Information-theoretic security from correlated signals

Yicheng CUI
Supervisor: Amin GOHARI

November 2023

Abstract

Information-theoretic security has been considered to be the most ideal type of security. It is known by its robustness to eavesdropping. Many researchers have been theoretically proving the upper bound and the lower bound of the secret key capacity. In this project, we considered information-theoretic security in source model, focused on the upper bound of the secret key capacity and did some simulations with binary correlated sources and logic function XOR and AND. More precisely, we tried to find the convex hull of each scenario to help us estimate the upper bound of the secret key capacity.

1 Introduction

The most ideal type of security is information-theoretic security, which makes no assumptions about the adversary's computational capability. This question is pioneered by Shannon[7]. He considered communication of a message M from Alice to Bob over a noiseless public broadcast channel in the presence of an eavesdropper who observes the channel output L. Alice and Bob

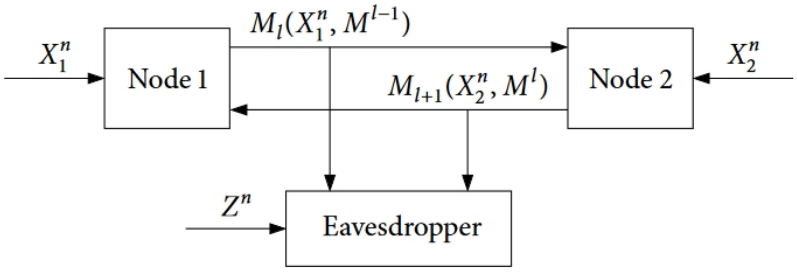

Figure 1: Source model

share a key, which is unknown to the eavesdropper, and they can use it to encrypt M into L and vice versa. Shannon showed that to achieve perfect secrecy, that is information leakage $I(M;L) = 0$, the size of the key must be at least as large as the size of the message, i.e., $H(K) \geq H(M)$.

We focus on the secret key agreement problem. Suppose that the sender and the receiver observe correlated sources. Then it turns out that they can agree on a secret key through interactive communication over a public channel that the eavesdropper has complete access to. We will discuss this key agreement scheme under the source model.

Consider a network with two sender-receiver nodes, an eavesdropper, and a 3-DMS (X, Y, Z) as depicted in the figure below. Node 1 observes the DMS X, node 2 observes Y and the eavesdropper observes Z. Nodes 1 and 2 communicate through a noiseless broadcast channel, to which the eavesdropper has complete access. Our goal is to agree on a key that the eavesdropper has almost no information about and we want to find the maximum achievable secret key rate. Suppose that the nodes communicate in a round-robin fashion and node 1 transmits first, i.e., node 1 transmits during the odd rounds and node 2 transmits during even rounds[4].

Define a key agreement code to be $(2^{nr_1}, 2^{nr_2}, ..., 2^{nr_n}, n)$, consisting of two randomized encoders and two decoders. In odd rounds, encoder 1 generates an index $M_l \in [1 : 2^{nr_l}]$, where l is the number of the round, according to its source vector and all previously transmitted indices, i.e., $M_l = f_l(X^n, M_{l-1})$. In even rounds, encoder 2 generates an index $M_l \in [1 : 2^{nr_l}]$, according to its source vector and all previously transmitted indices, i.e., $M_l = f_l(Y^n, M_{l-1})$. Decoder 1 generates a key K_1, decoder 2 generates a key K_2, according to a conditional pmf $p(k_j|m^q, x_j^n)$, i.e, the key depends on its source sequence and all received indices[7].

The probability of the key agreement error is defined as $P_e^{(n)} = P(K_A \neq K_B)$, The key leakage rate is defined as $R_L^{(n)} = \max_{j\in 1,2}(1/n)I(K_j; Z^n, M^q)$. Define (R, R_L) to be the key rate-leakage pair. A key-leakage pair is said to be achievable if there exists a sequence of $(2^{nr_1}, 2^{nr_2}, ..., 2^{nr_n}, n)$ codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$, $\limsup_{n\to\infty} R_L^{(n)} \leq R_L$, and $\liminf_{n\to\infty}(1/n)H(K_j) \geq R$, for $j = 1, 2$. Define $\mathscr{R}^*$ to be the key rate-leakage region, which is the closure of the set of achievable rate-leakage pairs (R, R_L). Define $S(X; Y\|Z) = \max\{R : (R, 0) \in \mathscr{R}^*\}$ to be the secret key capacity[4]. One major research direction is to consider the upper bound and the lower bound of the secret key capacity. For semester 1, we would like to do some simulations on the upper bound of the secret key capacity, given the sources are binary and correlated. We will try to find out the lower convex envelops of different settings and try to find out the minimizer of each case.

