Medical Data Protection in transit and at rest during the OpenQKD testbed operation in Graz

Hannes Hübel, Andreas Poppe, Florian Kutschera: *AIT Austrian Institute of Technology GmbH, Vienna, Austria*

Werner Strasser, Bernhard Zatoukal: *fragmentiX Storage Solutions GmbH, Klosterneuburg, Austria*

Heimo Müller, Kurt Zatloukal: *Diagnostic and Research Institute of Pathology, Medical University Graz, Graz, Austria*

Sigurd F. Lax: *Department of Pathology, Hospital (LKH)-Graz II, Graz, Austria*

Andreas POPPE andreas.poppe@ait.ac.at

25.08.2021, QCrypt 3b

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857156.

https:\\openqkd.eu

Coordinated by:

18 OpenQKD Testbed Sites

Large geographic reach-out

Madrid ES
Telecom

Berlin DE
Telecom

Posnan PL
Governement

Vienna AT
Government

Delft NL
MDI QKD

Ostrava CZ
High Perf. Comp.

Cambridge UK
Data Centers

Bratislava CZ
Government

Paris FR
Academic network

Graz AT
Healthcare

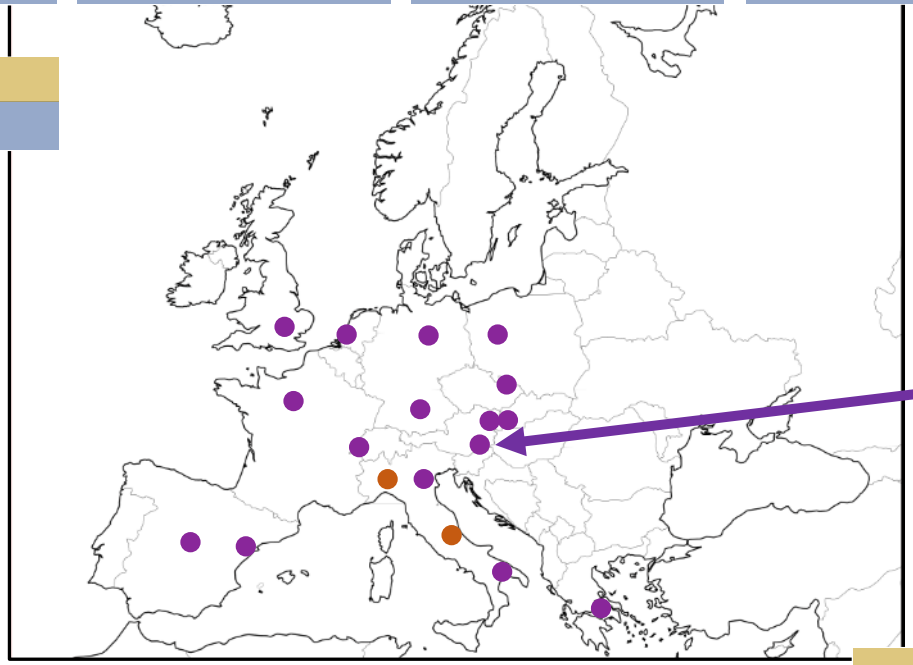
Oberpfaffenhofen DE
Satellite QKD

Padua IT
Free-space QKD

Geneva CH
Smart Grid

Matera IT
Satellite QKD

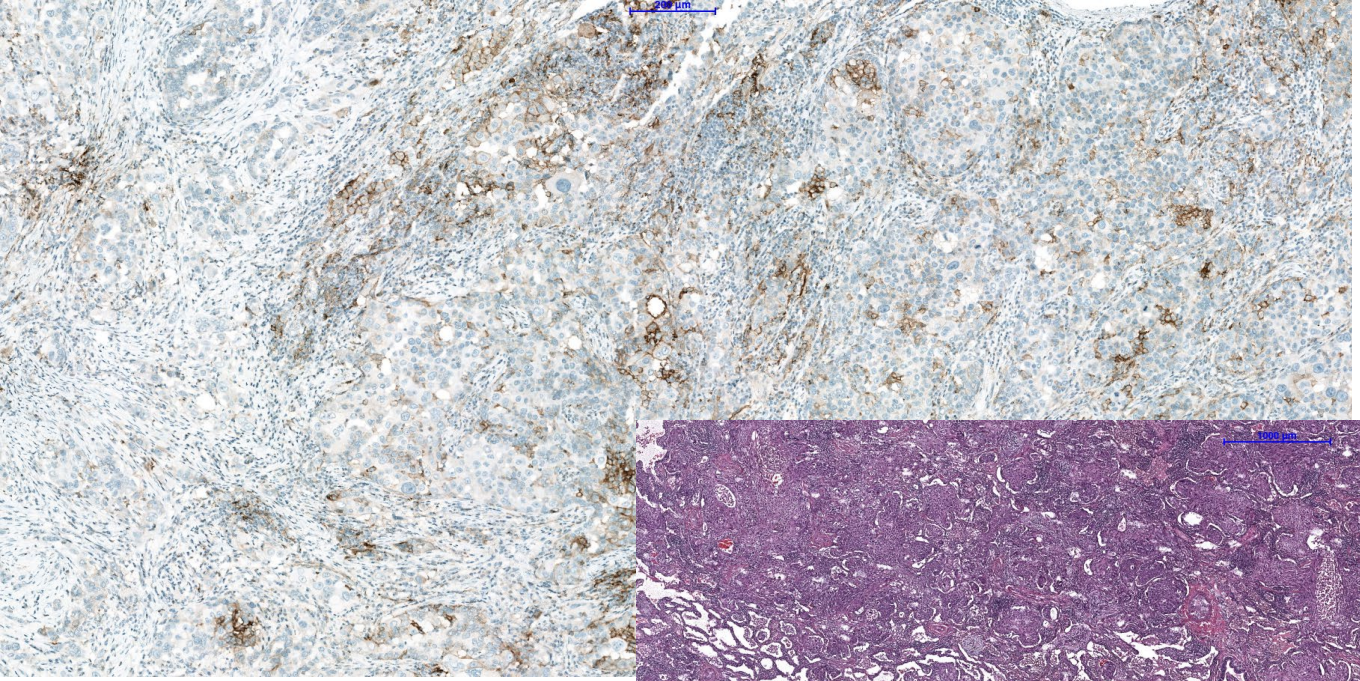
