Computer Networks 109 (2016) 21–30

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Reliable and perfectly secret communication over the generalized Ozarow-Wyner's wire-tap channel

Giulio Aliberti[a,b], Roberto Di Pietro[a,d,*], Stefano Guarino[c]

[a] Security Research, Nokia Bell Labs, Paris, France
[b] Università di Roma Tre, Dip.to di Matematica, Roma, Italy
[c] Istituto per le Applicazioni del Calcolo "Mauro Picone" (IAC), Consiglio Nazionale delle Ricerche (CNR), Italy
[d] Università di Padova, Dip.to di Matematica, Padova, Italy

ARTICLE INFO

Article history:
Received 14 October 2015
Revised 9 May 2016
Accepted 26 June 2016
Available online 29 June 2016

Keywords:
Physical layer security
Wire-tap channel
Perfect secrecy
Error-correcting codes
Secret sharing

ABSTRACT

In a typical secure communication system, messages undergo two different encodings: an error-correcting code is applied at the physical layer to ensure correct reception by the addressee (integrity), while at an upper protocol layer cryptography is leveraged to enforce secrecy with respect to eavesdroppers (confidentiality). All constructive solutions proposed so far to concurrently achieve both integrity and confidentiality at the physical layer, aim at meeting the secrecy capacity of the channel, *i.e.*, at maximizing the rate of the code while guaranteeing an asymptotically small information leakage.

In this paper, we propose a viable encoding scheme that, to the best of our knowledge, is the first one to guarantee both perfect secrecy (*i.e.*, no information leakage) and reliable communication over the *generalized* Ozarow-Wyner's wire-tap channel. To this end, we first introduce a metric called *uncertainty rate* that, similarly to the *equivocation rate* metric, captures the amount of information leaked by a coding scheme in the considered threat model, but it is simpler to apply in the context of linear codes. Based on this metric, we provide an alternative and simpler proof of the known result that no linear error-correcting code alone can achieve perfect secrecy. Finally, we propose a *constructive* solution combining secret sharing and linear error-correcting codes, and we show that our solution provides the desired combination of reliable and perfectly secret communication. The provided solution, other than being supported by thorough analysis, is viable in practical communication systems.

© 2016 Elsevier B.V. All rights reserved.

1. Introduction

Secure communications require two equally important conditions being concurrently guaranteed: (i) integrity, *i.e.*, correct reception of the message by the intended recipient; and, (ii) confidentiality, *i.e.*, only authorized users should be able to access the content of the message. The integrity of the message received by the addressee may be voluntarily endangered by an adversary (*e.g.*, through jamming) or disturbed by natural phenomena such as noise, distortion, and fading. Even when the adversary is not able (or not intending) to modify the message, she can easily eavesdrop on the transmissions whenever the communication channel is insecure (*e.g.*, wireless). Regardless of the origin of the noise, reliable communication over *noisy* channels is usually made possible by adding redundancy to the data transmitted through Error-Correcting Codes (ECC), whereas cryptography is the standard solution to enforce data confidentiality and integrity under active attacks [1].

In many circumstances, the adversary can access and/or modify only a limited amount of information with respect to the intended recipient. To describe a similar scenario, Wyner introduced a model for physical layer security, called wire-tap channel model [2], in which the message travels over two different channels: the *main* channel, accessible to the addressee, and the *eavesdropper's* channel, suffering from superior noise. The model was later simplified by Ozarow and Wyner with the introduction of the wire-tap channel II (or Ozarow-Wyner's wire-tap channel) [3], in which the main channel is noiseless, and the concept of eavesdropper's channel is substituted by the assumption that the adversary can choose any subset of $l \leq n$ noiseless digits, where n is the message length. The Generalized Ozarow-Wyner's wire-tap (GOW) channel [4] combines the wide applicability of the original wire-tap channel with the precisely defined eavesdropper of the wire-tap II, as-

[*] Corresponding author.
E-mail addresses: aliberti@mat.uniroma3.it (G. Aliberti), roberto.di_pietro@nokia.com, dipietro@mat.uniroma3.it (R. Di Pietro), s.guarino@iac.cnr.it (S. Guarino).

http://dx.doi.org/10.1016/j.comnet.2016.06.034
1389-1286/© 2016 Elsevier B.V. All rights reserved.

suming that the main channel is a Discrete Memoryless Channel (DMC), and that the adversary can eavesdrop on a subset of l codeword digits of her choice.

For traditional channels, Shannon proved that it is possible to reliably communicate at rates arbitrarily close to the channel's capacity, provided that codewords are sufficiently long. Similarly, Wyner proved that it is possible to reliably and securely communicate (*i.e.*, achieving perfect secrecy) over the wire-tap channel at rates arbitrarily close to what he called the *secrecy capacity* of the channel. Wyner did not propose any practical construction for a perfectly secret and reliable code, but recent work showed how the secrecy capacity of the channel can be actually achieved with advanced coding schemes [5,6]. Unfortunately, all similar results consider the asymptotic behaviour of the code, *i.e.*, perfect secrecy is only guaranteed when the message becomes "infinitely long". Traditional ECCs that achieve some level of secrecy exist [7], and secret sharing [8] or similar techniques can provide perfect secrecy over the wire-tap channel II, but none of them alone can provide both security requirements over the GOW channel.

While trying to maximize the rate of secure communications is extremely fascinating, it is likewise important to understand whether current protocols, that do not require cryptography or unrealistically long codewords, can concurrently guarantee perfect secrecy and resilience to transmission errors, and what is the related overhead. In this paper, we show how to combine ECCs and secret sharing to achieve perfect secrecy while enforcing arbitrary error correction capabilities in the GOW wire-tap channel model. What we propose is a thorough analysis of a *constructive* solution that can serve as a benchmark to which previous and future proposals can be compared.

Contributions

In this paper we provide the following contributions:

- We introduce the *uncertainty rate* security metric, defined as a special case of the well known equivocation rate [9]. We show that the proposed metric is particularly suitable for measuring the security of a code in the GOW channel;
- Relying on the proposed uncertainty rate, we show how to easily measure the level of confidentiality guaranteed by a linear ECC when used over the GOW channel. In particular, we exhibit a simple proof that such codes alone cannot achieve perfect secrecy—as already known in the literature for the traditional wire-tap channel;
- We propose a novel, general and constructive procedure based on secret sharing that transforms any ECC into a secure wire-tap code. Analytic results prove that through this procedure we achieve perfect secrecy and resilience to data loss;
- We thoroughly analyse the pros and cons of the solution proposed, discussing them with the help of a toy example, and outlining a more realistic case study.

To the best of our knowledge, our approach to secure communications leveraging the physical layer is completely independent from similar solutions in the literature, with the further benefit of being extremely practical and constructive.

Roadmap

We start with a complete characterization of our system model in Section 2, that includes an overview of linear ECCs and secret sharing schemes[1]. In Section 3 we discuss related work. In Section 4 we introduce the notion of uncertainty rate and use it to discuss deficiencies and limitations of linear codes under the considered threat model. In Section 5, after highlighting why secret sharing alone is not a feasible option, we propose a constructive solution based on a combination of secret sharing with an ECC, and discuss it via a toy example. Finally, Section 6 reports our conclusions.

2. Coding primitives and channel model

In this section, we recall the definition and the main properties of the coding primitives that will be used in the sequel of this paper, and we characterize our channel model. More specifically, in Section 2.1 we briefly review linear ECCs and secret sharing schemes, while in Section 2.2 we describe the Generalized Ozarow-Wyner's wire-tap (GOW) channel model [3]. Hereinafter, $\mathbf{F}_q$ will denote the finite field of order q, where $q = p^\nu$ is a prime power.

