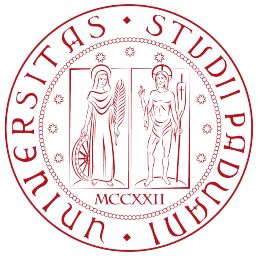

Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea in
Ingegneria Informatica

On secret-key agreement as source coding with side information

Relatore
Prof. Stefano Tomasin

Laureando:
Giovanni Artico
2000178

Anno Accademico 2022/2023

Abstract

The key reconciliation stage in the secret key generation process may leak partial information to the eavesdropper through the public channel. In this thesis, two metrics, based on rate-distortion and entropy are considered to gauge the secrecy achievable with a channel scheme with side information at the receivers. Two theorems that provide bounds on the performance in this scenario according to different metrics are considered, and the resulting performance in terms of secret key rate is assessed.

Contents

Chapter 1

Secret Key Generation

1.1 Secret Key Generation Process

The generation of a secret key from a random source as described in [3] and [4] is divided in various stages as shown in figure 1.1 from [5]. This process must be repeated periodically, as the number of generated secrecy bits of a key is limited, therefore a new one must be created. This pushes for higher key generation rate, which is related to the b bits sent between Alice and Bob to generate a key of length B. The process Includes the steps of channel probing, advantage distillation and information reconciliation.

1.1.1 Channel Probing

Alice and Bob have to determine one or more parameters of the received signal used to generate the keys. The parameter must be chosen so that it is random and enough time correlated. The latter condition is because Alice and Bob are operating in half-duplex, therefore they will probe the same channel with delay Δt between the two.

We assume, without loss of generality, that the communication is started by Alice, who sends Bob the ith signal at time $t_{i,A}$. The latter will evaluate the chosen parameters, after which Bob repeats the same process, sending a signal at time $t_{i,B}$ until all the needed samples are measured.

The channel feature chosen is usually Received Signal Strength (RSS), as it provides enough randomness and its measurement is featured in most telecommunication devices. Even if Alice and Bob send signal with period Δt small enough, there is still going to be a difference between the two signals.

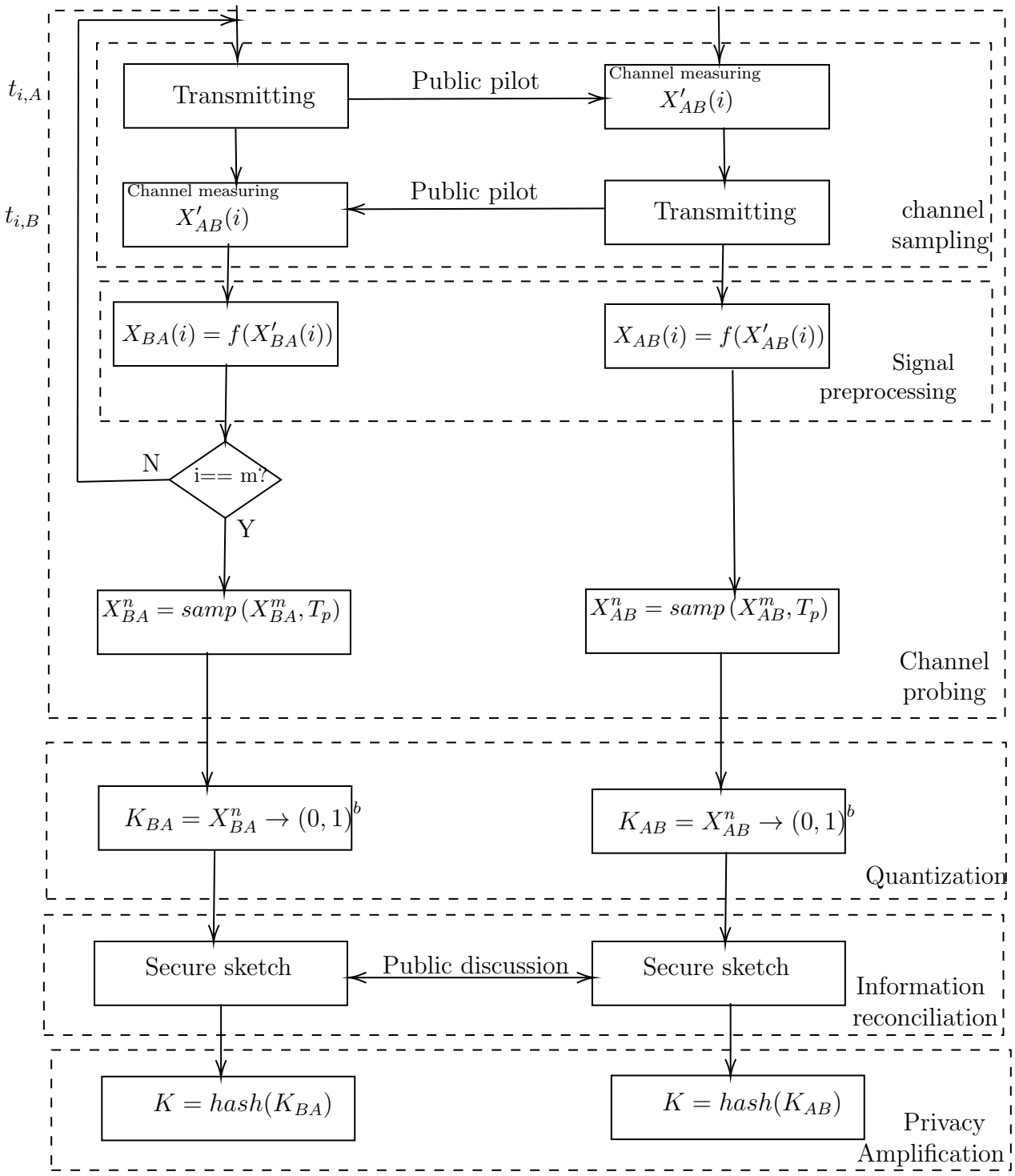

Figure 1.1: Scheme of the secret-key generation process

It is also to be noted that Eve's received signal is not going to be correlated to the Alice and Bob's if it is more than half a wavelength away from the source of the signal, making it impossible for them to reconstruct the original signal to recreate the generated key. We also assume the channel is partially reciprocal, so the noise added to Bob's and to Alice's received signals is correlated.

1.1.2 Quantization

In order to generate the key bits, the real values of the probing stage are quantized into bits. In most cases, so that the generated keys at Bob and Alice have a small number of differing bits, the quantizer uses a Gray code, since the sampled values at the legitmate receivers are not going to be the same.

In [3], the distribution function of the parameters is known, the authors propose to generate random bits from the samples is by dividing the space into M equi-probable intervals. Guard intervals are inserted on quantization intervals borders, with width proportional to the standard deviation of the signal.

However, with this technique some samples are bound to be discarded and, instead of a single signal, only escursions of length L are used as valid samples.

We consider a case in which the receivers also have access to side-information, corresponding to the measurements obtained through channel probing, which forms Markov chain $B-X-W$. In this case (as explained in [4]), a way to achieve randomness is to optimize the quantizer so that the secret key capacity C_{sk} is maximized, where $s_A = \{X\}$, $s_B = \{M, B\}$ and $s_E = \{M, W\}$ are respectively the side information and the message received by Alice, Bob and Eve. Since the expression of the secrecy capacity is not known in closed form we maximise the secrecy capacity lower bound

$$C_{sk}^{low}(\mathcal{T}_A, \mathcal{T}_B, \mathcal{T}_E) = I(s_A, s_B) - \min\{I(s_A, s_E), I(s_B, s_E)\} \tag{1.1}$$

1.1.3 Information Reconciliation

The distillation phase as described in [4] makes the two sequences potentially close enough to be within error code correction range.

Therefore Alice, who has already calculated the key $\underline{X} \notin \mathcal{C}_n$ from the real value X uses the error correction code $\mathcal{C}_n$, to calculate the syndrome $\sigma = H\underline{X}$, in order to find the coset leader $\xi(\sigma)$, which is then used to calculate the codeword $c = \underline{X} + \xi(\sigma) \in \mathcal{C}_n$.

$\xi(\sigma)$ is sent to Bob who has calculated the key $\underline{B} \notin \mathcal{C}_n$ from the real value B, and uses it to calculate $\underline{B'} = \underline{B} + \xi(\sigma)$. This step ensures that the same codeword is decoded by Bob, as it closes the Hamming distance between $\underline{B'}$ and $\underline{X}$ to be small enough to be within correction distance. The same process done by Alice is reapeated for Bob, therefore

$$\sigma' = H\underline{B'} \tag{1.2a}$$

$$c' = \underline{B'} + \xi(\sigma') \tag{1.2b}$$

If the code correction went accordingly $\underline{c'} = \underline{c}$, so Alice and Bob obtained the same key.

1.1.4 Privacy Amplification

As the reconciliation is done through public channel, part of the information is revealed to the eavesdropper. In order to remove such leakage [5] and obtain a secret key, Alice and Bob use privacy amplification. Privacy amplification can be implemented by extractor, universal hashing function, cryptographic hash function and Merkle-Damgard hash function

Chapter 2

Performance Constraints Measures

In order to compute the limits of the secrecy of a channel with eavesdropper we use two constraint metrics, as explained in [1], [2].

We consider a channel where the transimitter Alice sending over a channel message M, given information X. A passive attacker Eve decodes the information Z given side information W and received message M. Analogously the legitimate receiver Bob decodes information Y given side-information B message M. X and B are correlated but their statistics are not the same in general. The goal is to use a key reconciliation scheme that exploits the correlation advantage between X and B, in order to leak the least amount of information to Eve. We summarize the scheme in figure 2.1.

2.1 Performance Constraints Measures

To compute the performance constraints of the secret key generation process we consider the information reconciliation, as during this stage M, which is a function of X, is sent over the public channel.

A positive secrecy capacity is achievable if the error rate between Alice's and Bob's side information is lower than the error rate between Alice's and Eve's side information. This is because the message through the public channel, as explained in the following section, can be decoded only using the side information. For this reason we want to minimize the mutual information between the side information W and X.

We consider two metrics, one based on distortion [1], the other [2] based on the equivocation between the side information at Eve and the information it retrieves from the channel. We'll consider $M = f(U, V, X)$, where f is an

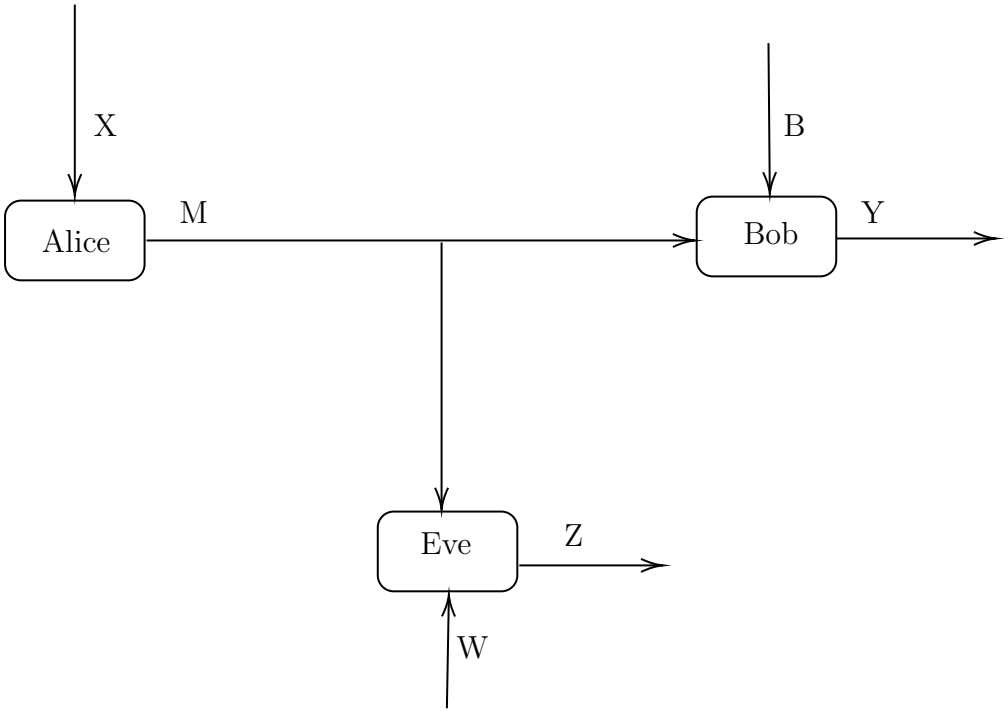

Figure 2.1: block diagram of the channel considered

invertible function given X, where the variables are connected as a Markov chain, such that

$$U - V - X - (B, W)$$

2.1.1 Rate-distortion metric

The metric described in [1] bases the constraints on rate-distortion. The rate-distortion function is defined as [6]

$$R^{(I)}(D) = \min_{p(X|\hat{X}):E[d(X,\hat{X})]<D} I(X;\hat{X}), \tag{2.1}$$

representing the minimum rate so that the distortion D is achievable, where distortion function d, usually in the form $d(X,\hat{X}) = \|X - \hat{X}\|^n$, defines the distortion caused by lossy transmission between the input X and decoded message $\hat{X}$.

The considered decoder is stochastic, as V and U aren't deterministic given X. From [6], the rate-distortion function with side information B given the

distortion D is

$$\begin{aligned} R_B(D) &= \min_{P(V|X)} \min_{f} I(X;B|V) = \\ &= \min_{P(V|X)} \min_{f} [I(X;V) - I(B;V)], \end{aligned} \tag{2.2}$$

$$\sum_x \sum_v \sum_b P(X=x, B=b) P(V=v|X=x) d(X=x, f(B=b, V=v)) \leq D, \quad \text{with } |V| \leq |X| + 1, \tag{2.3}$$

which is a non-increasing convex function of D. Going back to our scenario we introduce the following distortion metrics:

- D_b: the distortion of the decoded signal at Bob
- D_w: the distortion of the decoded signal at Eve
- R: rate of the encoder

Next we introduce the following theorems

Theorem 1 (Distortion Achievability [1]) *A rate-distortion triple (R, D_b, D_w) is achievable if there exist a sequence of rate R encoder and decoder tuple (f_n, g_n) such that:*

$$E[d_b(X^n, Y^n)] \leq_n D_b \tag{2.4a}$$

$$\min_{P_{Z^n|MW^n}} E[d_w(X^n, Z^n)] \geq_n D_w \tag{2.4b}$$

We assume that Eve decodes M using $P_{Z^n|MW^n}$.

