Title: Title: The Simulation Paradigm and Deniable Communications

Abstract: In this talk I will survey the area of Deniable Communication and the use of the Simulation Paradigm to define and prove what deniability is. I will discuss the fundamental differences between zero-knowledge and deniability simulations, and then focus on the specific application of deniable authentication and key-exchange. I will conclude by presenting a recent work that analyzes the deniability of widely used messaging protocols such as Signal. The recent work is in collaboration with Nihal Vatandas, Bertrand Ithurburn and Hugo Krawczyk

Bio: Prof. Gennaro received his Ph.D. from the Massachusetts Institute of Technology in 1996, and was a researcher at the IBM T.J.Watson Research Center before joining City College in the Summer of 2012. Rosaio's research focuses on cryptography and network security and more in general on theoretical computer science. His most recent works address the security of the cloud computing infrastructure, the issues of privacy and anonymity in electronic communication, and proactive security to minimize the effects of system break-ins.