Information-Theoretic Security: an overview

Rui A. Costa

Relatório para a disciplina de Seminário, do Mestrado em Informática da Faculdade de Ciências da Universidade do Porto, sob a orientação do Prof. Doutor João Oliveira Barros.

I. Introduction

One of the most important problems in cryptography is the transmission of a secret message between two legitimate users (the sender Alice and the receiver Bob) over an insecure communication channel such that an enemy (Eve) with access to the channel is unable to get useful information about the message being sent.

With the goal of solving this problem (or some of its instances), cryptography has provided schemes (ciphers) that “assure security”, in some sense. In our days, almost all the ciphers used are based on the assumption that an enemy has full access to the cryptogram, i.e. the enemy receives an exact copy of the cryptogram, and the goal of these ciphers is to guarantee that there exists no efficient algorithm for breaking, for some reasonable definition of breaking. The problem is that for no existing cipher can this so called “computational security” be proved, without invoking an unproven intractability result. The security of the majority of the most used ciphers is based on the (unproven) difficulty of factoring large integers (for example, the RSA public-key crytosystem [1]) or on the unproven difficulty of computing discrete logarithms in certain groups (for example, see [2]).

On the other hand, information-theoretic (or unconditional) security gives us the strongest definition of security, but it was, in its beginning, impractical. To be more precise, [3] introduced a model of a cryptosystem (see Figure 1). In this model, Eve has perfect access to the insecure channel, i.e. she receives an exact copy of the cryptogram C, where C is obtained by Alice as a function of the plaintext M and a secret key K, shared by Alice and Bob. According to Shannon’s definition, a cipher system is *perfect* if

$$I(M;C) = 0,$$

i.e. Eve gains no knowledge about M by knowing C. Notice that in this definition of a secure cipher system, no assumption about the enemy’s computational power is made, therefore making the information-theoretic security more desirable in cryptography than computational security.

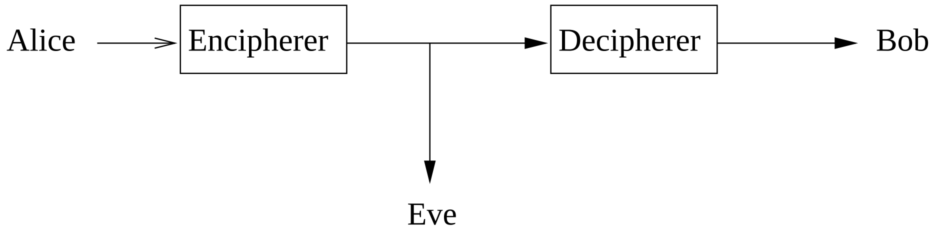

Fig. 1. Shannon’s model for a secrecy system.

Shannon also presents an example of a perfect cipher called the one-time pad, in which the cryptogram is obtained by adding modulo 2 the plaintext and a random binary secret key of the same length. Obviously, this system is impractical, because it requires a key of the same length as the plaintext. But Shannon proved an even more pessimistic result: he proved that perfect secrecy can be achieved only when the secret key is at least of the size of the plaintext, i.e.

$$H(K) \geq H(M),$$

making, under these conditions, perfect secrecy unachievable in practice.

II. The wiretap channel

One of the features in Shannon’s model that leads to his pessimistic result is the fact that he assumes that the enemy Eve has perfect access to the cryptogram C, i.e. it is assumed that the channel from Alice to Eve has the same capacity as the channel from Alice to Bob. Therefore, the key to guarantee perfect secrecy is to modify Shannon’s model such that the enemy has not the same information as the legitimate receiver. Wyner [4] and later Csiszár and Körner [5] proposed a new model, called the *wiretap channel*.

In this model, the legitimate users communicate over a main channel and an eavesdropper has access to the messages received by the legitimate receiver over a wiretap channel. The general setup for this model is shown in Figure 2.

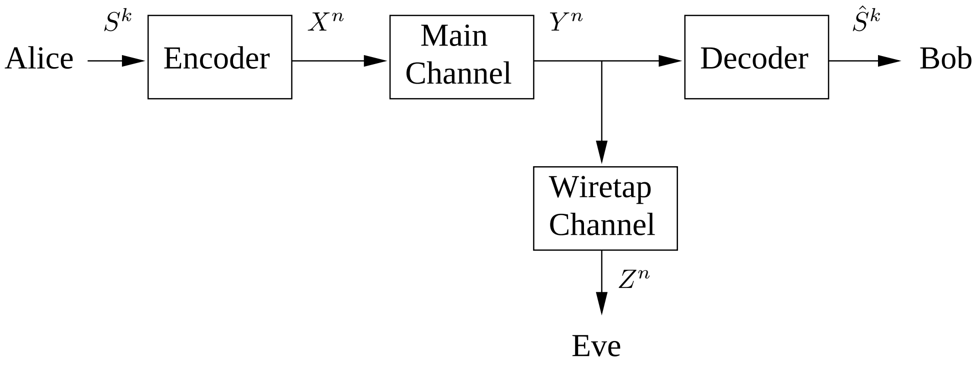

Fig. 2. The wiretap channel model.

In this section, we will study Wyner's wiretap model. First, to be able to describe properly Wyner's main results [4], we need a rigorous definition for the model presented in Figure 2.

