www.firstlight.cn
北京雷速科技有限公司

返回首页

Better Key Sizes (and Attacks) for LWE-Based Encryption

http://www.firstlight.cn　2010-11-30

We analyze the concrete security and key sizes of theoretically sound lattice-based encryption schemes based on the ``learning with errors'' (LWE) problem. Our main contributions are: (1)~a new lattice attack on LWE that combines basis reduction with an enumeration algorithm admitting a time/success tradeoff, which performs better than the simple distinguishing attack considered in prior analyses; (2)~concrete parameters and security estimates for an LWE-based cryptosystem that is more compact and efficient than the well-known schemes from the literature. Our new key sizes are up to 10 times smaller than prior examples, while providing even stronger concrete security levels.

存档文本