INTRODUCTION TO MCNIE, A CODE-BASED PUBLIC KEY ENCRYPTION SCHEME

Jon-Lark Kim [1] Young-Sik KimE [2] Lucky Galvez [3] Myeong Jae Kim [4] and Nari Lee [5]

1) *Department of Mathematics, Sogang University, Seoul 04107, KOREA*

2) *Department of Information and Communication Engineering, Chosun University, Gwangju 61452, KOREA*

3) *Department of Mathematics, Sogang University, Seoul 04107, KOREA*

4) *Department of Mathematics, Sogang University, Seoul 04107, KOREA*

5) *Department of Mathematics, Sogang University, Seoul 04107, KOREA*

Corresponding Author : Jon-Lark Kim, jlkim@sogang.ac.kr

ABSTRACT

McNie is a code-based public key encryption scheme submitted to the first Post Quantum Cryptography standardization conference arranged by NIST as a candidate for Post Quantum Cryptography. In this talk, we introduce Low Rank Parity Check(LRPC) codes. Then we describe the algorithm of McNie and compare our parameters with known parameters.