MSc project idea: **Quantum Readout PUFs**

Physical Unclonable Functions (PUFs) are complex, hard to clone physical structures with a unique challenge-response behaviour. They can be used e.g. for read-proof key storage, authentication and anti-counterfeiting. (See the lecture notes of the course "Physical Aspects of Computer Security", http://security1.win.tue.nl/~bskoric/physsec/files/).

Recently it was proposed to use quantum states to read out PUFs. http://eprint.iacr.org/2009/369. This approach brings several new benefits:

1. remote authentication of a (weak) PUF without a trusted device in the field
2. a robust authenticated quantum channel
3. Quantum Key Exchange based on *public* information.

The Quantum Readout concept has been experimentally demonstrated using speckle-based optical PUFs.

Some possible project topics are:

- Quantum systems other than laser speckle
- Improved protocols and/or proof methods.

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

Jan. 18, 2013