MSc project idea:
Quantum protocols

Quantum protocols are cryptographic protocols that make use of quantum physics to achieve security feats that are impossible with classical physics. The best known example is Quantum Key Distribution, but many other schemes have been developed. The following topics can lead to a nice MSc project:

1. Quantum readout of PUFs.
   Optical PUFs (Physical Unclonable Functions) are strong scattering media that produce unique speckle patterns and are therefore suitable for physical authentication. When *quantum* light is used to probe PUFs, the optical challenge is hidden from the adversary, which results in an authentication protocol that works even if the PUF properties are publicly known.
   https://theconversation.com/quantum-physics-can-fight-fraud-by-making-card-verification-unspoofable-35632
   However, transport of transversal modes through fibers incurs high losses. A protocol has been proposed that uses the time-frequency domain for the transport of challenges. The assignment is to do a security analysis/proof for this kind of protocol and to improve it.

2. 8-state encoding.
   Most Quantum Key Distribution (QKD) methods and more sophisticated schemes such as quantum key recycling, quantum copy protection, delegated storage, revocable commitments etc make use of the so-called "BB84 states", i.e. two complementary bases for the qubit space. Recently a different choice of bases has been suggested, wich is based on quantum one-time pad encryption: 8-state encoding.
   https://eprint.iacr.org/2016/1122.pdf
   https://eprint.iacr.org/2017/331.pdf
   The assignment is to find out where 8-state encoding can lead to efficiency improvements, and to work on the corresponding security proofs.

Please contact Boris Škorić if you are interested,
MF 6.059
040-247 4870
b.skoric@tue.nl

[March 2021]