2 Background

Pioneers have found lower bounds and upper bounds of secret key capacity. A lower bound of the secret key capacity is $S(X; Y\|Z) \geq I(X; Y) - I(X; Z)$, while an upper bound is $S(X; Y\|Z) \leq \min_J I(X; Y|J) + I(X, Y; Z|J)$[5],

where J is an auxiliary random variable. We can show later that the lower bound and the upper bound match each other if given DSBS sources and $Z = X \oplus Y$.

A lot of work related to the source model for the secret key capacity has been done by pioneers of in this field. The source model for the secret key agreement was introduced by Ahlswede and Csiszár[1], they also introduced the on-way secret key capacity. The one-round secret key capacity with rate constraint is due to Csiszár and Narayan[2]. Maurer and Wolf[6] provided an upper bound for the 2-node case. Gohari and Anantharam[5] established the lower bound on the secret key capacity for interactive key agreement between 2 nodes and its extension to multiple nodes. They also established a tighter upper bound[5].

3 Methodology

The way we tackle this problem is doing some simulations. With various resources and references, the simulation code is written in Python. To calculate the convex hull, We also refer to a GitHub repository[3].

4 Simulation Results

4.1 Source distributions and the relationship between Z and (X, Y)

In this section, we want to focus on the standard case of this problem. We assume that X and Y are binary and correlated. While at the same time, Z is also binary and is a function of X and Y.

$P(X=0,Y=0)=\alpha$	$P(X=0,Y=1)=\beta$
$P(X=1,Y=0)=\beta$	$P(X=1,Y=1)=\alpha$

Table 1: DSBS source

$P(X=0,Y=0)=\alpha$	$P(X=0,Y=1)=\beta$
$P(X=1,Y=0)=\beta$	$P(X=1,Y=1)=\gamma$

Table 2: Non-DSBS source

We are interested in the doubly symmetric binary source (DSBS), i.e., $P(X=0,Y=0)=P(X=1,Y=1)$, $P(X=0,Y=1)=P(X=1,Y=0)$. The distribution of this source is represented in Table 1.

In Table 1, $\alpha+\beta=0.5$, $0\leq\alpha\leq 1$ and $0\leq\beta\leq 1$.

We also would like to consider a non-DSBS source. This is just a little bit different from the DSBS source. We simply change the symmetric manner of the original DSBS source, and still keep some symmetric property of it. In this case, we choose to make one diagonal not symmetric anymore. The distribution of this source is represented in Table 2.

In Table 2, $\alpha+2\beta+\gamma=1$, $0\leq\alpha\leq 1$, $0\leq\beta\leq 1$ and $0\leq\gamma\leq 1$.

For the binary function $Z=f(X,Y)$, we will focus on two trivial cases. One is $Z=X\oplus Y$, the other is $Z=X\wedge Y$. Therefore, we have four cases to study in total: DSBS source with XOR function, DSBS source with AND function, non-DSBS source with XOR function and non-DSBS source with AND function. This can be organized in Table 2.

Before doing simulation, we would like to do a symmetrization argument first. Suppose P_{XY} is the distribution depicted in Table 1. J is an auxiliary random variable with support S_J, which is non-empty. Hence, $P_{XY}=$

a_1	b_1
c_1	d_1

Table 3: $P(XY|J=1)$

a_2	b_2
c_2	d_2

Table 4: $P(XY|J=2)$

$\sum_{i\in S_J} P(J=i)P(XY|J=i)$ and $\sum_{i\in S_J} P(J=i)=1$. For simplicity, consider $J\in\{1,2\}$. $P_{XY}=P(J=1)P(XY|J=1)+P(J=2)P(XY|J=2)$. Suppose $Z=X\wedge Y$ for example, and we consider the non-DSBS source. Suppose P_XY is the distribution depicted in Table 2. We would assume $P(XY|J)$ in Table 3 and Table 4.

