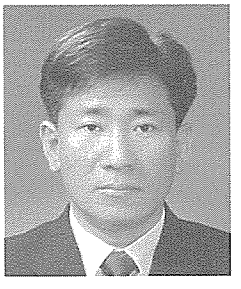
제20차 EUROCRYPT 2001 학술회의

「경제와 암호학」 주제 … 5백여명 참가

● 일자 : 2001년 5월 6일~10일 ● 장소 : 오스트리아 인스브루크



李 東 勳
〈고려대 정보보호대학원 교수〉

지난 5월 6일부터 10일까지 오스트리아의 인스브루크에서 '경제와 암호학'이라는 주제 아래 EUROCRYPT2001이 개최되었다. 올해로 20번째 개최되는 EUROCRYPT는 세계 암호학회인 IACR(International Association for Cryptologic Research)이 주관하는 CRYPTO, ASIACRYPT와 함께 암호학분야 최고 권위의 3대 학회 중의 하나이다. CRYPTO는 매년 여름 미국의 산타바바라에서, EUROCRYPT는 매년 봄 유럽에서, 그리고 ASIACRYPT는 매년 겨울 아시아에서 개최된다.

33개 논문 채택 열띤 토론

이번 학술회의에는 모두 1백55편의 논문이 투고된 중에서 33개의 논문이 채택됨으로써 5대 1의 높은 경쟁률을 보였다. 논문 채택비율에서는 미국이 단연 돋보였으며, 공개키 암호 뿐만 아니라 대칭키 암호, 암호 프로토콜 등의 분야에서도 이론적인 안전성 분석이 다양하게 시도된 논문들이 주류를 이루었다.

참가자는 등록된 사람만 4백80여명이었고, 등록하지 않은 참가자를 포함하면 5백명이 넘는 인원이 참가하여 성황을 이루었고, 특히 이집트, 가나 등 아프리카 국가들에서도 참가하여 암호학의 저변이 세계적으로 확산되어 있음을 보였다. 참고로 현재 암호 강국으로는 미국과 이스라엘이 선두를 달리고 있으며, EU와 아시아국가들이 그 뒤를 달리고 있다. 저명한 암호학자들은 국적을 불문하고 유태인 학자들이 대부분이며, 한국에서도 최근 정보보호분야의 교육과 연구에 많은 관심을 갖게되어 지난 몇년 동안 국제학회에 좋은 논문을 발표하고, 국제학회를 국내에 유치하는 등, 이 분야에 가능성을 보이고 있다.

AT&T의 Andrew Odlyzko박사가 'Economics and Cryptography'라는 제목으로 기조연설을 하였으며, 초청강연으로 MIT의 Silvio Micali교수의 'Zero Knowledge has come of age'가 있었다. 토론세션은 Jean-Jacques Quisquater박사의 진행으로 재미있는 분위기 속에서 19명의 발표자가 각 5분 정도의 시간으로 발표하였는데 밤 10시까지 지속되는 학구적인 분위기였다. 특히 당일 오전에 발표된 논문(NTRU의 서명방식인 NSS)에 대한 공격 방법을 RSA사에서 설명할 정도로 최근 결과에 대한 신속하고 효과적인 노력들이 진행되고 있음을 보여 주었다. 암호학분야의 학술회의에서는 종종 있는 일이지만 이러한 공격들은 발표된 논문의 저자들을 당혹케 하였다.

마지막날 저녁에 있었던 연회장의 분위기는 이 회의의 성격을 잘 나타내고 있었다. 물론 학술회의의 성격이 최근 결과의 신속한 발표와 학자들간의 교류에 있지만, 이 연회장에서는 각국의 학자들이 소그룹으로 모여 서로의 관심 분야와 주제에 대하여 토론

'경제와 암호학' 이라는 주제 아래 막을 올린
EUROCRYP 2001 국제학술회의가 지난 5월 6일 오스트리아 인스부르크에서 개최되었다.
5백여명의 과학자들이 참가한 이번 학술회의에서는 1백55편의 논문중
33개의 논문이 채택된 가운데 5일 동안 열띤 토론과 함께 성황을 이루었다.

마지막 연회에서 일본, 벨기에 학자들과 함께(오른쪽에서 두번째가 필자)

하여 다음에 개최되는 회의에 발표할 논문들을 미리부터 준비하는 인상을 받았다. 보통 세계적으로 유명하고 연로한 학자들은 사교에 주력한다는 고정관념이 있으나, 이 곳에서는 예외없이 모두가 학구적인 분위기여서 자정이 가까이 되서야 끝날 정도였다.

귀로 機內서도 토론 계속

학회가 열린 오스트리아의 인스부르크는 참으로 인상적인 곳이었다. 공항은 조그마했지만, 한쪽에 병풍처럼 펼쳐져 있는 눈 덥힌 알프스산맥의 봉우리들은 아름다우면서도 자연의 웅장함을 눈 앞에서 잘 나타내고 있었다. 오스트리아의 숲, 길거리의 잡초들은 한국의 그것과 유사하기로 잘 알려져 있지만 도로변에서 흔히 볼 수 있는 쑥은 더욱 오스트리아를 친숙하게 만들었다. 시내의 중심부는 20분 정도 도보로 걸어다닐 수 있는 크기이며 알프스산맥에서 흘러 내려오는 조그마한 강이 중심부를 통과하고 있었다. 공기가 어찌나 맑은지 지구상에 존재하는 최후의 피신처가 아닐까 할 정도였다. 시내를 감싸고 있는 봉우리 중의 하나인 Innsbruck Nordkettenbahnen at Hafelekar(2,269m)로 올라가는 여정은 흥미로웠다. 케이블카로 약 40분 정도를 올라가는데, 산 밑의 기온은 초여름 기온이어서 여름복장을 하고 탑승을 했다. 약 20분 정도 올라가서는 눈을 볼 수 있었고 정산부근에서는 반팔을 입고 중간에 스키를 타고 내려오는 사람을 만날 수 있었다.

더욱 인상적인 일은 학회를 마치고 인스부르크에서 네덜란드로 가는 비행기에서의 분위기였다. 대부분의 승객들이 학회에 참석하고 자국으로 돌아가는 사람들이었는데 통상적으로 여행의 피로로 잠을 청하는 것이 보통이었으나, 비행기 안은 서로의 결과를 정리하기 위한 대화로 시끄러울 정도였으며, 필자의 앞 좌석에 앉은 두 젊은 미국인들은 논문의 제목을 정하고 요약문을 논의하기까지 하였다. 진지하면서도 순수하게 학문을 사랑하는 사람들과, 신이 인간을 위하여 만들어 준 자연을 잘 보존하는 노력들이 지금 이 시간에도 생생하게 떠오른다. ST