OKCN/AKCN/CNKE: A Modular and Systematic Approach to Key Establishment and Public-Key Encryption Based on LWE and Its Variants

- **Principal submitter:** Yunlei Zhao, School of Computer Science, Fudan University, 825 Zhangheng Road, Shanghai 201203, China. Telephone: 86-13564812886; Email: ylzhao@fudan.edu.cn
- **Auxiliary submitters:** Zhengzhong Jin, Boru Gong, Guangye Sui
- **Inventors and developers:** Yunlei Zhao, Zhengzhong Jin, Boru Gong and Guangye Sui
- **Owners:** The same as the submitters
- **Siganture:** Yunlei Zhao , Zhengzhong Jin, Boru Gong, Guangye Sui

Notes:

- We hope the proposals are first considered as KEM mechanisms. In the submission, we focus on ephemeral-only key-establishment/encryption based on LWE and its variants, and its extensions to CCA-secure public-key encryption (PKE) and authenticated key-establishment (AKE) are modular and black-box. We also explicitly present new constructions of CCA-secure PKE and privacy-preserving AKE schemes for considerations and evaluations.
- Our proposal could also serve as a general framework for understanding and evaluating the various proposals of KE/PKE from LWE and its variants.
- Security categories: The security of RLWE (resp., MLWE) based schemes lies in Category-5 (resp., Category-4). The security of LWE/LWR based schemes lies in Category-3.
- We present key establishments from LWE and its variants in a modular and systemized way. With this submission, we focus on the implementations of practical schemes based on RLWE and MLWE. Implementations based on LWE and LWR are available from http://github.com/OKCN
- For all the proposed schemes, the referenced implementation is also the cross-platform optimized implementation.
- Copyright: The documents required in Section 2.D in CFP will be given to NIST at the first PQC Standardization Conference.