European Information Technologies Certification Institute
Avenue des Saisons 100-102, 1050 Brussels, Belgium, EU
Web: https://www.eitci.org, E-mail: info@eitci.org
Phone: +32 2 588 73 51, Fax: +32 2 588 73 52

Reference Standard

RS-EITCI-QSG-OQP-IMPLEMENTATION-STD-VER-1.0

Reference Standard for the One Qubit Pad (OQP) implementation (technical specification of processes, devices and operative parameters for qubits encryption)

EITCI INSTITUTE QUANTUM STANDARDS GROUP

EITCI-OQP-QSG

Brussels, 25th August 2021
Version: 1.0

Table of contents

The One-Qubit Pad (OQP) - fundamental entanglement based encryption scheme for quantum information

Introduction

((1)) Over one hundred years ago, in 1917 Gilbert Vernam invented and then patented his additive polyalphabetic stream cipher, known as the Vernam Cipher [1]. Vernam invented and described in his patent a teleprinter encryptor in which a previously prepared key, kept on a paper tape, is combined character by character with the message to encrypt it. In order to decrypt the encrypted information, only the same key must be used, again combined character by character, producing the decrypted message. The combining function that was described in the Vernam's Patent is the XOR operation (exclusive alternative of the Boolean algebra or binary sum modulo 2, which is essentially the classical logic control not operation, i.e. CNOT gate, only discarding the controlling bit and leaving the target bit to accommodate irreversible Boolean algebra requirements), applied to bits (impulses in the original patent) used to encode the characters in the Baudot code [2] (an early form of binary encoding). While Vernam did not use explicitly the term "XOR" in his technical description of the patent, he implemented that operation in relay logic. The following example is dervied from the description of the Vernam's patent, with XOR procedure replacing original electrically combining function implementing the logic of the teleprinted device operation: the plaintext character is "A", encoded as "$+ + - - -$" in Baudot code, and the key character is "B", encoded as "$+ - - + +$"; when one applies XOR (logic operation returning true only if two inputs are true and false) for plaintext "$+ + - - -$" and key "$+ - - + +$", one obtains the code "$- + - + +$" which reads "G" character in Baudot; there is no way to guess that character "G" actually decrypts to character "A", unless one knows the key used was character "B"; again applying XOR on "G" ("$- + - + +$") with "B" ("$+ - - + +$") produces the Baudot code "$+ + - - -$" which reads the decrypted character "A". In a modern generalized representation Vernam cipher operates on bits of classical information: either 0 or 1. Any classical information can be encoded binarily as sequences of 0's and 1's, and that is of course the information architecture that great majority of contemporary electronic devices operate within (including computers and networks). Let's consider the following example: A message reading "Hello" is encoded (UTF8) as M=0100100001100101011011000110110001101111 (with 8 bits per character it is 40 bits long). If one uses a random (meaningless) key, e.g. K=1101010110110001011101011101 001000110100, the XOR encrypted message (M XOR K) will read E=1001110111010100000110011011111001011011, which also doesn't have any meaning. If the key is truly random and private, then without it there is no way to compute what was the original message. Only if one has the key K then the encrypted message E can be again XOR'ed bitwise with the key K to return original message M.

((2)) Few years after the patent was awarded to Vernam, Joseph Mauborgne (a captain in the US Army Signal Corps) modified Vernam's invention changing the key to random. These two ideas combined, implement what is now famously known as the One-Time Pad (OTP) classical cipher. Only about 20 years later Claude Shannon, also at Bell Labs, proved formally within his now foundational Informationn Theory that the One-Time Pad, properly implemented with random key is unbreakable (these proofs were done in 1941 during World War II and were published after declassification in 1949 [3]). In the same paper Shannon also proved that any unbreakable (i.e. theoretically secure) system must have essentially the same characteristics as the One-Time Pad: the key must be as long as the message and truly random (which also implies for the key to be never reused in whole or part and kept secret). The US National Security Agency has called Gilbert Vernam's patent that lead to the One-Time Pad concept "perhaps one of the most important in the history of cryptography." [4]. More recently, in 2011 it came to light that the One-Qubit Pad has been actually first invented 35 years prior to the patent issued to Gilbert Vernam by Frank Miller in 1882.[**?**].

!!!!!XXX refbellovin-otp-history: Bellovin, Steven. "Frank Miller: Inventor of the One-Time Pad" (PDF). Columbia University. Retrieved 20 October 2017.

((3)) Since these discoveries defining information-theoretic secure classical cryptography (referred to as private-key or symmetric cryptograohy) not much have changed in terms of fundamental cryptographic ideas. The main problem of the OQP is the key distribution (to ensure the communicated parties have the symmetric key). In the 1970s there has been a shift towards a novel paradigm called asymmetric cryptography (or public-key cryptography),

that originated in the proposal of Diffie-Helman protocol [5] to solve the problem of the secure key distribution between the One-Time Pad parties. But the public-key cryptography (generalized from Diffie-Helmann's approach from key distribution to actual encryption and authentication within digital signatures), practical as it is, does not offer the level of unconditional or absolute (information-theoretic) security – it is fully computationally conditioned. Wheras classical models of computation (based on classical physics laws) seemingly do not pose threat to some of mathematical difficult problems (e.g. factorization of large numbers into primes as used e.g. in the RSA scheme [6] or finding discrete logarithms in elliptic curve cryptography used e.g. in ECDSA scheme included e.g. into Bitcoin definition [7, 8]), the quantum computation model actually very much does so and both mentioned cryptosystems would be broken if practical (universal and scallable) quantum computer is constructed. In 1984 Bennett and Brassard proposed the Quantum Key Distribution[9] to solve the central problem of the OTP (based on the ideas of Wiesner[**?**]), which is considered birth of the quantum cryptography, resistant to the threath of future quantum computers. Most of the advancements of quantum cryptography focus on encryption of classical information and there is little analysis of possible encryption of quantum information itself (securing it not from a measurement, which cannot access quantum information due to the fundamental limitations of the classical information and the projective nature of the measurement in quantum mechanics, but rather from unauthorized quantum processing).
!!!!!XXX refbb84: C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984. !!!!!XXX refwiesner: Wiesner, Stephen (1983-01-01). "Conjugate Coding". SIGACT News. 15 (1): 78–88. doi:10.1145/1008908.1008920. ISSN 0163-5700.

((4)) The present paper proposes and discusses a fundamental primitive to quantum cryptography considered in terms of encrypting quantum information, which is corresponding to the general nature of OTP for encrypting classical information. From the properties of quantum information it turns out, that the most general scheme of encryption of quantum information requires just a single qubit quantum key to encrypt in an quantum-information-theoretic way an arbitrarily long quantum message (understood as n-qubits register) with use of entanglement by the quantum CNOT gate, hence this scheme is referred to as the One-Qubit Pad.

The One-Qubit Pad

((5)) The One-Qubit Pad scheme enables quantum-information-theoretic secure encryption of the quantum information (quantum message) of n qubits register (M) in unknown arbitrary states with just a single key qubit (K) also in unkown arbitary quantum superposition upon provision of a multi-qubit entanglement between the single key qubit and the n qubits of the quantum message. The proposed scheme's central concept is the use of the quantum CNOT gate iteratively applying it on the single qubit key (control qubit) and subseqnent n qubits of the quantum information (message) in order to encrypt it.

((6)) The iterative use of CNOT on the key qubit and qubits of the message will entangle all n+1 qubits (introducing a jointly entangled state), which means that both K' and M' together entangled were individually evolving in a non-unitary transformations bringing those states to their mixed quantum configurations. The OQP protocol is presented in the Fig. 2 and Fig. 3 The original quantum message M cannot be obtained from the encrypted message in M' without the single qubit K'. To decrypt the quantum message M' to its original state of M (by disentanglement) one needs to have the single qubit-key K' and either reverse the protocol (applying CNOT operations in the reversed order) or simply measure the entangled qubit-key K' and then depending on the outcome having either straightforwardly restored the quantum message M from M' or its quantum negation, i.e. needing to quantumly negate all qubits of the message by applying the σ_x pauli matrix controlled by single classical bit being the outcome of the measurement of K' what is presented in the Fig. 4 (this can be understood as a CNOT with classical control bit realized upon measurement of the key qubit K' projection state and the quantum target qubits of all n qubits in the quantum message).

((7)) One of the most important difference of the OQP versus classical OTP and schemes based on quantum information encryption with classical keys (so called Quantum Private Channels[**?**]) is that in the latter cases the key can be copied. In OQP the single-qubit quantum key (K) cannot be copied due to the no-cloning theorem applying in quantum mechanics [10]. In comparison to some discussion of the quantum information encryption with quantum keys, as e.g. in [11], the proposed OQP protocol has an edge in its extreme efficiency, reducing the key to just a single qubit, hence the scheme is referred to the One-Qubit Pad. The main application of the scheme is to lock (secure) the quantum information M with the key K of just a single qubit in order to disallow any potential access to the original n qubits quantum information M by an adversary (e.g. the quantum information M might be some valuable output of quantum computation and it might be considered important for it to be locked from an adversary thus not able to use it as an input in his quantum computation which is gaining importance in the advent of quantum computers and quantum networks processing and communicating quantum rather then classical information implementing distributed quantum computation applications of the future, such as the quantum AI, etc.). A less general application of the protocol towards communication is best described in combination with the Quantum Teleportation protocol [12], which without the OQP scheme requires pre-sharing of n pairs of Bell states between Alice and Bob to securely communicate n qubits of quantum message, whereas in contrast with the OQP it requires sharing of just a single Bell state to securely teleport only the single quantum key qubit K' with sending the encrypted M' quantum message through a standard, insecure local quantum channel.

!!!!!XXX refquant-priv-channel: A. Ambainis; M. Mosca; A. Tapp; R. De Wolf, Priavate quantum channels, Proceedings 41st Annual Symposium on Foundations of Computer Science, DOI: https://doi.org/10.1109/SFCS.2000.892142, 2000

The problem definition and the solution

((8)) The problem for which the proposed scheme can be applied as the most fundamental primitive concerns unconditionally (i.e. information-theoretic) secure encryption of quantum information. Quantum information is fundamentally different from classical information and in general it could be identified with the states of quantum systems (physical systems governed by quantum mechanics laws), whereas classical information could be identified with states of classical systems (i.e. physical systems of properties governed by classical physics laws). While the classical information (encoding bits) is the subject of classical computation and communication, the quantum information (encoding qubits, the quantum analog of classical bits incorporating superposition) is basic notion of quantum computation and communication. The two areas differ significantly. The OQP scheme focuses on the domain of purely quantum information and communication and solves the problem of finding the most efficient protocol to unconditionally securely encrypt quantum information with a quantum key (in contrast to the classical case sufficiently consisting of only a single qubit to still provide information-theoretic, i.e. unconditional security). The proposed OQP scheme is the most primitive and general quantum version of the classical concept of the One-Time Pad (OTP), in contrast to a straightforward translation of OTP to a quantum case, using the CNOT with n-qubit key (with n corresponding to the number of qubits in the quantum message register to be encrypted). It turns out that due to properties of quantum information (and infinity information capacity of a single qubit) n-qubits long quantum key is not necessary and just a single qubit is sufficient as the key, thus reducing the quantum OTP, to OQP, the One-Qubit Pad, offer unconditional security of n qubits message due to introduction of a multi-qubit quantum entanglement.

((9)) The OQP protocol and defines the following basic notions:

1. Alice and Bob are two parties of the scheme. In principle the quantum information can also be locked only by Alice to be unlocked later, thus in the meantime remaining secure against adversary (Eve).
2. The quantum information or quantum message M (this is a quantum register of n qubits, each storing certain unknown quantum state either pure or mixed, if these qubits' states are known e.g. upon measurement then M stores classical information - in general case M can be of some meaning to Alice, e.g. constitute an output of a certain complex quantum computation which could be highly valuable).
3. The quantum key K consisting of a single qubit in unknown state (this single qubit is kept well protected - in a straightforward generalization of the classical OTP to Quantum One-Time Pad or QOTP, the key K can be understood as a register of n qubits also in unknown quantum states, either pure or mixed: if K single-qubit key in OQP or n-qubits key in QOTP is/are measured then K reduces to the classical information key; the length of K register equal to M is due to straightforward extension of classical One-Time Pad to quantum case herewithin referred to as QOTP where entanglement is only introduced in pairs of corresponding subsequent qubits of K and M; the main aspect of the One-Qubit Pad protocol is in provision that the quantum key can

be reduced to a single qubit due to proper utilization of the multi-qubit entanglement between the single-qubit key and whole encrypted n-qubits message of an arbitrary length).

