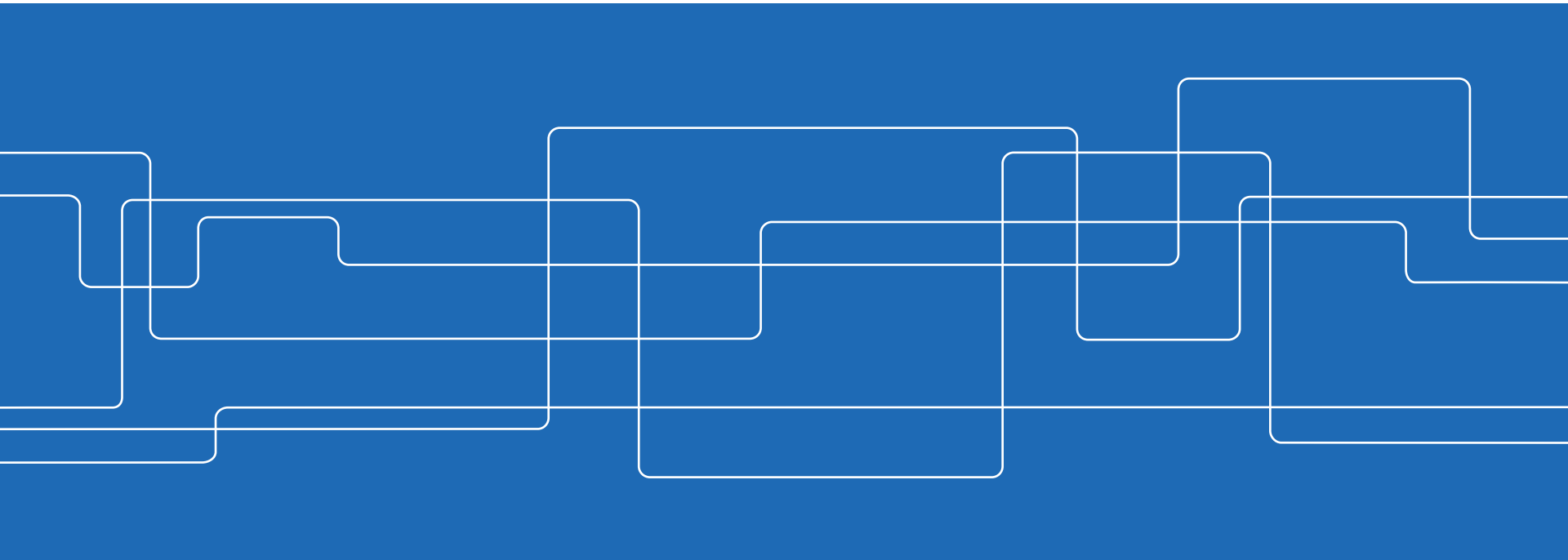
Key Research Problems in Information Forensics and Security for the Next Five Years

Tobias Oechtering,
Department Information Science and Engineering



Two major trendsetters for research

- Security & Forensic challenges in 5G
  - Enables numerous (IoT) applications
  - Features: high connection density, low communication latency
  - Need for mechanisms for authentication, intrusion detection, etc.
    - Handshake phase is most vulnerable

- EU legislation on privacy implemented 05/2018
  - Calls for *privacy-by-design* approaches
  - Requests *privacy risk analysis*
  - Calls for *data minimization principle* for processing of personal data

