Abstract

Multilinear maps are known to have numerous applications to cryptography. Unfortunately, current proposals for multilinear maps suffer from major security vulnerabilities due to a class of attacks known as zeroizing attacks. These attacks have broken many of the desired applications. In this talk, I will outline how these attacks work, and then explain how to use weakened multilinear maps securely for applications, neutralizing the threat of zeroizing attacks. In particular, we show how to build indistinguishability obfuscation, which can be used to build most of cryptography. We also give a direct construction of multiparty non-interactive key exchange. We formally prove that our constructions are secure against zeroizing attacks.

* Based on joint work with Sanjam Garg, Fermi Ma, Eric Miles, Pratyay Mukherjee, Amit Sahai, and Akshayaram Srinivasan