

Physical Layer Security: A Paradigm Shift in Data Confidentiality

Arsenia Chorti, Camilla Hollanti, Jean-Claude Belfiore, Harold Vincent Poor

▶ **To cite this version:**

Arsenia Chorti, Camilla Hollanti, Jean-Claude Belfiore, Harold Vincent Poor. Physical Layer Security: A Paradigm Shift in Data Confidentiality. Physical and Data-Link Security Techniques for Future Communication Systems, 2015, Lecture Notes in Electrical Engineering. hal-01686208

HAL Id: hal-01686208
https://hal.science/hal-01686208

Submitted on 17 Jan 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Physical Layer Security: a Paradigm Shift in Data Confidentiality

Arsenia Chorti, Camilla Hollanti*, Jean-Claude Belfiore and Harold Vincent Poor†

Abstract Physical layer security (PLS) draws on information theory to characterize the fundamental ability of the wireless physical layer to ensure data confidentiality. In the PLS framework it has been established that it is possible to simultaneously achieve reliability in transmitting messages to an intended destination and perfect secrecy of those messages with respect to an eavesdropper by using appropriate encoding schemes that exploit the noise and fading effects of wireless communication channels. Today, after more than fifteen years of research in the area, PLS has the potential to provide novel security solutions that can be integrated into future generations of mobile communication systems. This chapter presents a tutorial on advances in this area. The treatment begins with a review of the fundamental PLS concepts and their corresponding historical background. Subsequently it reviews some of the most significant advances in coding theory and system design that offer a concrete platform for the realization of the promise of this approach in data confidentiality.

Arsenia Chorti
School of Computer Science and Electronic Engineering, Wivenhoe Park, Colchester, CO4 3SQ, UK, e-mail: achorti@essex.ac.uk

Camilla Hollanti
Department of Mathematics and Systems Analysis, Aalto University School of Science, 00076 Aalto, Finland, e-mail: camilla.hollanti@aalto.fi

Jean-Claude Belfiore
Telecom ParisTech, Dept of Communications and Electronics, 46, rue Barrault, 75634 Paris CEDEX 13, France, e-mail: jean-claude.belfiore@telecom-paristech.fr

Harold Vincent Poor
Department of Electrical Engineering, EQUAD, 19 Olden Street, Princeton University, Princeton, New Jersey 08544, USA, e-mail: poor@princeton.edu

* The financial support from the Academy of Finland (grants #276031, #282938, #283262) and Magnus Ehrnrooth Foundation is gratefully acknowledged. Part of this work was carried out under the European Science Foundation's COST Action IC1104.

† This work was supported by the U. S. National Science Foundation Grant CMMI-1435778.



1 Introduction

1.1 Historical background

In the design of any communication system two fundamental requirements are taken into consideration: (i) reliability in the exchange of information between a source node (in our context, commonly referred to as *Alice*) and an intended destination (*Bob*), and (ii) security in terms of data confidentiality and message integrity with respect to an adversary (*Eve*). These two aspects in the design of any actual communication system have traditionally been addressed separately. The principal reason behind this divide is due to a decisive difference in the setup of the elementary models proposed first by Claude Shannon for the investigation of the two issues, depicted in Figs. 1 and 2.

In terms of reliability, a noisy transmission channel was assumed to connect Alice and Bob. On the other hand, for the study of security a noiseless medium linking Alice, Bob and Eve was considered. Using this latter model, Shannon proved in [32] that in the noiseless scenario *perfect secrecy* (unconditional security) in a symmetric key encryption system can be achieved only when the entropy of the security key is at least equal to that of the message; *i.e.*, one needs to use "one-time-pad" to achieve perfect secrecy in this setting. As a consequence of this pessimistic result, the conclusion that perfect secrecy is not attainable in realistic communication systems was

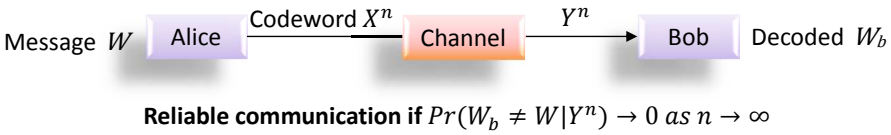


Fig. 1 Reliability model

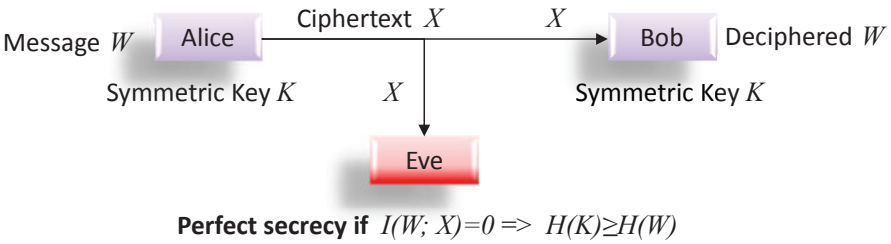


Fig. 2 Data confidentiality model

drawn and alternative approaches to security were sought based on computational complexity properties.

