NAME: Amir Kalev
AFFIL: Center for Quantum Information and Control (CQuIC)
TITLE: Encoding secret information in measurement settings
REF: Int. J. Quantum Inf. 12, 1450016 (2014)

Secure quantum communication protocols are often formulated in a paradigm where quantum states are used to encode the message alphabet whereas measurements are designed to extract the secure information. In this work, we propose a rather unexplored framework in which the secure message is encoded in measurement settings rather than in quantum states. In particular, we study two secure variants of a primitive proposed in [1] in which the disturbance induced by a nonselective measurement of mutually unbiased bases (MUB) can be used to establish a communication channel.

In this primitive, the two communicating parties, Alice and Bob, agree beforehand upon a code, associating messages with the parameters specifying MUB. There is no classical communication between Alice and Bob beyond this point. The protocol involves an entangled state shared between Alice and Bob. To communicate a message from the code to Alice, Bob measures his part of the system in the corresponding basis. He must complete the measurement yet may ignore its outcome and then send his measured system to Alice. Now Alice measures the entire system, and deduces, almost always, the message encoded by Bob, and, hence, decodes the message.

While, in classical mechanics, performing a measurement without reading the measurement outcome is equivalent to not exploiting the measurement at all, here we show that the situation is remarkably different when quantum mechanical systems are concerned. A nonselective measurement on one part of a maximally entangled pair can allow secure communication between two parties.

References

[1] A. Kalev, A. Mann and M. Revzen, Phys. Rev Lett. **110** 260502 (2013).