

A Theoretic-framework for Quantum Steganography

M. Dobší ek, J. Kolá , R. Lórencz

dobsicm@fel.cvut.cz

Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University, Technická 2, 166 27 Prague 6, Czech Republic

Quantum information processing has proved to be a fruitful tool in several advanced cryptographic tasks. For example quantum key distribution establishes a string of random bits shared by two spatially separated parties in an information-theoretically secure manner. Classical solutions for this problem offer only computational security. Beyond quantum key distribution there are other promising directions of research such as quantum secret sharing, quantum data hiding, authentication of quantum messages and quantum steganography, to name a few of them. It is important to note that while in classical theory the terms 'data hiding' and 'steganography' are interchangeable, in quantum theory they have different meaning. Quantum data hiding is rather closer to secret sharing.

Our research during the last year focused on quantum steganography. By this term we refer to methods of hidden communication within framework of quantum mechanics. Similar to classical steganography, hidden communication is done via embedding a message into a redundant part of a cover medium.

Embedding methods differ significantly in the medium access level. The main levels are 1) quantum noise, 2) error correcting codes and 3) data formats, protocols, etc. Quantum noise level is not much about theory of information in the sense of entropy but it is a clean race in the technology available to the steganographer and steganalyst. To put it more to the context, let us take a look at the first commercially available products for quantum key distribution. For these tools to work as securely as proposed by the theory the single photon emitters and detectors are crucial. Nevertheless, usable single photon sources are often substituted with industry-standard weak coherent pulse approach. Whilst practical, this approach suffers from non-zero probability of multiple-photons events. Apart from the introduced security loophole, these extra photons can be used for steganographic purposes while legitimate key distribution seems to happen.

On the level of quantum error correcting codes (QECC) the situation is very similar. First steps along this line were accomplished by J. Gea-Banaclóche in [1]. He proposed to encode the message to be hidden into the error syndrome. When compared to the classical counterpart, the QECC scheme has a greater capacity for such purposes. This is due to the fact that quantum errors are continuous and a bunch of extra qubits is needed to preserve the desired quantum state. For example, the Shor code is a [9,1,3]-QECC. On the other hand, QECC- based embedding techniques are not suitable for steganography in the sense of communication but rather for watermarking tasks. To let the QECC work correctly most of the time it is needed to remove the deliberately inserted errors before the ordinary correcting stage takes place otherwise the data could be corrupted. Of course, such an error-based watermark can be removed only by a person who knows the mark exactly, i.e. instead of an unknown communicated message only a yes/no-kind of copyright statement is delivered. Interesting results arise from data authentication perspective. In order to tie up the mark with the data properly the mark has to have a form of superposition (linear combination) of basic errors, e.g. of bit-flip and phase-flip error.

M. Dobšíek studied the connection with authentication schemes of quantum messages in more depth. He analyzed a scheme proposed by M. Curty et al. in [2] and concluded that the data and the authenticating tag have to be tied using an entangling unitary operation, see [3] for more details. In a subtle way this coincides with the demand for 'superposition of errors'.

Finally, embedding messages at the level of data format is expected to be the most widely used in the future. In digital data formats, tens of methods are known that exploit redundancy in JPEG images, MP3 music files, binary executable files and so on. However, there are no such formats in quantum domain by this time. It is too early to predict how and when will the technology reach this stage. Generally speaking, we distinguish quantum steganography without entanglement and with entanglement independently of the format.

Consider the following situation using the least significant bit technique. We have a digital information and deliver this information quantum-mechanically. It is the most expected scenario – classical enduser interface accompanied with quantum coprocessor and broadcasting quantum channel. Two parties who want to establish a steganographic channel agree on a non-standard base encoding and measurement on the qubits which correspond to least significant bits. Other parties who are not aware of this deal treat all qubits in a standard base. In consequence, these parties may obtain wrong classical bit values but due to their low significance they can hardly detect it. Additionally, once the qubit carrying hidden information is collapsed by a measurement, no later leakage of the stego key used for encoding enables to obtain that past hidden information. There is no classical analogue for this pretty striking property. Of course, the difficult part for the steganographer is to properly select positions of bits which are the least significant.

Regarding the quantum steganography with entanglement it is possible to use schemes which are based on superdense coding. Basically, an EPR-pair is being shared and an unitary transform applied by one party to its particle is immediately projected to the state of the particle of the other party. The first qubit is then sent off and joint measurement on both of them reveals the applied operation and in turn the communicated bit value. Another interesting possibility is to entangle own particles with a quantum machine in some corporation and see if it is possible to either retrieve 'secret' information from that corporation in an unobtrusive way or upload information (e.g. a virus code) if we go really far with imagination, in the same way.

To conclude, we have identified the basic framework for quantum steganography, recognized the usual elements such as superdense coding/teleportation and encoding to non-orthogonal quantum states, which are used through quantum cryptography, and pointed out few interesting questions.

References:

- [1] GEA-BANACLOCHE, J.: *Hiding messages in quantum data*. Journal of Mathematical Physics, 2002, Vol. 43, No. 9, 4531-4536.
- [2] CURTY, M., SANTOS, D. J., PÉREZ E., GARCÍA-FERNÁNDEZ P.: *Qubit authentication*. Physical Review A 66, 2001, 022301.
- [3] DOBŠÍEK, M.: *Simulation on Quantum Authentication*. To appear in the journal Physics of Particles and Nuclei, Letters, 2006.

This research has been supported by CTU grant No. CTU0507213.