Quantum Cryptography

from basics of quantum mechanics to secure key distribution

Christoph Hamsen

Berlin Crypto Meetup

Who am I?

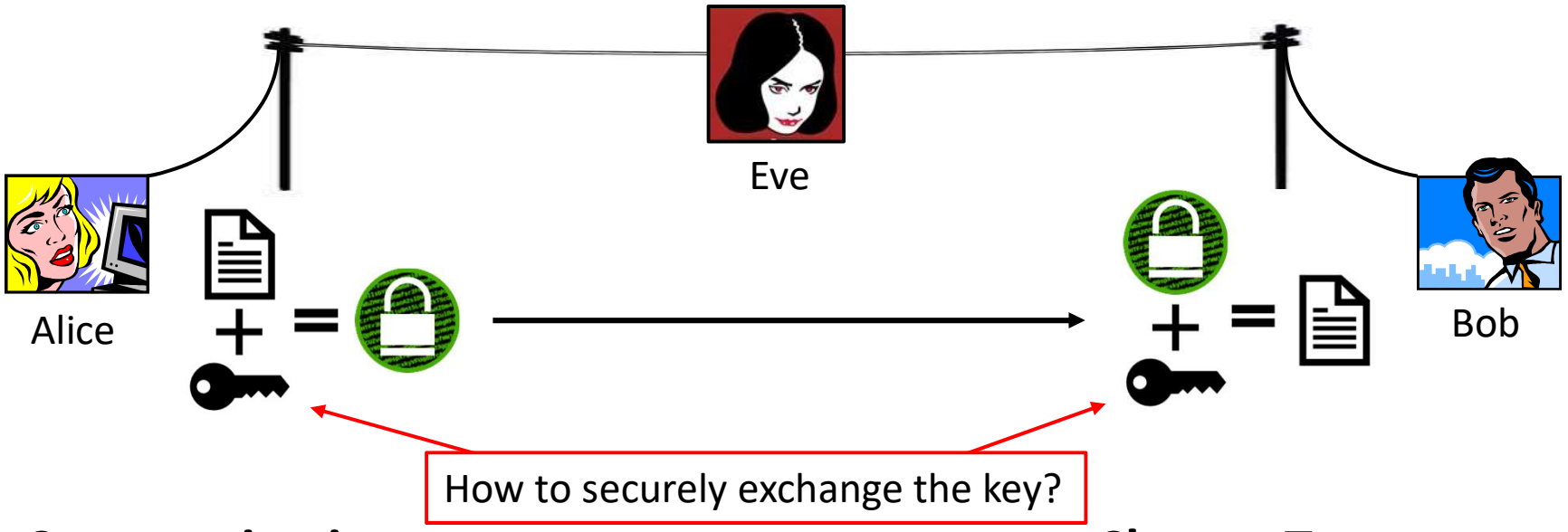
- Studied Physics @ TU Ilmenau, MIT, TU Munich and Harvard
- Researched on quantum optics for PhD @ MPQ
- Developed software for robots @ Magazino
- Bringing IT security to software @ SSE

MPQ

SSE

Podcasts enthusiast (Logbuch Netzpolitik, Lage der Nation) and frequent visitor to c3!

Cryptography and Key Distribution



Communication should be secure!

- Authentic
- Confidential
- Integrity

Choose Transport Layer Security (TLS)!

- v1.2 or higher!
- Select Cipher suite

Key Exchange **Encryption**

DHE – RSA – AES128 – SHA256

Authentication **Message Authentication**

Only computationally secure → **Quantum Key Distribution offers physical security**

Enter the photon!

