Linking Classical and Quantum Key Agreement: Possibility of purification of mixed quantum states obtained from classical probability distributions

Term project of V. Galliard[1],
supervised by S. Wolf[2] and U. Maurer[2]
(1) Engineer ETH, Swiss Federal Institute of Technology (ETH Zürich), Switzerland
(2) Dept. of Computer Science, Swiss Federal Institute of Technology, Switzerland
(September, 2000)

We assume the reader to have basic knowledge of quantum information (mixed quantum states, density matrices, entanglement) and notation. For computer scientists, [7] will be quite a good introduction. Furthermore, some information-theoretical knowledge (information-theoretically secure secret-key agreement, secret-key rate and intrinsic information) is useful as well. A good introduction to this can be found in [1].

Abstract

One approach to investigating the connection between the quantum and classical case in key agreement is to start from a quantum state and to study the behaviour of the resulting classical probability distribution. Gisin and Wolf [3] could show that there is a close relationship between the conditional mutual intrinsic information [1] and the separability of mixed quantum states. They started with a quantum state and analyzed the classical outcome after certain measurements. Another approach is to start with a probability distribution coming from a key generation scenario and find corresponding quantum states. There is not only one quantum state which matches a chosen classic probability distribution (similar to the possibility of obtaining different probability ditributions performing measurement of quantum states with respect to different bases). We show in this documentation that generating mixed quantum states from classical probability distributions with no intrinsic information could lead to entanglement and in some cases to disentanglement, depending on the phase function. Furthermore we show that the positivity of intrinsic information does not imply that all the corresponding quantum states are entangled.

Keywords. Key agreement, quantum cryptography, quantum privacy amplification, purification, entanglement, intrinsic mutual information, secret-key rate, information theory.

1 Introduction

At first sight it is not obvious that quantum information processing is more powerful than classical algorithms. Grover, however (described in [7] p. 275), as a good example could show in 1998 that searching elements in a unsorted quantum database is potentially (unfortunately not exponentially) faster than what classical computers can achieve. This opens new ways. The secret lies in the quantum states that behave very 'non-classical'. One bit (binary digit) information in the classical case in contrast to a ‚qubit' (quantum bit) representing a probability between 0 and 1 in the quantum case. It is easy to see that by measuring one classical register, we have all information that was (and still is) stored in it. On the other hand, the laws of quantum mechanics restrict the possible measurements to be carried out. If perfect measurement were possible then one would be able to clone quantum states and that leads to a conflict (No-cloning Theorem, [4] p. 68). Measurement are irreversible an therefore information will get lost. From the physical point of view we have some particles (photons or electrons for example) and could take their polarization or energy level as state. In practice it is difficult to handle quantum states because it is almost impossible to protect the state from the environment. This issue leads to small errors that change the state of the particle. In theory, however, quantum states can be treated as they were perfect and this often leads to very surprising results.

2 Information-theoretically secure secret-key agreement

In general it is impossible to achieve information-theoretically secure secret-key agreement only using authentic, but completely insecure communication between Alice and Bob. This is because if Eve can obtain all the information that flows from Alice to Bob and back, $C_1,...C_n$, than the conditional Shannon-entropy $H(S|C_1,...C_n)$ of the common secret-key S is zero. So Eve can reconstruct the secret-key S. From that point of view there exists only computationally secure key agreement such as Diffie-Hellman for example. The point is now to have an additional ‚source' of information. Using this we can use protocols to finally achieve unconditionally secure secret-key agreement with arbitrary high probability.

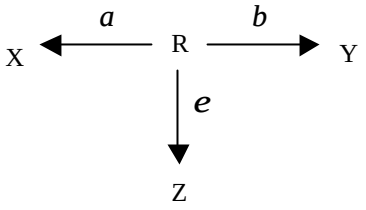


Figure 1: Secret-key agreement using random bits

We take this completely classical approach as described in detail in [1] p. 35. We have three parties Alice, Bob, and Eve. Alice and Bob want to generate a secret key using a random bit generator as source R, for example a satellite sending random bits as a stream. All Alice, Bob and Eve are receiving the random bits with certain error bit rates (a, b, e) depending of the qualitity of the connection from the satellite (see Figure 1). We assume the bits received behave like coming from a binary-symmetric channel. Than we can formalize this scenario by setting up a joint probability distribution $P_{XYZ}(x, y, z)$. Depending on the error probabilities, this will lead to different distributions (see Appendix A). Depending on a, b, and e, secret-key agreement with additional public but authentic communication is possible or not. It is a little surprising that a, b can be greater than e and is it is still possible to generate a common secret-key in spite of the initial drawback of Alice and Bob, using classical privacy amplification. This scenario we take as a motivation to investigate the distribution P_{XYZ}.

3 Entangled states and intrinsic information

There are several criteria for wether quantum privacy amplification (also known as purification) is possible or not. One of them is the a-entropic inequality [12] to decide if the state is separable. Peres [9] showed that this criterion is weaker than the one we consider here. We check the eigenvalues of the partial transpose of the density matrix (defined in Section 5) for the occurrence of negative values [10, 13]. M., P., and R. Horodecki found that if there is at least one of them negative, it is necessary and sufficient condition (if $\dim(\rho_{AB}) = 4$) for entanglement (coming from the german word „verschränkt", mentioned the first time in the early 20th century from Schrödinger). Entangled means that the mixed quantum state cannot be remotely prepared by classical communication. In this case quantum privacy amplification (QPA) is possible (how to do so is explained in [6]) and these mixed states Alice and Bob can be used for generating a common secret-key using laws of quantum mechanics.

We will have a closer look at mixed states such as ρ_{AB}. A state is called separable (i. e., not entangled) if it is possible to write its density matrix as a product state such as $\rho_{AB} = \sum_j p_j \rho_{Aj} \otimes \rho_{Bj}$. This is the case if the states ρ_{Aj} and ρ_{Bj} can be generated by purely classical communication and thus QPA is not possible. If it were, one could generate entangled states with purely classical communication using these states to generate a secret-key in the quantum domain by carrying out a quantum protocol. And this is a contradiction to a generalization of Shannon's Theorem.

