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-PROTOCOL-STD-VER-3.0

Reference Standard for the One Qubit Pad (OQP) protocol (definitions, key theoretical concepts and use cases for qubits encryption)

EITCI INSTITUTE QUANTUM STANDARDS GROUP

EITCI-OQP-QSG

Brussels, 20th January 2024
Version: 3.0

Table of contents

1. Introduction 1
2. The Protocol 2
3. Conclusions 5

The One-Qubit Pad (OQP) – a fundamental quantum information entanglement encryption primitive

The One-Qubit Pad (OQP) scheme is a maximally efficient quantum information encryption primitive. It uses a quantum key of just a single qubit in an arbitrary unknown quantum state enabling encryption of quantum information of n qubits register upon a multi-qubit entanglement between the single qubit key and the n qubits of the quantum message. This entanglement is achieved by an iterative application of the CNOT gate on the same single-qubit key (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 restoring the original quantum message without access to the single-qubit key. In order to decrypt the quantum message by its disentanglement one needs to access the single-qubit key and either reverse the protocol (applying CNOT operations in the reversed order) or measure the entangled key qubit and depending on the outcome either straightforwardly obtain the decrypted quantum message or its quantum negation (dealt with by applying the σ_x gate 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 elucidating how much quantum and clasical information differ. It is of course impossible to securely encrypt classical sequence of n bits with just 1 bit classical key. In contrast it is theoretically possible for the quantum information upon the proposed OQP scheme, with the use of only a single qubit as the key to enable information-theoretic security of n qubits quantum information encryption following from utilization of a multi-qubit entanglement. The main application of the OQP protocol is to encrypt quantum information with the single key qubit in order to prevent any unathorized access (not only a classical access upon a measurement, but 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 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 be securely sent through a standard (local) quantum channel.

I. INTRODUCTION

The OQP scheme enables information-theoretic encryption of quantum information (n-qubits register, M) with only a single-qubit key K. It differs from a straightforward generalization of the classical One-Time Pad (OTP) into the quantum case, in processing sequentially each qubit of the register M with only the single qubit key K upon a CNOT quantum gate (the single qubit key K is looped as a control qubit of the CNOT gate, while subsequent qubits of the quantum message M are target qubits). In first iteration the qubit K will thus entangle with the first qubit of M. In second iteration, when already entangled qubit K is in CNOT with the second qubit of M, the resulting state will be a joint 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-qubit entanglement of all qubits - the single-qubit key K and n-qubits of the quantum message M).

After the OQP entangling encryption the message register M is in a new state M' jointly entangled with the single-qubit key K'. If the key qubit K' is kept by Alice, then there is no way to extract original quantum information from M'. Furthermore due to the no-cloning theorem there cannot exist a copy of the original quantum message (M) and neither of the key (K). The result of OQP providing information-theoretic security of quantum information encryption with just a single qubit key is of a fundamental significance. It is due to the continuously infite information capacity (of cardinal number c) of a single qubit K' that can in fact encrypt (here non-locally in quantum entanglement with M') the quantum information of n-qubits sequence M (along with original information of single qubit key K), even if n is infinite (but discrete with a cardinal number $\aleph_0$).

In order to decrypt (disentangle) the quantum message M from M' using the single-qubit 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. This procedure iterated n times will eventually lead to disentanglement of M' with K' and restoring the quantum message register to state M, while the key qubit to state K.

II. THE PROTOCOL

The protocol's principle of operation is presented in the Fig. 1.