enhance technology trust, security, resilience…

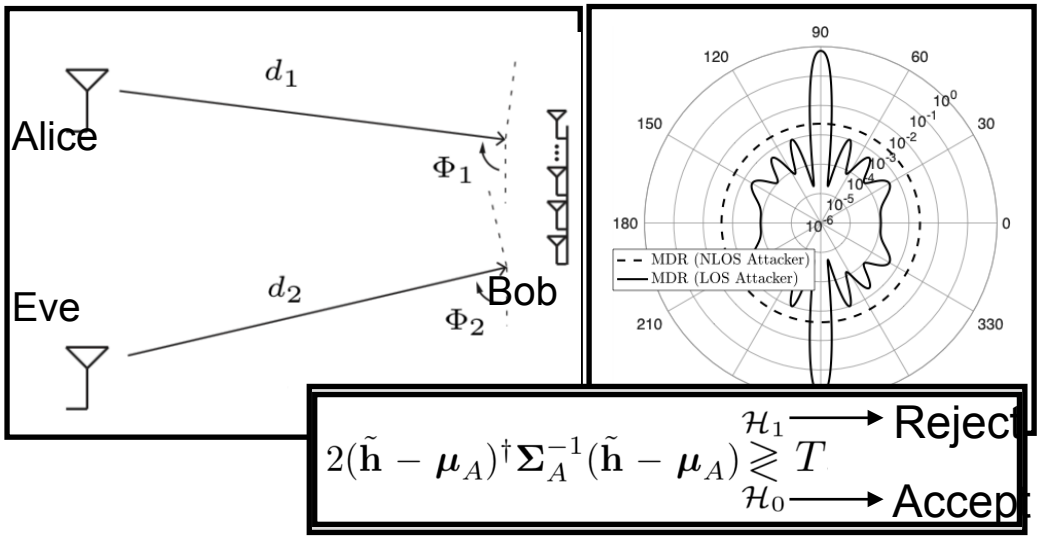
Physical Layer Authentication –
Ex: Use Channel State Information for Intrusion Detection

- Lightweight & secure authentication

”reduced security overhead” ”fast authentication”

mMTC ⟵ 5G ⟶ URLLC

”resilience against impersonation attacks”



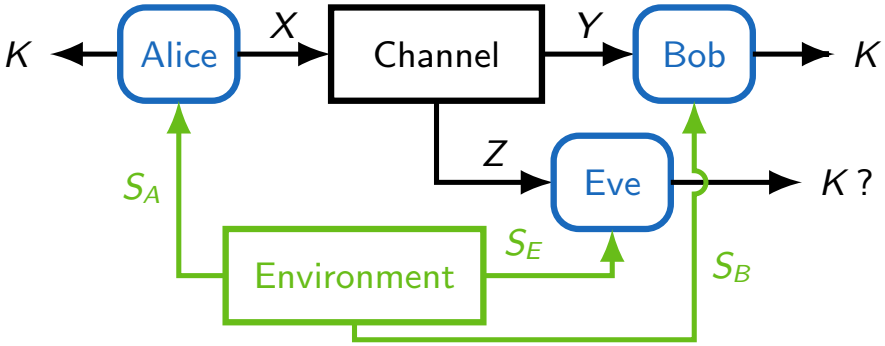
(Massive) machine type communication

- Complexity matters
- Latency matters

H. Forssell, R. Thobaben, H. Al-Zubaidy, and J. Gross, “Physical layer authentication in mission-critical MTC networks: A security and delay performance analysis,” submitted to J-SAC 2018, available ArXiv

Crucial for Security: Secret Key Generation

- Frequent renewal of keys for critical networks
- Computational hardness assumption may become questionable (Shor algorithm + quantum computers)
  - One-time pad is quantum-safe



- **Key generation:** Nearby devices with sensing capabilities could exploit the correlation among measurements as way to generate a key

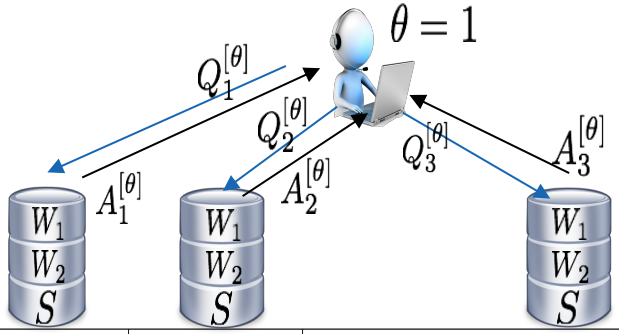
G. Bassi, P. Piantanida, and S. Shamai, “Secret Key Generation over Noisy Channels with Correlated Sources,” arXiv:1609.08330 [cs, math], Sep. 2016.

