Bound Entanglement and Bound Information

Luca Dolfi
Advisor: Prof. Stefan Wolf
Tutor: Arne Hansen

A thesis presented for the degree of
BSc in Informatics

Department of Informatics
Università della Svizzera Italiana
Spring 2018

Contents

Chapter 1

Motivation

There are nonetheless distributions of probabilities that can hold a value of privacy and can therefore used in cryptographic systems. These joint probabilities have the properties

It has been noticed that these concepts of privacy also appear in nature and the strongest analogy comes from quantum mechanics.[1]From this theory arises the famous *quantum entanglement* that appears to be the equivalent of privacy in many ways. Both phenomena are composed of correlations between known parties that no other person can access or copy. As summed in [1] "If systems are in pure entangled state then at the same time (i) systems are correlated and (ii) no other system is correlated with them.". This can be seen as Alice and Bob holding a secret that Eve can not get to know.

quantum theory	**classical information**
quantum entanglement	secret classical correlations
quantum communication	secret classical communication
classical communication	public classical communication
entanglement distillation	classical key agreement (CKA)
local actions	local actions
bound entanglement	bound information ?

Table 1.1: Table showing key QM concepts and their analog in classical key agreement, following [5].

From table 1.1 we see that some the resources and operations of QM have a one-to-one analog in classical information theory. Such a close relation suggests that the two theories can be viewed together and to use one to better understand

[1]While those analogies are present in many sources, they can be found summed up in the paper by Collins and Popescu [5], which also shortly addresses the question of bound information.

the other. It is important however to point out that quantum entanglement and its effects *are not* a quantum manifestation of classical effects and one theory does not explain the other.
For example there is no known instance — and it is believed to not exist – of a classical correspondence to super-dense coding (a quantum effect). Other entities like a classical correspondence to bound entanglement, *bound information*, are not excluded a priori and remain yet to be observed or disproved.

Common Secret Intuitively a common secret is a piece of information (i.e. *bits* of information) known to trusted parties — for example Alice and Bob — and to none else. In an environment where we allow the presence of an eavesdropper Eve, reaching such state is not always trivial.
There exist methods and protocols to generate such secrets, even from nothing, although they differ at different levels of secrecy. A notable one is the famous Diffie-Hellman method to generate a common cryptographic key [7] .

A more formal and precise definition — one that we may also use in calculations – of a common secret is given later in section 2.3.2.

The Question

- Is there a tripartite probability P_{ABE}, that has some **cost** associated to it to create it, but has 0 possible key bits distillable from it?

1.1 A Comparison between Securities

1.1.1 Security Bounded by Computational Complexity

The majority of cryptographic systems used are built on computational complexity security. The so-called cryptographic functions are functions that are easy to compute in one way, but have a much higher complexity the other way round.

The Diffie-Hellman key exchange

A famous and widely used protocol for the exchange of cryptographic keys is the Diffie-Hellman key-exchange method. The whole process can be summarized in five basic steps:

1. Alice and Bob *publicly* communicate and agree on two numbers, that will serve as basis for the computations.

2. Each party generates *locally* a personal and distinct secret (s_A and s_B) without ever communicating it .

3. They mix their own secret with the common agreed basis, producing a result R_A and R_B. The mathematical properties of this operation make

it so it is computational infeasible to go back and retrieve the secrets s from R.

4. Both parties exchange *publicly* their result, so that they now posses the inseparable secret-base mixture of the other party.

5. Each party applies again their secret but to the received mixture this time. The outputs are equal for Alice and Bob so they can use this result as a common secret to create a key.

The parts exchanged over the public channel — the ones that Eve knows — are only the mutually agreed base and the two partial mixtures. It can be proven that those two elements alone give no information about the complete final shared secret and that it is virtually impossible to obtain the correct final product with only those two.

The security in this method relies mainly in step 3. Here an action as $R_A = g^{s_A} \bmod p$ is performed, where g and p are the public common basis agreed beforehand. To get back to s_A one will need to find the prime factors of R_A, which is a known hard problem. It is not impossible however. The difficulty of breaking this step is bounded only by the length of the number chosen one one side and the computational power available to the adversary on the other.