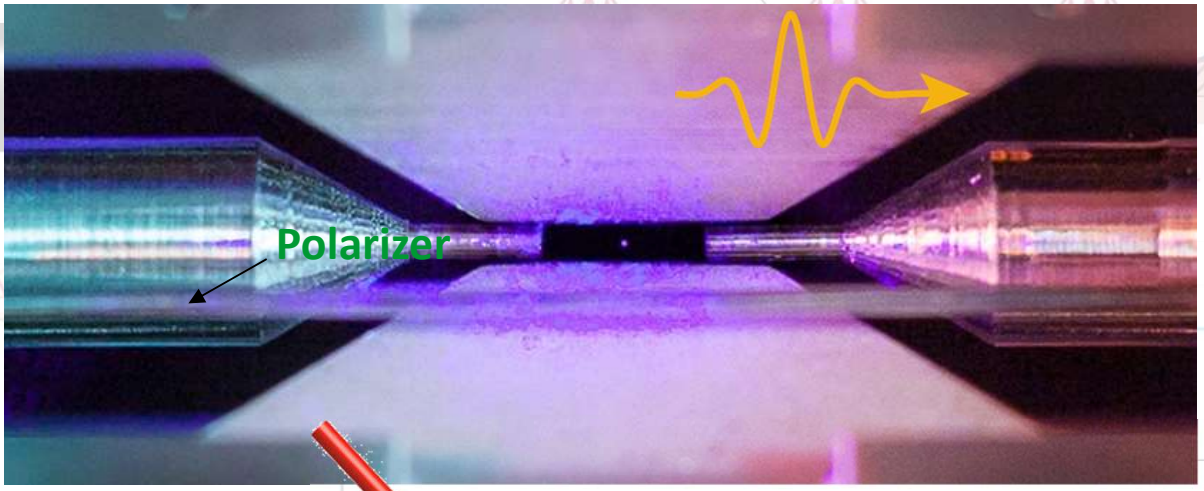
< 1900: Light is a wave!

Magnetic field

Electric field

≈ **Polarization**

Direction of propagation



Probability: 100%

0%

50%

Image sources: Anton Paar (wiki.anton-paar.com), oPhysics.com, Wikipedia

Image sources:

- David Nadlinger @ Ion Trap Quantum Computing Group at University of Oxford
- Rempe Group @ Max Planck Institute of Quantum Optics

Quantum Key Distribution

á la "BB84"

Alice

RNG

+/×

RNG

0/1

h/v basis

"0" "1"

Bob

click

NG

"No cloning theorem"

Protocol:

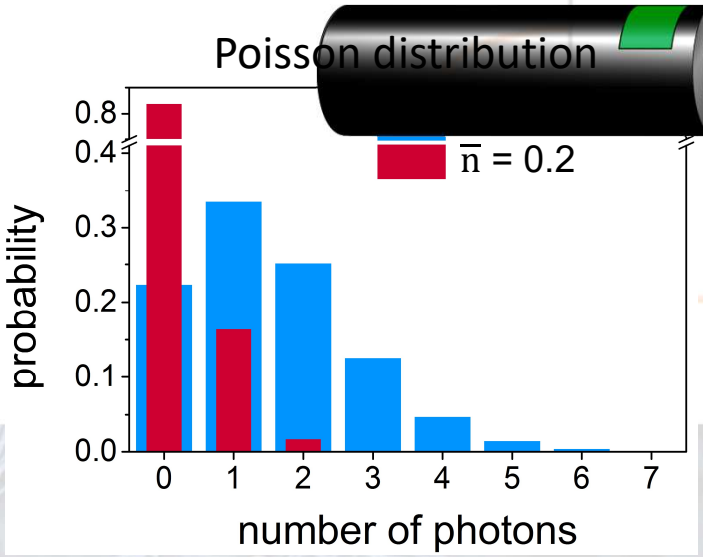
1. Alice sends random values in random bases
2. Bob measures in random base
3. Alice communicates chosen bases via classical channel
4. Both compare random subset of values

25% error rate on comparison

Provably secure!

Source: http://www.vad1.com/

Attacks & Vulnerabilities



$$\mathcal{P}(k) = \frac{\overline{n}^k e^{-\overline{n}}}{k!}$$

with k – number of photons
$\overline{n}$ – mean photon number

→ single-photon sources

→ privacy amplification

→ other protocols, e.g. decoy state QKD

N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt and G. Leuchs, "Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems", *IEEE* 21 (3), 168-177 (2015)