2.1. Coding primitives

Linear error-correcting codes

A linear Error-Correcting Code is a deterministic map E from a set of messages $M = \mathbf{F}_q^k$ into a set of codewords $C \subset \mathbf{F}_q^n$, such that, for each $m \in M$, the digits of $c = E(m) \in C$ are obtained as n linear combinations of the digits of m. The set C is a linear subspace of $\mathbf{F}_q^n$ of dimension k, and it uniquely determines the code. The code is usually defined by either means of its $n \times k$ matrix G, called generating matrix of the code, such that $c = G \cdot m$, or by its $(n-k) \times n$ parity-check matrix H, such that $H \cdot c = 0$ if and only if $c \in C$. Each codeword of length n conveys k information digits and the ratio $r = k/n$ is called code *rate*. k and n are called the *dimension* and the *length* of the code, respectively.

Secret sharing

Assume a user U knows a secret S. A (i, j)-threshold *secret sharing* scheme allows U to choose two positive integers j and $i \leq j$ and to generate j pieces of information, such that any i out of them are necessary and sufficient to recover S. The most known construction of secret sharing schemes relies on polynomial interpolation,[2] leveraging on the fact that any point of the curve defined by a polynomial of degree $i-1$ determines a linear equation satisfied by the i coefficients of the polynomial. If $S \in \mathbf{F}_q$, a random polynomial $f(x) \in \mathbf{F}_q[x]$ with free term S is chosen, and j pieces of information $d_1, \ldots, d_j \in \mathbf{F}_q$, denoted *shares*, are generated as $d_t = f(t) \bmod \mathbf{F}_q$, for $t = 1, \ldots, j$. Anyone with access to i or more shares can recover $f(x)$, and thus S, but with less than i shares anyone of the possible q values for S is exactly equally likely, and no information about S is leaked.

2.2. The generalized Ozarow-Wyner's wire-tap channel model

Wire-tap channel

The wire-tap channel model, depicted in Fig. 1, describes a scenario where two parties, Alice and Bob, want to communicate over a noisy channel, but an adversary Eve tries to eavesdrop on the communications. Since the channel between Alice and Bob, referred to as the *main* channel, is noisy, Alice uses an encoder E to obtain a codeword $c \in \mathbf{F}_q^n$ from the original message $m \in \mathbf{F}_q^k$. Bob receives a noisy version c_B of c and uses a decoder D_B to remove the noise and obtain a message m_B. The communication is successful if $m_B = m$. To model Eve having limited eavesdropping capacity, in Wyner's model she is assumed to have physical access to a channel noisier than that of Bob, called the *eavesdropper's* channel, over which the same codeword c is sent. Eve receives a different noisy version c_E of c, and tries to decode it with her own decoder D_E, obtaining a message m_E.

[1] This section can be safely jumped by readers familiar with the topic.

[2] Sharing schemes were formally introduced independently by Shamir [8] and Blakley [10]. The two schemes are *de facto* equivalent, but Shamir's definition, based on polynomial interpolation, is the most renowned.

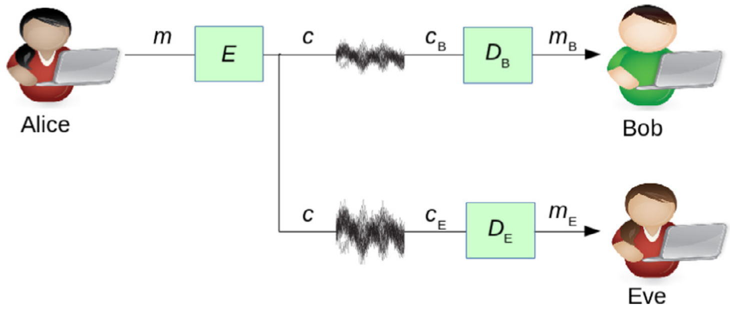

Fig. 1. A graphical representation of the wire-tap channel.

Generalized Ozarow-Wyner's channel

The wire-tap channel is a generic model, whose performance is considerably dependent on the type of noise experienced by the recipient Bob and the adversary Eve. To simplify the analysis, the Ozarow-Wyner's model (OW) was proposed as a variation of the wire-tap. It consists in a noiseless main channel, and in an adversary Eve that is capable of gaining access to a subset of $l \leq n$ noiseless digits of c of her choice, where n is the codeword length. A middle ground between such two configurations is the Generalized Ozarow-Wyner's (GOW) model, in which the main channel is modelled as a Discrete Memoryless Channel (DMC), but the eavesdropper's channel is modelled as in the OW. From a security standpoint, without specific assumptions on the type of noise affecting the main channel (except for it being *memoryless*), and by letting l vary from 0 to n, the GOW model covers all possible scenarios, from the best- to the worst-case. Assuming that Eve is able to extract l noiseless digits allows neglecting both the noise affecting the adversary and the unknown quantity of information she intercepts, while only focusing on what is ultimately relevant. Besides, application settings where a similar eavesdropper is realistic do exist: if the codewords are split into several sub-codewords, each one transmitted over a different noiseless physical link, the assumption that the adversary cannot earn more than l digits can be replaced with the assumption that the adversary cannot eavesdrop from more than l physical links.

3. Related work

Whenever communication occurs over an insecure channel, it is fundamental to concurrently ensure integrity and confidentiality of the transmitted data. In particular, the recent rise of wireless transmissions drew the attention to physical-layer security as a promising paradigm to protect communications against eavesdropping attacks by exploiting the physical characteristics of the channel [11]. The fundamentals for physical-layer security [7] were laid in the early seventies with the introduction and elaboration of Wyner's wire-tap channel [2]. Since then, several extensions of Wyner's channel model have been considered: for instance, the Broadcast Channel with Confidential messages (BCC) [12] in which, similarly to the wire-tap channel, a message intended for one of the receivers is confidential; the Gaussian channel [13], that is the Wyner's wire-tap channel when data transmission errors are modelled through Additive White Gaussian Noise (AWGN); and, channels that impose a combinatorial constraint, rather than probabilistic, on the adversary [3,6].

To discuss the security of the wire-tap channel, Wyner introduced the notions of *reliability condition* and *security condition* [2]. The reliability condition is verified if $\lim_{k\to+\infty} \Pr[m' \neq m] = 0$, *i.e.*, if the error probability approaches zero as the size of the message grows. The security condition, instead, is verified if $\lim_{k\to+\infty} I(m, y)k^{-1} = 0$, *i.e.*, if the normalized mutual information between the eavesdropped data and the message is zero. Based on such two requirements, Wyner also introduced the concept of *secrecy capacity* of the channel, that is the maximum rate at which information can be transmitted over the channel with the reliability and security conditions holding. Wyner proved that when the receiver's channel is subject to less noise than the wire-tapping opponent's one the secrecy capacity is positive, *i.e.*, it is possible to communicate over that channel without violating either of the two conditions. Several papers [14,15] (even very recently [16–20]) followed Wyner's work, focusing on the concept of secrecy capacity and the security properties of error-control coding techniques.

Wyner's work had two main limitations. On the one hand, its security condition was too weak, as highlighted by Maurer [14], who suggested to replace Wyner's security condition with the requirement that the mutual entropy approaches zero as the size of the message grows; that is: $\lim_{k\to+\infty} I(m, y) = 0$. However, even Maurer's definition responds to an idea of asymptotic security, while perfect secrecy actually means to leak *no* information at all. On the other hand, Wyner did not provide any constructive indication for designing codes approaching the secrecy capacity. Several researchers tried to fill in this gap, but the best results were obtained under precise assumptions on the channel model (*e.g.*, Binary Erasure Channel [21], Binary Symmetric Channel [22], combinatorial constrained model [6], Gaussian wire-tap channel [23,24], compound wire-tap channel [25], broadcast channel with confidential messages [26]). In general, what emerges is that LDPC codes [21,23,25] and Polar Codes [22,24,26] seem the most promising solutions.

