The LWE problem is foundational in post-quantum cryptography. While LWE remains theoretically hard even against quantum adversaries, practical vulnerabilities, such as side-channel attacks, can reveal auxiliary information (i.e., hints) that undermines its security. Current methods for solving LWE with hints fall into two categories: lattice reduction, which is effective for error-free hints and requires a small number of them, and probabilistic statistical techniques, which can process erroneous hints but demand a large quantity. However, a general method for handling erroneous hints with a limited number remains lacking.

In this paper, we introduce a combinatorial attack that integrates lattice reduction and probabilistic statistical approaches to address this gap. By combining the strengths of both approaches, our method enables effective key recovery with fewer hints, including erroneous ones. The attack proceeds in three stages: (1) applying probabilistic methods to process hints and generate an approximate secret key; (2) using the approximate key to transform the original LWE instance into a refined variant with corresponding hints; and (3) embedding these refined hints into a DBDD instance (converted to a uSVP problem), which is then solved via lattice reduction to recover the secret key.

We validate our attack on LWE instances with diverse hint types and demonstrate that it outperforms lattice reduction or probabilistic statistics alone. Our approach also improves existing attacks, reducing the required BKZ block size for key recovery by 16 in a decryption failure attack on Kyber512.