Problem 2. «Studying quantum security»

Problem for a special prize!

Starting from papers of O. Goldreich, Sh. Goldwasser, and S. Micali cryptographers study how to construct random functions. Ok, let the function be random if *it looks random* to adversaries. It is possible to define a *pseudorandom function (PRF) / pseudorandom permutation (PRP)* as a function/permutation with the following property: no efficient classical algorithm, when given oracle access, can distinguish it from a truly random function/permutation.

There are some modern variants of modeling quantum adversaries for ciphers, see the paper M. Kaplan, G. Leurent, A. Leverrier «Quantum Differential and Linear Cryptanalysis» // IACR Transactions on Symmetric Cryptology, Vol. 2016, No. 1, pp. 71–94. DOI: 10.13154/tosc.v2016.i1.71-94. Namely, there are

Standard security: a block cipher is *standard secure* against quantum adversaries if no efficient quantum algorithm can distinguish the block cipher from PRP (or a PRF) by making only *classical* queries (denote this type as Q1).

Quantum security: a block cipher is *quantum secure* against quantum adversaries if no efficient quantum algorithm can distinguish the block cipher from PRP (or a PRF) even by making *quantum* queries (denoted this type as Q2).

The Q2 model of attacks assumes that an adversary can query a quantum cryptographic oracle in superposition. This model can be implemented, when an algorithm under analysis runs on a quantum computer with adequate resources. It is known that most of standardized modes of operation for block ciphers are insecure in the Q2 model. You can read about it for example in the paper M. V. Anand, E. E. Targhi, G. N. Tabia, and D. Unruh «Post-quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation» // Lecture Notes in Computer Science, Vol. 9606, pp. 44-63, 2016. DOI: 10.1007/978-3-319-29360-8_4. This means that such block ciphers modes of operation can be considered broken after appearing a quantum computer with resources enough for implementing an attacked algorithm.

Propose and describe a new (previously unknown) block cipher mode of operation secure in the Q2 model, and justify its security in the Q2 model.