Cryptology ePrint Archive: Report 2011/439

Optimal Data Authentication from Directed Transitive Signatures

Philippe Camacho

Abstract: An authenticated dictionary of size N is said to be optimal when an update operation or proof computation requires at most $O(\log N)$ accesses to the data-structure, and the size of a proof is $O(1)$ with respect to N. In this note we show that an optimal authenticated dictionary (OAD) can be built using transitive signatures for directed graphs (DTS). As the existence of DTS and OAD are both still open, our result can be interpreted as following: if optimal authenticated dictionaries do not exist then transitive signatures for directed graphs do not exist either.

Category / Keywords: cryptographic protocols / transitive signatures; authenticated data structures;

Date: received 12 Aug 2011

Contact author: philippe camacho at gmail com