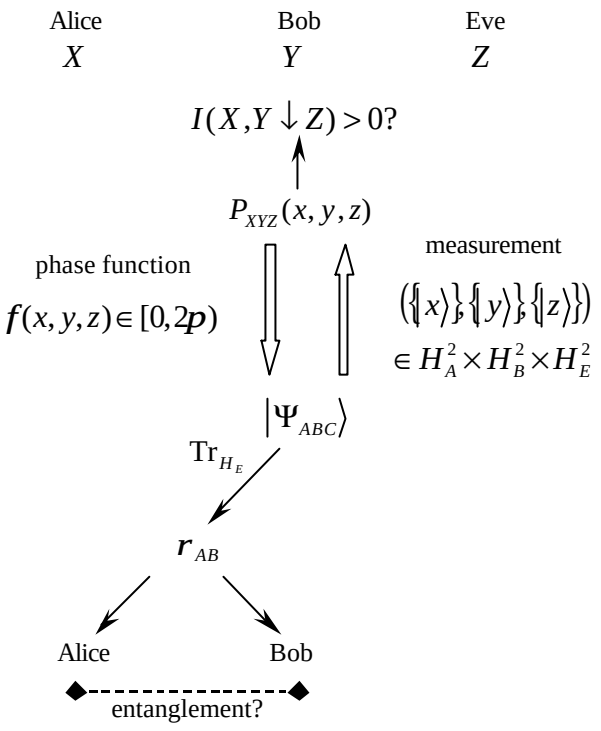
Gisin and Wolf could show in [3] that entangled mixed quantum states are strongly correlated with mutual intrinsic information. They prove that if a mixed state is entangled then it is possible to generate a common secure secret-key with using a corresponding classical distribution coming from optimal measurements of this quantum state. They start with a pure quantum state $|\Psi\rangle \in H_A \otimes H_B \otimes H_E$ (H_i are the 2-dimensional Hilbert spaces equal to C^2, so $|\Psi\rangle \in C^8$) and trace out Eve to obtain the density matrix $\rho_{AB} = \mathrm{Tr}_{H_E}(\Psi)$. That means the Alice and Bob are only looking at their sub-quantum-system and make their measurements there in. On one hand, when starting from an entangled state (i. e., not separable) the positivity of the intrinsic conditional mutual information I(X; Y↓ Z) is shown. In other words the possibility of information-theoretically secure key agreement is given in the classical and quantum scenario, no matter how Eve behaves. On the other hand if the state is separable (i. e., not entangled) the common conditional information I(X; Y|Z) is zero (hence the common mutual intrinsic information I(X; Y↓ Z) is zero as well) and so it is impossible to generate a secret-key neither in the classical nor in the quantum case.

4 From classical distributions to quantum states

We now take another approach to establish a connection between classical and quantum key agreement. Gisin and Wolf showed that there is a connection by assuming quantum states are given, as mentioned in the previous section. Now we start with a classical probability distribution (perhaps coming from a quantum scenario) and end up with quantum states. As we said before, measuring a quantum system destroys it and we ‚only' get classical information from it. It is hence not surprising that one distribution corresponds to many, somehow related quantum states as we will see. By getting classical information we have to measure a quantum system with certain bases that leads to the following equation:

$$P_{XYZ}(x,y,z) := \left|\langle x,y,z|\Psi\rangle\right|^2 . \tag{1}$$

The result of a measurement is a realization of the probability distribution corresponding to the state $|\Psi\rangle$ by measuring in certain bases $\{|x\rangle\}\subset H_A$, $\{|y\rangle\}\subset H_B$, $\{|z\rangle\}\subset H_E$, respectively. When measuring, we have to use observables. The standard basis $\{|0\rangle,|1\rangle\}$ (also known as computational basis) as one observable or the dual basis (also called Hadamard basis) $\{|0'\rangle,|1'\rangle\}=\{1/\sqrt{2}(|0\rangle+|1\rangle),\ 1/\sqrt{2}(|0\rangle-|1\rangle)\}$ as an another observable are two examples of orthonormal measurements ($\{|a_1\rangle,|a_2\rangle\}\subset H, \langle a_1|a_2\rangle=0\Leftrightarrow|a_1\rangle,|a_2\rangle$ are othogonal, if $\langle a_1|a_2\rangle$ is scalar product in H^2). Measurements are hermitian and the result is an eigenvalue of the corresponding projection operator. This eigenvalue belongs to the associated eigenvector, for example $|0\rangle=(1,0)^T$ or $|1\rangle=(0,1)^T$ in the standard basis. In the case of a single qubit $|j\rangle=l_0|0\rangle+l_1|1\rangle$ (quantum states are defined in Section 6) the probability to measure the state $|0\rangle$ is $|l_0|^2$ in the standard basis. It is important to note that after the measurement the state falls to one of the eigenvectors and the superposition vanishes.



If we want to find a quantum state corresponding to a specific classical distribution $P_{XYZ}(x,y,z)$, we have to define a phase $f(x,y,z)\in[0,2p)$ for each state $|x,y,z\rangle$ (we abbreviate $|x\rangle\otimes|y\rangle\otimes|z\rangle$ by $|x,y,z\rangle$, $\otimes$ stands for the tensor product) to create a quantum state. Our goal is to investigate the effect of the choice of the phase function for the discussed connection between the classical and quantum world.

5 How to find corresponding quantum states

By ‘generating' a quantum state we must have a close look at the possible measurements. As we stated before, measuring a quantum state is equivalent to taking an instance of a certain probability distribution $P_{XYZ}(x,y,z)$ with $\mathsf{X}=\mathsf{Y}=\mathsf{Z}=\{0,1\}$. Now we have to rebuild the whole sample space from all the events that could be happen. We have to summarize all possible outcomes with the corresponding probability. By definition (see [4, 9]) we have

$$|\Psi\rangle=\sum_{(i,j,k)\in\mathsf{X}\times\mathsf{Y}\times\mathsf{Z}} c_{i,j,k}\cdot|i,j,k\rangle \tag{2}$$

with

$$c_{i,j,k} \in \mathbb{C},\ 0 \le \left|c_{i,j,k}\right|^2 \le 1 \text{ and } \sum_{i,j,k} \left|c_{i,j,k}\right|^2 = 1 \tag{3}$$

to $|\Psi\rangle$ be a valid quantum state. We have to insert the classical information coming from the distribution. We know the probability of being measured from each state. We see that every

$$\left|c_{x,y,z}\right|^2 = P_{XYZ}(x,y,z) \tag{4}$$

because of (1), (2) and (3). Then quantum states can be described as vectors of unit length in a Hilbert space ($Ç = C^2$). Because of this we have one more degree of freedom to define our quantum state. There exists not only one $\left|c_{x,y,z}\right|^2$ satisfying (4). For every potential state we have to define a phase which sets the direction of the vector in the Hilbert space. This is done with the phase function $f(x,y,z) \in [0, 2p)$ in the factor $e^{i \cdot f(x,y,z)}$, which satisfies of course $\left|e^{i \cdot f(x,y,z)}\right| = 1$. Now we can completely describe our state with the following summation

$$|\Psi\rangle = \sum_{(x,y,z) \in X \times Y \times Z} e^{i \cdot f(x,y,z)} \sqrt{P_{XYZ}(x,y,z)} \cdot |x,y,z\rangle \cdot \tag{5}$$

At the moment we know almost nothing about influences of the phase function. This will be the subject of our investigations.

