

Seminar

# Information Theory and Biometric Security

The topic of physical unclonable functions (PUFs) can be seen as a part of biometric security. Biometric security itself is a wide research area which involves various aspects one of which is an information theoretical analysis. The goal of this research is determine how good a system can be in theory.

In [1] the authors target a basic scenario, in which they evaluate the trade-off between privacy (i.e. protecting the biometric data) and security (i.e. roughly speaking how many key bits can be derived).

This seminar topic is supposed to summarize key aspects of such an information-theoretic approach and possibly translate it to the context of PUFs. It is highly recommended to have some background in either information theory or PUFs.

[1] Lai, Lifeng, Siu-Wai Ho, and H. Vincent Poor. "Privacy–security trade-offs in biometric security systems—Part I: Single use case." IEEE Transactions on Information Forensics and Security 6.1 (2010): 122-139.

## Contact

[Request topic](#)

## Advisors

Christoph Frisch