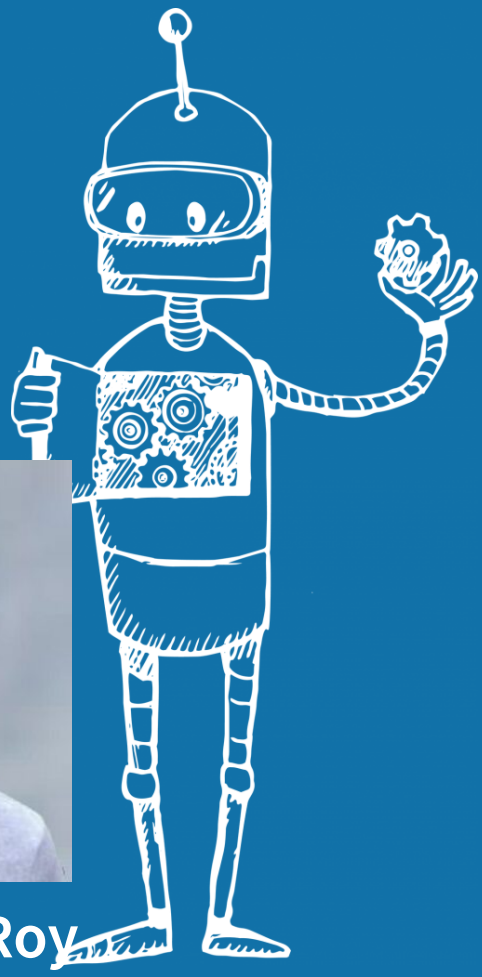
System Security

Team Gruss

Team Mangard

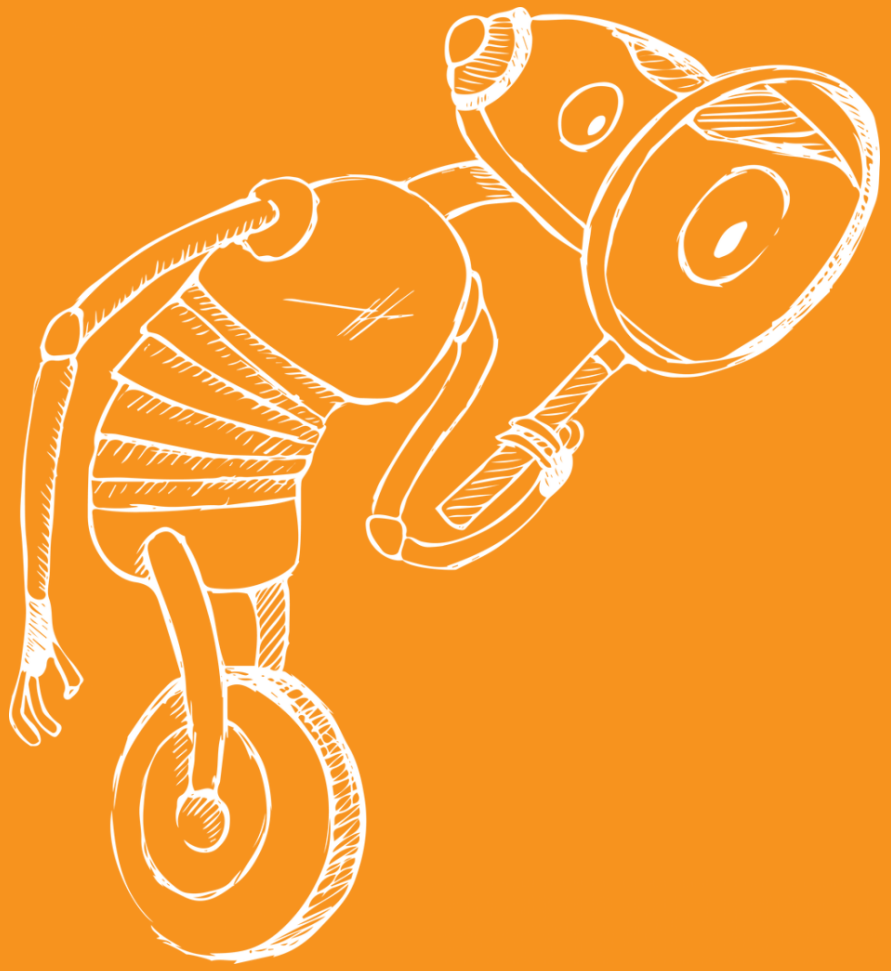
Team Sinha Roy

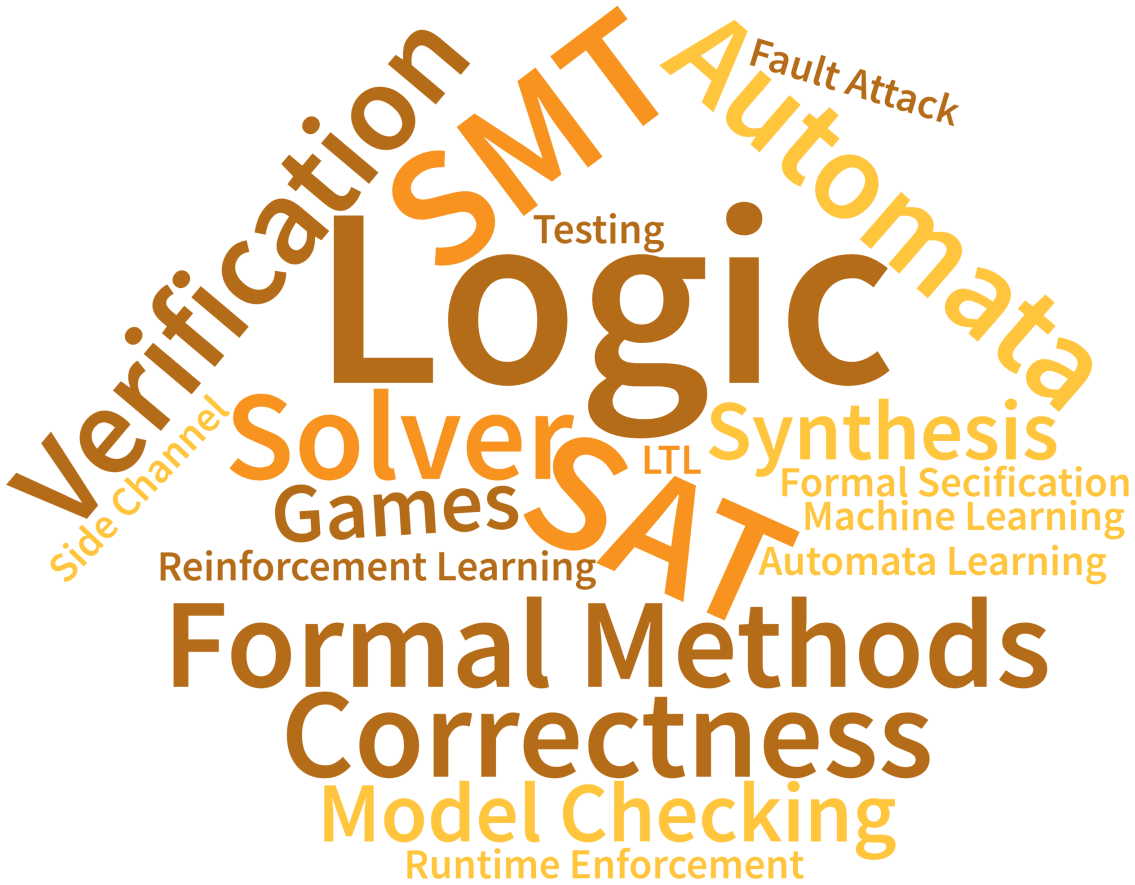


Control Flow Integrity
Power Analysis
Hardware Design
Countermeasures
System Security
ZombieLoad
Intel
Crypto Implementations
Rowhammer
Timing
Microarchitecture
Process Isolation
Spectre
Operating Systems
Sandbox
Cache
Meltdown
Software Security
Attacks
Defenses
Fault Attacks
Compiler Construction
Post-Quantum Crypto
Secure Implementations
RISC-V
Symmetric Cryptography
Secure Enclaves