We will study the behaviour of the eigenvalues of the partial transpose of r_{AB}. In this special case we do not need to generate the state $|\Psi_{ABE}\rangle$ from (5) with tracing out Alice with $r_{AB} = \mathrm{Tr}_{H_E}(\Psi_{ABE})$ (see Figure 2). We can directly produce the state r_{AB} by using the conditional probability distribution $P_{XY|Z}(x,y \mid z)$ obtained from $P_{XYZ}(x,y,z)$. We compute $|\Psi_0\rangle$ and $|\Psi_1\rangle$ for both possible measurements 0 and 1 of Eve. This is done with

$$|\Psi_z\rangle = \sum_{(x,y) \in X \times Y} e^{i \cdot f(x,y,z)} \sqrt{P_{XY|Z}(x,y \mid z)} \cdot |x,y\rangle \tag{6}$$

for z equal 0 and 1. We want to investigate the density matrix of the mixed state r_{AB}, so we have to use the projectors of (6) $P_{\Psi_z} = |\Psi_z\rangle\langle\Psi_z|$ and build the density matrix r_{AB} for as follows:

$$r_{AB} = \sum_{z \in Z} P_Z(z) \cdot P_{\Psi_Z} \cdot \tag{7}$$

It is obvious that at most two of the four eigenvalues of r_{AB} can be different from 0 (and of course at least one). This is because this mixed state is a statistic mixture of two the pure states $|\Psi_0\rangle$ and $|\Psi_1\rangle$. If these two states are not equivalent, that will lead to the fact that exactly two eigenvalues are different from 0 (if two eigenvalues are equal then they are counted twice).

Now we have completely defined the mixed state (7) we will check for entanglement. One really efficient way to do so is by calculating the partial transpose and check this matrix for negative eigenvalues [13] as mentioned above. If this new matrix r^{t}_{AB} has at least one negative eigenvalue then r_{AB} is called with negative partial transpose. We define the partial transpose in general and have a closer look to the much easier case with $\dim(H_A) = \dim(H_B)$ is equal to 2. We rewrite r_{AB} as $(r_{AB})_{nm,mn}$. Now we can define the partial transpose as $(r^t_{AB})_{mm,nn} = (r_{AB})_{nm,mn}$, just transposing the Latin indices, but not the Greek ones [9]. This is no unitary transformation, but a hermitian one. In our case when $\dim(H_A) = \dim(H_B) = 2$ it is very easy to calculate it, only by transposing the four 2×2 sub-matrices of r_{AB} (see Appendix B). When the dimension of the Hilbert spaces is equal to 2, we are very lucky, because negative partial transpose of r_{AB} implies entanglement and vice versa [9]. Now we are going ahead by checking several phase functions and studying the behaviour of the eigenvalues of the partial transpose.

6 Linking classical and quantum scenarios

We want $P_{XYZ}(x,y,z)$ with I(X; Y↓ Z) > 0 on one hand and entangled states on the other hand for the key-generation phase. Now we start with the classical probability distribution $P_{XYZ}(x,y,z)$ and build the density matrix r_{AB} to check if it has negative partial transpose to see if r_{AB} is entangled or not. It is proven in [14] that r_{AB} can be purified (quantum privacy amplification is possible) if the mixed state is not separable (i.e., entangled). We only consider the case where $\dim(H_A) = \dim(H_B) = \dim(H_E) = 2$. We define a class of functions $f_{\{a_i\}}(x,y,z)$ that allows us for generating related, but different quantum states from one classical probability distribution. Related means that we can

see in all those states that the eigenvalues of ρ_{AB}^{t} remain the same, how ever the parameters $\{a_1,..,a_k\}$ are chosen. By defining a special class of functions $f(\cdot)$, we show with a numerical evaluation that the eigenvalues of the partial transpose of the density matrix of our states are the same using certain probability distributions (yet not in general).
As the easiest example we consider the phase function

$$f^{(0)}(x,y,z)=0. \tag{8}$$

That means nothing else than that the phase is independent from x,y and z respectively and equal 0. The density matrix will have real entries only. Sometimes it is useful to take the state generated by the phase function (5) as reference to compare the other outcomes (see Appendix A for a list of the tables and Appendix C for results).
We consider the following phase function by using a linear combination of inputs x,y,z with completely random coefficients $(a_1,a_2,a_3)\in_R R^3_{[0..1)}$:

$$f^{(1)}_{\{a_1,a_2,a_3\}}(x,y,z)=(a_1x+a_2y+a_3z)\cdot 2/(a_1+a_2+a_3)\cdot\pi. \tag{9}$$

It is obvious that $f^{(1)}{}_{\{a_1,a_2,a_3\}}(x,y,z)$ lies in the interval $[0,2\pi)$, so that this is a valid phase function. We will conjecture in Appendix C the somewhat surprising fact that eigenvalues of ρ_{AB} do not change; that is possible because of the special character of (9) as a linear function in its parameters. This eigenvalues depend only on $P_{XYZ}(x,y,z)$. But it is more interesting, that the eigenvalues of ρ_{AB}^{t} remain the same, although all of ρ_{AB} matrix elements change, and so does the statistic mixture.
Now we chose another function:

$$f^{(2)}(x,y,z)=(x\cdot y+y\cdot z+x\cdot z)\cdot 2/3\,\pi. \tag{10}$$

No additional parameters are needed for our purpose. We will see in Appendix C that $f^{(2)}(\cdot)$ will generate a valid quantum state as well ($\mathrm{Tr}(\rho_{AB})=1$), but in this case the eigenvalues of ρ_{AB}^{t} are different (wavy underlined) compared to those calculated with (8) or (9). However there still exists one negative eigenvalue that shows the corresponding quantum state is still entangled.
The question is now if there exists (at least for the distribution given in table 2) any function $f^{(3)}(\cdot)$ that turns out a completely non-negative set of eigenvalues of ρ_{AB}^{t}.
We are approaching this problem by generating several phase functions $f^{(3)}(x,y,z)$ with comletely random behaviour. There exist exactly 8 different outcomes within a parameter range $(x,y,z)\in\{0,1\}^3$ for $f^{(3)}(x,y,z)$. We define the function

$$f^{(3)}_{\{a_{000},a_{001},a_{010},a_{011},a_{100},a_{101},a_{110},a_{111}\}}(x,y,z)=a_{xyz}, \tag{11}$$

with the parameters $a_{000},...,a_{111}\in[0,2\pi)$ as a completely general function. The parameters are chosen randomly within the interval $[0,2\pi)$. We will numerically calculate partial transpose using hundreds of different $f^{(3)}_{(.)}(x,y,z)$ (i. e., different randomly chosen parameters $a_{000},...,a_{111}$ for each $f^{(3)}_{(.)}(x,y,z)$) and check if it has positive partial transpose. It is performed with Maple V as listed in Appendix B. With this approach by randomly chosing 500 different phase functions we did not find a mixed quantum state that does not have negative partial transpose using (11). In other words, we cannot easily find a phase function $f(\cdot)$ that generates a mixed state ρ_{AB} from the distribution defined in table 2 with I(X; Y↓ Z) > 0 that is not entangled. But we found some phase functions for which the corresponding density matrix is separable by using only phases that are multiples of $1/4\,\pi$ (see Theorem 2, Section 7).
Now let us consider a distribution as depicted in table 4 with I(X; Y↓ Z) = 0 (hence S(X; Y‖Z) = 0, [1]). In this case Alice and Bob cannot use these random bits coming from the random bit source to generate a secret-key. We will generate mixed quantum states ρ_{AB} with these different phase functions (8), (9), (10) and (11). Using (8) we have exactly one eigenvalue in ρ_{AB}^{t} and therefore it is equal to 1. ρ_{AB} has positive partial transpose and thus we have no entanglement, and ρ_{AB} can be written as $\sum_j p_j \rho_{Aj}\otimes\rho_{Bj}$. This separable state ρ_{AB} can be generated by purely classical communication and therefore QPA is impossible.
The special case that ρ_{AB} has exactly one eigenvalue, namely 1 (Appendix C) is evident. We have equivalent states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ which is a consequence that $P_{XYZ}(x,y,z)$ is completely symmetric and $f(\cdot)$ is equal to 0. Generating ρ_{AB} with (7) will therefore lead to a pure state.
Now we use phase function (9) and at the first sight we are very surprised about the behaviour of the eigenvalues of ρ_{AB}^{t} in the quantum domain. The number of eigenvalues of ρ_{AB} is, as expected, 2. But ρ_{AB}^{t} has one negative

