1139-68-476   **Giovanni Di Crescenzo** (`gdicrescenzo@vencorelabs.com`), **Matluba Khodjaeva***
(`mkhodjaeva@jjay.cuny.edu`), **Delaram Kahrobaei** (`dkahrobaei@gc.cuny.edu`) and **Vladimir
Shpilrain** (`shpil@groups.sci.ccny.cuny.edu`). *Computing Multiple Exponentiations in Discrete
Log and RSA Groups: From Batch Verification to Batch Delegation.*

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. (Received February 19, 2018)