UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR IT SECURITY

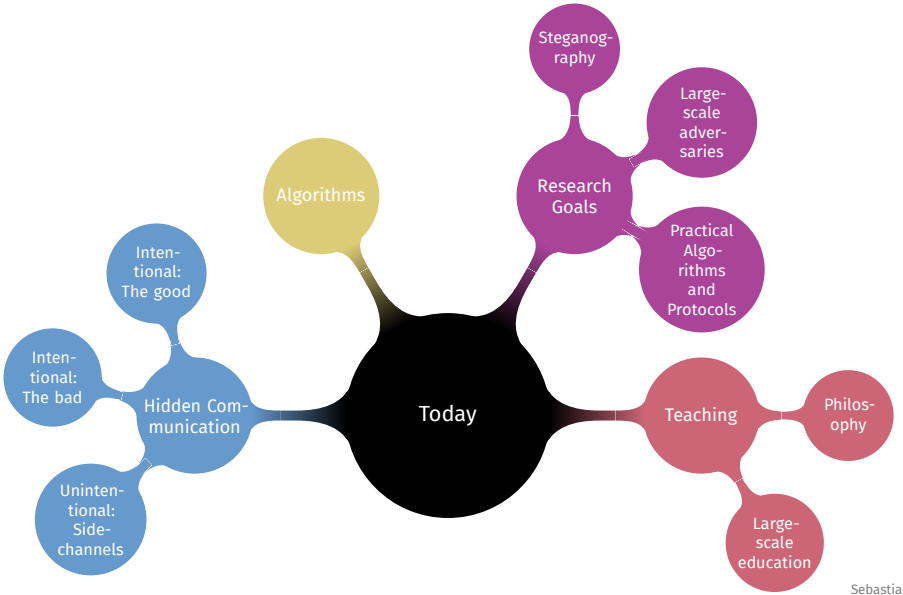
# The many facets of hidden communication

Sebastian Berndt

Institute for IT Security
University of Lübeck

IM FOCUS DAS LEBEN

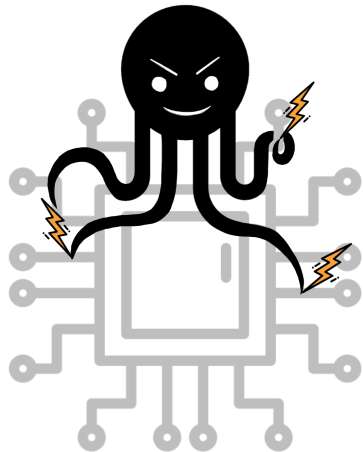
# Overview


Today
Algorithms
Research Goals
Steganography
Large-scale adversaries
Practical Algorithms and Protocols
Hidden Communication
Intentional: The good
Intentional: The bad
Unintentional: Side-channels
Teaching
Philosophy
Large-scale education

# Recent Research: Hidden communication

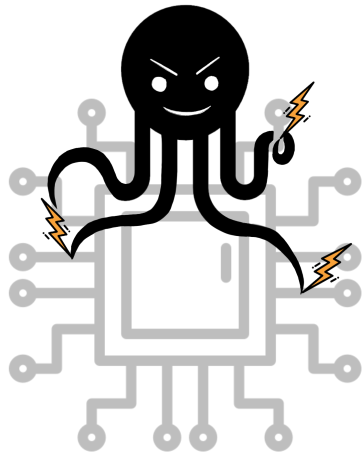
# Unintentional Communication: Side-channels

- *Implementation* leaks sensitive information via side-channels (Power consumption, Timing, etc.)



