Cryptology ePrint Archive: Report 2011/511

The Cryptographic Power of Random Selection

Matthias Krause and Matthias Hamann

Abstract: The principle of random selection and the principle of adding biased noise are new paradigms used in several recent papers for constructing lightweight RFID authentication protocols. The cryptographic power of adding biased noise can be characterized by the hardness of the intensively studied Learning Parity with Noise (LPN) Problem. In analogy to this, we identify a corresponding learning problem called RandomSelect for random selection and study its complexity. Given L secret linear functions f_1,...,f_L : {0,1}^n -> {0,1}^a, RandomSelect(L,n,a) denotes the problem of learning f_1,...,f_L from values (u,f_l (u)), where the secret indices l \in {1,...,L} and the inputs u \in {0,1}^n are randomly chosen by an oracle. We take an algebraic attack approach to design a nontrivial learning algorithm for this problem, where the running time is dominated by the time needed to solve full-rank systems of linear equations over O(n^L) unknowns. In addition to the mathematical findings relating correctness and average running time of the suggested algorithm, we also provide an experimental assessment of our results.

Category / Keywords: secret-key cryptography / Lightweight Cryptography, Algebraic Attacks, Algorithmic Learning, Foundations and Complexity Theory

Publication Info: Full Post-Proceedings Version (Accepted to SAC 2011. Scheduled to be published in the LNCS series.)

Date: received 16 Sep 2011, last revised 5 Oct 2011

Contact author: hamann at uni-mannheim de