The mechanics of quantum cryptography in aspects of dichotomy, transgression and synaesthesia

1. Introduction

This paper wants to outline the relationship of quantum cryptography towards a contemporary concept of synaesthesia and the production of meaning on the side of the recipient. In order to describe this relationship, it is necessary to provide some information relevant to this subject.

At first, there will be an introduction of the "Mathematical Theory of Communication" by Claude Shannon published in 1949, in order to show how information theory deals with the phenomenon of communication and that this model in particular is not only suitable to describe and explain the technical issues that are involved here, it also complies to the conditions of spoken and written language. By establishing this more natural scientific interpretation of the term "communication" , it is now possible to describe the processes involved in cryptography, for which Shannon also provides a "communication theory of secrecy systems".

By knowing the basic conditions of cryptography, the text will then introduce quantum cryptography and will show why this form of cryptography is different from the traditional forms and why this particular technique of enciphering and deciphering messages that carry meaning may be able to contribute to an extension our understanding of communication and logic and our view towards nature. In quantum physics, it is only possible to give rules by formulating mathematical probabilities because our traditional concepts of logic and physics – in a Newtonian sense – do not apply here any longer. Although we may not be able to determine the nature and "logic" of quantum physics definitively by the methods that have been proven reliable in the past, we are able to encode information and meaning by quantum states that can only be measured through probabilities.

Although Kant pointed out in his "Kritik der reinen Vernunft" that the "thing by itself" is not recognizable and only appears to us through our senses, it is now possible to use this phenomena of the unrecognizable "thing as such" as a carrier of information, it gets augmented by synaesthesia and the production of meaning. To describe it in Luhmannian terms, the synaesthesia has undergone a process of out-differentiation in domains that not only are part of the nature as we perceive it, but to the underlying principle of nature that we are unable to perceive.

In order to examine the relationship of nature in our perception opposed to the principles of nature a bit further, the text will also focus on Werner Heisenberg's philosophical outlines towards quantum physics. After making it understandable that the classical logic is merely a special case of something called "quantum logic", the text will reflect the reception of quantum theory of the physicists as well as in literary science.

2. The mathematical theory of communication

In his "mathematical theory of communication", Claude Shannon refers to the word "communication" in a broad definition by which one mind may affect another and, to broaden the definition of the term a bit further, it could also include the procedures by means of which one mechanism affects another mechanism. In this initial outline are three levels of communication problems, whereas the focus of this chapter will be the first level of problems. The technical problem, described as Level A, deals with the accuracy of transference from sender to receiver in general, may it be a set of symbols as in written speech or a continuously varying signal as in the transmission of voice and music or a continuously varying two-dimensional pattern as in television. In a mathematical sense, written speech involves the transmission of a discrete set of symbols, voice and music involve the transmission of a continuous function of time, and television deals with the transmission of either many continuous functions of time or of one continuous function of time and two space coordinates.

Shannon's concept of a general communication system involves five main parts (Fig. 1). First, there is the information source which selects a message out of a set of possible messages. The transmitter then changes the message into a signal which is actually sent over the communications channel to the receiver, which can be described as a sort of inverse transmitter that is changing the transmitted signal back into a message and forwarding this message to the destination. In the process of this transmission, there are changes in the initial signal involved which were not intended by the information source. All of these changes in the transmitted signal are referred to as noise.

Having established this communication system, it is now vital to be concerned with the measurement of information. Due to the technical nature of this theory, it is important to point out that within this communication system, information is considered apart from its meaning, it is merely defined as a measure of the freedom of choice in selecting a message. The logarithm of the number of available choices is defined as a measurement of the amount of information. If there are only two choices, it is equal to the logarithm of two to the base two ($\log_2 2 = 1$) which results in one, so that this situation is characterized by information of unity. This particular unit of information is called a "bit", which is a short form of "binary digit". If there, for example, would be a situation where it would be possible to choose out of sixteen alternative messages, this situation is characterized by four bits of information ($16 = 2^4$; $\log_2 16 = 4$).

If the information source gives out a sequence of choices from one set of elementary symbols, the sequence selected is responsible for the articulation of the message. The choice of successive symbols is governed by probabilities which depend upon preceding choices at any stage of the process. A system which produces a sequence of symbols as described is called a stochastic process and such a process in which the probabilities depend on previous events is called a Markoff process. The quantity which meets the natural requirements that are kept up for "information" is what is known in thermodynamics as entropy. In physics, the entropy associated with a situation serves a measurement of the degree of randomness in this situation and the tendency of systems to reduce their degree of organization. It is now possible to make statements about the degree of information of a communication source as in the case of physical systems. The more organized a system is and the less it is characterized by a large degree of randomness of choice, the lower the value of entropy or the value of information is. By calculating this entropy of a certain information source, it is possible to compare this to the maximum value the entropy could have, given the condition that the source continues to operate with the same symbols. The ratio of the actual to the maximum entropy is called the "relative entropy" of the source. This relative entropy is necessary to determine the amount of redundancy in a message, which is calculated by one minus the relative entropy. The redundancy refers to those parts of the message that could be deleted without losing the essential completeness of the message. This structural part of the message is not determined by the free choice of the sender, but by the accepted statistical rules governing the use of the particular symbols.

