



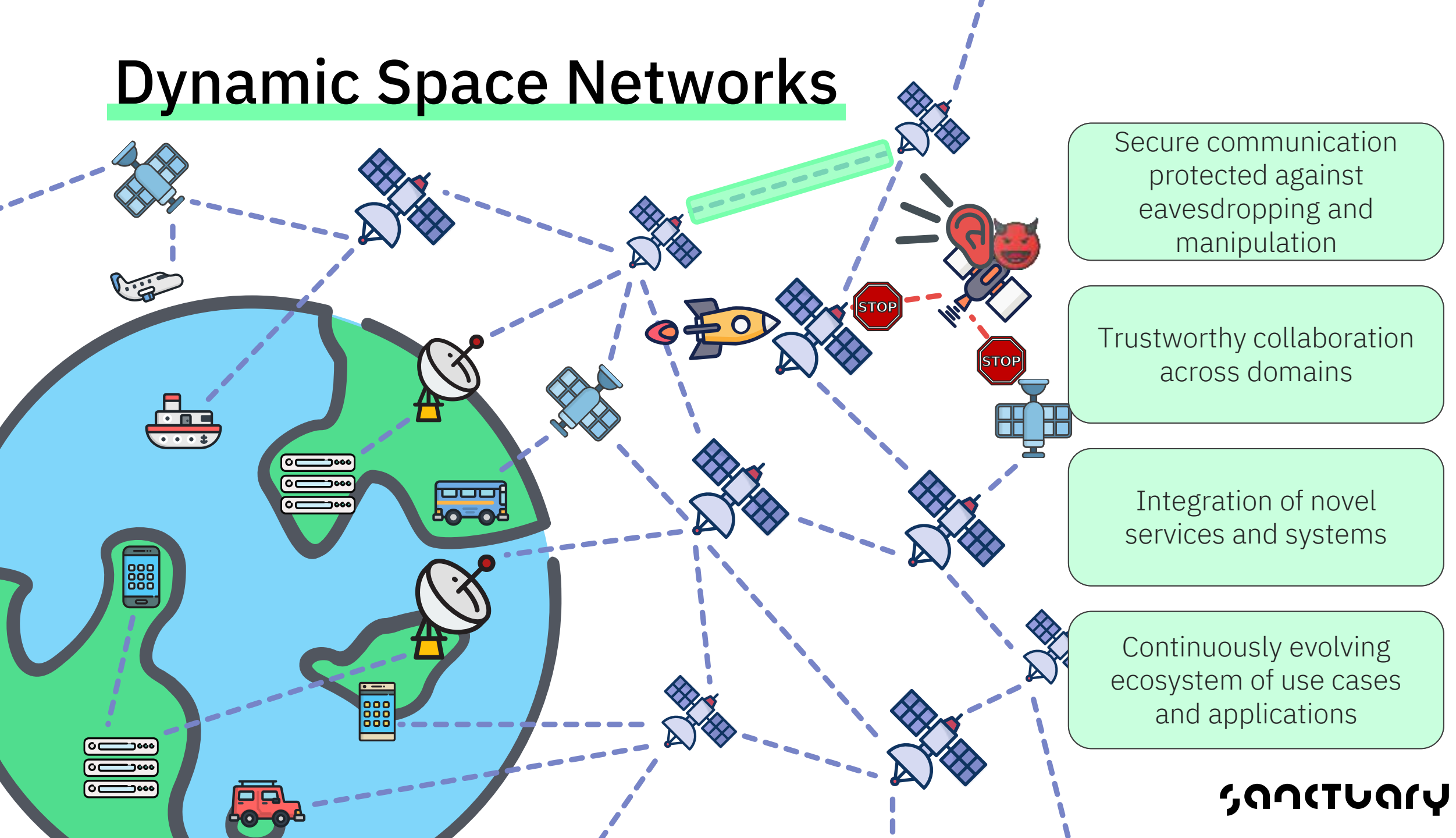
SHED-SPKI: Scalable Public Key Infrastructure for Large Constellation Secure Communications