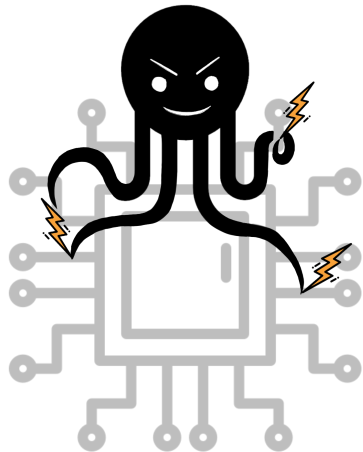
# Unintentional Communication: Side-channels

- *Implementation* leaks sensitive information via side-channels (Power consumption, Timing, etc.)
- Attacks and countermeasures for general MPC-in-the-head constructions **[CCS 2020]**



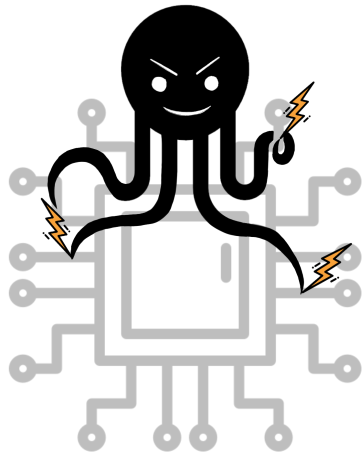
# Unintentional Communication: Side-channels

- *Implementation* leaks sensitive information via side-channels (Power consumption, Timing, etc.)
- Attacks and countermeasures for general MPC-in-the-head constructions **[CCS 2020]**
- Attacks and countermeasures for Picnic, a NIST PQC alternate **[CHES 2021]**



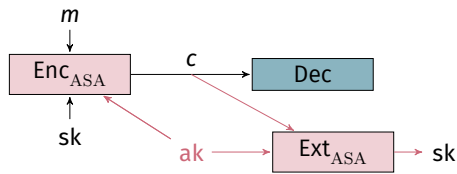
# Unintentional Communication: Side-channels

- *Implementation* leaks sensitive information via side-channels (Power consumption, Timing, etc.)
- Attacks and countermeasures for general MPC-in-the-head constructions **[CCS 2020]**
- Attacks and countermeasures for Picnic, a NIST PQC alternate **[CHES 2021]**
- Attacks against base64 decoding of RSA keys (includes OpenSSL, Botan, NSS, wolfSSL, ...) **[CCS 2021]**



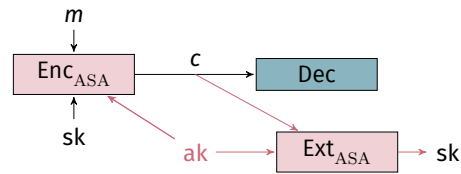
# Intentional Communication: The bad

- Large-scale adversaries can provide *subverted* implementations to leak sensitive information



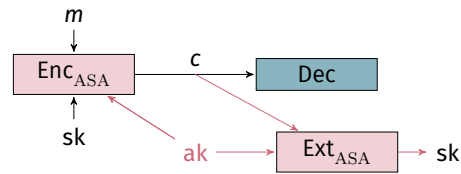
# Intentional Communication: The bad

- Large-scale adversaries can provide *subverted* implementations to leak sensitive information
- Attacks against widely used protocols (TLS, Signal, WireGuard) **[AsiaCCS 2022]**



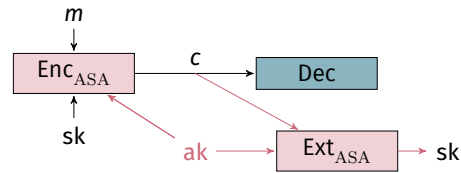
# Intentional Communication: The bad

- Large-scale adversaries can provide *subverted* implementations to leak sensitive information
- Attacks against widely used protocols (TLS, Signal, WireGuard) **[AsiaCCS 2022]**
  - Signal does not have post-compromise security **[DIMVA 2021]**



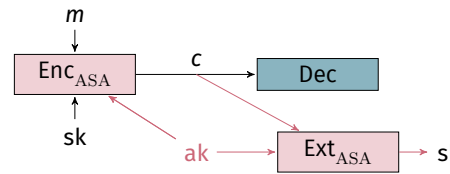
# Intentional Communication: The bad

- Large-scale adversaries can provide *subverted* implementations to leak sensitive information
- Attacks against widely used protocols (TLS, Signal, WireGuard) **[AsiaCCS 2022]**
  - Signal does not have post-compromise security **[DIMVA 2021]**
- *Efficient* countermeasures for authenticated encryption **[2022]**