> "It is most interesting to note that the redundancy of English is just about 50 per cent, so that half of the letters or words we choose in writing or speaking are under

> our free choice and about half (although we are not ordinarily aware of it) are really controlled by the statistical structure of the language. Apart from more serious implications, which again we will postpone to our final discussion, it is interesting to note that a language must have at least 50 per cent of real freedom (or relative entropy) in the choice of letters if one is to be able to construct satisfactory crossword puzzles. If it has complete freedom, then every array of letters is a crossword puzzle. If it has only 20 per cent of freedom, then it would be impossible to construct crossword puzzles in such complexity and number as would make the game popular. Shannon has estimated that if the English language had only about 30 per cent redundancy, then it would be possible to construct three-dimensional crossword puzzles." [1]

To give a mathematical expression of the measurement of information in similar to the behaviour of entropy, let us assume a set of n independent symbols or n independent messages, with the probabilities of choice like $p_1, p_2, \ldots p_n$, then the actual expression for the information is $H= - [p_1 \log p_1 + p_2 \log p_2 + \ldots + p_n \log p_n]$, or, to put it simpler,
$H = - \sum p_i \log p_i$. H stands for the information, or the entropy, whereas $\sum$ indicates to sum all terms that may occur like the one given in the example, $p_i \log p_i$. Let us now assume further that it is only possible to choose between two possible messages, with the probabilities p_1 for the first and $p_2 = 1 - p_1$ for the second. Now H has its greatest value, which is 1, when the two messages are equally probable, when $p_1 = p_2 = ½$, or, as mentioned before, when one is completely free to choose between the two. Just as soon as one message gets more probable than another, the value of H decreases. When one probability is unity and the other is zero, then H is zero as well. The latter case may also be described as certainty, because there is no other probable possibility than just one. If there is no uncertainty and no freedom of choice, then there is no information in the sense as described above. So, if all choices possess the same probability ,the more choices will exist and the larger H will be.

Another matter that the mathematical theory of communication is concerned with is the capacity of a communication channel. This capacity is described by the amount of information it transmits and not by the number of symbols. If the source emits symbols that all have the same duration of time, each symbols represents s bits of information and the

[1] Warren Weaver, Some Recent Contributions to the Mathematical Theory of Communication, pp. 13, in: Claude E. Shannon, Warren Weaver, The Mathematical Theory of Communication

channel is able to transmit *n* symbols per second, then the capacity *C* of the channel is defined as *ns* bits per second, which serves as a unit for the amount of information.

A further process which is important for the mathematical communication model is the process of coding. When the transmitter turns the initial message into a signal, it encodes the message, whereas the receiver decodes the signal in order to get the message again. In a noiseless channel that is transmitting discrete symbols and has the capacity of *C* bits per second and is accepting signals from a source of information of *H* bits per second, it is now possible to formulate a theorem which states that ‚given a proper coding procedure for the transmitter, it is possible to transmit symbols over the channel at an average rate of nearly *C/H* but at the same time can never exceed *C/H*. Since the information associated with the process which generates signals or messages is determined by the statistical character of the process, the statistical nature of messages is entirely determined by the character of the source.

While information is a measure of the freedom of choice in selecting a message, the greater this freedom of choice is, the greater is the uncertainty that the message selected can be defined as a particular one, as explained in the relationship of information, entropy and its probabilities. When it comes to noise, the received signal contains certain distortions or errors that may lead to the conclusion of an increased uncertainty due to the effects of noise, which may again lead to the irritating conclusion that noise could be regarded as something beneficial within the mathematical model of communication. In order to prevent this, it is vital to distinguish between desirable and undesirable forms of uncertainty. To obtain the useful information in the received signal, the spurious parts have to be subtracted. If, in a certain communication ensemble, it is known that a certain signal symbol has been received, a certain probability for each message symbol is assigned, relatively large for the symbol similar to the one received, and relatively small for all the others. By using this set of probabilities, it is now possible to calculate a “tentative entropy” value, which is the entropy of the message on the assumption of a definite known received signal or a symbol. It is further possible to calculate those tentative message entropies for each assumption that is similar to the one described, namely the signal symbol that is received, by calculating and averaging all of them and weighting each one in accordance with the probability of the signal symbol assumed in calculating it. Entropies that are calculated in this way when there are two sets of symbols to consider are called “relative entropies”. The particular entropy of the message relative to the signal as described is also called equivocation. This equivocation measures the average uncertainty in the message when the signal is known.

If *H (x)* is the entropy or the information of the source of messages, *H (y)* the entropy of information of the received signals, H_y *(x)* the equivocation and H_x *(y)* the uncertainty in the received signal which occurs due to noise, it's not hard to prove that

$H(x) – H_y(x) = H(y) – H_x(y)$, the right side of this equation being the useful information which is transmitted despite the undesirable effects of noise. Under those circumstances, the capacity *C* of a noisy channel is defined to be the equal maximum rate, in bits per second, at which useful information, that is, the total uncertainty minus the "noisy" uncertainty, can be transmitted over the channel. If now this noisy channel has a capacity *C*, as described, and is accepting signals from an information source which has an entropy of *H (x)* bits per second, the entropy of the received signals being *H (y)* bits per second. If the capacity *C* is equal to or larger than *H (x)* , the output signal of the source can be transmitted over the channel with as little error as desired. If the capacity *C* is less than *H (x)*, it is impossible to reduce the error frequency. After a signal is received, there will always remain some undesirable uncertainty, or noise, regardless of the efficiency of the coding process ,which will always be equal to or greater than *H (x) – C*. There is always at least one code that is able to reduce the noise down to a value which exceeds *H (x) – C*. The important aspect of those implementations is that the minimum of remaining noise cannot be reduced any further, no matter how sophisticated the coding process.