By the property of DSBS source, we know that $P(J=1)b_1+P(J=2)b_2=P(J=1)c_1+P(J=2)c_2=\beta$. Therefore, we can flip the 2 distributions in Table 3 and 4. They are depicted in Tabel 5 and 6.

Let $P_1=P(J=1)$. Let $P_2=P(J=2)$. Hence, we know that $P(XY)=P_1*(Table3)+P_2*(Table4)=\frac{P_1}{2}*(Table3)+\frac{P_1}{2}*(Table5)+\frac{P_2}{2}*(Table4)+\frac{P_2}{2}*(Table6)$.

We can further combine Table 3 with Table 5, combine Table 4 and Table 6. We get Table 7 and Table 8.

We can get a representation $P_1*(Table7)+P_2*(Table8)$.

a_1	c_1
b_1	d_1

Table 5: Flipped $P(XY|J=1)$

a_2	c_2
b_2	d_2

Table 6: Flipped $P(XY|J=2)$

a_1	$\frac{b_1+c_1}{2}$
$\frac{b_1+c_1}{2}$	d_1

Table 7: Combined Table 3 and Table 5

By Jensen's Inequality, we have $P_1 * (Table7) + P_2 * (Table8) \leq \frac{P_1}{2} * (Table3) + \frac{P_1}{2} * (Table5) + \frac{P_2}{2} * (Table4) + \frac{P_2}{2} * (Table6) = P(XY)$, since $H(X)+H(Y)-H(XY)$ is convex in $P(XY)$. This finishes our symmetrizaion argument. The same argument can be applied to each simulation in the later sections.

We would start simulating the upper bound $S(X;Y\|Z) \leq \min_J I(X;Y|J)+ I(X,Y;Z|J)$ with the DSBS source with function XOR first, and then extend it to the non-DSBS source, with function XOR and AND.

4.2 DSBS sources with function $Z = X \oplus Y$

We first consider the case when X and Y are DSBS sources, and the function is XOR. Our objective function is $I(X;Y|J) + I(X,Y;Z|J)$, which is equivalent to simulate objective function $I(X;Y|J) - H(X,Y|Z,J)$.

By the symmetrization argument, our objective function becomes $I(X;Y)-$

a_2	$\frac{b_2+c_2}{2}$
$\frac{b_2+c_2}{2}$	d_2

Table 8: Combined Table 4 and Table 6

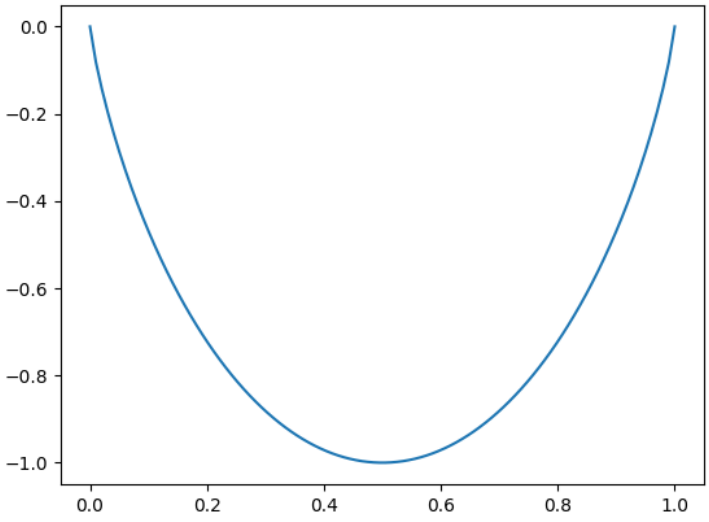

Figure 2: DSBS source with function XOR

$H(X, Y|Z)$. This can be written as a function of α since our sources are DSBS sources in Table 1. By simulation in Python, we can get the result in Figure 2.