4. Eve is the third party understood to be an adversary of Alice and Bob (in general she is interested in obtaining the decrypted quantum message M, and in both storage and communication scenarios of the protocol she wants to access the original quantum information from its encrypted form without the quantum key, which is kept secure from her, not in terms of measurement, but in terms of unauthorized processing of the original quantum information).

Description of the OQP scheme

((10)) Before we proceed to defining the OQP scheme and discussing its properties, lets first consider the trivial extension of the classical One-Time Pad (OTP) to the quantum case, thus introducing the concept (not very well defined in the current literature) that can be referred to as the Quantum One-Time Pad QOTP protocol. In most general terms the QOTP will work in the way described below with the following assumption made on the quantum key K register: that it will contain the same number of qubits as the quantum message M it aims to encrypt. Upon the QOTP protocol each qubit of the quantum message register M is processed with corresponding qubit of quantum key register K upon a controlled NOT two-qubits quantum gate (CNOT) (i.e. analogically to the classical OTP, in which corresponding bits of the key and message undergo a classical CNOT gate, i.e. a XOR operation on the target bit of the message, resulting with encrypted sequence). In analogy to the OTP scheme the QOTP key (K) qubits are control qubits, while the message (M) qubits are target qubits. In classical terms CNOT operation is equivalent to XOR (just leaves the first/controlling input bit as the first/controlling output bit without change, and applies logic negation on the second/target input bit as the output bit if and only if the first/controlling input bit is equal to 1 - this is also equivalent to output bit being set as the bit sum modulo 2 of two input bits). In contrast to classical case the quantum generalization of CNOT gate introduces quantum entanglement. For the non-classical both pure and mixed quantum states of M and K the CNOT gate will entangle two corresponding qubits of M and K. Hence if M (and thus K) registers consist of n qubits, then after n-iterations, all the qubits in M will be entangled with corresponding qubits in K. Each corresponding pair of qubits from the original quantum message (M) and the quantum key (K) registers are now entangled (but only in 2-qubits entanglement, i.e. in pairs). Both registers in new pairwise entangled states we will call by M' and K'. This means that each corresponding qubit of M' with the paired (entangled) qubit of K' are individually in their mixed (non-normalized) states (it should be stressed that the entanglement involved here is only pairwise - between the individual key qubit and its corresponding quantum message qubit, together implementing entangled n pairs on those n corresponding positions of both registers). The operation of the QOTP protocol is presented on the Fig. 1.

((11)) Now if the entangled key register K' is kept secret, then the register M' contains fully quantumly (and non-locally due to entanglement) encrypted quantum message. If one has no quantum key K' it is impossible to obtain original quantum message M from M' (even if one had infinite computational resources, as this is guaranteed by quantum mechanics laws). Also the original K and M do not exist anymore (as quantum information they couldn't have been copied) which is also guaranteed by fundamental quantum mechanics laws (the no-cloning theorem[10]), which adds up to the fundamental and absolute security of the protocol. It should be stressed that the QOTP quantum encryption scheme encrypts quantum information non-locally (it non-locally stores both the original M and K quantum information between the M' and K' qubits registers that are entangled - none of the two register individually stores the original quantum information anymore). K' without M' is informationless in regard to the original quantum information it contained and vice-vera. The quantum information has been non-locally hidden in both registers in their pairwise entanglement.

((12)) One may ask how exactly the above described quantum generalization of classical OTP - referred herewithin as the QOTP is related to the original One-Time Pad (OTP), proven information-theoretic, i.e. unconditionally secure by Shannon. In fact the more general QOTP can be reduced to the classical OTP in case if both qubits of K and M reside only in a given Hilbert basis states (e.g. both are states of the computational basis $\{|0\rangle, |1\rangle\}$)). This reduction will lose however the crucial in the quantum information case non-locality aspect. In this situation (of basis states in both K and M, actually representing classical information) the quantum CNOT gate will act as purely classical CNOT gate and thus as classical Boolean logic XOR operation exactly like in the classical OTP. Yet if the key qubits K are not in basis states (i.e. they are not of classical information), but rather their superpositions (quantum information), then the CNOT will inevitable introduce quantum entanglement between corresponding qubits of M and K, generalizing the scheme to QOTP (even if the register M consists of qubits in basis states, i.e. actually stores classical information encoded on qubits - meaning that the QOTP can also encrypt the classical information with entanglement).

((13)) What however is fully detached from the classical domain is the concept of the One-Qubit Pad (OQP).

((14)) The OQP scheme, presented in its principle in the Fig. 2, will allow the use for perfectly locking (quantum encrypting within non-local entanglement) of quantum information (quantum message) of n-qubits register (M) with just a single qubit (one qubit) key K. In OQP we will have same definitions and same processing of message M and key K as in QOTP instead of one change: now the quantum key K is containing only one qubit, and the protocol will differ in processing sequentially each qubit of the register M with this single qubit of K upon the CNOT quantum gate (again the single key qubit K will always be a looped control qubit in the CNOT gate, while subsequent qubits of the quantum message M will be target qubits of the CNOT). Upon the first iteration the qubit K will thus entangle with first qubit of M. In the second iteration when qubit K is in CNOT with the second qubit of M, the resulting state will be entanglement between the qubit K and the first two qubits of M). In n-th iteration of the qubit K in CNOT with the last qubit of M the result will be a fully entangled n+1 state (a joint multi-entanglement of all qubits - a qubit contained in a single-qubit key register K and n-qubits in the register of the quantum message M).

((15)) After the OQP entangling encryption again the message register M is in new state M' (entangled altogether with the new state of key K'). If the key K' is kept by Alice, then there is no way to extract original quantum information from M' guaranteed by quantum mechanics laws. Additionally same laws guarantee that there cannot exist a copy of original quantum message (M) and neither of the key (K) (which is due to no-cloning theorem). Therefore the OQP similarly as discussed above QOTP is absolutely secure even in contrast to classical OTP which is absolutely secure only under the assumption that the used classical key had not been copied (or conversely the classical message being encrypted had not been copied before encryption) - because in classical physics there are no laws that would disallow such situation. In principle even after encryption in classical OTP the original message can be found and copied without access to the key (hence even if the original message is deleted this deletion is doomed to be imperfect and sufficiently advanced technology could be used to determine the classical message M, e.g. by detailed analysis of the radiation resulting to classical storing and processing on macroscopic physical carriers of the message M). Such hypothetical situation is however fully ruled out on the fundamental level by the laws of quantum mechanics in the QOTP and OQP protocols. However the result of OQP is of a fundamental significance. It is due to the information capacity of a single qubit K' that can in fact encode (however here non-locally in quantum entanglement with M') the information from n-qubits sequence M (along with original information on single qubit key K), even if n is infinite (but discrete with a cardinal number $\aleph_0$). It is not surprising as the informational capacity of each single qubit is continously infinite, i.e. infinite in terms of continous cardinal number c.

((16)) In order to decrypt (disentangle) the quantum message M from M' using key K' one needs to revert the process: using the same quantum CNOT gate, one needs to process the qubit K' with each subsequent qubit from register M' but in the reversed order: in the first step the key qubit K' will be in CNOT gate with the last qubit from M' (this will disentangle the last qubit in M' and return it to original state of the last qubit in M register), then again the key qubit will need to be in CNOT gate with the one before last of M' qubits (the result will be two disentangled last qubits of M' now in their original states as they had in M register). This procedure iterated n times will eventually lead in the last step to finally the key qubit being under CNOT operation with the first qubit of M', and after this the disentanglement of M' with K' will be complete, the quantum message register will now be fully in the original state as it was in the M register, and also the key qubit will return to its original state as in K). The applications scenarios of the OQP scheme are surely more communication-friendly than of QOTP, as will be also discussed.

((17)) Description of a generic quantum circuit device implementing the proposed OQP protocol (One-Qubit Pad) is very simple and involves a single CNOT gate with a looped control qubit (a single-qubit key) or alternatively n

CNOT gates with control input fed sequentially by the single-qubit key.

((18)) Let us first assume that we have a single qubit key K in the state $\left|K\right\rangle = a\left|0\right\rangle + b\left|1\right\rangle$ (this is unknown quantum information of only one qubit, that we will use to information-theoretically secure quantum information of any arbitrary number of qubits). For now, as a simplification, we can assume that the key qubit K is in a pure state (i.e. $\left|a\right|^2 + \left|b\right|^2 = 1$). One can ascertain upon a more general analysis that it doesn't matter whether the key or the message qubits are in pure or mixed states before the encryption.

((19)) Let's then assume we have some important quantum information (quantum message) contained within n-qubits register M (again for simplicity these message qubits are in pure states, and can be easily generalized to mixed states if states of M share entanglement either with themselves or also externally with some other qubits - this doesn't change anything in the OQP scheme).

((20)) To illustrate operation of the OQP scheme we will limit the number of qubits in M register to 3, thus $\left|M\right\rangle = \left(c\left|0\right\rangle + d\left|1\right\rangle\right)\left(e\left|0\right\rangle + f\left|1\right\rangle\right)\left(g\left|0\right\rangle + h\left|1\right\rangle\right) = \left|\psi_1\right\rangle$. The density matrix of M is

$$\begin{aligned}&\rho_M = \rho_{\psi_1} = \left|\psi_1\right\rangle\left\langle\psi_1\right| \\ &= \left(c\left|0\right\rangle + d\left|1\right\rangle\right)\left(e\left|0\right\rangle + f\left|1\right\rangle\right)\left(g\left|0\right\rangle + h\left|1\right\rangle\right)\left(c^*\left\langle 0\right| + d^*\left\langle 1\right|\right)\left(e^*\left\langle 0\right| + f^*\left\langle 1\right|\right)\left(g^*\left\langle 0\right| + h^*\left\langle 1\right|\right).\end{aligned} \tag{1}$$

((21)) Of course the implementation of the CNOT gare (similarily as of qubits) doesn't play any role for the OQP scheme. The CNOT quantum circuits logical operation represents a 2-qubits gate of controlled quantum negation (the X or σ_x Pauli gate, interchanging the qubit superposition coefficients). It is a generalization of the classical CNOT gate (a 2-bits gate generalizing the Boolean algebra gate called the exclusive alternative XOR to a reversible case). The quantum CNOT gate acting on classical information (or the basis states of the qubit definition) is essentially reducing to a classical CNOT gate, implementing on the target bit a sum with control bit modulo 2 (the rest of division by 2) which is also fully equivalent to the exclusive alternative XOR logical operation (while in CNOT control bit left unchanged is outputted for reversibility). For quantum information (qubits in superpositions of the qubit definition basis $\left|0\right\rangle$ and $\left|1\right\rangle$) the quantum CNOT introduces entanglement (it is representing a unitary evolution on both qubits together which takes however their state out of a separable configuration in regard to the tensor product form to a non-separable configuration which is referred to as entangled, and thus it implements a non-unitary evolution on each of the individual qubits taking their individual states from pure to mixed, or if they were already mixed on their own, to states entangled with some other qubits, it additionally entangles them together as well).

((22)) The cyclic operation of the CNOT gate controlled by the key qubit K' and targeting subsequent qubits of quantum message register M will have the following effect:

((23)) After the first iteration we have:

$$\left(a\left|0\right\rangle + b\left|1\right\rangle\right)\mathrm{CNOT}\left(c\left|0\right\rangle + d\left|1\right\rangle\right) = \left(ac\left|00\right\rangle + ad\left|01\right\rangle + bc\left|11\right\rangle + bd\left|10\right\rangle\right). \tag{2}$$

((24)) This is now an inseparable 4-terms entangled state of two qubits (key qubit K and first qubit of M register).