1.1.2 Security Bounded by the Laws of Physics

The BB84 protocol

1.1.3 Information Theoretical Security

The One-time Pad

Chapter 2

Fundamentals

2.1 Mathematical Framework (for QM)

In order to understand subsequent sections of this thesis a basic knowledge of the mathematical framework behind quantum mechanics is needed. It is also important to specify a standard notation as used in literature.

Dirac's bra-ket notation and Hilbert spaces

Every pure quantum state can be represented a vector in a vector space with inner product, i.e. a *Hilbert space*. The implication of this will be explained in the next section; for now we only look of this vector representation.
A complex Hilbert space $\mathcal{H}$ of dimension n is isomorphic to $\mathbb{C}^n$ with the standard inner product. In $\mathbb{C}^n$ one can choose a basis and then represent vectors with coordinates with respect to this basis.
The bra-ket notation is a handy notation introduced by physicist Paul Dirac to deal with such vector representation of quantum states. First of all we note that a state $\varphi' \in \mathcal{H}$ corresponds via the isomorphism to $\varphi \in \mathbb{C}^n$. It can be represented as a vector with respect of some basis as follows

$$|\varphi\rangle = \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \vdots \end{pmatrix} \text{ is a coloumn "ket" vector over } \mathcal{H}$$

$$\langle\varphi| = \begin{pmatrix} \varphi_1 & \varphi_2 & \dots \end{pmatrix} \text{ is a row "bra" vector over } \mathcal{H}$$

To be representative of a quantum state the vector has to have unitary length, $\|\varphi\| = 1$. Furthermore the conjugate transpose of a *bra* vector is the corresponding *ket* vector, and vice versa.

$$\langle\varphi|^\dagger = |\varphi\rangle,\ |\varphi\rangle^\dagger = \langle\varphi|$$

More specifically, for a complex vector space as $\mathcal{H}$, the components of $\langle\varphi|$ are each the complex conjugate of the components of $|\varphi\rangle$.

It is worth noting that in quantum information we will consider only vectors of finite dimensions, and more often than not, the standard basis for qubits represented by

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

which are recognizable as the equivalent of $\vec{e_1}$ and $\vec{e_2}$ in $\mathbb{C}^2$.

To summarize then, $|\varphi\rangle$ represents a column vector on a complex vector space with inner product equivalent to $\mathbb{C}^n$ in some basis, and $\langle\varphi|$ is its complex conjugate.

Inner/outer product

In standard vector notation we define the inner (scalar) product of complex vectors as

$$(\vec{v}, \vec{w}) = \begin{pmatrix} \bar{v_1} & \bar{v_2} \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} \bar{w_1} & \bar{w_2} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = (\vec{w}, \vec{v})^\dagger$$

Written in bra-ket notation, the inner product of two state vectors $|v\rangle$ and $|w\rangle$ is

$$(|v\rangle, |w\rangle) = \langle v|w\rangle = (|w\rangle, |v\rangle)^\dagger = \langle w|v\rangle^\dagger$$

Where $\dagger$ represents the conjugate transpose, which produces a scalar (complex) value.

It is important also to note that through the inner product of two vectors we also define the norm $\||v\rangle\| = \sqrt{\langle v|v\rangle}$.

The outer product of two vectors, on the other hand, produces a matrix, with very important properties. So if we define the matrix[1] $A = |w\rangle\langle v|$ we observe that

$$|w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle$$

which is a convenient way of visualizing the action of matrix A. In particular if we divide it like $(|w\rangle\langle v|)(|v'\rangle)$ it is easy to interpret it as *matrix A acting on vector $|v'\rangle$*; but the other equivalent form $(\langle v|v'\rangle)(|w\rangle)$ can also be seen as multiplying vector $|w\rangle$ by a value $\langle v|v'\rangle$.
The meaning of this is that $|w\rangle\langle v|$ can indeed be defined as a (linear) operator from the vector space of $|v\rangle$ and $|v'\rangle$ to the vector space of $|w\rangle$. This comes in very handy when we later use it to define operations and measurements on quantum states.

[1]The fact that the result of $|w\rangle\langle v|$ is indeed a matrix can be seen more directly if we remember that this is nothing less than a column-row vectors multiplication.