Theorem 2 (Achievability using distortion measurement [1]) *A rate-distortion triple (R, D_b, D_w) is achievable if:*

$$R > I(V;X|B) \tag{2.5a}$$

$$D_b \geq E[d_b(X, Y)] \tag{2.5b}$$

$$D_w \leq \min_{z(u,w)} E[d_w(X, Z(U, W))] \tag{2.5c}$$

$$I(V;B|U) > I(V;W|U) \tag{2.5d}$$

for some $P_{UVXBW} = P_{XBW}P_{V|X}P_{U|V}$ *where* $Y = \phi(V,B)$ *for some function* ϕ

Theorem 3 (Converse (Distortion measure) [1]) *If a rate-distortion triple* (R, D_b, D_w) *is achievable then:*

$$R > I(V;X|B) \tag{2.6a}$$

$$D_b \geq E[d_b(X,Y)] \tag{2.6b}$$

$$D_w \leq \min_{z(w)} E[d_w(X, Z(W))] \tag{2.6c}$$

for some $\overline{P}_{VXBW} = \overline{P}_{XBW}\overline{P}_{V|X}$ *where* $Y = \phi(V,B)$ *for some function* ϕ*.*

If the legitimate receiver has strictly less noisy side information

$$I(V;B) > I(V;W) \tag{2.7}$$

the previous theorem is tight.

Additionally if the receivers must reconstruct the source sequence losslessly, we have the following inner bound.

Theorem 4 (Achievability using distortion measurement Corollary [1]) *A rate-distortion tuple* (R, D_w) *is achievable if:*

$$\begin{aligned} R &> H(X|B) \\ D_w &\leq \min_{z(u,w)} E[d_w(X, Z(U,W))] \\ I(X;B|U) &> I(X;W|U) \end{aligned} \tag{2.8a}$$

$$D_w \leq \min_{z(u,w)} E[d_w(X, Z(U,W))] \tag{2.8b}$$

$$I(X;B|U) > I(X;W|U) \tag{2.8c}$$

for some $P_{UVXBW} = P_{XBW}P_{V|X}P_{U|V}$ *where* $Y = \phi(V,B)$ *for some function* ϕ

2.1.2 Equivocation Measurement

In [2] the secrecy metrics are measured through the equivocation between the information at Alice (X) and the information at Eve (M and W).

Theorem 5 *[2] A tuple $(R, D, \Delta) \in \mathbb{R}_+^3$ is said to be achievable if, for any $\epsilon > 0$, there exists a $(n, R+\epsilon)$-code with encoder f and decoder g such that*

$$\mathbb{E}[d(X^n, g(f(X^n), B^n))] \leq D + \epsilon \tag{2.9a}$$

$$\frac{1}{n} H(X^n | f(X^n), W^n) \geq \Delta - \epsilon \tag{2.9b}$$

Theorem 6 (Equivocation Measure [2]) *Region $\mathcal{R}^*$ is the set of all tuples (R, D, Δ) such that there exist random variables U, V, on sum finite sets $\mathcal{U}$, $\mathcal{V}$, such that they form a Markov chain $U - V - X - (B, W)$, and a function $\hat{X} : \mathcal{V} \times \mathcal{U} \to \mathcal{X}$ such that*

$$R \geq I(V; X|B) \tag{2.10a}$$

$$D \geq \mathbb{E}[d(X, \hat{X}(V, B))] \tag{2.10b}$$

$$\Delta \leq [H(X|VB) + I(X; B|U) - I(X; W|U)]_+ \tag{2.10c}$$

intuition for third inequality: $H(X|VB)$ is the equivocation rate at Bob, exploited to increase the one at Eve, $I(X; B|U) - I(X; E|U)$ refers to how much Bob is more capable than Eve.

There exist the following cardinality constraints for $\mathcal{U}$ and $\mathcal{V}$:

$$\|\mathcal{U}\| \leq \|\mathcal{X}\| + 2 \tag{2.11a}$$

$$\|\mathcal{V}\| \leq (\|\mathcal{X}\| + 2)(\|\mathcal{X}\| + 1) \tag{2.11b}$$

Theorem 7 (B is less noisy than W(Equivocation Measure) [2]) *B is less noisy than W if*

$$I(U; B) \geq I(U; W) \tag{2.12}$$

In this case (R, D, Δ) is achievable if

$$R \geq I(V; X|B) \tag{2.13a}$$

$$D \geq \mathbb{E}[d(X, \hat{X}(V, B))] \tag{2.13b}$$

$$\Delta \leq [H(X|VB) + I(X; B) - I(X; W)]_+ \tag{2.13c}$$

The worst case is the one in which the two quantizers are exactly the same.

We assume B is strictly less noisy than W as, if the contrary was the case, Eve's measurements are on par with Alice's and Bob's ones, meaning that if the

key generation algorithm is known, Eve will always be able to generate the same private key as Alice.

U and V are discrete variables and the probability $P(U|V)$ determines the maximum distortion Z that can be achieved within the theorem bounds.

2.2 Codebook generation

The following section gives context to the relation between U, V and M, using the proof of achievability in [1]. X is encoded into four messages M_s, M'_s, M_p, M'_p, where M'_p and M'_s aren't sent over but they will be decoded from the other two messages. Fix a distribution $P_{UVXBW} = P_U P_{V|U} P_{X|V} P_{BW|X}$ satisfying the achievability conditions. Fix rates:

$$R_p + R'_p > I_P(U;X), \tag{2.14a}$$

$$R'_p < I_P(U;B) \tag{2.14b}$$

$$R_s + R'_s > I_P(X;V|U) \tag{2.14c}$$

$$I_P(V;W|U) < R'_s < I_P(V;B|U) \tag{2.14d}$$

the joint distribution is:

$$\begin{aligned} P(x^n, b^n, w^n, m_p, m'_p, m_s, m'_s, y^n) \triangleq \\ P_{X^n B^n W^n}(x^n, b^n, w^n) P_E(m_p, m'_p, m_s, m'_s|x^n) \\ P_D(m'_p, m'_s|x^n, m_p, m_s, b^n) P_\phi(y^n|m_p, \hat{m}'_p, m_s, \hat{m}_s, b^n) \end{aligned} \tag{2.15}$$

where P_E is the source encoder, P_D the first part of the decoder, decoding m', P_ϕ is the decoder of the sequence. Index by $(m_p, m'_p) \in \{1...2^{nR_p}\} \times \{1...2^{nR'_p}\}$ the sequences of $2^{n(R_p, R'_p)}$ symbols in $\mathcal{U}^n$ generated from the distribution $\prod_{t=1}^n P(u_t)$, the codebook called $\mathcal{C}_U^n$.

$(m_s, m'_s) \in \{1...2^{nR_s}\} \times \{1...2^{nR'_s}\}$ in the same way according to the distribution of $\mathcal{V}^n$ with distribution $\prod_{t=1}^n P(v_t|u_t(m_p, m'_p))$ this codeboox is denoted as $\mathcal{C}_v^{(n)}(m_p, m'_p)$ indexed by (m_p, m'_p, m_s, m'_s)

We compute the encoded message distribution as:

$$P_E(m|x^n) = \frac{\mathcal{L}(m|x^n)}{\sum_{\overline{m} \in \mathcal{M}} \mathcal{L}(\overline{m}|x^n)} \tag{2.16}$$

where

$$\mathcal{L}_E(m|x^n) = P_{X^n|V^n}(x^n|v^n(m)) \tag{2.17}$$

The decoder is composed of two parts:

1. channel decoder $P_D(\hat{m}'_p, \hat{m}'_s|m_p, m_s, b^n)$ a good channel decoder in respect to the superposition sub-codebook $\{v^n(m_p, a_p, m_s, a_s)\}_{a_p,a_s}$ and memoryless channel $P_{B|V}$

2. fix a function $\phi(\cdot,\cdot)$ as the concatenation $\{\phi(v_t, b_t)\}_{t=1}^n$ and set the decoder P_ϕ to be the deterministic function

$$\begin{aligned} P_\Phi(y^n|m_p, \hat{m}'_p, m_s, \hat{m}'_s) \stackrel{\Delta}{=} \\ 1\{y^n = \phi^n(v^n(m_p, \hat{m}'_p, m_s, \hat{m}'_s))\} \end{aligned} \tag{2.18}$$

where U and V are discrete variables

Chapter 3

System design

In the following chapter two examples of channel with eavesdropper and side-information are shown in order to formulate an optimization problem of the performance parameters shown in chapter 2. the GEKKO python library was used to solve the optimization problems.

3.1 Example from [1]

For validation purposes we now reproduce the results in [1].

3.1.1 Problem setup

The transition probabilities used in the following section (identical to the ones in [1]) for the side-information are as shown in the scheme in figure 3.1, where

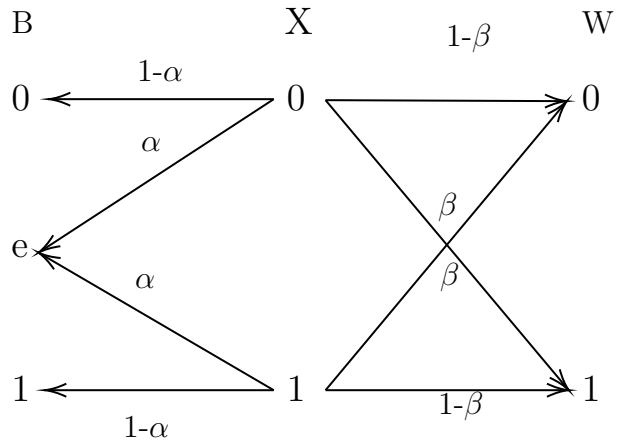

Figure 3.1: Transition probabilities of the problem, from [1]

- binary variable with lossless compression sent over binary channel as U to all receivers, therefore the corollary 4 can be used in such case.
- the distortion function used is Hamming distance.
- the channel ahs the following transition probabilities:

$$P_X(0) = 1 - P_X(1) = 1 - p \tag{3.1a}$$

$$B \in \{0, e, 1\} \tag{3.1b}$$

$$P_{B|X}(e|x) = \alpha \tag{3.1c}$$

$$P_{B|X}(b \neq e|x) = 1 - \alpha \tag{3.1d}$$

$$P_U(i) = u_i \tag{3.1e}$$

$$P_{X|U}(0|i) = \delta_i \tag{3.1f}$$

$$P_{X|U}(1|i) = 1 - \delta_i \tag{3.1g}$$

$$P_{W|X}(1 - x|x) = \beta \tag{3.1h}$$

3.1.2 Results

As explained previously, this particular case fits the hypothesis of corollary 4, therefore (R, D_w) is achievable if:

Rate

The rate has the following constraint:

$$R > H(X|B) = \alpha h(p) \tag{3.2a}$$

where

$$P(X = 0|B = 1) = P(X = 1|B = 0) = 0 \tag{3.2b}$$

$$P(X = 1|B = 1) = P(B = 0|B = 0) = 1 \tag{3.2c}$$

$$P(X = 0|B = e) = 1 - p \tag{3.2d}$$

$$P(X = 1|B = e) = p \tag{3.2e}$$

$$P(B = e) = \alpha \tag{3.2f}$$

Distortion at Eve

In order to minimize the expected value of the distortion at Eve can be defined as

$$\sum_{u_i} (P_{distortion}(u_i)P(U=i)) \tag{3.3}$$

(as the distortion is either 0 or 1), where $P_{distortion}$ is the probability of distortion if u_i is received, fixed the probability distribution of U, the decoder can either choose to use w as the value of the decoded x, with distortion probability β, or interpret u_i as value 0 or 1, with respective distortion probability $1-\delta_i$, δ_i so the minimum expected distortion is

$$D_w \leq \sum_{u_i} \min\{\delta_i, 1-\delta_i, \beta\} P_U(i) \tag{3.4}$$

In order to find the maximum achievable distortion at Eve D_w we need to maximize it over the probability u_i and δ_i

Mutual Information Constraint Formula

The following constraint represents the constraint of mutual information between X and the side-information at the receivers

$$\begin{aligned} I(X;B|U) =& H(X|U) - H(X|B,U) > I(X;W|U) = \\ =& H(X|U) - H(X|W,U) \\ \Rightarrow& - H(X|B,U) > -H(X|W,U) \end{aligned} \tag{3.5}$$

$$P(X=0|B=1,u_i) = P(X=1|B=0,u_i) = 0 \tag{3.6aa}$$

$$P(X=1|B=1,u_i) = P(X=0|B=0,u_i) = 1 \tag{3.6ab}$$

$$\begin{aligned} P(X=0|B=e,u_i) &= \frac{P(X=0,B=e,u_i)}{P(B=e,u_i)} = \\ &= \frac{P(B=e|X=0,u_i)P(X=0|u_i)P(u_i)}{P(B=e|u_i)P(u_i)} = \delta_i \end{aligned} \tag{3.6ac}$$

$$P(X=1|B=e) = p \tag{3.6ad}$$

$$p(b=e) = \alpha \tag{3.6ae}$$

$$H(X|B,U) = \sum_i u_i P(B=e|u_i)((1-\delta_i)\log_2 \frac{1}{1-\delta_i} + \\ +\delta_i \log_2 \frac{1}{\delta_i}) = \sum_i u_i \alpha h(\delta_i) \tag{3.6b}$$

$$P(W=0|u_i) = \delta_i(1-\beta) + (1-\delta_i)\beta \tag{3.6ca}$$

$$P(W=1|u_i) = \delta_i\beta + (1-\delta_i)(1-\beta) \tag{3.6cb}$$

$$P(X=0|W=1,u_i) = \frac{P(W=1|u_i,X=0)P(u_i,X=0)}{P(u_i,W=1)} = \\ = \frac{P(W=1|u_i,X=0)P(u_i,X=0)}{P(W=1|u_i)} = \\ = \frac{\beta\delta_i}{P(W=0|u_i)} \tag{3.6cc}$$

$$P(X=0|W=0,u_i) = \frac{P(W=0|u_i,X=0)P(u_i,X=0)}{P(u_i,W=0)} = \\ = \frac{P(W=0|u_i,X=0)P(u_i,X=0)}{P(W=0|u_i)} = \\ = \frac{(1-\beta)\delta_i}{P(W=0|u_i)} \tag{3.6cd}$$

$$
\begin{aligned}
H(X|W,U) = \\
&= \sum_i u_i (P(W=0|u_i)(P(X=0|W=0,u_i)\log_2 P(X=0|W=0,u_i) = \\
&+ P(X=1|W=0,u_i)\log_2 P(X=1|W=0,u_i)) + P(W=0|u_i)(\\
&P(X=0|W=0,u_i)\log_2 P(X=0|W=0,u_i) \\
&+ P(X=1|W=0,u_i)\log_2 P(X=1|W=0,u_i))) = \\
&\sum_i u_i (\\
&\beta(1-\delta_i)\log_2 \frac{\delta_i(1-\beta)+(1-\delta_i)\beta}{\beta(1-\delta_i)} + (1-\beta)\delta_i \log_2 \frac{\beta(1-\delta_i)+(1-\delta_i)\beta}{\delta_i 1-\beta} \\
&+ (1-\beta)(1-\delta_i)\ \log_2 \frac{(1-\delta_i)(1-\beta)+\delta_i\beta}{(1-\beta)(1-\delta_i)} + \beta\delta_i \\
&\log_2 \frac{\beta\delta_i+(1-\delta_i)(1-\beta)}{\delta_i\beta}) \\
&= \sum_i u_i (\beta(1-\delta_i)(\log_2 \delta_i(1-\beta)+\beta(1-\delta_i))+ \\
&+ \log_2 \frac{1}{\beta(1-\delta_i)} + \delta_i(1-\beta)(\log_2 \delta_i(1-\beta)+\beta(1-\delta_i) \\
&\log_2 \frac{1}{\delta_i(1-\beta)}) + \delta_i\beta(\log_2 (1-\delta_i)(1-\beta)+\beta\delta_i+ \\
&+ \log_2 \frac{1}{\beta\delta_i}) + (1-\delta_i)(1-\beta)(\log_2 (1-\delta_i)(1-\beta)+\beta\delta_i \\
&\log_2 \frac{1}{(1-\delta_i)(1-\beta)})) = \\
&(\text{decomposing } \log\frac{1}{ab} = \log\frac{1}{a} + \log\frac{1}{b}) \\
&= \sum_i u_i (\beta \log_2 \frac{1}{\beta} + (1-\beta)\log_2 \frac{1}{(1-\beta)} + \\
&+ \delta_i \log_2 \frac{1}{\delta_i} + (1-\delta_i)\log_2 \frac{1}{(1-\delta_i)} + \\
&+ \log\left((1-\delta_i)(1-\beta)+\beta\delta_i\right)\left((1-\delta_i)(1-\beta)+\beta\delta_i\right) + \\
&+ \log\left((1-\delta_i)\beta+(1-\beta)\delta_i\right)\left((1-\delta_i)\beta+(1-\beta)\delta_i\right) \\
&\geq 0
\end{aligned}
\tag{3.6d}
$$

