KVANTOVÁ DISTRIBUCE KLÍČŮ
QUANTUM KEY DISTRIBUTION (QKD)

Rudolf Vohnout, Josef Vojtech, et al
Optical networks department, CESNET, Czech Republic

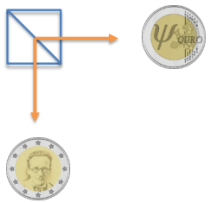
Sep 8th 2020
CSNOG

Outline

- QKD Princip
- Význam a mezinárodní projekty a iniciativy
- CESNET a QKD
- T/F a QKD
- První skutečný generátor náhodných čísel

QKD Princip

- Odolnost asymetrické kryptografie proti kvantovým počítačům?
- Kvantové provázání fotonů
  - Skutečná náhodnost



- Kvantová distribuce klíčů toto řeší.
  - Odposlechem dojde ke narušení integrity informace.
- Princip klasické symetrické kryptografie.
  - Standardně je největší slabina distribuce klíče
  - Pokud je klíč zachycen, komunikace může být dešifrována.

The horizontal axis is the length of the number to be factored. The steep curve is NFS, with the marked point at $L = 768$ requiring 3,300 CPU-years. The vertical line at $L = 2048$ is NIST's 2007 recommendation for RSA key length for data intended to remain secure until 2030. The other lines are various combinations of quantum computer logical clock speed for a three-qubit operation known as a Toffoli gate (1Hz and 1MHz), method of implementing the arithmetic portion of Shor's algorithm (BCDP, D, and F), and quantum computer architecture (NTC and AC, with the primary difference being whether or not long-distance operations are supported). The assumed capacity of a machine in this graph is $2L^2$ logical qubits. This figure illustrates the difficulty of making pronouncements about the speed of quantum computers.

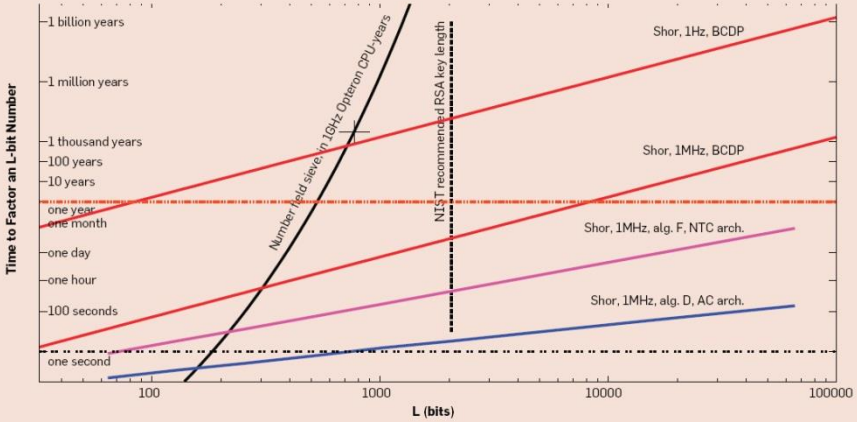
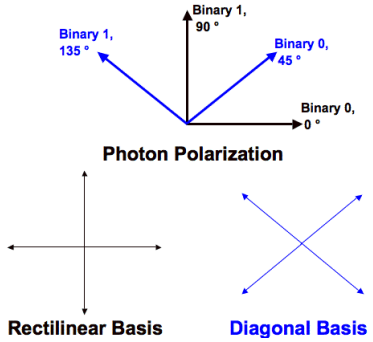


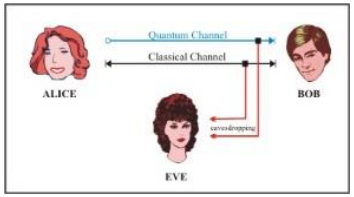
Figure: R. Van Meter and C. Horsman, "A blueprint for building a quantum computer," Communications of the ACM, vol. 56, no. 10, pp. 84–93 (2013)