Barcelona ES
Video Com



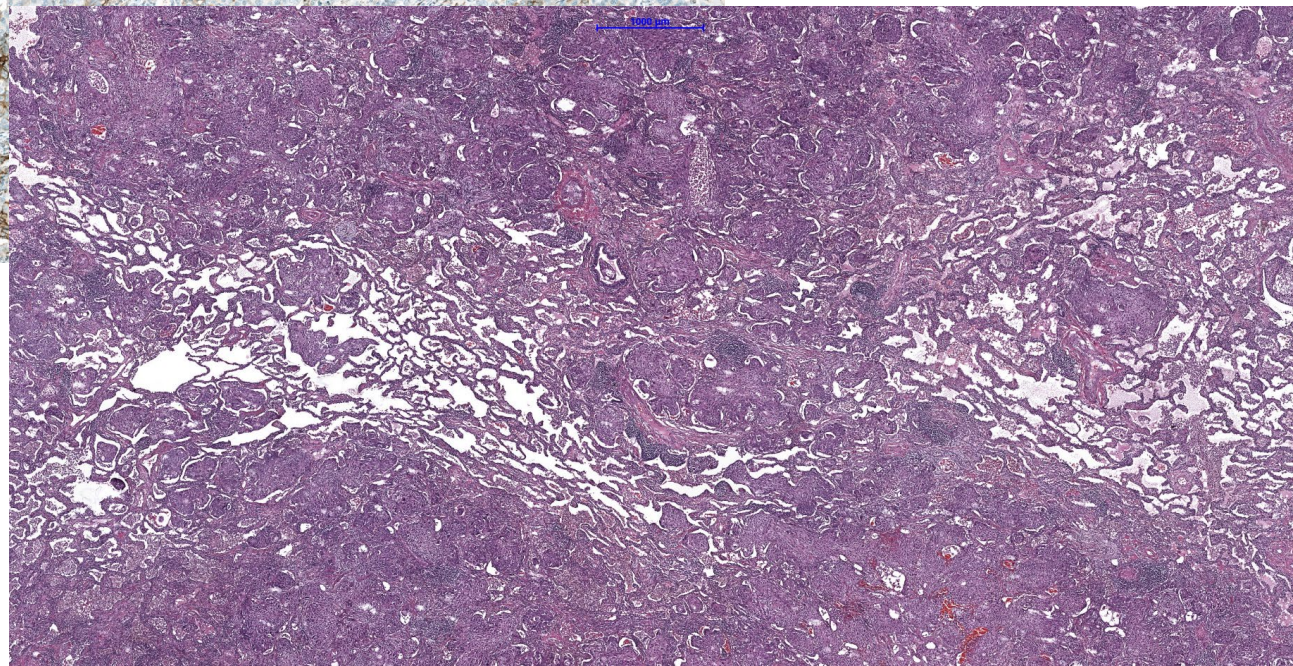
Torino IT
Telecom 5G

L'Aquila IT
Telecom multi-core

Athens GR
Data Com



OPEN QKD

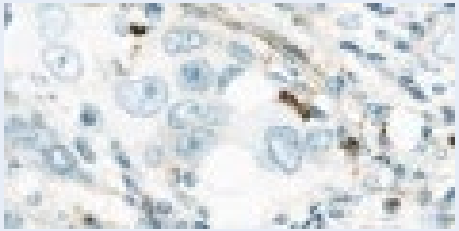


Use-case + Shamir's Secret Sharing

OPEN QKD

Medical user data (Med. Univ. Graz MUC):

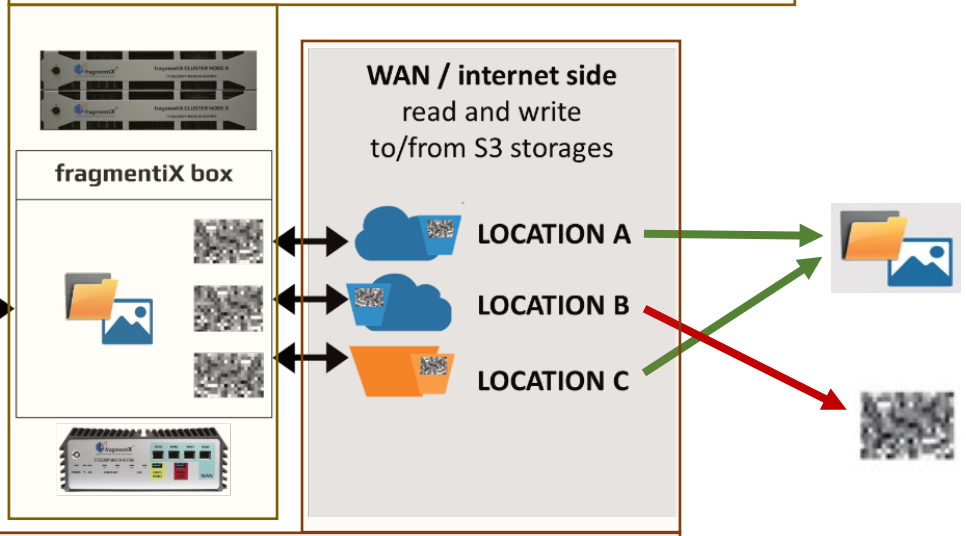
- Cuts of tissue to search for cancer cells
- Optimize drug doses
- Test data of 30 patients transmitted
- High-resolution pictures (Whole Slide Images)
- Resolution: 300.000 x 200.000 pixels
- Typical image sizes: 16 GB / slice



