Abstract:
Fully homomorphic encryption (FHE) is a kind of (public key) encryption scheme that allows anyone to perform arbitrary operations on plain-texts via certain special operations on the corresponding ciphertexts. In 2008, Ostrovsky and Skeith III suggested an approach towards achieving FHE from group-theoretic viewpoint, but no observations on how to actually construct FHE based on their approach have been given so far. In this talk, I explain my recent work based on this approach, which is still incomplete but would show several potential, interesting connections between group theory and cryptography.