Formal Methods

Team Bloem

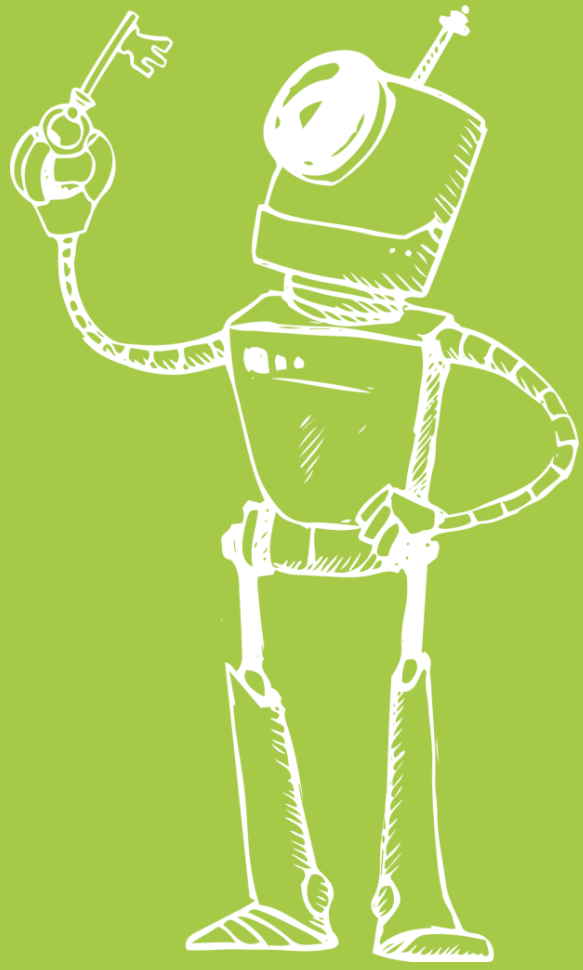



Verification
SMT
Automata
Fault Attack
Testing
Logic
Solver
Synthesis
Side Channel
LTL
Formal Secification
Games
SAT
Machine Learning
Reinforcement Learning
Automata Learning
Formal Methods
Correctness
Model Checking
Runtime Enforcement