Original source unclear

Hardware/Implementation attacks

Attack	Target component	Tested system
Intersymbol interference	intensity modulator in Alice	research system
K. Yoshino et al., poster at QCrypt (2016)		
Laser damage	any	ID Quantique, research system
V. Makarov et al., Phys. Rev. A 94, 030302 (2016)		
Spatial efficiency mismatch	receiver optics	research system
M. Rau et al., IEEE J. Quantum Electron. 21, 6600905 (2015); S. Sajeed et al., Phys. Rev. A 91, 062301 (2015)		
Pulse energy calibration	classical watchdog detector	ID Quantique
S. Sajeed et al., Phys. Rev. A 91, 032326 (2015)		
Trojan-horse	phase modulator in Alice	SeQureNet
I. Khan et al., presentation at QCrypt (2014)		
Trojan-horse	phase modulator in Bob	ID Quantique
N. Jain et al., New J. Phys. 16, 123030 (2014); S. Sajeed et al., arXiv:1704.07749		
Detector saturation	homodyne detector	SeQureNet
H. Qin, R. Kumar, R. Alleaume, Proc. SPIE 88990N (2013)		
Shot-noise calibration	classical sync detector	SeQureNet
P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A 87, 062313 (2013)		
Wavelength-selected PNS	intensity modulator	(theory)
M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A 86, 032310 (2012)		
Multi-wavelength	beamsplitter	research system
H.-W. Li et al., Phys. Rev. A 84, 062308 (2011)		
Deadtime	single-photon detector	research system
H. Weier et al., New J. Phys. 13, 073024 (2011)		
Channel calibration	single-photon detector	ID Quantique
N. Jain et al., Phys. Rev. Lett. 107, 110501 (2011)		
Faraday-mirror	Faraday mirror	(theory)
S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A 83, 062331 (2011)		
Detector control	single-photon detector	ID Quantique, MagiQ, research system
I. Gerhardt et al., Nat. Commun. 2, 349 (2011); L. Lydersen et al., Nat. Photonics 4, 686 (2010)		

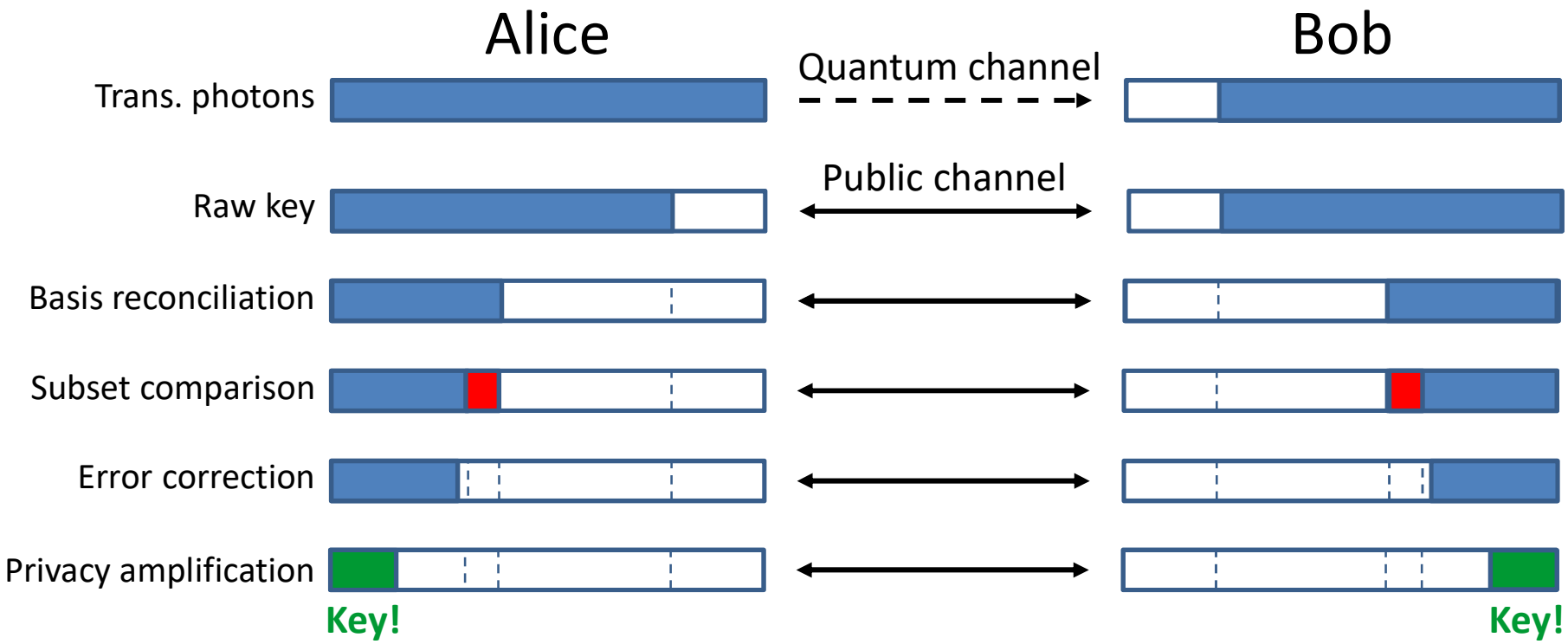
Table by V.Makarov: http://www.vad1.com/

→ need hardening of components and implementation!

Real world QKD

Handle losses due to e.g. sources, quantum channel, detector, Eve, ...

→ **Key Distillation**



→ Transmission losses ultimately limit QKD distance!

