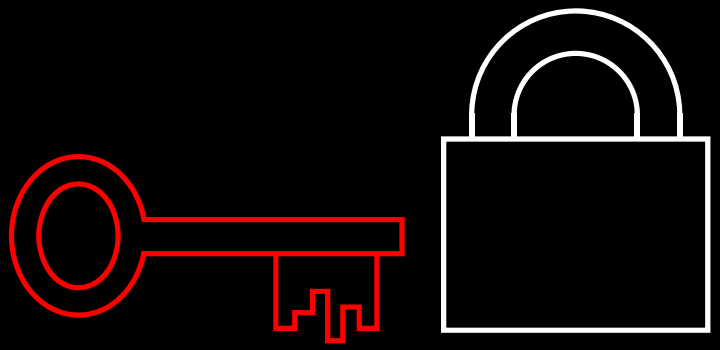
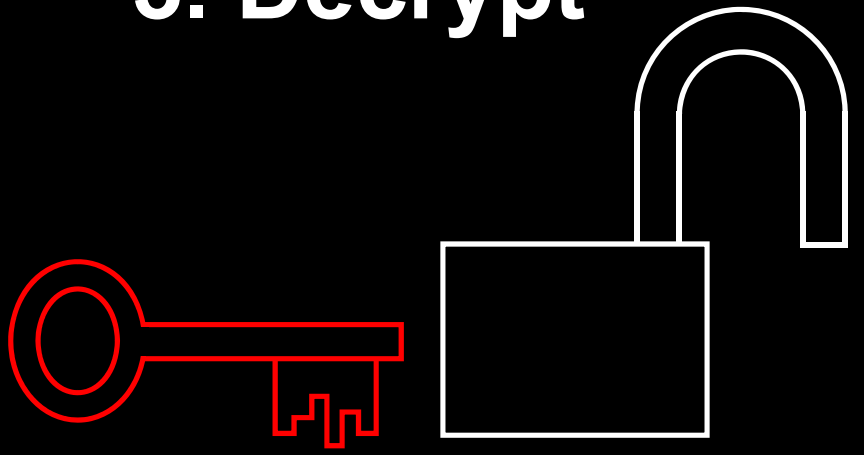
Cryptography