Linear operators

A linear operator between two vector spaces is defined as

$$\mathbf{A} : V \longrightarrow W \ , \ |v_i\rangle \mapsto A|v_i\rangle$$

$$\text{linear in all inputs, i.e. } A\left(\sum_i a_i|v_i\rangle\right) = \sum_i a_i A|v_i\rangle \text{ for all } i$$

Looking back at the definition of the matrix $A = |w\rangle\langle v|$ we can now refer to it as a linear operator from now on.
Some well-known linear operators acting on single qubits that we will use later on are the *Pauli Matrices*

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

In particular it is safe to say that, unless stated otherwise, the operators that will be presented all have a set of properties and are called Hermitian operators, or self-adjoint operators.

$$A = A^\dagger \quad \Longrightarrow (A|v\rangle)^\dagger = \langle v|A^\dagger$$

Operators have also to be positive, this means that it holds, for every $|v\rangle$: $\langle v|A|v\rangle$ is real non-negative. Any positive operator is also self-adjoint and therefore it has diagonal (spectral) representation $\sum_i \lambda_i|i\rangle\langle i|$ with non-negative eigenvalues λ_i.

Tensor product

The tensor product $V \otimes W$ is an operation between vector spaces that combines every element of the first vector space and every element of the second vector space in a bigger vector space. Tensor product is linear and from its properties emerges the famous phenomenon of quantum entanglement, which simply is that not all vectors in $\mathcal{H} = V \otimes W$ can be divided into $|v\rangle \otimes |w\rangle$ with $|v\rangle \in V, \ |w\rangle \in W$. This will later be explained in the next section.
Notation and abbreviation for the tensor product is

$$|v\rangle \otimes |w\rangle = |v\rangle|w\rangle = |v, w\rangle = |vw\rangle$$

It has the following properties:

$\forall|v\rangle \in V, \ \forall|w\rangle \in W, \ \forall z \in \mathbb{C}$
$\quad z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$

$\forall |v_1\rangle, |v_2\rangle \in V,\ \forall |w\rangle \in W$
$\quad (|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1 w\rangle + |v_2 w\rangle$

$\forall |v\rangle \in V,\ \forall |w\rangle \in W,\ A : V \to V'\ B : W \to W'$
$\quad (A \otimes B) \left(\sum_i a_i |v_i w_i\rangle\right) = \sum_i a_i A|v_i\rangle \otimes B|w_i\rangle$

The inner product on V and W can be used to define (linearly) an inner product on $V \otimes W$.

2.2 Quantum Mechanics

> The simplest quantum mechanical system, and the system which we will be most concerned with, is the *qubit*. A qubit has a two-dimensional state space. [...] The way a qubit differs from a bit is that superpositions of these two states, of the form $a|0\rangle + b|1\rangle$, can also exist, in which it is not possible to say that the qubit is definitely in the state $|0\rangle$, or definitely in the state $|1\rangle$. [2]

The three postulates

> **Postulate 1**: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space. [2]

> **Postulate 2**: The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on times t_1 and t_2,
>
> $$|\psi'\rangle = U|\psi\rangle$$
>
> [2]

> **Postulate 3**: Quantum measurements are described by a collection $\{M_m\}$ of *measurements operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occur is given by
>
> $$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle\ ,$$
>
> and the state of the system after the measurement is
>
> $$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}\ .$$

The measurement operators satisfy the *completeness equation*,

$$\sum_m M_m^\dagger M_m = I\ .$$

The completeness equation expresses the fact that probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle\ .$$

[2]

Quantum mechanics is a very large and complex theory. For our purposes it is enough for us to only consider the quantum system called *qubit* and its rules of computation following from the tensor product algebra. ...