Dr.-Ing. Ferdinand Brasser

Scalable Public Key Infrastructure for Large Constellation Secure
Communications ESA Contract No. 4000143927/24/NL/RK

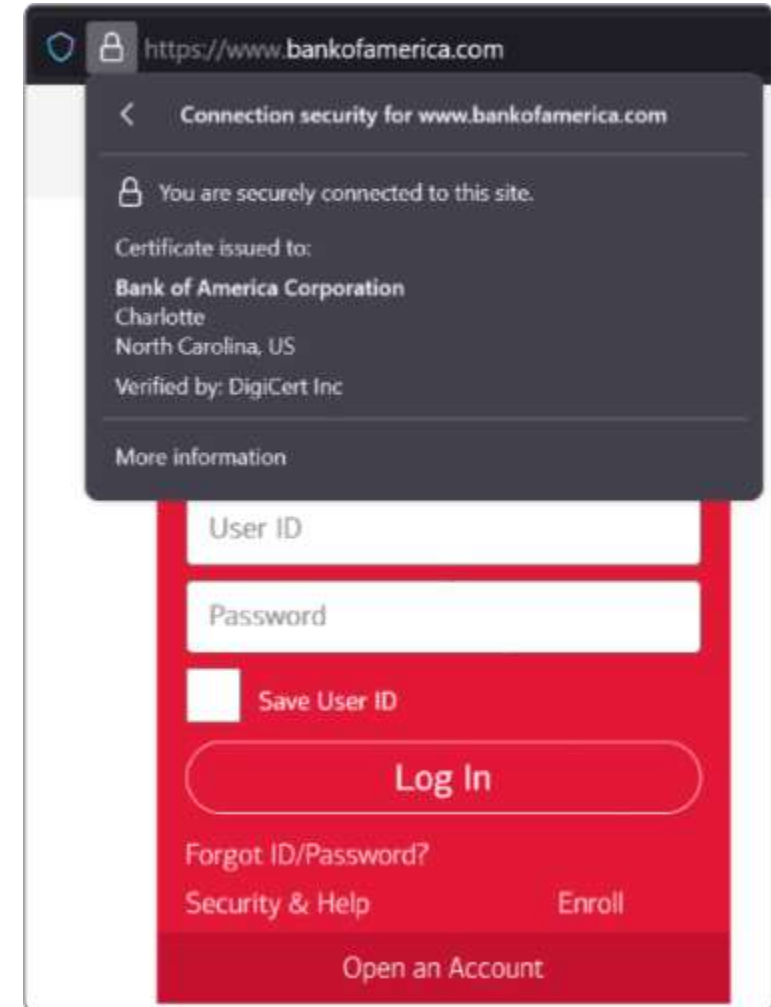


Dynamic Space Networks

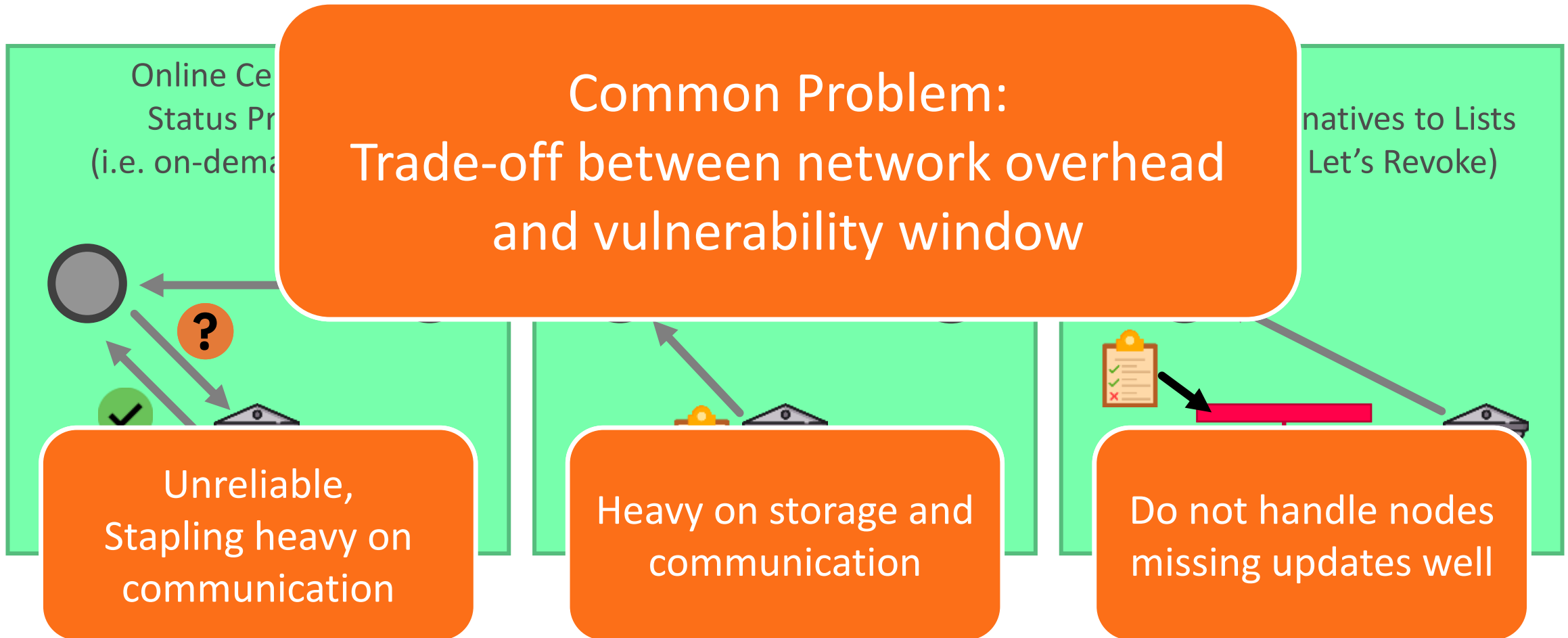


Scalable Secure Communication