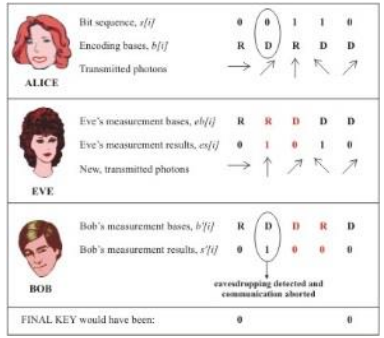
QKD podrobněji

- Zjišťuje se SoP provázaných fotonů.
  - Nejjednodušší pro pochopení je základní BB84 protokol.
  - Oddělené trasy pro distribuci provázaných fotonů a datové přenosy.
- Distribuce klíčů na dlouhé vzdálenosti je problematická
  - Největší problém je vzájemná autentizace při porovnávání SoP.
- Využití sestavených klíčů pro šifrování datových přenosů.
- Optický přenosový systém (s kryptovacími kartami) pro šifrování datových přenosů.
  - ETSI Key Delivery API
  - Cache pro ukládání klíčů (pro vyčítání dle potřeby).



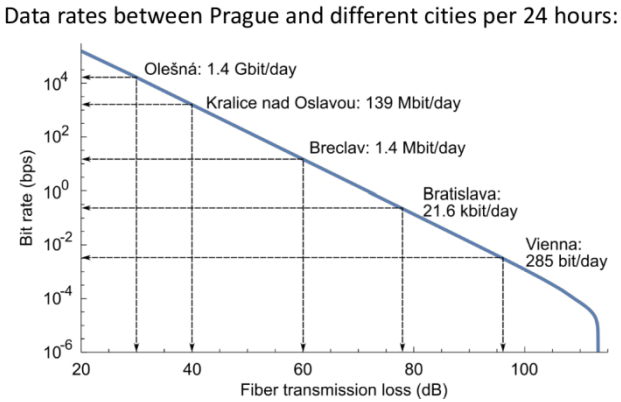
https://www.youtube.com/watch?v=LaLzshIosDk





Omezení

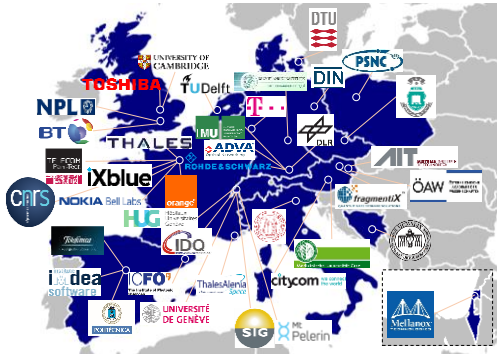
- Se vzdáleností téměř lineárně klesá množství „správně doručených“ provázených párů fotonů.
  - Je nutné nasazení opravných kódu (např. LDPC)
- One-time Pad (Vernamova šifra)
  - Nejvíce bezpečné (ale nejpomalejší).
  - One-to-one bit šifrování
    - Každý bit klíče odpovídá jednomu bitu zprávy.
- Využití bitů pro vytvoření symetrické šifry (např. AES)
  - A její využití po nejkratší možnou dobu.
  - Sledovat doporučení NIST!

