NORWEGIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY, MATHEMATICS AND ELECTRICAL ENGINEERING

PROJECT ASSIGNMENT

Student's name:	Eirik Klevstad
Course:	TTM4501, specialization project
Project title:	Exploring CryptDB: A Practical HE Scheme for SQL Queries

Project description:

Homomorphic encryption (HE) has become a hot research topic in the last few years due to breakthroughs in algorithms, as well as new applications such as cloud computing security. The idea of HE is to allow computation on encrypted data (ciphertexts) without decrypting first. When decrypted, the result should be equivalent as if the same computation had been performed on already decrypted data (plaintext). The most powerful HE algorithms (so-called fully homomorphic schemes) remain largely impractical due to their huge computational requirements. However, practical variants have emerged for more limited homomorphic operations.

The aim of this project is to investigate CryptDB, a practical HE scheme for SQL queries. This scheme enables the possibility of performing queries and computing on encrypted data. CryptDB was developed at MIT in 2011, and is able to emulate homomorphic encryption for most of the functions that an SQL database is capable of performing.

The outcomes of the project should be an understanding and analysis of the system, why it works securely and a comparison to related homomorphic encryption schemes and systems. It should also include a simple demonstration system and suggestions for useful future applications.

Department:	Department of Telematics
Supervisor:	Chris Carr
Responsible professor:	Colin Boyd