Definition 1: The Wyner's wiretap model is defined by the following:

- the *source* is the sequence $\{S_i\}_{i=1}^{\infty}$, where S_i are i.i.d. random variables that take values in the finite set $\mathcal{S}$. Let $H(S_i) = H_S$;
- the *main channel* is a discrete memoryless channel (DMC) with finite input alphabet $\mathcal{X}$, finite output alphabet $\mathcal{Y}$ and transition probability $Q_M(y|x), x \in \mathcal{X}, y \in \mathcal{Y}$. For n vectors,
$$Q_M^{(n)}(y|x) = \prod_{i=1}^{n} Q_M(y_i|x_i).$$
Let C_M denote the main channel capacity;
- the *wiretap channel* is a DMC with input alphabet $\mathcal{Y}$, finite output alphabet $\mathcal{Z}$ and transition probability $Q_W(z|y)$, $y \in \mathcal{Y}$, $z \in \mathcal{Z}$. For n vectors, $Q_W^{(n)}(z|y) = \prod_{i=1}^{n} Q_W(z_i|y_i)$. Let C_W denote the main channel capacity;
- the channel between Alice and Eve is also a DMC, with transition probability
$$Q_{MW}(z|x) = \sum_{y \in \mathcal{Y}} Q_M(y|x) Q_W(z|y).$$
The capacity of the channel Q_{MW} is denoted by C_{MW};
- the *encoder*, with parameters (k, n), is a (possibly probabilistic) function $e : \mathcal{S}^k \rightarrow \mathcal{X}^n$ and the *decoder* is a function $d : \mathcal{Y}^n \rightarrow \mathcal{S}^k$.

Next, we define a quantity to measure the ability of Bob to read properly the confidential messages sent by Alice (through the main channel).

Definition 2: For $\hat{S} = (\hat{S}_1, ..., \hat{S}_k) = d(Y)$, the *error-rate* is defined by $P_e = \frac{1}{k}\sum_{i=1}^{k} \mathcal{P}\left(S_i \neq \hat{S}_i\right)$.

Now, we define the quantity that will be used to characterize the confidentiality of the messages sent through the main channel, with respect to Eve.

Definition 3: Let Y^n and Z^n be the output of the channels $Q_M^{(n)}$ and $Q_{MW}^{(n)}$, respectively, when the input is X^n. The *equivocation* of the source (the confidential messages to be sent) at the output of the wiretap channel (what Eve receives) is defined by:
$$\Delta = \frac{1}{k} H\left(S^k | Z^n\right).$$
We will refer to the encoder-decoder described in *Definition 1* as a (k, n, Δ, P_e) encoder-decoder.

Ideally, we want for the channel to have a small error-rate, while keeping Eve's equivocation high. Thus, the first question that arises is the following: is it possible to communicate over the main channel at a transmission rate R with small error-rate, while keeping Eve with no significant information about the confidential messages sent through the main channel? To answer this question, Wyner characterizes the region of all (R, d) achievable pairs:

Definition 4: For $R > 0$ and $d > 0$,[1] we say that the pair (R, d) is *achievable* if, for every $\epsilon > 0$, there exists an (n, k, Δ, P_e) encoder-decoder such that:

- $k \cdot H_S/n \geq R - \epsilon$;
- $\Delta \geq d - \epsilon$;
- $P_e \leq \epsilon$.

Let $\mathcal{R}$ denote the set of all (R, d) achievable pairs.

In order to characterize the set $\mathcal{R}$, we need to study first the following quantity.

Definition 5: Let $p_X(x),\ x \in \mathcal{X}$, be a probability mass function and let $\mathcal{P}(R)$ denote the set of all distributions p_X such that $I(X;Y) \geq R$.[2] For $0 \leq R \leq C_M$, let

$$\Gamma(R) = \sup_{p_X \in \mathcal{P}(R)} I(X;Y|Z).$$

Because, for any distribution p_X on $\mathcal{X}$, the corresponding X, Y and Z form a Markov chain, we have that

$$\Gamma(R) = \sup_{p_X \in \mathcal{P}(R)} \left[I(X;Y) - I(X;Z) \right].$$

Lemma 1: For $0 \leq R \leq C_M$, $\Gamma(R)$ satisfies the following:

- for each R, there exists $p_X \in \mathcal{P}(R)$ such that $I(X;Y|Z) = \Gamma(R)$;
- $\Gamma(R)$ is a concave function of R;
- $\Gamma(R)$ is nonincreasing in R;
- $\Gamma(R)$ is continuous in R;
- $C_M - C_{MW} \leq \Gamma(R) \leq C_M$

Now, we are able to state Wyner's main result on the set of all achievable pairs.

Theorem 1: The set of all achievable pairs is given by

$$\mathcal{R} = \left\{ (R, d) : 0 \leq R \leq C_M, 0 \leq d \leq H_S, \frac{d}{H_S} \leq \frac{\Gamma(R)}{R} \right\}.$$

In Figure 3, it is presented a sketch of the region $\mathcal{R}$ of the (R, d) achievable pairs. The points in this region for which $d = H_S$ are of special interest, because these correspond to the maximum equivocation possible for Eve, i.e. perfect secrecy. Thus, a quantity of interest is the maximum rate for which (R, H_S) is achievable.