Wrapping up, past research concerning the wire-tap channel mostly focused on understanding if and how it is possible to communicate at rates approaching the secrecy capacity of the channel, *i.e.*, only trying to guarantee (to some extent) asymptotic secrecy. Conversely, this paper aims at providing a constructive solution to obtain perfect secrecy with practical encoding and decoding algorithms. We achieve this goal by applying secret sharing as a preliminary step to any ECC encoder. The joint use of ECCs and some sort of secret sharing is not new in the literature [27] and, indeed, theoretical results suggest that secret sharing problems can be reformulated as equivalent secure communication problems via wire-tap channel models [28]. Some practical solutions [5,6] are based on Rivest's *All-Or-Nothing Transform* (AONT) [29], a primitive assimilable to (*i, j*) secret sharing[3]. Reliability for transmission errors could in principle be obtained combining AONTs with error-correction codes, as successfully proposed for data security in dispersed storage systems [30]. However, analogous solutions for the wire-tap channel have never been investigated and—differently from the proposed solution—they would rely on a cryptographic construction. A different cryptographic based

[3] A more typical notation is (k, n) secret sharing. However, k and n are reserved for denoting dimension and length of a code, respectively. See Section 2.1 for our notations.

construction [31] relies on invertible extractors and focuses also on providing reliability properties. Finally, a more recent approach [32] considers a channel model called *Adversarial WireTaP* (AWTP) channel, in which Eve is able to eavesdrop on a noiseless fraction ρ_r and to mask a fraction ρ_w of the transmitted codeword, with $\rho_r + \rho_w < 1$. To achieve secrecy and reliability over the AWTP, the authors propose a solution based on AMD codes , Subspace Evasive Sets, and Folded Reed-Solomon codes. However, the code here proposed requires very long messages and codewords, achieving secrecy capacity only *asymptotically*. With respect to this work, we will present a scheme that has the desirable properties of being both more flexible and readily usable. Additionally, the AWTP is a fully adversarial model characterized by the restrictive condition $\rho_r + \rho_w < 1$, contrarily to the hybrid GOW model where the eavesdropper's channel is adversarial, but there are no limitations on the main channel except for it being probabilistic. This means that our scheme guarantees perfect secrecy and reliability under identical assumptions on the eavesdropper's channel, but more widely applicable assumptions on the main channel.

4. Security of linear codes in the generalized Ozarow-Wyner's model

In this section we provide fundamental results helpful to determine the level of security provided by linear ECCs when used as encoders in the Generalized Ozarow-Wyner's (GOW) model. To this end, we first introduce in Section 4.1 the notion of uncertainty rate, to capture to which extent a code used over a specific channel leaks information concerning the transmitted data. Then, in Section 4.2 we introduce two practical formulas binding the uncertainty rate of the code to its parameters and to the code rate, respectively. Our results are discussed in Section 4.3, and compared with the state of the art in Section 4.4.

4.1. Uncertainty rate

As we discussed in Section 3, Wyner [2] proposed a definition of security for the wire-tap channel based on two desiderata, that he defined reliability and security conditions. Based on such requirements, he introduced the notion of secrecy capacity of a channel, that intuitively corresponds to the maximum rate at which information can be securely transmitted over that channel. However, while Wyner's definition focuses on the intrinsic and asymptotic properties of the channel, we are more interested in discussing security under a different perspective: we want to measure the amount of information leaked as a function of both the specific threat model and coding scheme considered. Since recent work [33,34] demonstrates the validity of the *equivocation rate* [35] as a secrecy metric, to achieve our goal we opted to specialize such a measure to meet our needs. The result is the *uncertainty rate*, a very practical secrecy metric defined in the following.

Let us assume that Alice and Bob are communicating over a wire-tap channel using a linear ECC of dimension k and length n. The adversary Eve eavesdrops on the transmission of a codeword c, obtaining a noisy version c_E of c.

Definition 1 (Dimension of uncertainty)**.** Let us assume that, based on c_E and leveraging on the linear equations binding the digits of c, Eve is able to reduce the space where c varies to a set of q^s equally likely codewords. We call the parameter $s \le k$, which depends on both the system and the threat model, the *dimension of uncertainty* of the adversary

Since the total number of admitted codewords is q^k, the ratio between the two dimensions $\epsilon = s/k \in [0, 1]$ is a normalized measure of the adversary uncertainty.

Definition 2 (Uncertainty rate)**.** Let $s \le k$ be the dimension of uncertainty of the adversary, and let $\epsilon = s/k \in [0, 1]$. We refer to ϵ as the *uncertainty rate* of the adversary.

Let us observe that, in the worst case for security, given a dimension of uncertainty equal to s the adversary can reconstruct at most

$$k - s = \lceil (1 - \epsilon)k \rceil \tag{1}$$

digits of the original message m. In case of a systematic linear code, the adversary can directly obtain exactly $k - s$ digits of m, since she has the freedom to choose which digits to eavesdrop. Even when a non-systematic linear code is used, there could exist $k - s$ parity digits binding exactly $k - s$ message digits. On the other hand, if the adversary was able to recover more than $k - s$ digits of the original message, her uncertainty would be limited to less than q^s codewords, which contradicts the definition.

The dimension of uncertainty s coincides with the Shannon's entropy of the codeword c, conditioned to the intercepted word c_E. In fact, if knowing c_E allows Eve to infer that the codeword c is uniformly distributed in a set of size q^s, then

$$\mathcal{H}(c|c_E) = -\sum_{i=1}^{q^s} \frac{1}{q^s} log_q\left(\frac{1}{q^s}\right) = s$$

where $\mathcal{H}$ denotes the entropy function.[4]

The uncertainty rate is in fact a normalized metric that depends on the dimension k of the code, and such that the higher it is, the lesser is the information leakage of the code. Ideally, we would like to find a code with uncertainty rate $\epsilon = 1$ since this would guarantee zero leakage. Unfortunately (yet intuitively), in the next section we will prove that no code can achieve $\epsilon = 1$ under the GOW model with positive parameter $l > 0$.

4.2. Measuring security through the uncertainty rate

In the GOW model, the adversary Eve eavesdrops l noiseless digits of her choice from the transmitted codeword c. We assume that the specifications of the code used are known to Eve, *i.e.*, she knows the linear parity-check equations that bind the digits of c. Based on the l digits available to her and on such equations, Eve can infer information about the original message m. Relying on our notion of uncertainty rate, Theorem 1 and Corollary 1 establish to which extent this happens. To enhance readability, all proofs are postponed to Appendix A.

Theorem 1. *Assume that a linear ECC code of dimension k and length n is used as an encoder in the GOW wire-tap channel model, in which the adversary has access to l noiseless digits of the transmitted codeword c. The dimension of uncertainty of the code is 0, and so is the uncertainty rate, if and only if $l \ge k$. For all $l < k$, the dimension of uncertainty of the code is $s = k - l$, and the uncertainty rate is $\epsilon = \frac{s}{k} = 1 - \frac{l}{k}$. In particular, $\epsilon = 1$ if and only if $l = 0$. Hence, a linear code alone cannot guarantee perfect secrecy.*

Observe that Theorem 1 could be equivalently stated in terms of the rank of the parity check matrix H of the code, recalling that such rank is $n - k$. This may turn to be especially useful since some powerful families of linear codes (*e.g.*, LDPC codes), are usually described and generated by means of the matrix H.

While Theorem 1 binds the uncertainty rate of the code to its parameters and to the number l of intercepted digits,

[4] Our uncertainty rate coincides with the equivocation rate of the message in the traditional Wyner's model (except for base q logarithm, as we are assuming digits in $\mathbf{F}_q$), but it is a more direct measure of the level of uncertainty of the adversary when we focus on the GOW channel.

