Matthew Franklin

Capsule Introduction

SNU CSE Distinguished Lecture Series

Matt Franklin 교수는 암호학(cryptography) 분야의 세계적인 석학이다. 암호학 분야의 주요 학술회의인 Crypto와 Eurocrypt에서 심사위원장 및 심사위원을 역임하였으며, 암호학 분야의 주요 학술지인 Journal of Cryptology의 편집위원장을 맡고 있다.

Franklin 교수는 암호학 분야에서 중요한 연구결과를 많이 발표하였는데, 그중 하나가 "identity-based encryption"이다. 공개키 암호시스템(public-key cryptosystem)에서는 각 사용자가 공개키와 비밀키를 가져야 되는데, identity-based encryption은 공개키로 이메일 주소 같이 "알려진 ID"를 사용할 수 있게 해주는 방식이다. 그렇게 함으로써 공개키 암호시스템을 훨씬 쉽게 구현하게 해주는 암호화 방식이다.

Franklin 교수는 University of California, Davis에 교수로 부임하기 전에 Bell Lab, AT&T 연구소, Xerox PARC 연구소에 재직하면서 "identity-based encryption", "privacy and trust in e-community", "secure auction system" 등 많은 미국 특허를 얻었다.

Franklin 교수는 나와 같이 Columbia 대학교에서 Galil 교수의 박사과정 학생으로 대학원 생활을 같이 보냈는데, 그때 같이 샌드위치를 먹고 바둑을 두던 것이 생각난다.

http://www.cs.ucdavis.edu/ franklin/

박근수, 2010년 12월