(Zoom at the level of cells)

fragmentiX (FRX) - SSS:

- Data is spit in 3 shares (can be more on request)
- Need at least 2 shares to retrieve full data
- A single share yields no information

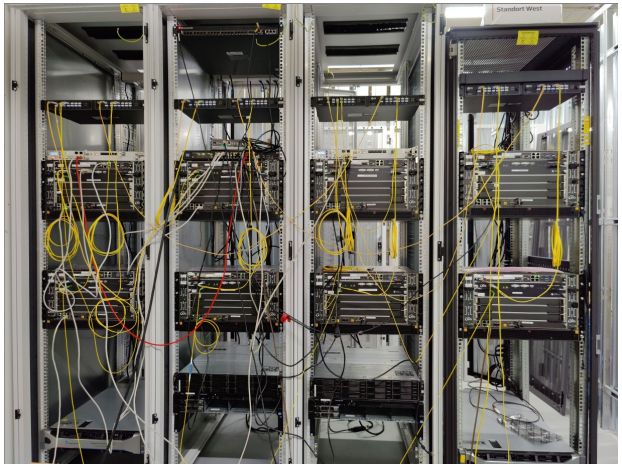


QKD network (AIT, Citycom Graz, ADVA, idq, Toshiba)

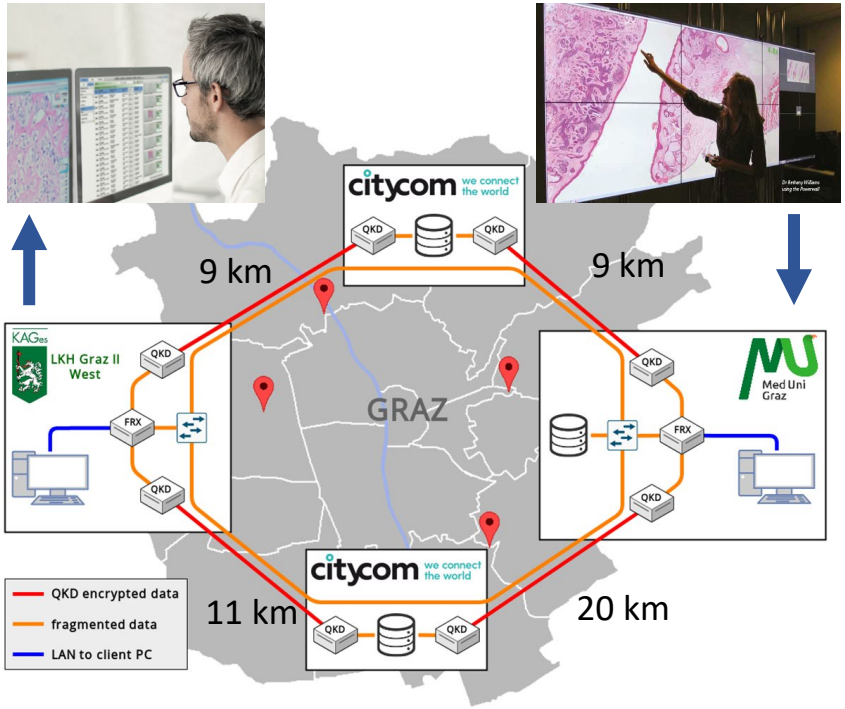
Medical Use-Case in Graz

Deployment finalized in Graz:

- ❑ Test of QKD links (4 from IDQ, 2 from Toshiba) and completed under realistic conditions
- ❑ Fiber infrastructure (Citycom) characterized
- ❑ Interface to encryptors (ADVA) implemented
- ❑ Storage solution by FragmentiX