((25)) After the second iteration:

$$\begin{aligned}&\left(ac\left|00\right\rangle + ad\left|01\right\rangle + bc\left|11\right\rangle + bd\left|10\right\rangle\right)\mathrm{CNOT}\left(e\left|0\right\rangle + f\left|1\right\rangle\right) \\ &= \left(ace\left|000\right\rangle + acf\left|001\right\rangle + ade\left|010\right\rangle + adf\left|011\right\rangle + bce\left|111\right\rangle + bcf\left|110\right\rangle + bde\left|101\right\rangle + bdf\left|100\right\rangle\right)\end{aligned} \tag{3}$$

((26)) The second iteration has produced an unseperable 8-terms entangled state of 3 qubits (key qubit K and two first qubits of M). One should note only the first qubit - the key qubit K - is conditioning the CNOT gate applied in this iteration to the third qubit, i.e. the second of the quantum message register M.

((27)) Then, the third iteration produces the following state:

$$\begin{aligned}&\left(ace\left|000\right\rangle + acf\left|001\right\rangle + ade\left|010\right\rangle + adf\left|011\right\rangle + bce\left|111\right\rangle + bcf\left|110\right\rangle + bde\left|101\right\rangle + bdf\left|100\right\rangle\right)\mathrm{CNOT}\left(g\left|0\right\rangle + h\left|1\right\rangle\right) \\ &= \left(aceg\left|0000\right\rangle + aceh\left|0001\right\rangle + acfg\left|0010\right\rangle + acfh\left|0011\right\rangle + adeg\left|0100\right\rangle + adeh\left|0101\right\rangle + adfg\left|0110\right\rangle + adfh\left|0111\right\rangle\right. \\ &\left.+bceg\left|1111\right\rangle + bceh\left|1110\right\rangle + bcfg\left|1101\right\rangle + bcfh\left|1100\right\rangle + bdeg\left|1011\right\rangle + bdeh\left|1010\right\rangle + bdfg\left|1001\right\rangle + bdfh\left|1000\right\rangle\right)\end{aligned} \tag{4}$$

((28)) This is now unseperable 16-terms entangled state of 4 qubits (key qubit K and three qubits of M register). Again only the first qubit - the key qubit K - is conditioning the CNOT gate applied now to the fourth qubit, i.e. the third in the quantum message register M. If the quantum message M has more than 3 qubits then subsequent iterations (up to n-th iteration) would be analogous to the above.

((29)) After the above described iterations the quantum message M has been non-locally encrypted (locked) within a multiple entanglement with just the single key qubit K. Now both K and M have transformed to K' and M' in a jointly entangled pure state, that we could call Z' (separately both K' and M' are in their mixed states). If the key qubit K' is to be hidden and kept secret and secure, one may consider what is the mixed state of the M'. Let's consider simplified example of 3 qubits quantum message M, now in mixed state M' (entangled with qubit K'). A naive writing down of the vector state of M' would have the following form (one must note however that this is not a pure state anymore, it is not normalized and thus the vector states formalism falls short to be used in representing of the mixed states and one must resort to the density matrix formalism):

((30)) A naively (and not correctly) written vector state form of the unnormalized mixed state M' is following:

$$\begin{aligned}&(ceg\,|000\rangle + ceh\,|001\rangle + cfg\,|010\rangle + cfh\,|011\rangle + deg\,|100\rangle + deh\,|101\rangle + dfg\,|110\rangle + dfh\,|111\rangle\\&+ceg\,|111\rangle + ceh\,|110\rangle + cfg\,|101\rangle + cfh\,|100\rangle + deg\,|011\rangle + deh\,|010\rangle + dfg\,|001\rangle + dfh\,|000\rangle)\,.\end{aligned} \tag{5}$$

((31)) Now correctly the same mixed state M' expressed in the form of the reduced density matrix after tracing out the state of the key qubit K' will constitute a mixture with probabilities $|a|^2$ and $|b|^2$ (determined by the original state of the secret key qubit K) of projection operators (which are also pure density matrices) upon the following two pure states with the probabilities:

- $|a|^2$: $ceg\,|000\rangle + ceh\,|001\rangle + cfg\,|010\rangle + cfh\,|011\rangle + deg\,|100\rangle + deh\,|101\rangle + dfg\,|110\rangle + dfh\,|111\rangle = |\psi_1\rangle$
- $|b|^2$: $ceg\,|111\rangle + ceh\,|110\rangle + cfg\,|101\rangle + cfh\,|100\rangle + deg\,|011\rangle + deh\,|010\rangle + dfg\,|001\rangle + dfh\,|000\rangle = |\psi_2\rangle$

((32)) This is equivalent with writing down the reduced density matrix of the mixed state of M' as:

$$\begin{aligned}\rho_{M'} &= \mathrm{Tr}_{K'}\left(\rho_{Z'}\right) = \langle 0|\,\rho_{Z'}\,|0\rangle + \langle 1|\,\rho_{Z'}\,|1\rangle = |a|^2\,|\psi_1\rangle\,\langle\psi_1| + |b|^2\,|\psi_2\rangle\,\langle\psi_2|\\&= |a|^2\,P_{\psi_1} + |b|^2\,P_{\psi_2} = |a|^2\,\rho_{\psi_1} + |b|^2\,\rho_{\psi_2} = |a|^2\,\rho_M + |b|^2\,\sigma_x^{\otimes^n}\rho_M\sigma_x^{\otimes^n}\end{aligned} \tag{6}$$

((33)) Note that trace was over the first qubit (the single-qubit key). Of course the above two pure states are not any seperate states in the current situation (i.e. the qubit key K' has not been measured and is kept hidden). The state of M' is now correctly described by the operator of reduced density matrix that has a spectral decomposition on $|a|^2\,P_{\psi_1} + |b|^2\,P_{\psi_2}$ (where P_{ψ_1} and P_{ψ_2} are projection operators on the pure states $|\psi_1\rangle$=$|M\rangle$ and $|\psi_2\rangle$=$\sigma_x^{\otimes^n}\,|M\rangle$).

((34)) Performing measurement on the 3-qubits of M' or performing any other unitary operation (change of basis) on them without knowledge of the key qubit K will not help in any way to restore the original M quantum information. For instance performing measurement of 3 qubits in M' in the computational basis $\{|0\rangle\,, |1\rangle\}$ will first realize the probability of choice of the pure state of 3 qubits in M' (either $|a|^2$ for $|\psi_1\rangle$ or $|b|^2$ for $|\psi_2\rangle$) then multiply it with one of the probabilities made up of multiplications of square of moduluses of corresponding to the projected state 3 of 6 linear combination complex coefficients: c d e f g h. E.g. if one will project the 3 qubits in M' to state $|000\rangle$ it could have happened only with probability equal to $|a|^2\,|c|^2\,|e|^2\,|g|^2$ or $|b|^2\,|d|^2\,|f|^2\,|h|^2$. Naturally if these coefficients are unknown (this is after all the uknown content of the original quantum information or quantum message M) to someone making the measurement it is impossible to infer anything about them upon the measurement outcome. In a hypothetical assumption of having at disposal a large set of copies of the state encrypted by entanglement quantum message register M', it would be possible to deduce some information about these coefficients after large number of measurements, however due to fundamental law in quantum mechanics (the no-cloning theorem [10]) the register M' cannot be copied just as any other quantum information (it contains unknown quantum states). Moreover the bigger number of qubits in the register M' the harder it would be to deduce information about coefficients and this difficulty will grow exponentially, due to unknown linear combination coefficients in M' and exponentially growing their number in the superposition in regard to the dimension of the Hilbert space 2^n, even if one assumes to have the copies of M'.

((35)) Upon the above discussion there is revealed one of the most important properties of the OQP protocol, namely the property of the single key qubit K' measurement. If someone performs the measurement on the key qubit K', then he will non-locally project with probability $|a|^2$ the 3-qubits state in M' to $|\psi_1\rangle$ pure state or with probability $|b|^2$ to $|\psi_2\rangle$ pure state. Each of the above two alternative pure states to which M' will be projected upon a measurement of the key qubit K' are not entangled anymore (this means measurement of the key qubit K' will disentangle M', thus returning it to the original quantum message M, or essentially decrypting it) but within the following two cases:

- with probability $|a|^2$: $ceg\,|000\rangle + ceh\,|001\rangle + cfg\,|010\rangle + cfh\,|011\rangle + deg\,|100\rangle + deh\,|101\rangle + dfg\,|110\rangle + dfh\,|111\rangle$ $= |\psi_1\rangle = (c\,|0\rangle + d\,|1\rangle)\,(e\,|0\rangle + f\,|1\rangle)\,(g\,|0\rangle + h\,|1\rangle)$ - this state is shown explicitly to be seperable not entangled states of the 3 original qubits of quantum message M,
- with probability $|b|^2$: $ceg\,|111\rangle + ceh\,|110\rangle + cfg\,|101\rangle + cfh\,|100\rangle + deg\,|011\rangle + deh\,|010\rangle + dfg\,|001\rangle + dfh\,|000\rangle$ $= |\psi_2\rangle = (c\,|1\rangle + d\,|0\rangle)\,(e\,|1\rangle + f\,|0\rangle)\,(g\,|1\rangle + h\,|0\rangle)$ - this state is shown to be also seperable not entangled states of the 3 qubits, but they are all quantum negated qubits of M. (with Pauli σ_x transformation)

((36)) To make sure this is the case one can follow below analysis in the density matrix formalism in simplified case of only 2 qubits: 1 key qubit $|K\rangle = a\,|0\rangle + |1\rangle$ and 1 message qubit $|M\rangle = c\,|0\rangle + d\,|1\rangle$ (the case for 3 qubits as discussed above easily generalizes the density matrix formalism analysis below, however due to number of terms in density matrix equal to 64 instead of 16 it is too robust to be presented here).

((37)) The CNOT operation on both qubits (K is control qubit and M is target qubit) gives: $(a\,|0\rangle + b\,|1\rangle)$ CNOT $(c\,|0\rangle + d\,|1\rangle) = ac\,|00\rangle + ad\,|01\rangle + bc\,|11\rangle + bd\,|10\rangle$.

((38)) The density matrix of the resulting entangled state of key qubit (K') and message qubit (M') is following:

$$\begin{aligned}
&ac\,|00\rangle + ad\,|01\rangle + bc\,|11\rangle + bd\,|10\rangle * a^*c^*\,\langle 00| + a^*d^*\,\langle 01| + b^*c^*\,\langle 11| + b^*d^*\,\langle 10| \\
&= aca^*c^*\,|00\rangle\langle 00| + aca^*d^*\,|00\rangle\langle 01| + acb^*c^*\,|00\rangle\langle 11| + acb^*d^*\,|00\rangle\langle 10| \\
&+ ada^*c^*\,|01\rangle\langle 00| + ada^*d^*\,|01\rangle\langle 01| + adb^*c^*\,|01\rangle\langle 11| + adb^*d^*\,|01\rangle\langle 10| \\
&+ bca^*c^*\,|11\rangle\langle 00| + bca^*d^*\,|11\rangle\langle 01| + bcb^*c^*\,|11\rangle\langle 11| + bcb^*d^*\,|11\rangle\langle 10| \\
&+ bda^*c^*\,|10\rangle\langle 00| + bda^*d^*\,|10\rangle\langle 01| + bdb^*c^*\,|10\rangle\langle 11| + bdb^*d^*\,|10\rangle\langle 10|
\end{aligned} \tag{7}$$

((39)) Hence the form of density matrix of mixed state of the message qubit (M') after tracing out key qubit K':

$$\begin{aligned}
&|a|^2\,|c|^2\,|0\rangle\langle 0| + |a|^2\,cd^*\,|0\rangle\langle 1| + |a|^2\,dc^*\,|1\rangle\langle 0| + |a|^2\,|d|^2\,|1\rangle\langle 1| \\
&+ |b|^2\,|c|^2\,|1\rangle\langle 1| + |b|^2\,cd^*\,|1\rangle\langle 0| + |b|^2\,dc^*\,|0\rangle\langle 1| + |b|^2\,|d|^2\,|0\rangle\langle 0|
\end{aligned} \tag{8}$$

((40)) From this form it is evident that if the key qubit (K) is measured then with the probabilities:

- $|a|^2$: the message qubit reduced density matrix has the form: $|c|^2\,|0\rangle\langle 0| + cd^*\,|0\rangle\langle 1| + dc^*\,|1\rangle\langle 0| + |d|^2\,|1\rangle\langle 1|$ $= (c\,|0\rangle + d\,|1\rangle)\,(c^*\,\langle 0| + d^*\,\langle 1|)$ – this is projection operator on the state $(c\,|0\rangle + d\,|1\rangle)$ which means that after measuring qubit K the qubit M returns to its original state,
- $|b|^2$: the message qubit reduced density matrix has the form: $|c|^2\,|1\rangle\langle 1| + cd^*\,|1\rangle\langle 0| + dc^*\,|0\rangle\langle 1| + |d|^2\,|0\rangle\langle 0|$ $= (c\,|1\rangle + d\,|0\rangle))\,(c^*\,\langle 1| + d^*\,\langle 0|))$ – this is projection operator on the state $(c\,|1\rangle + d\,|0\rangle)$ which means that after measuring qubit K the qubit M returns to the quantum negation of its original state (so if one measures the key qubit as $|1\rangle$ one knows that to restore original state of qubit in M it must be quantum negated).