eigenvalue in contrast to the example above using the phase function (8). That means that ρ_{AB} is entangled and QPA can be applied. Now we have positive partial transpose on one hand by using $f^{(0)}(x, y, z) = 0$ and negative partial transpose on the other hand by using $f^{(1)}_{\{a_1,a_2,a_3\}}(x, y, z)$ as another phase function. With [3] keeping in mind, this will lead to the assumption that there must be a close connection between choosing a basis when performing a measurement and choosing a phase function when finding corresponding quantum states. We can state that there must be 'better' and 'worse' choices for phase functions $f(x, y, z)$. We can show this in the example when starting from $P_{XYZ}(x, y, z)$ as described in table 4 with I(X; Y↓ Z) = 0. There exists at least one 'bad' choice for $f(x, y, z)$ in the meaning that the generated quantum state will be not entangled and a lot of 'good' choices. (8) is such a bad choice. All the other choices considered and calculate in Appendix C lead to a quantum entanglement such that QPA is possible.

The following conjecture has its reverse counterpart as mentioned above. Theorem 1 stated in [3] shows if ρ_{AB} is separable (i. e., not entangled) then there exists a generating set $\{|z\rangle\} \subset H_E$, such that I(X; Y|Z) = 0, how ever Alice and Bob choose their bases $\{|x\rangle\} \subset H_A$ and $\{|y\rangle\} \subset H_B$. Our conjecture is that for one distribution with I(X; Y↓ Z) = 0 (see Appendix A, table 4), there exists a at least one phase function $f(x, y, z)$ so that $f(\cdot)$ is entangled and hence QPA is possible (see Section 7). In general, arbitrary chosen phase function lead to entanglement.

Furthermore, our conjecture is now that for distributions with I(X; Y↓ Z) > 0 (e. g. Appendix A, table 2), there exists a at least one phase function $f(x, y, z)$ such that ρ_{AB} is entangled and hence QPA is possible. This is similar to Theorem 2 in [3] that says if $\rho(\cdot)$ is entangled then there exist generating sets $\{|x\rangle\} \subset H_A$ and $\{|y\rangle\} \subset H_B$ for Alice and Bob, such that I(X; Y↓ Z) > 0, however Eve chooses her basis $\{|z\rangle\} \subset H_E$.

7 Conclusions

Our main conlcusion is that, like the choice of the measurement bases in [3], the choice of the phase function when linking classical and quantum privacy amplification is crucial and must be closely studied.

Our observations lead to the following results:

In the statements below let $\Psi \in H_A \otimes H_B \otimes H_E$ with $\dim(H_A) = \dim(H_B) = \dim(H_E) = 2$ be a quantum state corresponding to a probability distribution $P_{XYZ}(x, y, z)$, $(x, y, z) \in \mathsf{X} \times \mathsf{Y} \times \mathsf{Z}$ with respect to a phase function $f(x, y, z) \in R_{[0,2p)}$, and let $\rho_{AB} = \mathrm{Tr}_{H_E}(P_\Psi)$.

Observation 1 *The eigenvalues of ρ_{AB} and its partial transpose ρ^t_{AB} depend on the choice of the phase function $f(x, y, z)$.*

This is suggested by numerical evaluations of the distribution described in tables 2, 3 and 4 using the phase functions (10) and (11).

We conjecture that for every $P_{XYZ}(x, y, z)$, the class of phase functions $f_{\{a_1,a_2,a_3\}}(x, y, z) = (a_1x + a_2y + a_3z) \cdot 2/(a_1+a_2+a_3) \cdot p$, with parameters $(a_1, a_2, a_3) \in R^3_{[0..1)}$ satisfies the property that the eigenvalues of ρ_{AB} and its partial transpose ρ^t_{AB} are equal for every choice of a_1, a_2 and a_3. This is suggested by numerical evaluations of the distribution described in tables 2, 3 and 4 using the phase function defined in equation (9).

Conjecture 1 *For every $P_{XYZ}(x, y, z)$ with I(X; Y|Z) = 0 there exists a phase function $f(x, y, z)$ such that ρ_{AB} is separable.*

We find an example that satisfies conjecture 1 by using the probability distribution in table 4 and the phase function defined in equation (8). However, most of times we ended in an entangled quantum state choosing an arbitrary phase function for every probability distribution we investigated. This is related to Theorem 1 in [3].

Conjecture 2 *For every $P_{XYZ}(x, y, z)$ with I(X; Y↓ Z) > 0 there exists a phase function $f(x, y, z)$ such that ρ_{AB} is entangled.*

This is similar to Theorem 2 in [3] but starting with a probability distribution in contrast to starting with a quantum state. This is suggested by the example with the distribution described in table 2. For both conjectures 1 and 2 it is not obvious that they follow from Theorems 1 and 2 respectively, because there can exist classical probability distributions which do not result from optimal measurements.
We observed that for a $P_{XYZ}(x,y,z)$ with I(X; Y|Z) > 0 it is hard to find a phase function $f(x,y,z)$ such that r_{AB} is separable with a numerical approach. The numerical search for phase functions $f(x,y,z)$ that satisfies the condition that all eigenvalues of r_{AB}^t corresponding to a arbitrary $P_{XYZ}(x,y,z)$ with I(X; Y|Z) > 0 are not negative is not easy in general (see Appendix D). There can be found a lot of negative eigenvalues close to 0. However, most of times we ended in an entangled quantum state choosing an arbitrary phase function for every probability distribution we investigated.