Nowadays, practical cryptographic approaches are built to alternatively achieve *semantic security*, *i.e.*, to withstand polynomial time chosen plaintext and chosen ciphertext attacks [11]. State of the art authenticated encryption schemes that guarantee data confidentiality and integrity have been built around the assumption that the underlying symmetric key block ciphers are semantically secure; however, no formal proof exists to-date for the most advanced block ciphers, including the AES-128, AES-196 and AES-256. Notably, for symmetric key authenticated encryption schemes to work the existence of a "shared" source of entropy that can be accessed by both Alice and Bob and that is inaccessible to Eve is still required, and, the entropy of this source should be sufficient to support a computational complexity proof in the semantic security setting. In protocols in which the keys are only used once this source of randomness is necessary for the continuous update of the symmetric keys. On the other hand, if the keys are used multiple times this source of randomness is used to update complementary parameters, *e.g.*, initialization vectors (IVs), nonces or salts of the particular enciphering schemes used.

On the other hand, in public key authenticated encryption schemes no pre-shared secret is assumed and the security of such schemes relies on the (unproven) intractability of certain "hard" algebraic problems typically involving the use of large prime numbers and elliptic curves. Furthermore, from a practical point of view, the computational resources required by such protocols are significant; this is a serious limiting factor in power limited or mobile applications. As a result, novel approaches for securing next generation mobile systems are needed.

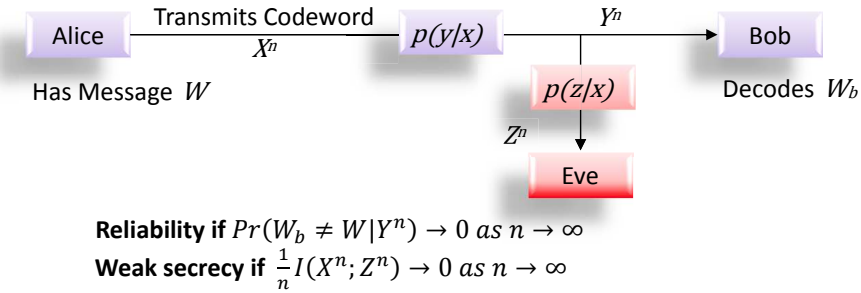


Fig. 3 Wyner's model

1.2 Physical Layer Security

Recently, a fundamentally different approach to security has emerged from the area of information theory under the generic term *physical layer security* (PLS). PLS encompasses all *keyless* security technologies that can ensure perfect secrecy by exploiting a source of entropy typically considered a foe rather than a friend: the noise and the interference in real communication media. PLS was pioneered by Wyner and was founded on the observation that Shannon's noiseless model in [32] is unnecessarily restrictive. In fact, in *all* realistic communication settings the observations of Bob and Eve are *different* realizations of a joint probability distribution (the output of the transmission channel).

Wyner in [35] investigated the so called *wiretap channel model* in which Eve's channel is a degraded version of the main channel between Alice and Bob, depicted in Fig. 3. He proved that in this setting Alice and Bob can exchange information reliably (with asymptotically zero error rates) and with perfect secrecy (with asymptotically zero rate of information leakage) with the use of a suitable pair of *encoder/decoder* functions. The rate at which information can be transmitted secretly from the source to its intended destination was termed an achievable secrecy rate, and the maximal achievable secrecy rate was termed the channel's *secrecy capacity* (SC).

Maurer in [22] and Ahlswede and Csiszár in [1] investigated the potential use of noisy channels for secret key distillation and introduced the concept of secret key capacity (SKC), in analogy to the SC. Key generation at the physical layer has been extensively discussed as it offers unique opportunities to generate symmetric secret keys without the overhead of public key encryption. In this context, there exist two different approaches: the channel-type model approach and the source-type model approach. According to the former, a random sequence is transmitted over the channel and observed by Alice and Bob. In the latter Alice and Bob observe a common source of randomness, *e.g.*, their channel gains in a reciprocal transmission medium setting (for example in slow fading channels).

To exploit either approach in order to distil a shared secret key, Bennet *et al.* [3] proposed a concrete three-step approach:

1. Advantage distillation: Alice and Bob identify from a set of correlated observations the ones over which they have an "advantage" with respect to Eve.
2. Information reconciliation: These observations are then further processed to "reconcile" discrepancies in order to obtain a mutual shared secret.
3. Privacy amplification: The shared secret is hashed with a universal hash function in order to remove redundancy and produce a uniformly distributed key sequence without leaking information to Eve.