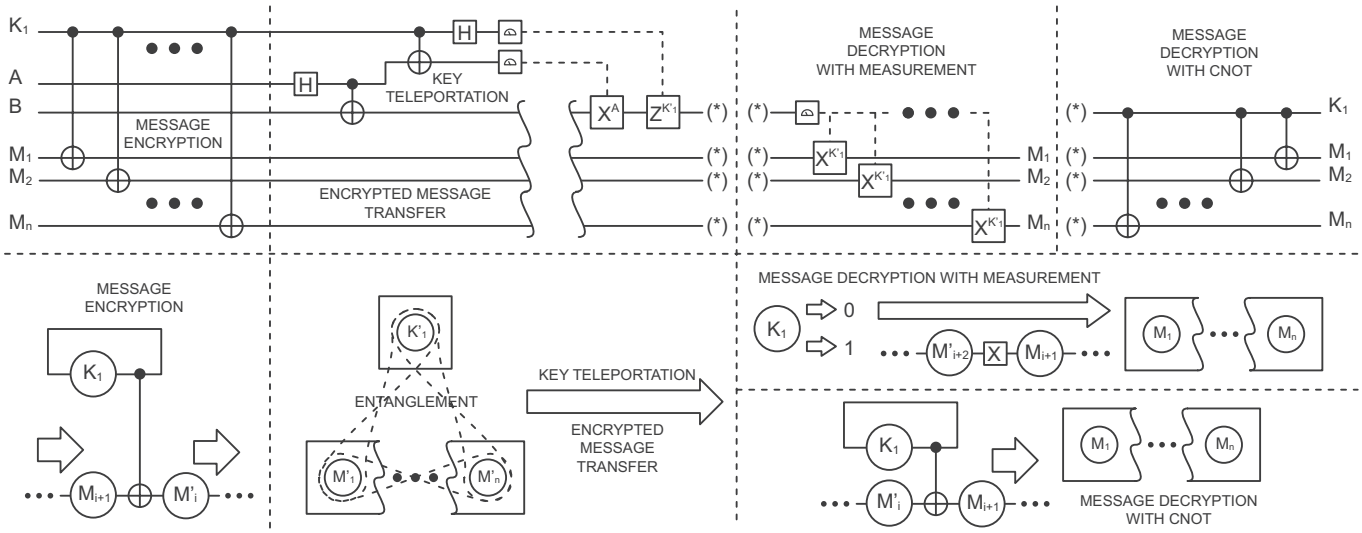

FIG. 1. The OQP scheme operation depicted in terms of logic (bottom part) and quantum circuitry (upper part) for the quantum message encryption and decryption by either CNOT gates reversal or the single-qubit key measurement (extended by an examplary application with Quantum Teleportation). Introducing multi-qubit entanglement by cyclically applying CNOT gate upon the single key qubit K (control qubit) and the subsequent quantum information qubits in M register (target qubits) securely encrypts the latter in a quantum information theoretic sense. The OQP's qualitative difference 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 [1]) is that both the message and the key are quantum information and thus are prohibited to be copied by the no-cloning theorem [2]. In PQC schemes the security is not 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 OQP scheme, due to its operation on a fully quantum single qubit key. On the other hand OQP scheme can be also compared to discussion of the quantum information encryption with quantum keys, as e.g. in [3] for the straightforward generalization of the classical OTP to the quantum case (with n-qubits key encrypting n-qubits quantum message in pairwise entanglement), where OQP has an efficiency edge by reducing the key to a single qubit upon utilization of a generalized multi-qubit entanglement.

Let us first assume that we have a single qubit key K in the state $|K\rangle = a|0\rangle + b|1\rangle$ (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. $|a|^2 + |b|^2 = 1$). 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.

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).

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

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

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). For quantum information (qubits in superpositions of the qubit definition basis $|0\rangle$ and $|1\rangle$) 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).

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:

After the first iteration we have:

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

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

After the second iteration:

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

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.

Then, the third iteration produces the following state:

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

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.

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' (as this is not a pure state anymore, it is not normalized and thus the vector states formalism falls short to be used in representing it and one must resort to the density matrix formalism):

The 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:

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

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

$$\begin{aligned}&\rho_{M'} = \mathrm{Tr}_{K'}\left(\rho_{Z'}\right) = \left\langle 0\right|\rho_{Z'}\left|0\right\rangle + \left\langle 1\right|\rho_{Z'}\left|1\right\rangle = |a|^2\left|\psi_1\right\rangle\left\langle\psi_1\right| + |b|^2\left|\psi_2\right\rangle\left\langle\psi_2\right|\\ &= |a|^2 P_{\psi_1} + |b|^2 P_{\psi_2} = |a|^2\rho_{\psi_1} + |b|^2\rho_{\psi_2} = |a|^2\rho_M + |b|^2\sigma_x^{\otimes n}\rho_M\sigma_x^{\otimes n}\end{aligned} \tag{5}$$

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 $\left|\psi_1\right\rangle$=$\left|M\right\rangle$ and $\left|\psi_2\right\rangle$=$\sigma_x^{\otimes n}\left|M\right\rangle$).

Performing measurement on the 3-qubits of M' or performing any other unitary operation 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 $\{\left|0\right\rangle, \left|1\right\rangle\}$ will first realize the probability of choice of the pure state of 3 qubits in M' (either $|a|^2$ for $\left|\psi_1\right\rangle$ or $|b|^2$ for $\left|\psi_2\right\rangle$) 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.

Furthermore it is easy to notice 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 single-qubit key K', then he will non-locally project with probability $|a|^2$ the 3-qubits state in M' to the $|\psi_1\rangle$ pure state or with probability $|b|^2$ to the $|\psi_2\rangle$ 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 of course means that the measurement of the key qubit K' disentangles 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)

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).