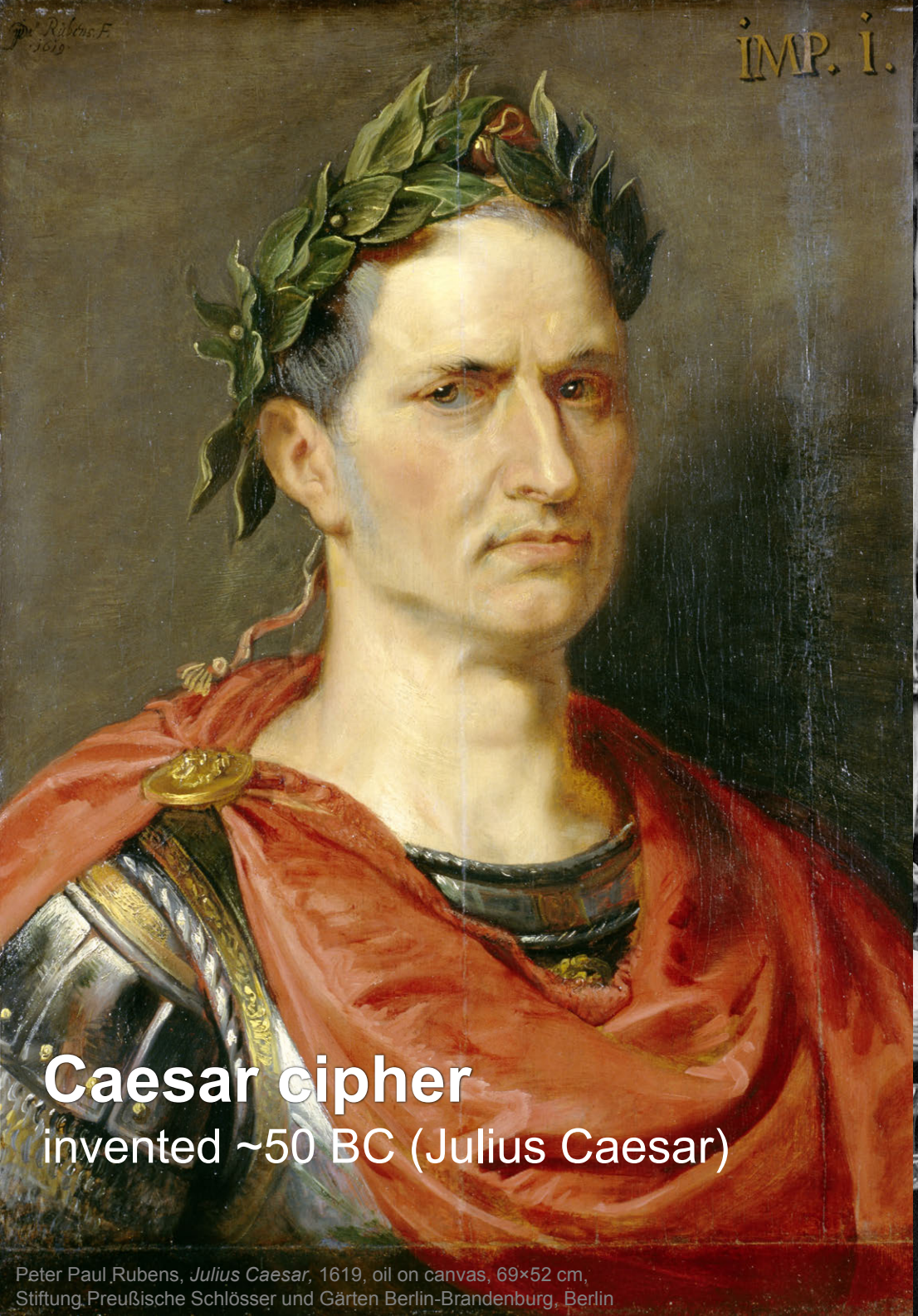
1. Make key

2. Encrypt



3. Decrypt

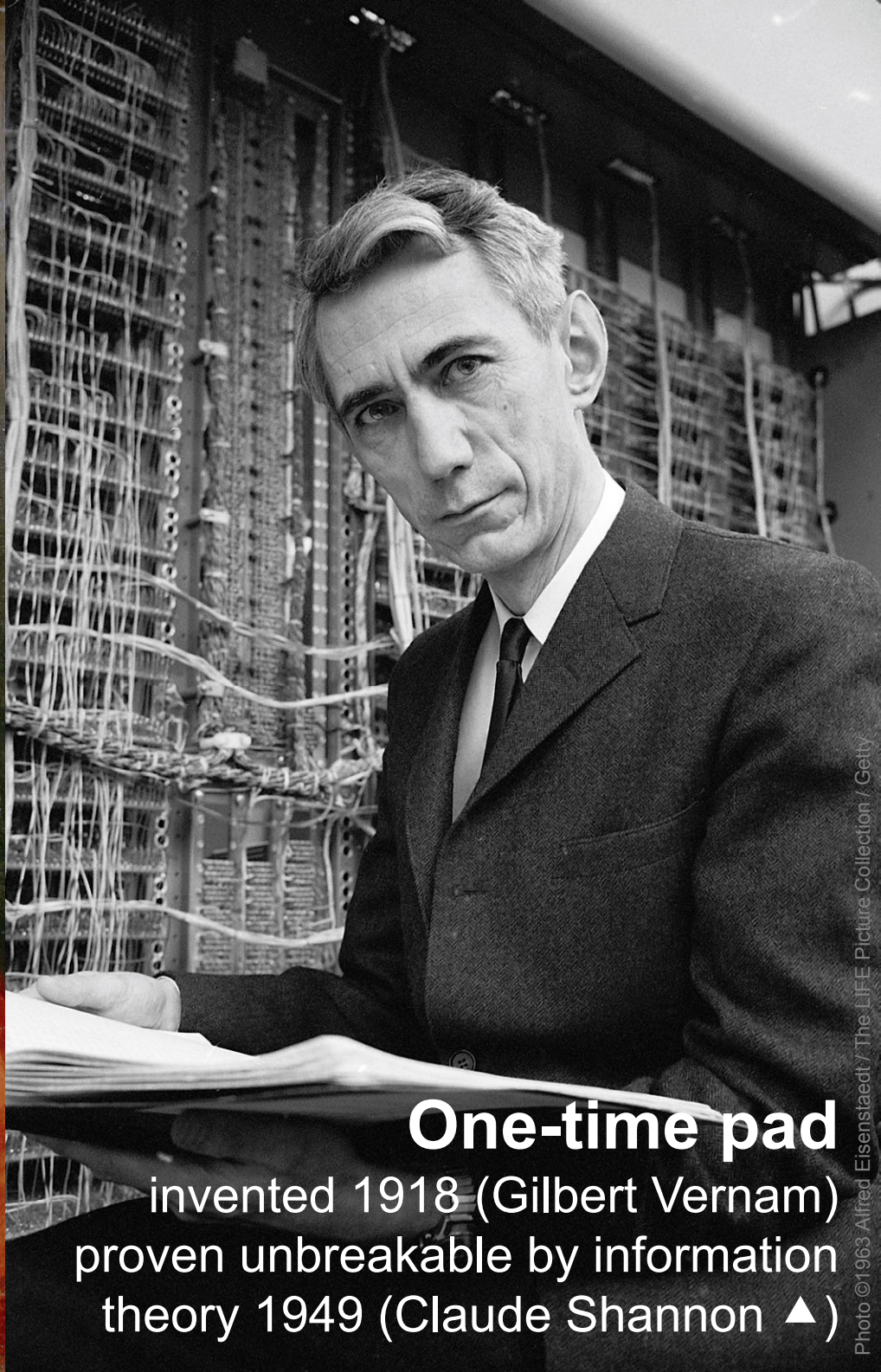




Caesar cipher

invented ~50 BC (Julius Caesar)

Peter Paul Rubens, *Julius Caesar,* 1619, oil on canvas, 69×52 cm, Stiftung Preußische Schlösser und Gärten Berlin-Brandenburg, Berlin