Theorem 1 *There exists at least one* $P_{XYZ}(x,y,z)$ *with I(X; Y|Z) = 0 and a phase function* $f(x,y,z)$ *such that* r_{AB} *is entangled and can be purified.*

Proof. In the probability distribution $P_{XYZ}(x,y,z)$ described in table 4 is I(X; Y|Z) = 0 because $P_X(x)$ and $P_Y(y)$ are uniformly distributed. The eigenvalues o f the partial transpose r_{AB}^t of the density matrix

$$r_{AB} = \begin{bmatrix} 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & 0 & 0 \\ 1/4 & 0 & 1/4 & 0 \\ 1/4 & 0 & 0 & 1/4 \end{bmatrix}$$

with respect to $P_{XYZ}(x,y,z)$ and to the phase function $f(x,y,z) = (x \cdot y \cdot z) \cdot p$ satisfies $\det(r_{AB}^t - lI_4) = 0$ [5]. $l = 1/4(1-\sqrt{3})$ is one of these eigenvalues and less than 0. Therefore r_{AB} has negative partial transpose and hence entangled. □

Theorem 2 *There exists at least one* $P_{XYZ}(x,y,z)$ *with I(X; Y↓ Z) > 0 and a phase function* $f(x,y,z)$ *such that* r_{AB} *is separable and can not be purified.*

Proof. In the probability distribution $P_{XYZ}(x,y,z)$ described in table 2 is I(X; Y↓ Z) > 0 because both $P_X(x)$ and $P_Y(y)$ are not uniformly distributed and therefore classical privacy amplification can be applied. We write $P_{XY|Z}(x,y \mid z) = 2 \cdot P_{XYZ}(x,y,z)$ because $P_Z(z) = 1/2$ for $z \in \{0,1\}$. By using the phase function $f(x,y,z) = f_{xyz}$ with $(f_{000},...,f_{111}) = (0,0,1/2\,p,1/2\,p,p,0,3/2\,p,1/2\,p)$ we will get $|\Psi_0\rangle = \left(1/4\sqrt{7}, 1/4\sqrt{3}\cdot i, -1/4\sqrt{3}, 1/4\sqrt{3}\cdot i\right)$ and $|\Psi_1\rangle = \left(1/4\sqrt{3}, 1/4\sqrt{3}\cdot i, 1/4\sqrt{3}, 1/4\sqrt{7}\cdot i\right)$ by using $|\Psi_z\rangle = \sum_{x,y \in \{0,1\}} e^{i \cdot f_{xyz}} \sqrt{2 \cdot P_{XYZ}(x,y,z)} \cdot |x,y\rangle$. The corresponding projectors

$$P_{\Psi_0} = \begin{bmatrix} 7/16 & 1/16\sqrt{21}\cdot i & -1/16\sqrt{21} & -7/16\sqrt{21}\cdot i \\ -1/16\sqrt{21}\cdot i & 3/16 & 3/16\cdot i & -3/16 \\ -1/16\sqrt{21} & -3/16\cdot i & 3/16 & 3/16\cdot i \\ 1/16\sqrt{21}\cdot i & -3/16 & -3/16\cdot i & 3/16 \end{bmatrix}, P_{\Psi_1} = \begin{bmatrix} 3/16 & 3/16\cdot i & 3/16 & 7/16\sqrt{21}\cdot i \\ -3/16\cdot i & 3/16 & -3/16\cdot i & 1/16\sqrt{21} \\ 3/16 & 3/16\cdot i & 3/16 & 1/16\sqrt{21}\cdot i \\ -1/16\sqrt{21}\cdot i & 1/16\sqrt{21} & -1/16\sqrt{21}\cdot i & 7/16 \end{bmatrix}$$

we obtain with $P_{\Psi_z} = |\Psi_z\rangle\langle\Psi_z|$. We find $r_{AB} = 1/2(P_{\Psi_0} + P_{\Psi_1})$ as

$$r_{AB} = \begin{bmatrix} 5/16 & 1/32(\sqrt{21}+3)\cdot i & 1/32(-\sqrt{21}+3) & 0 \\ 1/32(-\sqrt{21}-3)\cdot i & 3/16 & 0 & 1/32(\sqrt{21}-3) \\ 1/32(-\sqrt{21}+3) & 0 & 3/16 & 1/32(\sqrt{21}+3)\cdot i \\ 0 & 1/32(\sqrt{21}-3) & 1/32(-\sqrt{21}-3)\cdot i & 5/16 \end{bmatrix}.$$

We transposing the four sub-matrices of r_{AB} we get r_{AB}^t. The eigenvalues l_i of r_{AB}^t we get by solving $\det(r_{AB}^t - lI_4) = 0$ [5]. By straight on solving we find $l^4 - l^3 + 1/4\,l^2 = 0 \Leftrightarrow 1/4\,l^2(2l-1)^2$ and so the eigenvalues are 0 and $1/2$, each occurring twice. Therefore r_{AB} has positive partial transpose and hence separable. □

The choice $(0,0,1/2\,p,1/2\,p,p,0,3/2\,p,1/2\,p)$ for $(f_{000},...,f_{111})$ is not the only one that leads to disentanglement in Theorem 2. For the sets $(0,0,0,0,p,0,0,p)$, $(p,p,p,0,0,0,p,0)$, $(0,3/2\,p,1/2\,p,0,0,1/2\,p,3/2\,p,0)$ and $(p,0,1/2\,p,0,0,1/2\,p,p,p)$ for example, the corresponding density matrix r_{AB} has positive partial transpose as well.

Similarly to the case where quantum states are given and measurements in certain bases are performed, there is no clear connection between the quantum and the classical regime yet. When measuring a quantum state we can only make a statement under the assumption of optimal measurements in the sense of choosing on good basis. As we showed in this paper by considering quantum states corresponding to classical probability distributions it only makes sense to speak of linking the quantum and the classical domain in connection with suitable phase functions (where it is not clear what suitable means).

References

[1] S. Wolf, Information-Theoretical and Computationally Secure Key Agreement in Cryptography, *Diss. ETH No. 13138*, pp. 1-110, 1999

[2] N. Gisin and S. Wolf, Quantum cryptography on noisy channels: quantum versus classical key-agreement protocols, *Phys. Rev. Lett.*, Vol. 79, pp. 2153-2156, 1997

[3] N. Gisin and S. Wolf, Linking Classical and Quantum Key Agreement: Is There „Bound Information“?, *Proceedings of Crypt 2000*, 2000

[4] J. Gruska, *Quantum Computing*, Mc Graw Hill, 1999

[5] K. Nipp and D. Stoffer, *Lineare Algebra* , vdf Hochschulverlag der ETH Zürich, Chapter 2, 3, 4, 6 and 7, 1992

[6] A. Schoeb, Analyse et comparisation de protocoles de purification de l'intrication quantique, Faculté des arts et des sciences, Université de Montréal, 1999

[7] G. Brassard, *Quantum Information Processing*, pre-print to appear in MIT-Press

[8] J. Preskill, Lecture Notes for Physics 229: Quantum Information and Computation, California Institute of Technology, 1998

[9] A. Peres, Separability Criterion for Density Matrices, The American Physical Society, Vol. 77/No. 8, 1996

[10] M. Horodecki, P. Horodecki and R. Horodecki, *Phys. Rev. Lett.*, Vol. 78, 390, 1997

[11] A. Peres, *Phys. Rev. Lett*., Vol 76, 1413, 1997

[12] R. Horodecki, P. Horodecki and M. Horodecki, *Phys. Rev. Lett.* A 210, 277, 1996

[13] M. Horodecki, P. Horodecki and R. Horodecki, Separability of Mixed Quantum States: Necessary and Sufficient Conditions, quant-ph/96050308, 1996

[14] P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, *Phys. Lett. A*, Vol. 232, p. 333, 1997

Appendix A: Common probability distributions

Y \ X (Z)	0	1
0	(0) $(1-\alpha)^2(1-\varepsilon)+\alpha^2\varepsilon$	(0) $\alpha(1-\alpha)$
	(1) $(1-\alpha)^2\varepsilon+\alpha^2(1-\varepsilon)$	(1) $\alpha(1-\alpha)$
1	(0) $\alpha(1-\alpha)$	(0) $(1-\alpha)^2\varepsilon+\alpha^2(1-\varepsilon)$
	(1) $\alpha(1-\alpha)$	(1) $(1-\alpha)^2(1-\varepsilon)+\alpha^2\varepsilon$

Table 1: General common probability distribution in the satellite scenario for Alice, Bob and Eve with the corresponding error bit rates α, β and ε respectively. The distribution must be normalized by the factor $1/2$.