Obviously, the objective function is convex. We can state it as a theorem below:

Theorem 4.1. *Given DSBS sources and $Z = X \oplus Y$, the objective function $I(X;Y) - H(X, Y|Z)$ is convex.*

Now we give a simple proof:

Proof. To prove it, we just need to represent the objective function in terms of $f(\alpha)$ and check $f''(\alpha) \geq 0$.

$$I(X;Y) - H(X,Y|Z) = H(X) + H(Y) - 2H(X,Y) + H(Z)$$
$$= 2 + 3\alpha \log \alpha + (2 + 4\alpha) \log(\frac{1}{2} + \alpha) - (1 - \alpha) \log(1 - \alpha) = f(\alpha).$$

By a routine calculation, we have

$$f''(\alpha) = \frac{11.5416(\alpha^3 + 0.125\alpha^2 - 0.5\alpha - 0.09375)}{(\alpha - 1)\alpha(0.5 + \alpha)^2} \geq 0.$$

when $0 \leq \alpha \leq 0.5$. Hence, the objective function is convex. □

Alternate Proof. Note that

$$H(X,Y) - H(Z) = H([\alpha, \alpha, \beta, \beta]) - H([2\alpha, 2\beta])$$
$$= \log 2 + H([2\alpha, 2\beta]) - H([2\alpha, 2\beta]) = \log 2.$$

We have

$$I(X;Y) - H(X,Y|Z) = H(X) + H(Y) - 2H(X,Y) + H(Z)$$
$$= 2H([\alpha + \beta, 1 - \alpha - \beta]) - H([\alpha, \alpha, \beta, \beta]) - \log 2$$
$$= \log 2 - H([\alpha, \alpha, \beta, \beta]).$$

Since entropy is concave for any input distribution, the objective is convex in α.

□

Since the objective function is convex, J must be constant. The upper bound becomes $I(X;Y|J) + I(X,Y;Z|J)$ now becomes $I(X;Y)$. Note that the lower bound of the secret key capacity is $I(X;Y) - I(X;Z) = I(X;Y)$, since $Z = X \oplus Y$. Hence, the upper bound and lower bound meet each other, i.e., $S(X;Y\|Z) = I(X;Y)$.

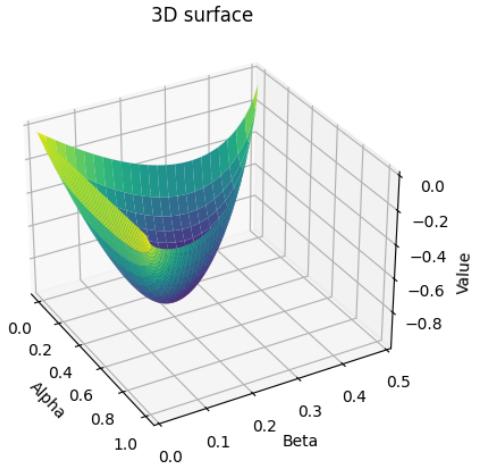

Figure 3: The surface of non-DSBS source and $Z = X \oplus Y$

4.3 Non-DSBS sources with function $Z = X \oplus Y$

We did some simulations with none-DSBS sources and $Z = X \oplus Y$. The plot of the function is depicted in Figure 3.

This figure looks convex. We drew the hull of this function to verify it is convex. The projection of the convex hull on $\alpha - \beta$ plane is depicted in Figure 4.

Theorem 4.2. *Given non-DSBS sources and $Z = X \oplus Y$, the objective function $I(X;Y) - H(X,Y|Z)$ is convex.*

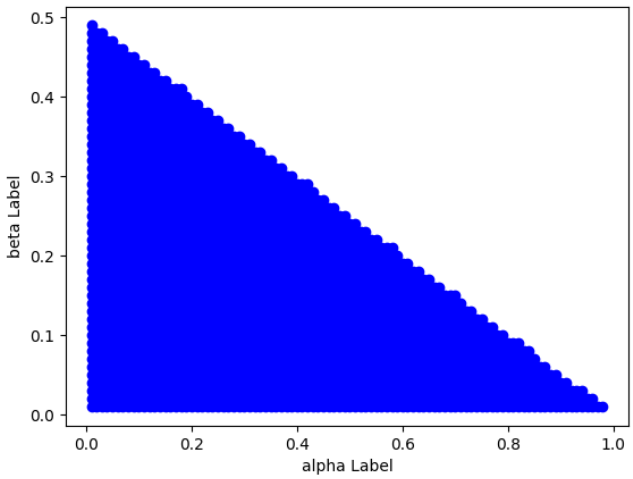

Figure 4: Projection on $\alpha - \beta$ plane of the convex hull of non-DSBS source and $Z = X \oplus Y$