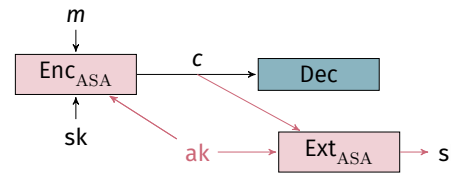
# Intentional Communication: The bad

- Large-scale adversaries can provide *subverted* implementations to leak sensitive information
- Attacks against widely used protocols (TLS, Signal, WireGuard) **[AsiaCCS 2022]**
  - Signal does not have post-compromise security **[DIMVA 2021]**
- *Efficient* countermeasures for authenticated encryption **[2022]**
- Upper bounds on transmission rate **[2022]**



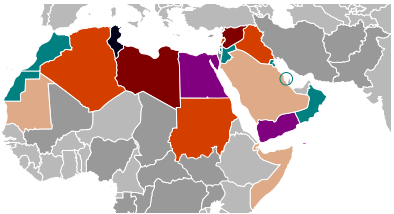
# Intentional Communication: The bad

- Large-scale adversaries can provide *subverted* implementations to leak sensitive information
- Attacks against widely used protocols (TLS, Signal, WireGuard) **[AsiaCCS 2022]**
  - Signal does not have post-compromise security **[DIMVA 2021]**
- *Efficient* countermeasures for authenticated encryption **[2022]**
- Upper bounds on transmission rate **[2022]**
- Earlier: Can be seen as steganography **[CCS 2017]**



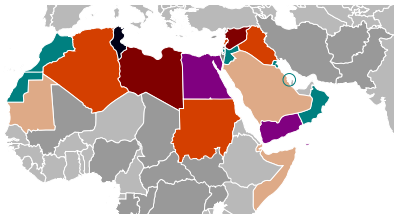
# Intentional Communication: The good

- *Steganography* is used to hide communication (not only content)



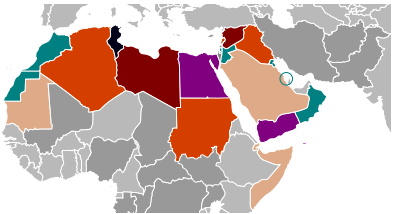
# Intentional Communication: The good

- *Steganography* is used to hide communication (not only content)
- Public key communication over blockchains **[2022]**



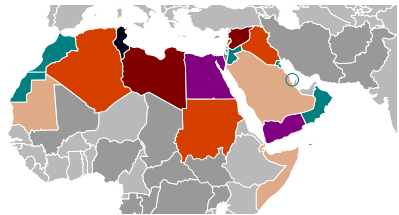
# Intentional Communication: The good

- *Steganography* is used to hide communication (not only content)
- Public key communication over blockchains **[2022]**
- Implementation of covert MPC **[2022]**



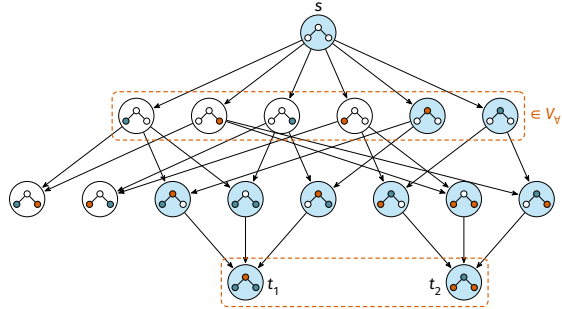
# Intentional Communication: The good

- *Steganography* is used to hide communication (not only content)
- Public key communication over blockchains **[2022]**
- Implementation of covert MPC **[2022]**
- Earlier: Limits of public-key steganography **[Eurocrypt 2018]**, Limits of universal steganography **[ISAAC 2016, IH&MMSec 2015]**, Communicate via patterns **[LATA 2016]**



