◎ 전 산 수 학 ◎
(Computer Math.)

함남우*(인천대), **홍범일**(인천대)

CM-1 **A Numerical Approximation to a Continuous Function by Neural Networks**

신경망에 관한 이론은 전산학에서 뿐만이 아니라 천체물리학, 인지이론, 로봇공학 및 자동 목표 추적 등의 다양한 응용분야에서 사용되고 있다. 수학적인 관점에서 신경망은 단순한 형태의 비선형 함수이 선형적인 결합으로 된 함수들을 의미한다. 이번 발표에서는 단순한 형태의 sigmoidal 함수와 squashing 함수를 활동함수로 갖는 신경망이 조밀한 집합위에 연속함수로 정의된 목표함수에 접근하는 과정에 대한 이론적 검증과 실험적인 결과를 설명하고자 한다. 특히, 기존의 연구 결과와는 달리 weight를 고정한 신경망으로도 목표함수에 원하는 정도로 가깝게 접근이 가능함을 보이고자 한다.

박미애*(국민대), **김용희**(광운대), **이종근**(국민대),
김창범(국민대), **이옥연**(국민대)

CM-2 **암호의 안전성 분석을 위한 S-box 설계 기준 검증에 관한 연구**

정보보호(Information Security) 분야의 기반이 되는 암호 알고리즘은 다양한 컴퓨터 및 통신환경에서 효율적인 구현(efficiency)이 가능하도록 설계되는 것과 함께 충분한 안전성(security)을 제공하는 것이 필수적이다. 따라서 다양한 암호 알고리즘에 대한 많은 안전성 검증 방법이 제시되고 있으며, 이에 대한 정확한 검증 결과를 제시하는 것은 매우 중요하다.

본 논문 발표에서는 2002년 현재 유럽연합(EU)에서 진행 중인 NESSIE(New European Schemes for Signatures, Integrity, and Encryption) project에 제안된 CS-cipher, Camellia, Grand CRU, SC-2000, Q, Noekeon, Hierocrypt-3 등의 블록암호 알고리즘의 S-box에 대한 안전성 분석을 위하여 balanceness, avalanche criterion, strict avalanche criterion, bit independence criterion, algebraic degree, XOR distribution, linear structure, nonlinearity 등의 안전성 기준을 연구하고 각 암호 알고리즘의 안전성 검증을 직접 수행한 결과를 제시한다.

또한 NIST에서 채택한 AES(Rijndael) 알고리즘에 사용된 S-box에 대한 상기 테스트의 결과와 비동기 IMT-2000 시스템의 무선구간 암호화 및 무선구간 무결성 검증을 위한 f8, f9 알고리즘의 핵심(kernel) 함수로 사용되는 KASUMI의 S7-box, S9-box에 대한 안전성 테스트 결과를 발표한다.