, M. Wilhelm, I. Martinovic, A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols. Lect. Notes Comput. Sci. including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma. **7459 LNCS**, 235–252 (2012). https://doi.org/10.1007/978-3-642-33167-114
79. S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, in *Proc. 14th ACM Int. Conf. Mob. Comput. Netw. - MobiCom '08*, Radio-telepathy, (2008), p. 128. https://doi.org/10.1145/1409944.1409960
80. M. I. AlHajri, N. T. Ali, R. M. Shubair, Classification of Indoor Environments for IoT Applications: A Machine Learning Approach. IEEE Antennas Wirel. Propag. Lett. **17**(12), 2164–2168 (2018). https://doi.org/10.1109/LAWP.2018.2869548
81. A. P. Fournaris, K. Lampropoulos, O. Koufopavlou, in *2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Hardware Security for Critical Infrastructures - The CIPSEC Project Approach (IEEE, Bochum, Germany, 2017), pp. 356–361. https://doi.org/10.1109/ISVLSI.2017.69
82. H. Ju, Y. Jeon, J. Kim, in *2015 International Conference on Computational Science and Computational Intelligence (CSCI)*, A Study on the Hardware-Based Security Solutions for Smart Devices (IEEE, 2015), pp. 833–834. https://doi.org/10.1109/CSCI.2015.105
83. L. Karter, L. Ferhati, I. Tafa, D. Saatciu, J. Fejzaj, in *2015 Science and Information Conference (SAI)*, Security evaluation of embedded hardware implementation (IEEE, London, United Kingdom, 2015), pp. 1272–1276. https://doi.org/10.1109/SAI.2015.7237307
84. , in *Presented as Part of the 6th USENIX Workshop on Offensive Technologies*, Baseband attacks: remote exploitation of memory corruptions in cellular protocol stacks (USENIX, Bellevue, WA, 2012). https://www.usenix.org/conference/woot12/workshop-program/presentation/Weinmann
85. Y. Zou, J. Zhu, X. Wang, L. Hanzo, *A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends*, vol. 104, (2016), pp. 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521
86. A. Mukherjee, Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. Proc. IEEE. **103**(10), 1747–1761 (2015). https://doi.org/10.1109/JPROC.2015.2466548
87. M. Alioto, Trends in Hardware Security: From basics to ASICs. IEEE Solid-State Circ. Mag. **11**(3), 56–74 (2019). https://doi.org/10.1109/MSSC.2019.2923503
88. L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, Using the physical layer for wireless authentication in time-variant channels. IEEE Trans. Wirel. Commun. **7**(7), 2571–2579 (2008). https://doi.org/10.1109/TWC.2008.070194
89. P. L. Yu, J. S. Baras, B. M. Sadler, Physical-layer authentication. IEEE Trans. Inf. Forensics Secur. (2008). https://doi.org/10.1109/TIFS.2007.916273
90. J. Han, C. Qian, P. Yang, D. Ma, Z. Jiang, W. Xi, J. Zhao, GenePrint: Generic and Accurate Physical-Layer Identification for UHF RFID Tags. IEEE/ACM Trans. Netw. **24**(2), 846–858 (2016). https://doi.org/10.1109/TNET.2015.2391300
91. C. Pei, N. Zhang, X. S. Shen, J. W. Mark, *Channel-based physical layer authentication*, (2014), pp. 4114–4119. https://doi.org/10.1109/GLOCOM.2014.7037452
92. W. E. Cobb, E. D. Laspe, R. O. Baldwin, M. A. Temple, Y. C. Kim, Intrinsic Physical-Layer Authentication of Integrated Circuits. IEEE Trans. Inf. Forensics Secur. **7**(1), 14–24 (2012). https://doi.org/10.1109/TIFS.2011.2160170
93. W. Hou, X. Wang, J.-Y. Chouinard, A. Refaey, Physical Layer Authentication for Mobile Systems with Time-Varying Carrier Frequency Offsets. IEEE Trans. Commun. **62**(5), 1658–1667 (2014). https://doi.org/10.1109/TCOMM.2014.032914.120921
94. D. R. Reising, M. A. Temple, J. A. Jackson, Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints. IEEE Trans. Inf. Forensics Secur. **10**(6), 1180–1192 (2015). https://doi.org/10.1109/TIFS.2015.2400426
