Non-abelian cryptography

Spyros S. Magliveras, Florida Atlantic University

Contrary to a widely held opinion, the advent of cryptographic primitives based on non-abelian groups is not a recent event. However, new results and publications on such primitives have been accelerated since P. Shor's quantum algorithms for integer factorization and the classical discrete logarithm problem. In this talk we present i) group factorizations, and ii) discrete logarithms for arbitrary finite groups. For group factorizations, the notions of *logarithmic signatures*, and *covers* will be reviewed, along with some of the existent theory, and proposed systems like MST_1, MST_2, and MST_3. For ii) we present a natural generalization of the notion of *discrete logarithm*, and related *discrete logarithm problem* to arbitrary finitely presented groups, but restrict our examples to finite groups. We discuss an insecure example, as well as examples we strongly believe to be secure. It is not surprising that the intractability (or otherwise) of the general DLP is intimately connected with the particular representation of the group, and further related to group presentations. We exhibit some results related to the distributional characteristics of elemens α^x in the group G, where $G = \langle \alpha_1, \ldots, \alpha_t \rangle$, $\alpha = (\alpha_1, \ldots, \alpha_t)$, and α^x is defined appropriately for $x \in \mathbb{Z}$. Open problems will be discussed.