In the following sections we will briefly review the SC of the most important classes of channels and the design of the respective state-of-the-art encoders for secrecy. Subsequently, we will discuss in detail the feasibility of PLS technologies and outline open research issues and future directions of study. This review will be concluded with an overview of the key points regarding PLS technologies.

2 Secrecy Capacity of Important Classes of Channels

Following Wyner's contribution, the SC of the scalar Gaussian wiretap channel was analyzed in [16]. It was shown that in this class of channels the SC, denoted by C_s, is given simply as the difference of the capacities of the main link, denoted by C_m, and of Eve's link, denoted by C_e, *i.e.*,

$$C_s = (C_m - C_e)^+ \tag{1}$$

with $(\cdot)^+ = \max(\cdot, 0)$. In [6], Wyner's approach was generalized to the transmission of confidential messages over broadcast channels, depicted in Fig. 4.

The broadcast channel with confidential messages (BCC) [6] investigates the scenario in which Alice wishes to broadcast a common message to both Bob and Eve and a confidential message only to Bob. The channel is modeled through a joint probability distribution function for Bob's and Eve's observations, conditioned on the channel input (broadcast by Alice). It was shown in [6] that the SC is the maximum of the difference of the mutual information of the link between Alice and Bob and of the mutual information in the link between Alice and Eve, expressed as follows when the rate of the common message is set to zero:

$$C_s = \max_{\substack{p_{UX}(u,x) \\ U \to X \to YZ}} I(U;Y) - I(U;Z), \tag{2}$$

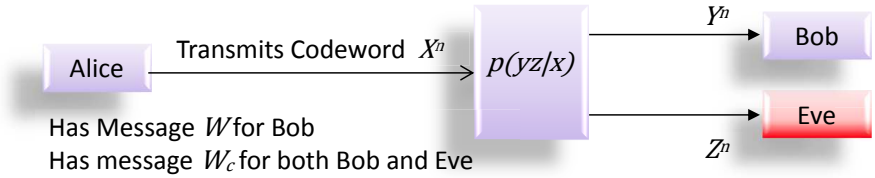


Fig. 4 Criszár-Körner's model

where U denotes the output of the source[3], X the input of the channel, Y the observation at the intended destination and Z the observation of the eavesdropper, while the maximization is over all possible joint input distributions $p_{UX}(u,x)$ and $U \to X \to YZ$ form a Markov chain.

As a result, in contrast to the Gaussian wiretap channel, depending on the joint distribution of Bob's and Eve's observations, it can be possible to have a non-zero SC even in the non-degraded case, *i.e.*, even when Eve has a better channel than Bob on average. Such an example is the BCC fading channel, see [18] for more details. For the fading BCC where the confidential message for one receiver must be perfectly secret from the other, it was demonstrated that the secrecy capacity is non-zero even when on average Eves channel is better than Bob's channel. This can be achieved if the transmitted encoded symbols are multiplexed over the time slots during which Bob's channel fading gain is larger than Eve's fading gain. The key to achieving the SC of the fading channel is optimal power allocation, [9] for the ergodic fading channel and [18] for the the parallel Gaussian BCC. Finally, a positive SC can be achieved with only statistical channel state information of the eavesdropper's channel, by multiplexing the codewords across all fading realizations [4].

The SC of the multiple-input multiple-output (MIMO) channel allowing an arbitrary number of antennas at the transmitter, legitimate receiver, and eavesdropper was derived in [24], after a considerable amount of previous work that had provided partial proofs or bounds in some limited cases. Since the broadcast channel is not degraded, a new proof technique involving a study of a Sato-like outer bound via the solution of a certain algebraic Riccati equation was introduced. The SC turned out to be the expected one — the results indeed revealed the difference of the mutual information to the legitimate receiver and that to the eavesdropper maximized over the input distribution, similarly to the previous cases. The MIMO SC was independently proved in various other works using different techniques, see [12], [13] among many others. The concept was later extended to the case of three messages (one common and two confidential messages) and to the imperfect secrecy setting by Ekrem-Ulukus [8] and Liu *et al.* [20], as well as to the delayed channel state information (CSI) feedback case by Yang *et al.* [37].

In the MIMO multi-receiver case with an external eavesdropper, the SC was derived in [8], and a variant of dirty-paper coding with Gaussian signals was shown to

[3] The channel prefixing random variable U accounts for randomness introduced in the encoding process.

be capacity-achieving. An interesting feature was that the previous converse proof techniques turned out to be insufficient, and thus a new proof technique involving the Fisher information matrix and the generalized De Bruijn identity was adopted.