> "One practical consequence, pointed out by Shannon, should be noted. Since English is about 50 per cent redundant, it would be possible to save about one-half the time of ordinary telegraphy by a proper encoding process, *provided* one were going to transmit over a noiseless channel. When there is noise on a channel, however, there is some real advantage in not using a coding process that eliminates all of the redundancy. For the remaining redundancy helps to combat the noise. This is very easy to see, for just because of the fact that the redundancy of English is high, one has, for example, little or no hesitation about correcting errors in spelling that have arisen during transmission."[2]

The mathematical theory of communication not only applies to messages formed out of concrete symbols, but also to continuous messages which have variations in their signal.

[2] Warren Weaver, Some Recent Contributions to the Mathematical Theory of Communication, p. 22, in: Claude E. Shannon, Warren Weaver, The Mathematical Theory of Communication

Those variations are considered as frequencies which should not be observed entirely but rather within a band of zero to a frequency of *W* cycles per second. Mathematically spoken, it is possible to specify a continuous signal with *T* seconds in duration and band-limited in frequency to the range from zero to *W*, by stating *2TW* numbers. Normally, it is only possible to characterize a continuous curve by stating a finite number of points through which the curve passes. Therefore, an infinite number of points would be required for complete information about the curve, but if simple harmonic constituents of a limited number of frequencies built up the curve, a finite number of parameters is all that is necessary. Given the assumption of a maximum capacity *C* of a channel of frequency bandwidth *W* and the average power used in transmitting is *P*, the channel being exposed to a noise of power *N*, this noise is characterized as white thermal noise that is band limited in frequency and the amplitudes of those frequencies are subject to a normal, that is Gaussian, probability distribution, it is possible to transmit, by the best coding, binary digits by the rate of

$W \, log_2 \frac{P+N}{N}$ bits per second and have an arbitrarily low error frequency, which cannot be reduced any further once a definite minimum frequency of errors is calculated.

Recapitulating all mentioned processes concerning the mathematical theory of communication, it is to say that the sheer generality of its scope and the fundamentality with which the occurring problems are treated were the main reasons that the theory was introduced in the broader context of this paper. The lack of a need to specify the symbols that are used in a specific case and the profoundness of the relationships involved in a given communication process make it applicable to all forms of communication, especially when the relationship of a total of three forms of communication is considered, which are a message that is understandable to humans is being transformed into binary or computational language, then being encrypted by a specific process, that is to be introduced shortly, and finally being send to a receiver which reverses all the processes described. It may not seem surprising that Shannon also formulated a theory of cryptography which he considers a special form of coding that is to be introduced in the following chapter.

Furthermore, the concept of information developed in this theory as a concept of entropy applies to the broader context of this particular approach, since it has been used to contribute to a reconciliation of the theories and the factions of the natural sciences and the humanities or the cultural sciences, as it was done by authors like Thomas Pynchon and theoreticians like Gilles Deleuze who also mention the importance of the second law of thermodynamics which is concerned with entropy and could be regarded as an intersection between poststructuralist or post-modern thinking and chaos theory.

3. Shannon's theory of secrecy systems and methods of modern cryptology

Shannon's work on secrecy systems contains two main parts, theoretical secrecy and practical secrecy. In the first part Shannon applies the mathematical apparatus developed in his "theory of mathematical communication" to cryptography and defines random, pure, perfect and ideal types of cryptosystems. He shows that perfect security in information theoretic settings can only be obtained in extreme cases, for example, when the amount of the key is longer or equal to the amount of message symbols. A secrecy system is defined as a set of transformations T of the set of possible messages M into the set of possible cryptograms E. Each particular transformation T_k: $M \rightarrow E$ of the set T corresponds to enciphering with a particular key k. Transformations are supposed to work one on one, so that unique decryption is possible when the key is known (Fig. 2). The key source produces a key from among those which are possible in the specified system. This key is transmitted in a non-interceptable way to the receiving end. Then, the message source produces a message which is enciphered and the resulting cryptogram is send to the receiver, where the cryptogram and the key are combined in the decipherer to recover the message. It is possible to represent the enciphering and deciphering operations as $e = f\ (m,k)$ and $m = g\ (e,k)$, with m being the message, k the key, and e the enciphered message or the cryptogram. It is preferable to think of this not as a function of two variables but as a family of transformations, that is $e = T_k m$. At the receiving end, it must be possible to recover m by knowing e and k. Thus the transformation T_k in the family must have unique inverses T_k^{-1} such that $T_k T_k^{-1} = I$, the identity transformation, thus the message can be defined as $m = T_k^{-1} e$. Such an inverse must exist uniquely for every e which can be obtained from a message m with key k.

Assume that there are only a finite number of possible keys, each has an associated probability p_i and there are a finite number of possible messages $m_1, m_2, \ldots, m_n$ with associated "a priori" probabilities $q_1, q_2, \ldots, q_n$. The possible messages might be the possible sequences of English letters all of length N, and the associated "a priori" probabilities are the relative frequencies of occurrence of these sequences in normal English text. If the enemy intercepts the cryptogram, he can calculate from it “a posteriori” probabilities of the different possible messages and keys which might have produced this cryptogram. Thus the “a posteriori” probabilities constitute knowledge of the key and message after the interception.

In a pure system, the messages can be divided into a set of “residue classes” C_1 , $C_2,\ldots,$ C_s and the cryptograms into corresponding sets of residue classes C'_1 , $C'_2,\ldots,$ C'_s with the following properties, that first, the message residue classes are mutually exclusive and collectively contain all possible messages. Similarly for the cryptogram residue classes. Second, enciphering any message in C_i with any key produces a cryptogram in C'_i. Deciphering any cryptogram in C'_I with any key leads to a message in C_i. Third, the number of messages φ_I in C_i is equal to the number of cryptograms in C'_I and is a divisor of $/K/$ the number of keys. Fourth, each message in C_i can be enciphered into each cryptogram in C'_I by exactly $/K//\varphi_I$ different keys and similarly for decipherment.