"Applications"

- Many research groups world-wide
  - Components
  - Theory
- Commercial systems
  - IDQuantique, MagiQ Technologies, QuintessenceLabs, SeQureNet, …
- Several long-distance test networks…

Slide taken from V.Makarov (http://www.vad1.com/)

Classical encryptors:

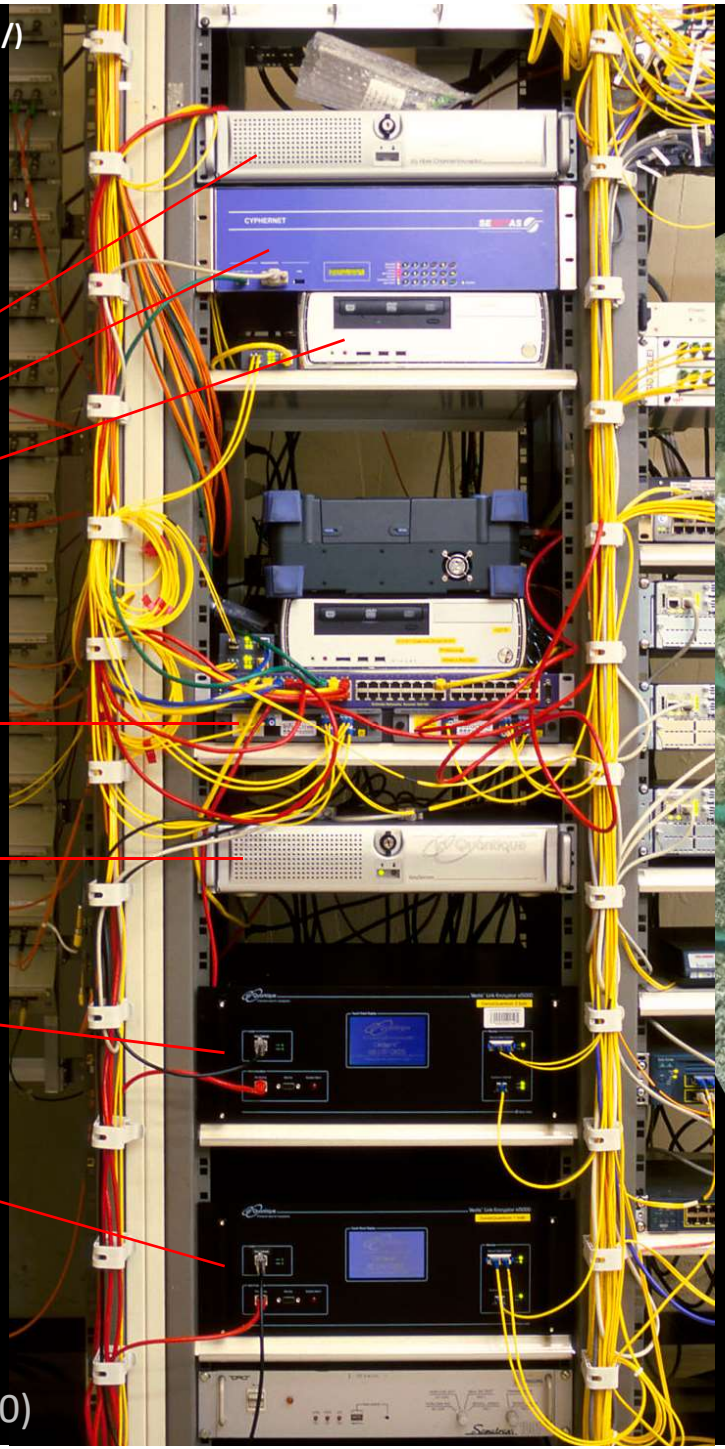
L2, 2 Gbit/s
L2, 10 Gbit/s
L3 VPN, 100 Mbit/s

WDMs

Key manager

QKD to another node
(4 km)

QKD to another node
(14 km)



www.swissquantum.com
ID Quantique *Cerberis* system (2010)

