JOHN JAY COLLEGE OF CRIMINAL JUSTICE

The Math & CS Dept. and
Center for Cybercrime Studies
Present

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

Matluba Khodjaeva

CUNY Graduate Center

Ph.D. Program in Computer Science

Date: Wednesday, Jan. 10, 2018
Time: 11:30 – 12:15
Math & CS Dept. Conference Room, 6.63.37

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) where solutions depended on 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 protocol