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:	CryptDB

Project description:

Homomorphic encryption (HE) has become a hot research topic in the last few years due to break-throughs in algorithms, as well as new applications such as cloud computing security. 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. The outcomes of the project should include an understanding of the system and a comparison to related systems. If could also be interesting to include a simple demonstration system and suggestions for useful future applications.

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