A cryptosystem is called perfect if the “a posteriori” probability is equal to the “a priori” probability, namely $P_e(m) = P\ (m)$, with P being the probability of the decrypted message m and P_e being the probability of the encrypted message , whereas $P\ (m) = 0$ is a solution that has to be excluded since it is vital to demand equality between $P_e(m)$ and $P\ (m),$ independent of the values of $P\ (m)$. Perfect systems in which the number of cryptograms, the number of messages and the number of keys are all equal are characterized by the properties that each m is connected to each e by exactly one possible conjunction and that all keys are equally likely. The one-time pad system, for example, first proposed by Gilber Vernam of AT&T in 1926, is such a perfect system. This algorithm requires the generation of many sets of matching encryption keys pads. Each pad consists of a number of random key characters. These key characters are chosen completely at random and are not generated by any kind of cryptographic key generator. Now, each party involved receives a matching sets of pads and each key character in this pad is used to encrypt only one plain text character, then the key character is never used again. Any violation of these conditions negates the perfect security available in the one-time pad.

The standard for cryptography that is used today is called RSA, after the developers Rivest, Shamir and Adleman, all three being researchers of the MIT Laboratory for Computer Science, who developed this system in April 1977. They looked for a procedure that could ensure two operations. First, the message source, which will be called Alice in the following, must create a public-key, which has to be published, so that the receiver, which will be called Bob, can use it to encrypt messages for Alice. Because the public-key serves as a one-way function, it must be virtually impossible for anybody to reverse the Alice's message. Second, Alice needs to have a private-key as well, which allows her to decrypt the messages being sent to her and to reverse the effect of the public key, but it is necessary that she alone possesses the ability to decrypt any messages sent to her.

Alice picks two giant prime numbers, p and q, which she must keep secret and multiplies them together to get another number, N. She now picks another random and most preferably prime number e. Alice can now publish e and N. Since these numbers are necessary for encryption, they must be available to anybody who might want to encrypt a message to her. Together, these numbers constitute the public-key. To encrypt a message, the message must be first converted into a number, M. For example, a word is changed into binary digits, and the binary digits can be considered as a decimal number. M is then encrypted to give the ciphertext C, according to the formula $C=M^e(mod\ N)$.[3] To encrypt a message to Alice, Bob begins by looking up her public-key, namely N and e. This provides him with the encryption formula and allows him to send a ciphertext C to Alice. Since exponentials in modular arithmetic are one-way functions, it is very difficult to work backwards from C and recover the original message M. Hence, an enemy cryptanalyst, which will be called Eve, cannot decipher the message. However, Alice can decipher the message because she knows the values of p and q .She now calculates a special number d, the decryption key, otherwise known as her private-key. The number d is calculated according to the formula $ed = 1\ (\ mod\ (p - 1\ )\ (q - 1))$. To finally decrypt the message that was being sent, she uses the formula $M = C^d\ (\ mod\ N)$. The RSA cipher is used to protect the most important military, diplomatic, commercial and criminal communications today and is considered to be a cornerstone of modern encryption. The efficiency of RSA lies in the unreasonable amount of time a regular, and even powerful, computer would need to calculate, in Shannon's terms, the exact "a posteriori" probabilities to break its encryption. The next chapter will illustrate how it could be possible, at least theoretically, to break the RSA cipher in an acceptable amount of time and how this still theoretical problem is already solved.

4. Quantum computing and quantum cryptography

One thinkable approach of breaking an RSA cipher would be to check each prime number one at a time in order to find out if it divides into the number N .As mentioned before, the

[3] *mod* stands for the mathematical operation modulo which is used to calculate the remainder of a whole-numbered division. For example: 7 mod 3=1 , because 7:3=2, remainder 1.

sheer amount of time required for those calculations would make the attempt impractical, since a ordinary computer can only process one arithmetic operation at a time. But the, still theoretical, concept of a quantum computer, which was first introduced by David Deutsch in 1985 and works with spinning particles as constituents of its binary code, could provide a solution. A spinning particle has two spinning directions, east and west, and the binary code applies to those spinning directions. Having the same mathematical value as binary digits, a combination of seven particles, for example, can represent any number between zero and 127. The particle spins can be altered with pulses of energy and if this is done in a place that is out of a beholder's view, quantum laws apply to those particles as they enter a state of superposition, a term that was first phrased by Erwin Schrödinger in his famous example of "Schrödinger's cat" in 1935. With all particles being in a state of superposition, they have entered a value between the binary values of zero and one and effectively represent all possible combinations of eastward and westward spins and therefore, the quantum computer would be able to perform one calculation on all 128 numbers, according to the given example, simultaneously, whereas a common computer would need 128 single calculations on each number.

> "Quantum computing is *Twilight Zone* technology. […] When traditional computers operate on 1's and 0's, the 1's and 0's are called bits, which is short for binary digits. Because a quantum computer deals with 1's and 0's that are in quantum superposition, the are called quantum bits, or *qubits* […]. The advantage of qubits becomes even clearer when we consider more particles. With 250 spinning particles, or 250 qubits, it is possible to represent roughly 10^{75} combinations, which is greater than the number of atoms in the universe. If it were possible to achieve the appropriate superposition with 250 particles, then a quantum computer could perform 10^{75} simultaneous computations, computing them in just one second"[4]

It should have become obvious that the concept of quantum computing could easily break the RSA cipher. Inevitably, the question arises in how far this potential security leak could be fixed. In contrast to the theory of quantum computing, which is still a purely theoretical idea, the concept of quantum cryptography is already being tested under practical

[4] Simon Singh, The Code Book, p. 329

circumstances and the number of little technical improvements and new theoretical insights grow further each day.