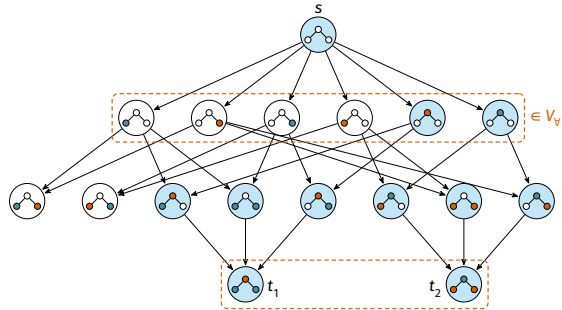
# Algorithms

- Structure of integer programs **[SOSA 2021, SOFSEM 2021]**



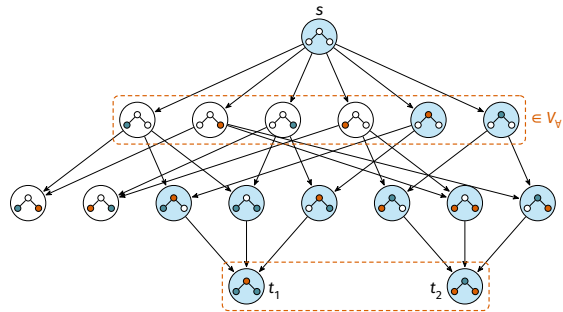
# Algorithms

- Structure of integer programs **[SOSA 2021, SOFSEM 2021]**
- Parameterized algorithms for operations research **[CIE 2021, MFCS 2020]**



# Algorithms

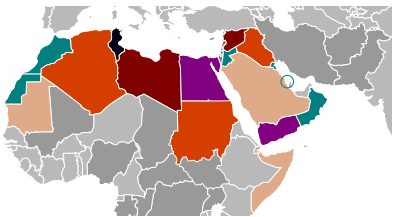
- Structure of integer programs **[SOSA 2021, SOFSEM 2021]**
- Parameterized algorithms for operations research **[CIE 2021, MFCS 2020]**
- Efficient implementation of *theoretical* algorithms **[ALENEX 2022, IPEC 2020]**



# Long-term Research Goals: Combine Theory and Practice

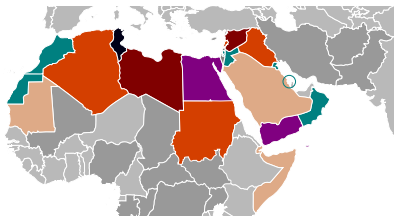
# Steganography

- Develop *usable* steganographic systems for *realistic* covert channels



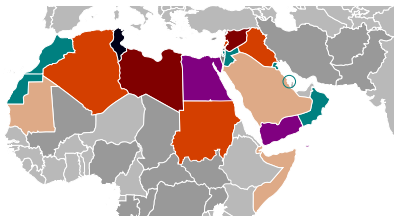
# Steganography

- Develop *usable* steganographic systems for *realistic* covert channels
- Combine practical steganography (realistic channels) and theoretical steganography (provable security) **Security for data**



# Steganography

- Develop *usable* steganographic systems for *realistic* covert channels
- Combine practical steganography (realistic channels) and theoretical steganography (provable security) **Security for data**
- Understand application scenarios and restrictions **Data for security**



# Large-Scale Adversaries

- Develop *realistic* threat models of large-scale adversaries

# Large-Scale Adversaries

- Develop *realistic* threat models of large-scale adversaries
- Understand possible attack vectors

# Large-Scale Adversaries

- Develop *realistic* threat models of large-scale adversaries
- Understand possible attack vectors
- Develop and analyze *usable* countermeasures

# Practical Algorithms and Protocols

- Make theoretical algorithms/protocols *usable* in the real-world

# Practical Algorithms and Protocols

- Make theoretical algorithms/protocols *usable* in the real-world
- Integrate real-world constraints into theoretical models

# Practical Algorithms and Protocols

- Make theoretical algorithms/protocols *usable* in the real-world
- Integrate real-world constraints into theoretical models
- Provide clear theoretical explanations of real-world behavior (Machine Learning)

# Practical Algorithms and Protocols

- Make theoretical algorithms/protocols *usable* in the real-world
- Integrate real-world constraints into theoretical models
- Provide clear theoretical explanations of real-world behavior (Machine Learning)
- I enjoy collaboration
  (> 30 co-authors from > 7 countries)