Furthermore, the multiple-access channel (MAC) with one or two confidential messages was studied in [17] in the binary and Gaussian cases. Inner and outer bounds on the capacity-equivocation region were obtained, where the equivocation (or, conditional entropy) characterizes the level of secrecy maintained at the eavesdropper. In the case of a degraded MAC, the region was explicitly characterized.

Regarding relay networks, the first study of the SC of the relay channel with confidential messages has appeared in [26] while further analyses followed [27], [10]; these contributions established that the SC of one-way relay channels is zero, unless the source-destination channel is better than the source relay channel. In essence, relay topologies of practical interest in which the link to the relay is better than the direct link were shown to be inherently insecure. Due to this limiting result, subsequent work focused primarily on cooperative relay channels with trustworthy relays [2].

3 Code Design for Secrecy

Theoretical limits on the SC of wiretap channels have been extensively studied for a broad set of scenarios. On the other hand, the richness of results for the characterization of capacity-equivocation regions is in sharp contrast with the limited amount of actual wiretap code designs, an area in which little is yet known. Theoretical approaches suggest that such code designs should possess a nested code structure and (probably) exploit stochastic encoding. The term "double-binning" encoders was introduced to describe such nested structures with an "outer encoder" essentially generating public codewords that act as cosets to secret codewords generated from an "inner encoder". Nevertheless, designing explicit SC achieving codes based on this principle is a challenging task as it requires a fine understanding and analysis of a code's algebraic structure. As a first step to facilitate such designs, Ozarow and Wyner proposed the so-called wiretap II codes [28] adhering to the scenario in which the channel to Bob is a noiseless binary channel, while Eve experiences erasures.

As noted previously, Wyner proved that both robustness to transmission errors and a prescribed degree of data confidentiality can simultaneously be attained by channel coding without any secret key. Wyner replaced Shannon's perfect secrecy with the weak secrecy condition, namely the asymptotic rate of leaked information between the transmit message and the channel output at Eve's side should vanish as the code length tends to infinity. Unfortunately, it is still possible for a scheme satisfying weak secrecy to exhibit some security flaws, *e.g.*, the total amount of leaked information may go to infinity, and now it is widely accepted that a physical-layer security scheme should be secure in the sense of Csiszár's strong secrecy, *i.e.*, the total information leakage should vanish when the code length tends to infinity.

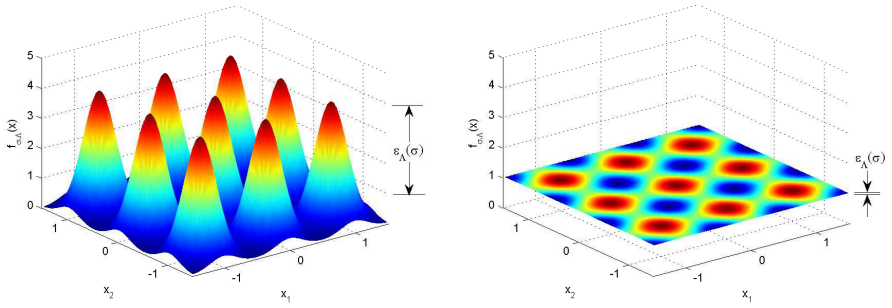


Fig. 5 Eve's likelihood when using a two-dimensional lattice. Flatness factor measures the span.

In this framework, recently Mahdavifar and Vardy [21] have proposed polar wiretap codes for symmetric binary input channels and demonstrated that they can be SC achieving for long lengths. Alternatively, the most exploited approach to the design of practical codes so far has been to use low density parity check (LDPC) codes [34], both for binary erasure and symmetric channels and for Gaussian channels with binary inputs.

An important recent development concerns the case of the Gaussian wiretap channel with a power constraint which has been addressed by using lattice codes [19]. This channel model is key in further developments since coding schemes for it include both modulation and coding. Importantly, strong secrecy for any message was proven in this situation in [19]. The proposed coding scheme uses two nested lattices, a fine and a coarse one. A point in the fine lattice is the sum of a coarse lattice point and a point of minimal energy which is in the fine lattice, but not in the coarse lattice. This latter point is similar to the remainder of a Euclidean division.

The proposed coding scheme works as follows:

- A sequence of pseudorandom bits labels the points of the coarse lattice.
- The data labels the pseudo remainder.

If the lattice scheme is correctly designed, then the legitimate receiver, Bob, can reliably decode the fine lattice while Eve has no information concerning the data. A lattice scheme which is good for the wiretap channel is designed in the following manner:

- The fine lattice is good for coding.
- The coarse lattice is good for secrecy, which means that its "flatness factor" [19] vanishes when the code length goes to infinity.

