

Implementing Practical Provably Secure Authenticated Key Exchange for the Post-quantum World

University of Cincinnati



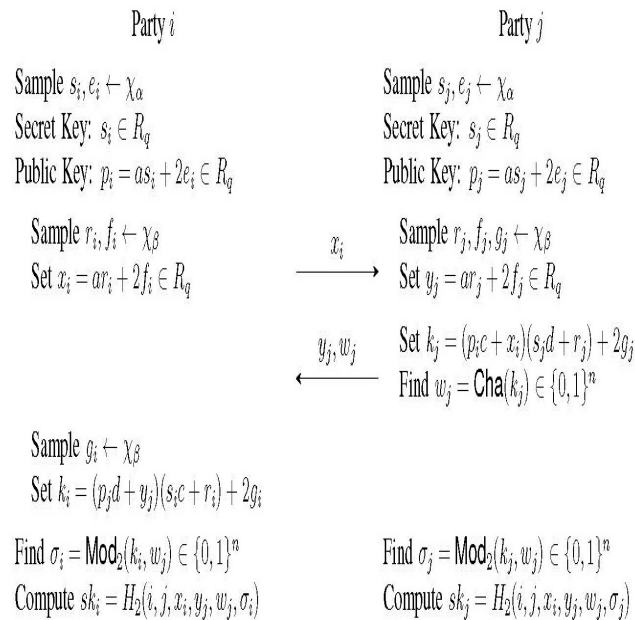
Challenge:

- How to make LWE-based authenticated key exchange more efficient and more secure for practical applications

Solution:

- Find better parameters
- Build new type of protocol to improve the security and performance

The LWE-BASED AKE SCHEME



Scientific Impact:

- Better understanding the fundamentals of LWE-based AKE
- Build next generation quantum resistant algorithm for authenticated key exchange

Broader Impact:

- These new algorithms can be strong candidate for NIST standards
- Can be used to improve greatly Cyber security in communication systems like Internet
- Practical broad applications like SSL/TLS
- Excellent tool to attract student to STEM program
- Train graduate students and bring frontier research into graduate education new knowledge

Project info:

Award #1565748

Jintai Ding