Definition 6: The *secrecy capacity* of the channel pair (Q_M, Q_W) is defined by

$$C_S = \max_{(R, H_S) \in \mathcal{R}} R.$$

The following theorem proves that the secrecy capacity is well defined, gives a way to compute the secrecy capacity and also provides bounds on it.

Theorem 2: If $C_M > C_{MW}$, there exists a unique solution C_S of

$$C_S = \Gamma(C_S).$$

Further, C_S is the maximum R such that $(R, H_S) \in \mathcal{R}$ and verifies

$$0 < C_M - C_{MW} \leq \Gamma(C_M) \leq C_S \leq C_M.$$

Notice that, in the previous result, it is required that $C_M > C_{MW}$ to have strictly positive secrecy capacity. This means that, in order to be able to communicate with perfect secrecy, Alice and Bob must have a better channel than Alice.

[1] Do not confuse parameter d in the definition, which is the amount of Eve's equivocation, with the decoder $d()$.

[2] Notice that, for $R > C_M$, $\mathcal{P}(R) = \emptyset$.

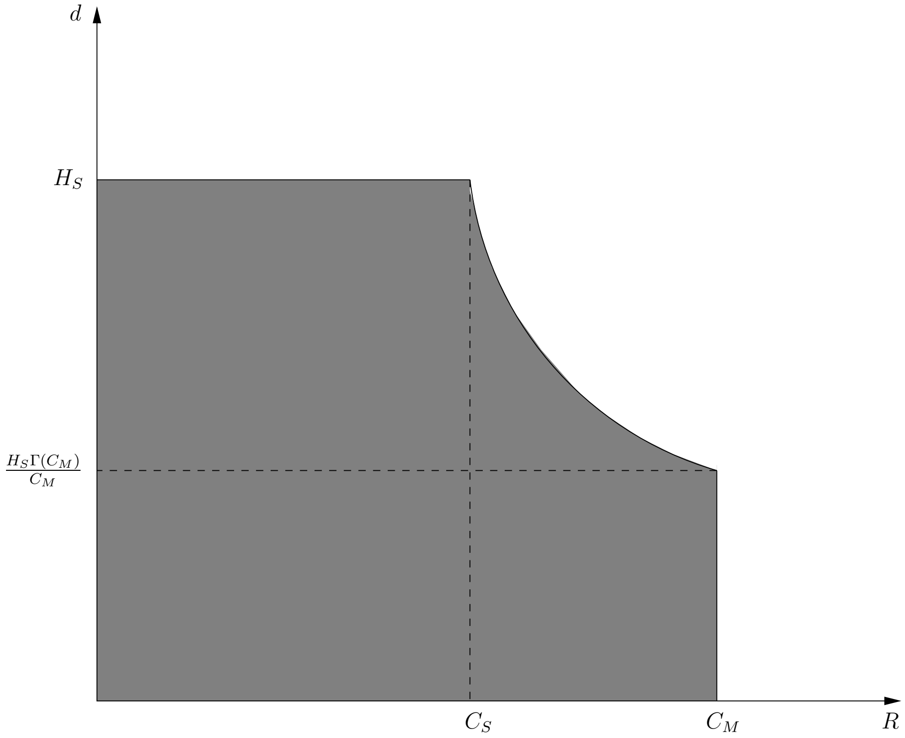

Fig. 3. Region of (R, d) achievable pairs.

III. Using public discussion to achieve a perfect secret key

Due to the fact that the results in the previous section demand that Alice and Bob have significant advantage over the eavesdropper, and also to the development of the RSA public-key crytosystem [1], Wyner's work [4] had a limited impact. More recently, Maurer [6] made a breakthrough, by developing a new model and proving that, for this model, a strictly positive secrecy capacity is possible, even if Eve's channel is stronger than the legitimate users' channel. The main feature about Maurer's model is that a public insecure channel (yet authenticated) is used to generate a secret key.

First, we start by defining the model without the public channel, and stating Maurer's definition for secrecy capacity. An illustration of this model can be seen in Figure 4.

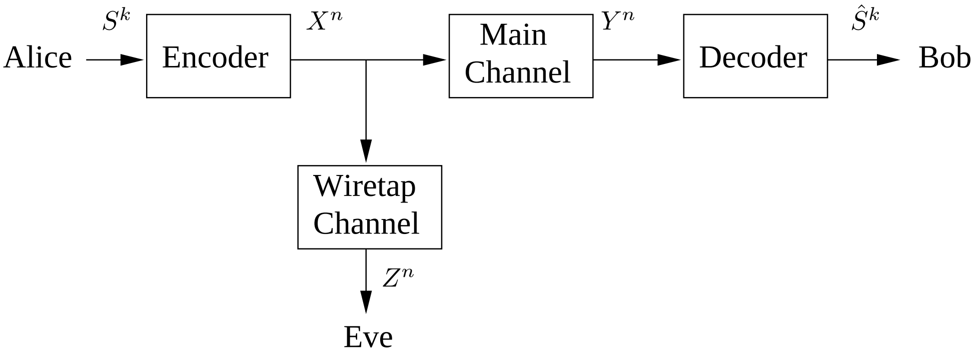

Fig. 4. Maurer's broadcast channel without a public channel.

