誤り訂正符号と離散数学およびそれらの応用

教授 ・ 城本　啓介

大学院先端科学研究部 (工学系) 応用数理・データ解析分野

研究内容

●誤り訂正符号とその応用

雑音のある通信路を通して情報を送受信する場合(Figure 1)において、誤りを正しく訂正するためには、様々な数学的な性質を満たす符号が必要とされる。そこで、与えられたパラメータや性質を満たすような符号の存在問題や構成問題について研究している。特に、近年はネットワーク符号化等への応用が期待されている階数 行列 符号について、その構成法や他分野との境界問題について研究を進めている。

●離散数学とその応用

与えられた条件を満たす対象の集まりについて、主にそれらの数理構造の存在問題や構成法およびアルゴリズム的手法について研究を行うのが組合せ論であり、近年ではIoTやAIをはじめとした情報関連分野へ様々な応用が考えられているある。特に、符号を軸に、組合せデザインやマトロイドにおける共通な数理構造について研究することで、耐量子計算機暗号や秘密分散法の構成法に関する応用研究を進めている。

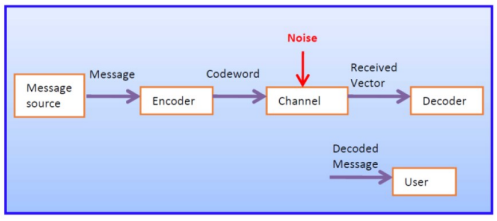

Figure 1 A general digital communication system

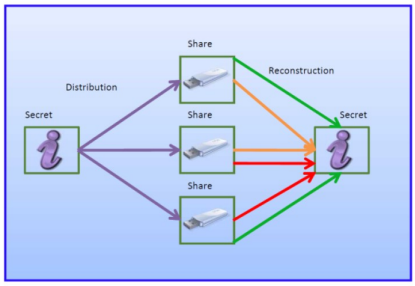

Figure 2 A secret sharing threshold scheme

提供できる技術

誤り訂正符号技術 暗号技術 情報セキュリティ技術

関連リンク

夢ナビ「デジタル情報をノイズから守る 数学の符号理論」

キーワード

誤り訂正符号理論　暗号理論　離散数学

《ご連絡先》　コーディネータ 和田　翼 TEL **096-342-3247** FAX:**096-342-3239** mail:**t-wada@jimu.kumamoto-u.ac.jp**