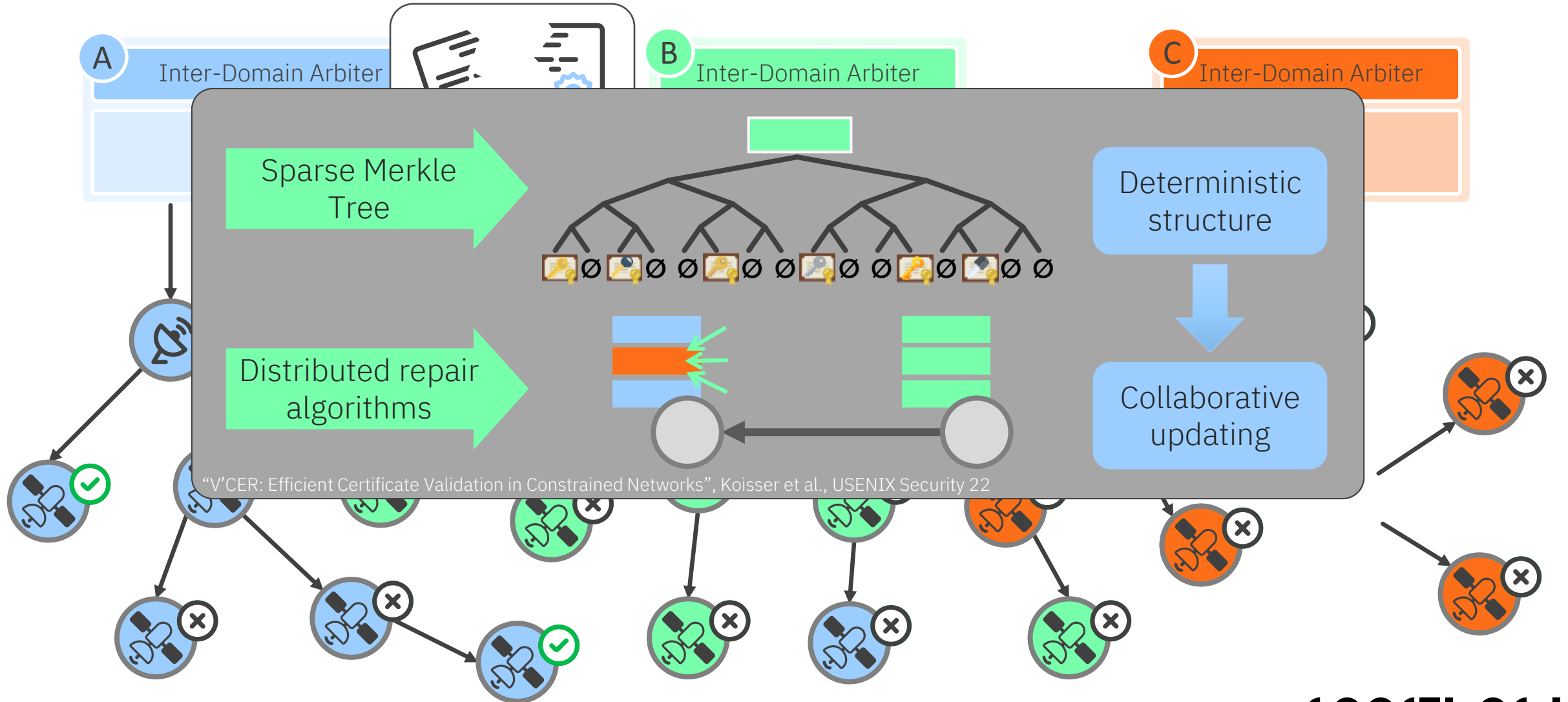
- Asymmetric cryptography enables secure communication without pre-shared keys
 - Public keys can be shared openly over untrusted channels
 - Symmetric session key established via handshake protocol
- Handshake relying on the correct public key
 - Ensuring authenticity and integrity of public keys is essential
 - Handshake protocol needs to be efficient
- Public Key Infrastructure (PKI) provides an internet-proven trust framework
- TLS1.3 provides a standardized and flexible handshake protocol



