ERIC CULF, University of Waterloo

Coset states in Uncloneable Cryptography

The coset state structure has proven useful on multiple occasions in quantum information, for example in the context of the hidden subgroup problem and stabiliser codes. A basis of coset states exists for every vector subspace of a space of bitstrings, and the elements of the basis are indexed by the coset representatives of the subspace and its orthogonal complement — this provides a large amount of algebraic structure. Recently, Coladangelo, Liu, Liu, and Zhandry [Crypto 2021] introduced a monogamy-of-entanglement (MoE) game based on this structure. We extend this game to construct a variety of uncloneable cryptographic protocols.

First, we show that one of the two cooperating players can learn the other player's answer without significantly affecting the winning probability of the MoE game. This allows to construct a variety of novel cryptographic primitives including a form of uncloneable encryption where decryption uses an interaction between the sender and the receiver, and a stronger form of one-sided device independent quantum key distribution (1S DI QKD) where the receiver's classical device may also be assumed to be untrusted. Our other extension is to show that a comparable MoE property holds for coset states of a wide variety of groups, including infinite-order compact and locally compact abelian groups. This gives rise to an extension of the 1S DI QKD protocol to continuous-variable quantum systems.

This talk is based on joint work with Anne Broadbent (arxiv.org/abs/2303.00048); and with Victor V. Albert and Thomas Vidick (arxiv.org/abs/2212.03935).