((41)) This means that measurement on the key qubit K' instantly (non-locally) decrypts the entangled M' to disentangled M (while in the case of projecting the key qubit K' upon its measurment to state $|0\rangle$ with probability $|a|^2$ the M' is in no time, instantly, projected to M, however in the opposite case with probability $|b|^2$ the key qubit K' upon measurement projects to $|1\rangle$, which will mean that each qubit in the register M must be quantum negated, i.e. under action of Pauli σ_x transformation, what effectively restores original quantum information M. Another decrypting (disentangling) procedure to obtain original quantum message M (also only possible with the key qubit K'), is to reverse all unitary operations by applying tho CNOT operations in a reversed order (all unitary operations are reversible, but the ones used here, i.e. quantum negation σ_x and more generally CNOT transformation are all self-reversible, which means if applied twice, they reduce to identity transformations). Therefore to this end of decrypting M' one needs to cyclically transform the key qubit K' (as the control qubit) with subsequent qubits in M' (target qubits) but in a reversed order (first the K' single key qubit CNOT with last M' qubit, second the single key qubit output from previous CNOT operation again in CNOT with one before the last qubit of M', and finally in n-th iteration the single key qubit CNOT with the first qubit of M'). This will revert all unitary operations and thus completely disentangle the state of the single qubit key K' with quantum message register M', returning both registers to their original configurations of K and M and hence decrypting the original quantum information (even if the key qubit K or the qubits of quantum message register M were in mixed states before the encryption).

Conclusions

((42)) It is puzzling on a first glance that one can use just a single qubit (key K) to unconditionally (quantum information theoretic) lock (encrypt) arbitrarily long sequence of n qubits (in register M). The question arises how comes the ability to store the quantum information in the form of entanglement with infinitely many (n) qubits of quantum message M just in the single key qubit K. One should notice that qubit information capacity is continuously infinite (due to linear combination coefficients being two complex numbers from the continuous domain, which is due to defining quantum mechanics systems' spaces of states as Hilbert spaces upon the field of complex numbers). Therefore the discrete infinity (infinite number of qubits – n with cardinal number $\aleph_0$) is nothing in comparison to continuous infinity of the information capacity of just a single qubit. However it should be stressed that actually the information is non-locally stored in the phase of all n+1 qubits (the phase is due to the special non-separable entangled forms of multiplications of the involved superposition coefficients non-locally shared among all the qubits), which means that the essential entanglement information is also shared within M'. However it is true that this information is stored non-locally in the entanglement. If one only has the single qubit key K', one can by just measuring it decrypt the M' to M (by disentangling it with the von Neumann projective measurement), wherever it is located (and this will happen instantly as a result of the projection based quantum measurement). It will however require to transfer 1 bit of the classical information (at most with velocity of light) to the location of the decrypted M message that will tell the receiver of M, whether or not it is in the original or quantum negated configuration of the quantum message, thus for it to be properly recovered).

((43)) The result of the proposed OQP scheme as a most general quantum information encryption primitive can be discussed upon a topological approach. In a simplified and illustrative analogy the entanglement is related to phase changes upon encircling one particle by the other with virtual loops that entangle particles together (in single-qubits corresponding dimension-reduced projections of involved multidimensional rotations entangling the qubits in the action of the CNOT). In limited dimensions of phase spaces such as would apply to qubits this could be interepreted in terms of non-reducible loops of trajectories with one qubit around the other. Each abstractly-modeled in topological sense loop of entanglement (corresponding to action of each CNOT cycle) of the key qubit K around subsequent qubits of the quantum message M is entangling M' qubits together and all of them with K'. This will produce a joint knot of entanglement between all the qubits, however characterized by a certain symmetry in relation to the key qubit K. Each such abstract loop (CNOT) is effectively changing the phase and will result finally in the non-local phase entanglement for all n+1 qubits (a multi-qubit entanglement state). Upon density matrix formal consideration this has been be analyzed in detail in the previous section. All the entangling phase terms due to phase representation of complex linear combination coefficients for each qubit superposition occupy non-diagonal elements in the density matrix of the whole n+1 qubits system. Due to special symmetry in relation to the qubit K' only the measurement done over the qubit key K' will dephase the density matrix in such a manner that will result in a seperable in regard to tensor product pure states density matrices for M' qubits and thus will be equivalent with disentangling of the whole M' qubits register from the qubit key K'. This means that entangling phase of the whole system can be freed by measuring the key qubit K', which in the topological terms can be interpreted as cutting the entanglement knot in such a way that frees all the loops entangling remaining qubits (as these loops, also referred as to topological rings, will be cut at the ring of the K' entanglement – all other rings representing remaining qubits will disentangle, however cutting any other ring which would mean measuring of any other qubit from M' will just disentangle this only one qubit – with losing its original state – and leaving all other qubits of the message still entangled, i.e. encrypted). In a very simplified illustrative comparison one could say that the key qubit K' is the ring holding other small rings together (each of these small rings is an illustrative analog of the respective original qubit from M only when all are disentangled from the main ring of K' qubit). If K' is hidden so are effectively all qubits from M upon joint entanglement of K' and M'. The difference to classical analogy is non-locality, which could be visualized in this simplified analogy in the situation that one would be able to still hide only the large ring of individual small rings in a pocket without the small rings themselves, leaving them however useless on the table (securely encrypted, with no access to original quantum information possible). Only if one cuts the K' ring (measures the single-qubit key) the non-locally bound to it rings on the table will be freed and will revert to the original quantum message qubits' states (ot their σ_x quantum negation). Any manipulation on individual encrypted quantum message qubits M' will not reveal original quantum message M without the key ring K'. A more advanced discussion of the relation between quantum physics and the topology can be found in e.g. [13–15] in regard to the links between the two domains – in particular in context of braid groups enabling a geometrical explanation of quantum statistics, i.e. distinction of fermions and bosons in 3D by topological differences in trajectories for elementary particles quantum states replacements, as well as to the concept of anyons [16] in 2D physical systems and discussion of the QHE (Quantum Hall Effect) in topological terms.

Further discussion of the OQP properties

((44)) The main advantage of the OQP protocol and is that it uses only a single qubit as the one-qubit key to uncondtionally (in quantum information-theoretic sense) secure the n-qubits quantum information (quantum message) encrypted with this one-qubit key. At the basis of the invention is a novel concept not previously described in the literature that very drastically improves efficiency of quantum information encryption due to the non-local quantum entanglement that can be not only used (as discussed previously, e.g. in [11]) pairwise between the subsequent qubits' positions of the key in n-qubits register (or even $2n$-qubits splitted in two n-qubits keys registers as proposed in [11]) and the quantum information (message) in also n-qubits register (thus forming pairwise key-qubit and message-qubit entanglements), but rather much more generally utilizing the multi-qubit encryption of then only required just unknown and secret single-qubit key, sequentially co-entangled with qubits of the n-qubits quantum message to be encrypted. This concept provides a qualitative gain: a single (unknown and arbitraty) qubit constituting a key entangled but upon a complex mutli-qubit entanglement with the n qubits of the quantum information can secure this quantum information just as well as n (or in some propositions $2n$) qubits of the key. It could be discussed how this difference affects security of quantum communication in for example a general scheme of quantum teleportation. Generally in standard quantum teleportation one needs n pairs of maximally entangled qubits (Bell states - together $2n$ qubits pairwise entangled) to securely and non-locally communicate quantum information of n-qubits. With the OQP protocol there is need for just a single Bell state shared between the parties to teleport securely and non-loclly the single key qubit for the encrypted by multi-qubit entanglement message that is transmitted in the local quantum channel (without pre-shared entanglement). This is however in detail discussed in the Industrial Applicability section below. The list of advantageous effects of invention is also stipulated in a point by point form within the section of Claims.

((45)) It should be noted that some publications in the literature interestingly point to discussing the reasons and motivations behind encryption of quauntum information. E.g. in [17] it is pointed out that quantum information is already encrypted, as only one bit of information can be revealed from a qubit - but of course the statement that quantum information is by itself encrypted may be considered valid only in the context of classical information. In the context of quantum information, the non-encrypted quantum information can be of course straightforwardly accessed by an adversary not neccessarily upon a measurment but more likely e.g. as an input for quantum computation (or more generally quantum information processing). If one would like to secure quantum information of some value from this kind of unauthorized access, the encryption of quantum information is thus neccessary. But how to encrypt quantum information? Generally there are two ways to do it: one can either consider some ceretely parametrized unitary or non non-unitary evolution of quantum states, while the latter is due to a unitary evolution of a complex system containing the quantum state in question as a subsystem. Due to the formulation of quantum mechanics of complex systems involving tensor products of Hilbert spaces of their subsystems and the algebraic structure of the tensor product it follows that if complex system evolves unitarily, then its constituting linear combination become non-separable in terms of basis states of subsystems' of Hilbert spaces and thus those subsystems in general do not undergo unitary evolution but are instead non-unitarily transformed from normalized pure states to non-normalized mixed states. In the language of quantum circuits the two mentioned above ways of encrypting quantum information can be realized as quantum gates, controlled by either classical or quantum information. If controlled gates and for clarity let's assume the CNOT gates (the most simple ones and also universal together with one-qubit gates of Hadamard and Phase) are conditioned by classical information they do not introduce entanglement on quantum information (and thus implement the former method of encryption of quantum information - the unitary one without entanglement, in case of CNOT simply the quantum negation Pauli σ_x transformation upon the target qubit). If however they are conditioned by quantum information (superposition of basis states) then they entangle the control qubit with the target qubit (setting them in non seperable in regard to tensor product pure state of complex system consisting of two qubits) which means, that they bring the target qubit out of its normalized pure state to non-normalized mixed state upon non-unitary evolution (what can be described correctly within the density matrix formalism). So summarizing the encryption of the quantum information can be done either by some secret parametrizing of the unitary evolution (classically controlled quantum gates) in which case the key (condition of controlled quantum gates) is classical information or by a secret parametrizing of the non-unitary evolution (quantumly controlled quantum gates) where in this case the key for encryption is quantum information inevitable inrocuding entanglement. It should be noted that the former method is just a special case of the latter one. Therefore for the most general consideration of quantum information encryption, the encryption with a quantum key and entanglement is the most general consideration (which also has one fundamental advantage over the former case of classical information based encryption of quantum states: the quantum key cannot be copied as guaranteed by the no-cloning theorem [10]).