Private Information Retrieval

Design of framework, codes & Fundamental bounds

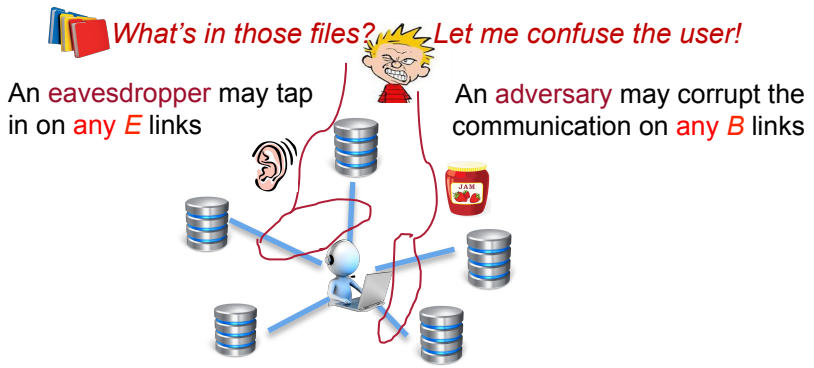
PIR: To retrieve a message
without revealing the interest in that message

$$I\Big(\underbrace{\text{Information available to database/server (messages, queries, answers)}}\ ;\ \underbrace{\text{the requested message index}}\Big) = 0$$



Server 1	Server 2	Server 3
$a_1 + r$	$a_3 + r$	$a_1 + a_3 + r$
$b_1 + s$	$b_3 + s$	$b_3 + (b_4 - b_2) + s$
$a_2 + b_2 + t$	$a_4 + b_4 + t$	$(a_2 + a_4) + (b_3 - b_1) + (2b_4 - b_2) + t$

Security (adversary/eavesdropper):

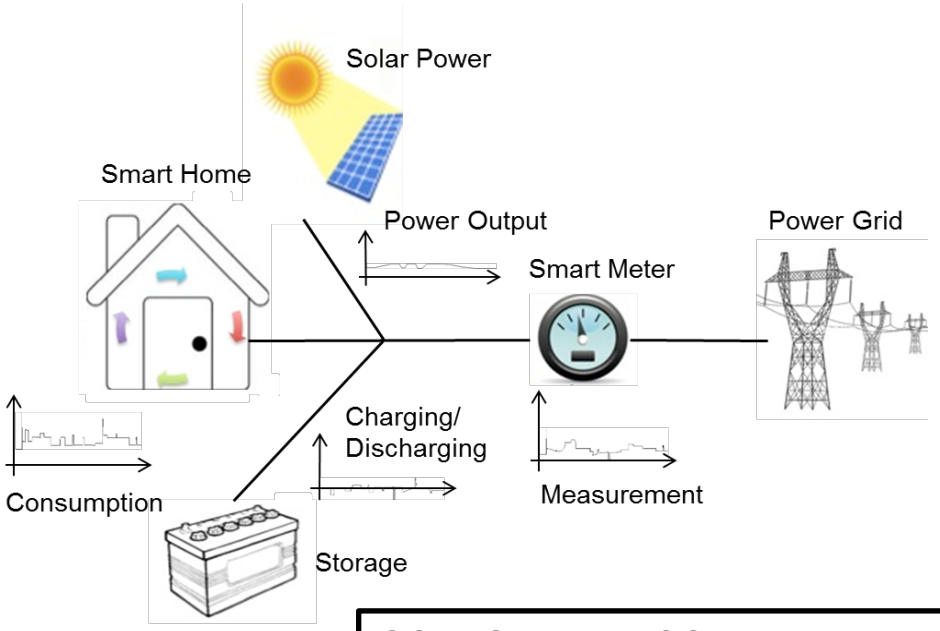


Qiwen Wang, Hua Sun and Mikael Skolgund. "The capacity of private information retrieval with eavesdroppers." Accepted by *IEEE Transactions on Information Theory* (2018)

Smart Meter Privacy

Ex. for privacy-by-design in control

- Energy consumption profile reveals personal information
  - PET by load signature manipulation
- Design of privacy preserving energy control strategies
- Privacy risk?
  - What is the right measure?



COPES project: COnsumer-centric Privacy in smart Energy gridS

Z. Li, T. J. Oechtering and D. Gunduz. “Privacy against a Hypothesis Testing Adversary,” to appear *IEEE Transactions on Information Forensics and Security.*