Quantum Backbone

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes

  31 fiber links
- Metropolitan networks

  Existing: Hefei, Jinan

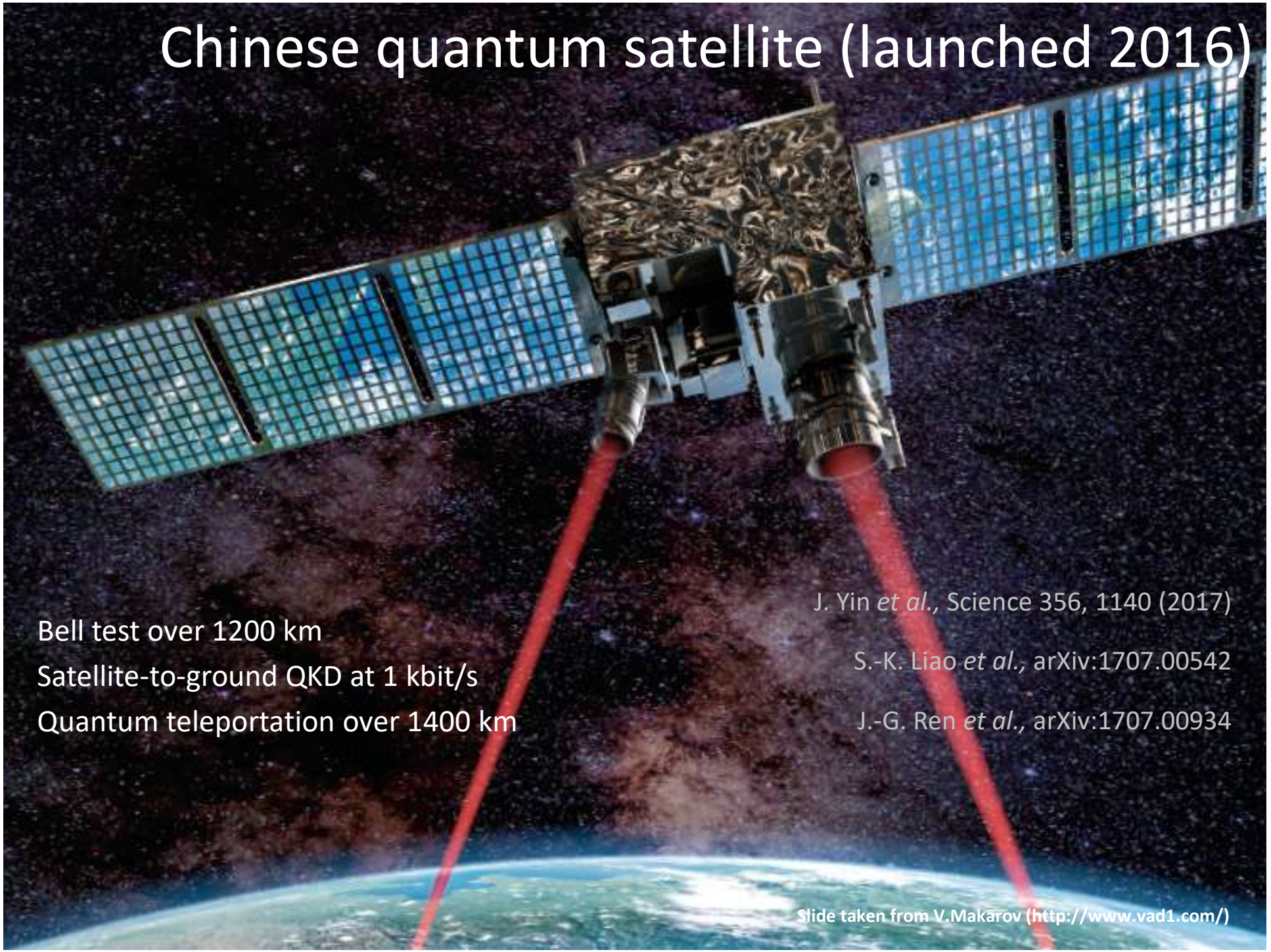
  New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC

Q. Zhang, talk at QCrypt 2014

Slide taken from V.Makarov (http://www.vad1.com/)


Global quantum key distribution
Slide adapted from V.Makarov (http://www.vad1.com/)

Chinese quantum satellite (launched 2016)



Bell test over 1200 km

Satellite-to-ground QKD at 1 kbit/s

Quantum teleportation over 1400 km

J. Yin *et al.*, Science 356, 1140 (2017)

S.-K. Liao *et al.*, arXiv:1707.00542

J.-G. Ren *et al.*, arXiv:1707.00934

Slide taken from V.Makarov (http://www.vad1.com/)

Challenges & Developments

- Developments
  - Quantum Relays and Repeaters
  - Device-independent QKD (E91 protocol)
  - Multi-mode, quantum signatures, quantum one-way functions, …

the end

Bye

Alice

Thank you for your attention!

Bob

You're welcome ;-)

Eve

https://www.linkedin.com/in/hamsen/