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

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

$$\begin{aligned} &ac|00\rangle + ad|01\rangle + bc|11\rangle + bd|10\rangle * a^*c^*\langle 00| + a^*d^*\langle 01| + b^*c^*\langle 11| + b^*d^*\langle 10| \\ &= aca^*c^*|00\rangle\langle 00| + aca^*d^*|00\rangle\langle 01| + acb^*c^*|00\rangle\langle 11| + acb^*d^*|00\rangle\langle 10| \\ &+ ada^*c^*|01\rangle\langle 00| + ada^*d^*|01\rangle\langle 01| + adb^*c^*|01\rangle\langle 11| + adb^*d^*|01\rangle\langle 10| \\ &+ bca^*c^*|11\rangle\langle 00| + bca^*d^*|11\rangle\langle 01| + bcb^*c^*|11\rangle\langle 11| + bcb^*d^*|11\rangle\langle 10| \\ &+ bda^*c^*|10\rangle\langle 00| + bda^*d^*|10\rangle\langle 01| + bdb^*c^*|10\rangle\langle 11| + bdb^*d^*|10\rangle\langle 10| \end{aligned} \tag{6}$$

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

$$\begin{aligned} &|a|^2|c|^2|0\rangle\langle 0| + |a|^2 cd^*|0\rangle\langle 1| + |a|^2 dc^*|1\rangle\langle 0| + |a|^2|d|^2|1\rangle\langle 1| \\ &+ |b|^2|c|^2|1\rangle\langle 1| + |b|^2 cd^*|1\rangle\langle 0| + |b|^2 dc^*|0\rangle\langle 1| + |b|^2|d|^2|0\rangle\langle 0| \end{aligned} \tag{7}$$

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).

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 require that each qubit in the register M must be quantum negated, i.e. under action of the Pauli σ_x gate, 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 the CNOT operations in a reversed order. 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.

III. CONCLUSIONS

It is puzzling on a first glance that one can use just a single qubit (key K) to unconditionally (quantum information theoretic) 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 even 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 joint entangled state), which means that the essential entanglement information is also shared within M'. However it is crucial that this information is stored non-locally in the entanglement – if one only has the single qubit key K', one can still by just measuring it decrypt the M' to M (by disentangling it with the von Neumann projective measurement of the qubit K'), wherever M' is located (and this will happen instantly as a result of the projection based quantum measurement of K'). 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, in order for the quantum information to be fully recovered).

The main advantage of the OQP protocol is that it uses only a single qubit as the one-qubit key to uncondtionally secure the n-qubits quantum information (quantum message) encrypted with this one-qubit key. At the basis of this scheme is a concept not previously described in the literature that greatly improves theoretical efficiency of quantum information encryption due to the multi-qubit quantum entanglement that can be not only used (as discussed previously, e.g. in [3]) pairwise between the subsequent qubits' positions of the n-qubits quantum key register and the n-qubits quantum message register, but rather more generally, jointly between a single-qubit key and all qubits of the message. This concept provides a qualitative theoretical gain in encryption and is also a most basic quantum information encryption theoretic primitive. How this difference affects secure quantum communication efficiency in e.g. a general scheme of Quantum Teleportation? Normally one needs n pairs of maximally entangled qubits (Bell states) shared between the parties 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 securely, non-locally teleport the single key qubit for the multi-qubit entanglement encrypted message that is meanwhile transmitted in the local unsecure quantum channel.

The proposed scheme is of a theoretical significance as the most simple quantum information encryption primitive (corresponding to a quantum analogue of the classical One-Time Pad, well illustrating the fundamental difference between classical and quantum information). It is not possible to encrypt a classical message of n bits with just a singe-bit key, whereas in quantum information theory it is possible with a single-qubit key, even for arbitrarily long quantum message, due to employing multi-qubit entanglement. The main application of the scheme (in practice certainly limited by the decoherence) is to maximally efficiently secure the quantum information M in order to disallow any potential access to the original n qubits quantum information M by an adversary (scenarios of quantum information encryption gain importance in the advent of quantum computers and quantum networks processing and communicating quantum rather then classical information for distributed quantum computation applications of the future).

The presented results extend on the authors' patent on the One-Qubit Pad from 2017 [4].

[1] 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.

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

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

[4] J. E. Jacak and W. A. Jacak. The One-Qubit Pad (OQP) for entanglement encryption of quantum information, PCT Patent, WO2019132680, World Intellectual Property Organization, 2017.