3.1.3 Problem definition

Using the previous result the constraints are expressed in an optimization problem of D_w

Constants

α, β

Problem

$$D_w = \max_{\{u_i, \delta_i\}} \sum_{i=1}^{3} u_i \min\{\delta_i, 1-\delta_i, \beta\} \tag{3.4}$$

s.t.

$$R \geq \alpha h(p) \tag{3.5a}$$

$$\sum_{i=1}^{3} u_i = 1 \tag{3.5b}$$

$$\sum_{i=1}^{3} u_i \delta_i = 1 - p \tag{3.5c}$$

Information constraint

$$\begin{aligned} & h(\beta) + \sum_{i=1}^{3} u_i [(1-\alpha) h(\delta_i) + \\ & + \log\left((1-\delta_i)(1-\beta) + \beta\delta_i\right)\left((1-\delta_i)(1-\beta) + \beta\delta_i\right) + \\ & + \log\left((1-\delta_i)\beta + (1-\beta)\delta_i\right)\left((1-\delta_i)\beta + (1-\beta)\delta_i\right)] \\ & \geq 0 \end{aligned} \tag{3.5d}$$

3.2 Distortion measure with arbitrary cardinality of the side information

The general case is considered using theorem 2, without assumption of the cardinality of B and W. This is done to more easily derive particular cases in the next sections

Rate Constraint

The rate has the following constraint:

$$R > I(V; X|B) = I(X; V|B) = H(X|B) - H(X|V, B) \tag{3.6a}$$

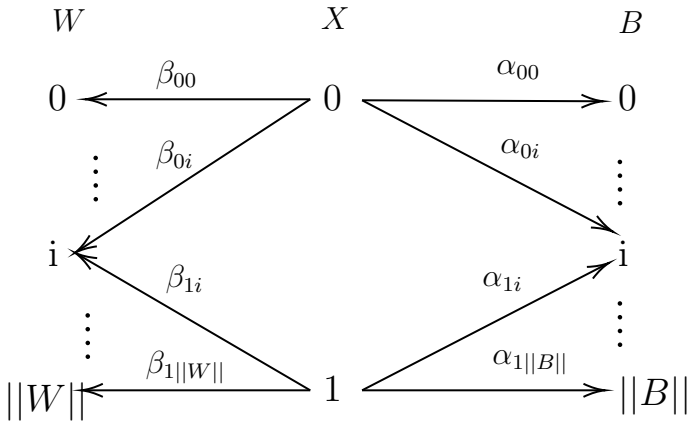

Figure 3.2: transition probabilities for the side information in the general case

where:

$$
\begin{aligned}
&H(X|B) = \\
&-\sum_i P(B=i)(\sum_j P(X=j|B=i)\log_2 P(X=j|B=i)) = \\
&-\sum_{ij} P(B=i|X=j)P(X=j)\log_2 \frac{P(B=i|X=j)P(X=j)}{P(B=i)}
\end{aligned}
\tag{3.6b}
$$

$$
\begin{aligned}
&H(X|V,B) = \\
&-\sum_{i,j} P(V=i,B=j)(\\
&\sum_k P(X=k|V=i,B=j)\log_2 P(X=k|V=i,B=j)) = \\
&-\sum_{i,j}\sum_k P(B=j|X=k)P(V=i|X=k)P(X=k) \\
&\log_2 \frac{P(B=j|X=k)P(V=i|X=k)P(X=k)}{\sum_{k'} P(V=i|X=k')P(B=j|X=k')P(X=k')}
\end{aligned}
\tag{3.6c}
$$

distortion at Bob constraint

$D_b \geq E[d_b(X,Y)]$ choose $Y = \phi(V,B)$ in order to minimize the distortion of Y within the bounds. Assuming the cardinality is finite the number of ϕ is finite, therefore the complexity is exponential to the cardinality of V and B

constraint on the distortion at Eve

$D_w \leq \min_{Z(u,w)} E[d_w(X,Z)]$, where the $Z(u,w)$ that minimizes the distortion is therefore, if X is binary, the distiortion is

$$D_w \leq \sum_{ij} \min\{P(U=i,W=j,X=0), P(U=i,W=j,X=1)\} \tag{3.7}$$

Noisiness of the side information Contraint

$I(V;B|U) > I(V;W|U) \Rightarrow H(B|U) - H(V,B|U) > H(W|U) - H(V,W|U)$ the computation for $H(B|U) - H(V,B|U)$ is shown, $H(W|U) - H(V,W|U)$ is analogous:

$$\begin{aligned}
&H(B|U) = -\sum_j P(U=j)(\sum_i P(B=i|U=j)\log(P(B=i|U=j))) = \\
&[P(B=i|U=j) = \frac{P(B=i,U=j)}{P(U=j)}] \\
&-\sum_{i,j}(\sum_k P(B=i,X=k,U=j))\log\frac{\sum_k P(B=i,X=k,U=j)}{P(U=j)} = \\
&[P(B=i,X=k,U=j) = P(B=i,U=j|X=k)P(X=k) = \\
&P(B=i|X=k)P(U=j|X=k)P(X=k)] \\
&-\sum_{i,j}(\sum_k P(B=i|X=k)P(U=j|X=k)P(X=k)) \\
&\log\frac{\sum_k P(B=i|X=k)P(U=j|X=k)P(X=k)}{P(U=j)} =
\end{aligned} \tag{3.8a}$$

$$\begin{aligned}
&H(V,B|U) = \\
&-\sum_{i,j,k} P(V=i,B=j,U=k)\log_2\left(\frac{P(V=i,B=j,U=k)}{P(U=k)}\right) = \\
&-\sum_{i,j,k}\left(\sum_l P(B=j|X=l)P(U=k|V=i)P(V=i|X=l)P(X=l)\right) \\
&\log_2\left(\frac{\sum_l P(B=j|X=l)P(U=k|V=i)P(V=i|X=l)P(X=l)}{P(U=k)}\right)
\end{aligned} \tag{3.8b}$$

$$\begin{aligned}
H(X,B) = -\sum_{ij} P(B=j|X=i)P(X=i) \\
\log_2 P(B=j|X=i)P(X=i)
\end{aligned} \tag{3.8c}$$

3.2.1 Problem definition

In the following the constraints are formulated as an optimization problem where we find the maximum value of D_w, with X binary.

Constants

$\alpha_{ij}, \beta_{ij}, \phi, D_b, p$

Problem

$$D_w = \max \sum_{ij} \min\{\omega_{i0}\beta_{0j}p_0, \omega_{i1}\beta_{1j}p_1\} \tag{3.9}$$

s.t.

$\alpha_{ij} = P(X = i|B = j)$

$$\alpha_{ij} \in [0, 1], i \in [0, 1] \tag{3.10a}$$

$\beta_{ij} = P(X = i|W = j)$

$$\beta_{ij} \in [0, 1], i \in [0, 1] \tag{3.10b}$$

Transition probability $P(V = j|X = i)$

$$\delta_{ij} \in [0, 1], i \in [0, 1] \tag{3.10c}$$

Transition probability $P(U = j|V = i)$

$$\gamma_{ij} \in [0, 1], i \in [1, 3] \tag{3.10d}$$

where $p_0 = P(X = 0)$

$$p_0 = p, p_1 = 1 - p_0 \tag{3.10e}$$

constraint of the transition probabilities $\sum_i P(B = i|X = k) = 1$

$$\sum_i \alpha_{ki} = 1 \tag{3.10f}$$

constraint of the transition probabilities $\sum_i P(W = i|X = k) = 1$

$$\sum_i \beta_{ki} = 1 \tag{3.10g}$$

constraint of the transition probabilities $\sum_i P(V = i|X = k) = 1$

$$\sum_i \delta_{ki} = 1 \tag{3.10h}$$

constraint of the transition probabilities $\sum_i P(U = i|X = k) = 1$

$$\sum_i \gamma_{ki} = 1 \tag{3.10i}$$

$v_i = P(V = i)$

$$v_i = \sum_{j=0,1} \delta_{ji} p_j \tag{3.10j}$$

$u_i = P(U = i)$

$$u_i = \sum_j \gamma_{ji} v_j \tag{3.10k}$$

$b_i = P(B = i)$

$$b_i = \sum_j \alpha_{ji} p_j \tag{3.10l}$$

$\Delta_{ij} = P(X = i|V = j)$

$$\Delta_{ij} = \frac{\delta_{ij} p_i}{v_j} \tag{3.10m}$$

$\xi_i j = P(X = i|U = j)$

$$\xi_{ij} = \frac{\sum_k \gamma_{kj} \delta_{ik} p_i}{u_j} \tag{3.10n}$$

$\omega_{ij} = P(U = j|X = i)$

$$\omega_{ij} = \frac{\xi_{ij} u_j}{p_i} \tag{3.10o}$$

$$R > -\sum_{ij} \alpha_{ji} p_j \log_2 \frac{\alpha_{ji} p_j}{b_i} \quad + \sum_{ijk} \alpha_k j \delta_{ki} p_k \log_2 \frac{\alpha_k j \delta_{ki} p_k}{\sum_l \alpha_{l,j} \delta_{li} p_l} \tag{3.10p}$$

$$D_b \geq E[d_b(X, \phi(B, V))] \tag{3.10q}$$

(noisiness of the side information constraint)

$$\begin{aligned} &-\sum_{ij}(\sum_{k}\alpha_{ki}\omega jkp_k)log_2\frac{(\sum_k \alpha_{ki}\omega jkp_k)}{u_j} \\ &+\sum_{ijk}(\sum_{l}\alpha_{lj}\gamma ik\delta lip_l)\log_2\frac{(\sum_l \alpha_{lj}\gamma ik\delta lip_l)}{u_j} > \\ &-\sum_{ij}(\sum_{k}\beta_{ki}\omega jkp_k)log_2\frac{(\sum_k \beta_{ki}\omega jkp_k)}{u_j} \\ &+\sum_{ijk}(\sum_{l}\beta_{lj}\gamma ik\delta lip_l)\log_2\frac{(\sum_l \beta_{lj}\gamma ik\delta lip_l)}{u_j} \end{aligned} \tag{3.10r}$$

3.3 Equivocation measure with arbitrary cardinality of the side information

In this section the purpose is the same as the previous but using theorem 6. The setup is the same, with transition probabilities shown in figure 3.2

$$R \geq I(V; X|B) \tag{3.11a}$$

$$D_b \geq E[d(X, \hat{X}(V, B))] \tag{3.11b}$$

$$\Delta \leq [H(X|V, B) + I(X; B|U) - I(X; W|U)]_+ \tag{3.11c}$$

Δ parameter formula

$H(X|V, B)$ is computed in the previous section, only $I(X; B|U) - I(X; W|U)$ is shown.

$$\begin{aligned} &I(X; B|U) - I(X; W|U) = \\ &= H(X|U) + H(B|U) - H(X, B|U) - (H(X|U) + H(W|U) - H(X, W|U)) \\ &= H(B|U) - H(X, B|U) - (H(W|U) - H(X, W|U)) \end{aligned} \tag{3.12}$$

$$
\begin{aligned}
&H(X,B|U) = \\
&= -\sum_{i} P(U=i) \sum_{i,k} P(X=j,B=k|U=i) \log_2 P(X=j,B=k|U=i) = \\
&= \sum_{i,k,j} P(U=i|X=j)P(B=k|X=j)P(X=j) \\
&\log_2 \frac{P(U=i|X=j)P(B=k|X=j)P(X=j)}{P(U=i)}
\end{aligned}
\tag{3.13}
$$

3.3.1 Side information B is less noisy than side information E

We also considered the theorem 7 as the hypothesis is coherent with the requirements to achieve secrecy in our case. Most of the formulas are analogous to previous examples, therefore omitted here

Noisiness Constraint

$$I(U;B) \geq I(U;E) \Rightarrow H(B) - H(U,B) \geq H(W) - H(U,W) \tag{3.14a}$$

$$
\begin{aligned}
&H(U,B) = -\sum_{i,j} \left(\sum_{k} P(U=i|X=k)P(B=j|X=k)P(X=k) \right) \\
&\log_2 \sum_{k} P(U=i|X=k)P(B=j|X=k)P(X=k) =
\end{aligned}
\tag{3.14b}
$$

Δ parameter formula

$$\Delta \leq [H(X|VB) + I(X;B) - I(X;W)]_+ \tag{3.15a}$$

$$
\begin{aligned}
H(X,B) = &-\sum_{ij} P(B=j|X=i)P(X=i) \\
&\log_2 P(B=j|X=i)P(X=i)
\end{aligned}
\tag{3.15b}
$$

3.3.2 Problem definition

In the following, the previous constraints are formulated as an optimization problem where we find the maximum value of Δ, with X binary.