Fig. 5 shows Eve's likelihood when the noise variance is small and large. When it is large, then Eve cannot distinguish the points of the fine lattice (almost identically distributed). When the flatness factor is small, then points are almost undistinguishable for Eve. The flatness factor is closely related to the theta series of the coarse lattice, which was first studied by Oggier *et al.* [25].

4 Privacy Amplification Techniques

As explained in Section 3, the SC and the SKC are asymptotic metrics - achieved as the length of the respective encoders becomes arbitrarily long. These metrics are defined according to a "weak secrecy" requirement so that the *rate of information leakage* to Eve should be arbitrarily small. As noted previously, the adequacy of this secrecy definition has been questioned on the grounds that the absolute amount of information that can be observed by the adversary is not bounded and in general can be non-negligible.

In this context, Maurer, Bennet *et al.* in [22], [3] and other related work [23] have proven that the use of *privacy amplification techniques* can effectively transform a weakly secure channel to a strongly secure channel, in which the adversary can at most observe a negligible absolute amount of information. Favorably, it was demonstrated that the definitions of the SC and of the SKC can be strengthened *without any penalty in terms of achievable rates*. Interestingly, strong secrecy can be obtained from weak secrecy "for free" through the use of a public feedback channel, in essence extending the one-way communication models to two-way communication models.

The core idea behind these techniques is the use of appropriate feedback messages chosen to provide enough *side information* to Bob's secrecy decoder to completely resolve any residual ambiguity, while at the same time leaking only a negligible absolute amount of information to Eve.

- *Toy example:* Let us assume the following scenario of a two phase secret key distillation process. First, Alice broadcasts a random bit sequence. For the sake of simplicity, let us assume that Bob and Eve obtain *independent* noisy observations of this sequence and respective "soft" bit sequences at the outputs of their decoders. In the second phase of the key distillation Bob broadcasts the positions of his most "reliably decodable" bits (bits he decoded with probability arbitrarily close to unity). Assuming that there is sufficient noise in the channel and the sequences are long enough, the probability that Eve has reliably decoded the exact same subsequence as Bob becomes negligible. Finally, Alice and Bob distill their common keys by using a universal hash function to compress the mutually established subsequence. As a result of the use of an *information reconciliation phase* and of a *privacy amplification phase* Alice and Bob have thus distilled a secret key while the absolute amount of information leaked to Eve is kept arbitrarily small.

In the key distillation example discussed above the adversarial channel need not be degraded with respect to (w.r.t.) the main channel; it suffices that it is not almost noiseless, *i.e.*, that Eve cannot reliably decode the whole sequence. In analogy, the use of feedback to ensure secrecy can be further generalized to enable the broadcasting of secret messages in non-degraded channels.

- *Toy example:* let us assume the case in which Alice wishes to transmit a secret message d to Bob while the links between Alice, Bob and Eve are scalar Gaussian channels and the main link is noisier than the eavesdropping link. Under these assumptions, the SC of the one-way Gaussian channel between Alice and Bob is zero.

However, this negative setting can be reversed by allowing for two-way communication between Alice and Bob as described in Table 1.

Table 1 Privacy Amplification in Non-Degraded Gaussian Channel

First Phase	
Bob transmits	local random symbol x
Alice receives	$x+n, n \sim \mathcal{N}(0,\sigma_m^2)$
Eve receives	$x+w, w \sim \mathcal{N}(0,\sigma_e^2), \sigma_e^2 \leq \sigma_m^2$
Second Phase	
Alice transmits	encoded symbol $f(d+x+n)$
Bob's optimal decoder	cancels out x and retrieves d from $f(d+n)$
Eve's optimal decoder	retrieves d from $f(d+n-w)$ (degraded channel w.r.t. Bob)

5 Applications of PLS Technologies and Extensions to Systems with Active Attacks

In the absence of a feedback channel and under the assumption that only the statistics of the adversarial channel are known, the question of feasibility of PLS technologies can be reduced to whether the intended destination has a measurable statistical advantage w.r.t. to the adversary. There exist important realistic scenarios in which such opportunities can be substantiated, as described in the following.

5.1 Massive MIMO and small cell systems

Fifth generation ($5G$) technologies with hundreds of antennas at the base stations can be promising candidates for the use of PLS technologies. In massive MIMO systems [7] there can exist channel degrees of freedom (DoF) that are unobservable by the adversary. As an example, based on the transmitter gain pattern the signal-to-interference-and-noise-ratio (SINR) is not necessarily higher in receivers in the proximity of the base station. The possibility of designing adaptive beamforming strategies accounting for the generation of highly secure regions of a guaranteed minimum SC arises. In parallel, millimeter wave, wireless optical systems and in general small cell networks are prominent candidates for the use of PLS techniques due to the sharp decline in signal quality outside a short range radius around the transmitter.