Definition 7: The broadcast channel of interest in the following is defined as:

- the *source* is the sequence $\{S_i\}_{i=1}^{\infty}$, where S_i is a binary random variable, $\forall i$;
- the *main channel* has a finite input alphabet $\mathcal{X}$ and a finite output alphabet $\mathcal{Y}$;
- the *wiretap channel* has the same input as the main channel, and a finite output alphabet $\mathcal{Z}$;

- the channel behavior is completely specified by the conditional probability distribution $\mathcal{P}(Y = y, Z = z|X = x)$, which we refer to as $P_{YZ|X}$;
- the *encoder* is a (possibly probabilistic) function $e : \{0, 1\}^k \to \mathcal{X}^n$, where R is the rate and $k = \lfloor nR \rfloor$; the *decoder* is a function $d : \mathcal{Y}^n \to \{0, 1\}^k$.

Definition 8: The *secrecy capacity* of a broadcast channel specified by $P_{YZ|X}$ is the maximum rate R for which, for every $\epsilon > 0$, for all sufficiently large n, there exists an encoder-decoder such that for S uniformly distributed over $\{0, 1\}^k$ the following two conditions are satisfied:

- $\mathcal{P}(d(Y) \neq S) < \epsilon$, where $X = e(S)$;
- $\frac{1}{k}H(S|Z^n) > 1 - \epsilon$.

Maurer also noticed that, in the previous definition, it would be equivalent the two conditions to hold for all probability distributions.

Now, consider a broadcast channel for which both the main and the wiretap channel are independent binary symmetric channels, i.e.

$$P_{YZ|X} = P_{Y|X}P_{Z|X},$$

$$P_{Y|X}(y|x) = \begin{cases} 1 - \epsilon & \text{if } x = y \\ \epsilon & \text{if } x \neq y \end{cases}$$

and

$$P_{Z|X}(z|x) = \begin{cases} 1 - \delta & \text{if } x = z \\ \delta & \text{if } x \neq z \end{cases}$$

Without loss of generality, consider the case $\epsilon \leq 1/2$, $\delta \leq 1/2$. Denote this channel by $D(\epsilon, \delta)$. The next result characterizes the secrecy capacity for this channel. It shows that, as expected, the secrecy capacity for this channel is only strictly positive if the legitimate users' channel is better than Eve's channel.

Lemma 2: The secrecy capacity of the binary broadcast channel $D(\epsilon, \delta)$ is given by:

$$C_S(D(\epsilon, \delta)) = \begin{cases} h(\delta) - h(\epsilon) & \text{if } \delta > \epsilon \\ 0 & \text{otherwise} \end{cases},$$

where $h(p)$ is the binary entropy function, i.e. $h(p) = -p\log(p) - (1 - p)\log(1 - p)$.

To overcome the need of an advantage of the legitimate users over the eavesdropper, Maurer introduced a public channel, insecure but with unconditional secure authentication[3]. Moreover, it is assumed that Eve can listen to the communication over the public channel, but cannot perform an identity spoofing attack. For an illustration of this model, see Figure 5.

Definition 9: The *secrecy capacity with public discussion*, denoted $\hat{C}(P_{YZ|Z})$, is the secrecy capacity of the broadcast channel defined in *Definition 7* with the additional feature that Alice and Bob can communicate over an insecure (yet authenticated) public channel.

The next theorem characterizes the secrecy capacity with public discussion, showing that, even if the eavesdropper has a better channel than the legitimate users, perfect secure communication can still be performed.

Theorem 3: The secrecy capacity with public discussion of a broadcast channel is given by

$$\hat{C}(D(\epsilon, \delta)) = h(\epsilon + \delta - 2\epsilon\delta) - h(\epsilon).$$

Moreover, $\hat{C}(D(\epsilon, \delta))$ is stricly positive unless $\epsilon = 0.5$, $\delta = 0$ or $\delta = 1$, i.e. unless X and Y are statistically independent or Z uniquely determines X.

Although the goal of this work is not to provide rigorous proofs for the results presented, but to present an overview of the main results on Information Theoretic Security, it is worthwile to study a sketch of proof for *Theorem 3*. The idea is to construct a conceptual broadcast channel similar to the broadcast channel of Wyner [4], such that the conceptual main channel is equivalent to the real main channel between

[3] In order to guarantee unconditional secure authentication, one can use, for example, the scheme of [7], which is based on universal hashing and only requires that a short key is shared initially by the legitimate users.