95. A. M. Ali, E. Uzundurukan, A. Kara, Assessment of Features and Classifiers for Bluetooth RF Fingerprinting. IEEE Access. **7**, 50524–50535 (2019). https://doi.org/10.1109/ACCESS.2019.2911452
96. J. Jagannath, N. Polosky, A. Jagannath, F. Restuccia, T. Melodia, *Machine Learning for Wireless Communications in the Internet of Things: A Comprehensive Survey*, (2019). 1901.07947. https://doi.org/10.1016/j.adhoc.2019.101913
97. X. Li, F. Dong, S. Zhang, W. Guo, A Survey on Deep Learning Techniques in Wireless Signal Recognition. Wirel. Commun. Mob. Comput. **2019**, 1–12 (2019). https://doi.org/10.1155/2019/5629572
98. C. Zhang, P. Patras, H. Haddadi, Deep learning in mobile and wireless networking: a survey. CoRR. **abs/1803.04311** (2018)
99. J. Zhang, A. Marshall, R. Woods, T. Q. Duong, Efficient Key Generation by Exploiting Randomness From Channel Responses of Individual OFDM Subcarriers. IEEE Trans. Commun. **64**(6), 2578–2588 (2016). https://doi.org/10.1109/TCOMM.2016.2552165
100. W. Trappe, The challenges facing physical layer security. IEEE Commun. Mag. **53**(6), 16–20 (2015). https://doi.org/10.1109/MCOM.2015.7120011
101. P. Walther, C. Janda, E. Franz, M. Pelka, H. Hellbruck, T. Strufe, E. Jorswieck, in *2018 IEEE 43rd Conf. Local Comput. Networks, vol. 2018-Octob*, Improving Quantization for Channel Reciprocity Based Key Generation, (2018), pp. 545–552. https://doi.org/10.1109/LCN.2018.8638248
102. Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, *Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. Cryptology ePrint Archive, Report 2003/235*, (2003). https://eprint.iacr.org/2003/235
103. C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, T. Güneysu, Information reconciliation schemes in physical-layer security: a survey. Comput. Netw. **109**, 84–104 (2016). https://doi.org/10.1016/j.comnet.2016.06.014
104. U. Gustavsson, C. Sanchez-Perez, T. Eriksson, F. Athley, G. Durisi, P. Landin, K. Hausmair, C. Fager, L. Svensson, On the impact of hardware impairments on massive MIMO. **1**, 294–300 (2014). https://doi.org/10.1109/GLOCOMW.2014.7063447

105. J. Samuel, P. Rosson, L. Maret, C. Dehos, A. Valkanas, in *2008 IEEE 10th Int. Symp. Spread Spectr. Tech. Appl.*, Impact of RF Impairments in Cellular Wireless Metropolitan Area Networks, (2008), pp. 766–769. https://doi.org/10.1109/ISSSTA.2008.149
106. Y. Zou, P. Zetterberg, U. Gustavsson, T. Svensson, A. Zaidi, T. Kadur, W. Rave, G. Fettweis, in *2016 IEEE Globecom Work. (GC Wkshps) (Ici)*, Impact of Major RF Impairments on mm-Wave Communications Using OFDM Waveforms, (2016), pp. 1–7. https://doi.org/10.1109/GLOCOMW.2016.7848927
107. A. C. Polak, S. Dolatshahi, D. L. Goeckel, Identifying wireless users via transmitter imperfections. IEEE J. Sel. Areas Commun. (2011). https://doi.org/10.1109/JSAC.2011.110812
108. Z. Li, L. Sun, L. Zhang, Y. Wang, Z. Yu, in *2014 IEEE Int. Conf. Electron Devices Solid-State Circuits*, Effects of RF impairments on EVM performance of 802.11ac WLAN transmitters, (2014), pp. 1–2. https://doi.org/10.1109/EDSSC.2014.7061173
109. R. Stuhlberger, R. Krueger, B. Adler, J. Kissing, L. Maurer, G. Hueber, A. Springer, in *2007 Eur. Conf. Wirel. Technol. (October)*, LTE-Downlink Performance in the Presence of RF-Impairments, (2007), pp. 189–192. https://doi.org/10.1109/ECWT.2007.4403978
110. S. Salous, *Radio propagation measurement and channel modelling*. (Wiley, 2013). isbn:978-0-470-75184-8
111. B. Sklar, *Digital Communications: Fundamentals and Applications*, (Prentice Hall, 2017). isbn:978-0134724058
