**SCIS 2022** 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

# Quantum-Accessible Security of Stateless Hash-based Signature Schemes

Quan Yuan [*] Mehdi Tibouchi [*†] Masayuki Abe [*†]

**Abstract:** In post-quantum cryptography, hash-based signatures are considered as attractive choices since their security is only based on security notions of hash functions. Most existing stateless hash-based signature schemes are proved to be secure in post-quantum security models, where the adversaries are able to execute quantum computations and query to a signing oracle. Note that the signing oracle is classical but quantum, meaning that an adversary can only query a single message with its classcal state and receive the corresponding signature. In 2013, Boneh and Zhandry proposed a stronger security model, where the signing oracle also permits quantum queries. The security in quantum-accessible security model of hash-based signature schemes is lack of research, especially of stateless ones. In this paper, we reprove the security of stateless hash-based signature schemes and analyze the security level in quantum-accessible security models.

**Keywords:** hash-based signatures, quantum-accessible security, post-quantum cryptography, digital signatures

[*] Kyoto University, Kyoto, JP (yuan.quan.87x@st.kyoto-u.ac.jp)
[†] NTT Laboratories, Tokyo, Japan