Constants

$\alpha_{ij}, \beta_{ij}, \phi, D_b, p$

Problem

$$\begin{aligned}\Delta = max\{ &- \sum_{ijk} \alpha_{kj}\delta_{ki}p_k \log_2 \frac{\alpha_{kj}\delta_{ki}p_k}{\sum_l \alpha_{l,j}\delta_{li}p_l} \\ &- \sum_{ij}(\sum_k \alpha_{ki}\omega jkp_k) log_2 \frac{(\sum_k \alpha_{ki}\omega jkp_k)}{u_j} \\ &+ \sum_{ijk}(\omega_{ij}\alpha jkp_j) \log_2 \frac{\omega_{ij}\alpha jkp_j}{u_i} \\ -(&- \sum_{ij}(\sum_k \beta_{ki}\omega jkp_k) log_2 \frac{(\sum_k \beta_{ki}\omega jkp_k)}{u_j} \\ &+ \sum_{ijk}(\omega_{ij}\beta jkp_j) \log_2 \frac{\omega_{ij}\beta jkp_j}{u_i})\}\end{aligned} \tag{3.16a}$$

s.t.

$$\alpha_{ij} \in [0,1], i \in [0,1] \tag{3.17a}$$

$$\beta_{ij} \in [0,1], i \in [0,1] \tag{3.17b}$$

$$\delta_{ij} \in [0,1], i \in [0,1] \tag{3.17c}$$

$$\gamma_{ij} \in [0,1], i \in [1,3] \tag{3.17d}$$

$$p_0 = p, p_1 = 1 - p_0 \tag{3.17e}$$

$$\sum_i \alpha_{ki} = 1 \tag{3.17f}$$

$$\sum_i \beta_{ki} = 1 \tag{3.17g}$$

$$\sum_i \delta_{ki} = 1 \tag{3.17h}$$

$$\sum_i \gamma_{ki} = 1 \tag{3.17i}$$

$$v_i = \sum_{j=0,1} \delta_{ji}p_j \tag{3.17j}$$

$$u_i = \sum_j \gamma_{ji}v_j \tag{3.17k}$$

$$b_i = \sum_j \alpha_{ji}p_j \tag{3.17l}$$

$$w_i = \sum_j \beta_{ji} p_j \tag{3.17m}$$

$$\Delta_{ij} = \frac{\delta_{ij} p_i}{v_j} \tag{3.17n}$$

$$\xi_{ij} = \frac{\sum_k \gamma_{kj} \delta_{ik} p_i}{u_j} \tag{3.17o}$$

$$\omega_{ij} = \frac{\xi_{ij} u_j}{p_i} \tag{3.17p}$$

$$R > -\sum_{ij} \alpha_{ji} p_j * \log_2 \frac{\alpha_{ji} p_j}{b_i} \quad + \sum_{ijk} \alpha_k j \delta_{ki} p_k \log_2 \frac{\alpha_k j \delta_{ki} p_k}{\sum_l \alpha_{l,j} \delta_{li} p_l} \tag{3.17q}$$

$$D_b \geq E[d_b(X, \phi(B, V))] \tag{3.17r}$$

3.3.3 Problem definition side information at Bob less noisy than he one at Eve

In the following the problem is formulated as an optimization problem where we find the maximum value of Δ, with X binary. The definition of the proxy variables is the same as the previous section

Constants

$\alpha_{ij}, \beta_{ij}, \phi, D_b, p$

Problem

$$\begin{aligned} \Delta = \max\{ & -\left(\sum_{ijk} \alpha_{kj} \delta_{ki} p_k \log_2 \frac{\alpha_{kj} \delta_{ki} p_k}{(\sum_l \alpha_{l,j} \delta_{li} p_l)}\right) \\ & -\left(\sum_i b_i \log_2 b_i\right) \\ & +\left(\sum_{ij} \alpha_{ij} p_i \left(-\left(\sum_i w_i \log_2 b_i\right) + \left(\sum_{ij} \beta_{ij} p_i\right)\right)\right)\} \end{aligned} \tag{3.18a}$$

s.t.

$$\alpha_{ij} \in [0,1], i \in [0,1] \tag{3.19a}$$

$$\beta_{ij} \in [0,1], i \in [0,1] \tag{3.19b}$$

$$\delta_{ij} \in [0,1], i \in [0,1] \tag{3.19c}$$

$$\gamma_{ij} \in [0,1], i \in [1,3] \tag{3.19d}$$

$$p_0 = p, p_1 = 1 - p_0 \tag{3.19e}$$

$$\sum_i \alpha_{ki} = 1 \tag{3.19f}$$

$$\sum_i \beta_{ki} = 1 \tag{3.19g}$$

$$\sum_i \delta_{ki} = 1 \tag{3.19h}$$

$$\sum_i \gamma_{ki} = 1 \tag{3.19i}$$

$$v_i = \sum_{j=0,1} \delta_{ji} p_j \tag{3.19j}$$

$$u_i = \sum_j \gamma_{ji} v_j \tag{3.19k}$$

$$b_i = \sum_j \alpha_{ji} p_j \tag{3.19l}$$

$$\Delta_{ij} = \frac{\delta_{ij} p_i}{v_j} \tag{3.19m}$$

$$\xi_{ij} = \frac{\sum_k \gamma_{kj} \delta_{ik} p_i}{u_j} \tag{3.19n}$$

$$\omega_{ij} = \frac{\xi_{ij} u_j}{p_i} \tag{3.19o}$$

$$R > -\sum_{ij} \alpha_{ji} p_j * \log_2 \frac{\alpha_{ji} p_j}{b_i} \quad + \sum_{ijk} \alpha_k j \delta_{ki} p_k \log_2 \frac{\alpha_k j \delta_{ki} p_k}{\sum_l \alpha_{l,j} \delta_{li} p_l} \tag{3.19p}$$

$$D_b \geq E[d_b(X, \phi(B,V))] \tag{3.19q}$$

side information noisiness constrains

$$\begin{aligned} & -\sum_i b_i \log_2 b_i \\ & + \sum_{ij} (\sum_k \omega_{ki} \alpha k j p_k) \log_2 (\sum_k \omega_{ki} \alpha k j p_k) \\ & > -\sum_i w_i \log_2 w_i \\ & + \sum_{ij} (\sum_k \omega_{ki} \beta k j p_k) \log_2 (\sum_k \omega_{ki} \beta k j p_k) \end{aligned} \tag{3.19r}$$

3.4 Equivocation measure with arbitrary cardinality of the side information and $R = 0$

The setup is the same as the previous case, however now we don't assume the cardinality of X, B and W and we assume no message is sent($R = 0$). This is needed in order to compare the performance of the equivocation with the case in which no message is sent.

$$D_b \geq E[d(X, B))] \tag{3.20a}$$

$$\Delta \leq [H(X|B) + I(X;B) - I(X;W)]_+ \tag{3.20b}$$

Formulas

$$\begin{aligned} & I(X;B) - I(X;W) = \\ & = H(X) + H(B) - H(X,B) - (H(X) + H(W) - H(X,W)) \\ & = H(B) - H(X,B) - (H(W) - H(X,W)) \end{aligned} \tag{3.21}$$

$$\begin{aligned} & H(X,B) = \\ & = -\sum_{i,k} P(X=j, B=k) \log_2 P(X=j, B=k) = \\ & = \sum_{i,k} P(B=k|X=j) P(X=j) \\ & \log_2 P(B=k|X=j) P(X=j) \end{aligned} \tag{3.22}$$

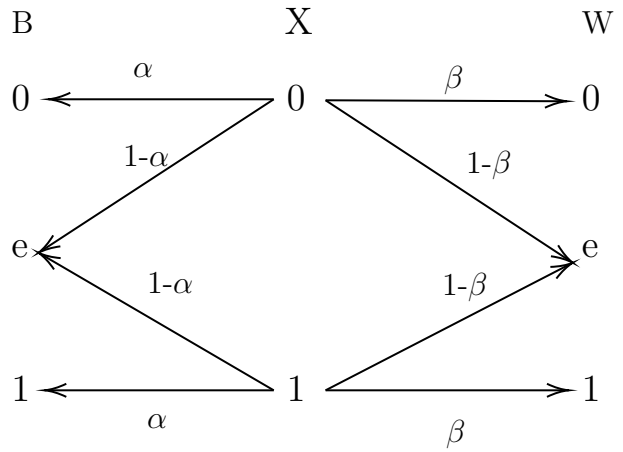

Figure 3.3: transition probabilities for the side information at the receivers for the considered case study

$$
\begin{aligned}
&H(B) = \\
&= -\sum_k \left(\sum_j P(X=j, B=k) \right) \log_2 \sum_j P(X=j, B=k) = \\
&= \sum_k \left(\sum_j P(B=k|X=j) P(X=j) \right) \\
&\log_2 \sum_j P(B=k|X=j) P(X=j)
\end{aligned}
\tag{3.23}
$$

3.5 Binary Deletion Channel Example Using Rate-Distortion Measure [1]

Using the general formulas obtained in previous sections in order to solve a particular case. In the following section we consider the case in which B and W are binary variables with deletion.U, V, B, W have cardinality 3 and X is a binary source. The transition probabilities are shown in figure 3.1

Parameters

$$P(B=0|X=0) = P(B=1|X=1) = \alpha \tag{3.24a}$$

$$P(B=1|X=0) = P(B=0|X=1) = 0 \tag{3.24b}$$

$$P(B=e|X=0) = P(B=e|X=1) = 1-\alpha \tag{3.24c}$$

$$P(W=0|X=0) = P(W=1|X=1) = \beta \tag{3.24d}$$

$$P(W = 1|X = 0) = P(W = 0|X = 1) = 0 \tag{3.24e}$$

$$P(W = e|X = 0) = P(W = e|X = 1) = 1 - \beta \tag{3.24f}$$

Variables

the following transition probabilities are considered variables in this context

$$P(V = i|X = j) = \delta_{ji} \tag{3.25a}$$

$$P(U = i|V = j) = \gamma_{ji} \tag{3.25b}$$

Definitions

$$v_i \triangleq P(V = i) = \sum_j P(V = i|X = j)P(X = j) \tag{3.26a}$$

$$u_i \triangleq P(U = i) = \sum_j P(U = i|V = j)P(V = j) \tag{3.26b}$$

$$\Delta_{ji} \triangleq P(X = j|V = i) = \frac{P(V = i|X = j)P(X = j)}{P(V = i)} \tag{3.26c}$$

$$\Gamma_{ji} \triangleq P(V = j|U = i) = \frac{P(U = i|V = j)P(V = j)}{P(U = i)} \tag{3.26d}$$

$$\begin{aligned}\omega_{ji} \triangleq & P(U = j|X = i) = \frac{\sum_k P(U = j, X = i, V = k)}{P(X = i)} = \\ & \sum_k P(U = j|V = k)P(V = k|X = i)\end{aligned} \tag{3.26e}$$

Constraints

The following formulas are obtained using theorem 2

Rate Constraint

$$R > I(V; X|B) = I(X; V|B) = H(X|B) - H(X|V, B) \tag{3.27a}$$

where the entropy can be computed as following:

$$
\begin{aligned}
&H(X|B) = \\
&-\sum_i P(B=i)(\sum_j P(X=j|B=i)\log_2 P(X=j|B=i)) = \\
&\text{every value of } B \neq e \text{ yields zero information} \\
&-P(B=e)((P(X=1|B=e)\log P(X=1|B=e) + P(X=0|B=e)\log P(X=0|B=e))) \\
&= (1-\alpha)h(p)
\end{aligned}
\tag{3.27b}
$$

$$
\begin{aligned}
&H(X|V,B) = \\
&-\sum_{i,j} P(V=i,B=j)(\\
&\sum_k P(X=k|V=i,B=j)\log P(X=k|V=i,B=j)) = \\
&\text{analogous to the previous case, every value of } B \neq e \text{ yields zero information} \\
&-\sum_i P(V=i,B=e) \\
&(\sum_k P(X=k|V=i,B=e)\log P(X=k|V=i,B=e)) = \\
&-\sum_{ik} P(V=i|X=k)P(B=e|X=k)P(X=k) \\
&\log \frac{P(V=i|X=k)(B=e|X=k)P(X=k)}{P(V=i,B=e)} = \\
&-\sum_{ik}(1-\alpha)P(X=k|V=i)P(V=i) \\
&\log \frac{P(V=i|X=k)(1-\alpha)P(X=k)}{\sum_{k'} P(V=i|X=k')P(B=e|X=k')P(X=k')} = \\
\\
&1-\alpha = P(B=e|X=k), k \in \{0,1\} \\
&\text{and } v_i = \sum_k P(V=i|X=k)P(X=k) \\
&-(1-\alpha)\sum_{ik} P(X=k|V=i)P(V=i)\log \frac{P(X=k|V=i)P(V=i)}{v_i} = \\
&-(1-\alpha)\sum_{i,k} \Delta_{ki} v_i \log \Delta_{ki} = (1-\alpha)\sum_i v_i h(\Delta_{ki})
\end{aligned}
\tag{3.27c}
$$

Distortion at Bob constraint

$D_b \geq E[d_b(X,Y)]$ choose $Y = \phi(V,B)$ in order to minimize the distortion of Y within the constraints

Distortion at Eve constraint

$D_w \leq \min_{Z(u,w)} E[d_w(X,Z)]$ analogous to the general case, however some considerations are to be made. In this case if Eve receives either 0 or 1 the distiortion is 0 in all cases, as the probability of transition between the two values is zero. Only if Eve receives e the value received is ambiguos, therefore the previous inequality is:

$$\begin{aligned} D_w \leq & \sum_i \min\{1P(X=0,W=e,U=i), 1P(X=0,W=e,U=i)\} = \\ & \sum_i \min\{P(W=e|X=0)P(X=0|U=i)P(U=i), \\ & P(W=e|X=1)P(X=1|U=i)P(U=i)\} = \\ & \sum_i (1-\beta)(P(U=i)) \min\{P(X=0|U=i), P(X=1|U=i)\} \end{aligned} \tag{3.28}$$

Noisiness of the side information constraint

$I(V;B|U) > I(V;W|U) \Rightarrow H(B|U) - H(V,B|U) > H(W|U) - H(V,W|U)$ the formula for $H(B|U) - H(V,B|U)$ is shown, $H(W|U) - H(V,W|U)$ is analogous:

$$
\begin{aligned}
&H(B|U) = -\sum_j P(U=j)(\sum_i P(B=i|U=j)\log(P(B=i|U=j))) = \\
&[P(B=i|U=j) = \frac{P(B=i,U=j)}{P(U=j)}] \\
&-\sum_{i,j}(\sum_k P(B=i,X=k,U=j))\log\frac{\sum_k P(B=i,X=k,U=j)}{P(U=j)} = \\
&[P(B=i,X=k,U=j) = P(B=i,U=j|X=k)P(X=k) = \\
&P(B=i|X=k)P(U=j|X=k)P(X=k)] \\
&-\sum_{i,j}(\sum_k P(B=i|X=k)P(U=j|X=k)P(X=k)) \\
&\log\frac{\sum_k P(B=i|X=k)P(U=j|X=k)P(X=k)}{P(U=j)} = \\
&[P(B\in\{0,1\}, B\neq X)=0] \\
&-\sum_j (P(B=0|X=0)P(U=j|X=0)P(X=0)) \\
&\log\frac{P(B=0|X=0)P(U=j|X=0)P(X=0)}{P(U=j)} + \\
&(P(B=1|X=1)P(U=j|X=1)P(X=1)) \\
&\log\frac{P(B=1|X=1)P(U=j|X=1)P(X=1)}{P(U=j)} + \\
&(P(B=e|X=0)P(U=j|X=0)P(X=0) + \\
&P(B=e|X=1)P(U=j|X=1)P(X=1)) \\
&\log(\frac{P(B=e|X=0)P(U=j|X=0)P(X=0)}{P(U=j)} \\
&+\frac{P(B=e|X=1)P(U=j|X=1)P(X=1)}{P(U=j)})
\end{aligned}
\tag{3.29a}
$$

$$
\begin{aligned}
&H(V,B|U) = \\
&-\sum_{i,j,k} P(V=i,B=j,U=k)\log(\frac{P(V=i,B=j,U=k)}{P(U=k)}) = \\
&-\sum_{i,j,k}(\sum_{l} P(B=j|X=l)P(U=k|V=i)P(V=i|X=l)P(X=l)) \\
&\log(\frac{P(V=i,B=j,U=k)}{P(U=k)}) = \\
&-\sum_{i,k}(P(B=0|X=0)P(U=k|V=i)P(V=i|X=0)P(X=0)) \\
&\log(\frac{P(V=i,B=0,U=k)}{P(U=k)})+ \\
&(P(B=1|X=1)P(U=k|V=i)P(V=i|X=1)P(X=1)) \\
&\log(\frac{P(V=i,B=1,U=k)}{P(U=k)})+ \\
&(P(B=e|X=0)P(U=k|V=i)P(V=i|X=0)P(X=0)+ \\
&P(B=e|X=1)P(U=k|V=i)P(V=i|X=1)P(X=1)) \\
&\log(\frac{P(V=i,B=e,U=k)}{P(U=k)})
\end{aligned}
\tag{3.29b}
$$

3.5.1 Problem definition

In the following the previous formulas are formulated as an optimization problem where we find the maximum value of D_w, by using proxy variables to make the formulas more readable.