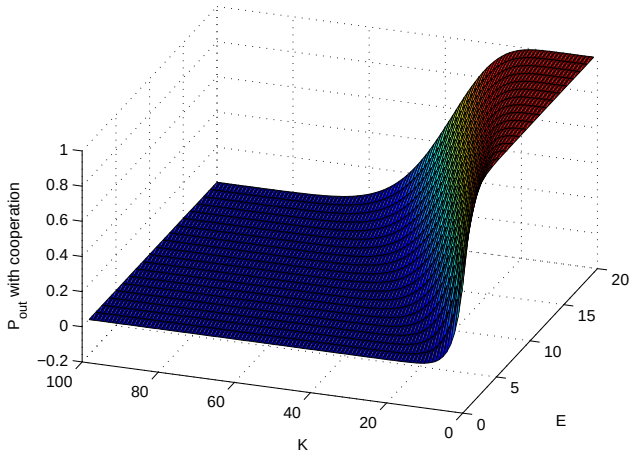


Fig. 6 Probability of secrecy outage for a target rate 1bps/Hz as a function of the diversity order K of Bob and E of Eve [4].

5.2 Multiple access and multi-user cooperative networks

In multiple access systems the employment of interference alignment techniques has been demonstrated to offer concrete opportunities for employment of PLS technologies, e.g. see Koyluoglu *et al.* [14]. Using interference alignment along with secrecy precoding, it has been proven that in a generic K user Gaussian interference channel $\frac{K-2}{2K}$ secure DoF can be achieved by each user in the ergodic setting when only the statistics of the adversarial channel are available. Furthermore, in cooperative networks with K legitimate users and E eavesdroppers the probability that the SC is below a target rate, denoted by P_{out}, has been shown to exhibit an abrupt phase transition characteristic as shown in Fig.6 [4]. As a result, in large multi-user networks, the feasibility of PLS can be incorporated in the network architecture design.

5.3 Interference assisted PLS technologies

In non-degraded one-way wiretap channels the use of helping interferers (HI) has been extensively investigated in the literature, e.g. [33]. In the generic HI framework a transmitter sends a confidential message to its intended receiver in the presence of a passive eavesdropper whose reception is jammed with the help of an independent interferer. The achievable secrecy rate and several computable outer bounds on the SC of the wiretap channel with an HI were evaluated in [11] for both discrete memoryless and Gaussian channels.

5.4 OFDM systems

Orthogonal frequency division multiplexing (OFDM) is a ubiquitous signaling technique for current mobile, WiFi and other systems. Thus, in the application of PLS, consideration of OFDM systems is an important element. This problem was addressed by Renna *et al.* [29], [30] by considering the physical layer of an OFDM transmitter/receiver pair in the presence of an eavesdropper that might either use an OFDM structure or choose a more complex receiver architecture. The analysis was made possible by modeling the system as a particular instance of a high dimensional MIMO wiretap channel. The problem of determining the SC was formulated as a maximization problem under a trace constraint, and simple expressions were given for its high signal-to-noise (SNR) limit.

5.5 Backscatter systems

Backscatter wireless communication lies at the heart of many practical low-cost, low-power, distributed passive sensing systems. The inherent cost restrictions coupled with the modest computational and storage capabilities of passive sensors, such as radio frequency identification (RFID) tags, render the adoption of classical security techniques challenging; which motivates the introduction of PLS approaches in this setting. This problem has been studied in [31], where, first, the secrecy rate of a basic single-reader, single tag RFID model was studied. Then, the unique features of the backscatter channel were exploited to maximize this secrecy rate.

5.6 Use of PLS technologies against active eavesdroppers

PLS techniques have been investigated for their potential use against various types of active attacks [36]. Lai et al. in [15] proposed a straightforward application of PLS for authentication purposes. The use of double-binning secrecy encoders was studied with the outer bin containing a public message and the inner bin a secret key to be used for authentication purposes. Furthermore, in [5] impersonation type of attacks were considered, with the active eavesdropper using false feedback to mislead the transmitter w.r.t. the achievable secrecy rate. Interestingly it was shown that in the high SNR regime the SC of such broadcasting systems is in essence unaffected by these type of attacks.

6 Open Research Issues and Future Directions in PLS

During the last fifteen years considerable research effort has concentrated on the area of information theoretic security. Today, the fundamental limits of secure communications over noisy channels have been established in the form of the respective capacity equivocation regions as discussed in Section 2. Furthermore, practical coding schemes that achieve the SC of certain channels have already come to light as discussed in Section 3. Despite significant results in the above-mentioned areas, a lot remains to be done before PLS technologies can be incorporated into practical engineering designs and their full potential for secure transmissions over noisy channels is achieved.

