Ben-Gurion University of the Negev

NJIT New Jersey Institute of Technology

CYBER SEMINAR SERIES

Shlomi Dolev
Ben-Gurion University

Post-Quantum Cryptography for Privacy and Security of the Internet

Vulnerabilities of the public key infrastructure currently used to secure the Internet are enhanced with the development of quantum computers; with privacy, security, and cryptocurrency severe implications. The distribution of information is a key solution for future security infrastructures. Quantum computers' development road map predicts a serious threat to today's encrypted data within less than a decade. This is an opportunity to reconsider the security of the Internet, based on the public key infrastructure architecture.

Having all information on a particular site or sent over a particular channel is a big risk for privacy. Information distribution can serve us today inefficient solutions for data in motion and data in rest. Ownership of information is preserved when sending a credit card number, sending a random number through email, and a random number through SMS, such that their xor is the actual number. Storing photos in your own computer/server may risk data leakage and/or ransomware attacks, storing in Google Drive and alike, yield a trust in a single entity (and all the employers of the entity) and loss of data ownership, hence, a multi-cloud solution, each cloud storing random numbers is preferred. Blockchain distributed trust complements the above solutions allowing private logic contracts.

Shlomi Dolev is a Chair Professor, IEEE Fellow, EAI Fellow, founding chair of the Department of Computer Science at the Ben-Gurion University of the Negev, served as faculty of Natural Science Dean, and as Chair of the Board of the Inter-University Computation Center (IUCC first ISP of Israel). Currently, Dolev is the Computer Science Discipline Committee Chair in the Israeli Education Ministry. He has over three hundred publications in computer science, distributed computing, networks, cryptography, security, optical and quantum computing, nanotechnology, brain science, and machine learning. He authored the book Self-Stabilization, published by MIT press. Additionally, Dolev is a serial entrepreneur, co-founder of Secret Double Octopus and SecretSkyDB.

Thursday, November 11th, 2021 | 10:00 AM ET | 5:00 PM Israel

Click Here: Zoom Meeting Link