The One-Qubit Pad (OQP) for entanglement encryption of quantum information

W. Jacak, J. Jacak
Department of Quantum Technologies, Wrocław University of Science and Technology
Wybrzeże Wyspiańskiego 27, 50-370, Wrocław, Poland
CompSecur sp. z o.o. ul. Piłsudskiego 74, 52-020, Wrocław, Poland

The One-Qubit Pad (OQP) protocol is proposed as a maximally efficient scheme for encryption of quantum information with a quantum key consisting of just a single qubit in an arbitrary unknown quantum state. The OQP enables encryption of quantum information of n qubits register (quantum message) with a single qubit key upon introducing a multi-qubit entanglement between the single qubit of the key and the n qubits of the quantum register by an iterative application of the CNOT gate, always with the same key qubit (control qubit) and subsequent qubits of the quantum register (target qubits). This results in an entanglement of all n+1 qubits (cf. figure below), which non-locally locks original quantum information of the message qubits with the single qubit of the key in a joint, multi-qubit entangled state that cannot be disentangled recovering original quantum information of the message qubits without access to the single qubit key. In order to decrypt quantum register (recover original states of n message qubits) 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 depending on the binary projection outcome either straightforwardly recover the decrypted quantum message or its quantum negation (then dealt with by applying quantum negation subsequently on all of the message qubits thus restoring their original states).

The OQP protocol is proposed and discussed as a quantum generalization of the One-Time Pad (the Shannon proven information-theoretic secure classical encryption scheme based on the Vernam cipher). The paper analyzes the properties of the OQP protocol pronouncing the differences between the two schemes to show how significantly quantum and classical information differ in this context. 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 properties of multi-qubit entanglement, a non-local quantum resource of topological nature. The main application of the OQP protocol and its technologically achievable implementation is to encrypt (or lock) quantum information with the single key qubit in order to prevent any unauthorized access to its original state (both in classical and quantum terms). The protocol can be also applied to communication scenario jointly with the Quantum Teleportation, which without OQP requires pre-sharing of n pairs of qubits in Bell states between Alice and Bob to securely communicate n qubits long quantum message, whereas in contrast with the OQP protocol just one pair on qubits in a Bell state is required to securely teleport only the single qubit key for the OQP encrypted quantum message that could be sent through an insecure quantum channel and still be access-protected from an adversary.

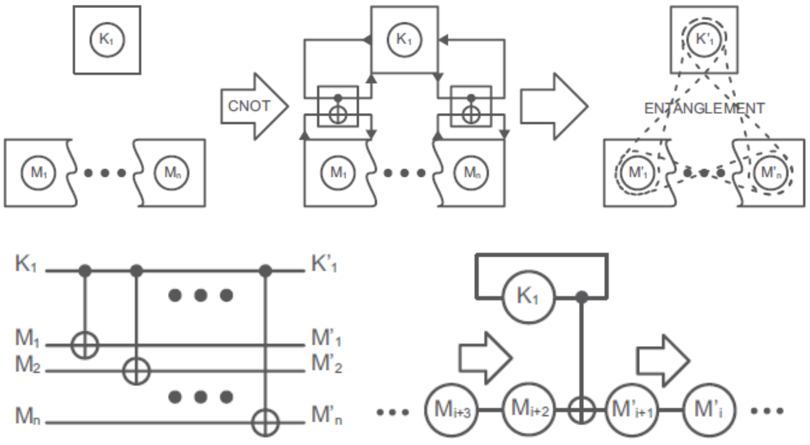

Fig. 1. Principle of the OQP protocol operation and its quantum circuits implementation