Semantically Secure Order-Revealing Encryption:

Multi-Input Functional Encryption Without Obfuscation

Abstract

Deciding “greater-than” relations among data items just given their encryptions is at the heart of

search algorithms on encrypted data, most notably, non-interactive binary search on encrypted data.

Order-preserving encryption provides one solution, but provably provides only limited security guarantees.

Two-input functional encryption is another approach, but requires the full power of obfuscation machinery

and is currently not implementable.

We construct the first implementable encryption system supporting greater-than comparisons on

encrypted data that provides the “best-possible” semantic security. In our scheme there is a public

algorithm that given two ciphertexts as input, reveals the order of the corresponding plaintexts and nothing

else. Our constructions are inspired by obfuscation techniques, but do not use obfuscation. For example,

to compare two 16-bit encrypted values (e.g., salaries or age) we only need a 9-way multilinear map.

More generally, comparing k-bit values requires only a (k/2 + 1)-way multilinear map. The required

degree of multilinearity can be further reduced, but at the cost of increasing ciphertext size.

Beyond comparisons, our results give an implementable secret-key multi-input functional encryption

scheme for functionalities that can be expressed as (generalized) branching programs of polynomial length

and width. Comparisons are a special case of this class, where for k-bit inputs the branching program is

of length k + 1 and width 4.