112. A. Albehadili, K. Al Shamaileh, A. Javaid, J. Oluoch, V. Devabhaktuni, An Upper Bound on PHY-Layer Key Generation for Secure Communications Over a Nakagami-M Fading Channel With Asymmetric Additive Noise. IEEE Access. **6**, 28137–28149 (2018). https://doi.org/10.1109/ACCESS.2018.2827925. Accessed 13 Jan 2020
113. M. Patzold, F. Laue, Level-Crossing Rate and Average Duration of Fades of Deterministic Simulation Models for Rice Fading Channels. IEEE Symp. Comput. Commun. **48**, 272–276 (1999). https://doi.org/10.1109/ISCC.2015.7405513
114. A. Abdi, K. Wills, H. A. Barger, M.-S. Alouini, M. Kaveh, Comparison of the level crossing rate and average fade duration of Rayleigh, Rice and Nakagami fading models with mobile channel data, 1850–1857 (2002). https://doi.org/10.1109/vetecf.2000.886139
115. C.-X. Wang, J. Bian, J. Sun, W. Zhang, M. Zhang, A Survey of 5G Channel Measurements and Models. IEEE Commun. Surv. Tutorials. **20**(4), 3142–3168 (2018). https://doi.org/10.1109/COMST.2018.2862141
116. A. Meijerink, A. Molisch, On the physical interpretation of the Saleh-Valenzuela model and the definition of its power delay profiles. IEEE Trans. Antennas Propag. **62**(9), 4780–4793 (2014). https://doi.org/10.1109/TAP.2014.2335812
117. L. Bernado, T. Zemen, F. Tufvesson, A. F. Molisch, C. F. Mecklenbrauker, Delay and doppler spreads of nonstationary vehicular channels for safety-relevant scenarios. IEEE Trans. Veh. Technol. **63**(1), 82–93 (2014). https://doi.org/10.1109/TVT.2013.2271956. 1305.3376
118. G. Matz, F. Hlawatsch, *Fundamentals of Time-Varying Communication Channels*. (Elsevier, 2011), pp. 1–63. isbn:9780123744838. https://doi.org/10.1016/B978-0-12-374483-8.00001-7. https://linkinghub.elsevier.com/retrieve/pii/B9780123744838000017
119. Y. C. Eldar, A. V. Oppenheim, MMSE whitening and subspace whitening. IEEE Trans. Inf. Theory. **49**(7), 1846–1851 (2003). https://doi.org/10.1109/TIT.2003.813507
120. J. Zhang, A. Marshall, L. Hanzo, Channel-Envelope Differencing Eliminates Secret Key Correlation: LoRa-Based Key Generation in Low Power Wide Area Networks. IEEE Trans. Veh. Technol. **67**(12), 12462–12466 (2018). https://doi.org/10.1109/TVT.2018.2877201
121. Y. Huang, A. Rajkotia, S. Soliman, *UWB Channel Estimation: Design and Performance Evaluation*, vol. 4, (2006), pp. 1961–1966. https://doi.org/10.1109/VETECS.2006.1683189
122. V. Raghavan, J. Li, Evolution of Physical-Layer Communications Research in the Post-5G Era. IEEE Access. **7**, 10392–10401 (2019). https://doi.org/10.1109/ACCESS.2019.2891218
123. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, M. D. Renzo, Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag. **53**(4), 20–27 (2015). https://doi.org/10.1109/MCOM.2015.7081071
124. X. Lin, J. Li, R. Baldemair, T. Cheng, S. Parkvall, D. Larsson, H. Koorapaty, M. Frenne, S. Falahati, A. Grövlen, K. Werner, *5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology*, (2018), pp. 1–8. 1806.06898
125. Z. Chen, X. Ma, B. Zhang, Y. Zhang, Z. Niu, N. Kuang, W. Chen, L. Li, S. Li, A survey on terahertz communications. China Commun. **16**(2), 1–35 (2019). https://doi.org/10.12676/j.cc.2019.02.001
126. Fraunhofer-HHI, *QUAsi Deterministic RadIo channel GenerAtor*, (2019). https://quadriga-channel-model.de. Accessed 2019
127. 3GPP, *Release 14, TR 38.901, Study on channel model for frequencies from 0.5 to 100 GHz*, (2017). https://portal.3gpp.org/desktopmodules/Specifications. Accessed 2019
128. Y. Cai, Z. Qin, F. Cui, G. Y. Li, J. A. McCann, Modulation and Multiple Access for 5G Networks. IEEE Commun. Surv. Tutor. **20**(1), 629–646 (2018). https://doi.org/10.1109/COMST.2017.2766698
129. Wired, *The Biggest iPhone News Is a Tiny New Chip Inside It*, (2019). https://www.wired.com/story/apple-u1-chip. Accessed 2019
