MSc in CS Thesis Proposal

Title : Format and Order Revealing Encryption

University Supervisor(s) (UBI)

- Prof. Dr. Paul Crocker : Email: crocker@di.ubi.pt
- Prof. Dr. Simão Melo de Sousa (Co-Supervisor)

Description

Format preserving encryption is a method to encrypt data whilst still preserving its format, such as a valid IP address or Credit Card Number. This has many applications, such as the offline fraud analysis of credit card transactions whilst retaining privacy of the original transactions and also using encrypted plaintexts directly in legacy applications. On the hand order preserving cryptographic schemes enable the cryptograms to retain the original ordering of the pain texts whilst order revealing schemes permit the relative order of two or more plain texts to be revealed using a publicly available function of the cryptograms.

The objectives of this work are to investigate further the concepts of format and order revealing encryption. In particular in order to implement semantically Secure Order-Revealing Encryption methods Boneh et al [1] survey several methods and implement a construction based on matrix branching and multi-linear maps. In the context of format preserving encryption to challenge is to define methods that given an encrypted plain text then using a publically available function a format and length valid element of the plain texts can be quickly and efficiently recovered.

Work Plan

- Literature and State of the Art Review.
- Formal Specification of the Problem.
- Analysis of Possible Implementations.
- Implementation of a prototype.
- Testing and Evaluation.
- Writing of the Dissertation.

Expected Results.

As well as the dissertation the results of this thesis will include a formal specification of the cryptographic problem and a software proof of concept.

References:

[1] Dan Boneh and Kevin Lewi and Mariana Raykova and Amit Sahai and Mark Zhandry and Joe Zimmerman, Semantically Secure Order-Revealing Encryption: Multi-Input Functional Encryption Without Obfuscation, Cryptology ePrint Archive, Report 2014/834.