MSc project idea: **Security with Noisy Data**

An essential property of cryptographic primitives is an extreme sensitivity to small changes in their inputs. However, a number of important security applications use physical measurements as a source of (secret) randomness. On the one hand, these measurements are inherently noisy. On the other hand, we often wish to use them as input for hash functions, block ciphers etc. Some form of error correction is obviously needed if we want reproducible results. This requires storage/transfer of redundancy data. It is prudent to assume that attackers have access to this data. Hence the challenge is to develop efficient error correction methods where the redundancy data does not compromise security: the so-called Fuzzy Extractors. This leads to an interesting mix of physics, information theory, coding theory and cryptography. The techniques developed in this field are useful in applications such as privacy preserving biometric identification & authentication, and PUFs for secure key storage, authentication and anti-counterfeiting.

The project concentrates on the efficency of Fuzzy Extractors and related primitives such as Locatity-Sensitive Hash Functions. Some possible research directions are:

- Zero-Leakage helper data systems (e.g. optimization of discretisation intervals in ZL Secure Sketches)
- The use of soft information in error correction for helper data schemes
- Comparison of schemes based on fuzzy extractors and Locatity-Sensitive Hash Functions.
- Quantum Readout of Physical Unclonable Functions
- The Spammed Code Offset Method
- Efficient search in privacy-preserving biometric databases

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

October 23, 2014