All pure states in QM are normalized vectors in $\mathcal{H}$.

$$|\psi\rangle \text{ is a state vector } \Rightarrow |\psi\rangle \in \mathcal{H} \text{ and } |\langle\psi|\psi\rangle| = 1$$

This is instrumental in seeing them as probability vectors. Every linear operator has then to be unitary to maintain this property.
A statistical mixture of states corresponds to a *density matrix*, which is itself a new state. It is important to note that a mixture of probability of states is not the same thing as superposition of states. In the latter we don't have a measure of uncertainty of the state, meaning also that in theory we are always able to find a measurement basis that will always output the same result for that state. In the former, however, this is not possible given by the direct intrinsic uncertainty of the state.
Density matrices have then the properties:

$$M = \rho = \sum_i p_i|\psi_i\rangle\langle\psi_i| = \sum_i p_i P_{|\psi_i\rangle}\ \text{, where state } |\psi_i\rangle \text{ has probability } p_i$$

ρ is a positive, trace-1 operator meaning that $\mathrm{Tr}\,\rho = 1$ and all eigenvalues of ρ are positive. Moreover ρ is a linear combination of projectors $|\psi_i\rangle\langle\psi_i|$ which makes $\rho \in \mathbf{P}(\mathcal{H})$ a projector itself on the the Hilbert space.

2.2.1 Quantum Measurements

To get an actual value out of a qubit one has to *measure* it. Measurement is, mathematically, a projection onto some chosen computational basis. The result for each base vector projection is then interpreted as a *probability*. The state then changes after measurement, meaning for example that it will not retain it value as superposition any more.
...

If Alice has the state $|psi_i\rangle$ out of $i = 1..n$ and all states are orthonormal, then Bob can find out what the choice of i was. If the states are not orthonormal

there is no quantum measurement capable of distinguishing the states.
From this follows that if the states $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal, then $|\psi_2\rangle$ has a component orthogonal to $|\psi_1\rangle$ but also a component parallel to it which will give probability not 0 of measuring differently.

Example 1.

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad P_{+1} = |0\rangle\langle 0|,\ P_{-1} = |1\rangle\langle 1|$$

Measurement on qubit $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ has probability $p_{+1} = \langle\psi|P_{+1}|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = \frac{1}{2}$ and similarly $p_{-1} = \frac{1}{2}$ [2]

2.2.2 Quantum Entanglement

There exist vectors in $V \otimes W$ that can not be represented by a single tensor product: Given $v_1, v_2 \in V$ $w_1, w_2 \in W$ linear independent:

$$v_1 \otimes w_1 + v_2 \otimes w_2 = v_1 w_1 + v_2 w_2 \in V \otimes W$$

is *not* separable. this may be strange because on physical level tensor product is combination(merging) of quantum systems (??? this is not a complete sentence??)

[4]

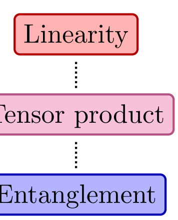

Figure 2.1: origin of entanglement via linearity

2.3 Information Theory

2.3.1 Mutual Information

Mutual information can be used as a measure of correlation between random variables.

Mutual information is defined as

$$I(X;Y) = \sum_{y\in\mathcal{Y}} \sum_{x\in\mathcal{X}} p(x,y) \log\left(\frac{p(x,y)}{p(x)p(y)}\right)$$

or equivalently, showing its relation to the entropies of the random variables

$$I(X;Y) = H(X) - H(X \mid Y) = H(X,Y) - H(X \mid Y) - H(Y \mid X)$$

This relation can be seen more directly in Fig. 2.2.
Mutual information is nonnegative and bounded by the entropy of random variable X

$$0 \leq I(X;Y) \leq H(X)$$

In this sense mutual information can also be interpreted as how much measuring one variable reduces the uncertainty of the other, thus being bounded by its uncertainty itself.

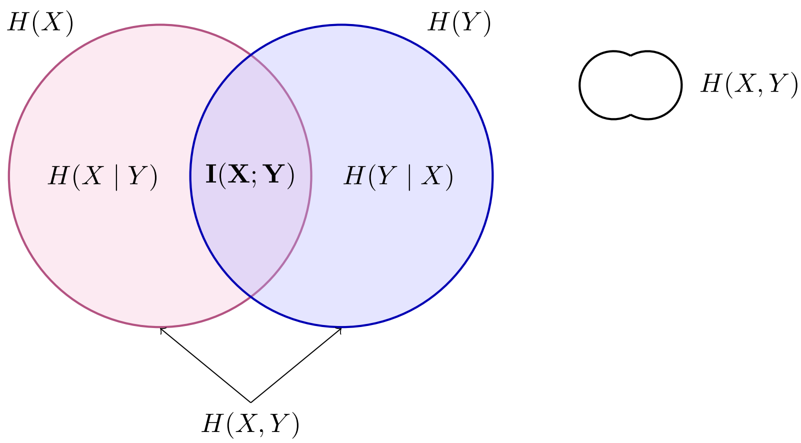

Figure 2.2: Representation of mutual information $I(X;Y)$ in relation with entropies $H(X)$ and $H(Y)$ and joint entropy $H(X,Y)$ of the random variables .

