



Quantenkommunikation

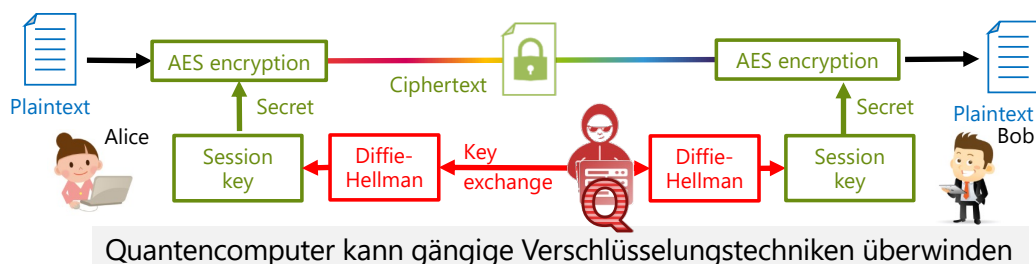
Aus Demonstratoren werden Produkte

Christoph Glingener, Berlin, Juni 2022 – OMNISECURE

ADVA Network Security

1

Einführung



Post-Quantum Cryptography (PQC)

- Rechnerische Sicherheit
- Basierend auf 'gehärteten' Algorithmen
- Unabhängig vom Übertragungskanal
- Benötigt Zugang zu Endpunkten

Quantum Key Distribution (QKD)

- Informations-theoretische Sicherheit
- Basierend auf Quantentechnologie
- Benötigt Übertragungskanal (Reichweite!)
- Benötigt Zugang zur phys. Infrastruktur

Komplementäre Techniken – PQC (Standard) & QKD (Zusatz)

2

© 2022 ADVA. All rights reserved. Confidential.

ADVA Network Security

2

Quantensichere Kommunikation

Post Quantum Cryptography

Verschiedene Kandidaten

- Code-basiert (z.B. McEliece)
- Gitterbasiert (z.B. FrodoKEM)

BSI

- TR-02102-1 (hybrid, McEliece FrodoKEM)

NIST

- SP800-65C Rev2, hybrid
- Laufendes PQC Projekt / Wettbewerb

Quantum Key Distribution

	CV	DV		
Protocol	CV-QPSK	Decoy BB84	BBM92 (Ent.)	Twin Field
Key rate	$\sim 1/\alpha$	$\sim 1/\alpha$	$\sim 1/\alpha$	$\sim 1/\sqrt{\alpha}$
Complexity				
side channels security				
Topology	p2p	p2p	p2mp	p2mp
Fiber				
Free space				
Costs				

Standardisierung und Zertifizierung notwendig!

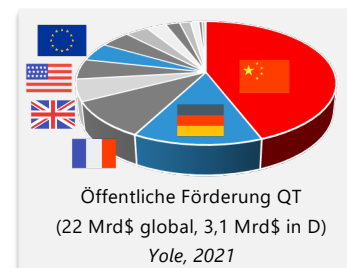
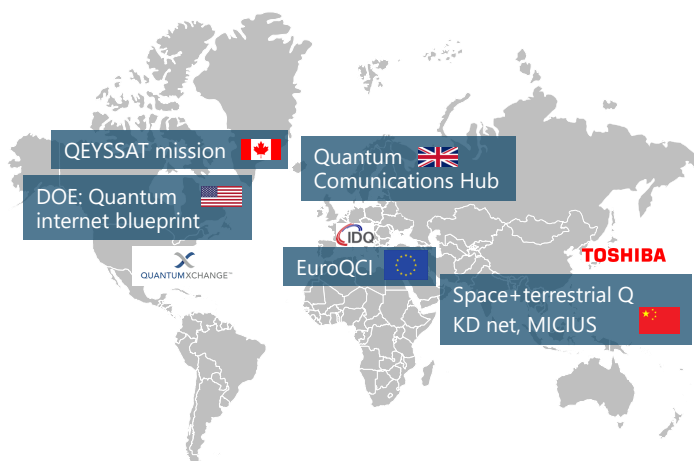
3

© 2022 ADVA. All rights reserved. Confidential.

