

# *Discrete Logarithms in non-Abelian Groups*

**Ivana Ilic\* and Spyros Magliveras**

*Department of Mathematical Sciences, Florida Atlantic University*

*Boca Raton, FL 33431*

*{iilic, spyros}@fau.edu*

The intractability of the traditional discrete logarithm problem (DLP) forms the basis for the design of numerous cryptographic primitives. M. Sramka et al. have generalized the DLP to arbitrary finite groups. One of the reasons mentioned for this generalization is P. Shor's quantum algorithm which solves efficiently the traditional DLP. The DLP for a non-abelian group is based on a particular representation of the group and a choice of generators.

In this talk we show that care must be taken to insure that the representation and generators indeed yield an intractable DLP. We show that in  $PSL(2, p) = \langle \alpha, \beta \rangle$  the discrete logarithm problem with respect to  $(\alpha, \beta)$  is easy to solve for a specific representation and choice of generators  $\alpha$  and  $\beta$ . As a consequence, such representation of  $PSL(2, p)$  and generators should not be used to design cryptographic primitives.

We also comment on secure choices in the context of  $PSL(2, p)$ .