What Else is Revealed by Order-Revealing Encryption?

Fatma Betl Durak
Dept. of Computer Science
10/5/2016 at 11:00 am
CoRE B (305)

Abstract

The security of order-revealing encryption (ORE) has been unclear since its invention. Dataset characteristics for which ORE is especially insecure have been identified, such as small message spaces and low-entropy distributions. On the other hand, properties like one-wayness on uniformly-distributed datasets have been proved for ORE constructions.

In this work, we show that more plaintext information can be extracted from ORE ciphertexts than was previously thought. We identify two issues: First, we show that when multiple columns of correlated data are encrypted with ORE, attacks can use the encrypted columns together to reveal more information than prior attacks could extract from the columns individually. Second, we apply known attacks, and develop new attacks, to show that the leakage of concrete ORE schemes on non-uniform data leads to more accurate plaintext recovery than is suggested by the security theorems which only dealt with uniform inputs.

Examination Committee: Prof. David Cash (chair), Prof. Rebecca Wright, Prof. Vinod Ganapathy and Prof. Abhishek Bhattacharjee