Karlsruhe Institute of Technology

KASTEL

Student Worker (Hiwi)

Real World Implementation of Anamorphic Channels

KASTEL Security Research Labs (C&C)

Welcome to the KASTEL Security Research Labs and the Topic "Engineering Secure Systems" (ESS) of the Helmholtz Association. Within the research group of Cryptographic Protocols, we are currently working on the recently emerging topic called *Anamorphic Cryptography* [PPY22] [BGHM+23] [KPPY+23] which considers a powerful authoritarian government who constantly surveils secret communication between its citizens by demanding their private keys, while the citizens use covert anamorphic channels within regular channels to communicate secret anamorphic messages. Our current project is two-fold. In a recent work, we developed a methodology [BPRS25] to embed anamorphic channels within well-known simple standardized cryptographic protocols such as, ElGamal, Regev, BBS Signatures and Waters Signatures. The first part of this project is to adapt, integrate and implement this methodology over popular open-source messaging applications such as Signal. The second part of the project considers implementing anamorphic channels within Code-based communication.

We Offer:

- Opportunity to contribute to scientific publications
- Close supervision and support

Scope and Requirements:

- Bachelors in Computer Science student
- Identify new security aspects of anamorphic cryptography within Anamorphic Code-based communication
- Familiarity with popular encryption and signature schemes
- Familiarity with Information Coding Theory
- Familiarity with programming languages, such as C and Python
- Familiarity with networking protocols

"BIG BROTHER IS WATCHING YOU"

How to protect your data from the BIG BROTHER?

Tasks:

- Get an overview of Anamorphic Cryptography
- Design and Implementation of anamorphic channels over Signal.
- Design and Implementation of anamorphic channels within Codes and its applications.
- Design Android applications based on the above implementations.

Contact emails: tapas.pal@kit.edu, shalini.banerjee@kit.edu

Please include your CV in the application.

References:

[PPY22]: Perisano, Phan and Yung. "Anamorphic Encryption: Private Communication against a Dictator." EUROCRYPT 2022.

[BGHM+23]: Banfi et al. "Anamorphic Encryption, Revisited." EUROCRYPT 2024.

[KPPY+23]: Kutylowski et al. "Anamorphic Signatures: Secrecy From a Dictator Who Only Permits Authentication!" CRYPTO 2023.

[BPRS25]: Banerjee et al. "Simple Public Key Anamorphic Encryption and Signature using Multi-Message Extensions." EPRINT 2025/370 (https://iacr/2025/370).