((46)) The Solution to Problem section above had in detail explained and illustrated relation of the OQP to QOTP (the Quantum One-Time Pad being straightforward extension of the classical One-Time Pad) (compare Fig. 1 with Fig. 2 and Fig. 3) and the advantages of the former over the latter. It should be noted here that in the literature the Quantum One Time Pad has not been widely discussed. Even though the "quantum one time pad" has been used in previous scientific publications it did not refer not only to the invention presented herewithin (the One-Qubit Pad protocol) but even to the trivial extension of the classical One-Time Pad to quantum case as discussed in the above section. The reference to Quantum One-Time Pad in known scientific literature was applied to a specturm of different concepts within quantum information with overlaps with the classical information. In most cases described in the scientific literature the QOTP was used to refer to few different methods of quantumly securing communication of classical messages (most prominently this was addressed to the original Quantum Superdense Coding protocol by Bennett, et al. [18] or the QSDC, sometimes also referred to as Quantum Secure Direct Communication). These examples of literature include [19–23]. Also in the context of QOTP in the literature there have been discussed proposals regarding private commmunication (or also authentication) of quantum information but using only classical information (classical keys composed not of qubits but rather of classical bits). This approach has been for example discussed in [17, 24–26]. Those propositions and discussions can be generalized to the concept of the Private Quantum Channel (PQC) as introduced in [24], but the PQC for encrypting quantum information is based upon classical keys (and thus employing only unitary operations witout introducing additional entanglement). Interesting is discussion presented in e.g. [17] as it builds on the concept of recycling of the key, which of the first glance might seem close to the proposed OQP protocol. However it is not the case as the recycling of the key as disccussed in this publication refers to the classical key and secondly is certainly very far from the limit of just 1 bit as would be the classical counterpart of the OQP protocol described herewithin.

((47)) Summarizing, the currently known in the literature concepts upon quantum information encryption resolve mainly to more fundamental concepts of the Superdense Coding (QSDC) [18], that can be assigned also different acronym expansion: Quantum Secure Direct Communication (which applies to securing classical information with quantum resources - in QSDC Alice and Bob share one copy of Bell state, e.g. —psi+¿ and Alice can send 2 classical bits to Bob by applying controlled σ_x and controlled σ_z operations to her Bell pair qubit and then send the qubit to Bob, who can determine the 2 bits of classical information by a Bell basis measurement on both qubits, thus the classical information is sent securely and non-locally encoded upon the entanglement) as well as to the Quantum Teleportation (QT) [12], addressing problem of secure communication of quantum information non-locally with both classical and quantum resources (with condition to pre-share n pairs of maximally entangled qubits in Bell states to securely communicate n qubits of quantum information), with the addition of the Private Quantum Channel PQC [24], referring to encrypting of quantum states with classical information and relating this issue with a more general problem of randomization of the quantum state. In one proposition referring to the quantum version of the Vernam cipher in [11] there is introduced generalized PQC approach with quantum key, however consisting of 2n entangled pairs (2n Bell states or ebits as referred to units of maximal entangled pairs) required to encrypt n qubits quantum message. This proposal differs from the herewithin described protocol by using as a key not the unknown quantum information (unknown, arbitraty state of qubit) but rather entanglement itself upon perfectly known quantum states. These states within the key are fully symmetrical maximal entanglement paired (2-qubits) states of the known Bell states, known also to a potential adversary (measured in ebits as used by authors). This is fundamental difference. Defining known Bell states as the key is one of special cases of the QOTP as discussed in the section above and is rather pointing towards a more general protocol of Quantum Teleportation. Moreoever it also generalizes the PQC notion from [24], however it doesn't relate to the more general QOTP and OQP protocols. First in our proposition the entanglement in encryption scheme is not a key itself (the key is a quantum state both in straightforward generalization of classical OTP to QOTP and in the novel OQP invention, but in contrast to the discussed in [11] variation of the quantum Vernam chipher - in our more extended generalization of what we understand as a quantum key in both generalized Vernam cipher or QOTP and OQP - the unknown one and therefore certainly not symmetrical). To better contextualize the proposed OQP invention - in up-to-date literature regarding quantum analogs of OTP (or Vernam cipher), the quantum information (message) in the register is encrypted by either classical information or the entanglement key in known quantum state of Bell basis (shared between Alice and Bob) and additionally it is done bitwise, i.e. on each position of the quantum message M using subsequent blocks of the quantum key K with double the number of qubits (to securely send the n qubits quantum information a one qubit protocol is applied bitwise using for each encrypted qubit two Bell states or two ebits). In terms of pointing out advantages of the proposed OQP protocol, this kind of known from the literature proposition [11] may be criqued by the lack of reasonable motivation, in view that OQP can secure quantum information with just a single qubit (and send it securely between communication parties by pre-shared single Bell state, as one can refer to the Fig. 5) whereas in the proposal of [11] the quantum analog of Vernam cipher can securely transmit n qubits of quantum message M by use of the entanglement key consisting of 2n ebits (i.e. Alice and Bob sharing 2n pairs of maximally entangled qubits). Such prerequisite seems to be quite non-efficient, because there are well known means to do it much more efficiently even without the OQP protocol - by the use of Quantum Teleportation (QT). It should be stressed that upon a fundamental approach the more efficient and also more evident generalization of the classical One-Time Pad (Vernam cipher) to the quantum regime in case of meeting prerequiste of sharing n Bell states between the communication parties is the Quantum Teleportation protocol [12] (in QT only one ebit, i.e. one shared Bell state is required to securely transmit one qubit in any arbitrary quantum state, what is sufficient to securely and non-locally transfer the single key qubit in OQP).

((48)) Discussing the quantum information in general will fast point to one important aspect: namely that each unknown quantum state of qubit posseses continous classical information capacity and this fact is of a fundamental importance that exceeds all classical results upon analyses how one can use classical information as keys to encrypt quantum information. In some of the mentioned above literature this concept is shortly discussed but not used as the central aspect of provided security in quantum information encryption. The proposed protocol is fully based on this property of quantum information (the continously infinite informational capacity of a single qubit). In the OQP protocol an unknown arbitraty quantum state of a single qubit can be effectively used to fully securely encrypt arbitrary quantum message. This result stands out from discussion currently known from the literature. This discussion however applies also to the proposed protocol or more straightforward generalization of the OTP towards QOTP in one of their border cases: i.e. if either the qubit key K or the unknown quantum information in qubits M or both of them consist of qubits in some symmetrical states (e.g. either the basis states $|0\rangle$ and $|1\rangle$ or $|+\rangle$ and $|-\rangle$ which however represent classical information, or the symmetrical computational basis Bell states which are pairwise quantum entangled, however still with special symmetries related to classical information identified with the states from the basis representing classical information bits). If the above border cases are not realized then the information-theoretic secure encryption upon entanglement will take place by CNOT action of just the single key qubit K on

n-qubits quantum message M, transforming it to a jointly entangled state of K' and M', and thus M' will be then fully indenpendent from M, so there is no any possible operation of either measurement or unitary operation to restore the original quantum information M if the adversary (Eve) would not have the single qubit key K' at her disposal (only the previous existance of some symmetric relations in either K or M qubits to classical information would cause that the independence of M' from M would not be provided). Indeed the concepts that reduce the herewithin proposed protocol to its border cases are discussed in the mentioned literature (as these border cases are equivalent with the special cases discussed in these publications), especially in [24] as related to limitations regarding the amount of classical information key to securely encrypt n-qubits quantum information (a proof that 2n classical bits is necessary to theoretic-securely encrypt n-qubits which can be generalized to earlier concepts of quantum teleportation and superdense coding in both of which 1 qubit relates with 2 bits of classical information) and in [11] as regarding the result showing then recycling quantum key (however made of symmetrical Bell states or ebits) also resolves to the classical key case limitations (that is to recycling the classical key in the Private Quantum Channel PQC as that paper itself proves). The recycling of the quantum key concept as described in [11] is also limited conceptually in regard to not having the multi-qubit entanglement included within the currently proposed OQP protocol. The main advantage of the OQP proposed protocol lies in its efficiency. Only one arbitraty unknown quantum state (the single quantum key K) is used for quantum-information-theoretic secure ecnryption of an arbitraty number of n qubits in their arbitraty unknown quantum states. In more fundamental approach upon quantum teleportation, a non-local secure communicating of the n qubits quantum message M will require n entangled qubits shared beforehand for the teleportation of each subsequent qubit of the quantum message M (the entanglement shared between the parties will form a non-local key, however utilizing only 2-qubits pairwise entanglement between qubits in the key – the quantum key in such of quantum teleportation can be understood to be distributed between Alice and Bob who both share each qubit out of entangled pair). In the OQP protocol the encryption of the quantum key with the message will form multi-qubit entanglement which should be hightlighted as the fundamental difference.

Brief Description of Drawings

((49)) [Fig. 1] Quantum One-Time Pad (QOTP), a straightforward generalization of the classical One-Time Pad (OTP) to quantum case is illustrated on the Fig. 1 There are two registers: the register of the quantum message M and the register of the quantum key K, both registers have n qubits. The quantum information encryption operation of the QOTP protocol is based on the pairwise entanglement between subsequent qubits in M and K on their corresponding positions which is introduced by quantum controlled negation (CNOT) gate with the key qubits of K being control qubits and the message qubits of M being target qubits (the concept is presented in section A). In the case that all qubits in M and K are basis states (i.e. represent classical information) the QOTP reduces to classical OTP encryption as the operation of quantum CNOT reduces to classical CNOT (the classical CNOT is equivalent to XOR, just additionally outputting the key bit). If the key register K consists of qubits in unknown quantum states then quantum CNOT will entangle them with the respective qubits of M resulting in jointly pairwise entangled registers of M' and K'. It is important to stress that in this situation there will be no multi-qubit entanglement, entanglement will be only between the pairs of corresponding M' and K' qubits. To decrypt the entangled message M' one needs to be at disposal of K' and either use again the CNOT gates or measure the states of K' register - both operations will disentangle the M' qubits returning them to original states of the quantum message M register. On the bottom of the Fig. 1 there are represented: the quantum circuit implementing QOTP: n qubits of quantum message M and n qubits of quantum key K are entangled together pairwise by CNOT gates (B) and its two decrypting configurations by measurement (D) or reversal of CNOT gates (E). Additionally there is also a time-like encrypting operation with a single CNOT gate (C).

((50)) [Fig. 2] The basic idea of the One-Qubit Pad (OQP) protocol and its implementing generic device is to apply CNOT operation with the same single qubit key K as the control qubit but targeting subsequent qubits in n-qubits quantum message register M - this eventually produces a joint (n+1)-qubit entanglement between the key qubit and quantum message as presented in the Fig. 2.

((51)) [Fig. 3] The implementation of the OQP protocol as a generic device in quantum circuit theory can be referred to the Fig. 3 It should be noted that the quantum circuit scheme of the device doesn't have to rely on n

CNOT gates. There could be just a single CNOT gate and single key qubit K' could be looped to go from the output of control CNOT qubit to its control input in subsequent iterations of n qubits in M fed to the target input of this single CNOT gate (as illustrated on the right of Fig. 3). Nevertheless in the quantum circuit theory the proper representation is given as on the left of the Fig. 3 with step-like form of subsequent CNOT operations entangling qubits of M with the single key qubit K. After the quantum message has been encrypted upon its entanglement with key qubit K', to decrypt it (disentangle) one must have the key qubit K' at his disposal, and either reverse the quantum circuit with CNOT gates applied in reversed order, i.e. first for the key qubit K' and the last qubit in M' and so on finally up to the key qubit with the first qubit of encrypted quantum message M', what will disentangle and thus decrypt M' to original quantum message register M of n-qubits, or to measure the single qubit key K' (this is illustrated on the Fig. 4)

((52)) [Fig. 4] The procedure of decryption (disentanglement) by the single key qubit K' measurement is illustrated on the Fig. 4 upon a quantum circuit representation. The left part of the figure is referring to quantum measurement on the single key qubit K' that will condition by either —0¿ or —1¿ measurement projection outcome the quantum negation (σ_x Pauli matrices gates) on all qubits in disentangling M (if the key projects to —0¿ the quantum negation is not applied and the M' is decrypted to original quantum message qubits register M, while in opposite case the quantum negation gate must be applied to all message qubits after disentanglement to decrypt M). The classical output of the measurement of the single key qubit K' is shown to condition the quantum negation on the quantum message M to decrypt it. On the right section of the figure the reversed order of CNOT operations are presented to also decrypt quantum message M with the single qubit key.