# Teaching Visions

# Show the path

- Show the *path*, not just the end

# Show the path

- Show the *path*, not just the end
- Work together to create *constructive* environment

# Show the path

- Show the *path*, not just the end
- Work together to create *constructive* environment
- Allow students to do real research

# Show the path

- Show the *path*, not just the end
- Work together to create *constructive* environment
- Allow students to do real research
- Wide range of interest:

# Show the path

- Show the *path*, not just the end
- Work together to create *constructive* environment
- Allow students to do real research
- Wide range of interest:
  - security

# Show the path

- Show the *path*, not just the end
- Work together to create *constructive* environment
- Allow students to do real research
- Wide range of interest:
  - security
  - algorithms

# Show the path

- Show the *path*, not just the end
- Work together to create *constructive* environment
- Allow students to do real research
- Wide range of interest:
  - security
  - algorithms
  - theory

# Show the path

- Show the *path*, not just the end
- Work together to create *constructive* environment
- Allow students to do real research
- Wide range of interest:
  - security
  - algorithms
  - theory
  - math

# Show the path

- Show the *path*, not just the end
- Work together to create *constructive* environment
- Allow students to do real research
- Wide range of interest:
  - security
  - algorithms
  - theory
  - math
  - ...

# Large-scale education

- Use *active* teaching: requires smaller groups

# Large-scale education

- Use *active* teaching: requires smaller groups
- Use *experts* wisely

# Large-scale education

- Use *active* teaching: requires smaller groups
- Use *experts* wisely
  - Flipped classroom

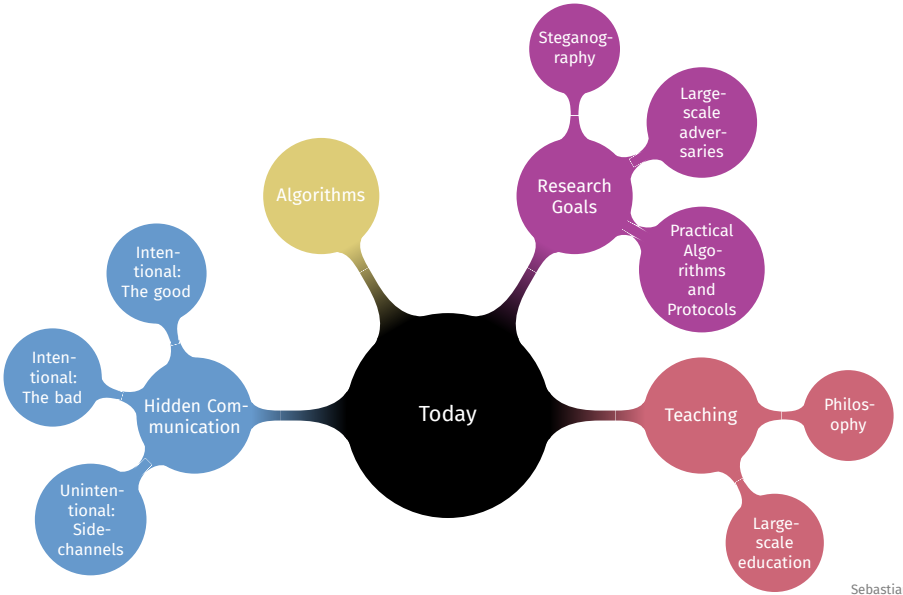
# Large-scale education

- Use *active* teaching: requires smaller groups
- Use *experts* wisely
  - Flipped classroom
  - Problem-based learning

# Large-scale education

- Use *active* teaching: requires smaller groups
- Use *experts* wisely
  - Flipped classroom
  - Problem-based learning
- Use the lessons from the online semesters

# Summary


Today
Algorithms
Hidden Communication
Intentional: The good
Intentional: The bad
Unintentional: Side-channels
Research Goals
Steganography
Large-scale adversaries
Practical Algorithms and Protocols
Teaching
Philosophy
Large-scale education