Recent Developments in Format-Preserving Encryption

Stefano Tessaro, University of Washington

Format-preserving encryption (FPE) is a widely deployed technique in industry to encrypt databases, in particular when the format of the stored data cannot easily be changed. FPE is a deterministic encryption scheme where ciphertexts have the same format as plaintexts, e.g., a credit card number is encrypted into a credit card number.

The problem of building secure FPE has been very challenging, both in practice and in theory. I will survey some of the recent works in this area, mostly focusing on attacks against constructions and standards.

Based in part on joint works with Mihir Bellare, Viet Tung Hoang, and Ni Trieu.