((53)) [Fig. 5] The application of OQP in secure quantum communication is shown on the Fig. 5 with combining the OQP protocol with the quantum teleportation (QT). For Alice to securely send n-qubits message M to Bob quantum teleportation protocol is good choice. She would need however to pre-share with Bob exactly n pairs of entangled qubits in Bell states. Then each qubit of message M Alice could teleport to Bob non-locally, thus the quantum information in M would remain safe and inaccessible to an adversary (Eve). Additionally for each of the teleported qubit Alice would need to send 2 bits of classical information to let Bob restore the correct state of teleported subsequent qubit of M (altogher for n qubits in teleporting M Alice needs to send 2n bits of classical information). The advantage of the OQP protocol is following: when Alice implements the OQP protocol (runs her n qubits quantum message register M through the OQP generic device thus entangling all qubits of M with the single qubit K, obtaining n+1-qubits jointly entangled state of K' and M') she can send the M' through a standard quantum channel and only securely and non-locally teleport the single qubit key K'. If Eve intercepts quantum message M' she won't be able to restore the original quantum message M out of M' without the single key qubit K' entangled with M'. The key qubit K' will be however secured from Eve being non-locally teleported to Bob along with 2 bits of classical information to enable Bob to restore the proper state of K'. When Bob gets the single qubit key K' teleported to him and the message M' arrives in standard quantum channel (a local one without pre-shared entanglement for n-qubits), he can the use the key to decrypt (disentangle) the quantum message M (by reversing OQP protocol operation or simply measuring the key K'). Thus for secure communication in the latter scenario of OQP only 1 qubit (of the key) needs to be teleported to securely (privately) communicate n-qubits of quantum message (which means Alice and Bob need to share only 1 maximally entangled pair of qubits, the Bell state) in contrast to full teleportation of M which would require Alice and Bob to share n maximally entangled pairs of Bell state qubits). One should point however that this gain (1 pre-shared Bell state and just 2 bits of classical information broadcast to securely send n qubits of quantum message from Alice to Bob with OQP against the n pre-shared Bell states and 2n bits of classical information broadcast to do the same without OQP in the teleportation only scenario) comes at a price. The price in the OQP communication scenario is with the possibility to intercept the encrypted message M' and destroying or changing it by Eve. It should be stressed however that it won't allow Eve to access the original decrypted quantum message M (one can do this only if at disposal of the single key qubit K'), but Eve will still be able to prevent Bob from receiving the M' (which is impossible in the teleportation-only scenario, assumed of course that classical communication channel is authenticated and Eve cannot interfere with it, as if she could, then the teleportation won't work properly). Therefore one can have the impression that the communication related applications of OQP are somewhat more limited than general teleportation based secure communication of quantum information. This is however not justified, as it comes evident from the fact that OQP with quantum teleportation of the single qubit key is also much more efficient in terms of required resources: prerequisite of only 1 Bell state shared between Alice and Bob in contrast to n Bell states required for teleportation-only secure communication. In the latter case one needs to provide for a method to distribute the n perfect Bell states between Alice and Bob and this must happen through a normal, local quantum channel. In most extreme situation (Eve completely controls the local quantum channel between Alice and Bob) there is no way to do this, i.e. both QT and OQP are doomed to failure. In less extreme situation this quantum channel for QT Bell states distribution (exactly as in the OQP communication scheme) is a potential subject of only partial adversary manipulation or also decoherence (i.e. the same two issues regarding the quantum channel for sending encrypted M' in OQP). In case of QT of course Alice and Bob can in principle use the known methods for entanglement distillation [27–33], but this will result in the neccessity to actually exchange many more then n imperfect (decohered or manipulated in the local quantum channel) qubits between them, from a large number of which they can eventually obtain the much smaller number of n perfect Bell states. This is corresponding to the possibility to correct for adversary manipulation or decoherence by introducing some redundancy or more advanced error correction codes into the quantum message M (extending its size from n qubits to much larger number of qubits) then encrypted upon the entanglement based OQP to M' (thus even if Bob receives partially manipulated or decohered M' then knowing the state of K' he will be able to apply quantum error correction to obtain much shorter but true original message M). The discussion of imperfect quantum channels is however out of the scope of the proposed OQP protocol and its generic device (the results from quantum error correction can be applied into the extension of OQP protocol application schemes).

Description of Embodiments

((54)) The invention consisting of technical generic device implementing the proposed OQP protocol will use the following components: already maturing in the current-state-of-the-art implemented technically CNOT gates and related to their implementation, implementations of qubits themselves and their quantum channels. The CNOT gates and related to their definitions qubits are implemented for many years (cf. e.g. [34–48]). Building of the generic device implementing the OQP protocol can be realized on any technological implementation of qubits and their CNOT operations and is currently achievable technologically. While the qubits and CNOT gates are basic components of the OQP device, the invention doesn't depend on particular implementation technology used for quantum information carriers (qubits) and interactions between the qubits carriers (implementing CNOT gates). These can be realized in the regimes of orbital or spin degrees of freedom in matter or with polarization or phase degrees of freedom of light, etc. It should be stressed that implementation of OQP protocol / device doesn't require universal quantum computation in principle (only the qubits carriers and the CNOT gate technology is required). The generic device abstracts from the actual realization of its components and even abstracts of physical carriers that will implement qubits. These can be either photon qubits or matter qubits (e.g. atoms, ions, excitons in quantum dots, nuclues, etc. both with their orbital and spin degrees of freedom). It means that the patented device will work in any physically valid implementation of CNOT gates, qubits and their channels. The technical schema of the device is presented in the Fig. 3 and Fig. 4 while implementation in combining with quantum teleportation (also succesfully implemented, cf. e.g. [49, 50]) towards secure quantum communication applications is presented in the Fig. 5.

((55)) As there are many succesful implementations of CNOT gates and qubits the preferred choice for implementation of the generic OQP device lies within photon implementations (e.g. [35, 40–44, 46, 47]), much more sensible for quantum communication scenarios. In OQP case, similarily as in case of quantum cryptography, the device does not need scallable and universal quantum gates architectures assuming noiseless channels. Imperfect quantum channels would require quantum error-correction (cf. e.f. [29, 51]) for M. The scallabe universal quantum computers were not built as of yet, but progress is ongoing and there might be a breakthrough in one of the explored technology regimes, which will support this technology for OQP implementation to be compatible with the succesful implementation regime of the universal quantum computer - which technology it will be it is however hard to predict now.

((56)) In principle the OQP device can be built on a single CNOT gate in which the single control qubit K (the key qubit) would be looped for n times while n-qubits register of M would be fed sequentially to CNOT interaction with qubit K (this is illustrated on the Fig. 3). **((57))** As mentioned the whole setup for utilizing OQP in quantum communication involves also Quantum Teleportation [12] of the single key qubit, and this technology is achievable and already implemented for many years [49], recently from Earth to the orbit as well [50].

Industrial Applicability

((58)) It should be noted that likewise classical OTP the proposed invention of OQP can have applications not only in communication. The OQP can be used as the Quantum Safe (QS), to lock valuable quantum information (this however requires protection from decoherence, i.e. a good implementation of qubit: proper quantum memory). The Quantum Safe is thus a technological device based on the OQP generic device in which some crucial quantum information is being locked by the quantum key. The crucial quantum information is any information of some important value (a result of advanced quantum computation, quantum entanglement currency wallet or any another quantum data that one wants to keep secured from unauthorized access). If the quantum information M is locked in the Quantum Safe by entangling it with the single qubit key, then it cannot be accessed without this key. One interesting property however is that it can be destroyed.

((59)) The OQP protocol by itself is not suited for the communication scenario, unless it is combined with quantum teleportation [12], but only of the single key qubit. If Alice and Bob want to communicate and Alice had entangled her quantum message with the single qubit quantum key, then she will need to teleport this single qubit key to Bob (upon the non-local channel of the shared Bell pair) but also additionally send the encrypted message in n qubits register to Bob by insecure quantum channel. If Alice does this, Bob will be able to decrypt (disentangle) the encrypted quantum message register with the single qubit key and thus access the original quantum information (that he can use accordingly, e.g. in his quantum computation). Of course in that situation Eve can eavesdrop on the insecure quantum channel (it should be noted that in contrast to classical eavesdropping in quantum case the eavesdroping is fundamentally different, because since the quantum information cannot be copied guaranteed by the no-cloning theorem [10] to be eveasdropped it must be actually hi-jacked - of course under the assumption of the full man-in-the-middle type of attack when Eve is able to fully impersonate Bob for Alice and Alice for Bob, after hi-jacking encrypted quantum message she still cannot access it, because she is unable to disentangle it from the single qubit key, protected from her by the non-local QT transfer to Bob. The application of OQP in secure quantum communication is shown on the Fig. 5 with combining the OQP protocol with the quantum teleportation (QT).

((60)) Normally when Alice would like to securely send n-qubits message M to Bob, she could have used quantum teleportation protocol. However to do this she would need to pre-share with Bob exactly n pairs of entangled qubits in Bell states. Then each qubit of message M Alice could teleport to Bob non-locally, thus the quantum information in M would remain safe and inaccessible by an adversary (Eve). Additionally for each of the teleported qubit Alice would need to send 2 bits of classical information to let Bob restore the correct state of teleported subsequent qubit of M (alltogether for n qubits in teleporting M Alice needs to send 2n bits of classical information). The advantage of the OQP protocol is following: when Alice implements the OQP protocol (runs her n qubits quantum message register M through the OQP generic device thus entangling all qubits of M with the single qubit K, obtaining n+1-qubits jointly entangled state of K' and M') she can send the M' through a standard quantum channel and only securely and non-locally teleport the single qubit key K'. If Eve intercepts quantum message M' she won't be able to restore the original quantum message M out of M' without the single key qubit K' entangled with M'. The key qubit K' will be however secured from Eve being non-locally teleported to Bob along with 2 bits of classical information to enable Bob to restore the proper state of K'. When Bob gets the single qubit key K' teleported to him and the message M' arrives in standard quantum channel (a local one without pre-shared entanglement for n-qubits), he can the use the key to decrypt (disentangle) the quantum message M' (by reversing OQP protocol operation or simply measuring the key K'). Thus for secure communication in the latter scenario of OQP only 1 qubit (of the key) needs to be teleported to securely (privately) communicate n-qubits of quantum message (which means Alice and Bob need to share only 1 maximally entangled pair of qubits, the Bell state) in contrast to full teleportation of M which would require Alice and Bob to share n maximally entangled pairs of Bell state qubits). One should point however that the gain (1 pre-shared Bell state and just 2 bits of classical information broadcasted to securely send n qubits of quantum message from Alice to Bob with OQP against the n pre-shared Bell states and 2n bits of classical information broadcast to do the same without OQP in the teleportation only scenario) comes at a price. The price in the OQP communication scenario is the possibility to intercept the encrypted message M' and destroying or changing it by Eve. It should be stressed however that it won't allow Eve to access the original decrypted quantum message M (one can do this only if at disposal of the single key qubit K'), but she will still be able to prevent Bob from receiving the M' (which is impossible in the teleportation-only scenario, assumed of course that classical communication channel is authenticate and Eve cannot interfere with it, as if she could then the teleportation won't work properly too). Therefore one can have the impression that the communication related applications of OQP are somewhat more limited than general teleportation based secure communication of quantum information. This is however not fully justified, as it comes evident from the fact that OQP with quantum teleportation of the single qubit key is also much more efficient in terms of required resources: prerequisite of only 1 Bell state shared between Alice and Bob in contrast to n Bell states required for teleportation-only secure communication. In the latter case one needs to provide for a method to distribute the n perfect Bell states between Alice and Bob and this must happen through a normal, local quantum channel (without pre-sharing of the entanglement). In most extreme situation (Eve completely controls the local quantum channel between Alice and Bob) there is no way to do this, i.e. both QT and OQP are doomed to failure. In less extreme situation this quantum channel for QT Bell states distribution (exactly as in the OQP communication scheme) is a potential subject of only partial adversary manipulation or also decoherence (i.e. the same two issues regarding the quantum channel for sending encrypted M' in OQP). In case of QT of course Alice and Bob can in principle use the known methods for entanglement distillation [27–33], but this will result in the neccessity to actually exchange many more than n imperfect (decohered or manipulated in the local quantum channel) qubits between them, from a large number of which they can eventually obtain the much smaller number of n perfect Bell states. This is effectively similar to the possibility to correct for adversary manipulation or decoherence by introducing some redundancy or more advanced error correction codes into the quantum message M (extending its size from n qubits to much larger number of qubits) then encrypted upon the entanglement based OQP to M' (thus even if Bob receives partially manipulated or decohered M' then knowing the state of K' he will be able to apply quantum error procedures to obtain much shorter but true original message M). The discussion of imperfect quantum channels is however out of the scope of the proposed OQP protocol and its generic device (the results from quantum error correction [29, 51] can be applied into the extension of OQP protocol application schemes).