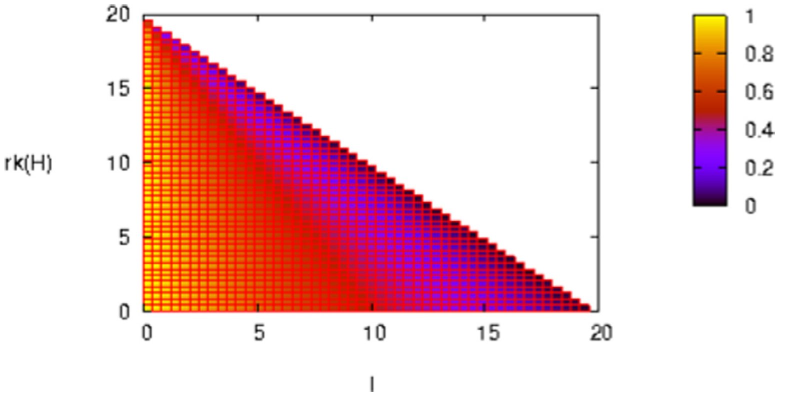

Fig. 2. Values for the uncertainty rate $\epsilon = s/k \in [0, 1]$ achievable by an ECC code with code length $n = 20$. The colour matches with the value of ϵ (darker is lower) that is depicted as a function of both the rank of the parity-check matrix rk(H) and the number of digits eavesdropped by the adversary l.

Corollary 1 expresses the same results in terms of rates of information transmitted, and eavesdropped.

Corollary 1. *Assume that a linear ECC code of dimension k and length n is used as an encoder in the GOW wire-tap channel model, in which the adversary has access to l noiseless digits of the transmitted codeword c. Let* $\rho = \frac{k}{n}$ *denote the code rate, and let* $\lambda = \frac{l}{n}$ *denote the eavesdropping rate of the adversary. The uncertainty rate of the code is 0 if and only if* $\rho \le \lambda$. *For all* $\rho > \lambda$, *the uncertainty rate is* $\epsilon = 1 - \frac{\lambda}{\rho}$. *In particular,* $\epsilon = 1$ *if and only if* $\lambda = 0$.

When the code length n grows, the number l of digits accessible to the adversary can be reasonably expected to grow proportionally, exactly as the code dimension k. The eavesdropping rate λ is exactly the proportionality constant between l and n, similarly to the code rate ρ for k and n. Corollary 1 shows how ϵ depends on ρ and λ, capturing the idea that the uncertainty rate does not really depend on the code dimension and length, but rather on the rates to which information is transmitted and eavesdropped. The corollary shows that there exists a critical value for the code rate under which the code becomes completely unreliable for security purposes under the GOW channel model, and that such a critical value is exactly the eavesdropping rate of the adversary.

4.3. Discussion

The uncertainty rate is remarkably suitable to measure the level of security guaranteed by a linear code under the GOW model. Corollary 1 is particularly interesting, relating the uncertainty rate with the code rate ρ and the eavesdropping rate λ. The code rate, that is, the ratio between the dimension k of the code and its length n, measures how much information a code conveys. The eavesdropping rate, that is, the ratio of code digits available to the adversary, measures the amount of information leaked. The smaller is the code rate, the larger is the redundancy introduced by the code, improving the error correcting capabilities of the code, but concurrently facilitating the attack. Secure communications when $\rho \le \lambda$ are impossible, and, in general, the security depends of the ratio $\frac{\lambda}{\rho}$.

In the following, we exhibit a graphical representation of achievable values of uncertainty rate for linear codes with fixed code length, by varying the rank of the parity-check matrix and the eavesdropping ability of the adversary. In particular, Fig. 2 shows achievable uncertainty rates $\epsilon \in [0, 1]$ for a linear code with $n = 20$ as a function of both the rank of the parity-check matrix rk(H) and the number l of digits eavesdropped by the adversary. The larger is l, the lower must be the rank of the parity-check matrix to ensure a positive value of uncertainty. The special cases $l = 5, 10, 15$ are further depicted in Fig. 3; for instance, the maximum value of uncertainty rate achievable when the adversary gets $l = 10 = n/2$ digits of the codeword is $\epsilon = 0.5$. Notably, for different values of n, the graphics in both figures show the same qualitative trend.

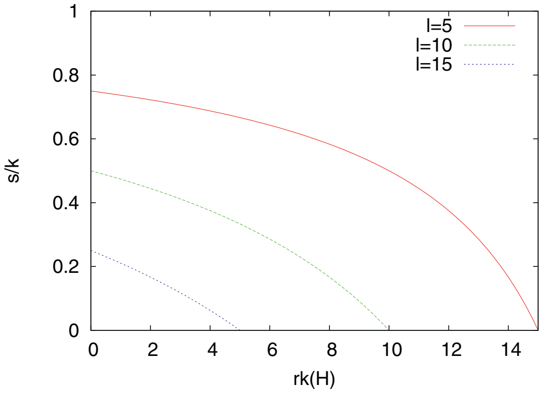

Fig. 3. Values for the uncertainty $\epsilon = s/k \in [0, 1]$ achievable by an ECC code with $n = 20$ for different values of $l = 5, 10, 15$ and for different ranks of the parity-check matrix.

4.4. Comparison with similar results in the literature

Ozarow and Wyner [3] supported their OW model describing its mathematical properties. The most important difference between their model and the GOW model is that the main channel is noiseless in the OW, while noisy in the GOW. Considering a noiseless channel allows enhancing secrecy by adding some sort of randomness to the transmitted codeword through so-called randomized coset codes, a randomized construction *based* on linear codes. To the best of our knowledge, the use of such codes over wire-tap channels has been proved secure only when the main channel is noiseless, so that the random bits added in randomized coset coding, sent in clear using a systematic encoding, are correctly received by Bob and end up increasing the entropy of the message only from Eve's point of view. Conversely, if the main channel is noisy, especially if a non-systematic code is used, the random bits become *de facto* undistinguishable from the secret message, and randomized coset coding offers unreliable error-correcting capabilities since Bob has to struggle to remove randomness from the codewords, even though to a lesser extent than Eve. For this reason, in this paper we consider only deterministic applications of linear encoders. Additionally, the main results achieved by Ozarow and Wyner aim at proving non-constructive existence theorems for showing that encoders with given security parameters must exist, while our main focus is to propose a practicable solution.

In a similar way, the more recent work of Cheng *et al.* [36] provides theoretical results for characterizing the achievable values of code rate in the OW model. In our work, instead, we focused on linear codes to obtain more specific and practical results concerning the secrecy of the less restrictive GOW model. In particular, Theorem 1 and Corollary 1 provide precise formulae to compute the uncertainty rate of the adversary, which allowed us to plot in Fig. 2 all the uncertainty rates achievable by linear codes under the assumption of specific conditions. In their work, Ozarow and Wyner also found interesting properties related to the uncertainty achieved by linear codes that have been further refined by Wei [37]. However, linear codes were not explicitly considered and there is no result similar to the uncertainty rate formula that we provided. Applications of some families of linear codes (*e.g.*, LDPC codes) to the wire-tap channel model have been considered [16,38] but, to the best of our knowledge, their application on the GOW model has not been deeply investigated.

5. A constructive solution: combining secret sharing and ECC

In Section 4, we showed that deterministic ECCs cannot offer perfect secrecy, and that the error correcting capability of a code is proportional to the information leakage it causes. Randomized encoders can represent a viable solution, but only when the main channel is noiseless, as discussed in Section 4.4. However, the negative results of deterministic encoders suggest exploring other constructions relying on the same rationale of randomized encoders, that is, obfuscating the codeword of deterministic encoders so as to leverage the different levels of noise experienced by Bob and Eve. Along this line, a possible approach to obtain perfect secrecy while allowing reliable communications is secret sharing, described in Section 2.1. More precisely, so-called *threshold* secret sharing schemes allow generating j pieces of information, called shares, from a single secret S, such that any $i \leq j$ of them are necessary and sufficient to recover S. i is the threshold that determines the amount of information needed to reconstruct S: perfect secrecy is guaranteed provided that at most $i - 1$ shares are leaked; correct reception is ensured if no more than $j - i$ shares are lost.