Existing Revocation Checks



Scalable PKI: Epidemic Revocation



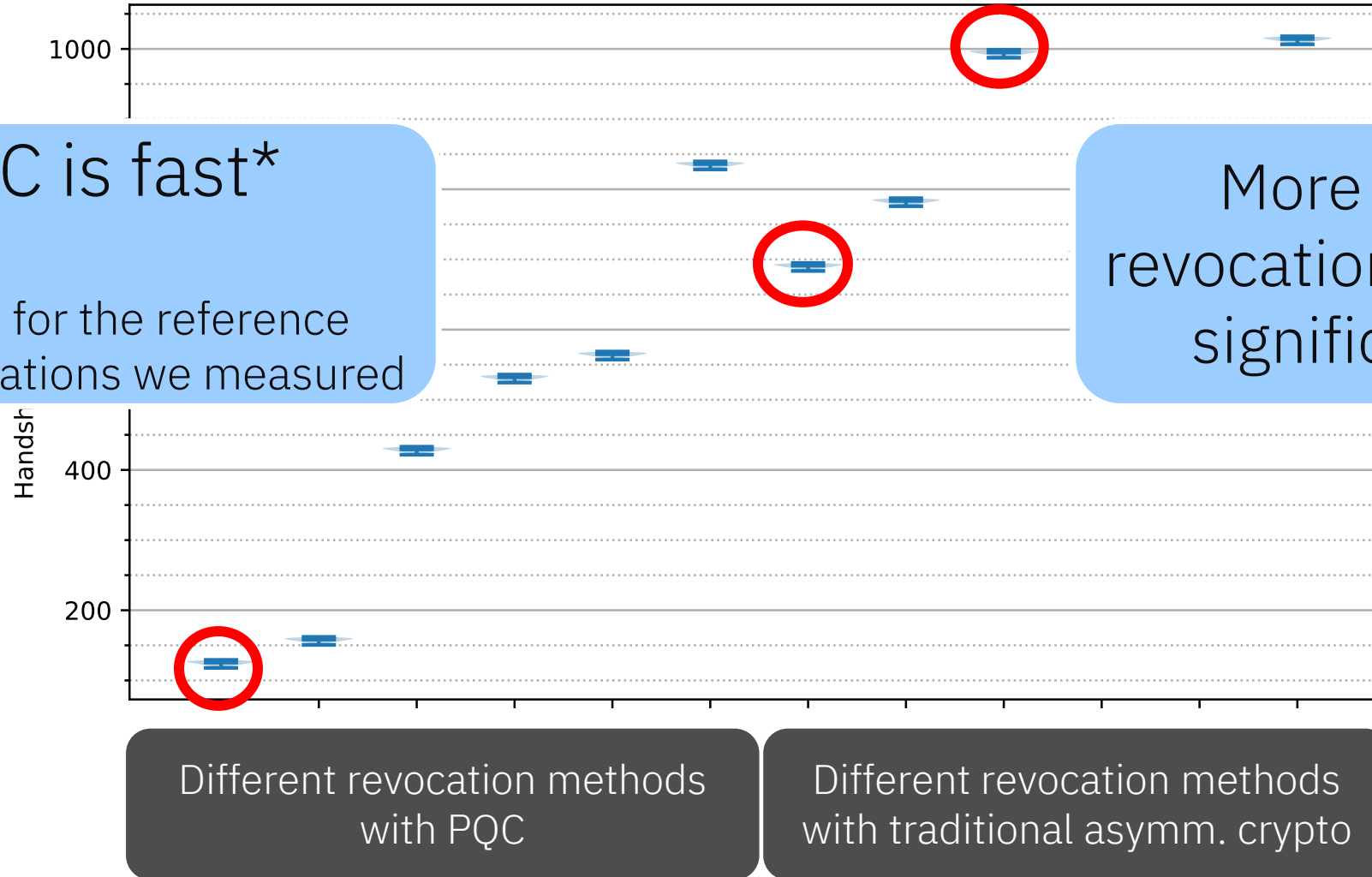
Experiments and KPIs

Handshake Delay

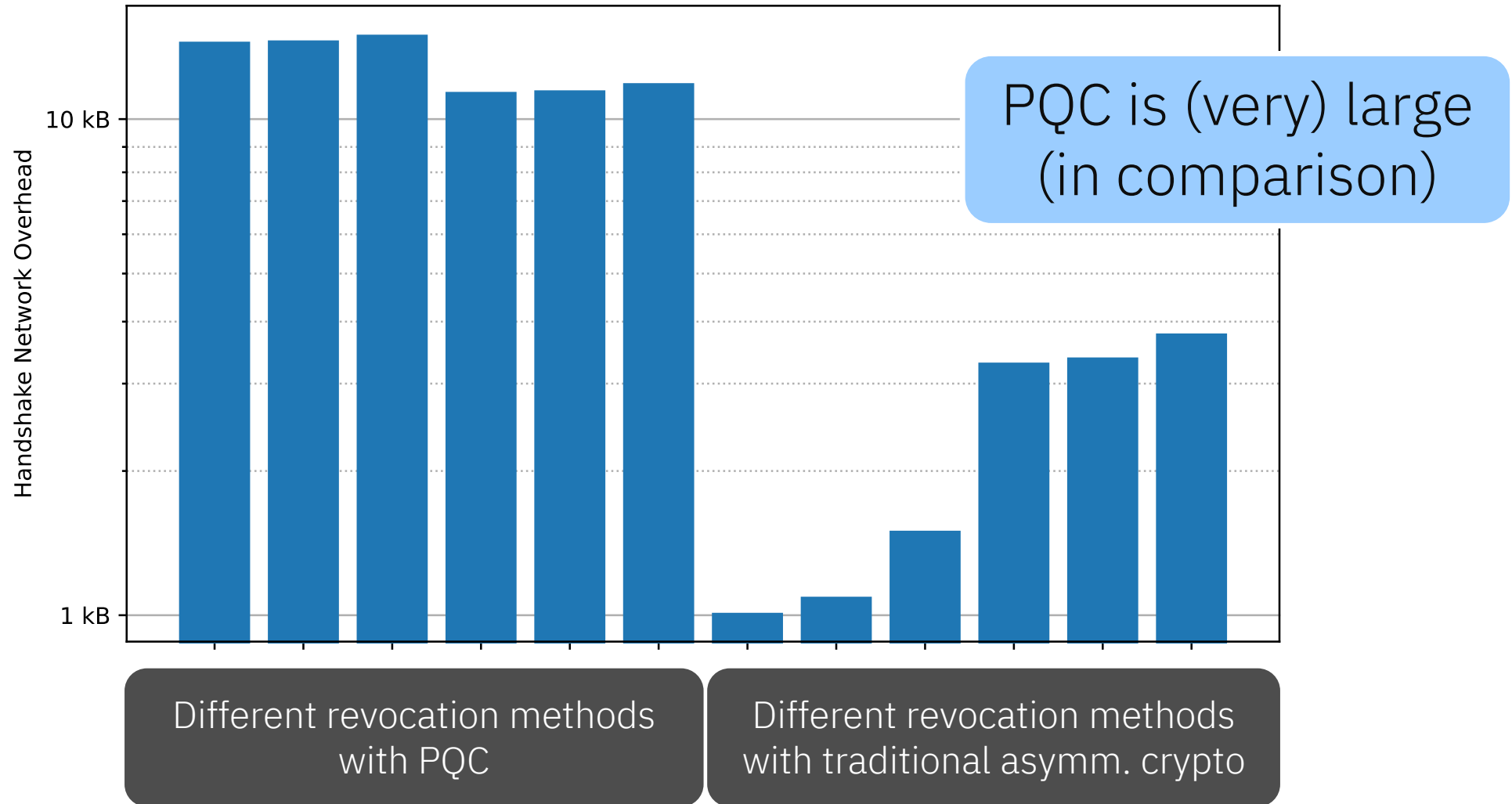
PQC is fast*

*at least for the reference implementations we measured

More complex revocation check adds significant delay



Handshake Bytes



CyberCUBE Experiments

TLS 1.3 with Mutual Authentication

- Measure the performance of a full TLS 1.3 handshake between the satellite and the ground station.
- Metrics: Computational time
Memory usage
Processing load

Cryptographic Primitives


- Assess the performance of classical and PQC algorithms in core cryptographic operations
- Operations: Key generation
Signing
Signature verification
Key exchange


Revocation Strategies and Operations

- Evaluate the efficiency of certificate revocation mechanisms
- Operations: Verification of Merkle Tree Proof-of-Inclusion (PoI)
Application of PoI revocation updates
Processing of *Let's Revoke* Updates




SANCTUARY Systems GmbH

 Robert-Bosch-Str. 7, D-64293 Darmstadt

 info@sanctuary.dev

 www.sanctuary.dev

 www.linkedin.com/company/sanctuary-dev/

Fuzzing Security Designs
Attestation

IP Protection

Secure Boot

Public Key Infrastructures

SBOM

CVE Scanning

Real-time Hypervisor

OT Asset Management

Arm TrustZone

TPM

Zero Trust Concepts