The phenomenon of quantum cryptography is to be located at the intersection of quantum mechanics and information theory and the inherent tension between those two categories is closely connected to the security of quantum cryptography. Quantum cryptography contributes to revaluate the negative viewpoint of quantum physics and its establishing of rules out that viewpoint. There are five basic rules concerning quantum mechanics, which are that first, it is impossible to take measurement without perturbing the system, second, it is not possible to determine simultaneously the position and the momentum of a particle with arbitrary high accuracy, third, it is impossible to simultaneously measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis, fourth, it is not possible to draw pictures of individual quantum processes and fifth, it is impossible to duplicate an unknown quantum state. What is done in quantum cryptography is that Alice and Bob do not use the quantum channel to transmit information, they merely use it to transmit a random sequence of bits, or more precisely, qubits, which serves as the key, explained in the context of the RSA cipher, which is an asymmetrical cryptosystem or the one-time pad, which is a symmetrical one. As Shannon already pointed out, a symmetrical cryptosystem that has to be perfectly secure produces long sequences of key bits. A potential threat to its security is the distribution of the key to the receiving end.

In terms of physics, the one-time pad can be regarded as "classical teleportation". If Alice wants to make a copy of a classical system, merely a classical communication system that constitutes a message, for example a written text, her and Bob only have access to an insecure classical channel. If the secret key is arbitrarily long and they both have access to it over the channel, Alice is able to measure the state of the classical system with arbitrarily high accuracy and by using the one-time pad to securely communicate this information to Bob, who can then reconstruct the classical system in its initial state. Since the phenomenon of quantum teleportation has been discovered in 1993, it can be regarded as the quantum version of a one-time pad, or as the form of quantum cryptography, since the situation here is only slightly different. If Alice aims to transfer a copy of a quantum system to Bob, they both must have access to a quantum key, which is build of an arbitrarily high number of qubits. If they share a classical communication channel as well, the quantum teleportation protocol provides them with a means transferring the quantum state of the system from the information source to the receiving end. If the initial quantum system is a quantum message encoded in the form of a qubit sequence, it is possible to transfer this message without any security threats.

Particles that could serve as qubits are photons which can be polarised by energy impulses. The polarisation of a photon is the oscillation level of its surrounding electric field. If the oscillation happens only in one level, the polarisation is called linear, whereas the polarisation is circular if the whole field is spinning. Every polarisation is constituted out of two components, if those two polarisation components are superimposed in the horizontal and vertical level and the superimposition is taking place with the same phase level, there will be a linear polarisation in a level of 45° and if the phase levels vary about 90°, the outcome will be a circular polarisation. As mentioned before, it is only possible to measure the amplitudes of a polarised photon, namely horizontal or vertical, and it is not possible to simultaneously measure the phase level of the polarised components, due to Heisenberg's uncertainty principle, whereby the initial polarisation of the photon is indeterminable. The first protocol for quantum cryptography exploiting this seeming disadvantage was the BB84 protocol, which was proposed in 1984 by Charles H. Bennet of IBM and Gilles Brassard of the University of Montreal. In this protocol, Alice possesses a source which could emit single photons with one of four total possible polarisations, namely 0°, 90° and 45°, 135°, and both Alice and Bob have access to an additional public communication channel. It is important that Alice randomly chooses the mode of polarisation of a photon, whereas Bob tries to analyse the photon emitted by Alice with his polariser that has two exits, "+" and "-", according to the orthogonal polarisation directions. Photons with a polarisation of 0° or 90° can only be measured with a polariser adjusted at 0°, similarly for photons polarised at 45° or 135°, which only can be measured with a polariser adjusted to 45°. Any measurement taken with an improper adjustment for the specific photons, for example measuring a polarised photon at 0° with a polariser adjusted to 45,° delivers totally random results that do not lead to any conclusions about the photon and its polarisation. Since Bob cannot know anything about the photons in the first place, he just has to switch between the two adjustments randomly and has a probability of fifty per cent to get the right adjustment for the right polarisation. He now notes the result of the measurement along with the polariser adjustment for every photon that is being sent to him. This particular procedure makes it impossible for any recipient, be it Bob or an enemy cryptanalyst Eve, to verify the correctness of the measurement taken. When every qubit is being sent, Bob tells Alice over the public channel which polariser adjustment he had taken for every photon, without telling her the result. Alice now compares Bob's adjustments with the actual polarisation of each photon and tells Bob which photons he had measured with the right adjustment. Out of those correct measurements, the quantum key is being built. For each 0° polarisation, a binary zero is allocated and for each 90° polarisation a binary one. Likewise for the 45° and the 135° polarisation. The verification of the quantum key is accomplished by an extraction of a sample from the gathered data that is compared by Alice and Bob. From this sample, the error rate is concluded. If Eve would attempt an attack with a beam-splitter, this would result in an incompleteness of the key, since photons or qubits cannot be separated or copied. If a qubit would be copied, the total information of one qubit would be divided into two qubits which would then possess an amount of information that would be less than one binary digit ,and therefore, they would not have the right quantum condition. An attempt to eavesdrop all photons and afterwards sending them to Bob would result in an error rate of twenty five per cent, because Eve has, like Bob, a probability of fifty per cent to measure the incoming photons correctly. If Bob would do a new measurement with the photons being sent to him by Eve, twenty five per cent of the results would be wrong, which would be above the predefined error rate of fourteen per cent.

