“Symbolic Computations and Post-Quantum Cryptography” Online Seminar

Hang Dinh

(Indiana University South Bend)

“Code Equivalence is Hard for Shor-like Quantum Algorithms.”

May 17, 12:00pm (New York Time).

Abstract:

The Code Equivalence problem is that of determining whether two given linear codes are equivalent to each other up to a permutation of the coordinates. This problem is related to the security of McEliece-type cryptosystems in the case where the private code is known to the adversary. While Sendrier's Support Splitting Algorithm (SSA) provides an efficient classical attack in this case for many codes, including the popular case of Goppa codes, there may still be hard instances due to Petrank and Roth's reduction from Graph Isomorphism to Code Equivalence.

On the other hand, Code Equivalence has a direct reduction to a nonabelian hidden subgroup problem (HSP), suggesting a possible quantum algorithm analogous to Shor's algorithms for factoring or discrete log. We will show that in many cases of interest, however, solving this case of the HSP requires rich, entangled measurements. Thus, solving these cases of Code Equivalence appears to be out of reach of current families of quantum algorithms. Our results apply to a fairly broad family of codes, including both Goppa codes and Reed-Muller codes, the latter of which are used in the Sidelnikov cryptosystem and give difficult instances for the SSA.

Our results suggest that "Shor-like" algorithms --- i.e., algorithms based on measurements of a coset state --- are unlikely to help break code-based cryptosystems. While most such systems have classical weaknesses when the private code is known, we hope that these results will strengthen the case that these systems are candidates for post-quantum cryptography.

This is joint work with Alexander Russell and Cristopher Moore.

Algebraic Cryptography Center