Cryptology & Privacy

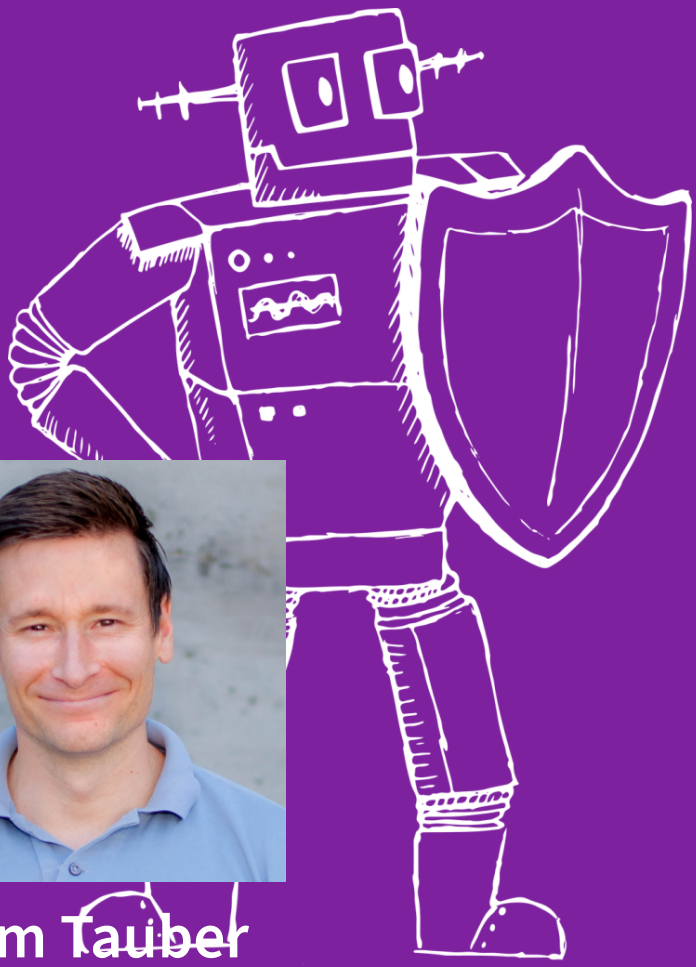
Team Eichlseder

Team Rechberger



Cryptanalysis
Multi-Party Computation
secure
key
Private AI
brute-force
MPC
Cryptography
lightweight
symmetric
Ascon
attack
Cipher
Privacy
PETs
FHE
Crypology
exercises
misuse
Encryption
Post-Quantum Cryptography
implementation
Homomorphic Encryption
Cloud Computing
competition

Secure Applications

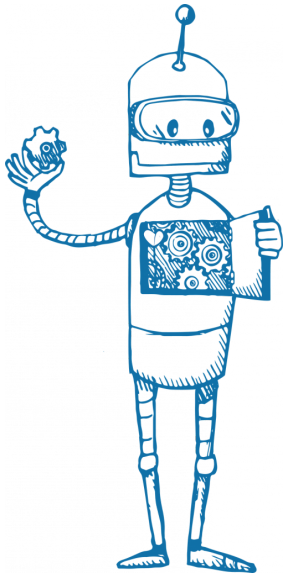


Team Leitold

Team Lipp

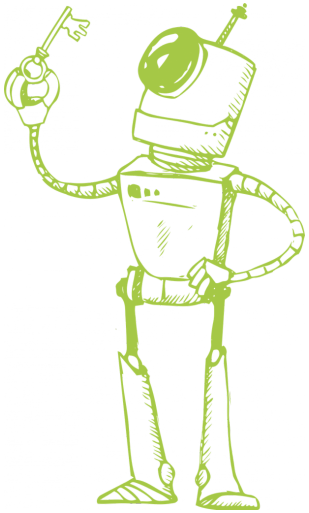
Team Tauber

Public Key Infrastructure
Blockchain
Mobile Signature
Electronic Identity (eID)
Digital Education
Secure Applications
Applied Cryptography
Identity
IPFS
eIDAS Regulatiuon
mGovernment
Certificates
Credentials
Identity Protocols
eGovernment
Trust Management
Trust
Identity Models
Citizen Card
Cross-border Authentication
Trust Service Provider



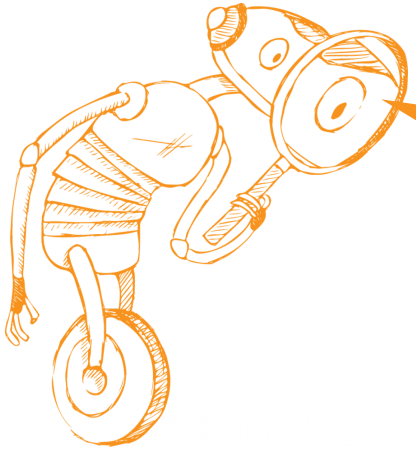
System Security

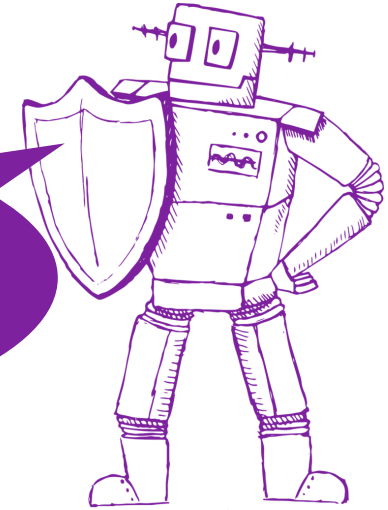
Cryptology & Privacy



#isw

https://discord.gg/ypDW5fKHSC



Formal Methods

Secure Applications