Quantum cryptography in its practical realisation demands two major criteria. First, it has to be assured, that only one photon is emitted from the information source and second, the initial polarisations have to be chosen by perfect coincidence. In order to achieve that, physicists nowadays work with entangled photon pairs which are characterized by a correlation in polarisation, no matter how large the distance between them is. Because of this, it is also called "non-locality". This phenomenon was first described in 1935 by Albert Einstein, Boris Podolsky and Nathan Rosen in a theoretical outline, known as the EPR experiment. It hasn't been carried into execution for almost thirty years, but as John Bell formulated his inequality in 1964, quantum physics finally found possibilities to test the phenomenon of non-locality in entangled photon pairs in praxis. If entangled photon pairs are measured by two opposite polarisers with the same angle adjustments, they always measure opposite results which is called anti-correlation. If, for example, Alice and Bob have adjusted their polarisers at 0°, one of them will measure a "-" polarisation whereas the other will measure a "+" polarisation. The combinations of those measurements, that is, which will occur first, "-" or "+", are perfectly random and cannot be conducted or predicted. If their polarisers differ in their angle adjustments, the anti-correlation decreases up to a difference of 45° between them. From this point on, they get total independent results, which means that even combinations of "-/-" and "+/+" results occur in equal randomness and frequency. A quantum key with entangled photon pairs is generated by Eve and Bob if they measure all incoming photons by randomly switching between the 0° and 45° positions on the polarisers and keeping the results secret at first. Over the public channel, they search for all measurements that were taken with the same polariser adjustments for which they get perfect complementary sequences. Those sequences are finally transformed into a quantum key.

> "Quantum cryptography is a fascinating illustration of the dialog between basic and applied physics. It is based on a beautiful combination of concepts from quantum physics and information theory and made possible by the tremendous progress in quantum optics and the technology of optical fibers and free-space optical communication. Its security principle relies on deep theorems in classical information theory and on a profound understanding of Heisenberg's uncertainty principle […]."[5]

Having explained the mechanics of quantum physics and information theory in mathematical detail, it now seems necessary to focus on the philosophical aspects of those concepts. Within this effort, it is noteworthy that Werner Heisenberg, although being a physicist in the first place, has also made several publications concerning the ontological and epistemological aspects of quantum physics, which try to point out the relevance of quantum theory in relation to our basic understanding of reality and the laws that we regard as applicable to it.

5. Werner Heisenberg and the philosophical value of uncertainty

In his work "Physics and Philosophy" which was first published in 1958, Heisenberg tries to reflect upon the various aspects concerning the importance of modern physics in relation to the current modes of the perception of reality, which include matters like language and reality in relation to modern physics as well as the history of quantum theory or the development of philosophical ideas in comparison to the new circumstances within quantum theory.

This paper will only focus on some of his ideas, which could be regarded relevant to outline the historical methods and processes of natural science and how this understanding

[5] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Quantum cryptography, Reviews of Modern Physics, Volume 74, January 2002

has changed during the course of the twentieth century, resulting in such interdisciplinary techniques as quantum cryptography. Renè Descartes, the famous French philosopher of the seventeenth century, who was concerned with a formation of a consistent natural science on a mathematical basis, recognized that the knowledge about our own thinking could be regarded as more reliable than our thinking about the outer world. In contrast to Greek philosophy, which was always concerned of establishing an order within the infinite variety of things and apparitions by searching for one main principle, Descartes proposed to find order throughout a basic division into the "res cogitnas" and the "res extensa", that is, the intellectual and the extended. Whereas the intellectual is taking place only in a human mind, the extended applies to all forms of matter that does not possess intellect. This dichotomy was quite efficient in the natural sciences for several centuries because it created the possibility of describing the world without the necessity of making statements about ourselves or god. Natural science doesn't try to describe nature by itself but more nature as it is exposed to our methods and questions. Since the development of quantum physics, the philosophical thesis of all cognition being based on experience or, more precisely empiricism, has been proven insufficient. In relation to the kind of knowledge gained in the field of quantum theory, it seems that it is not possible to determine the limits of practicability of certain terms in accordance to the expansion of our knowledge. All terms that have been built out of the relationship between the world and ourselves are blurry defined in respect of their meaning. They can be used in various fields of our inner and outer experience but we cannot definitively know where the limits of their applicability, for example, terms like time and space. What is indeed precise is the definition of their conjunctions to other terms when they are part of a system of axioms and definitions that could be transferred into a mathematical system without any contradiction as it has been done in classic information theory where the term "information" is made equal to the term "entropy" and thus, it is then possible to define "information" within mathematical theorems and calculations. As those terms, assigned to different scientific categories in the first place, build a new category by their redefined meanings that have been proven efficient by mathematical calculations, they are now applicable to an even broader field of empiricism, what allows us to map this empiric field by our logical methods, as it was done in information theory, although the limits of applicability in a newly mapped empiric field still remain not clearly defined. That information theory would have the ability to establish something like quantum cryptography could not be known by the originators, but it was the uncertainty of applicability that has been redefined over and over in the course of their development in both fields, quantum physics and information theory, that finally allowed the possibility to combine specific elements of each scientific field into a new one called quantum cryptography.

