Abstract:
Partly because of design outsourcing and migration of fabrication to low-cost areas across the globe, and partly because of increased reliance on third-party intellectual property and design automation software, the integrated circuit (IC) supply chain is now considered far more vulnerable to malicious modifications than ever before. Such modifications, known as hardware Trojans, provide additional functionality which is unknown to the designer and user, but which can be exploited by the perpetrator after deployment to sabotage or incapacitate a chip, or to steal sensitive information. In this talk, I will introduce the challenges associated with certifying IC trustworthiness and I will elucidate the multi-disciplinary expertise required to address this problem. I will also discuss my group’s activities in developing various hardware security solutions and I will highlight research opportunities for students interested in pursuing a funded Ph.D. in this topic.

Short Biography:
Yiorgos received the Diploma of Computer Engineering and Informatics from the University of Patras in 1995, and the M.S. and Ph.D. in Computer Engineering from the University of California, San Diego, in 1997 and 2001, respectively. After spending eleven years on the faculty of Electrical Engineering and Computer Science at Yale University, he recently moved to the University of Texas at Dallas, where he directs the Trusted and RELiable Architectures (TRELA) laboratory. His research interests focus on applications of machine learning and statistical analysis in the design and implementation of robust and secure digital and analog integrated circuits and systems. He serves on the organizing committees of various conferences in these areas and he is the Program Chair for this year’s VLSI Test Symposium (VTS’13). He is the recipient of the Sheffield Teaching Award and a senior member of the IEEE.