Cryptology ePrint Archive: Report 2011/614

On Security of the Utility Preserving RASP Encryption

Keke Chen

Abstract: Many potential users hesitate to use cloud computing because of the data confidentiality issue. Can we compute on untrusted public cloud platform with both data confidentiality and data utility preserved? Recent study has revealed that a convexity preserving encryption RASP can be used to construct confidentiality preserving and efficient range query service, which is one of the most frequently used query types for online data analytics. Convexity preserving encryption schemes, such as the RASP encryption, preserve the topology of the queried range in the encrypted space. It allows the encrypted data to be indexed and queried with transformed secure range queries. The initial study shows the range query service built on the RASP encrypted data can efficiently handle queries. However, there is no in-depth security analysis on the RASP encryption. In this paper, we focus on the security of the RASP encryption method. Concretely, we show that RASP is resilient to distributional attack, but it is not indistinguishable to chosen plaintext attack. We propose a relaxed security definition based on the statistical learning theory. We develop the Amount of Preserved Confidentiality (APC) measure to evaluate the security in terms of estimation attacks. We also show that the RASP encryption is resilient to estimation attacks and its encryption parameters can be appropriately tuned to meet different levels of confidentiality requirements.

Category / Keywords: secret-key cryptography / convexity-preserving encryption

Publication Info: no

Date: received 14 Nov 2011

Contact author: keke chen at wright edu