Proof. Note that

$$\begin{aligned}
H(X) &= H([\alpha+\beta, \beta+\gamma]),\\
H(Y) &= H([\alpha+\beta, \beta+\gamma]),\\
H(X,Y) &= H([\alpha,\beta,\beta,\gamma]) = (\alpha+\gamma)H\left(\left[\frac{\alpha}{\alpha+\gamma}, \frac{\gamma}{\alpha+\gamma}\right]\right) + 2\beta\log 2,\\
H(Z) &= H([\alpha+\gamma, 2\beta]).
\end{aligned}$$

This implies

$$\begin{aligned}
f &= H(X) + H(Y) - 2H(X,Y) + H(Z)\\
&= 2H([\alpha+\beta,\beta+\gamma]) - H([\alpha,\beta,\beta,\gamma]) - (\alpha+\gamma)H\left(\left[\frac{\alpha}{\alpha+\gamma}, \frac{\gamma}{\alpha+\gamma}\right]\right) - 2\beta\log 2.
\end{aligned}$$

From this expression, it is hard to use the convex property of entropy. We

need to check the Hessian matrix of the function.

$$\text{Hess}(f) = \frac{2}{\log 2}\begin{bmatrix} -\frac{1}{2(\gamma-\alpha+1)} - \frac{1}{2(\alpha-\gamma+1)} & \frac{1}{2(\gamma-\alpha+1)} + \frac{1}{2(\alpha-\gamma+1)} \\ \frac{1}{2(\gamma-\alpha+1)} + \frac{1}{2(\alpha-\gamma+1)} & -\frac{1}{2(\gamma-\alpha+1)} - \frac{1}{2(\alpha-\gamma+1)} \end{bmatrix} - \frac{2}{\log 2}\begin{bmatrix} \frac{1}{\alpha+\gamma-1} - \frac{1}{\alpha} & \frac{1}{\alpha+\gamma-1} \\ \frac{1}{\alpha+\gamma-1} & \frac{1}{\alpha+\gamma-1} - \frac{1}{\gamma} \end{bmatrix} + \frac{1}{\log 2}\begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{\gamma-1} - \frac{1}{\gamma} \end{bmatrix}$$

It is easy to show that this matrix is positive semi-definite by doing simulations to see that eigenvalues are both non-negative. By the property of convex and positive semi-definite, the objective is convex in α and γ. □

4.4 Non-DSBS sources with function $Z = X \wedge Y$

We did some simulations with none-DSBS sources and $Z = X \wedge Y$. The plot of the function is depicted in Figure 5 and 6.

This time it is not obvious whether the function is convex or not. We tried to plot the convex hull of this surface and get the following results in Figure 7 and 8.

From the output of the convex hull, we can find that the function is partly non-convex because not every point is in the convex hull. In Figure 8, we can see clearly a curve dividing the triangle region into two parts. Our future goal is to study the function of this curve and the relationship between the curve and the objective function. This will be well studied in the next semester.

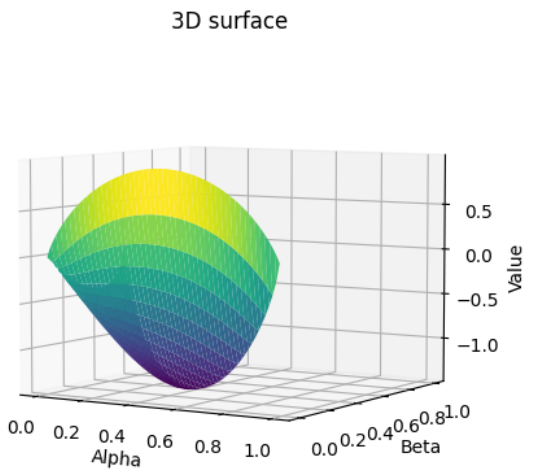

Figure 5: The surface of non-DSBS sources with function $Z = X \wedge Y$ (1)

