Speaker: Kazuhiro Ogata

Title: Formal Specification and Verification of Post-quantum Cryptographic Protocols with Proof Scores

Abstract: It is expected that practical-scale quantum computers will emerge in the near future, rendering most public-key cryptosystems insecure due to Shor's algorithm. Consequently, post-quantum cryptographic primitives have been actively studied, and several existing high-level security protocols—such as TLS—have been revised to withstand attackers equipped with practical quantum computers. In this talk, we present two case studies. These studies formally specify post-quantum OpenPGP and post-quantum SSH using CafeOBJ, an algebraic specification language, as observational transition systems (OTSs). We then formally verify that the protocols satisfy certain desired properties using proof scores. In the case of post-quantum SSH, we identified a counterexample that violates the authentication property. We revised the protocol accordingly and formally verified that the updated version satisfies the property.