Cryptology ePrint Archive: Report 2013/129

An Ideal-Security Protocol for Order-Preserving Encoding

Raluca Ada Popa and Frank H. Li and Nickolai Zeldovich

Abstract: Order-preserving encryption - an encryption scheme where the sort order of ciphertexts matches the sort order of the corresponding plaintexts - allows databases and other applications to process queries involving order over encrypted data efficiently. The ideal security guarantee for order-preserving encryption put forth in the literature is for the ciphertexts to reveal no information about the plaintexts besides order. Even though more than a dozen schemes were proposed, all these schemes leak more information than order.

This paper presents the first order-preserving scheme that achieves ideal security. Our main technique is mutable cipher- texts, meaning that over time, the ciphertexts for a small number of plaintext values change, and we prove that mutable ciphertexts are needed for ideal security. Our resulting protocol is interactive, with a small number of interactions.

We implemented our scheme and evaluated it on microbenchmarks and in the context of an encrypted MySQL database application. We show that in addition to providing ideal security, our scheme achieves 1–2 orders of magnitude higher performance than the state-of-the-art order-preserving encryption scheme, which is less secure than our scheme.

Category / Keywords: order-preserving encoding, encryption

Publication Info: A short version of this paper was accepted at 2013 IEEE Symposium of Security and Privacy. This paper is the long version with additional proofs.

Date: received 2 Mar 2013, last revised 6 Mar 2013

Contact author: ralucap at mit edu