

Tobias Heider: Profile

- Crypto Systems Development
@genua
- OpenIKED Developer
@OpenBSD
- IPsec IETF Work:
 - Minimal G-IKEv2: Group based key exchange for constraint settings
 - Hybrid PQKE in IKEv2



Research Question

- Secure encrypted network communication (for everyone).
 - Encrypted communication in constrained environments (IoT)
 - High-speed networking and hardware offloading
 - Cryptographic agility and mitigations against future threats (PQKE)