Krause, Matthias; **Stegemann, Dirk**

More on the security of linear RFID authentication protocols. (English) Zbl 1267.94077

Jacobson, Michael J. jun. (ed.) et al., Selected areas in cryptography. 16th annual international workshop, SAC 2009, Calgary, Alberta, Canada, August 13–14, 2009. Revised selected papers. Berlin: Springer (ISBN 978-3-642-05443-3/pbk). Lecture Notes in Computer Science 5867, 182-196 (2009).

Summary: The limited computational resources available in RFID tags implied an intensive search for lightweight authentication protocols in the last years. The most promising suggestions were those of the HB-familiy (HB^+, $HB^\#$, TrustedHB, ...) initially introduced by Juels and Weis, which are provably secure (via reduction to the Learning Parity with Noise (LPN) problem) against passive and some kinds of active attacks. Their main drawbacks are large amounts of communicated bits and the fact that all known HB-type protocols have been proven to be insecure with respect to certain types of active attacks. As a possible alternative, authentication protocols based on choosing random elements from L secret linear n-dimensional subspaces of $\mathrm{GF}(2)^{n+k}$ (so-called CKK-protocols) were introduced by Cichoń, Klonowski, and Kutyłowski. These protocols are special cases of (linear) (n, k, L)-protocols which we investigate in this paper. We present several active and passive attacks against (n, k, L)-protocols and propose $(n, k, L)^{++}$-protocols which we can prove to be secure against certain types of active attacks. We obtain some evidence that the security of (n, k, L)-protocols can be reduced to the hardness of the learning unions of linear subspaces (LULS) problem. We then present a learning algorithm for LULS based on solving overdefined systems of degree L in Ln variables. Under the hardness assumption that LULS-problems cannot be solved significantly faster, linear (n, k, L)-protocols (with properly chosen n, k, L) could be interesting for practical applications.

For the entire collection see [Zbl 1177.94012].

MSC:

94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing

Keywords:

lightweight cryptography; RFID authentication; algebraic attacks; HB^+; CKK; CKK^2

Software:

FGb; Magma

Full Text: DOI