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

Party i		Party j
Sample $s_i, e_i \leftarrow \chi_\alpha$ Secret Key: $s_i \in R_q$ Public Key: $p_i = as_i + 2e_i \in R_q$		Sample $s_j, e_j \leftarrow \chi_\alpha$ Secret Key: $s_j \in R_q$ Public Key: $p_j = as_j + 2e_j \in R_q$
Sample $r_i, f_i \leftarrow \chi_\beta$ Set $x_i = ar_i + 2f_i \in R_q$	$\xrightarrow{x_i}$	Sample $r_j, f_j, g_j \leftarrow \chi_\beta$ Set $y_j = ar_j + 2f_j \in R_q$
	$\xleftarrow{y_j, w_j}$	Set $k_j = (p_i c + x_i)(s_j d + r_j) + 2g_j$ Find $w_j = \mathsf{Cha}(k_j) \in \{0,1\}^n$
Sample $g_i \leftarrow \chi_\beta$ Set $k_i = (p_j d + y_j)(s_i c + r_i) + 2g_i$		
Find $\sigma_i = \mathsf{Mod}_2(k_i, w_j) \in \{0,1\}^n$ Compute $sk_i = H_2(i, j, x_i, y_j, w_j, \sigma_i)$		Find $\sigma_j = \mathsf{Mod}_2(k_j, w_j) \in \{0,1\}^n$ Compute $sk_j = H_2(i, j, x_i, y_j, w_j, \sigma_j)$

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 cab 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