Notwithstanding their interesting properties, secret sharing schemes were not designed to allow communication over a noisy channel. This is particularly evident if we consider a channel model where transmissions may be subject to a combination of erasures and errors. For instance, assume that Bob receives $i + 2$ out of the j shares originated and transmitted by Alice. Bob has $\binom{i+2}{i}$ available combinations of i shares to try to reconstruct the secret message S. Even if one of the received shares is corrupted, $\binom{i+1}{i} = i + 1$ of such combinations will produce the same value for S, while the remaining ones will most likely give uniformly distributed values: Bob can correctly decode S by majority. However, if two or more shares are corrupted, only one combination will certainly produce the true secret S, making it impossible for Bob to identify such correct value. More generally, secret sharing schemes are conceived to offer protection with respect to data loss, not to data corruption. In coding theory terminology, it means that secret sharing can be used to tackle erasures, not errors. While potentially suitable for the OW channel model, the applicability of secret sharing to the GOW model is therefore severely limited.

In Section 5.1, we describe a family of encoding schemes based on combining secret sharing with ECCs. The rationale is that the underlying secret sharing scheme is used for security purposes (provided that the adversary cannot correctly eavesdrop enough data), while the outer ECC allows reliable communication in the presence of errors. Later in Section 5.2, we discuss a toy example where a (j, j) secret sharing scheme is combined with a $(l + 1)$ repetition code (a special case of a linear ECC).

5.1. Combining secret sharing and ECC

An ECC can guarantee reliable communication over a noisy channel, but it cannot provide perfect secrecy in the GOW channel model, as it has uncertainty rate $\epsilon = 1 - \frac{l}{k} < 1$ for each $l > 0$. On the opposite side of the spectrum, a (i, j) secret sharing based encoding scheme can guarantee perfect secrecy if $l < i$, but cannot provide suitable error correcting capabilities. Therefore, we propose to combine the two primitives to obtain a coding technique that concurrently achieves both requirements.

The proposed scheme, described in Algorithm 1, produces a codeword $c \in \mathbf{F}_q^n$ from a message $m \in \mathbf{F}_q$ composed of a single digit. The encoding consists of the following steps: (i) $i - 1$ coefficients are randomly picked in $\mathbf{F}_q$ [lines 1-3] and used together with m to define the polynomial $f(x) \in \mathbf{F}_q[X]$ [line 4]; (ii) $f(x)$ is used to implement a (i, j) secret sharing scheme, obtaining the j shares $d_1, \ldots, d_j \in \mathbf{F}_q$ [lines 5-7]; and, finally, (iii) the word $(d_1, \ldots, d_j) \in \mathbf{F}_q^j$ is encoded with a liner ECC E to obtain the codeword $c \in \mathbf{F}_q^n$ [line 8].

Let us assume that the codeword c is sent over a GOW channel, where the adversary Eve is able to eavesdrop l noiseless digits. Theorem 2 and Corollary 2 provide precise results concerning the security properties of the proposed scheme.

Theorem 2. *Under the GOW channel model, the proposed scheme guarantees perfect secrecy if and only if $l < i$.*

Proof. Theorem 1 establishes that the uncertainty rate of the considered model is $\epsilon = 1 - \frac{l}{j}$ or, equivalently, that the dimension of uncertainty is $s = j - l$. The number of digits of the word $(d_1, \ldots, d_j)$ that the adversary can reconstruct is upper bounded by $j - s = l$; this happens, for instance, when systematic codes are employed (see Eq. (1)). This means that the attacker cannot recover more than l shares, and the thesis follows from the properties of (i, j) secret sharing schemes. □

Given Theorem 2, the following corollary is straightforward.

Corollary 2. *Under the GOW channel model, the proposed scheme guarantees perfect secrecy and reliable communication if the adversary can access a number of noiseless digits $l < i$, while the recipient can recover a number of noiseless digits $l \geq i$.*

The condition for reliable communication expressed by Corollary 2 is only a sufficient one. More generally, according to the error correcting capabilities of the linear ECC used, whenever the corresponding decoder allows the recipient Bob

ALGORITHM 1: general procedure for transforming any ECC into a secure and data loss resilient wire-tap code.

```
input  : $m \in \mathbf{F}_q$ message to encode; $E : \mathbf{F}_q^j \to \mathbf{F}_q^n$ linear ECC
         encoder.
output : $c \in \mathbf{F}_q^n$ encoded message.
1 for $u = 1, \ldots, i - 1$ do
2     $\alpha_u = \xleftarrow{R} \mathbf{F}_q$;
3 end
4 $f(X) \in \mathbf{F}_q[X] = m + \alpha_1 X + \cdots + \alpha_{i-1} X^{i-1}$;
5 for $u = 1, \ldots, j$ do
6     $d_u = f(u) \mod \mathbf{F}_q$;
7 end
8 $c = E(d_1, \ldots, d_j)$
```

to reconstruct at least i digits of the word $(d_1, \dots, d_j)$, Bob can recover $f(X)$ by interpolation and obtain the constant term m.

Remark. Although generalizing our results to other channel models is not straightforward, the proposed solution is flexible enough to be promising for all applications in which the noise affecting the eavesdropper's channel is “worse” than the one affecting the main channel (a basic assumption of all wire-tap channel models). For instance, let us assume the case that both the main and the eavesdropper's channel are binary symmetric channels with crossover probabilities p_m (Bob's side) and p_e (Eve's side), respectively, and with $p_m < <p_e$. Intuitively, a suitable (non-systematic) ECC can be chosen so as to guarantee that reconstructing at least i digits (*i.e.*, shares) of the original message is possible with *high* probability when the crossover probability is p_m, but not when the crossover probability is p_e. Yet, a more technical analysis is beyond the scope of this paper and we leave it as a possibility for future work.

5.2. A toy example

In this section, we discuss the performance of a toy example code combining a (j, j) secret sharing scheme (*i.e.*, all j shares are necessary to recover the secret S) with a $(l+1)$ repetition code. More specifically: (i) we provide a brief description of repetition codes and compute their uncertainty rate, and (ii) we show that our toy example achieves perfect secrecy and error correcting capabilities in the considered model.

Repetition codes

Repetition codes are a special family of linear ECCs. As the name suggests, in a r repetition code each digit of the original message is simply repeated r times. That digit can be recovered by majority if at least half of the r copies are correctly received, regardless of the fact that the other copies are erased or corrupted. Formally, k message digits $(x_1, \dots, x_k) \in \mathbf{F}_q^k$ are encoded into $n = rk$ code digits $(x_1, \dots, x_1, \dots, x_k, \dots, x_k) \in \mathbf{F}_q^n$, where each digit x_i, $i = 1, \dots, k$ is replicated $r \in \mathbb{N}$ times. The code rate is $\rho = \frac{1}{r}$. Thanks to the results of Section 4, the following corollary holds.

Corollary 3. *Under the GOW channel model, if the adversary eavesdrops l digits, the uncertainty rate of a r repetition code is $\epsilon = 0$ if $l \geq k$, while it is $\epsilon = 1 - \frac{l}{k}$ otherwise, regardless of r. Equivalently, if the eavesdropping rate of the adversary is λ, the uncertainty rate is $\epsilon = 0$ if $\lambda \geq \frac{1}{r}$, while it is $\epsilon = 1 - r\lambda$ otherwise.*

Corollary 3 tells us that a repetition code guarantees positive uncertainty provided that the adversary Eve eavesdrops less than k noiseless digits. Indeed, the best-case scenario for Eve is when she eavesdrops one copy each of l distinct digits of the original message. However, the uncertainty rate is pretty low, especially if compared to the level of reliability provided by the code: to be sure to correctly recover all the original message, the intended recipient Bob needs at least $\frac{r}{2}$ copies of *all* message digits.

