Professorship for Coding for Communications and Data Storage
Fakultät für Elektrotechnik und Informationstechnik
Technische Universität München

Overview of the COD Group

Code-based Cryptography

- Sufficiently large quantum supercomputer will render classical public-key algorithms (e.g., RSA) insecure
- Encryption based on error-correcting codes
- Provides cryptographic systems with security against quantum computers

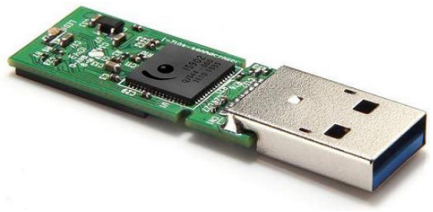
Network Coding

- Higher throughput than in routing by linear combinations of packets.
- Packets can get lost due to congestion
- Erroneous packets propagate widely
- We work on assigning the combinations to the nodes and choosing a suitable error-correcting code for the case when packets are lost or adversaries inject erroneous packets.

Coding for Storage

- **Cloud Storage**: design codes to cope with failures of data servers; minimize download costs...
- **DNA Storage**: Novel approach for long-term & high-density data storage: develop codes to correct errors in read/write processes
- **Coding for Memories**: Write-once codes, coding for stuck cells.

Poster: Coding for Stuck Memory Cells



- Errors in storage media as **flash memories**: manufacturing imperfections, wearout, read/write errors...
- Flash memory: writing can be done word-wise, but erasing only block-wise

$\Longrightarrow$ Avoid erasing, only increase levels: "Write-Once-Memory Codes"

- Defect cells cannot change their level (happens after too many Program/Erase Cycles)
- If charge is stuck, level can only be increased
- Error-correcting codes can be used to reliably write on malfunctioning devices

This work was **published in IEEE Trans. Inform. Theory** & initiated a collaboration with SanDisk® Israel.