Implementing Post-Quantum AKE

Jintai Ding -- University of Cincinnati
www.quantumproof.org
Jintai.Ding@gmail.com

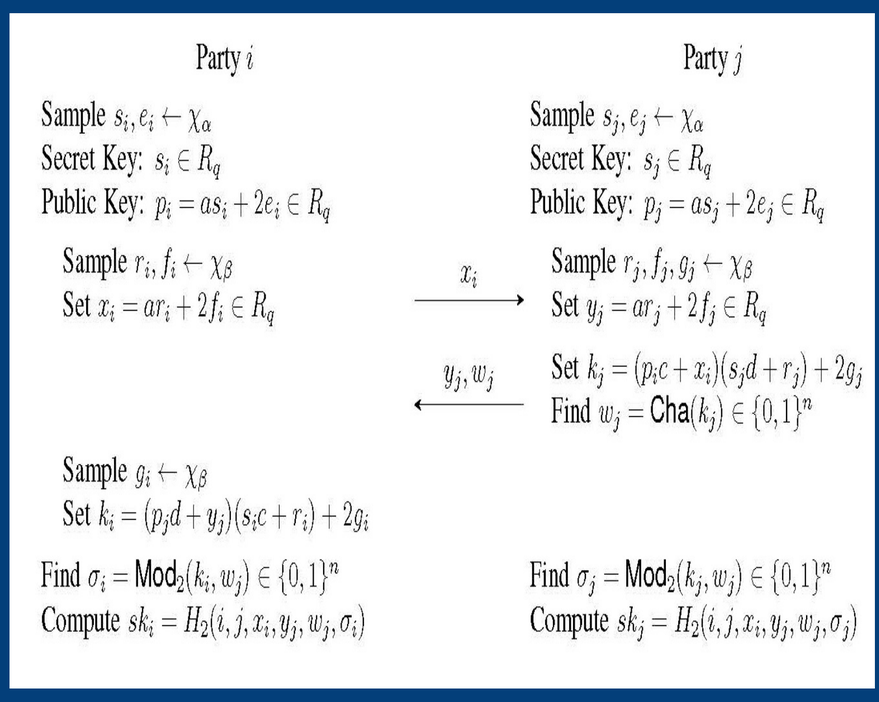
The Objective

The objective of this project is to make LWE-based authenticated key exchange more efficient and more secure for practical applications

Authenticated Key Exchanges play fundamental roles in our communication systems.
Internet Security relies on AKE in SSL/TLS

NSA announced plan to migrate to quantum resistant algorithm in 2015

NIST announced call for proposals for next generation quantum resistant algorithm with a deadline of November 2017



Approach

- To find better parameters for AKEs
- To find new type of implementations
- To design new protocols to be more efficient and more secure
- To make the system more resilient

We have developed new type of simpler and more efficient protocols but still need to work on security proofs

Building a new password-based LWE key exchange

(CT-RSA 2017)

Developing complete attack on key reuse for LWE-based key exchange

Developing new techniques to build resilient LWE-based KE

Finding new type of LWE-like problems to build more efficient protocols with better parameters

Interested in meeting the PIs? Attach post-it note below!