Within the process of expansion of scientific knowledge, the language that is used to reflect, store and distribute this knowledge expands as well. This process either results in introducing new terms for specific circumstances or in redefining terms that are already known apart from their common usage. One of the basic problems of quantum physics was the lack of a language that would allow to discuss the given situations without any form of contradiction. Common language relied upon the traditional terms of time and space which constituted the means of non-ambiguous communication about the arrangement and the results of measurements, whereas simultaneously the conducted experiments allowed the conclusion, that those classical terms weren't able to apply to all given circumstances. Due to this uncertainty that occurs by the usage of a common language, there have been efforts to define a precise language that allows logical well-defined logical conclusions that apply to the mathematical pattern of quantum theory. One of those attempts was made by physicist and philosopher Carl Friedrich von Weizsäcker, which concluded in the assumption that the mathematical pattern of quantum theory can be interpreted as an extension or modification of classical logic. One basic assumption of classical logic, that either a predication or its negation have to be true for the predication to make sense and that the rule of "tertium non datur" has to apply to it. In quantum logic, the prevalence of "tertium non datur" is reduced, again, "Schrödinger's cat" with its superposition would be a good counterexample to this rule of classical logic. In order for language to apply to those seemingly uncommon circumstances, von Weizsäcker proposes different levels of language. The first level deals with objects, the second level is related to predications about those objects and the third level refers to predications about predications of objects and so on. This would allow the possibility to establish various methods of logical conclusions in the different levels of language, but sooner or later, the need for the common language and the classical logic will reoccur. Weizsäcker refers to the relationship of classical and quantum logic as an "a priori" relationship, which means that classical logic is similarly "a priori" to quantum logic as classical physics is to quantum physics. Classical logic would be included in quantum logic as a kind of borderline case, whereas the latter would represent the more general pattern.

In order to talk about circumstances that are connected with an interference of probabilities, as in superposition or measurement of emitted single photons, Weizsäcker introduced logical values to predications about the given circumstances. For every predication that could be considered true, the logical value accounts one and for every false predication, the value is zero. It is important to note that values between those zero and one are possible and because of this, the meaning of the term “predication” is extended to a form of statement of mere tendencies where intersections of coexistent possibilities could be expressed in logical values in contrast to complementary statements that only accept values that are either zero or one.

> “In den Experimenten über Atomvorgänge haben wir mit Dingen und Tatsachen zu tun, mit Erscheinungen, die ebenso wichtig sind die irgendwelche Erscheinungen im richtigen Leben. Aber die Atome oder die Elementarteilchen sind nicht ebenso wirklich. Sie bilden eher eine Welt von Tendenzen oder Möglichkeiten als eine von Dingen und Tatsachen.“[6]

It still seems noteworthy that exactly this „interference of probabilities“ makes quantum cryptography so secure towards cryptanalysts. By being able to measure only one condition of the incoming photon, be it the vertical-horizontal or the diagonal polarisation, and the additional quantum laws , like impossibility of duplication or perturbation of the system through measurement, a set of interfering probabilities is established that only allows the designated receiver to decode those probabilities into “useful”, or static, information if he gets additional data from the sender. The mathematical obstacle in cryptanalysis of reversing a logarithmic process without knowing the initial values is extended by an ensemble of interfering probabilities of quantum physics where the attempt of reversing a quantum process without having access to data about the initial condition would result in a recognizable discrepancy among the official information source and the receiver.

6. The relationship of dichotomy, transgression and synaesthesia in quantum cryptography

[6] Werner Heisenberg, Physik und Philosophie, p. 156

By having outlined the history and development of the processes that finally led to quantum cryptography, this last chapter tries to focus on quantum cryptography as an intermedial concept. According to McLuhan's principle that the content of a medium is always another medium or a network of media, this also applies to quantum cryptography. Furthermore, it should be shown how the initial scientific concept of dichotomy is transgressed beyond its boundaries to a concept of synaesthesia that allows the recipient to produce a meaning by recognizing the transferred signal.

Heisenberg in his comment on Descartes pointed out that the division of inner and outer processes, that is, the "res extensa" and the "res cogitans", paved the way for the natural sciences we know today. This concept can be considered as dichotomizing or binary since it followed the rules of classical logic with its "tertium non datur". It helped to extend the amount of knowledge about the world or, more precisely, about establishing methods to perceive and predict phenomena within the world. Along with this extension of knowledge also came empiricism in order to verify the methods of scientific perception and prediction. If experiments cannot be conducted under the same circumstances over and over again, the result of thesis originating from that experiment would not be called scientific. Empiricism was the underlying principle of modelling and redesigning scientific methods until they applied to the current level of awareness. But since quantum theory and relativity theory were introduced, this understanding of empiricism changed. The binary principle itself was reformulated to a principle of tendencies and probabilities like the uncertainty principle. This secularisation of empiricism for the benefit of new insights into the very basic mechanisms of nature led to an interdisciplinary reflection of those changes in the literary field as well as it spawned an opposition towards this particular intertextual or interdiscoursive approach that still believes in the authority of empiricism in natural science as well as in our perception of nature by arguing that those theories concerning quantum mechanics are only aborning and literary critics cannot make any statements about their ontological conditions. Alan Sokal may serve as an example of the latter group. Nevertheless and apart from its ontological condition, quantum mechanics expanded again the applicability of its knowledge to quantum cryptography due to the non-locality principle and made it possible to use singular entangled photon pairs as an information channel. Again, it cannot be mentioned enough that exactly the uncertainty of the ontological condition of those photon pairs is the efficient underlying principle of the performance of this cryptography system. Here, cryptology is not used as a mathematic algorithm to encode the ontological "substance" of a message, but the "substance" by itself is removed from all ontological attempts and mathematics and stochastic theory in particular are the only connection to decode the complete ontological value of the message again.