Literature

[1] Patent US 1 310 719 A (1919).

[2] Patent US 388244 A (1888) and French Patent No. 146,716 (1882).

[3] C. E. Shannon. Communication theory of secrecy systems. *Bell Sys. Tech. J.*, 28:656–715, 1949.

[4] K. Melville. Securing record communications: The tsec/kw-26. `www.jproc.ca/crypto/kw26.pdf`, 2004.

[5] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22:644–654, 1976.

[6] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 26:96–99, 1983.

[7] V.S. Miller. *Use of Elliptic Curves in Cryptography.* Springer, Berlin, 1986.

[8] Accredited standards committee X9, american national standard X9.62-2005, public key cryptography for the financial services industry, the elliptic curve digital signature algorithm ECDSA, 2005.

[9] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[10] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, 1982.

[11] D. W. Leung. Quantum Vernam cipher. *Quant. Inf. Computat.*, 2:14–32, 2002.

[12] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[13] J. Jacak, I. Jóźwiak, and L. Jacak. New implementation of composite fermions in terms of subgroups of a braid group. *Phys. Lett. A*, 374:346–350, 2009.

[14] J. Jacak, R. Gonczarek, L. Jacak, and I. Jóźwiak. *Application of braid groups in 2D Hall system physics: composite fermion structure.* WorldScientific, Singapore, 2012.

[15] Janusz Jacak. Unconventional fractional quantum hall efect in bilayer graphene. *Sci. Rep.*, 7:8720, 2017.

[16] Frank Wilczek. Quantum mechanics of fractional-spin particles. *Phys. Rev. Lett.*, 49:957–959, 1982.

[17] Jonathan Oppenheim and Michał Horodecki. How to reuse a one-time pad and other notes on authentication, encryption, and protection of quantum information. *Phys. Rev. A*, 72:042309, 2005.

[18] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992.

[19] F.-G. Deng and G. L. Long. Secure direct communication with a quantum one-time pad. *Phys. Rev. A*, 69:052319, 2004.

[20] Benjamin Schumacher and Michael D. Westmoreland. Quantum mutual information and the one-time pad. *Phys. Rev. A*, 74:042305, 2006.

[21] Bin Gu, ChengYi Zhang, GuoSheng Cheng, and YuGai Huang. Robust quantum secure direct communication with a quantum one-time pad over a collective-noise channel. *Sci. China Phys. Mech. Astron.*, 54:942, 2011.

[22] Fernando G. S. L. Brandão and Jonathan Oppenheim. Quantum one-time pad in the presence of an eavesdropper. *Phys. Rev. Lett.*, 108:040504, 2012.

[23] K. Sharma, E. Wakakuwa, and M. M. Wilde. Conditional quantum one-time pad. *ArXiv e-prints*, 2017. arXiv:1703.02903.

[24] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf. Private quantum channels. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 547–553, 2000.

[25] P. Oscar Boykin and Vwani Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67:042317, 2003.

[26] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pages 449–458, 2002.

[27] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53:2046–2052, 1996.

[28] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722–725, 1996.

[29] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, 1996.

[30] Paul G. Kwiat, Salvador Barraza-Lopez, André Stefanov, and Nicolas Gisin. Experimental entanglement distillation and 'hidden' non-locality. *Nature*, 409:1014, 2001.

[31] J.-W. Pan, C. Simon, C. Brukner, and A. Zeilinger. Entanglement purification for quantum communication. *Nature*, 410:1067, 2001.

[32] Takashi Yamamoto, Masato Koashi, Sahin Kaya Özdemir, and Nobuyuki Imoto. Experimental extraction of an entangled photon pair from two identically decohered pairs. *Nature*, 421:343, 2003.

[33] Jian-Wei Pan, Sara Gasparoni, Rupert Ursin, Gregor Weihs, and Anton Zeilinger. Experimental entanglement purification of arbitrary unknown states. *Nature*, 423:417, 2003.

[34] D. M. Zajac, A. J. Sigillito, M. Russ, F. Borjans, J. M. Taylor, G. Burkard, and J. R. Petta. Resonantly driven CNOT gate for electron spins. *Science*, 2017.

[35] Serge Rosenblum, Yvonne Y. Gao, Philip Reinhold, Chen Wang, Christopher J. Axline, Luigi Frunzio, Steven M. Girvin, Liang Jiang, Mazyar Mirrahimi, Michel H. Devoret, and Robert J. Schoelkopf. A CNOT gate between multiphoton qubits encoded in two cavities. *ArXiv e-prints*, 2017. arXiv:1709.05425 [quant-ph].

[36] Yan Liang, Chong Song, Xin Ji, and Shou Zhang. Fast CNOT gate between two spatially separated atoms via shortcuts to adiabatic passage. *Opt. Express*, 23:23798–23810, 2015.

[37] Cristian Bonato, Florian Haupt, Sumant S. R. Oemrawsingh, Jan Gudat, Dapeng Ding, Martin P. van Exter, and Dirk Bouwmeester. Cnot and bell-state analysis in the weak-coupling cavity qed regime. *Phys. Rev. Lett.*, 104:160503, 2010.

[38] L. Isenhower, E. Urban, X. L. Zhang, A. T. Gill, T. Henage, T. A. Johnson, T. G. Walker, and M. Saffman. Demonstration of a neutral atom controlled-not quantum gate. *Phys. Rev. Lett.*, 104:010503, 2010.

[39] J. H. Plantenberg, P. C. de Groot, C. J. P. M. Harmans, and J. E. Mooij. Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits. *Nature*, 447:836, 2007.

[40] Li-Ping Deng, Haibo Wang, and Kaige Wang. Quantum CNOT gates with orbital angular momentum and polarization of single-photon quantum logic. *J. Opt. Soc. Am. B*, 24:2517–2520, 2007.

[41] Z. Zhao, A.-N. Zhang, Y.-A. Chen, H. Zhang, J.-F. Du, T. Yang, and J.-W. Pan. Experimental demonstration of a nondestructive controlled-NOT quantum gate for two independent photon qubits. *Phys. Rev. Lett.*, 94:030501, 2005.

[42] Marco Fiorentino and Franco N. C. Wong. Deterministic controlled-not gate for single-photon two-qubit quantum logic. *Phys. Rev. Lett.*, 93:070502, 2004.

[43] Sara Gasparoni, Jian-Wei Pan, Philip Walther, Terry Rudolph, and Anton Zeilinger. Realization of a photonic controlled-not gate sufficient for quantum computation. *Phys. Rev. Lett.*, 93:020504, 2004.

[44] Kae Nemoto and W. J. Munro. Nearly deterministic linear optical controlled-not gate. *Phys. Rev. Lett.*, 93:250502, 2004.

[45] Ferdinand Schmidt-Kaler, Hartmut Häffner, Mark Riebe, Stephan Gulde, Gavin P. T. Lancaster, Thomas Deuschle, Christoph Becher, Christian F. Roos, Jürgen Eschner, and Rainer Blatt. Realization of the Cirac-Zoller controlled-NOT quantum gate. *Nature*, 422:408, 2003.

[46] T. B. Pittman, M. J. Fitch, B. C Jacobs, and J. D. Franson. Experimental controlled-not logic gate for single photons in the coincidence basis. *Phys. Rev. A*, 68:032316, 2003.

[47] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning. Demonstration of an all-optical quantum controlled-NOT gate. *Nature*, 426:264, 2003.

[48] D. DeMille. Quantum computation with trapped polar molecules. *Phys. Rev. Lett.*, 88:067901, 2002.

[49] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390:575, 1997.

[50] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. Ground-to-satellite quantum teleportation. *Nature*, 549:70, 2017.

[51] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, 1995.

[52] G. Cantor. Ueber eine eigenschaft des inbegriffes aller reellen algebraischen zahlen. *J. Reine Angew. Math.*, 77:258—-262, 1874.

[53] D.M. Greenberger, M.A. Horne, and Zeilinger A. *Going Beyond Bell's Theorem.* Springer, Dordrecht, 1989.

Claims

Claim ((1)) The invented One-Qubit Pad (OQP) protocol and its generic implementing device describe how to securely (with quantum-information-theoretic security) encrypt (upon multi-qubit entanglement) the unknown quantum information (message) of n qubits register (M) in arbitrary states with just a single key qubit (K) in unkown arbitary quantum superposition. This is a novel result in terms of technical invention and application of Quantum Information not described in the literature previously. The main application of the protocol and its related generic device is to lock the quantum information M with the key K of just a single qubit in order to disallow any potential access to the original n qubits quantum information M by an adversary (e.g. the quantum information M might be some valuable output of quantum computation and it should be locked from an adversary disallowing her to use it as an input in her quantum computation, which is gaining importance in the advent of quantum computation and quantum networks processing and communication quantum rather then classical information, e.g. for distributed quantum computation applications, such as the quantum AI, etc.).

Claim ((2)) The proposed OQP protocol and device confirm that quantum information is very distinct from classical information upon showing that generalization of the classical One-Time Pad (upon Vernam's cipher) to the quantum case can be reduced to just One-Qubit Pad (a single qubit is only required to serve as the key, still offering unconditional, i.e. information-theoretic security of encrypted quantum message). One doesn't need to use unkown n-qubits (or even 2n-qubits) states for the key to securely encrypt unkown quantum information of n-qubits: just one key qubit is sufficient but this is due to utilization of the multi-qubit (n+1-qubits) entanglement of the whole joint state of both the key qubit and message qubits (in the known from literature scenarios for encryption of quantum information there is prominently used the pairwise, i.e. 2-qubits entanglement). The proposed invention shows that introducing multi-qubit entanglement by cyclically applying CNOT gate upon the single key qubit K (control qubit) and the subsequent qubits in M (target qubits) can reduce the number of the required key qubits to only one. Additional qualitative difference of the proposed OQP protocol in relation to fully or partly classical encryption protocols (e.g. of quantum information encryption using classical keys, known as Quantum Private Channels or PQC as introduced in [24]) is that both the message and key are quantum information and thus are prohibited to be copied by quantum mechanics laws (the no-cloning theorem [10]). E.g. in PQC schemes the security is not fully information-theoretic because one cannot guarantee that the used classical information key has not been copied, which is precluded on the fundamental level in the proposed OQP protocol, due to its operation on the fully quantum single qubit key.