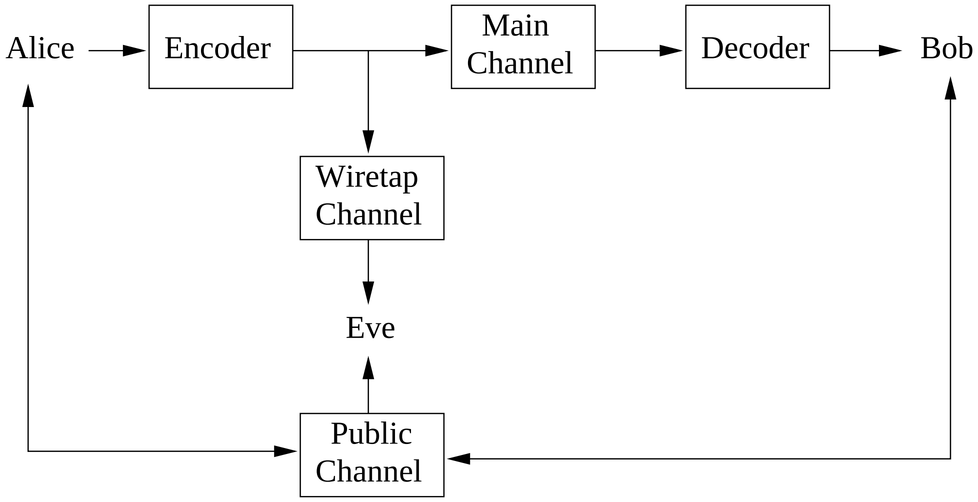

Fig. 5. Maurer's broadcast channel with a public channel.

Alice and Bob, and the conceptual wiretap channel is a cascade of the real main channel and the real wiretap channel.

Alice sends a random bit X over the real broadcast channel, with $\mathcal{P}(X=0)=\mathcal{P}(X=1)=1/2$. Let E and D denote the (independent) error bits of the main and of Eve's channel, respectively, i.e. let $Y=X+E$ and $Z=X+D$ where $\mathcal{P}(E=1)=\epsilon$ and $\mathcal{P}(D=1)=\delta$. Bob chooses a bit V and sends $W=Y+V$ over the public channel. Alice computes

$$W+X=V+E,$$

thus Alice receives V with error probability ϵ. Eve knows $Z=X+D$ and $W=X+E+V$, and can compute

$$Z+W=V+E+D.$$

In fact, it is easy to prove that

$$H(V|ZW)=H(V|Z+W),$$

thus Eve can indeed compute $Z+W$ and discard Z and W. Now, it is easy to prove that the conceptual broadcast channel can be seen as $D(\epsilon,\epsilon+\delta-2\epsilon\delta)$.

Next, Maurer studies the use of this broadcast channel with a public channel to develop unconditional secure secret key agreement protocols. Consider the following general key agreement problem. Alice, Bob and Eve know random variables X,Y and Z, respectively, with joint probability distribution P_{XYZ}. Assume that Eve has no information about X and Y other than through her knowledge of Z, i.e. if T represents all the information that Eve has, then $I(XY;T|Z)=0$. Alice and Bob share no secret key initially (other than a short key required for authentication in the public channel), but they are assumed to know P_{XYZ}, or at least an upper bound on the quality of Eve's channel. Assume also that Eve knows the protocol and the codes used.

Without loss of generality, consider only protocols in which Alice sends messages at odd steps ($C_1, C_3, \dots$) and Bob sends messages at even steps ($C_2, C_4, \dots$). At the end of the t-step protocol, Alice computes a key S as a function of X and $C^t=[C_1,\dots,C_t]$, and Bob computes a key S' as a function of Y and C^t.

Definition 10: A secret key agreement protocol as described above is (ϵ,δ)-*secure* if, for some specified (small) ϵ and δ, the following conditions hold:

1) For odd i, $H(C_i|C^{i-1}X)=0$;
2) For even i, $H(C_i|C^{i-1}Y)=0$;
3) $H(S|C^tX)=0$;
4) $H(S'|C^tY)=0$;

5) $\mathcal{P}(S \neq S') \leq \epsilon$;

6) $I(S; C^t Z) \leq \delta$.

Conditions 1-4 guarantee that Alice and Bob have no uncertainty regarding the protocol procedures. Condition 5 guarantees that Alice and Bob agree on the same key with probability $1-\epsilon$. Finally, condition 6 guarantees that, given that Eve knows all the messages exchanged between Alice and Bob over the public channel during the protocol and also the output of her channel, the information on the key that Eve has is upperbounded by δ.

The next theorem provides an upper bound on the size of the key that Alice and Bob agree via a (ϵ, δ)-secure key agreement protocol.

Theorem 4: For every (ϵ, δ)-secure key agreement protocol, we have that

$$H(S) \leq \min\left[I(X;Y), I(X;Y|Z)\right] + \delta + h(\epsilon) + \epsilon \log(|S|-1).$$

To be able to provide a lower bound on the key size, we need to make further assumptions. Consider the case when Alice, Bob and Eve receive $X^N = [X_1, ..., X_N]$, $Y^N = [Y_1, ..., Y_N]$ and $Z^N = [Z_1, ..., Z_N]$, where $P_{X^N Y^N Z^N} = \prod_{i=1}^{n} P_{X_i Y_i Z_i}$. Next, we define the secret key rate, a quantity of interest in the rest of this section.

Definition 11: The *secret key rate* of X and Y with respect to Z, denoted $S(X;Y||Z)$, is the maximum rate R such that, for every $\epsilon > 0$, there exists a protocol, for sufficiently large n, satisfying conditions 1-5 in *Definition 10* (with X and Y replaced by X^n and Y^n, respectively) and also the two following conditions:

- $\frac{1}{n} I(S; C^t Z^n) \leq \epsilon$;
- $\frac{1}{n} H(S) \geq R - \epsilon$.

The next result provides an upper and a lower bound for the secret key rate.