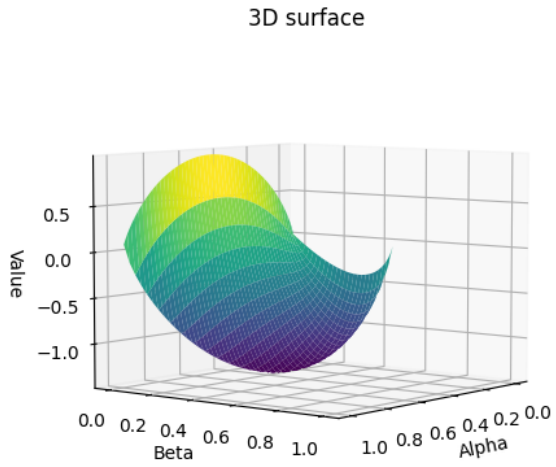

Figure 6: The surface of non-DSBS sources with function $Z = X \wedge Y$ (2)

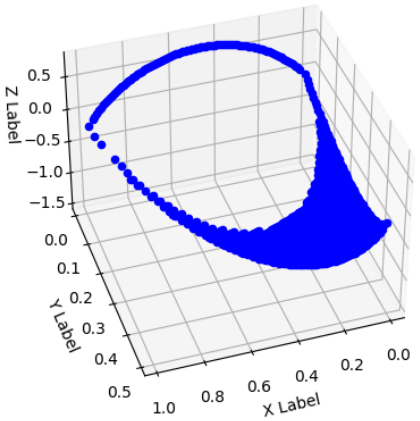

Figure 7: Plot of the convex hull of the function of non-DSBS sources with function $Z = X \wedge Y$. In the figure, X Lable represents α, Y Lable represent β and Z Lable represents the value of the objective function

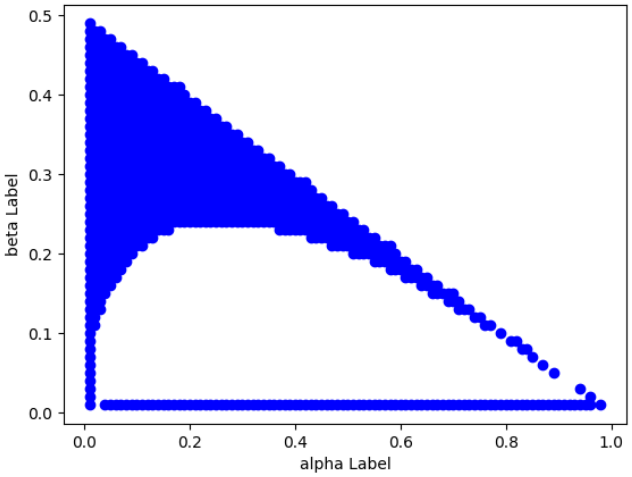

Figure 8: Projection on $\alpha - \beta$ plane of Figure 5

5 Conclusion

In this semester, we did some simulations on DSBS sources and non-DSBS sources, with functions $Z = X \oplus Y$ and $Z = X \wedge Y$. Especially, when given DSBS sources and $Z = X \oplus Y$, the objective function is convex and the upper bound and the lower bound of the secret key capacity meet each other. The secret key capacity is determined. When given non-DSBS sources and $Z = X \oplus Y$, the objective function is convex. This can be proved by looking into the Hessian matrix of the objective function. When given non-DSBS sources and $Z = X \wedge Y$, the objective function is partly non-convex. By simulations, we found that a curve divides the convex part from the non-convex part. We haven't looked into the function of the curve in detail. We will try to find the function of the curve in the next semester.

6 Future Directions

In the next semester, we will first look into the function of the curve in Figure 8. Later, we may extend the source distribution to 3 by 3 matrix and design the function $Z = f(X, Y)$ to see different results.

References

[1] R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography. i. secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, 1993.

[2] I. Csiszar and P. Narayan. Common randomness and secret key generation with a helper. *IEEE Transactions on Information Theory*, 46(2):344–366, 2000.

[3] Swapnil Das. Convex-hull, 2021. Accessed on November 15, 2023.

[4] Abbas El Gamal and Young-Han Kim. *Network information theory*. Cambridge university press, 2011.

[5] Amin Aminzadeh Gohari and Venkat Anantharam. Information-theoretic key agreement of multiple terminals—part i. *IEEE Transactions on Information Theory*, 56(8):3973–3996, 2010.

[6] U.M. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Transactions on Information Theory*, 45(2):499–514, 1999.

[7] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.