NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET
FAKULTET FOR INFORMASJONSTEKNOLOGI, MATEMATIKK OG ELEKTROTEKNIKK

PROSJEKTOPPGAVE

Kandidatens navn:	Haakon Garseg Mørk og Martin Kirkholt Melhus
Emne:	TTM4531, fordypningsprosjekt
Oppgavens tittel:	Side-channel attacks on cryptographic implementations

Oppgavens beskrivelse:

In late 2013, a team of researchers managed to extract a full 4096 bit RSA key using low-bandwidth acoustic noise as a side channel. In 2014, Daniel Genkin, Adi Shamir and Eran Tromer presented their work in the paper titled RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis.

In this project, we aim to verify the results from the original research. We will verify the existence of the acoustic side channel, and analyse the acoustic fingerprint resulting from a computer executing microinstructions. We will do this by building our own experimental setup, and verify its capability of identifying these fingerprints.

After verifying the existence of the side channel we will try to apply some of the techniques described in the original research and exploit the information leakage to obtain information about ongoing processes in various target computers.

Utført ved:	Institutt for telematikk
Ideinnehaver:	Sondre Rønjom
Veileder:	Markku-Juhani O. Saarinen
Faglærer:	Stig F. Mjølsnes