The first and foremost challenge in this direction is the design of explicit low complexity secrecy code constructions; unsurprisingly, similarly to the baseline scenario without secrecy constraints, this has proved to be a challenging task. In spite of existing results for certain specific models such as the discrete memoryless channel, much remains to be done. The most promising designs of secrecy encoders so far are based on polar codes and lattice codes; however, these schemes require large block lengths and therefore are only practical for delay unconstrained applications, *e.g.*, e-mail exchange. Unfortunately, they cannot be employed in delay constrained applications such as multimedia streaming or in networks with computationally limited devices such as wireless sensors. Secrecy encoder designs at short and medium block-lengths is the single foremost important open issue that needs to be investigated in the PLS framework.

Furthermore, several topics related to jointly authenticated and confidential transmissions remain unchartered areas of research. The exploitation of shared randomness techniques to establish a common source of randomness that is provably inaccessible to attackers could in principle form the basis of such schemes. In the same framework, the design of cross-layer security protocols is still in its infancy. Such designs could have the potential to exploit the unique properties of PLS techniques in demanding wireless scenarios such as ad hoc and device-to-device networks in which centralized key management schemes are not attainable and computational and power resources are constrained. Furthermore, the joint employment of PLS and encryption has only been considered from the viewpoint of independently using the respective approaches at different layers of the OSI protocol; no joint consideration of crypto-PLS designs yet exists. To this end, the systematic study of PLS in the active eavesdropping setting would be necessary, extending existing active attacker threat models to account for noisy communication channels.

7 Conclusions

Today, despite the indisputable success of established cryptographic approaches, recent advances in communications, networking and computing technologies require a paradigm shift in information security. In fact, the decentralized, relayed, virtual-

ized or even un-managed (device-to-device), and heterogeneous nature of modern networks (*e.g.*, 5G) renders the generation, management, and storage of secret keys particularly challenging under current security protocols. Additionally, the recent advances in the area of quantum computing have elicited the urgency of investigating alternative approaches to information security that do not rely on assumptions regarding the computational complexity of the associated problems.

Including the physical layer of communication systems in the security design has the potential to lead to this necessary paradigm shift. Several information-theoretic results suggest that the imperfections inherently present in a communication medium (fading, thermal noise, interference) may be harnessed to conceal information from potential eavesdroppers by coding at the physical-layer itself. In essence, the noise present in the communication channel can be exploited to achieve secrecy similar to one-time-pad encryption. After more than a decade of intense research in the area of PLS the fundamental limits of secure communications over noisy channels are now better understood and practical coding schemes exist that achieve the promises of information-theoretic results have come to light. Thus there is sufficient momentum and underlying science for PLS techniques to be considered for incorporation into practical engineering systems.

References

1. R. Ahlswede and I. Csiszàr, *Common randomness in information theory and cryptography-part I: Secret sharing*, IEEE Trans. Information Theory **39** (1993), no. 4, 1121–1132.
2. R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M.R. Bloch, S. Ulukus, and A. Yener, *Cooperative security at the physical layer: a summary of recent advances*, IEEE Signal Processing Magazine **30** (2013), no. 5, 16–28.
3. C.H. Bennett, G. Brassard, C. Crépeau, and U.M. Maurer, *Generalized privacy amplification*, IEEE Trans. Information Theory **50** (1995), no. 2, 394–400.
4. A. Chorti, K.P. Papadaki, and H.V. Poor, *Optimal power allocation in block fading channels with confidential messages*, IEEE Trans. Wireless Communications (2015), to appear.
5. A. Chorti, Samir M. Perlaza, Z. Han, and V. Poor, *On the resilience of wireless multiuser networks to passive and active eavesdroppers*, IEEE J. Selected Areas in Communications **31** (2013), no. 9, 1850–1863.
6. I. Csiszár and J. Körner, *Broadcast channels with confidential messages*, IEEE Trans. Information Theory **24** (1978), no. 3, 339–348.
7. T. Dean and A. Goldsmith, *Physical-layer cryptography through massive MIMO*, arXiv:1310.1861 [cs.IT], submitted to IEEE Transactions on Information Theory, 2013.
8. E. Ekrem and S. Ulukus, *The secrecy capacity of the Gaussian MIMO multi-receiver wiretap channel*, IEEE Trans. Information Theory **57** (2011), no. 4, 2083–2114.
9. P. Gopala, L. Lai, and H. El-Gamal, *On the secrecy capacity of fading channels*, IEEE Trans. Information Theory **54** (2008), no. 10, 4687–4698.
10. X. He and A. Yener, *Cooperation with an untrusted relay: a secrecy perspective*, IEEE Trans. Information Theory **56** (2010), no. 8, 3807–3827.
11. J. Katz and Y. Lindell, *Introduction to modern cryptography*, CRC Press Inc., Boca Raton, FL, August 2007.
12. A. Khisti and G.W. Wornell, *Secure transmission with multiple antennas-part I: The MISOME wiretap channel*, IEEE Trans. Information Theory **56** (2010), no. 7, 3088–3104.