Theorem 5: The secret key rate $S(X;Y||Z)$ verifies

- $S(X;Y||Z) \leq \min\left[I(X;Y), I(X;Y|Z)\right]$;
- $S(X;Y||Z) \geq \max\left[I(Y;X) - I(Z;X), I(X;Y) - I(Z;Y)\right]$.

The upper bound for the secret key rate in the previous theorem shows that if Eve has less information about Y than Alice or less information about X than Bob, then such a difference of information can be exploited.

The next theorem provides bounds on the secrecy capacity with public discussion of a general broadcast channel.

Theorem 6: The secrecy capacity with public discussion, $\hat{C}_S(P_{YZ|X})$, of a broadcast channel specified by $P_{YZ|X}$ verifies:

$$\max_{P_X} S(X;Y||Z) \leq \hat{C}_S(P_{YZ|X}) \leq \min\left[\max_{P_X} I(X;Y), \max_{P_X} I(X;Y|Z)\right].$$

IV. Wireless Information-Theoretic Security

More recently, Barros and Rodrigues [8] studied information-theoretic security in a wireless environment. The authors provide a characterization of the maximum rate at which the eavesdropper cannot decode any information. They prove that, even if the eavesdropper has a better channel than the legitimate users, information-theoretic security is achievable. Thus, and quoting, “fading turns out to be a friend and not a foe”. In [9], Barros *et al* present a complete set of results (which we will describe in the rest of this report) for this model and in [10] the authors develop practical secret key agreement protocols, that exploit the presence of fading in order to ensure information-theoretic security.

The model of interest in this section is illustrated in Figure 6. Before stating the main results related to the model, we need to provide a rigorous definition of the wireless broadcast channel.

Definition 12: The wireless broadcast channel, illustrated in Figure 6, is define by the following.

- the *source* is a sequence $\{S_i\}_{i=1}^{\infty}$;

- the *main channel* is a discrete-time Rayleigh fading channel, with input alphabet $\mathcal{X}^n$ and output alphabet $\mathcal{Y}_M^n$, i.e.
$$y_M(i) = h_M(i)x(i) + n_M(i),$$
where $h_M(i)$ represents the main channel fading coefficient and is a circularly symmetric complex Gaussian random variable with zero-mean and unit variance, and $n_M(i)$ represents the noise in the main channel and is a circularly symmetric complex Gaussian random variable with zero-mean;
- the *wiretap channel* is also a discrete-time Rayleigh fading channel, with input alphabet $\mathcal{X}^n$ and output alphabet $\mathcal{Y}_W^n$, described by
$$y_W(i) = h_W(i)x(i) + n_W(i),$$
where $h_W(i)$ and $n_W(i)$ are defined similarly to $h_M(i)$ and $n_M(i)$, respectively, but now for the wiretap channel;
- it is assumed that the channels' inputs, the channels' fading coefficients and the channels' noises are all independent;
- it is also assumed that both the main and the wiretap channel are *quasi-static* fading channels, i.e. the fading coefficients, although random, are constant during the transmission of an entire codeword ($h_M(i) = h_M$ and $h_W(i) = h_W$, $\forall i = 1, \ldots, n$) and independent from codeword to codeword;
- Alice's *encoder*, with parameters (k, n), is a (possibly probabilistic) function $e : \mathcal{S}^k \to \mathcal{X}^n$, Bob's and Eve's *decoders* are mappings $d_B : \mathcal{Y}_M^n \to \mathcal{S}^k$ and $d_E : \mathcal{Y}_W^n \to \mathcal{S}^k$, respectively. Let $\hat{S}_B^k = d_B(Y_M^n)$ and $\hat{S}_W^k = d_B(Y_W^n)$.

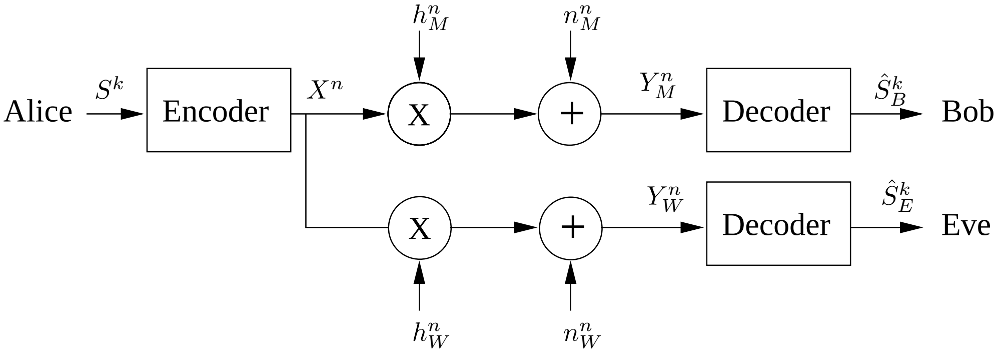

Fig. 6. Wireless broadcast channel. h_M and h_W represent the fading coefficients of the main channel and the wiretap channel, respectively, and n_M and n_W represent the noise of the main channel and the wiretap channel, respectively.

Let P be the average transmit power, i.e.
$$\frac{1}{n}\sum_{i=1}^{n} E[|X(i)|^2] \leq P,$$
and the average noise power in the main and in the wiretap channels to be N_M and N_W, respectively. Thus, the instantaneous *signal-to-noise ratio* (SNR) at Bob's receiver is
$$\gamma_M(i) = \frac{P \cdot |h_M(i)|^2}{N_M} = \frac{P \cdot |h_M|^2}{N_M} = \gamma_M,$$
and its average value $\overline{\gamma}_M = \frac{P \cdot E[|h_M|^2]}{N_M}$.

