A Practical Post-Quantum Signature: NOVA

Yen-Liang Kuan
Department of Applied Mathematics
National Dong Hwa University

Abstract

A universal quantum computer attack could break classical public key cryptography using Shor's algorithm. Therefore we need new public-key cryptosystems that can resist quantum computing. In this talk, we will talk about a new signature scheme which is a noncommutative ring based unbalanced oil and vinegar signature scheme with key-randomness alignment: NOVA (Noncommutative Oil and Vinegar with Alignment). This is a joint work with L.-C. Wang, P.-E. Tseng and C.-Y. Chou.