NTRU Prime -- reducing attack surface at low cost

Tanja Lange
University of Eindhoven, NL

Abstract :

Several ideal-lattice-based cryptosystems have been broken by recent attacks that exploit special structures of the rings used in those cryptosystems. The same structures are also used in the leading proposals for post-quantum lattice-based cryptography, including the classic NTRU cryptosystem and typical Ring-LWE-based cryptosystems.

This talk presents our proposal NTRU Prime, which tweaks NTRU to use rings without these structures; explains the Streamlined NTRU Prime system, a public-key cryptosystem optimized from an implementation perspective, subject to the standard design goal of IND-CCA2 security; and covers parameter choices and attacks for Streamlined NTRU Prime.