# "기밀 컴퓨팅 및 암호 컴퓨팅" 특집호 발간에 즈음하여

기밀 컴퓨팅 및 암호 컴퓨팅은 원격 클라우드나 엣지에서 저장·처리되는 사용자 데이터를 보호하는 기술로, 개인 및 기업의 민감 정보를 원격 클라우드에서 활용하고자 하는 수요가 증가하고 있는 오늘날 그 중요성이 더욱 부각되고 있습니다.

현대의 기업 단체, 개인들은 점점 많은 데이터를 생성하고 있고, 이들 중 많은 부분은 기업비밀, 사생활 등의 측면에서 민감한 정보를 담고 있습니다. 이런 데이터를 저장하는 안전한 방법은 데이터 소유자가 보유 및 관리하는 저장장치를 이용하는 것이지만, 이는 자연재해 등 특수 상황하에서의 데이터 무결성이나 데이터 공유 방법의 제약, 데이터 저장장치의 취약성에 대한 공격에 대한 취약성 등 여러 단점도 갖고 있습니다. 이런 이유로 많은 사용자들이 데이터를 클라우드 기반의 서비스를 통해 보관 및 관리하고 있으나, 여전히 민감한 데이터의 클라우드 상 보관은 기술적으로 클라우드 관리자가 데이터네 접근할 수 있다는 점 때문에 가능한 기피하고 있는 상황입니다. 이런 문제에 대한 해답으로 활발히 연구개발되고 있는 기밀 컴퓨팅 및 암호 컴퓨팅 기술은 이제 어느덧 상용화 수준에 다가왔으며, 여러 클라우드 서비스 기업들이 제품화에 나서고 있습니다. 생산단계에서 하드웨어에 내장된 암호 키와 특화 설계된 아키텍처를 이용하는 기밀 컴퓨팅 기술은 그 성능 및 무결성 보장 등에서 장점을 가지지만, 생산자에 대한 신뢰 필요성이나 지속적으로 연구되고있는 부채널 공격 취약성 등의 단점을 갖습니다. 동형암호라는 혁신 기술을 기반으로 하는 암호 컴퓨팅은 수학적으로 데이터의 기밀성을 보장해주지만, 성능 및 무결성 보장 수준 측면에서의 제약을 안고 있습니다.

본 특집호는 이와 같이 향후 더욱 필요성이 증대될 것으로 생각되며 각각의 장단점을 갖고 있는 기밀 컴퓨팅 및 암호 컴퓨팅 기술의 최신 동향 및 난제들과 그 해결 방안들에 대한 글들을 담고 있습니다. 먼저 기밀 컴퓨팅 분야에서는 기존 응용의 기밀컴퓨팅 환경 상 최적화 방안, 차세대 컴퓨팅 환경에서의 기밀 컴퓨팅 기법 및 도전과제, 그리고 기밀 컴퓨팅 환경을 대상으로 한 취약점 공격 대응 기법 등에 대한 내용을 소개합니다. 암호 컴퓨팅 분야에서는 먼저 위치정보 보호, 코로나 동선 정보 추적 지원, 개인정보보호 인공지능 등 암호 컴퓨팅 기술의 다양한 적용분야를 소개 하고, 암호 컴퓨팅 실용화의 가장 큰 걸림돌인 성능 문제 해결을 위한 최신 가속 기술들에 대해 다룹니다.

끝으로 바쁘신 중에도 소중한 시간을 내시어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 학회지 편집 위원회, 그리고 학회 사무국 관계자 여러분께 감사를 드립니다.

2023년 10월

울산과학기술원 컴퓨터공학과 부교수 설 현 곤