As a special case, consider for instance a scenario where Alice wants to transmit to Bob a single digit $x \in \mathbf{F}_q$, *i.e.*, $k = 1$. Alice applies a r repetition code to get the codeword $(x, \dots, x)$ composed of r copies of x. What Theorem 3 says is that, no matter how large r is, if Eve intercepts $l \geq 1$ digits of the codeword the uncertainty rate is $\epsilon = 0$. Indeed, all digits of the codeword coincide with x, so to intercept any one of them means to get to know x. Conversely, if $l < k$, *i.e.*, if $l = 0$, the uncertainty is clearly $\epsilon = 1$.

Analysis of the proposed toy example

To amplify the uncertainty rate provided by an r repetition code, we propose to combine it with a preliminary step consisting of a (j, j) secret sharing scheme. We will focus on the special case where Alice wants to send to Bob a single digit $m \in \mathbf{F}_q$, and prove that such a composed scheme achieves perfect secrecy for up to a suitable l, depending on the choice of r and j. The proposed toy example is described in Algorithm 2.

ALGORITHM 2: secretly shared single digit repetition code

```
input  : $m \in \mathbf{F}_q$ message to encode.
output : $c = (c_{1,1}, \dots, c_{1,r}, c_{2,1}, \dots, c_{j,r}) \in \mathbf{F}_q^{jr}$ encoded
         message.
1 for $i = 1, \dots, j-1$ do
2     $x_i \overset{R}{=\!\!\longleftarrow} \mathbf{F}_q$;
3 end
4 $x_j = m + x_1 + \dots + x_{j-1} \mod \mathbf{F}_q$;
5 for $i = 1, \dots, j$ do
6     for $t = 1, \dots, r$ do
7         $c_{i,t} = x_i$;
8     end
9 end
```

From a single message digit m, the encoder of Algorithm 2 produces a codeword of length $n = jr$ as follows: (i) $j-1$ digits $x_1, \dots, x_{j-1}$ are picked uniformly at random in $\mathbf{F}_q$ [lines 1-3]; (ii) one further digit is computed as $x_j = m + x_1 + \dots + x_{j-1} \mod \mathbf{F}_q$ [line 4]; and, finally, (iii) all j digits $x_1, \dots, x_j$ are replicated r times to produce the code digits $c_{1,1}, \dots, c_{j,r}$ [lines 5-9]. Steps (i) and (ii) implement a (j, j) secret sharing scheme.[5] Step (iii) is a simple r replication scheme, where each x_i is replicated r times.

Assume that the adversary Eve can eavesdrop l noiseless digits. Eve can recover m if and only if she gets access to all the shares $x_1, \dots, x_j$. If $l \geq j$, Eve might be able to pick l such digits so as to have at least one copy of all such digits. However, if $l < j$, there is no way for Eve to get all the digits $x_1, \dots, x_j$, and it is impossible for her to recover m. Consequently, the uncertainty is $\epsilon = 0$ if $l \geq j$, while it is $\epsilon = 1$ if $l < j$. Let us formalise the same concepts using our notion of uncertainty rate, together with the results of Section 4. If we only focus on the repetition code, it is used to encode the word $(x_1, \dots, x_j)$ of length j, so it produces an uncertainty rate $\epsilon = 1 - \frac{l}{j}$ concerning $(x_1, \dots, x_j)$. This means that Eve can recover $j(1 - \epsilon) = l$ digits of the set $(x_1, \dots, x_j)$. Once again, this yields perfect secrecy if $l < j$ thanks to the properties of secret sharing, while zero uncertainty if $l \geq j$.

For what concerns the impact of the proposed scheme on the reliability of the transmission, it is easy to realize that using only the first step of the example (*i.e.*, secret sharing) we could get even better secrecy: if Alice directly transmits the word $(x_1, \dots, x_j)$ without replication, perfect secrecy is guaranteed as long as Eve eavesdrops $l < j$ digits. This means that we can obtain the same level of secrecy for a much larger eavesdropping rate ($\frac{l}{j}$instead of $\frac{l}{jr}$). However, directly transmitting $(x_1, \dots, x_j)$ provides *no* correction capabilities to Bob in the presence of errors or erasures: if even a single digit x_i is not correctly received, it is impossible to recover m. Conversely, the toy example allows perfect reception of m, provided that at least $\frac{r}{2}$ of the r copies of each digit x_i are correctly received.

It is worth noticing that both our general scheme and our toy example can be easily extended to any message of length $k > 1$, and they still guarantee perfect secrecy whenever we know that the adversary can eavesdrop no more than $j-1$ noiseless digits *for each codeword sent*.

[5] When $i = j$, a (i, j) secret sharing scheme can be implemented as shown, without resorting to polynomial interpolation.

Towards more complex solutions

The toy example based on repetition codes discussed in this section has the unique feature of operating on single digits independently. This characteristic allowed us to illustrate a practical and easy implementation of the proposed scheme that achieves perfect secrecy (under specific assumptions) with the additional benefit of better showing that the security of the scheme is due to the secret sharing and not to the ECC. In fact, repetition codes are intuitively the less promising codes for security purposes. However, it is possible to consider more realistic application settings that suggest to employ a different ECC in our scheme. For instance, let us consider a scenario in which seven different physical links (*e.g.* seven radio frequencies) are available, and Eve's eavesdropping capabilities are limited to no more than three of them. In addition, let us assume that each of these physical links can be modelled as a binary symmetric channel with crossover probability $p < <1$. Based on the proposed construction, we can design a perfectly secure code wherein each bit is correctly received with probability $1-(1-p)^7-7p(1-p)^6$, combining a (4, 4) secret sharing scheme and the renowned Hamming (7,4) linear ECC. More precisely, for each message bit m_t Alice randomly picks three bits $d_{t,\,1}$, $d_{t,\,2}$, $d_{t,\,3}$ and sets $d_{t,4}=m_t\oplus d_{t,1}\oplus d_{t,2}\oplus d_{t,3}$, thus implementing a (4, 4) secret sharing scheme[6] on the secret m_t. Then Alice applies the Hamming code on the message $(d_{t,\,1},\ d_{t,\,2},\ d_{t,\,3},\ d_{t,\,4})$, obtaining seven bits $p_{t,\,1}$, $p_{t,\,2}$, $d_{t,\,1}$, $p_{t,\,3}$, $d_{t,\,2}$, $d_{t,\,3}$, $d_{t,\,4}$ ($p_{t,\,1}$, $p_{t,\,2}$, $p_{t,\,3}$ being parity bits), and she sends each of such bits over a different physical link. Since Eve can only eavesdrop over three channels (*i.e.*, $l=3$), she cannot recover more than three shares. Hence, she cannot recover m_t. On the other hand, Bob correctly recovers m_t as long as no more than one communication error occurs, which happen with probability $1-(1-p)^7-7p(1-p)^6$.

6. Conclusion

In this paper, we focused on the Generalized Ozarow-Wyner's wire-tap (GOW) channel model and, to the best of our knowledge, we are the first to provide constructive solutions that combine secret sharing and linear error-correcting codes to overcome the presence of transmission errors, while guaranteeing perfect security. We also introduced a security metric, called uncertainty rate, that specifies the equivocation rate in the context of linear error-correcting codes. This newly introduced metric, other than being instrumental to our proposal, also helped to state, in a simple way, theoretical results concerning the implementation of ECC encoders in the GOW channel model that were already known for the traditional wire-tap channel model—yet, requiring a complex technical machinery.

It is worth noticing that our work significantly deviates from the research trend in the area. In fact, most papers focus on the secrecy capacity, studying limiting behaviours of the model when the size of the message approaches infinity. Taking a different approach, we showed that reliable and perfectly secret communication is possible in practice, at the cost of a (slightly) lower communication rate. Moreover, we also provided a generic and constructive procedure for obtaining a secure wire-tap code from a linear encoder.

