Cryptology ePrint Archive: Report 2013/203

From oblivious AES to efficient and secure database join in the multiparty setting

Sven Laur and Riivo Talviste and Jan Willemson

Abstract: AES block cipher is an important cryptographic primitive with many applications. In this work, we describe how to efficiently implement the AES-128 block cipher in the multiparty setting where the key and the plaintext are both in a secret-shared form. In particular, we study several approaches for AES S-box substitution based on oblivious table lookup and circuit evaluation. Given this secure AES implementation, we build a universally composable database join operation for secret shared tables. The resulting protocol scales almost linearly with the database size and can join medium sized databases with 100,000 rows in few minutes, which makes many privacy-preserving data mining algorithms feasible in practice. All the practical implementations and performance measurements are done on the Sharemind secure multi-party computation platform.

Category / Keywords: cryptographic protocols / AES, secure database join, secure multi-party computation, implementation

Publication Info: This is an extended version of the paper presented at ACNS'13.

Date: received 9 Apr 2013

Contact author: riivo talviste at cyber ee