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:

Genkin et al. claim to be able to extract the 4096 bits private key from an RSA decryption computation, by method of chosen cipher-text and analyzing the side channel of acoustic noise from the computer [1]. The general claim is that CPU operations and input bits can be distinguished by frequency domain analysis of the ultrasound emanating from the CPU.

This project aims to verify these surprising research results by repeating the experiments reported in [1]. First verify the existence and characteristics of acoustic side channels of computer devices. Then analyse the acoustic fingerprints found, and attempt to relate them to machine instructions, register values, and other states of the computer, in particular with respect to cryptographic computations and keys. The project will require innovative instrumentation and experimental setup, which must be considered a significant challenge in itself.

[1] Daniel Genkin, Adi Shamir and Eran Tromer. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. Crypto 2014. Springer Verlag LNCS 8616, pp. 444/461, 2014.

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