Claim ((3)) The invention is based upon not widely discussed in the literature uncountable information capacity of the single qubit in contrast to single bit (which is of a countable and finite capacity: just 2 possible values 0 and 1). The qubit itself is a linear combination of two complex numbers fulfilling normalization condition (or upon the Bloch sphere representation of qubit: of real numbers and phase factors). The possible numbers defining the single qubit are thus of the continous set of uncountable inifite cardinal number of possible values (the cardinal number of the continuum is c). This means that one single qubit can hide uncoutably infinite classical information in its single own quantum state. From the proofs of Cantor [52] it follows that: 1) continuum cardinal number is $c = 2^{\aleph_0}$ (where $\aleph_0$ is the cardinal number of the countable set of natural numbers) and 2) that for any two real numbers $a > b$ in any open interval between them: (a, b), no matter how close they are, there are always infinite number of other real numbers set elements, but with the same cardinality of the inifinite as the whole real numbers set (the number c). This means that also any countable number of such intervals will have jointly equinumerous elements as the whole set of the real numbers (similarily the countably many sets of real numbers will be equinumerous jointly with their elements with a single set of real numbers). This also applies to qubits: since the countable inifinite sets of n-qubits are of $\aleph_0$ cardinality, the set of n qubits, even if n is infinite but still countable, will thus have the same information capacity as a single qubit: both sets of inifinities are equinumerous, i.e. the infinite information capacity of single qubit is equinumerous with the infinite capacity of n qubits set. This deep mathematical relation in the framework of Cantor's and later work on the infinities in the set theory constitutes a fundamental observation for the proposed invention to use only a single unknown arbitraty qubit (the single qubit key) to quantum-information-theoretically securely encrypt in entanglement an unkown arbitrary n qubits information (message) within the invented One-Qubit Pad (OQP) protocol, even if the message is inifinitely long (i.e. the number of qubits is infinite, however countable).

Claim ((4)) The OQP protocol and its generic device can be implemented very conveniently by just a single CNOT gate with the control qubit being the looped single key qubit (the subsequent n qubits of the quantum message M would be synchronically fed to target qubit input of this single CNOT gate) and even more importantly the protocol offers just a single key qubit K' to securely manage its secrecy. To decrypt the encrypted (entangled) quantum message it is not even neccessary to reverse the application of the CNOT gate - one only needs to measure the single qubit key and upon the measurement outcome either restore the original quantum message M or negate all qubits of the M register to restore them to their original state (in case of projecting the key qubit to the state —1¿ upon its measurement). No other quantum cryptographic scheme as yet discussed in the existing literature had this property: to decrypt n qubits quantum message by the measurement of just a single qubit (which is due to special symmetry of the involved multi-qubit entanglement).

Claim ((5)) The described invention of OQP is based on a special topology of the multi-qubit (n+1-qubits) entanglement between the single qubit key and n qubits in the quantum message M. This topology can be illustratively described as a non local ring of keys: if the ring is cut then all encrypted message qubits (illustratively small indivudual keys) are freed and decrypted, when the ring is not cut then all message qubits are non-locally bound to the ring (single key qubit) and are themselves illustratively the small keys trapping the original quantum message individual qubits - they are not accessible without the non-local ring (the single key qubit kept private and away from the adversary). Such a topological model of entanglement (however non-symmetrical in contast to e.g. the generalized GHZ states [53]) is claimed to be an important theoretical feature of the proposed invention of the OQP scheme.

Claim ((6)) The OQP invention allows to significantly reduce the number of required pre-shared Bell states qubits for secure communication of the quantum message: in the standard quantum teleportation-only secure communication scheme to securely send n qubits of quantum message Alice is required to share n Bell states with Bob to individually teleport all n qubits of M to Bob (thus also exchanging 2n bits of classical information that will allow Bob to restore the correct original state of M). The QT scheme could be understood as generalized quauntum analog of the classical OTP encryption with the quantum key being the n Bell states (or 2n maximally pairwise entangled qubits). In the case of OQP only one pre-shared Bell state is required to non-locally teleport the key (and thus also 2 bits of classical information) while the encrypted (by the n+1-qubits entanglement with K') M' quantum message can be sent through a standard local quantum channel and still be completely inaccessible to Eve (who cannot decrypt the M' message without the key qubit K').

Claim ((7)) The actual building of the generic device implementing the OQP protocol can be realized on any technological implementation of qubits and their CNOT operations and is currently achievable technologically (there are many successfully implemented qubits and their CNOT gates, cf. e.g. [34–48]). The qubits and CNOT gates are basic components of the OQP device and the invention doesn't depend on particular implementation technology used for quantum information carriers (qubits) and interactions between the qubits carriers (implementing CNOT gates). These can be realized e.g. in the regimes of orbital or spin degrees of freedom in matter or with polarization or phase degrees of freedom of light. It should be stressed that implementation of OQP protocol / device doesn't require universal quantum computation in principle (only the qubits carriers and the CNOT gate technology is required).

Abstract

The One-Qubit Pad (OQP) scheme is the most primitive maximally efficient scheme for encryption of quantum information with a quantum key of just a single qubit in an arbitrary unknown quantum state. The OQP enables encryption of the quantum information of n qubits register with a single qubit key upon provision of a multi-qubit entanglement between the single qubit key and the n qubits of the quantum message by the iterative application of the CNOT gate on the same key qubit (control input) and subsequent qubits of the message (target input). This results in an entanglement of all n+1 qubits, which locks original quantum information qubits and the single qubit of the key in a jointly entangled state that cannot be disentangled without the single qubit key. In order to decrypt the quantum message (by its disentanglement) one needs to have the qubit key and either reverse the protocol (applying CNOT operations in the reversed order) or simply measure the entangled key qubit and then depending on the outcome either straightforwardly obtain the decrypted quantum message or its quantum negation (dealt with by applying quantum negation on all of the message qubits thus restoring their original states). The OQP scheme is a quantum generalization of the One-Time Pad (OTP) scheme. The main differences between two schemes show how much quantum and clasical information differ. It is of course impossible to unconditionally securely encrypt classical sequence of n bits with just 1 bit of a key or guarantee that the random key that can be used for this purpose of n bits length (same as of the message) could not be copied. In contrast both these features are possible for the quantum information encryption as described upon the proposed OQP scheme. The main characteristic of the OQP protocol to use only a single qubit as the key to enable information-theoretic security of n qubits quantum information encryption follows from utilization of a multi-qubit entanglement. The main application of the OQP protocol is to lock (encrypt) quantum information with the single key qubit in order to prevent any unathorized access to it (not only a classical access upon a measurement, but much more importantly unauthorized quantum access by a quantum information processing device, e.g. future quantum computers in quantum networks). This application can be also extended to quantum information communication scenario jointly with the Quantum Teleportation protocol, which without OQP requires pre-sharing of n pairs of Bell states between Alice and Bob to securely communicate n-qubits long quantum message, whereas in contrast with the OQP protocol just one pair of Bell state is required to securely teleport only the single qubit key sufficient for the decryption of the OQP encrypted quantum message, which would could sent through an insecure quantum channel, but still be access-protected from an adversary.

Drawings

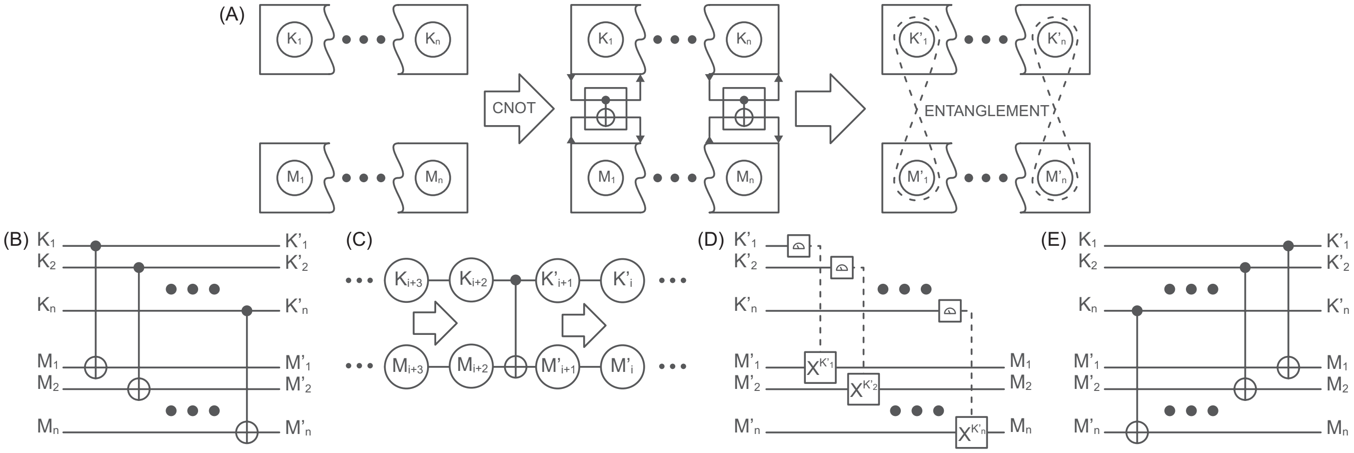

FIG. 1.

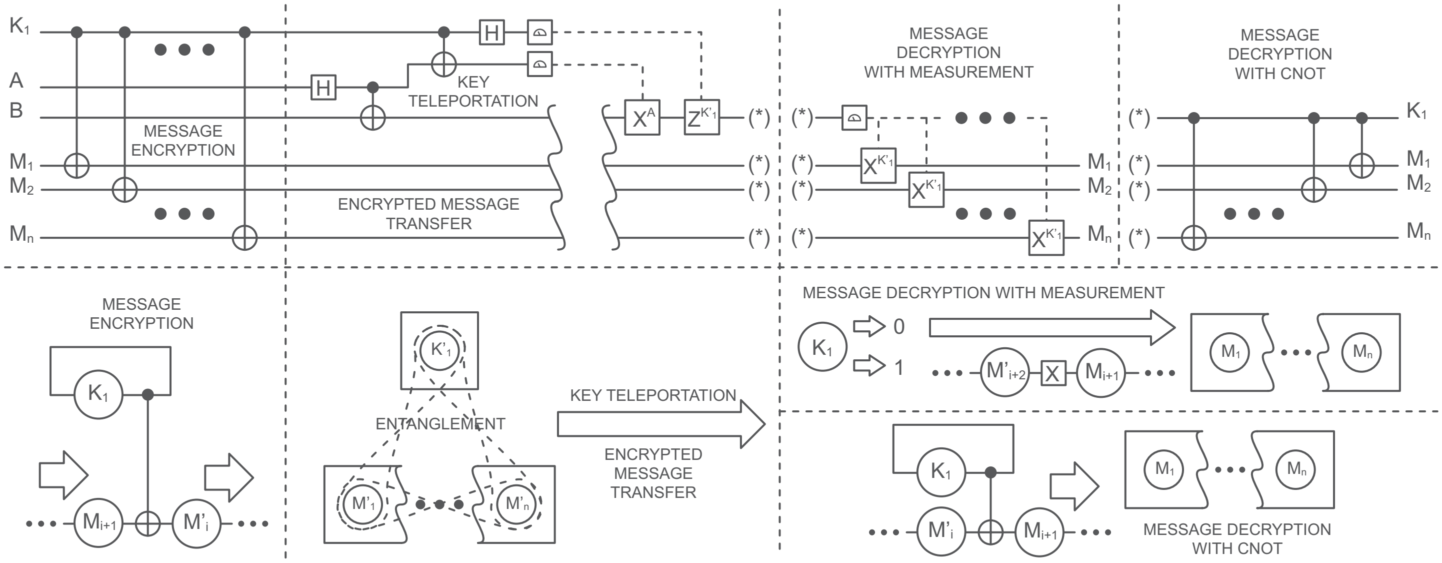
K₁
A
B
M₁
M₂
Mₙ
MESSAGE ENCRYPTION
H
KEY TELEPORTATION
ENCRYPTED MESSAGE TRANSFER
X^A
Z^K'₁
(*)
MESSAGE DECRYPTION WITH MEASUREMENT
X^K'₁
MESSAGE DECRYPTION WITH CNOT
MESSAGE ENCRYPTION
K₁
Mᵢ₊₁
M'ᵢ
K'₁
ENTANGLEMENT
M'₁
M'ₙ
KEY TELEPORTATION
ENCRYPTED MESSAGE TRANSFER
MESSAGE DECRYPTION WITH MEASUREMENT
0
1
M'ᵢ₊₂
X
Mᵢ₊₁
M₁
Mₙ
MESSAGE DECRYPTION WITH CNOT

FIG. 5.