The Department of Mathematical Sciences
Colloquium

Dr. Saed Alsayigh

Tenure-Track Candidate

Tuesday, February 28, 2017
Rm 119 WCharlton Hall
4 – 5 pm

Provably Secure PAKE Based on RLWE

The talk will give a historical introduction to KE protocols and why they are important. I also will give introduction about the post quantum cryptography and why it is important. Then I'm going to show how do we construct our PAK protocol and give a brief idea about its proof of security. Finally, I'll give some applications that where our protocol can be used in.

Refreshments will be served 3 – 3:45 pm in the Faculty & Graduate Student Lounge
Rm 4118 French Hall West

UNIVERSITY OF Cincinnati