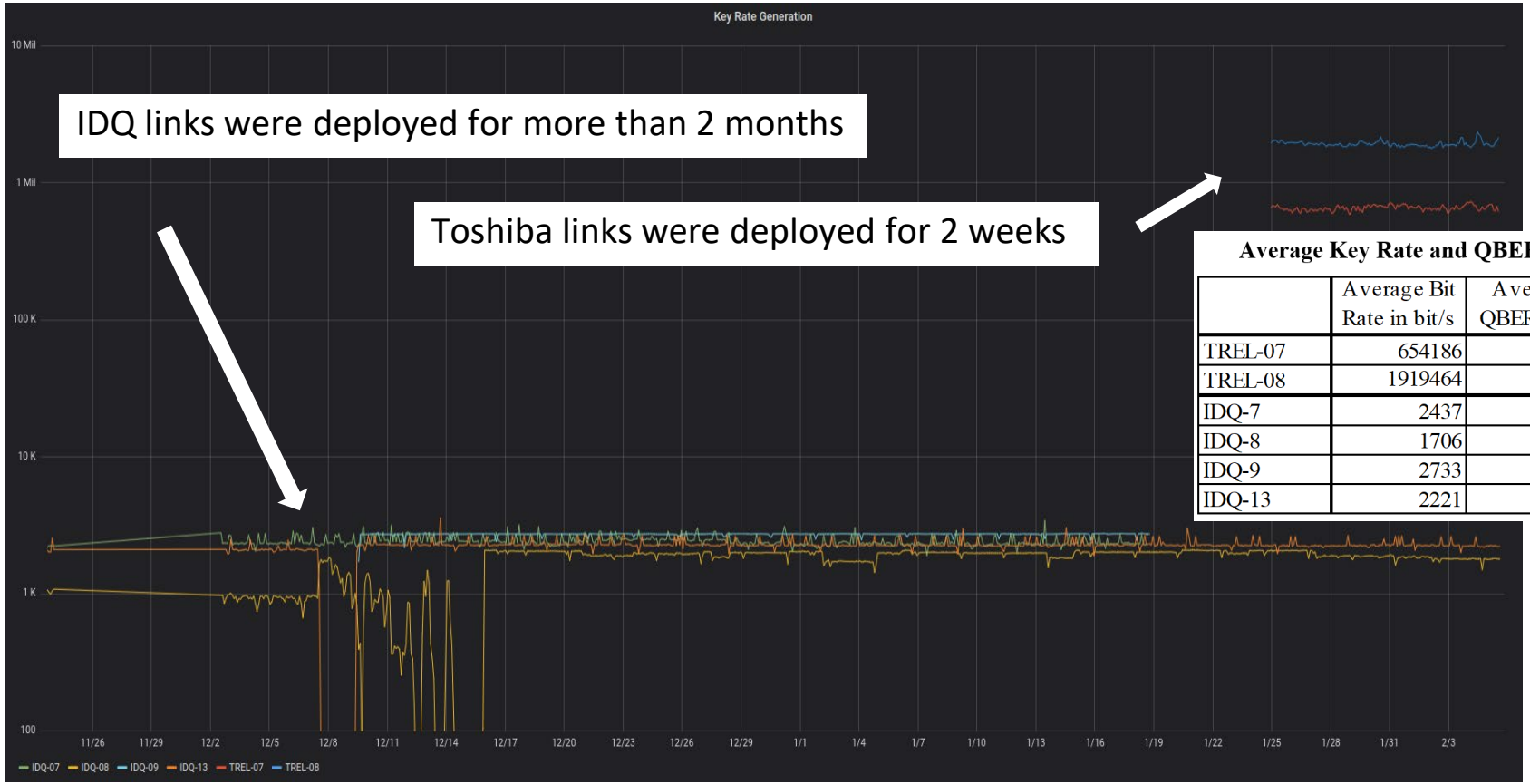
Dry-run of optical network in the lab



Geographic layout of network nodes

Secure Key Rates from the Field Test

OPEN QKD



IDQ links were deployed for more than 2 months

Toshiba links were deployed for 2 weeks

Average Key Rate and QBER

	Average Bit Rate in bit/s	Average QBER in %
TREL-07	654186	4,11
TREL-08	1919464	3,88
IDQ-7	2437	3,21
IDQ-8	1706	3,26
IDQ-9	2733	1,61
IDQ-13	2221	3,11