Constants

$\alpha, \beta, \phi, D_b, p$

Problem

$$D_w = \max_{\delta_{ij},\gamma_{ih}} \sum_i u_i(1-\beta)\min\{\xi_{0i},\xi_{1i}\} \tag{3.30}$$

s.t.

Transition probability $P(V=j|X=i)$

$$\delta_{ij} \in [0,1], i \in [0,1], j \in [1,3] \tag{3.31a}$$

Transition probability $P(U = j|V = i)$

$$\gamma_{ij} \in [0, 1], i \in [1, 3], j \in [1, 3] \tag{3.31b}$$

where $p_0 = P(X = 0)$

$$p_0 = p, p_1 = 1 - p_0 \tag{3.31c}$$

constraint of the transition probabilities $\sum_i P(V = i|X = k) = 1$

$$\sum_i \delta_{ki} = 1 \tag{3.31d}$$

constraint of the transition probabilities $\sum_i P(U = i|X = k) = 1$

$$\sum_i \gamma_{ki} = 1 \tag{3.31e}$$

$v_i = P(V = i)$

$$v_i = \sum_{j=0,1} \delta_{ji} p_j \tag{3.31f}$$

$u_i = P(U = i)$

$$u_i = \sum_j \gamma_{ji} v_j \tag{3.31g}$$

$\Delta_{ij} = p(X = i|V = j)$

$$\Delta_{ij} = \frac{\delta_{ij} p_i}{v_j} \tag{3.31h}$$

$\xi_i j = p(X = i|U = j)$

$$\xi_{ij} = \frac{\sum_k \gamma_{kj} \delta_{ik} p_i}{u_j} \tag{3.31i}$$

$$\omega_{ij} = P(U = j|X = i)$$

$$\omega_{ij} = \frac{\xi_{ij} u_j}{p_i} \tag{3.31j}$$

$$\begin{aligned} R > &(1 - \alpha)(p_0 \log_2 \frac{1}{p_0} + p_1 \log_2 \frac{1}{p_1}) - \\ &- (1 - \alpha)(\sum_i v_i(\Delta_{0i} \log_2 \frac{1}{\Delta_{0i}} + (1 - \Delta_{0i}) \log_2 \frac{1}{1 - \Delta_{0i}})) \end{aligned} \tag{3.31k}$$

$$D_b \geq E[d_b(X, \phi(B, V))] \tag{3.31l}$$

(information noisiness constraint)

$$\begin{aligned}
&-\sum_j \alpha\omega_{0j}p_0 \log_2 \frac{\alpha\omega_{0j}p_0}{u_j} + \alpha\omega_{0j}p_1 \log_2 \frac{\alpha\omega_{1j}p_1}{u_j} + \\
&(1-\alpha)(\omega_{0j}p_0 + \omega_{1j}p_1) \log_2 \frac{(1-\alpha)(\omega_{0j}p_0 + \omega_{1j}p_1)}{u_j} + \\
&\sum_{i,k} \alpha\gamma_{ik}\delta_{0i}p_0 \log_2 \frac{\alpha\gamma_{ik}\delta_{0i}p_0}{u_k} + \alpha\gamma_{ik}\delta_{1i}p_1 \log_2 \frac{\alpha\gamma_{ik}\delta_{1i}p_1}{u_k} + \\
&(1-\alpha)(\gamma_{ik}\delta_{0i}p_0 + \gamma_{ik}\delta_{1i}p_1) \log_2 \frac{(1-\alpha)(\gamma_{ik}\delta_{0i}p_0 + \gamma_{ik}\delta_{1i}p_1)}{u_k} > \\
&-\sum_j \beta\omega_{0j}p_0 \log_2 \frac{\beta\omega_{0j}p_0}{u_j} + \beta\omega_{0j}p_1 \log_2 \frac{\beta\omega_{1j}p_1}{u_j} + \\
&(1-\beta)(\omega_{0j}p_0 + \omega_{1j}p_1) \log_2 \frac{(1-\beta)(\omega_{0j}p + \omega_{1j}p_1)}{u_j} + \\
&\sum_{i,k} \beta\gamma_{ik}\delta_{0i}p_0 \log_2 \frac{\beta\gamma_{ik}\delta_{0i}p_0}{u_k} + \beta\gamma_{ik}\delta_{1i}p_1 \log_2 \frac{\beta\gamma_{ik}\delta_{1i}p_1}{u_k} + \\
&(1-\beta)(\gamma_{ik}\delta_{0i}p_0 + \gamma_{ik}\delta_{1i}p_1) \log_2 \frac{(1-\beta)(\gamma_{ik}\delta_{0i}p_0 + \gamma_{ik}\delta_{1i}p_1)}{u_k}
\end{aligned} \tag{3.31m}$$

3.6 Binary Deletion Channel Example Using Equivocation Measure

the problem set-up is the same as the previous section, formulas explained previously are omitted. The transition probabilities, as in the previous section, are shown in figure 3.3. In this section this type of channel is considered using the theorem 6 states that:

$$R \geq I(V; X|B) \tag{3.32a}$$

$$D_b \geq E[d(X, \hat{X}(V, B))] \tag{3.32b}$$

$$\Delta \leq [H(X|V, B) + I(X; B|U) - I(X; W|U)]_+ \tag{3.32c}$$

The formulas are derived from the general case.

Δ parameter Constraint

as $H(X|V,B)$ was computed in the previous section only $I(X;B|U) - I(X;W|U)$ is shown

$$\begin{aligned} &I(X;B|U) - I(X;W|U) = \\ &= H(X|U) + H(B|U) - H(X,B|U) - (H(X|U) + H(W|U) - H(X,W|U)) \\ &= H(B|U) - H(X,B|U) - (H(W|U) - H(X,W|U)) \end{aligned} \tag{3.33}$$

The entropies are computed in the following section.

$$\begin{aligned} &H(X,B|U) = \\ &= -\sum_i P(U=i) \sum_{i,k} P(X=j,B=k|U=i) \log_2 P(X=j,B=k|U=i) = \\ &= \sum_{i,k,j} P(U=i|X=j)P(B=k|X=j)P(X=j) \\ &\log_2 \frac{P(U=i|X=j)P(B=k|X=j)P(X=j)}{P(U=i)} = \\ &\sum_i P(U=i|X=0)P(B=0|X=0)P(X=0) \\ &\log_2 \frac{P(U=i|X=0)P(B=0|X=0)P(X=0)}{P(U=i)} + \\ &+ P(U=i|X=0)P(B=e|X=0)P(X=0) \\ &\log_2 \frac{P(U=i|X=0)P(B=e|X=0)P(X=0)}{P(U=i)} + \\ &+ P(U=i|X=1)P(B=1|X=1)P(X=1) \\ &\log_2 \frac{P(U=i|X=1)P(B=1|X=1)P(X=1)}{P(U=i)} + \\ &+ P(U=i|X=1)P(B=e|X=1)P(X=1) \\ &\log_2 \frac{P(U=i|X=1)P(B=e|X=1)P(X=1)}{P(U=i)} \end{aligned} \tag{3.34}$$

3.6.1 Problem definition

The constraints are shown in the following section as an optimization problem, using the composition of the results of the previous section, by using proxy variables to make the formulas more readable (defined in the same way as in the

previous problem). Analogously to the previous problem, we decide to maximize Δ.

Constants

$\alpha, \beta, \phi, D_b, p$

Problem

$$
\begin{aligned}
&\Delta = \\
&\max\{ -(1-\alpha)\sum_{i,k} \Delta_{ki} v_i \log \Delta_{ki} + (1-\alpha)\sum_i v_i h(\Delta_{ki}) \\
&\quad -\sum_j (\alpha\xi_{0,j}p_0)\log\frac{\alpha\xi_{0,j}p_0}{u_j} + (\alpha\xi_{1,j}p_1)\log\frac{\alpha\xi_{1,j}p_1}{u_j} + \\
&\quad ((1-\alpha)\xi_{0,j}p_0 + (1-\alpha)\xi_{1j}p_1) \\
&\quad \log\frac{(1-\alpha)\xi_{0,j}p_0 + (1-\alpha)\xi_{1j}p_1}{u_j} \\
&\quad \sum_{i,(j,k)\in[(0,e),(1,e)]} \omega_{ji}(1-\alpha)p_j \ \log_2\frac{\omega_{ji}(1-\alpha)p_j}{u_i} + \\
&\quad \sum_{i,(j,k)\in[(0,0),(1,1)]} \omega_{ji}\alpha p_j \ \log_2\frac{\omega_{ji}\alpha p_j}{u_i} \\
&\quad -(-\sum_j (\beta\xi_{0,j}p_0)\log\frac{\beta\xi_{0,j}p_0}{u_j} + (\beta\xi_{1,j}p_1)\log\frac{\beta\xi_{1,j}p_1}{u_j} + \\
&\quad ((1-\beta)\xi_{0,j}p_0 + (1-\beta)\xi_{1j}p_1) \\
&\quad \log\frac{(1-\beta)\xi_{0,j}p_0 + (1-\beta)\xi_{1j}p_1}{u_j} \\
&\quad \sum_{i,(j,k)\in[(0,e),(1,e)]} \omega_{ji}(1-\beta)p_j \ \log_2\frac{\omega_{ji}(1-\beta)p_j}{u_i} + \\
&\quad \sum_{i,(j,k)\in[(0,0),(1,1)]} \omega_{ji}\beta p_j \ \log_2\frac{\omega_{ji}\beta p_j}{u_i})\}
\end{aligned}
\tag{3.35}
$$

s.t.

$$\delta_{ij} \in [0,1], i \in [0,1], j \in [1,3] \tag{3.36a}$$

$$\gamma_{ij} \in [0,1], i \in [1,3], j \in [1,3] \tag{3.36b}$$

$$p_0 = p, p_1 = 1 - p_0 \tag{3.36c}$$

$$\sum_i \delta_{ki} = 1 \tag{3.36d}$$

$$\sum_i \gamma_{ki} = 1 \tag{3.36e}$$

$$v_i = \sum_{j=0,1} \delta_{ji} p_j \tag{3.36f}$$

$$u_i = \sum_j \gamma_{ji} v_j \tag{3.36g}$$

$$\Delta_{ij} = \frac{\delta_{ij} p_i}{v_j} \tag{3.36h}$$

$$\xi_{ij} = \frac{\sum_k \gamma_{kj} \delta_{ik} p_i}{u_j} \tag{3.36i}$$

$$\omega_{ij} = \frac{\xi_{ij} u_j}{p_i} \tag{3.36j}$$

$$\begin{aligned} R >& (1-\alpha)(p_0 \log_2 \frac{1}{p_0} + p_1 \log_2 \frac{1}{p_1}) - \\ & - (1-\alpha)(\sum_i v_i(\Delta_{0i} \log_2 \frac{1}{\Delta_{0i}} + (1-\Delta_{0i}) \log_2 \frac{1}{1-\Delta_{0i}})) \end{aligned} \tag{3.36k}$$

$$D_b \geq E[d_b(X, \phi(B, V))] \tag{3.36l}$$

3.6.2 Side information B is less noisy than side information W

Using the same metric as previous section but we assume side-information B is less noisy than side information W, therefore using theorem 7 Most of the formulas are analogous to previous examples, therefore omitted here

$$I(U;B) \geq I(U;W) \Rightarrow H(B) - H(U,B) \geq H(W) - H(U,W) \tag{3.37a}$$

$$\begin{aligned} & H(U,B) = -\sum_{i,j}(\sum_k P(U=i|X=k)P(B=j|X=k)P(X=k)) \\ & \log_2 \sum_k P(U=i|X=k)P(B=j|X=k)P(X=k) = \end{aligned} \tag{3.37b}$$

where $(j,k) \in [(0,0),(1,1),(e,0),(e,1)]$

$$\Delta \leq [H(X|VB) + I(X;B) - I(X;E)]_+ \tag{3.37c}$$

$$H(X,B) = -\sum_{i\in[0,1],j\in[i,e]} P(B=j|X=i)P(X=i) \log_2 P(B=j|X=i)P(X=i) \tag{3.37d}$$