While the proposed formalization and theoretical contributions stand on their own, they have also a wealth of practical applications, for instance in contexts where the amount of transmitted data is limited, or where key management and costly cryptographic algorithms are hard to implement—such as in many distributed and unattended application settings—or, finally, where perfect secrecy is at premium.

Acknowledgements

We would like to thank the anonymous reviewers for their comments, that helped improve the quality of the manuscript.

Appendix A. Proofs of the results in Section 4

This appendix contains the proof of the results presented in Section 4. We start with few preliminary definitions and results.

Definition 3 (Row-Column Permutation)**.** A row-column permutation of a $t\times u$ matrix H is a map $\sigma:\mathcal{M}_{t\times u}\longrightarrow\mathcal{M}_{t\times u}$ defined by $(h_{ij})\mapsto(h_{\sigma_t(i)\sigma_u(j)})$ where σ_t and σ_u are permutations of the sets $\{1,\ldots,t\}$ and $\{1,\ldots,u\}$, respectively.

A row-column permutation σ of a parity-check matrix H defines a new matrix $\tilde{H}=\sigma(H)$ that shares the same size of H and whose codewords are a permutation of those defined by H. In fact, $\sigma(H)\sigma_u(c)^T=0$ is satisfied if and only if $Hc^T=0$ (note that, since c is a vector of dimension u, it can be though as a matrix $1\times u$ and, thus, $\sigma(c)$ permutes its elements accordingly to $\sigma_u(c)$).

Lemma 1. *Let H be the $(n-k)\times n$ parity-check matrix of a linear code used as an encoder in the OW wire-tap channel model, and let c be the transmitted codeword. The adversary can recover the whole codeword c if and only if there is a row-column permutation $\sigma:H\mapsto\sigma(H)=\tilde{H}$ such that $\tilde{H}=[\tilde{H}_1\ \tilde{H}_2]$ is a two blocks matrix where $\tilde{H}_1$ is an $(n-k)\times l$ sub-matrix, and $\tilde{H}_2$ an $(n-k)\times(n-l)$ sub-matrix having $\mathrm{rk}(\tilde{H}_2)=n-l$. Further, the dimension of uncertainty of the LDPC is*

$$s=\min_{\sigma}\{n-l-\mathrm{rk}(\tilde{H}_2)\}. \tag{A.1}$$

Proof. ($\Longleftarrow$) Let us assume that there is a row-column permutation $\sigma:H\mapsto\sigma(H)=\tilde{H}=[\tilde{H}_1\ \tilde{H}_2]$ such that $\tilde{H}_1$ is an $(n-k)\times l$ sub-matrix and $\tilde{H}_2$ is an $(n-k)\times(n-l)$ sub-matrix with $\mathrm{rk}(\tilde{H}_2)=n-l$. We want to show that the adversary can recover any codeword c transmitted over the channel. Let us denote with $\tilde{c}=\sigma_n(c)$ the application of this permutation to a generic codeword c, namely $\tilde{c}=[c_{\sigma_n(1)}\ \ldots\ c_{\sigma_n(l)}\ c_{\sigma_n(l+1)}\ \ldots\ c_{\sigma_n(n)}]$. To ease notation, we write $\tilde{c}=[\tilde{x}\ \tilde{y}]$ where $\tilde{x}$ represents the first l elements of $\tilde{c}$ and $\tilde{y}$ the remaining $n-l$. Accordingly to the OW model, the adversary can choose to eavesdrop the l bits composing $\tilde{x}$. Noticing that $\tilde{H}\tilde{c}^T=0$ is equivalent to

$$\tilde{H}_1\tilde{x}^T=\tilde{H}_2\tilde{y}^T \tag{A.2}$$

and that $\tilde{H}_1\tilde{x}^T$ is a vector known to the adversary, she can retrieve the missing $n-l$ components of $\tilde{y}$ by solving the system defined in Eq. (A.2). In fact, it is made of $\mathrm{rk}(\tilde{H}_2)=n-l$ independent linear equations and it has, thus, a single solution. Finally, she can retrieve the original codeword c by applying the inverse of the row column permutation, namely $c=\sigma_n^{-1}$.

($\Longrightarrow$) If the adversary can retrieve a codeword c by exploiting the linear equations defined by $Hc^T=0$ and using only l bits, then it means that she has at least $n-l$ independent linear equations to work with; namely, $\mathrm{rk}(H)\geq n-l$. Then, a row-column permutation $\sigma(H)=\tilde{H}=[\tilde{H}_1\ \tilde{H}_2]$ with $\mathrm{rk}(\tilde{H}_2)=n-l$ must exists because $\mathrm{rk}(H)\geq n-l$ implies that H has a sub-matrix M with rank $n-l$ (the elements of M can be arbitrarily moved to match $\tilde{H}_2$ using an appropriate permutation σ).

We want to show that the dimension of uncertainty is $s=\min_\sigma\{n-l-\mathrm{rk}(\tilde{H}_2)\}$. We have already observed that the recovering of a codeword is linked to the solution of the Eq. (A.2). Thus, the adversary must recover $n-l$ bits using $\mathrm{rk}(\tilde{H}_2)$ independent linear equations. Taking the minimum of this value among all

[6] The implementation of standard secret sharing schemes based on polynomial interpolation is limited over $\mathbf{F}_2$. The scheme used here is an example of a well-known alternative construction for (*j*, *j*) binary secret sharing.

the possible row-column permutations σ, we obtain the claimed equation. □

The following statement is equivalent to Lemma 1 but easier to apply and provides a proof for the results presented in Section 4.

Theorem 3. *Let H be the $(n-k) \times n$ parity-check matrix of a linear code used as an encoder in the OW wire-tap channel model and let c be the transmitted codeword. The adversary can recover the whole codeword c if and only if $\mathrm{rk}(H) \geq n-l$. If the adversary cannot recover the whole codeword, then the dimension of uncertainty is $n-l-\mathrm{rk}(H)$.*

Proof. $(\Longleftrightarrow)$ Due to Lemma 1, we only need to prove that there is a row-column permutation $\sigma : H \mapsto \sigma(H) = \tilde{H} = [\tilde{H}_1\ \tilde{H}_2]$ such that $\tilde{H}_1$ is an $(n-k) \times l$ sub-matrix and that $\tilde{H}_2$ is an $(n-k) \times (n-l)$ sub-matrix with $\mathrm{rk}(\tilde{H}_2) = n-l$ if and only if $\mathrm{rk}(H) \geq n-l$. The condition $\mathrm{rk}(H) \geq n-l$ is equivalent to say that H has a $(n-k) \times (n-l)$ sub-matrix M with rank $\mathrm{rk}(M) = n-l$ obtained by removing l columns from H. Thus, the corollary is proved by picking σ as the rows column permutation that moves the elements of M to the sub-matrix $\tilde{H}_2$. □

Theorem 3 directly proves Theorem 1, by simply recalling that, for each linear code, the rank of the parity-check matrix H is $n-k$. Corollary 1 follows immediately by recalling that the code rate is defined as $\rho = \frac{k}{n}$.

