On Session Key Construction in Provably-Secure Key Establishment Protocols*

Kim-Kwang Raymond Choo, Colin Boyd, and Yvonne Hitchcock

Information Security Institute
Queensland University of Technology
GPO Box 2434, Brisbane, QLD 4001, Australia
{k.choo,c.boyd,y.hitchcock}@qut.edu.au

Abstract. We examine the role of session key construction in provably-secure key establishment protocols. We revisit an ID-based key establishment protocol due to Chen & Kudla (2003) and an ID-based protocol 2P-IDAKA due to McCullagh & Barreto (2005). Both protocols carry proofs of security in a weaker variant of the Bellare & Rogaway (1993) model where the adversary is not allowed to make any Reveal query. We advocate the importance of such a (Reveal) query as it captures the known-key security requirement. We then demonstrate that a small change to the way that session keys are constructed in both protocols results in these protocols being secure without restricting the adversary from asking the Reveal queries in most situations. We point out some errors in the existing proof for protocol 2P-IDAKA, and provide proof sketches for the improved Chen & Kudla's protocol. We conclude with a brief discussion on ways to construct session keys in key establishment protocols.

Keywords. Key establishment protocols, provable security

The full version can be downloaded from http://eprints.qut.edu.au/perl/user_eprints?userid=51.

* This work was partially funded by the Australian Research Council Discovery Project Grant DP0345775. This is the pre-print of the conference proceedings to appear in Mycrypt 2005, Lecture Notes in Computer Science, Springer-Verlag.