

# A Symbolic Logic with Exact Bounds for Cryptographic Protocols

John C. Mitchell

Department of Computer Science,  
Stanford University  
[mitchell@cs.stanford.edu](mailto:mitchell@cs.stanford.edu)

This invited talk will describe a formal logic for reasoning about security properties of network protocols with proof rules indicating exact security bounds that could be used to choose key lengths or other concrete security parameters. The soundness proof for this logic, a variant of previous versions of Protocol Composition Logic (PCL), shows that derivable properties are guaranteed in a standard cryptographic model of protocol execution and resource-bounded attack. We will discuss the general system and present example axioms for digital signatures and random nonces, with concrete security properties based on concrete security of signature schemes and pseudorandom number generators (PRG). The quantitative formal logic supports first-order reasoning and reasoning about protocol invariants, taking exact security bounds into account. Proofs constructed in this logic also provide conventional asymptotic security guarantees because of the way that exact bounds accumulate in proofs. As an illustrative example producing exact bounds, we use the formal logic to prove an authentication property with exact bounds of a signature-based challenge-response protocol.

This talk presents joint work with Anupam Datta (Carnegie Mellon University), Joseph Y. Halpern (Cornell University), and Arnab Roy (IBM Thomas J. Watson Research Center).

**Acknowledgements.** This work was partially supported by the National Science Foundation, the Air Force Office of Scientific Research, and the Office of Naval Research.