

1129-00-175

Ramón Flores and **Delaram Kahrobaei*** (dkharobaiei@gc.cuny.edu), PhD Program in Computer Science, CUNY Graduate Center, The City University of New York, 365 Fifth Av, New York, NY 10016. *Cryptography with right-angled Artin groups*. Preliminary report.

In this paper we propose right-angled Artin groups as a platform for secret sharing schemes based on the efficiency (linear time) of the word problem. Inspired by previous work of Grigoriev-Shpilrain in the context of graphs, we define two new problems: Subgroup Isomorphism Problem and Group Homomorphism Problem. Based on them, we also propose two new authentication schemes. For right-angled Artin groups, the Group Homomorphism and Graph Homomorphism problems are equivalent, and the later is known to be NP-complete. In the case of the Subgroup Isomorphism problem, we bring some results due to Bridson who shows there are right-angled Artin groups in which this problem is unsolvable. (Received March 14, 2017)