

1071-20-117

Delaram Kahrobaei, NY, **Charalambos Koupparis*** (ckoupparis@gc.cuny.edu), NY , and **Vladimir Shpilrain**, NY. *Public Key Exchange Using Matrices Over Group Rings.*

We propose to look at the Diffie-Hellman key exchange protocol using matrices over group rings. In order to determine the validity and security of this scheme the Decision Diffie-Hellman (DDH) and Computational Diffie-Hellman (CDH) problems will be addressed. We will be working with matrices defined over group rings $\mathbb{Z}_m[S_n]$, and specifically $\mathbb{Z}_2[S_5]$. (Received February 27, 2011)