

Keynote: Primitives for Physical Trust

Anish Arora

Department of Computer Science and Engineering
The Ohio State University
Columbus Ohio 43210, USA
anish@cse.ohio-state.edu

Abstract. This talk explores the question of whether wireless communication can achieve security - confidentiality (unicast and broadcast), authentication, non-repudiation, anonymity - without assuming any shared secrets and using only low-cost computation primitives. The key idea is to exploit physical characteristics of the network medium to develop a basis of physical primitives that suffice for rethinking a security protocol suite.