3.6.3 Problem definition (side information B is less noisy than side information W)

The previous formulas are shown in the form of an optimization problem

Constants

$\alpha, \beta, \phi, D_b, p$

Problem

$$\begin{aligned}\Delta = \\ \max\{&-(1-\alpha)(\sum_i v_i(\Delta_{0i}\log_2\frac{1}{\Delta_{0i}} + (1-\Delta_{0i})\log_2\frac{1}{1-\Delta_{0i}})) \\ &-(\sum_i b_i \log_2 b_i) - (-\sum_i \alpha p_i \log_2 \alpha p_i + (1-\alpha)p_i \log_2((1-\alpha)p_i)) \\ &-((-\sum_i w_i \log_2 w_i) - (-\sum_i \beta p_i \log_2(\beta p_i) + (1-\beta)p_i \log_2((1-\beta)p_i)))\}\end{aligned} \tag{3.38}$$

s.t

$$\delta_{ij} \in [0,1], i \in [0,1], j \in [1,3] \tag{3.39a}$$

$$\gamma_{ij} \in [0,1], i \in [1,3], j \in [1,3] \tag{3.39b}$$

$$p_0 = p, p_1 = 1 - p_0 \tag{3.39c}$$

$$\sum_i \delta_{ki} = 1 \tag{3.39d}$$

$$\sum_i \gamma_{ki} = 1 \tag{3.39e}$$

$$v_i = \sum_{j=0,1} \delta_{ji} p_j \tag{3.39f}$$

$$u_i = \sum_j \gamma_{ji} v_j \tag{3.39g}$$

$$\Delta_{ij} = \frac{\delta_{ij} p_i}{v_j} \tag{3.39h}$$

$$\xi_{ij} = \frac{\sum_k \gamma_{kj}\delta_{ik}p_i}{u_j} \tag{3.39i}$$

$$\omega_{ij} = \frac{\xi_{ij}u_j}{p_i} \tag{3.39j}$$

(Noisiness contraint)

$$\begin{aligned}
&-(\alpha p_0 \log_2 \alpha p_0 + \alpha p_1 \log_2 \alpha p_1 + (1-\alpha)(p_1+p_0)\log_2 (1-\alpha)(p_1+p_0)) \\
&+\sum_i ((\sum_{j\in[0,1]} \omega_{ij}(1-\alpha)p_j \log_2 \sum_{j\in[0,1]} \omega_{ij}(1-\alpha)p_j) \\
&+\omega_{i0}\alpha p_0 \log_2 \omega_{i0}\alpha p_0) \\
&+\omega_{i1}\alpha p_1 \log_2 \omega_{i1}\alpha p_1) > \\
&-(\beta p_0 \log_2 \beta p_0 + \beta p_1 \log_2 \beta p_1 + (1-\beta)(p_1+p_0)\log_2 (1-\beta)(p_1+p_0)) \\
&+\sum_i ((\sum_{j\in[0,1]} \omega_{ij}(1-\beta)p_j \log_2 \sum_{j\in[0,1]} \omega_{ij}(1-\beta)p_j) \\
&+\omega_{i0}\beta p_0 \log_2 \omega_{i0}\beta p_0) \\
&+\omega_{i1}\beta p_1 \log_2 \omega_{i1}\beta p_1)
\end{aligned} \tag{3.39k}$$

$$\begin{aligned}
R >& (1-\alpha)(p_0 \log_2 \frac{1}{p_0} + p_1 \log_2 \frac{1}{p_1}) - \\
&- (1-\alpha)(\sum_i v_i(\Delta_{0i}\log_2 \frac{1}{\Delta_{0i}} + (1-\Delta_{0i})\log_2 \frac{1}{1-\Delta_{0i}}))
\end{aligned} \tag{3.39l}$$

$$D_b \geq E[d_b(X, \phi(B,V))] \tag{3.39m}$$

3.7 Secret key capacity

We want to compute C_{sk}^{low} for the optimization solution, defined as

$$C_{sk}^{low} = I(s_a; s_b) - \min\{I(s_a; s_e), I(s_b; s_e)\} \tag{3.40}$$

The formulas for the binary deletion channel needed for the examples in sections 3.5.1 and 3.6.3 are omitted, as the value X must be the value of W or B if either of them is in $\{0,1\}$, otherwise its value is either 0 or 1 if W and B are equal to e, but the formulas remain almost the same.

C_{sk}^{low} is computed as explained next:

$$s_a = \{X\} \tag{3.41a}$$

$s_b = \{M, B\} = \{U, V, B\}$

We assume Bob is able to decode both U and V using side information B

(3.41b)

$s_e = \{M, B\} = \{U, B\}$

We assume Eve is able to decode only U using side information W (3.41c)

$$I(s_a; s_b) = H(s_a) + H(s_b) - H(s_a, s_b) \tag{3.41d}$$

$$I(s_a; s_e) = H(s_a) + H(s_e) - H(s_a, s_e) \tag{3.41e}$$

$$I(s_e; s_b) = H(s_e) + H(s_b) - H(s_e, s_b) \tag{3.41f}$$

$$H(s_a) = H(X) \tag{3.41g}$$

$$\begin{aligned} H(s_b) = H(U, V, B) = \\ = -\sum_{i,j,k} p(U = i, V = j, B = k) \log_2 p(U = i, V = j, B = k) \\ = -\sum_{i,j,k} (\sum_{l} p(B = k|X = l) p(U = i|V = j) p(V = j|X = l) p(X = l)) \\ \log_2 \sum_{l} p(B = k|X = l) p(U = i|V = j) p(V = j|X = l) p(X = l) \end{aligned} \tag{3.41h}$$

$$\begin{aligned} H(s_e) = H(U, W) = \\ - \sum_{ij} P(U = i, W = j) \log_2 P(U = i, W = j) = \\ - \sum_{ij} \left(\sum_{kl} P(U = i|V = k) P(V = k|X = l) P(W = j|X = l) P(X = l) \right) \\ \log_2 \left(\sum_{kl} P(U = i|V = k) P(V = k|X = l) P(W = j|X = l) P(X = l) \right) \end{aligned} \tag{3.41i}$$

$$
\begin{aligned}
H(s_a, s_e) = H(U, X, W) = \\
&- \sum_{ijl} P(U = i, W = j, X = l) \log_2 P(U = i, W = j, X = l) = \\
&- \sum_{ij} \left(\sum_{k} P(U = i|V = k) P(V = k|X = l) P(W = j|X = l) P(X = l) \right) \\
&\log_2 \left(\sum_{k} P(U = i|V = k) P(V = k|X = l) P(W = j|X = l) P(X = l) \right)
\end{aligned}
\tag{3.41j}
$$

$$
\begin{aligned}
H(s_a, s_b) = H(U, V, X, B) = \\
&= - \sum_{i,j,k,l} p(U = i, V = j, B = k, X = l) \log_2 p(U = i, V = j, B = k, X = l) \\
&= - \sum_{i,j,k,l} p(B = k|X = l) p(U = i|V = j) p(V = j|X = l) p(X = l) \\
&\log_2 p(B = k|X = l) p(U = i|V = j) p(V = j|X = l) p(X = l)
\end{aligned}
\tag{3.41k}
$$

$$
\begin{aligned}
H(s_b, s_e) = H(U, V, W, B) = \\
&= - \sum_{i,j,k,l} p(U = i, V = j, B = k, W = l) \log_2 p(U = i, V = j, B = k, X = l) \\
&= - \sum_{i,j,k,l} (\sum_{c} p(B = k|X = c) p(W = k|X = c) \\
&p(U = i|V = j) p(V = j|X = c) p(X = c)) \\
&\log_2 \sum_{c} p(B = k|X = c) p(W = l|X = c) p(B = k|X = c) \\
&p(U = i|V = j) p(V = j|X = c) p(X = c)
\end{aligned}
\tag{3.41l}
$$

3.8 Secret key capacity with R=0

We now consider the case in which no message is shared during the information reconciliation stage, therefore the information is used as is, at most converted to binary in the case of deletion. This formulas are needed to have a reference of the performance of the metrics.

$$s_a = \{X\} \tag{3.42a}$$

$$s_b = \{B\} \tag{3.42b}$$

$$s_e = \{W\} \tag{3.42c}$$

The formulas are analogous to the previous case

$$H(s_a) = H(X) \tag{3.43a}$$

$$H(s_b) = H(B) \tag{3.43b}$$

$$H(s_e) = H(W) \tag{3.43c}$$

$$H(s_a, s_e)\text{analogous to } H(s_a, s_b) \tag{3.43d}$$

$$\begin{aligned} H(s_a, s_b) = H(X, B) = \\ = -\sum_{k,l} P(B = k, X = l) \log_2 P(B = k, X = l) \\ = -\sum_{k,l} P(B = k|X = l)P(X = l) \\ \log_2 P(B = k|X = l)P(X = l) \end{aligned} \tag{3.43e}$$

$$\begin{aligned} H(s_b, s_e) = H(W, B) = \\ = -\sum_{k,l} P(B = k, W = l) \log_2 P(B = k, X = l) \\ = -\sum_{i,j,k,l} (\sum_{c} P(B = k|X = c)P(W = k|X = c) \\ P(X = c))log_2 \sum_{c} P(W = l|X = c)P(B = k|X = c)P(X = c) \end{aligned} \tag{3.43f}$$

Chapter 4

Numerical Results

In the following section the optimization problems obtained in chapter 3 are solved and the plots of the resulting values are shown. In the case of ambiguous values of the function only the maximum is shown (such as the values for different values of the ϕ function)

4.1 Reproducing Results of [1]

for validation purpose and check if the code is working correctly, the plots in [1] are going to be reproduced, using the formulas from section 3.1. As shown in figure 4.2, where we reproduce the inner bound of the distortion at Eve D_w, by fixing the transition parameters for the side information α and β. Leaving R unbound, we maximize D_w to reproduce the results in [1], by iterating over the values of p, with the constraint $I(X;B|U) > I(X;W|U)$. As expected the distortion is non-decreasing as a function of the entropy of the source, as this is a increasing function of p, for $p \in (0, 0.5]$. However, since distortion function in the optimization problem contains a min between a constant and two variables, the result saturates after a certain value, which in figure 4.2 corresponds to the transition probability.

4.2 Numerical Results For Binary Deletion Channel Example Using Rate-distortion Metric

In this section the optimization problem is taken from section 3.5.1. In order to find these values, without a fixed value of D_b and ϕ the optimization is computed

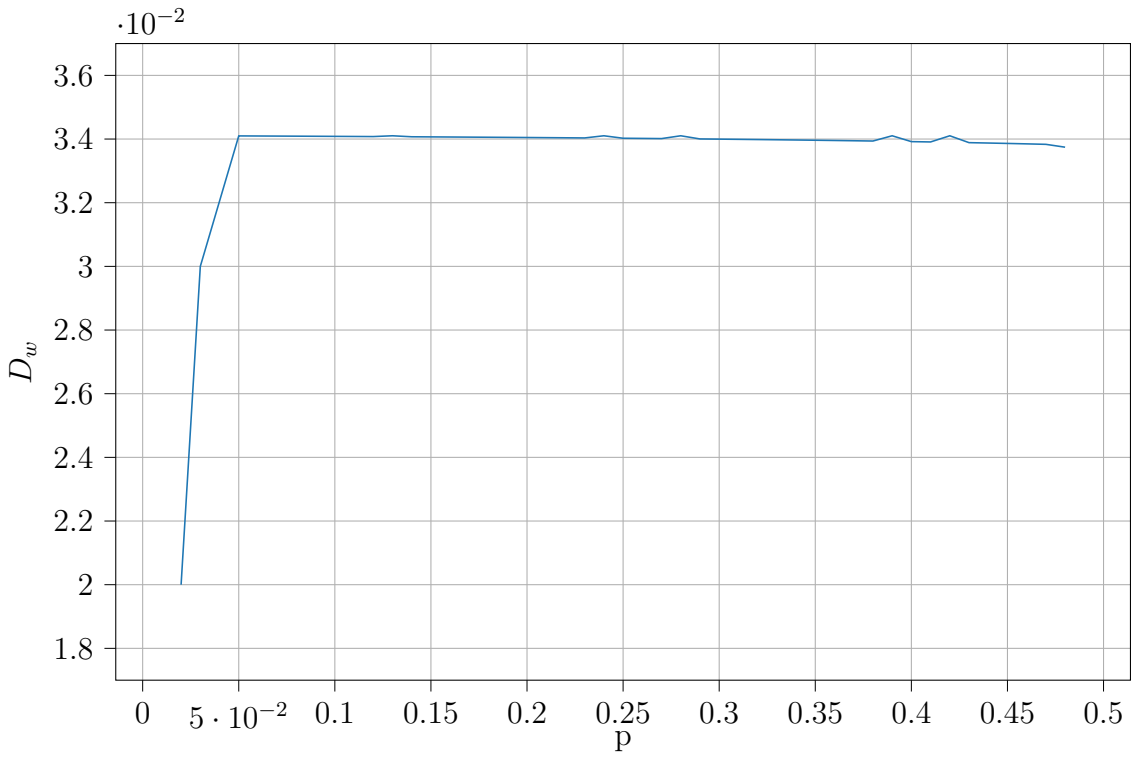

Figure 4.1: result of the optimization problem from example in [1] with $\alpha = 0.4$,$beta = 0.04$

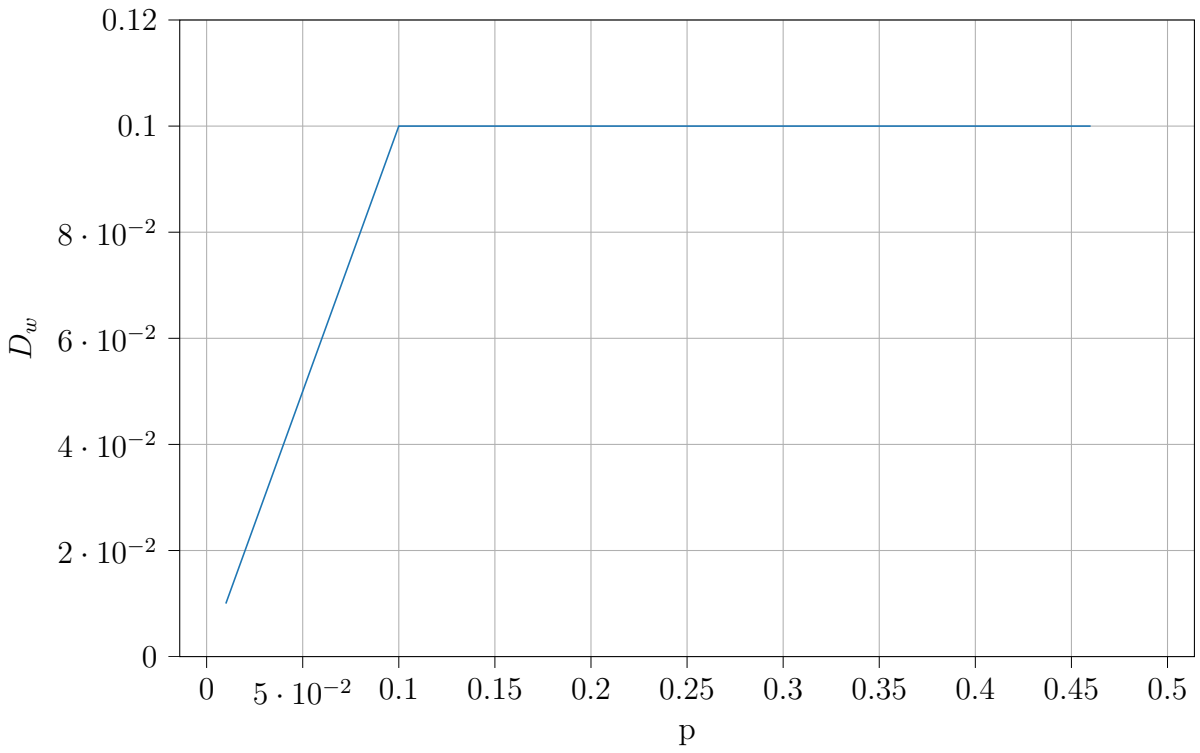

Figure 4.2: result of the optimization problem from example in [1] with $\alpha = 0.4$,$\beta = 0.1$