Analogously, the instantaneous SNR at Eve's receiver is
$$\gamma_W, = \frac{P|h_W|^2}{N_W},$$

and its average value $\overline{\gamma}_W = \frac{P \cdot E[|h_W|^2]}{N_W}$.

After defining the model of interest in this section, we now define important quantities that describe the quality of the channel.

Definition 13: For the channel described in *Definition 12*,

- the *transmission rate* between Alice and Bob is $R = \frac{1}{n} H(S^k)$;
- the *equivocation rate* is defined as $\Delta = \frac{H(S^k | Y_W^n)}{H(S^k)}$;
- the *error probability* is $P_e = \mathcal{P}(S^k \neq \hat{S}_B^k)$.

Next, we define the notion of an achievable rate-equivocation pair, and the rate-equivocation region.

Definition 14: A pair (R', d') is *achievable* if, for every $\epsilon > 0$, there exists an encoder-decoder such that $R \geq R' - \epsilon$, $\Delta \geq d' - \epsilon$ and $P_e \leq \epsilon$. The *rate-equivocation region* is the set of all (R', d') achievable pairs

Using the notion of achievability of a rate-equivocation pair, we define the secrecy capacity of the channel defined in *Definition 12*, which is the maximum transmission rate such that Eve's equivocation is the maximum possible.

Definition 15: The *secrecy capacity*, C_S, is the maximum rate R such that the pair $(R, 1)$ is achievable, i.e.

$$C_S = \max\{R : (R, 1)) \text{ is achievable}\}.$$

In the rest of this section, it is assumed that

- Alice and Bob have perfect knowledge of the main channel fading coefficient;
- Eve has perfect knowledge of the wiretap channel fading coefficient.

We will consider different channel state information (CSI) regimes for Alice's knowledge of the eavesdropper channel.

A. No CSI on the eavesdropper's channel

Now, we consider the case where Alice has no knowledge of the wiretap fading coefficient. The next result computes the value of the instantaneous secrecy capacity in terms of the SNR of both the main channel (γ_M) and the wiretap channel (γ_W).

Lemma 3: The secrecy capacity for one realization of the quasi-static complex fading wiretap channel is given by

$$C_S = \begin{cases} \log(1 + \gamma_M) - \log(1 + \gamma_W) & \text{if } \gamma_M > \gamma_W \\ 0 & \text{if } \gamma_M \leq \gamma_W \end{cases}$$

Next, we compute the probability of having a strictly positive secrecy capacity.

Lemma 4: For average SNR $\overline{\gamma}_M$ and $\overline{\gamma}_W$ of the main channel and the wiretap channel, respectively, we have that

$$\mathcal{P}(C_S > 0) = \frac{\overline{\gamma}_M}{\overline{\gamma}_M + \overline{\gamma}_W}.$$

Using the previous lemma, we can directly compute the probability of having strictly positive secrecy capacity as a function of the distances between Alice and Bob and between Alice and Eve.

Corollary 1: For distance d_M between Alice and Bob, distance d_W between Alice and Eve, and pathloss exponent α, we have that

$$\mathcal{P}(C_S > 0) = \frac{1}{1 + (d_M/d_W)^\alpha}.$$

The previous two results show that when $\overline{\gamma}_M >> \overline{\gamma}_W$ (or $d_M << d_W$) then $\mathcal{P}(C_S > 0) \approx 1$, and when $\overline{\gamma}_M << \overline{\gamma}_W$ (or $d_M >> d_W$) then $\mathcal{P}(C_S > 0) \approx 0$. It also shows that to ensure that the secrecy capacity is strictly positive with probability greater than p_0, then it is necessary to impose

$$\frac{\overline{\gamma}_M}{\overline{\gamma}_W} > \frac{p_0}{1 - p_0},$$

or, equivalently,

$$\frac{d_M}{d_W} < \sqrt[\alpha]{\frac{1-p_0}{p_0}}.$$

In particular, a strictly positive secrecy capacity exists even when $\overline{\gamma}_M < \overline{\gamma}_W$ (or $d_M > d_W$), although with probability less than $1/2$.

Definition 16: The *outage probability*, $\mathcal{P}_{\text{out}}(R_S)$, is the probability that the instantaneous secrecy capacity is less than a target secrecy rate R_S, i.e.

$$\mathcal{P}_{\text{out}}(R_S) = \mathcal{P}(C_S < R_S).$$

The significance of the outage probability is that, when setting the secrecy rate R_S, Alice is assuming that the capacity of the wiretap channel is given by $C'_W = C_M - R_S$. Thus, if $C_S \geq R_S$, Alice estimate of Eve's channel is better than the real wiretap channel, i.e. $C'_M > C_M$, thus perfect secrecy is ensured. On the other hand, if $C_S < R_S$, $C'_M < C_M$ thus Alice and Bob lose information-theoretic security.