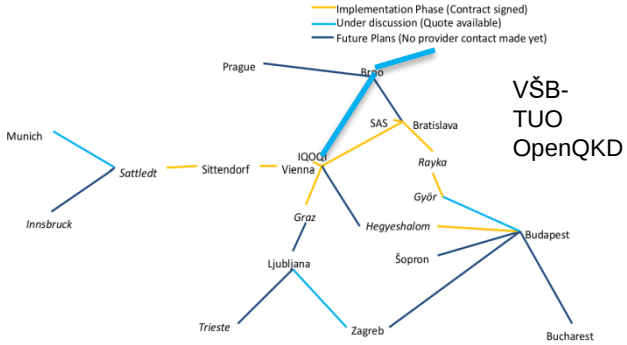


Ref: Neumann S. etc al. QUAPITAL

Případy užití a mezinárodní projekty

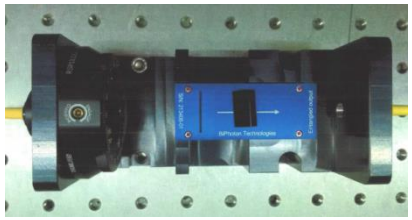
- Quantum Internet Use Cases (IETF RFC).
- Případy užití v ČR
  - Jakákoliv služba s vysokými nároky na bezpečnost přenosu.
    - Státní pokladna
    - MO ČR
    - MV CŘ (ověřování identity)
- Projekty a iniciativy
  - OpenQKD (Horizon 2020) - https://openqkd.eu/
  - QUAntum Photonic Intercity TrAnsmission Lattice (QUPITAL) - https://quapital.eu/
    - IQOQI Vienna, Austrian Academy of Sciences
  - Euro QCI
  - …

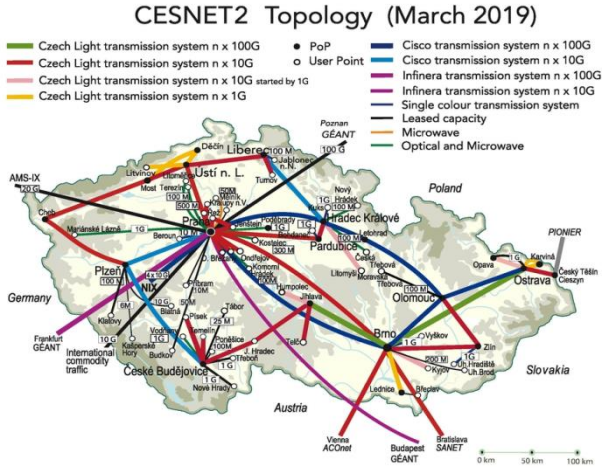




CESNET a QKD

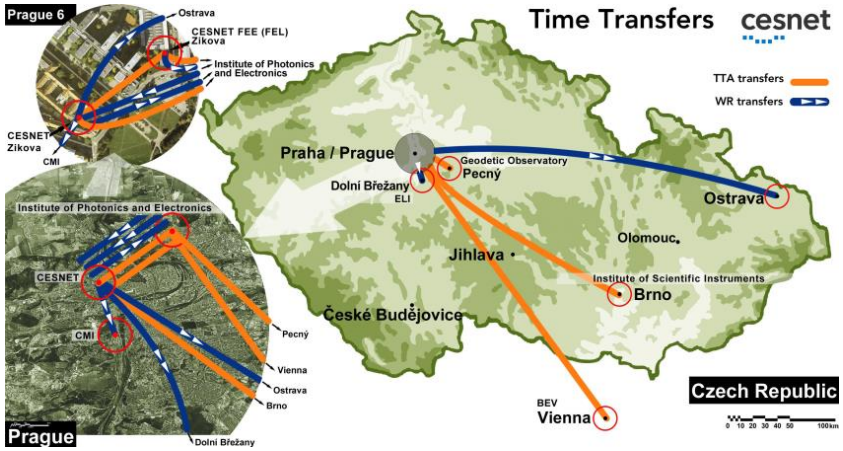
- Oddělení optických sítí
  - QKD Know-how a vybavení.
    - 2x MPD SPAD + IDQ SPAD
    - Uwaterloo BiPhoton Generator.
    - Generátor entaglovaných párů + čerpací laser
    - 3000 km optický testbed.
- Zapojení v:
  - GÉANT Network Evolution QKD subtask
    - Toshiba PoC testování v rámci OpenQKD OC
      - Příprava PoC trasy.
  - QUAPITAL
  - MVČR IMPAKT 1 (bezpečnostní výzkum)
    - VUT (koordinátor) + CESNET + VŠB-TUO