ADVA Network Security

3

Quantenkommunikation global



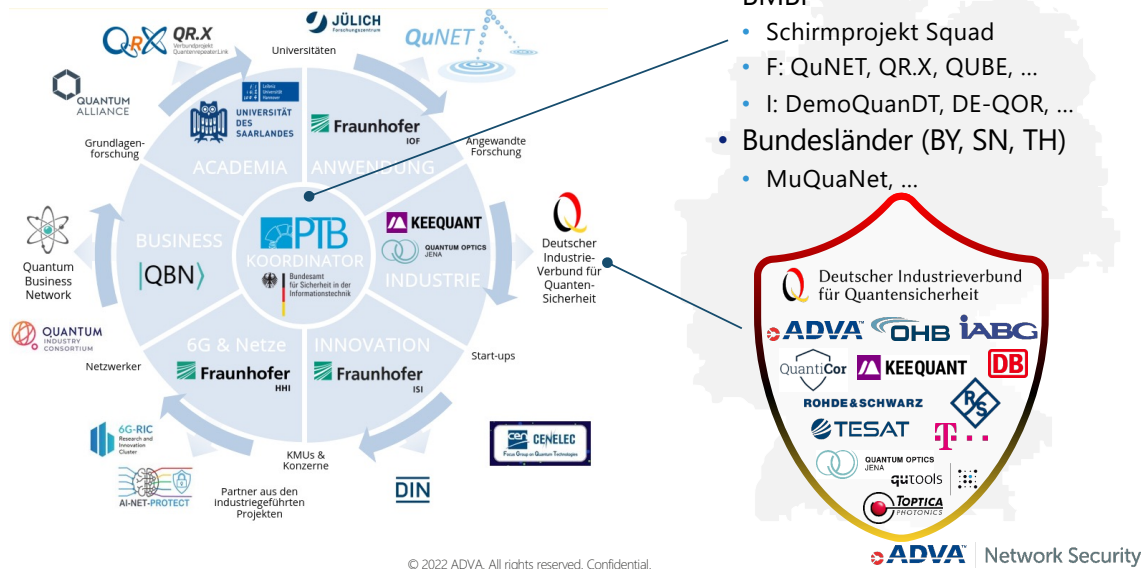
4

© 2022 ADVA. All rights reserved. Confidential.

ADVA Network Security

4

Quantenkommunikation in Deutschland



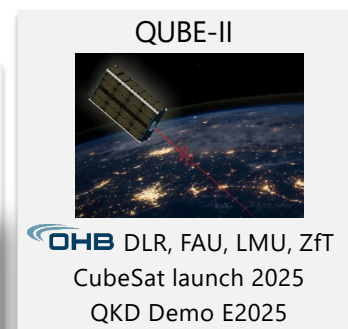
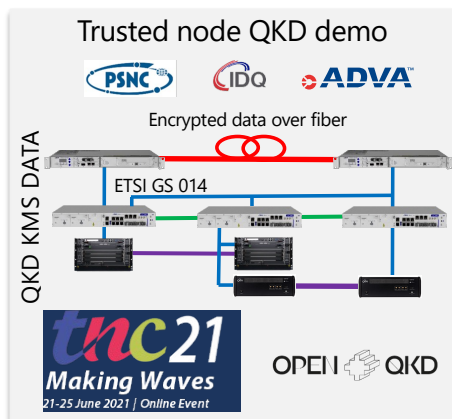
5

© 2022 ADVA. All rights reserved. Confidential.

5

Quantenkommunikation in Deutschland

Vom Labor und Demonstratoren ...



6

© 2022 ADVA. All rights reserved. Confidential.

ADVA Network Security

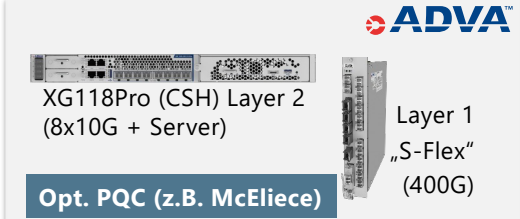
6

Quantenkommunikation in Deutschland

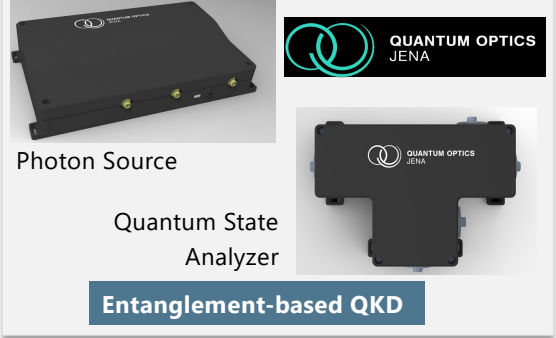
... zu Produkten



KEEQUANT
CV-QKD
QKD Device



ADVA
XG118Pro (CSH) Layer 2 (8x10G + Server)
Layer 1 "S-Flex" (400G)
Opt. PQC (z.B. McEliece)
CV-QKD



QUANTUM OPTICS JENA
Photon Source
Quantum State Analyzer
Entanglement-based QKD



DE-QOR
FSP3000 Module

- >2.5kb/s secret key rate
- 80km+ Reichweite (20dB+)
- Basierend auf Telekom Technologie
- Prototyp: Mitte 2023

7 © 2022 ADVA. All rights reserved. Confidential. **ADVA** Network Security

7

Quantenkommunikation

Aus Demonstratoren werden Produkte

- PQC (*must-have*) kann durch QKD (*nice-to-have*) ergänzt werden
- Hohe öffentliche Förderungen (inkl. *pre-commercial public procurement*)
- Starke Community in Deutschland (Forschung und Industrie)
- Erste kommerzielle Produkte und Installationen

Weitere Herausforderungen:

- Sicherheitsbeweise, Standards & Zertifizierung
- QKD Robustheit, Reichweite, Stabilität, Verfügbarkeit, Kosten ... verbessern!
- QKD – Trusted Nodes vs Repeater?

8

© 2022 ADVA. All rights reserved. Confidential.

ADVA Network Security

8

The ADVA logo is centered in the upper half of the slide, with a row of social media icons (Facebook, LinkedIn, YouTube, Twitter, etc.) to its right.

Thank you

cglingener@adva.com

IMPORTANT NOTICE
The content of this presentation is strictly confidential. ADVA is the exclusive owner or licensee of the content, material, and information in this presentation. Any reproduction, publication or reprint, in whole or in part, is strictly prohibited. The information in this presentation may not be accurate, complete or up to date, and is provided without warranties or representations of any kind, either express or implied. ADVA shall not be responsible for and disclaims any liability for any loss or damages, including without limitation, direct, indirect, incidental, consequential and special damages, alleged to have been caused by or in connection with using and/or relying on the information contained in this presentation. Copyright © for the entire content of this presentation: ADVA.