1072-68-68 **Nitesh Saxena*** (nsaxena@poly.edu). *Tree-based HB Protocols for Privacy-Preserving Authentication of RFID Tags.*

An RFID reader must authenticate its designated tags in order to prevent tag forgery and counterfeiting. At the same time, due to privacy requirements of many applications, a tag should remain anonymous and untraceable to an adversary during the authentication process. In this talk, we present an "HB-like" protocol for privacy-preserving authentication of RFID tags. Previous protocols for privacy-preserving authentication were based on PRF computations. Our protocol can instead be used on low-cost tags that may be incapable of computing traditional PRFs. Moreover, since the underlying computations in HB protocols are very efficient, our protocol also reduces reader-side load compared to PRF-based protocols.

We suggest a tree-based approach that replaces the PRF-based authentication from prior work with a procedure such as HB+ or HB#. We optimize the tree-traversal stage through usage of a "light version" of the underlying protocol and shared random challenges across all levels of the tree. This provides significant reduction of the communication resources, resulting in a privacy-preserving protocol almost as efficient as the underlying HB+ or HB#. (Received June 16, 2011)