Y \ X (Z)	0	1
0	(0) 7	(0) 3
	(1) 3	(1) 3
1	(0) 3	(0) 3
	(1) 3	(1) 7

Table 2: Common probability distribution from Table 1 with the corresponding error bit rates with $\alpha = \beta = 1/2$ and $\varepsilon = 1/4$. The distribution must be normalized by the factor $1/32$. Both I(X; Y↓ Z) > 0 and S(X; Y|Z) > 0 [1] so that secret-key agreement is possible.

Y \ X (Z)	0	1
0	(0) 3	(0) 1
	(1) 7	(1) 6
1	(0) 4	(0) 1
	(1) 2	(1) 8

Table 3: Random probability distribution. The distribution must be normalized by the factor $1/32$.

Y \ X (Z)	0	1
0	(0) 1	(0) 1
	(1) 1	(1) 1
1	(0) 1	(0) 1
	(1) 1	(1) 1

Table 4: Probability distribution derived from table 1 with $\alpha = \beta = 1/2$ and $\varepsilon = 1/2$ (norming factor $1/8$). Obviously I(X; Y↓ Z) = S(X; Y|Z) = 0, therefore no secret-key agreement is possible.

Appendix B: Maple program

This Program was running on Maple V Release 5 Version 5.00 with Intel 433. 1 precedure call of `GetEigenValues(·,·)` took less than half a second.

```
# Using linear algebra libraries:
restart: with(linalg):


####
# Function to generate quantum states, show their density matrix,
# eigenvalues of rohAB and rohABt using different phase functions.
####
GetEigenValues := proc (phasefn, PhasePhi)

# Environments:
local L2, L3, L4, Lnorm, Pxyz, phi, Pz, Phiz0, Phiz1, EV, x1, y1, x, y,
P_Phiz0, P_Phiz1, rohAB, A11t, A12t, A21t, A22t, rohABt, i, minEV;

# Number of valid digits+1:
Digits := 10:

# Classical distribution:
L2 := [[[7,3],[3,3]],[[3,3],[3,7]]]:  # see Table 2
L3 := [[[3,7],[4.5,2]],[[1,5.5],[1,8]]]:  # randum distribution, see Table 3
L4 := [[[4,4],[4,4]],[[4,4],[4,4]]]:  # see Table 4
# s := sum(sum(sum(L[i][j][k],i=1..2),j=1..2),k=1..2); # norming factor
Lnorm := L2/32; # choosing L2, L3 or L4
Pxyz := array(0..1, 0..1, 0..1, Lnorm):

# Defining Phase for conversion from Classic distribution to Quantum state:
phi := proc (x, y, z)
  if (phasefn = 0) then
    # all values a1, a2 and a3 are equal to zero:
    0;
  else
    if (phasefn = 1) then
      # values for a1, a2 and a3 for linear combination:
      (0.3626242 * x + 0.924623 * y + 0.4657161 * z) * 2/(0.3626242+0.924623+0.4657161) *
Pi;
    else
      if (phasefn = 2) then
        # no coefficients product of two parameters:
        (x * y + y * z + x * z) * 2/3 * Pi;
      else
        # chosen entries for phi coming from 2nd paramter in list:
        PhasePhi[4*x + 2*y + 1*z + 1];
      fi;
    fi;
  fi;
end;

# Get probability distribution of z:
Pz := proc(zp) Sum(Sum(Pxyz[xp,yp,zp], 'yp'=0..1), 'xp'=0..1) end;

# Calculating the quantum states Phiz0 and Phiz1:
Phiz0 := array(1..1, 1..2^2);Phiz1 := array(1..1, 1..2^2):
for x from 0 to 1 do
  for y from 0 to 1 do
    Phiz0[1, x*2+y+1] := exp(I*phi(x,y,0)) * sqrt(Pxyz[x,y,0] / Pz(0))
  od
od;
# and the same for Phiz1:
for x from 0 to 1 do
```

```
  for y from 0 to 1 do
   Phiz1[1, x*2+y+1] := exp(I*phi(x,y,1)) * sqrt(Pxyz[x,y,1] / Pz(1))
   # ...is that right?
  od
od;

# Creating projectors:
P_Phiz0 := transpose(conjugate(Phiz0)) &* Phiz0: evalm(P_Phiz0);
P_Phiz1 := transpose(conjugate(Phiz1)) &* Phiz1: evalm(P_Phiz1);

# Generating the mixed state:
rohAB := evalm(Pz(0) * P_Phiz0 + Pz(1) * P_Phiz1):# print("rohAB = ", evalf(%, 5));

# print rohAB:
if (phasefn <3) then # verbose output
  print("rohAB = ", evalf(%, 5));
fi;

# print eigenvalues of rohAB:
eigenvalues(evalf(rohAB)):
if (phasefn <3) then # verbose output
  print ("Eigenvalues of rohAB = ", evalf(%, 8));
fi;

# Calculate partial transpose of mixed state rohAB:
A11t := transpose(delcols(delrows(rohAB, 3..4), 3..4)): A12t :=
transpose(delcols(delrows(rohAB, 3..4), 1..2)):
A21t := transpose(delcols(delrows(rohAB, 1..2), 3..4)): A22t :=
transpose(delcols(delrows(rohAB, 1..2), 1..2)):
rohABt := stackmatrix (concat (A11t, A12t), concat (A21t, A22t)) :

# and finally get Eigenvalues 2 check if rohAB has positive partial transpose
EV := eigenvalues(evalf(rohABt)):
if (phasefn <3) then # verbose output
  print ("Eigenvalues of rohABt = ", evalf(EV, 8));
fi;
# and verify that rohAB is a valid quantum state:
if (phasefn <3) then # verbose output
  print ("Trace of rohAB = ", evalf(trace(rohAB), 8));
else
  minEV := Re(EV[1]);
  for i from 2 to 4 do # returns the smallest eigenvalue of rohABt
    if (Re(EV[i]) < minEV) then
      minEV := Re(EV[i]);
    fi;
  od; # postcondition: minEV := min (Re(EV[1]),...,Re(EV[4]))
  minEV;
fi;
end;


####
# Define random Phi(x,y,z) and show if rohABt is
# negative or positive partial transpose
####
Check4npt := proc (nums)  local j, rndnum, EV, count, MaxNums, PhiParams:
  count := 0; MaxNums := 10^10;
  # generate a random number from [0,2*Pi):
  rndnum := evalf(rand(0..MaxNums)*2*Pi/MaxNums, 10); # MaxNums := 4 is a good choice for
table 2

  print ("...looking for eigenvalues in rohABt for every Phi(x,y,z):");
  for j from 1 to nums do
    PhiParams := [rndnum(),rndnum(),rndnum(),rndnum(),
rndnum(),rndnum(),rndnum(),rndnum()];
```

```
    EV := (GetEigenValues(3, PhiParams)):
    if (EV >= 0) then # print only positive partial transpose
      count := count + 1: print (EV, "Phi: ", PhiParams);
    fi;
    if (j mod 50 = 0) then
      print ("checked ", j); # how far progressed
    fi;
  od;
  print (nums, " checked, ", nums - count, " rohAB are n.p.t., ",count, " are p.p.t");
end; # of proc
####
# Searching for eigenvalues.
# Probabilistic, adaptiv search over 8 parameters to find local maxima
####
SeekBigEV := proc (MaxCount, RoundsPerParam, Missrate)
  local count, ParamCount, AdjCount, MaxNums, ParamValueDelta, EVdelta, Missed, Hits,
        PhiParams, PhiParamsBest, CurrentParam, Delta, EV, EVbest, rndnum, rndParam,
        Direction, DirectReverses;
  count := 1; AdjCount := 0; Delta := 1;

  MaxNums := 6^10;
  # generate a random number from [0,2*Pi):
  rndnum := evalf(rand(0..MaxNums)*2*Pi/MaxNums, 10):
  rndParam := evalf(rand(0..7)+1, 1):

  # starting with these random parameters:
  PhiParams := [rndnum(),rndnum(),rndnum(),rndnum(), rndnum(),rndnum(),rndnum(),rndnum()]:
  PhiParamsBest := PhiParams:
  EVbest := -1: Missed := 1; Hits := 1;

  while (count <= MaxCount) do
    ParamCount := 1; Missed := 1;
    CurrentParam := round(rndParam()):
    print ("Param: ", CurrentParam):
    Direction := 1;
    PhiParams[CurrentParam] := PhiParams[CurrentParam] + .1; #rndnum()/20:
    if (PhiParams[CurrentParam] < 0) then
      PhiParams[CurrentParam] := -PhiParams[CurrentParam]:
    fi:
    while (evalf(PhiParams[CurrentParam] 2*Pi)) do
      PhiParams[CurrentParam] := evalf(PhiParams[CurrentParam] - 2*Pi):
    od:
    DirectReverses := 1;
    #while (DirectReverses <= RoundsPerParam) do
    while ((ParamCount <= RoundsPerParam) and (Missed < Missrate)) do
      EV := (GetEigenValues(3, PhiParams, Delta)):
      #print (EV, PhiParams):
      if (EV EVbest) then # good change
        EVdelta := EV - EVbest;
        ParamValueDelta := PhiParamsBest[CurrentParam] - PhiParams[CurrentParam]+0.0001:
        EVbest := EV:
        PhiParamsBest := PhiParams:
        AdjCount := AdjCount + 1: print (EV, "Phi: ", PhiParams, AdjCount):
        Missed := 1:
        Hits := Hits + 1:
      else
        Missed := Missed + 1:
        Hits := 1:
      fi;
      if (Missed mod 5 = 0) then
        Direction := -Direction; # change direction
        print ("reverse");
      fi;
      PhiParams[CurrentParam] := PhiParamsBest[CurrentParam] +
            EVdelta/ParamValueDelta*Missed*Hits*Direction;
```

```
      if (PhiParams[CurrentParam] < 0) then
        PhiParams[CurrentParam] := -PhiParams[CurrentParam]:
      fi:
      while (evalf(PhiParams[CurrentParam] 2*Pi)) do
        PhiParams[CurrentParam] := evalf(PhiParams[CurrentParam] - 2*Pi):
      od:
      if (count mod 50 = 0) then
        print ("progressing... ", count, " steps"); # how far progressed
      fi;
      count := count + 1;
    od;
  od;
end: # of proc
```