This process may be regarded as an indication that quantum mechanics finally gained synaesthetic aspects through quantum cryptography. In the common understanding of synaesthesia, meaning is produced by a combination of sensations. Scripture, for example, combines single letters that ate associated with single sounds to written words which again can be associated with spoken words which then denote a specific meaning in a specific language. In quantum cryptography, classical media like speech, text, and pictures are transformed into binary digits of discrete conditions of universal machines, that is, computers, which could then be encoded with a key that refers to specific quantum conditions of single entangled photon pairs. It still remains debatable if meaning which is encoded in quantum conditions can still be regarded as synaesthetic since we don't have any organs to perceive them but it remains important that the meaning that is encoded by quantum conditions stays complete in the decoding process and by that, synaesthetic aspects make their entrance to quantum theory through its usage as a medium.

> "One has the vague feeling that information and meaning may prove to be something like a pair of canonically conjugate variables in quantum theory they being subject to some joint restriction that condemns a person to the sacrifice of the one as he insists on having much of the other."[7]

It remains to be seen if "quantum information technology" will have a similar impact on humanity as the already established mass-media television and radio, which also work with wave patterns as an information channel. By imagining the first people being exposed to something like a radio and wondering by which invisible channel the signal is being sent, one might also imagine the first people who use a quantum computer and wonder by which indeterminable processes this machine calculates its operations.

[7] Warren Weaver, Some Recent Contributions to the Mathematical Theory of Communication, p. 28, in: Claude E. Shannon, Warren Weaver, The Mathematical Theory of Communication

Appendix

Figure 1: Schematic diagram of a general communication system

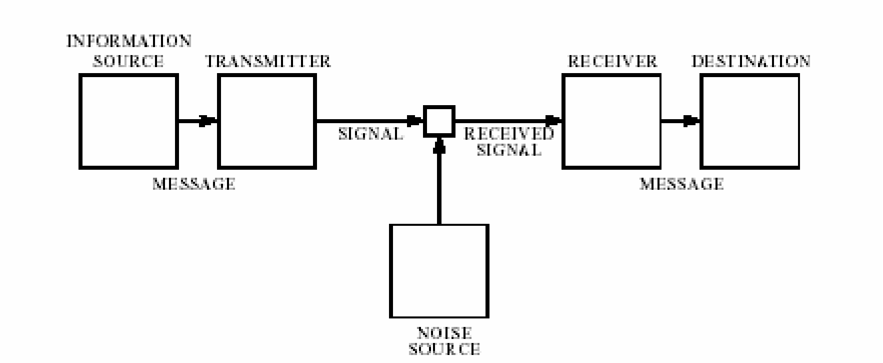
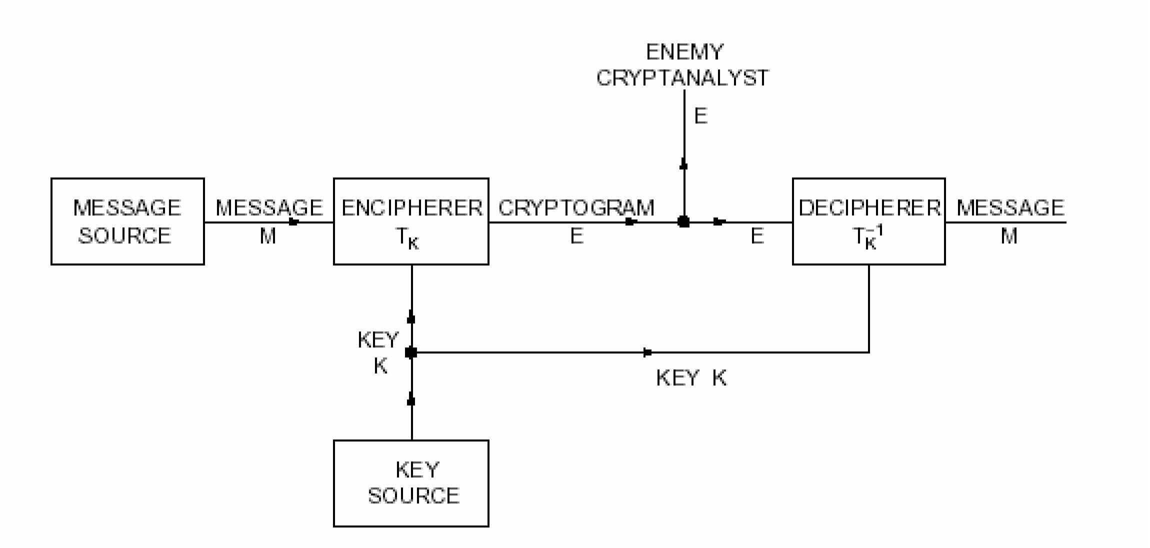


Figure 2: Schematic of a general secrecy system



Bibliography

Primary literature

Heisenberg, Werner. *Physik und Philosophie.*1959. Frankfurt: Ullstein, 1977

Gisin, Nicolas; Ribordy, Grègoire; Tittel, Wolfgang; Zbinden, Hugo. “Quantum cryptography.” 2002. *Reviews of Modern Physics.* Volume 74, January 2002. 145-190

Shannon, Claude E.; Weaver, Warren. *The mathematical theory of communication*. 1949. Urbana and Chicago: University of Illinois press, 1998

Shannon, Claude E. “Communication Theory of secrecy Systems.” 1949. *Bell System Technical Journal.* Volume 28-4. 656-715 <http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf>

Singh, Simon. *The Code Book. The secret history of codes and code – breaking.* 1999. London: Fourth Estate, 2000

Secondary literature

Jennnewein, Thomas; Weihs, Gregor; Zeilinger, Anton. „Schrödingers Geheimnisse“ 2001. *c’t Magazin für Computertechnik.* Ausgabe 6/2001. 260-269. Hannover: Heinz Heise