Theorem 7: The outage probability of the quasi-static complex fading wiretap channel is given by

$$\mathcal{P}_{\text{out}}(R_S) = 1 - \frac{\overline{\gamma}_M}{\overline{\gamma}_M + 2^{R_S}\overline{\gamma}_W} \exp\left(-\frac{2^{R_S}-1}{\overline{\gamma}_M}\right).$$

From the previous result, we can see that when $R_S \to 0$, $\mathcal{P}_{\text{out}}(R_S) \to \frac{\overline{\gamma}_M}{\overline{\gamma}_M + \overline{\gamma}_W}$, and when $R_S \to \infty$, $\mathcal{P}_{\text{out}}(R_S) \to 1$. It can also be seen that when $\overline{\gamma}_M >> \overline{\gamma}_W$, $\mathcal{P}_{\text{out}}(R_S) \approx 1 - \exp\left(-\frac{2^{R_S}-1}{\overline{\gamma}_M}\right)$, thus for high SNR regime, $\mathcal{P}_{\text{out}}(R_S) \approx \frac{2^{R_S}-1}{\overline{\gamma}_M}$, i.e. it decays proporcional to $1/\overline{\gamma}_M$. On the other hand, if $\overline{\gamma}_M << \overline{\gamma}_W$, $\mathcal{P}_{\text{out}}(R_S) \approx 1$.

B. Imperfect CSI on the eavesdropper's channel

Now, assume that Alice has imperfect information of the wiretap channel fading coefficient. The next definition gives a precise notion on this assumption.

Definition 17: Alice's estimate of Eve's channel is $\hat{h}_W = h_W + \delta_W$, where $\hat{h}_W$ is the estimate fading coefficient of the wiretap channel and δ_W is a circularly symmetric complex Gaussian random variable with mean zero and variance σ^2 per dimension.

Next, we define Alice's estimate of secrecy capacity.

Definition 18: Alice's instantaneous secrecy capacity estimate, $\hat{C}_S$ is

$$\hat{C}_S = \begin{cases} \hat{C}_M - \hat{C}_W & \text{if } \hat{C}_M > \hat{C}_W \\ 0 & \text{if } \hat{C}_M \leq \hat{C}_W \end{cases}$$

where $\hat{C}_M = \log(1+\overline{\gamma}_M)$ is the instantaneous main channel capacity estimate, and $\hat{C}_W = \log(1+\overline{\gamma}_W)$ is the instantaneous wiretap channel capacity estimate.

The next result presents an upper bound on the probability that Alice's estimate of secrecy capacity is greater than the real secrecy capacity.

Theorem 8: The probability of a secrecy outage, $\mathcal{P}_{\text{out}} = \mathcal{P}(\hat{C}_W < C_M, \hat{C}_W < C_W)$, is upper bounded by

$$\mathcal{P}_{\text{out}} \leq \frac{1}{2} - \frac{1}{2}\frac{1}{\sqrt{1+2/\sigma^2}}.$$

From the previous result, we see that when $\sigma^2 \to \infty$ (i.e. the error in Alice's estimate of the eavesdropper channel goes to infinity), $\mathcal{P}_{\text{out}} \to 0$. But in this case, Alice will always estimate the secrecy capacity by 0.

V. Conclusions

The computational model for security is based on unproven intractability results, thus it is not possible to state unconditional security results for the most chiphers used in our days. Although this unproven security problem is present in almost all used ciphers, there are so far no known efficient attacks for the majority of the ciphers, so they are applicable to a vast set of problems. Another advantage of the classical cryptography is the fact that no assumption about the plaintext to be encoded, and also the technology is inexpensive and widely deployed. But classical cryptography present some more disadvantages besides the unproven intractability assumptions. For example, the security of a cryptografic protocol is measured by whether it survives to a set of attacks or not. Moreover, for wireless networks, state-of-art key distribution schemes require a trusted third party, as well as complex protocols.

Information-theoretic provides a proper definition of security, because nothing is assumed on the computational capacity of the eavesdropper. It also allows for precise security results to be stated. In this report, we presented an overview on Information-Theoretic Security, stating some of the most famous results related to this subject and, in Section IV, a state-of-art set results on wireless fading channels information-theoretic security. It turns out that "fading is a friend, not a foe": even when the eavesdropper has a better channel than the legitimate users, it is possible to have strictly positive secrecy capacity.

One possible future direction is to develop practical codes that, in fact, achieve the secrecy capacity, and to design new models for different security problems.

References

[1] R. L. Rivest, A. Shamir, and L. M. Adelman, "A method for obtaining digital signatures and public-key cryptosystems," Tech. Rep. MIT/LCS/TM-82, 1977.

[2] Whitfield Diffie and Martin E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

[3] Claude E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[5] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[6] Ueli M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, pp. 733–742, 1993.

[7] Mark N. Wegman and J. Lawrence Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences*, vol. 22, pp. 265–279, 1981.

[8] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. of the IEEE International Symposium on Information Theory*, Seattle, USA, July 2006.

[9] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security - part i: Theoretical aspects," *Submitted to the IEEE Transactions on Information Theory, Special Issue on Information-Theoretic Security*, November 2006, arXiv:cs/0611120.

[10] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security - part ii: Practical implementation," *Submitted to the IEEE Transactions on Information Theory, Special Issue on Information-Theoretic Security*, November 2006, arXiv:cs/0611121.