비밀 나누기

비밀 나누기? 친구들과 커피 한잔하며 나누는 비밀스런 이야기라고 생각하겠지만, 내가 30대 초반에 사랑에 빠지게 된, 그래서 여전히 나를 기쁘게도 때로는 힘들게도 하는 내 삶의 일부분이다.

비밀 나누기에 대한 사랑은 이렇게 시작되었다. 2007년 Iwan M. Duursma 교수님의 지도하에 일리노이 대학(얼바나-샴페인)에서 대수적 곡선을 이용한 암호학과 부호론에 관한 연구로 박사학위를 취득하였다. 그 후 일리노이에서 여러 가지 재미있는 문제들을 접하였지만 가장 관심을 끈 문제가 바로 비밀 나누기 즉 비밀 분산(Secret Sharing)이다. '비밀 분산 스킴' 이란 비밀을 여러 사람에게 분산시킨 후 권한이 주어진 집단만 비밀을 복원할 수 있고, 권한이 주어지지 않은 집단은 비밀에 관한 아무런 정보도 얻지 못하는 스킴이다. 1979년 Shamir와 Blakley는 각자 독립적으로 (t,n) threshold scheme을 발표하였다. (t,n) threshold scheme은 n명 중 t명이 모이면 비밀을 복원할 수 있고 t명 보다 적게 모이면 비밀을 복원할 수 없을 뿐만 아니라 비밀에 관한 어떠한 정보도 얻지 못하는 스킴이다. Threshold scheme은 암호키를 관리하는데 유용하게 이용된다. 데이터를 보호하기 위해서 우리는 데이터를 복호(cipher)한다. 그러나 복호키 또한 보호해야 한다. 복호키를 하나의 서버에 보관한다면 그 서버가 해킹당하거나 고장이 나면 복호키가 노출되거나 복호키를 잃게 된다. 그렇다고 복호키를 여러 개 복사하여 여러 개의 서버에 보관하면 해킹당할 위험이 그만큼 커진다. 이러한 문제점을 해결하기 위하여 복호키를 여러 서버에 분산하여 보관하고 몇 개 이상의 서버가 바르게 작동을 하면 복호키를 복원할 수 있게 만드는 threshold scheme을 이용한다. 이 스킴을 이용하면 해커가 해킹하기 위해서는 여러 개의 서버를 해킹하여야 하며 설사 서버 한두 개가 고장이 나더라도 복호키를 복원할 수 있다. 비밀 분산 스킴의 또 다른 응용은 secure multi-party computation (SMPC)이다. SMPC 문제로 처음 소개된 것이 Yao의 백만장자 문제이다. 두 백만장자가 서로의 재산을 밝히지 않고 누가 더 재산이 많은지를 알아내는 문제이다. SMPC는 많은 분야에서 응용되고 있으며 대표적인 실생활에서의 응용은 '옥션' 과 '분배 선거' 가 있다.

KIAS에서의 비밀 나누기는 이제 어떤 모습으로 변해갈까? 유난히 무더웠던 지난해 여름, 송글송글 맺히는 땀방울이 홍릉길에서 만난 초록빛 가로수길에서 조금씩 식어가고 있었다. 그리고 첫 발걸음을 내딛은 고등과학원... 어느덧 8개월로 접어든 이곳에서의 생활이 조금은 익숙해져 가고, 매일 아침 인사 나누는 계산과학부 연구원들과 직원들도 정겹기만 하다. 남들이 고개를 절레절레 흔드는 카페테리아의 점심도 아직은 먹을 만해서 좋고!

내가 사랑하는 비밀 나누기는 창문 너머 사계절을 마음껏 즐길 수 있는 아늑한 연구실에서 계속되겠지만, 이렇게 설레는 마음은 왜일까? 내 일상의 '진짜 비밀 나누기' 도 따뜻한 봄햇살이 내리쬐는 캠퍼스 벤치에서 나눌 수 있을 거라는 기대감 때문일까? KIAS

글 _ **박승국** · 고등과학원 계산과학부 연구원