# BSKCN and BSAML: Blind Signatures From the Module Lattice and the Asymmetric Module Lattice

**Xiaofan LIU, Wei REN, Kim-Kwang Raymond CHOO**

Frontiers of Computer Science, DOI: 10.1007/s11704-023-2372-x

# Problems & Ideas

- Problems :
  - Classical cryptography assumptions (e.g., integer factoring problem and discrete logarithm problem) are not secure against attacks carried out using quantum computers.
  - Some existing lattice-based blind signature schemes are not secure or efficient enough.
- Ideas: Compared with Crystals-Dilithium, both SKCN and SAML are generally more efficient in terms of computation and bandwidth while achieving the same post-quantum security level. Hence, we propose two interactive lattice-based blind signature schemes based on these two signatures, that is SKCN and SAML, called BSKCN and BSAML.

# Main Contributions

- Contributions:
  - We analyze the properties of blind signature structure and propose two efficient and interactive blind signature schemes which inherit the advantages of SKCN and SAML, named BSKCN and BSAML;
  - We construct complete and specific signature generating processes of these two proposed schemes, interacted between the user and the signer, and set several restart checks to guarantee signatures whether are tampered with or not;
  - We provide extensive analyses of the correctness of our schemes.