2020 年度優秀学生表彰受賞者の研究紹介

一関工業高等専門学校
電気情報工学科
佐々木　郁哉

【研究紹介】

この度は優秀学生表彰に選出していただき誠にありがとうございます．受賞に際しましてこれまでご指導いただいた皆様に厚く御礼申し上げます．

私は環準同型暗号に関する研究を行っています．環準同型暗号とは，暗号化したままの状態で加法と乗法の計算が可能な暗号で，クラウドコンピューティングやデータ解析の手法として期待されています．例えばデータ解析では，暗号化していない状態で解析を行うと個人情報が漏洩する危険性がありますが，暗号化状態ではデータの中身が分からないため個人情報を秘匿できます．加法のみ，もしくは乗法のみの計算が可能な暗号は以前から存在していて，RSA 暗号や ElGamal 暗号，Paillier 暗号などが知られていますが，両方の演算の計算ができる環準同型暗号はそれほど多くありません．最近は任意の計算を実行できる完全準同型暗号の研究も進められていますが，公開鍵サイズや計算時間が大きいことから現状では実用性に乏しいという問題があります．そこで本研究では，環準同型暗号の一構成法に基づき，乗法のみの計算が可能である ElGamal 暗号を用いて環準同型暗号を構成しました．また，ElGamal 暗号を応用した方式である modified-ElGamal 暗号，lifted-ElGamal 暗号についても同様に環準同型暗号の構成を行い，lifted-ElGamal 暗号を用いた構成では公開鍵サイズと計算時間が比較的小さいことを示しました．今後は，構成した暗号を実装し検証を行いたいと考えています．

この受賞を糧に，本校専攻科進学後においても電子情報通信分野の勉学に一層熱を入れて取り組む所存です．特に研究では，多くの暗号方式の理解に努め，新たな暗号の構成や実装に取り組んでまいります．最後に，今回の受賞に対して改めて感謝申し上げます．誠にありがとうございました．