KENZA GUENDA, University of Victoria
A Secure New Variant of the McEliece Cryptosystem

In this work joined with H. Mofek and T.A Gulliver we will be presenting a new version of the McEliece cryptosystem based on quasi-cyclic (QC) low density parity check (LDPC) codes and QC moderate density parity check (MDPC) codes. A modified self-shrinking generator is used to obtain random bits which are utilized in the cryptosystem. It is shown that this system is secure against the known attacks.