Appendix C: Numerical results

As seen in the program in Appendix B the number of numerical valid digits can be arbitrarily high. Te keep track of the result we chose `Digits := 10`. With exacter evaluation the first digits are not affected, in this case it suffices to calculate with 10 digits.

```
> # Using distribution from Table 2
> GetEigenValues(0, [] ); # using distribution L2

            [.31250    .23696    .23696    .28642]
"rohAB = ", [.23696    .18750    .18750    .23696]
            [.23696    .18750    .18750    .23696]
            [.28642    .23696    .23696    .31250]
"Eigenvalues of rohAB = ", .97391098, .02608902, 0, 0
"Eigenvalues of rohABt = ", .12500000, .96104596, .01286502, -.09891098
"Trace of rohAB = ", 1.

> GetEigenValues(1, []); # using distribution L2

            [.31250 , -.23344 - .040686 I , .063441 + .22831 I , -.028158 - .28502 I]
"rohAB = ", [-.23344 + .040686 I , .18750 , -.080473 - .16935 I , .063439 + .22831 I]
            [.063441 - .22831 I , -.080473 + .16935 I , .18750 , -.23344 - .040688 I]

            [-.028162 + .28502 I , .063442 - .22831 I ,
                                                    -5
             -.23344 + .040685 I , .31250 + .64282 10   I]
                                                  -9
"Eigenvalues of rohAB = ", .97391098 + .28996933 10   I,
                                 -10
        .026089019 + .77308121 10    I,
                     -9               -11
        -.23567562 10   + .17046070 10    I,
                     -11                -11
        -.51227430 10    + .64982917 10    I
                                                 -9
"Eigenvalues of rohABt = ", .96104596 + .19687262 10   I,
                                -9                                  -10
        .12500000 + .15682310 10   I, .012865017 + .36304280 10    I,
                                 -9
        -.098910981 - .10000000 10   I
                                              -7
 "Trace of rohAB = ", 1.0000000 + .40608932 10   I

> GetEigenValues(2, []); # using distribution L2

            [.31250 , .096335 + .081192 I , .096335 + .081192 I , .071605 + .12403 I]
"rohAB = ", [.096335 - .081192 I , .18750 , .18750 , -.11848 - .042838 I]
            [.096335 - .081192 I , .18750 , .18750 , -.11848 - .042838 I]
            [.071605 - .12403 I , -.11848 + .042838 I , -.11848 + .042838 I , .31250]
"Eigenvalues of rohAB = ", .54429451, .45570549, 0, 0
"Eigenvalues of rohABt = ", .50426549, .04002903, .49637114, -.04066564
"Trace of rohAB = ", 1.0000000

> # Check negative partial transpose with random defined Phi(x,y,z):
> Check4npt (500); # using distribution L2
     "...looking for eigenvalues in rohABt for every Phi(x,y,z):"
                                ...
     500, " checked, ", 500, " rohAB are n.p.t., ", 0, " are p.p.t"
```

```
> # Using distribution from Table 3
> GetEigenValues(0, []); # using distribution L3
```

```
            [.31250    .23176    .24804    .28799]
"rohAB = ", [.23176    .20313    .16993    .19129]
            [.24804    .16993    .20313    .23854]
            [.28799    .19129    .23854    .28125]
                                        -10             -10
"Eigenvalues of rohAB = ", -.51480997 10   , .23346120 10   , .052599837, .94740016
"Eigenvalues of rohABt = ", -.090864779, .027680568, .12777850, .93540571
"Trace of rohAB = ", 1.0000000

> GetEigenValues(1, []); # using distribution L3

            [.31250 , -.22831 - .039794 I , .066406 + .23898 I , -.028312 - .28659 I]
"rohAB = ", [-.22830 + .039792 I , .20313 , -.072932 - .15349 I , .051213 + .18431 I]
            [.066406 - .23897 I , -.072931 + .15348 I , .20313 , -.23500 - .040960 I]
            [-.028318 + .28659 I , .051216 - .18431 I ,
                                                      -5
             -.23500 + .040956 I , .28125 + .73465 10   I]
                                                    -9
"Eigenvalues of rohAB = ", .94740016 + .24961809 10   I,
                                  -10
        .052599837 + .43117600 10    I,
                      -11               -10
        -.45497853 10    - .46249579 10    I,
                      -9                -10
        -.10264291 10   - .10151001 10    I
                                                   -9
"Eigenvalues of rohABt = ", .93540571 + .37176622 10   I,
                                  -9                                  -10
        .12777850 + .24433932 10   I, .027680568 + .82104520 10    I,
                                   -9
        -.090864779 - .17821006 10   I
                                             -9
"Trace of rohAB = ", 1.0000000 + .41020675 10   I

> GetEigenValues(2, []); # using distribution L3

            [.31250 , .056364 + .10127 I , -.042827 + .16793 I , .20680 + .046877 I]
"rohAB = ", [.056364 - .10127 I , .20313 , .16993 , -.095645 - .050847 I]
            [-.042827 - .16793 I , .16993 , .20313 , -.11928 - .15246 I]
