BIANCA SOSNOVSKI, Queensborough Community College/The City University of New York
Applications of Finite Fields in Cayley Hash Functions

Cayley hash functions are a class of cryptographic hashing algorithms that employ group-theoretic constructions based on Cayley graphs to achieve security and efficiency. This presentation explores the role of finite fields within Cayley hash functions, illustrating how finite field structures enable efficient encoding and provide a robust defense against conventional cryptographic attacks. We will examine specific examples of Cayley hash functions, analyze their constructions using various groups and finite fields, and discuss the key properties and trade-offs associated with different types of Cayley hash functions.