References

[1] W. Harrison, S. McLaughlin, Physical-layer security: combining error control coding and cryptography, in: Communications, 2009. ICC '09. IEEE International Conference on, 2009, pp. 1–5.
[2] A.D. Wyner, The Wire-tap Channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.
[3] L. Ozarow, A. Wyner, Wire-tap channel II, in: T. Beth, N. Cot, I. Ingemarsson (Eds.), Advances in Cryptology, Lecture Notes in Computer Science, vol. 209, Springer, Berlin Heidelberg, 1985, pp. 33–50.
[4] M. Nafea, A. Yener, Wiretap channel ii with a noisy main channel, in: Information Theory (ISIT), 2015 IEEE International Symposium on, IEEE, 2015, pp. 1159–1163.
[5] Y. Dodis, A. Sahai, A. Smith, On perfect and adaptive security in exposure-resilient cryptography., in: B. Pfitzmann (Ed.), EUROCRYPT, Lecture Notes in Computer Science, vol. 2045, Springer, 2001, pp. 301–324.
[6] M. Cheraghchi, F. Didier, A. Shokrollahi, Invertible extractors and wiretap protocols, Inf. Theor. IEEE Trans. 58 (2) (2012) 1254–1274.
[7] M. Bloch, J. Barros, Physical-Layer Security: From Information Theory to Security Engineering, Cambridge University Press, 2011.
[8] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.
[9] F. Oggier, B. Hassibi, The secrecy capacity of the mimo wiretap channel, Inf. Theor. IEEE Trans. 57 (8) (2011) 4961–4972.
[10] G. Blakley, Safeguarding cryptographic keys, in: Proceedings of the 1979 AFIPS National Computer Conference, AFIPS Press, Monval, NJ, USA, 1979, pp. 313–317.
[11] Y. Zou, J. Zhu, X. Wang, V. Leung, Improving physical-layer security in wireless communications using diversity techniques, Netw. IEEE 29 (1) (2015) 42–48.
[12] I. Csiszár, J. Körner, Broadcast channels with confidential messages., IEEE Trans. Inf. Theor. 24 (3) (1978) 339–348.
[13] S. Leung-Yan-Cheong, M. Hellman, The gaussian wire-tap channel, Inf. Theor. IEEE Trans. 24 (4) (1978) 451–456.
[14] U. Maurer, The strong secret key rate of discrete random triples, in: R.E. Blahut, J. Costello, J. Daniel, U. Maurer, T. Mittelholzer (Eds.), Communications and Cryptography, The Springer International Series in Engineering and Computer Science, vol. 276, Springer, US, 1994, pp. 271–285.
[15] U. Maurer, S. Wolf, Information-theoretic key agreement: From weak to strong secrecy for free, in: B. Preneel (Ed.), Advances in Cryptology - EUROCRYPT 2000, Lecture Notes in Computer Science, 1807, Springer, Berlin Heidelberg, 2000, pp. 351–368.
[16] W.K. Harrison, J. Almeida, M.R. Bloch, S.W. McLaughlin, J. Barros, Coding for secrecy: An overview of error-control coding techniques for physical-layer security., IEEE Signal Process. Mag. 30 (5) (2013) 41–50.
[17] H. Boche, R.F. Schaefer, H.V. Poor, On the continuity of the secrecy capacity of compound and arbitrarily varying wiretap channels, IEEE Trans. Inf. Foren. Security 10 (12) (2015) 2531–2546.
[18] M. Benammar, P. Piantanida, Secrecy capacity region of some classes of wiretap broadcast channels., IEEE Trans. Inf. Theor. 61 (10) (2015) 5564–5582.
[19] Z. Rezki, A. Khisti, M.-S. Alouini, On the secrecy capacity of the wiretap channel with imperfect main channel estimation, Commun. IEEE Trans. 62 (10) (2014) 3652–3664.
[20] T.S. Han, H. Endo, M. Sasaki, Reliability and secrecy functions of the wiretap channel under cost constraint, Inf. Theor. IEEE Trans. 60 (11) (2014) 6819–6843.
[21] A. Subramanian, A. Thangaraj, M.R. Bloch, S.W. McLaughlin, Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes., IEEE Trans. Inf. Foren. Security 6 (3-1) (2011) 585–594.
[22] H. Mahdavifar, A. Vardy, Achieving the secrecy capacity of wiretap channels using polar codes, Inf. Theor. IEEE Trans. 57 (10) (2011) 6428–6443.
[23] D. Klinc, J. Ha, S.W. McLaughlin, J. Barros, B.-J. Kwak, LDPC codes for the gaussian wiretap channel., IEEE Trans. Inf. Forens. Security 6 (3-1) (2011) 532–540.
[24] L. Liu, Y. Yan, C. Ling, Achieving secrecy capacity of the gaussian wiretap channel with polar lattices, CoRR (2015). abs/1503.02313.
[25] J. Boutros, V. Dedeoglu, M. Bloch, The Anti-Diversity Concept for Secure Communication on a Two-Link Compound Channel, ETH-Zürich, 2014.
[26] T.C. Gulcu, A. Barg, Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component, in: 2015 IEEE Information Theory Workshop, ITW 2015, Jerusalem, Israel, April 26 - May 1, 2015, 2015, pp. 1–5.
[27] R. Cramer, I.B. Damgård, N. Döttling, S. Fehr, G. Spini, Linear secret sharing schemes from error correcting codes and universal hash functions., in: E. Oswald, M. Fischlin (Eds.), EUROCRYPT (2), Lecture Notes in Computer Science, vol. 9057, Springer, 2015, pp. 313–336.
[28] S. Zou, Y. Liang, L. Lai, S. Shamai, An information theoretic approach to secret sharing, IEEE Trans. Inf. Theor. 61 (6) (2015) 3121–3136.
[29] R.L. Rivest, All-or-nothing encryption and the package transform., in: E. Biham (Ed.), FSE, Lecture Notes in Computer Science, vol. 1267, Springer, 1997, pp. 210–218.
[30] J.K. Resch, J.S. Plank, AONT-RS: blending security and performance in dispersed storage systems, in: 9th USENIX Conference on File and Storage Technologies, San Jose, CA, USA, February 15-17, 2011, 2011, pp. 191–202.
[31] M. Bellare, S. Tessaro, A. Vardy, Semantic security for the wiretap channel., in: R. Safavi-Naini, R. Canetti (Eds.), CRYPTO, Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 294–311.
[32] P. Wang, R. Safavi-Naini, A model for adversarial wiretap channels, IEEE Trans. Inf. Theor. 62 (2) (2016) 970–983.
[33] C.W. Wong, T.F. Wong, J.M. Shea, Secret-sharing LDPC codes for the bpsk–constrained gaussian wiretap channel, IEEE Trans. Inf. Foren. Security 6 (3-1) (2011) 551–564.
[34] M. Baldi, G. Ricciutelli, N. Maturo, F. Chiaraluce, Performance assessment and design of finite length LDPC codes for the gaussian wiretap channel, in: IEEE International Conference on Communication, ICC 2015, London, United Kingdom, June 8-12, 2015, Workshop Proceedings, 2015, pp. 435–440.
[35] Y. Liang, H.V. Poor, Generalized multiple access channels with confidential messages, CoRR (2006). abs/cs/0605014.
[36] F. Cheng, R.W. Yeung, K.W. Shum, Imperfect secrecy in wiretap channel ii, Inf. Theor. IEEE Trans. 61 (1) (2015) 628–636.
[37] V. Wei, Generalized hamming weights for linear codes, Inf. Theor. IEEE Trans. 37 (5) (1991) 1412–1418.
[38] A. Thangaraj, S. Dihidar, A.R. Calderbank, S.W. McLaughlin, J.-M. Merolla, Applications of LDPC codes to the wiretap channel., IEEE Trans. Inf. Theor. 53 (8) (2007) 2933–2945.

Giulio Aliberti is a third year PhD student in Mathematics at the University of Roma Tre. His main research interests include security and privacy in communication networks, models of complex networks, knowledge discovery and data mining, distributed algorithms and data compression techniques.

Prof. Dr. Roberto Di Pietro is Global Security Research Head for Nokia Bell Labs. His main research interests include security and privacy for wireless systems, cloud and virtualization security, security and privacy for distributed systems, applied cryptography, computer forensics, and analytics for role and profile mining. He is also an Associate Professor in Computer Science at University of Padova.

Dr. Stefano Guarino is a research fellow at the Institute for Applied Maths of the Italian National Research Council (IAC - CNR), within the Project IANCIS funded by the 2013 ISEC Programme of the European Commission. His main research interests comprehend coding theory, cryptography and distributed algorithms, with focus on information security and privacy, physical-layer security, ad-hoc networks, cloud storage, and automated (dark) web mining.