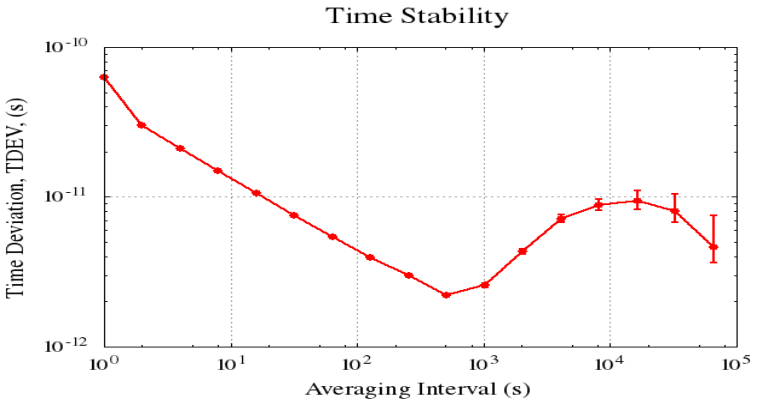




T/F a její důležitost pro QKD

- CITAF – Infrastruktura pro přenos a distribuci přesného času
- Nejsou třeba antény, nehrozí jamming
- Překonává GPS a další GNSS systémy (přenost 3-50 ns)
- Pro QKD (téměř) nutnost.
  - Lepší sync -> vyšší key-rate.
- Spojuje národní laboratoře UTC(TP), UTC(BEV), probíhá připojení UTC(PL).
  - Propojuje akademická pracoviště v ČR která provozují primární standardy (CS hodiny 5x a H maser 1x).
  - Technologie – Time Transfer Adapter + White Rabbit – přenos 10 MHz a 1PPs, cca na 1500 km vláken sdílených s daty.

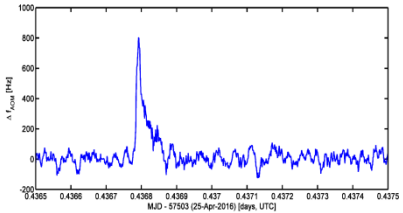




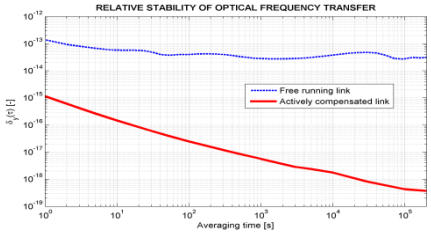
T/F a optický sensing

- CITAF – Infrastruktura pro přenos a ultrastabilní optické frekvence.
- Propojení optických hodin, distribuce ultrastabilní optické frekvence pro snímání.
- Snímání
  - diskrétní- např. stabilita kontejmentu.
  - distribuované: zemětřesení a především tampering s vlákny

poklep na kabel



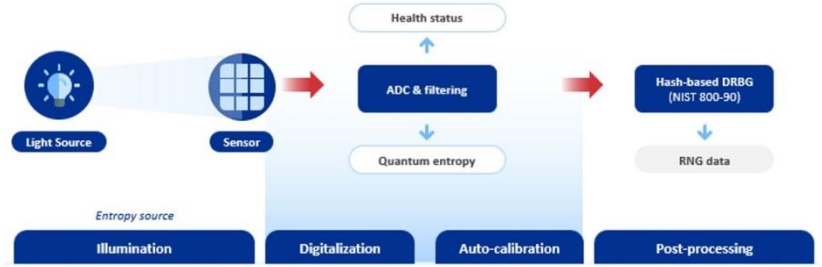
zemětřesení u Vídně



Kredit: Munster, Cizek, Mikel

Skutečný generátor náhodných čísel

- IDQ certifikovaný generátor náhodných čísel
  - Princip fotonů dopadajících na CMOS
  - IDQ QRNG
    - NIST 800-90A/B/C certifikace
  - Využití především v gaming sektoru!
    - Možná překvapivě až druhý je sektor finanční.



- IDQ PCI-X a 1U QRNG appliance.

- První 5G kvantový mobilní telefon na světě
  - Samsung s chipem SKT IDQ S2Q000
    - https://www.cnews.cz/samsung-ukazal-prvni-kvantovy-smartphone-galaxy-a-quantum/
    - A druhý:
      - https://www.idquantique.com/id-quantique-integrates-its-quantum-chip-in-vsmart-aris-5g-smartphone/

Děkuji velice za pozornost!
Otázky?

rudolf.vohnout@cesnet.cz