Queen's Centre for Security & Privacy

Distinguished Speaker Series

Dr. Paul C. Van Oorschot

How Diffie and Hellman Changed the World
(A Brief History of Internet Security)

Thursday, May 29th, 2:30-3:30 pm

Dupuis 217

Abstract

Whitfield Diffie and Martin Hellman won the 2015 Turing Award for their conception of public-key cryptography, laying the foundation for much of today's Internet security. Their broad work, including also symmetric-key cryptography and key management, moved cryptography from secret government agencies to openly published work by academics and industrial cryptographers. We trace the evolution of cryptography from their 1976 landmark paper to today, including the path through elliptic curve cryptography and most recently, post-quantum algorithms, with a focus on societal impact (not mathematical details).

Biography

Paul Van Oorschot is a Professor of Computer Science at Carleton University in Ottawa, Canada. He moved into academia in 2002 after an industrial career in the telecommunications and software security sectors. His research interests include authentication and identity management, computer and Internet security, software security, and applied cryptography. He is an ACM Fellow, IEEE Fellow, and Fellow of the Royal Society of Canada. His books include the Handbook of Applied Cryptography (1996), and Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin (2021).