Cryptology ePrint Archive: Report 2011/350

HB^N: An HB-like protocol secure against man-in-the-middle attacks

Carl Bosley and Kristiyan Haralambiev and Antonio Nicolosi

Abstract: We construct a simple authentication protocol whose security is based solely on the problem of Learning Parity with Noise (LPN) which is secure against Man-in-the-Middle attacks. Our protocol is suitable for RFID devices, whose limited circuit size and power constraints rule out the use of more heavyweight operations such as modular exponentiation. The protocol is extremely simple: both parties compute a noisy bilinear function of their inputs. The proof, however, is quite technical, and we believe that some of our technical tools may be of independent interest.

Category / Keywords: cryptographic protocols / authentication, secret-key cryptography, LPN, Learning Parity with Noise

Date: received 27 Jun 2011, last revised 5 Aug 2011

Contact author: bosley at cs stevens edu

Available formats: PDF | BibTeX Citation

Version: 20110805:171136 (All versions of this report)

Discussion forum: Show discussion | Start new discussion
