Another Look at Provable Security

Alfred Menezes

Department of Combinatorics & Optimization
University of Waterloo
ajmeneze@uwaterloo.ca

Abstract. Many cryptographers believe that the only way to have confidence in the security of a cryptographic protocol is to have a mathematically rigorous proof that the protocol meets its stated goals under certain assumptions. However, it is often difficult to assess what such proofs really mean in practice especially if the proof is non-tight, the underlying assumptions are contrived, or the security definition is in the single-user setting. We will present some examples that illustrate this difficulty and highlight the important role that old-fashioned cryptanalysis and sound engineering practices continue to play in establishing and maintaining confidence in the security of a cryptographic protocol.

This talk is based on joint work with Neal Koblitz [2, 3] and with Sanjit Chatterjee and Palash Sarkar [1].

References

1. S. Chatterjee, A. Menezes and P. Sarkar, "Another look at tightness", *Selected Areas in Cryptography — SAC 2011*, Lecture Notes in Computer Science, 7118 (2011), 293–319.
2. N. Koblitz and A. Menezes, "Another look at provable security", http://anotherlook.ca.
3. N. Koblitz and A. Menezes, "Another look at security definitions", Cryptology ePrint Archive: Report 2011/343.