# Efficient Algorithms for Isogeny Sequences and Their Cryptographic Applications

Katsuyuki Takashima[1]

1) *ITC, Mitsubishi Electric, Japan*

Corresponding Author: Katsuyuki Takashima,
Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

**ABSTRACT**

Cryptosystems using isogenies between supersingular elliptic curves are expected as a quantum-safe candidate, and Diffie-Hellman-type key exchange (SIDH), identification, signatures, and hash function have been studied. We proposed efficient isogeny sequence computations on elliptic curves and genus-2 Jacobians. For post-quantum cryptosystems, sequences of low-degree isogenies are important. Then, I explain our proposals on sequences of 2- and 3-isogenies on elliptic curves and (2,2)- and (3,3)-isogenies on genus-2 Jacobians. I will also show an application of our efficient 2-isogenies computation to Sutherland's supersingularity identification algorithm.