1147-94-564 **Jon-Lark Kim*** (ctryggoggo1@gmail.com), Department of Math, Building R 1401, Sogang University, Seoul, 04107, South Korea, and **Young-Sik Kim**, **Lucky Galvez** and **Myeong Jae Kim**. *A new code-based cryptosystem as an application of McNie with Gabidulin codes.*

McNie is a code-based public key encryption scheme submitted as a candidate to the NIST Post-Quantum Cryptography standardization. It combines the McEliece and Niederreiter public key cryptosystem. In this talk, we present McNie2-Gabidulin which is a modified version of McNie. By using Gabidulin codes, we eliminate the decoding failure, which is one of the limitations of the McNie public key cryptosystem that uses Low Rank Parity Check codes. We prove that this new cryptosystem is IND-CPA secure. Suggested parameters are also given which provides lowest key sizes compared to currently known code based cryptosystems with zero decryption failure probability. (Received January 26, 2019)