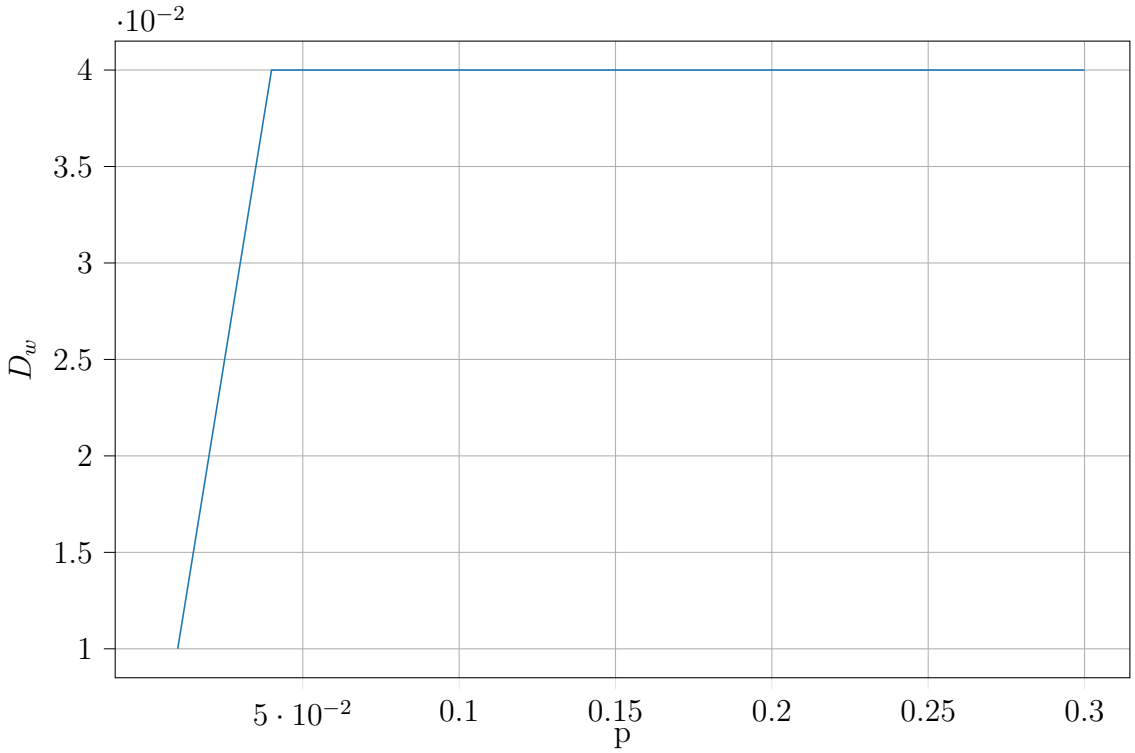

Figure 4.3: result of the upper bound of the optimization problem in [1] with $\alpha = 0.6$,$beta = 0.96$

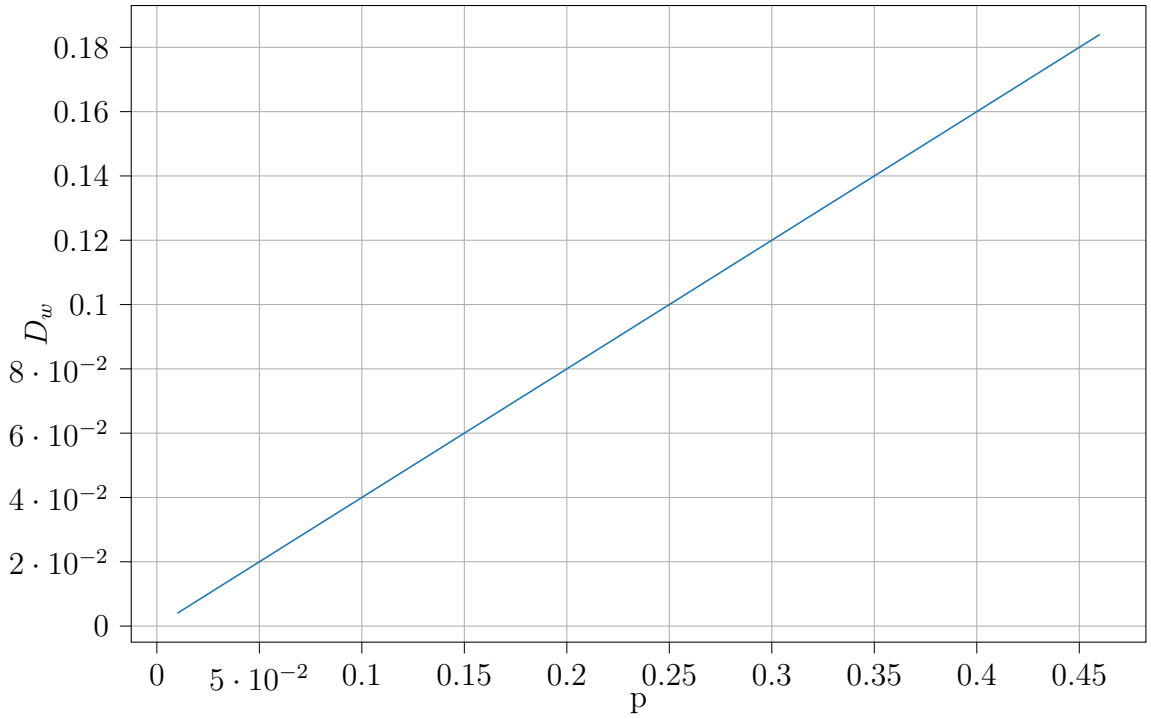

Figure 4.4: result of the optimization problem in 3.5.1 with $\alpha = 0.6$,$\beta = 0.9$

as explained in the following:

1. fix α and β
2. iterate over the values of $p = P(X = 0) \in [0.01, 0.5]$ as the entropy of the source is higher the most p is close to 0.5
3. for each p iterate over the possible ϕ functions(which in our case are $2^{||V||\cdot||B||}$, as the number of lines in the lookup table is determined by the number of V and U symbols combinations), which determines the value of D_b
4. for each ϕ iterate over the valid values of $D_b \in [0, 1]$ as X and Y are binary
5. compute the optimization of D_w for these values

This order of operation was determined so that, starting from a point where the distributions of δ_{ij} and γ_{ij} are uniform, at every step a better starting point for the optimization can be determined by adding one constraint at a time. R is not part of the optimization constraints in the program and is calcultated afterwards In figure 4.4 are shown the results of the optimization of the problem in section 3.5

4.3 Numerical Results For Binary Deletion Channel Example Using The Equivocation Metric

The optimization is computed analogously to the previous section, using formulas from section 3.6.3, by optimizing the Δ parameter. As we can see, the value converges to the value with $R = 0$, since the maximum equivocation is in the case that U carries no information about X.

4.4 Numerical results of the Secret key capacity

By optimizing the two metrics the following results are obtained by computing the skc using the obtained distribution from the optimization. As expected, since the value of the Δ and D_w parameters converge on the value with $R = 0$, the value of skcs are close to the value for $R = 0$.

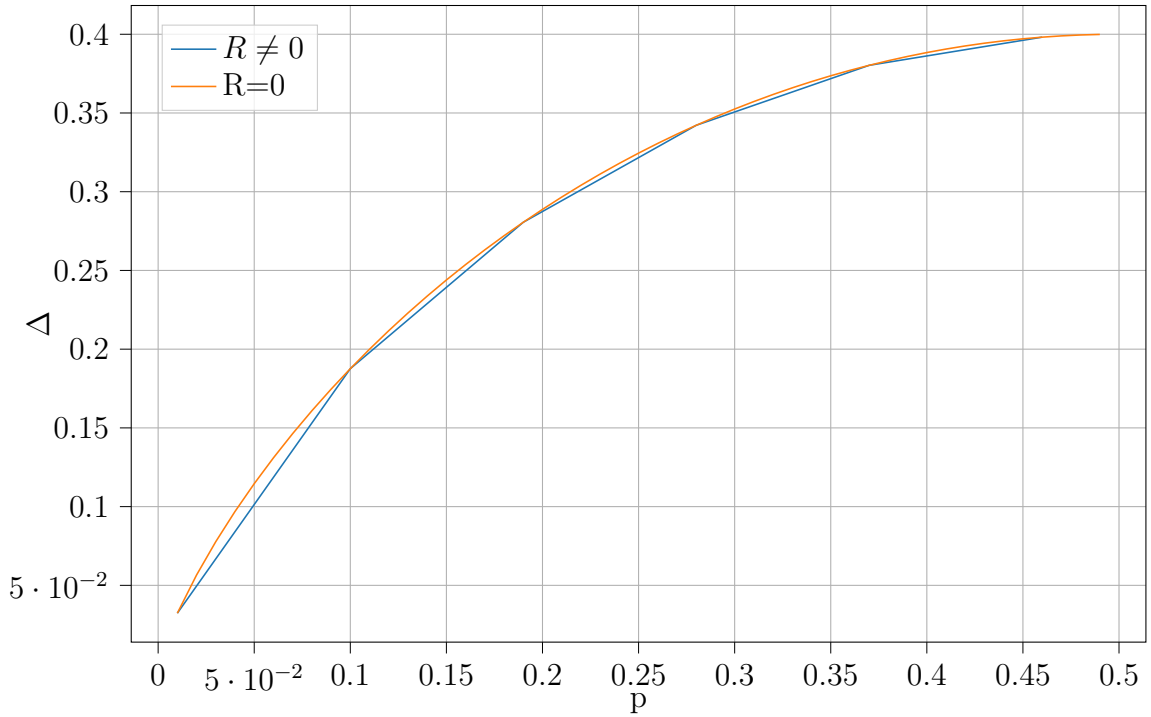

Figure 4.5: result of the optimization problem in 3.6.3 with $\alpha = 0.9$,$beta = 0.6$

