

**Master 2018**

**Navdeep Singh**

**Physical Layer Security: Key Reconciliation in FDD.**

***ABSTRACT - Masterthesis***

Physical layer key generation is using common randomness of bidirectional wireless channel measurements together with quantization. Typically, one assumes channel reciprocity from time-division duplexing (TDD). In case of frequency-division multiplexing, this complete symmetry is not given. However, ToA and DoA (Time of Arrival and Direction of Arrival) should still be roughly identical despite of different frequency bands used for both directions, at least, when the frequency bands are close. The assumption is that signal paths due to reflections and diffraction are roughly the same. Beamforming approaches and DoA algorithms, such as MUSIC, ESPRIT, or SAGE are assumed to be suitable tools.

For the practical measurements with a network analyzer, a circular antenna array with 40 equally spaced antennas is used, which is rotated with the help of a stepper motor and an Arduino motor shield. This allows to virtually measure at the whole antenna array without the need of rewiring the antennas. MATLAB and Arduino IDE are used to control the setup.

After finalizing a new antenna design with outside traction, we have performed some measurements and used the above-mentioned algorithms to determine the DoAs. This should give us an impression, how a suitable key generation scheme could be realized. This will then be worked out together with a possible reconciliation scheme, e.g., introducing some kind of guard band approach.