130. T. Hwang, C. Yang, G. Wu, S. Li, Y. G. Li, OFDM and Its Wireless Applications: A Survey. IEEE Trans. Veh. Technol. **58**(4), 1673–1694 (2008). https://doi.org/10.1109/tvt.2008.2004555
131. J. Zhang, A. Marshall, R. Woods, T. Q. Duong, Design of an OFDM Physical Layer Encryption Scheme. IEEE Trans. Veh. Technol. **66**(3), 2114–2127 (2017). https://doi.org/10.1109/TVT.2016.2571264
132. J. M. Hamamreh, H. M. Furqan, H. Arslan, in *2017 13th Int. Wirel. Commun. Mob. Comput. Conf.*, Secure pre-coding and post-coding for OFDM systems along with hardware implementation, (2017), pp. 1338–1343. https://doi.org/10.1109/IWCMC.2017.7986479
133. J. Zhang, T. Q. Duong, R. Woods, A. Marshall, *Securing wireless communications of the internet of things from the physical layer, an overview*, (2017). https://doi.org/10.3390/e19080420
134. H. Taha, E. Alsusa, in *2015 IEEE Glob. Commun. Conf.*, Physical Layer Secret Key Exchange Using Phase Randomization in MIMO-OFDM, (2015), pp. 1–6. https://doi.org/10.1109/GLOCOM.2015.7417210
135. Y. Liu, Z. Tan, H. Hu, L. J. Cimini, G. Y. Li, Channel estimation for OFDM. IEEE Commun. Surv. Tutorials. **16**(4), 1891–1908 (2014). https://doi.org/10.1109/COMST.2014.2320074
136. J. Hejselbaek, W. Fan, G. F. Pedersen, Ultrawideband VNA based channel sounding system for centimetre and millimetre wave bands. IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC (2016). https://doi.org/10.1109/PIMRC.2016.7794728

137. S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, S. V. Krishnamurthy, in *Proc. 15th Annu. Int. Conf. Mob. Comput. Netw. - MobiCom '09*, On the effectiveness of secret key extraction from wireless signal strength in real environments, (2009), p. 321. https://doi.org/10.1145/1614320.1614356
138. Q. Wang, H. Su, K. Ren, K. Kim, in *Proc. IEEE INFOCOM*, Fast and scalable secret key generation exploiting channel phase randomness in wireless networks, (2011), pp. 1422–1430. https://doi.org/10.1109/INFCOM.2011.5934929
139. K. Ren, H. Su, Q. Wang, Secret key generation exploiting channel characteristics in wireless communications. IEEE Wirel. Commun. **18**(4), 6–12 (2011). https://doi.org/10.1109/MWC.2011.5999759
140. S. M. MirhoseiniNejad, A. Rahmanpour, S. M. Razavizadeh, in *2018 15th Int. ISC (Iranian Soc. Cryptology) Conf. Inf. Secur. Cryptol.*, Phase Jamming Attack: A Practical Attack on Physical layer-Based Key Derivation, (2018), pp. 1–4. https://doi.org/10.1109/ISCISC.2018.8546920
141. E. M. Vitucci, F. Mani, T. Mazloum, A. Sibille, V. D. Esposti, *Ray Tracing simulations of indoor channel spatial correlation for Physical Layer Security*, (2015)
142. J. Xiong, K. Jamieson, in *Proc. 19th Annu. Int. Conf. Mob. Comput. Netw. - MobiCom '13*, SecureArray, (2013), p. 441. https://doi.org/10.1145/2500423.2500444
143. P. Sedlacek, M. Slanina, P. Masek, *An Overview of the IEEE 802.15.4z Standard its Comparison and to the Existing UWB Standards*, (2019), pp. 1–6. https://doi.org/10.1109/RADIOELEK.2019.8733537
144. V. Niemela, J. Haapola, M. Hamalainen, J. Iinatti, An Ultra Wideband Survey: Global Regulations and Impulse Radio Research Based on Standards. IEEE Commun. Surv. Tutor. **19**(2), 874–890 (2017). https://doi.org/10.1109/COMST.2016.2634593
145. J. A. R. Ruiz, S. F. Granja, Comparing Ubisense, BeSpoon, and DecaWave UWB Location Systems: Indoor Performance Analysis. IEEE Trans. Instrum. Meas. **66**(8), 2106–2117 (2017). https://doi.org/10.1109/TIM.2017.2681398
146. A. Yassin, Y. Nasser, M. Awad, A. Al-Dubai, R. Liu, C. Yuen, R. Raulefs, E. Aboutanios, Recent Advances in Indoor Localization: A Survey on Theoretical Approaches and Applications. IEEE Commun. Surv. Tutor. **19**(2), 1327–1346 (2017). https://doi.org/10.1109/COMST.2016.2632427
