Department of MATHEMATICS and COMPUTER SCIENCE

JOHN JAY COLLEGE OF CRIMINAL JUSTICE

Women in Tech and CS Seminar Series

When: April 16
Time: 1:40 – 2:45 pm
Location: 6.67 NB

"Computing Multiple Exponentiations in Discrete Log and RSA Groups: From Batch Verification to Batch Delegation"

Matluba Khodjaeva, John Jay College of Criminal Justice

Abstract

"We consider the problem of a client efficiently, privately and securely delegating the computation of multiple group exponentiations to a computationally more powerful server (e.g. a cloud server). We provide the first practical and provable solutions to this batch delegation problem for groups commonly used in cryptography, based on discrete logarithm and RSA hardness assumptions. Previous results either solved delegation of a single group exponentiation with limited security properties, or verification of multiple group exponentiations in prime-order groups (not applicable to RSA) and under certain simplifying assumptions on the exponentiation values (not applicable to some discrete logarithm groups). Our results directly solve batch delegation of various algorithms in cryptosystems, including RSA encryption and Diffie-Hellman key agreement protocols."

Biosketch

MATLUBA KHODJAEVA is a tenure track assistant professor in computer science and mathematics at the City University of New York, John Jay College. She finished her PhD in Computer Science at The Graduate Center CUNY (September 2017) under supervision of Professor D. Kahrobaei. Her research interest is in cryptography, it mainly concerns in the area of securely outsourcing computations to the cloud. My PhD thesis is on "Secure and Efficient Delegation of a Single and Multiple Exponentiations to a Single Malicious Server"

WiTNY

CENTER FOR CYBERCRIME STUDIES