            [.20680 - .046877 I , -.095645 + .050847 I , -.11928 + .15246 I , .28125]
                                                    -9
"Eigenvalues of rohAB = ", .71480009 + .10436641 10   I,
                                  -10
        .28519991 - .14257820 10    I,
                      -9                -10
        -.22343504 10   - .29543661 10    I,
                     -10                -10
        -.42546571 10    + .27213845 10    I
                                                   -10
"Eigenvalues of rohABt = ", -.19622293 + .21007227 10    I,
                                  -10                                 -10
        .57448515 + .72220110 10    I, .43428404 - .15028756 10    I,
                                  -10
        .18745374 + .20801418 10    I
"Trace of rohAB = ", 1.0000000

> # Check negative partial transpose with random defined Phi(x,y,z):
> Check4npt (500); # using distribution L3
     "...looking for eigenvalues in rohABt for every Phi(x,y,z):"
                                  ...
     500, " checked, ", 500, " rohAB are n.p.t., ", 0, " are p.p.t"
```

```
> # Using distribution from Table 4
> GetEigenValues(0, []); # using distribution L4
```

```
            [.25000    .25000    .25000    .25000]
"rohAB = ", [.25000    .25000    .25000    .25000]
            [.25000    .25000    .25000    .25000]
            [.25000    .25000    .25000    .25000]
"Eigenvalues of rohAB = ", 0, 0, 0, 1.
"Eigenvalues of rohABt = ", 0, 0, 0, 1.
"Trace of rohAB = ", 1.

> GetEigenValues(1, []); # using distribution L4

            [.25000 , -.24629 - .042925 I , .066935 + .24088 I , -.024557 - .24880 I]
"rohAB = ", [-.24629 + .042925 I , .25000 , -.10730 - .22581 I , .066910 + .24088 I]
            [.066935 - .24088 I , -.10730 + .22581 I , .25000 , -.24628 - .042951 I]
            [-.024562 + .24879 I , .066914 - .24088 I ,
                                                      -5
             -.24628 + .042947 I , .25000 + .36733 10   I]
                                                     -9
"Eigenvalues of rohAB = ", 1.0000000 + .19330127 10   I,
                    -10                -10
        .90494578 10    + .53962778 10    I,
                    -10                -10
        -.76558471 10    - .11973942 10    I,
                    -10                -10
        -.18747551 10    - .18928511 10    I
                                                    -10
"Eigenvalues of rohABt = ", 1.0000000 + .49019238 10    I,
                    -9                 -10
        .31050426 10   + .38233404 10    I,
                    -10                -10
        -.39924318 10    - .20758880 10    I,
                    -10                -10
        .56519825 10    - .64596857 10    I
                                               -7
"Trace of rohAB = ", 1.0000000 + .23205104 10   I

> GetEigenValues(2, []); # using distribution L4

            [.25000 , .062500 + .10826 I , .062500 + .10826 I , .062500 + .10826 I]
"rohAB = ", [.062500 - .10826 I , .25000 , .25000 , -.12500]
            [.062500 - .10826 I , .25000 , .25000 , -.12500]
            [.062500 - .10826 I , -.12500 , -.12500 , .25000]
"Eigenvalues of rohAB = ", 0, 0, .37500000, .62500000
"Eigenvalues of rohABt = ", -.53784696, -.08715304, .47391098, -.09891098
"Trace of rohAB = ", 1.0000000

> # Check negative partial transpose with random defined Phi(x,y,z):
> Check4npt (500); # using distribution L4
     "...looking for eigenvalues in rohABt for every Phi(x,y,z):"
                                  ...
     500, " checked, ", 500, " rohAB are n.p.t., ", 0, " are p.p.t"
```

Appendix D: Searching a suitable phase function

It is not easy to find, with a numerical approach, a phase function with the property that r^{t}_{AB} has only non-negative eigenvalues (if any exists at all). In Figure 3 we can see a surface obtained from the function $f(a_{000},...,a_{111})$ returning the smallest eigenvalue of r^{t}_{AB} with respect to the phase $f(x,y,z)$ as defined in (11) choosing $f(0,0,0)$ $f(0,0,1)$ and $f(0,1,0)$ (i. e., a_{000}, a_{001}

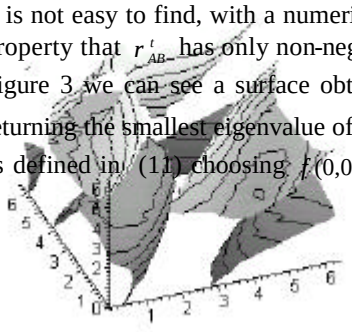


Figure 3: Lots of local maxima < 0

and a_{010}) as parameters within $[0,2\pi)$ and fixing the other 5 parameters to fixed values (see Appendix B). The values a_{xyz} correspond to the results for a call of the phase function $f(z,y,z)$ used in the algorithm. Figure 3 shows the surface with level with $f(\cdot) = -0.15$. This function has a lot of local maxima less than zero. So it was not possible to achieve a separable state ρ_{AB} corresponding to $P_{XYZ}(x,y,z)$ (table 2) with the approach by using an adaptive probabilistic algorithm (best result $f(\cdot)$ = -.0000125604 9187, with less than 500 evaluations). On the other hand a search with randomly chosen parameters spread over the unit circle spawned the solution in the proof of Theorem 2, where $f(\cdot) = 0$.

Thanks to Stefan and Remo for orthographical corrections...