On the Minimal Logarithmic Signature Conjecture for Simple Groups of Lie Type

Spyros Magliveras, Nidhi Singhi* and Nikhil Singhi
Department of Mathematics Sciences, Florida Atlantic University
Boca Raton, FL 33431-0991
nsinghi1@fau.edu

An ordered tuple $[A_1, A_2, \ldots, A_n]$ of ordered subsets of a finite group G is said to be a logarithmic signature (LS) for G, if for each $x \in G$, there exist unique $x_i \in A_i, 1 \leq i \leq n$ such that $x = x_1 x_2 \cdots x_n$. Logarithmic signatures provide several efficient ways to create cryptosystems. The well known minimal logarithmic signature conjecture (MLS conjecture) states that for every finite simple group G there is an optimal logarithmic signature, i.e. an LS of the form $[A_1, A_2, \ldots A_n]$, where each A_i is of size prime or 4. Known results so far imply that an MLS exists for solvable, symmetric, alternating groups and all groups of order $\leq 10^{10}$ with few exceptions. It is also known that MLS's exist for $PSL_n(q)$ when $gcd(n, q-1) = 1,\ 4$ or a prime, q a power of a prime. In this talk, the authors develop some new methods for creating such factorizations for the finite groups of Lie type. The methods use the relationship of these groups with the corresponding reductive algebraic groups over algebraically closed fields. In particular, the structure of unipotent and parabolic subgroups and Singer cycles of projective space are used. The logarithmic signatures so obtained will be algorithmically efficient because cyclic subgroups are used to define them. As an application of these methods it is shown that the MLS conjecture is true for $PSL_n(q)$ for all n and q. The applications to other families of classical groups and twisted groups of Lie type will also be discussed.