Chair of Communications Engineering
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Master's Thesis, Forschungspraxis, Bachelor's Thesis

[identification] Idnetification and Secrecy with Physically-Unclonable-Functions (PUFs)

Identification is a communication scheme that allows rate doubly exponential in the blocklemght, with the tradeoff that identities cannot be decoded (as messages do) but can only be verified.

- https://ieeexplore.ieee.org/document/42172
- https://ieeexplore.ieee.org/document/42173

Identification codes can be achieved by first removing the errors from the channel with regular transmission channel coding, and then sending a challenge though the corrected channel. For every identity i, The channenge is generated by picking a random input m and computing the corresponding output T_i(m) using a function T_i that depends on the identity. The challenge is then the pair m,T_i(m) and the receiver wanting to verify an identity j will verify whether j=i by testing the challenge. This is done by recomputing the output with T_j and verifying whether T_j(m)= T_i(m). The errors are reduced by ensuring that the various functions collide on a small fraction of the possible inputs.

It turns out that choosing good sets of funtions {T_i} is the same as choosing error-correction codes {c_i} with large distance, where now each codeword c_i defines a function by mapping positions m (sometimes called code locators) to symbols c_im of the codeword.
We can thus construct identification codes by choosing error-correction codes where we are only interested in the performance of the error correction encoders (we are not interested in the error-correction decoder or error-correction codes).

From previous work we have a fairly efficient implementation based Reed-Muller code which can be found at

- https://arxiv.org/abs/2107.07649
- https://arxiv.org/abs/2107.06801
- https://arxiv.org/abs/2007.06372

Secrecy in this identification codes has also been implemented in unpublished work. Furthermore, the theoretical work on Identification with PUF's has been done in

- https://ieeexplore.ieee.org/document/8445910
- https://ieeexplore.ieee.org/document/8600405

The goal of the project will be to bridge the three topics and create practical and efficient secret identification codes in the PUF setting.

The working language will be in English.

Environment: this is a project in collaboration with LTI. At LNT and LTI there is currently a lot of funding for research in identification. Therefore you will find a large group of people that might be available for discussion and collaboration.

Advisors

Christian Deppe, Roberto Ferrara