1046-94-503 **Dima Grigoriev**, Institut de Recherche Mathématique, Campus de Beaulieu, 35042 Rennes, France, and **Vladimir Shpilrain*** (shpil@groups.sci.ccny.cuny.edu), The City College of New York, New York, NY 10031. *Authentication schemes.*

In the first part of the talk, we will describe a couple of general ways of constructing Feige-Fiat-Shamir-like authentication schemes from actions of a semigroup on a set, without exploiting any specific algebraic properties of the set acted upon. Then we will give several concrete realizations of this general idea, and in particular, describe several authentication schemes where both forgery (a.k.a. impersonation) and recovering the prover's long-term private key are NP-hard. Computationally hard problems that can be employed in these realizations include Graph Homomorphism, Graph Colorability, Diophantine Problem, and many others.

In the second part of the talk, we will describe an authentication scheme, based on an altogether different idea, where forgery is apparently infeasible without finding the prover's long-term private key. (Received September 05, 2008)