특집 머리말

오류정정부호(Error Correcting Codes, ECC)는 약 65년전 Dr. C. E. Shannon이 완벽한 reliability를 가져다 줄 수 있으며 그러한 코드가 실제로 존재한다고 증명한 이후 많은 관심의 대상이었으며, 블록부호와 대수학적 복호방식과 컨벌루션 부호와 비터비 복호방식이 경쟁을 거듭하다가 종국에는 이 둘이 합성되어 많은 성과를 이루었는데, 최근에는 터보 부호와 LDPC 부호의 출현으로 사실상 Shannon이 예견한 코드가 찾아진 상황입니다.

오류정정부호는 시기를 막론하고 항상 차세대 통신시스템의 근간을 이루고 있지만, 오늘날 오류정정부호는 통신 채널의 reliability 뿐만 아니라 너무도 다양한 분야에서 응용되고 있습니다. 이번 호에는 이러한 다양한 분야를 간략히 소개하는 여섯 편의 논문을 모았습니다.

첫째 논문 "분산 저장 시스템을 위한 부분접속 복구부호"는 Big Data 시대에 다양한 저장 장치의 reliability를 높이는 방법에 관한 내용이며, 오래전 연구되었던 블록부호이론의 많은 부분을 사용합니다만, 적은 양의 패리티를 사용하여 빠르고 간단하게 복구하기 위한 추가의 노력이 필요한 연구분야 입니다. 둘째 논문 "오류정정부호를 이용한 실용적 분산 비디오 부호화 기술"은 비디오 부호화 분야의 새로운 패러다임을 개척하는 내용으로 여기에서 ECC는 채널의 오류정정이 아닌 비디오 정보의 전송량을 줄이는 역할을 수행합니다. 셋째 논문 "NAND Flash 메모리 저장 장치에서의 Error Control Code 응용"은 최근 화두가 되고 있는 NAND Flash 메모리 저장 장치의 reliability를 높이기 위한 방안으로서 ECC의 역할을 다루고 있습니다. 통신 채널과는 매우 다른 환경이기 때문에 이에 맞추어 전혀 다른 종류의 접근 방식을 사용하고 있습니다.

나머지 세 편의 논문은 암호이론 분야로의 응용을 다루고 있습니다. 넷째 논문 "부호 기반 McEliece 암호 체계와 안전성 분석"은 이제 양자 컴퓨터 시대에도 안전성이 유지될 것으로 예견되는 ECC 기반 암호체계에 대한 내용입니다. 다섯째 논문 "랜덤선형부호의 복호화 문제와 그의 암호학적 응용"은 기존의 간단한 블록부호에 임의로 오류를 주입하여 암호화 방식에 적용하는 문제를 다루고 있습니다. 주입하는 오류의 크기를 ECC가 해결할 수 있는 범위로 한정한다면 매우 우수한 암호화 프로토콜을 만들어낼 수 있다는 내용입니다. 여섯째 논문 "Error Correction Codes for Biometric Cryptosystem: An Overview"는 생체인식 암호화에 ECC가 사용되는 모습을 다루고 있습니다.

위의 여섯 편의 논문 각각은 통신채널의 reliability증대가 아닌 목적이지만 해당 분야의 기술을 가능케 하는 수준의 핵심적 역할을 담당하는 오류정정부호의 역할을 소개하고 있습니다. 이 논문들이 부디 회원님의 연구 활동에 많은 도움이 되길 바라며, 지난 수개월 동안 수시로 독촉 이메일에 시달렸을 모든 저자에게 감사의 말씀을 드립니다.

약 력

송 홍 엽 연세대학교 공과대학 전기전자공학부 교수

학력 : 연세대학교 학사, University of Southern California 석사 및 박사

경력 : USC-CSI 포닥연구원, Qualcomm Inc. 선임연구원, 2015 IEEE Information Theory Workshop 조직위원장, IEEE Information Theory Society Seoul Chapter Chair, 한국통신학회 부호 및 정보이론 연구회 운영위원장, 총무상임이사