147. M. Ko, D. L. Goeckel, *Wireless physical-layer security performance of UWB systems*, (2010), pp. 2143–2148. https://doi.org/10.1109/MILCOM.2010.5680483
148. M. Singh, P. Leu, S. Capkun, UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks. Proc. 2019 Netw. Distrib. Syst. Secur. Symp. (2019). https://doi.org/10.14722/ndss.2019.23109
149. M. G. Madiseh, M. L. McGuire, S. W. Neville, A. A. B. Shirazi, in *Proc. 6th Annu. Commun. Networks Serv. Res. Conf. CNSR 2008*, Secret key extraction in ultra wideband channels for unsynchronized radios, (2008). https://doi.org/10.1109/CNSR.2008.52
150. G. M. Madiseh, S. He, M. L. Mcguire, S. W. Neville, X. Dong, *Verification of Secret Key Generation from UWB Channel Observations*, (2009), pp. 1–5. https://doi.org/10.1109/ICC.2009.5199564
151. R. Wilson, D. Tse, R. A. Scholtz, Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels. IEEE Trans. Inf. Forensics Secur. **2**(3), 364–375 (2007). https://doi.org/10.1109/TIFS.2007.902666
152. M. Bulenok, I. Tunaru, L. Biard, B. Denis, B. Uguen, *Experimental channel-based secret key generation with integrated ultra wideband devices*, (2016), pp. 1–6. https://doi.org/10.1109/PIMRC.2016.7794705
153. R. Muller, R. Herrmann, D. A. Dupleich, C. Schneider, R. S. Thoma, in *8th Eur. Conf. Antennas Propag. (EuCAP 2014)*, Ultrawideband multichannel sounding for mm-wave, (2014), pp. 817–821. https://doi.org/10.1109/EuCAP.2014.6901887
154. T. Kuseler, I. A. Lami, Using Geographical Location as an Authentication Factor to Enhance mCommerce Applications on Smartphones. Int. J. Comput. Sci. Secur. **6**, 277–287 (2012)
155. S. T.-B. Hamida, J.-B. Pierrot, B. Denis, C. Castelluccia, B. Uguen, *On the Security of UWB Secret Key Generation Methods against Deterministic Channel Prediction Attacks*, (2012), pp. 1–5. https://doi.org/10.1109/VTCFall.2012.6399358
156. L. E. Bassham, et al., *NIST. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication 800-22*, (2010). https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic. Accessed 2019
157. M. S. Turan, et al., *NIST: Recommendation for the Entropy Sources Used for Random Bit Generation, NIST Special Publication 800-90B*, (2018). https://csrc.nist.gov/publications/detail/sp/800-90b/final. Accessed 2019
158. H. Okada, K. Umeno, Randomness Evaluation With the Discrete Fourier Transform Test Based on Exact Analysis of the Reference Distribution. IEEE Trans. Inf. Forensics Secur. **12**(5), 1218–1226 (2017). https://doi.org/10.1109/TIFS.2017.2656473. arXiv:1701.01960v1
159. J. Kelsey, K. A. McKay, M. S. Turan, *Predictive Models for Min-Entropy Estimation. Cryptology ePrint Archive, Report 2015/600*, (2015). https://eprint.iacr.org/2015/600
160. S. Zhu, Y. Ma, T. Chen, J. Lin, J. Jing, Analysis and improvement of entropy estimators in NIST SP 800-90B for non-IID entropy sources. IACR Trans. Symmetric Cryptol. **3**, 151–168 (2017). https://doi.org/10.13154/tosc.v2017.i3.151-168
161. T. Van Nguyen, Y. Jeong, H. Shin, M. Z. Win, Machine Learning for Wideband Localization. IEEE J. Sel. Areas Commun. **33**(7), 1357–1380 (2015). https://doi.org/10.1109/JSAC.2015.2430191
162. M. I. AlHajri, N. T. Ali, R. M. Shubair, Classification of Indoor Environments for IoT Applications: A Machine Learning Approach. IEEE Antennas Wirel. Propag. Lett. **17**(12), 2164–2168 (2018). https://doi.org/10.1109/LAWP.2018.2869548
163. E. Kurniawan, L. Zhiwei, S. Sun, in *2017 IEEE Glob. Commun. Conf. GLOBECOM 2017 - Proc. vol. 2018-Janua*, Machine Learning-Based Channel Classification and Its Application to IEEE 802.11ad Communications, (2018), pp. 1–6. https://doi.org/10.1109/GLOCOM.2017.8254052

Publisher's Note