2.3.2 Common Secret

Let X, Y, Z, S be random variables on the same range $\mathcal{X}$. Let X be owned by Alice, Y by Bob and Z by Eve. Then

$$P[X = Y = S] > 1 - \epsilon \qquad \text{(common)}$$
$$I(X;Z) = 0 \wedge I(Y;Z) = 0 \qquad \text{(secret)}$$

for all $\epsilon > 0$.
The first part defines the *common* property: X and Y must be asymptotically the same. The second part states that the amount of information Eve can gather about X and Y, through it's realization of Z, is 0.

Chapter 3

Bound Information

3.1 Conjectures

Bound entanglement is a kind of correlation between Alice and Bob inaccessible to Eve but nevertheless of no use for generating a secret (quantum) key.
Unfortunately the existence of such bound information, which would contradict the mentioned conjecture[1]on the classical side of the picture, could not be proven so far.

3.2 State of research

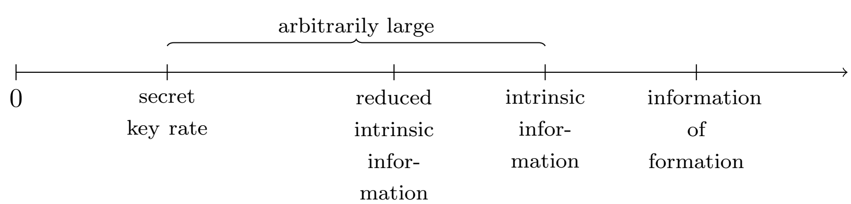

Figure 3.1: Bounds on the quantities as stated in Wolf + Renner 2003 proceeding

3.3 My considerations

[1]Shannon: Information theoretical security can be achieved only by parties sharing an unconditionally secret key initially. Maurer: this key can also not be generated from scratch. Maurer+Wolf: *Intrinsic information* between A and B given E == *secret key rate*(how much key can Alice and Bob generate from that P_{ABE}).

Bibliography

[1] Ryszard Horodecki et al. "Quantum entanglement". In: *Reviews of modern physics* 81.2 (2009), p. 865.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[3] Wikipedia contributors. *Bra-ket notation*. 2018. URL: `https://en.wikipedia.org/w/index.php?title=Bra%E2%80%93ket_notation&oldid=830232271`.

[4] Arne Hansen. "Swapped Bound Entanglement". Master Thesis. ETHZ, 2013.

[5] Daniel Collins and Sandu Popescu. "Classical analog of entanglement". In: *Phys. Rev. A* 65 (3 Feb. 2002), p. 032321. DOI: `10.1103/PhysRevA.65.032321`. URL: `https://link.aps.org/doi/10.1103/PhysRevA.65.032321`.

[6] Nicolas Gisin and Stefan Wolf. "Linking classical and quantum key agreement: is there "bound information"?" In: *Annual International Cryptology Conference*. Springer. 2000, pp. 482–500.

[7] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.

[8] Renato Renner and Stefan Wolf. "New bounds in secret-key agreement: The gap between formation and secrecy extraction". In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2003, pp. 562–577.

[9] Ueli M Maurer. "Secret key agreement by public discussion from common information". In: *IEEE transactions on information theory* 39.3 (1993), pp. 733–742.

[10] Ueli Maurer and Stefan Wolf. "Towards characterizing when information-theoretic secret key agreement is possible". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 1996, pp. 196–209.

[11] Thomas M Cover and Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[12] Antonio Acin, J Ignacio Cirac, and Ll Masanes. "Multipartite bound information exists and can be activated". In: *Physical review letters* 92.10 (2004), p. 107903.