QuNET - Quantentechnologien für sichere Netze

Eine vom Bundesministeriums für Bildung und Forschung geförderte Initiative der Fraunhofer-Gesellschaft,
des Deutschen Zentrums für Luft- und Raumfahrt und der Max-Planck-Gesellschaft

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Erster QuNET-Partnerworkshop
Stand 05.03.2021

Andreas Tünnermann
Fraunhofer-Institut für Angewandte Optik
und Feinmechanik IOF

Martin Schell
Fraunhofer Heinrich-Hertz-Institut HHI

Christoph Günther
Deutsches Zentrum für Luft- und Raumfahrt
Institut für Kommunikation und Navigation DLR-IKN

Gerd Leuchs
Max-Planck-Institut für die Physik des Lichts MPL

QuNET – Fehlbedarfe

Höchste Priorität – Projektbeginn so früh wie möglich

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Nanowire/SNSPD Detektoren (+ Kryo-Hardware für 19‘‘-Rack-kompatible Detektionssysteme)

C-Band Wellenlänge (ggf. angepasst auf SE2); Je nach Anwendungsszenario: multi-channel, ultra-low-noise (für QKD-Backbones), ultra-low-jitter (e.g. <50ps, High-dimensional QI), Transceiver mit Kryo-integrierten Einzelphotonenquellen, CE-zertifiziert, UL-zertifiziert, ROHS, Herstellungsstandort in D / Betrachtung der Supply-Chain.

Dazu passend: Kryostat-Hardware für 19‘‘ Rack Detektionssysteme: kompakt, wartungsarm, Potential für low cost / design-to-cost < 20k €, Temp < 4K, 100 pc/pA

Komponenten & Hardware
für QKD

QuNET – Fehlbedarfe

Höchste Priorität – Projektbeginn so früh wie möglich

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Praktische Sicherheitsbeweise & -aspekte (ε-Security, Schnittstelle BSI Anforderungen) & neuartige QKD Protokolle

Sicherheitsbeweise die langfristig Anforderungen an Zulassung-/Zertifizierung erfüllen; Abgestimmtes Konzept/Mapping/Empfehlung (z.B. mit Ergebnis: Paper): ε-Security auf BSI Kriterien.

Untersuchung: Kosten und Umsetzung von Bodenschnittstellen (Freistrahl-QKD)

aus Kundenperspektive Bodenschnittstelle: SWAP, Kosten, Aufwand, Integration der Hardware im Gebäude unter Berücksichtigung der lokalen Sicherheitsaspekte (z.B. Messung im Serverraum vs. Dach, Faserverbindung zum Labor), Standort der Bodenstation

***konzeptionelle & theoretische Arbeiten* im Zusammenhang mit QKD**

QuNET – Fehlbedarfe

Höchste Priorität – Projektbeginn so früh wie möglich

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Schlüsselverwaltung (KMS), SDN-Schnittstellen, Kombination in Verwendung mit symmetrischer Verschlüsselung, inkl. Hardware (e.g. FPGA), Berücksichtigung BSI Anforderungen

die langfristig Zulassungs-/Zertifizierungsstellen zufriedenstellen; z.B. Integration der informationstheoretischen Sicherheit in etablierte Sicherheitsmodelle; Einfache Handhabung, Quantum-safe; Schnittstellen und Protokolle gemäß ISO/ITU/Common Criteria/ETSI-SDN; dies soll auch Studien und konzeptionelle Vorarbeiten enthalten

QKD Post-Processing Implementation / Stack

in Software und/oder HDL, Informations-theoretische Sicherheit, QKD-Protokoll-Agil, Szenario-Agil, Parameter-Monitoring-Funktionalitäten, (FPGA-fähig), ggf. open source

***Software* für den Einsatz von QKD**

QuNET – Fehlbedarfe

Mittlere Priorität – Projektbeginn eher in 1-2 Jahren

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Deterministische Ein- und Multi-Qubit-Quellen (deterministische Photonenquellen)

Rate/bandwdith ratio, optimiert für BB84 (in einem QKD-relevanten Wellenlängenbereich, e.g. Telekom-Band, (vergleichbare/Aussicht auf Performanz eines decoy-Systems))

elektrooptische Komponenten für QKD-Systeme

ULL Phasenmodulator, < 0.5 dB IL, < V_pi < xx V, C-Band

Komponenten Packaging

gemäß Design und Schnittstellenspezifikation, CE-zertifiziert, UL-zertifiziert, ROHS

Komponenten & Hardware für QKD

QuNET – Fehlbedarfe

Niedrige Priorität – Projektbeginn eher in 2-4 Jahren

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

nichtlineare Kristalle

weites Frequenzspektrum, anpassbares phase matching

Handheld QKD Komplett-Systeme

geeignet für Schlüsseltankstellen

Entwicklung von integrierten Schaltkreisen

ASICs basierend auf vorangegangenen HDL-Implementierungen

Vertrauenswürdige Platformen (klass. Hardware & Software)

Gesamtarchitektur & Sicherheitsaspekte, Freistrahl, Faser, Komponenten & Schnittstellen

SDN-Optische Router

ETSI SDN-Standard, Szenarioanalyse, Anforderungen aus QKD&Q-Repeater-Protokollen (protokollagnostisch!)

Komponenten & Hardware
für QKD

QuNET – Fehlbedarfe

Mittlere Priorität – Projektbeginn eher in 1-2 Jahren

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

"Consulting" HW + mechanische Sicherheit (+ Seitenkanäle)

Untersuchung, Projekte zur Analyse der Systeme / Konzepte hinsichtlich klassischer HW-Sicherheit (e.g. *not* Quantum-Hacking). Gemäß BSI/Common Criteria/ISO, Tamper evident, Tamper resistant, Tamper detection + Response, CSP-Zeroization-Circuit, physische Trennung von CSP-Kanälen und Non-CSP-Kanälen, Robust gegen extreme Bedingungen

"Consulting" SW Sicherheit

Spezifikation des kryptographischen Moduls, der Krypto-Boundary, und kryptographischer Sicherheitsfunktionen. Trennung von Rollen und Services, Rollen-/Identitätsbasierte Authentifikation. Selbst-Tests, Power-up-Tests, Krypto-Algorithmen-Tests, SW/FW-Integritätstests, konditionierte Tests, Zufallszahlengenerierung/Extrahierung, Interne Generierung und Management von Schlüsseln und CSPs, CSP Input/Output/Speicherung/Rotierung, Split-Knowledge Inputs, CSP-zeroization

***konzeptionelle & theoretische Arbeiten* im Zusammenhang mit QKD**

QuNET – Fehlbedarfe

Niedrige Priorität – Projektbeginn eher in 2-4 Jahren

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

-

***konzeptionelle & theoretische Arbeiten* im Zusammenhang mit QKD**

QuNET – Fehlbedarfe

Mittlere Priorität – Projektbeginn eher in 1-2 Jahren

-

QuNET – Fehlbedarfe

Niedrige Priorität – Projektbeginn eher in 2-4 Jahren

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Entity Management System (EMS), Network Management System (NMS) , Teil auch Hardware

einfache Handhabung, Quantum-safe, Schnittstellen und Protokolle gemäß ISO/ITU/Common Criteria, no Vendor-Lock-In

Software für den Einsatz von QKD