13. A. Khisti and G.W. Wornell, *Secure transmission with multiple antennas-part II: The MIMOME wiretap channel*, IEEE Trans. Information Theory **56** (2010), no. 11, 5515–5532.
14. O. Koyluoglu, H. El Gamal, L. Lai, and H.V. Poor, *Interference alignment for secrecy*, IEEE Trans. Information Theory **57** (2011), no. 6, 3323 – 3332.
15. L. Lai, H. El Gamal, and H.V. Poor, *Authentication over noisy channels*, IEEE Trans. Information Theory **55** (2009), no. 2, 906–916.
16. S.K. Leung-Yan-Cheong and M.E. Hellman, *The Gaussian wire-tap channel*, IEEE Trans. Information Theory **24** (1978), no. 4, 451–456.
17. Y. Liang and H.V. Poor, *Multiple-access channels with confidential messages*, IEEE Trans. Information Theory **54** (2008), no. 3, 976–1002.
18. Y. Liang, H.V. Poor, and S. Shamai, *Secure communication over fading channels*, IEEE Trans. Information Theory **54** (2008), no. 6, 2470–2492.
19. C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehle, *Semantically secure lattice codes for the Gaussian wiretap channel*, IEEE Trans. Information Theory **60** (2014), no. 10, 63996416.
20. R. Liu, T. Liu, H.V. Poor, and S. Shamai, *New results on multiple-input multiple-output broadcast channels with confidential messages*, IEEE Trans. Information Theory **59** (2013), no. 3, 1346–1359.
21. H. Mahdavifar and A. Vardy, *Achieving the secrecy capacity of wiretap channels using polar codes*, IEEE Trans. Information Theory **57** (2011), no. 10, 6428–6442.
22. U. M. Maurer, *Secret key agreement by public discussion from common information*, IEEE Trans. Information Theory **39** (1993), no. 3, 733–742.
23. U. M. Maurer, R. Renner, and S. Wolf, *Unbreakable keys from random noise*, Security with Noisy Data, Springer, 2007, pp. 21–44.
24. F. Oggier and B. Hassibi, *The secrecy capacity of the MIMO wiretap channel*, IEEE Trans. Information Theory **57** (2011), no. 8, 4961 – 4972.
25. F. Oggier, P. Solé, and J.-C. Belfiore, *Lattice codes for the wiretap Gaussian channel: Construction and analysis*, arXiv:1103.4086v3 [cs.IT] (2011).
26. Y. Oohama, *Coding for relay channels with confidential messages*, Proc. of the Information Theory Workshop (ITW) (Cairns, Australia), September 2001, pp. 87–89.
27. ———, *Capacity theorems for relay channels with confidential messages*, IEEE International Symposium on Information Theory - ISIT 2007 (Nice, France), June 2007, pp. 926–930.
28. L. Ozarow and A. Wyner, *Wire-tap channel II*, Advances in Cryptology, Lecture Notes in Computer Science **209** (1985), 3350.
29. F. Renna, N. Laurenti, and H.V. Poor, *Physical layer secrecy for OFDM transmissions over fading channels*, IEEE Trans. on Information Forensics and Security **7** (2012), no. 4, 1354 – 1367.
30. F. Renna, N. Laurenti, S. Tomasin, M. Baldi, N. Maturo, M. Bianchi, F. Chiaraluce, and M. Bloch, *Low-power secret-key agreement over OFDM*, CoRR **abs/1302.4767** (2013).
31. W. Saad, X. Zhou, Z. Han, and H.V. Poor, *On the physical layer security of backscatter wireless systems*, IEEE Trans. on Wireless Communications **13** (2014), no. 6, 3442 – 3451.
32. C. Shannon, *Communication theory of secrecy systems*, Bell System Technical J. **28** (1949), 656–715.
33. X. Tang, R. Liu, P. Spasojevic, and H.V. Poor, *Interference assisted secret communication*, IEEE Trans. Information Theory **57** (2011), no. 5, 3153–3167.
34. A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, *Applications of LDPC codes to the wiretap channel*, IEEE Trans. Information Theory **53** (2007), no. 8, 2933–2945.
35. A.D. Wyner, *The wire-tap channel*, Bell System Technical J. **54** (1975), no. 8, 1355–1387.
36. Z. Xiangyun, B. Maham, and A. Hjorungnes, *Pilot contamination for active eavesdropping*, IEEE Trans. Wireless Communications **11** (2012), no. 3, 903–907.
37. S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai, *Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT*, IEEE Trans. Information Theory **59** (2013), no. 9, 5244–5256.