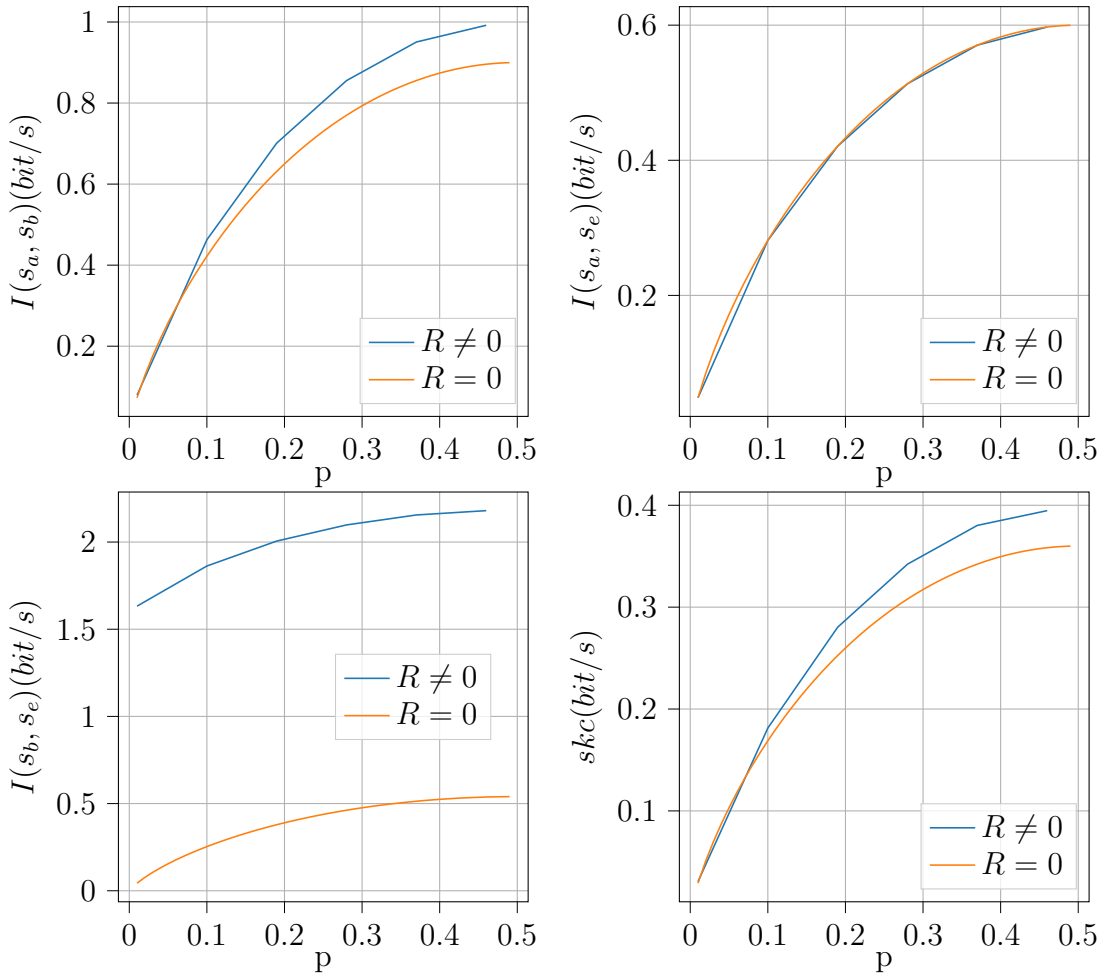

Figure 4.6: Results with the distortion measure $\alpha = 0.9$ and $\beta = 0.6$

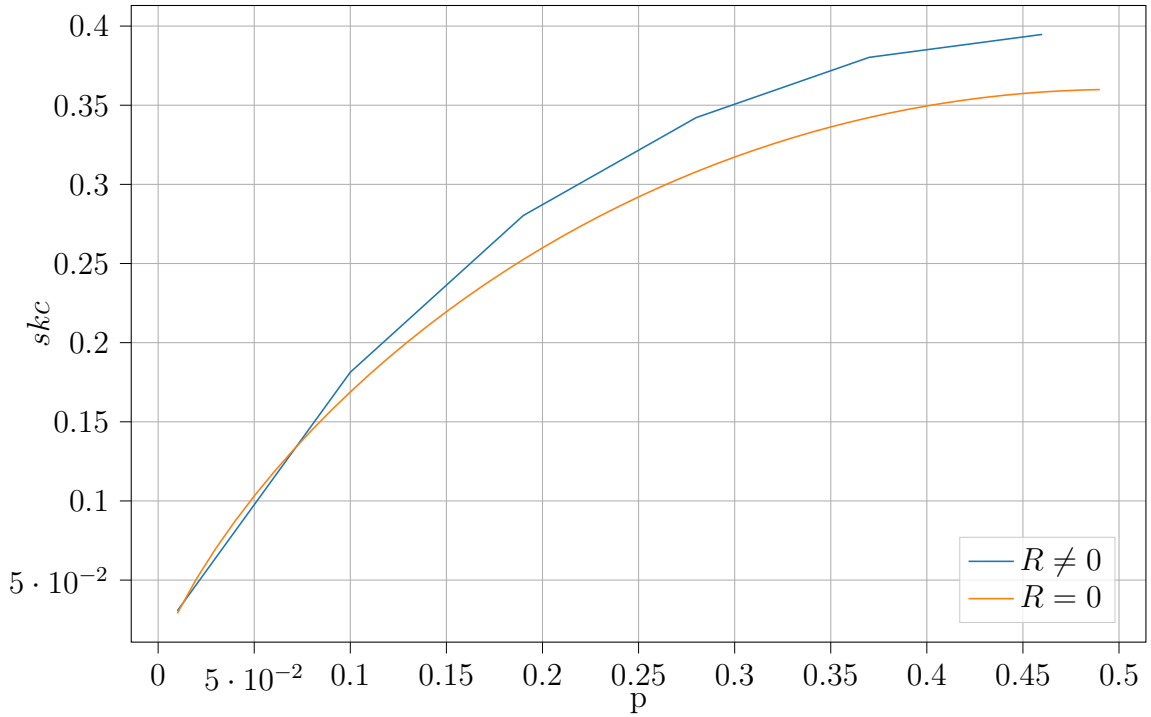

Figure 4.7: skc with the distortion metric $\alpha = 0.9$ and $\beta = 0.6$

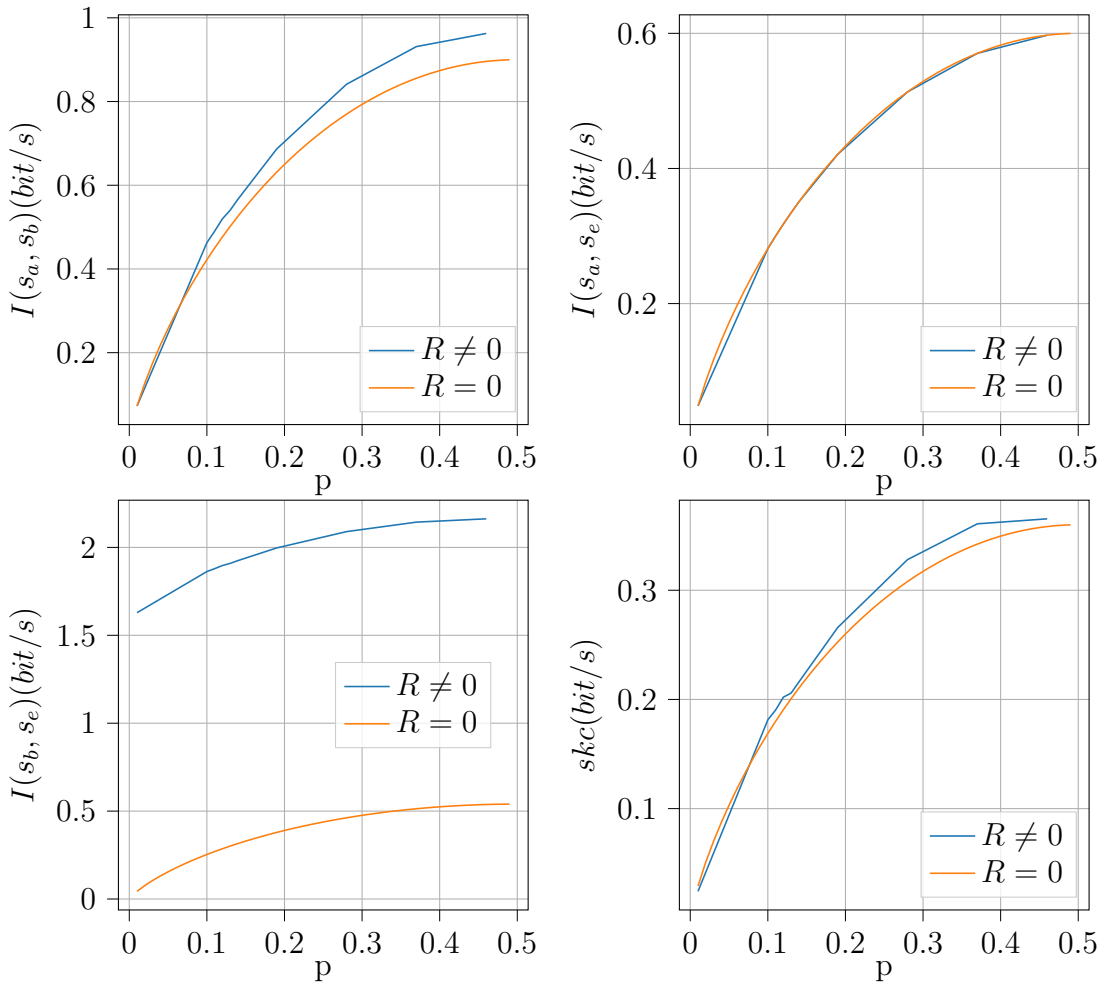

Figure 4.8: Results with equivocation measure $\alpha = 0.9$ and $\beta = 0.6$

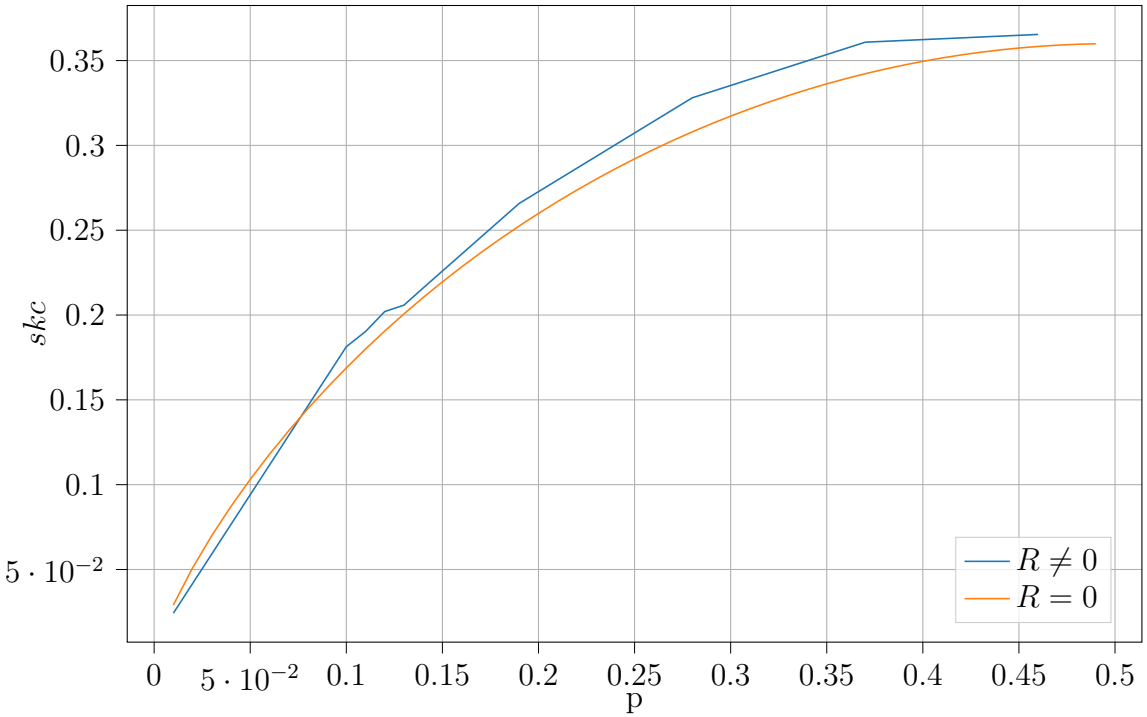

Figure 4.9: skc with equivocation metric $\alpha = 0.9$ and $\beta = 0.6$

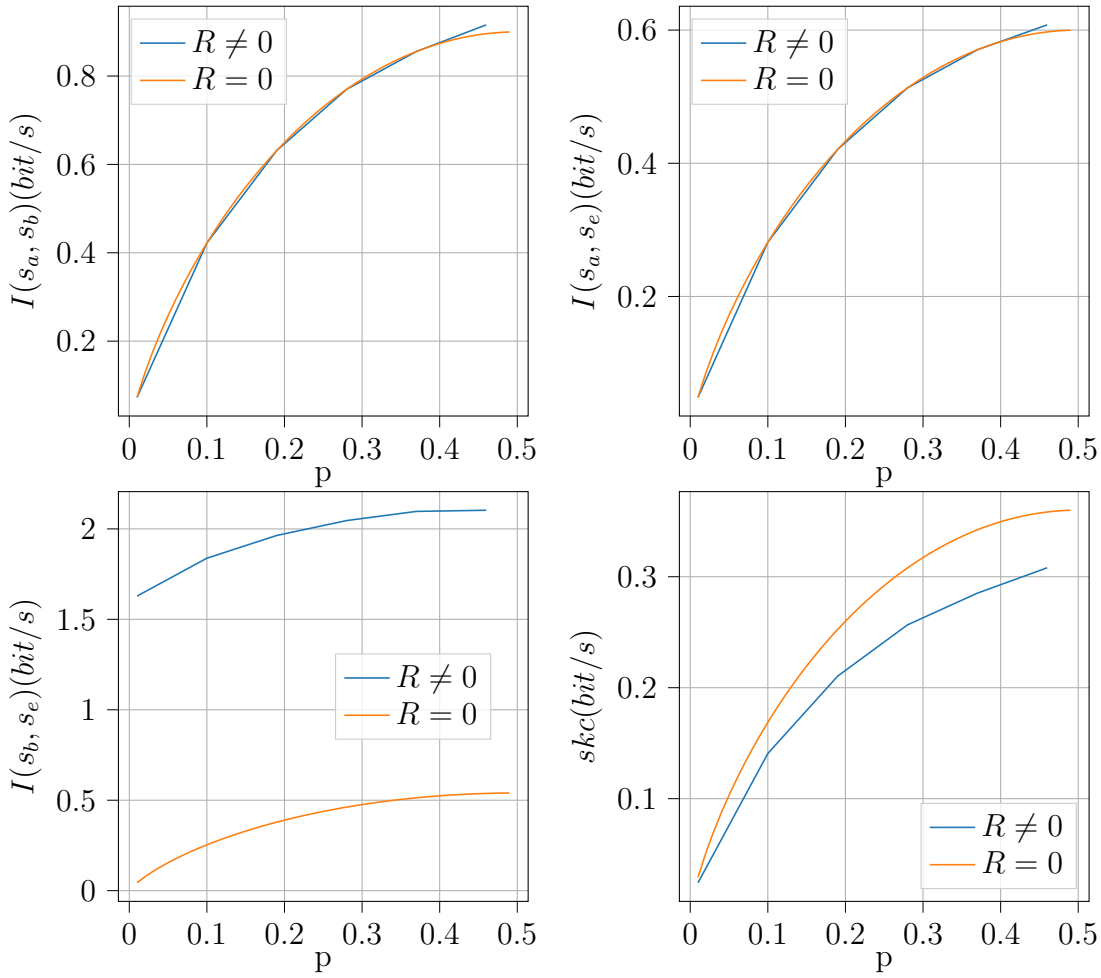

Figure 4.10: Results with entropy measure $\alpha = 0.9$ and $\beta = 0.6$ with constraints on the noise power

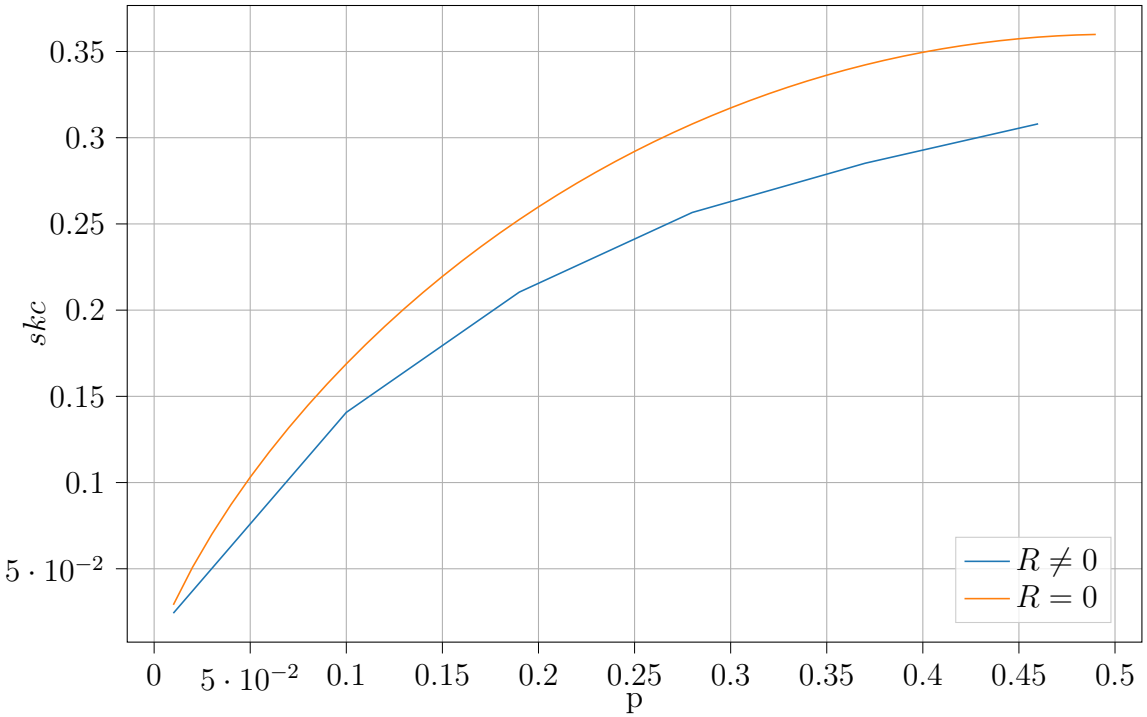

Figure 4.11: skc using entropy metric $\alpha = 0.9$ and $\beta = 0.6$ with constraints on the noise power

Chapter 5

Conclusions

From the results in the simple case shown in Chapter 4, the secret key capacity with $R \neq 0$ is higher than the one with $R = 0$. In particular both the distortion and equivocation metric converge to the value they have with $R = 0$, as the metrics focus mostly on the correlation between W and U to achieve secrecy, whereas uses V and X for the distortion at Bob. These constraints and the setup of the problem, allow U to converge to a transition probability such that it does not carry any information about X, as we can see in the plot of $I(s_a, s_e)$, as this is the same if $R = 0$ or $R \neq 0$.

This also shows that these schemes don't have a performance advantage significantly higher than without any information reconciliation. It is also to note that, unlike what was expected from the power constraints, the secret key capacity obtained with Theorem 7 is lower than the one obtained with Theorem 6. However, it must be considered that these theorems are meant for the case in which U and V as an embedding of X, whereas the simple cases considered use $\|U\| = \|V\| = 3 > \|X\| = 2$.

Bibliography

[1] E.C. Song, P. Cuff, H.V. Poor *A rate-distortion base secrecy system with side information at the decoders*,52nd Annual Allerton Conference on Communication, Control, and Computing, pp 755-761, Oct. 2014

[2] J. Villard, P. Piantanida, *Secure lossy source coding with side information at the decoders*,48th Annual Allerton Conference on Communication, Control, and Computing, pp 733-739, Oct. 2010

[3] M. Adil,S. Wyne,S.J. Nawaz *On Quatization for Secret Key Generation From Wireless Channel Samples*,IEEE-Access, pp. 21654-21668, Jan. 2021

[4] F. Ardizzon, F.Giurisato, S.Tomasin, *Secret-Key-Agreement Advantage Distillation with Shared Quantization Correction*, Communication Letters, pp 1-5, 2023

[5] J. Zhang, T.Q. Duong, R. Woods, A. Marshall, *Key generation from wireless channels: a survey and practical implementation* (Telecommunications, 2017), 'Trusted Communications with Physical Layer Security for 5G and Beyond', Chap. 18, pp. 457-474

[6] T.M. Cover and J.A. Thomas. Year. 'Network Information Theory', *Elements of Information Theory Second Edition*, Wiley-Interscience, 2006, pp 509-611