Advanced Encryption Standard (AES) implementation on UDOO board

Larsen, Espen Røvik             Mogstad, Magnus Settemesli
espenrl@gmail.com          magnussmogstad@gmail.com

April 24, 2015

Abstract

For our project in CS290G Cryptography Engineering we want to implement the advanced encryption standard (AES) onto a UDOO board. AES is a symmetric-key algorithm and uses a key with a set length of either 128, 192 or 256 bits. It is an encryption standard on top of the Rijndael block cipher algorithm. There is not any known analytical attacks which is proven to be effective towards decrypting messages, but AES can be vulnerable towards side channel attacks due to vulnerabilities in the implementation. We also want to analyze what kind of side channel attacks the implementations can be vulnerable against.

The biggest challenges for this project is that none of us have a great deal of experience using the programming language C and that we have no previous experience with the UDOO platform.