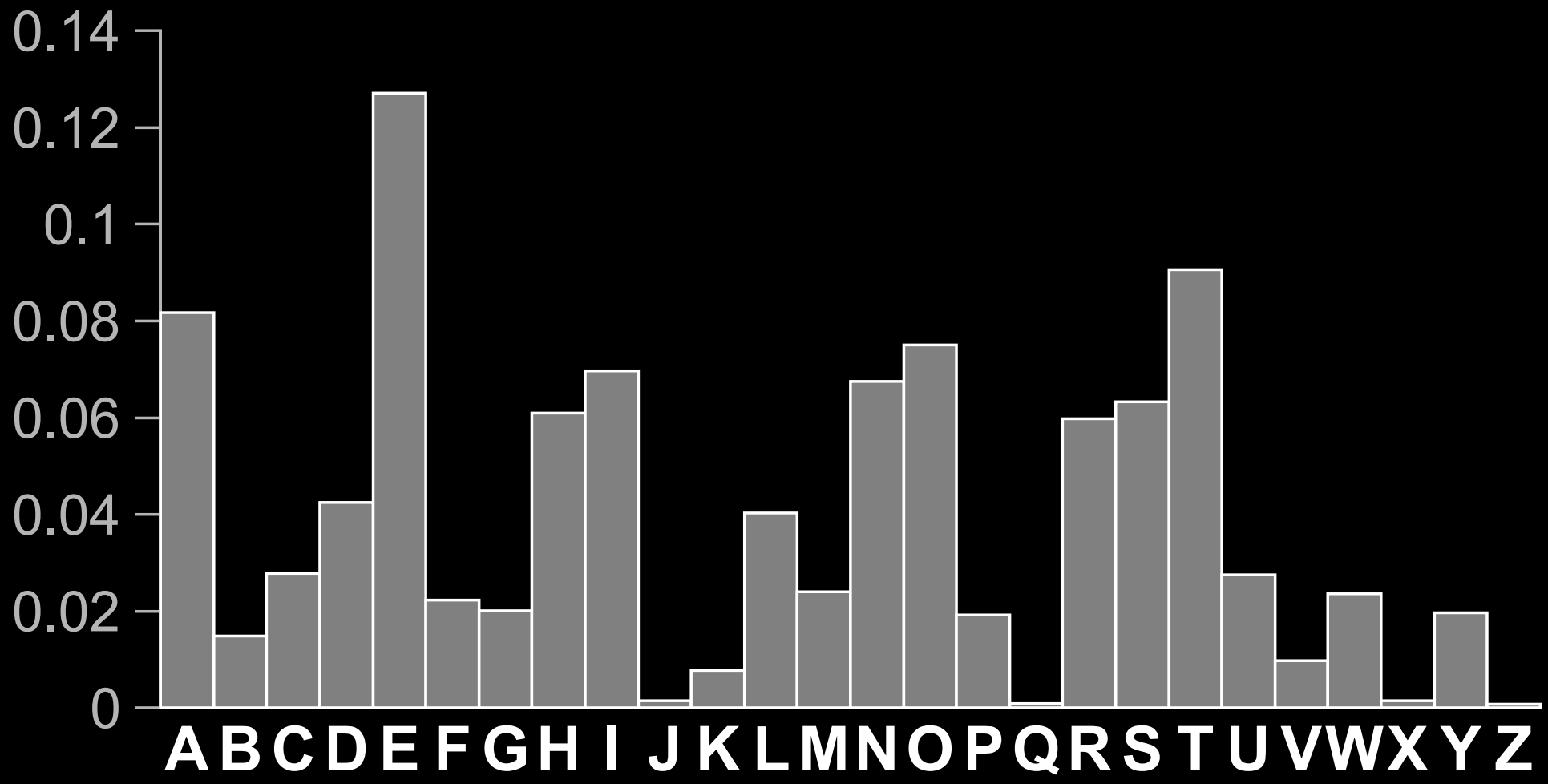
One-time pad

invented 1918 (Gilbert Vernam)
proven unbreakable by information theory 1949 (Claude Shannon ▲)

A (very) brief history of cryptography

		Broken?
Monoalphabetic cipher	invented ~50 BC (J. Caesar)	~850 (Al-Kindi)
Nomenclators (code books)	~1400 – ~1800	✓
Polyalphabetic (Vigenère)	1553 – ~1900	1863 (F. W. Kasiski)
…		
One-time pad	invented 1918 (G. Vernam)	**impossible** (C. Shannon 1949)
Polyalphabetic electromechanical (Enigma, Purple, etc.)	1920s – 1970s	✓
…		
DES	1977 – 2005	1998: 56 h (EFF)
Public-key crypto (RSA, elliptic-curve)	1977 –	will be once we have q. computer (P. Shor 1994)
AES	2001 –	**?**
Public-key crypto ('quantum-safe')	in development	**?**

Probability of letters in English text



https://en.wikipedia.org/wiki/Frequency_analysis

A (very) brief history of cryptography

		Broken?
Monoalphabetic cipher	invented ~50 BC (J. Caesar)	~850 (Al-Kindi)
Nomenclators (code books)	~1400 – ~1800	✓
Polyalphabetic (Vigenère)	1553 – ~1900	1863 (F. W. Kasiski)
…		
One-time pad	invented 1918 (G. Vernam)	**impossible** (C. Shannon 1949)
Polyalphabetic electromechanical (Enigma, Purple, etc.)	1920s – 1970s	✓
…		
DES	1977 – 2005	1998: 56 h (EFF)
Public-key crypto (RSA, elliptic-curve)	1977 –	will be once we have q. computer (P. Shor 1994)
AES	2001 –	**?**
Public-key crypto ('quantum-safe')	in development	**?**

Breaking cryptography retroactively

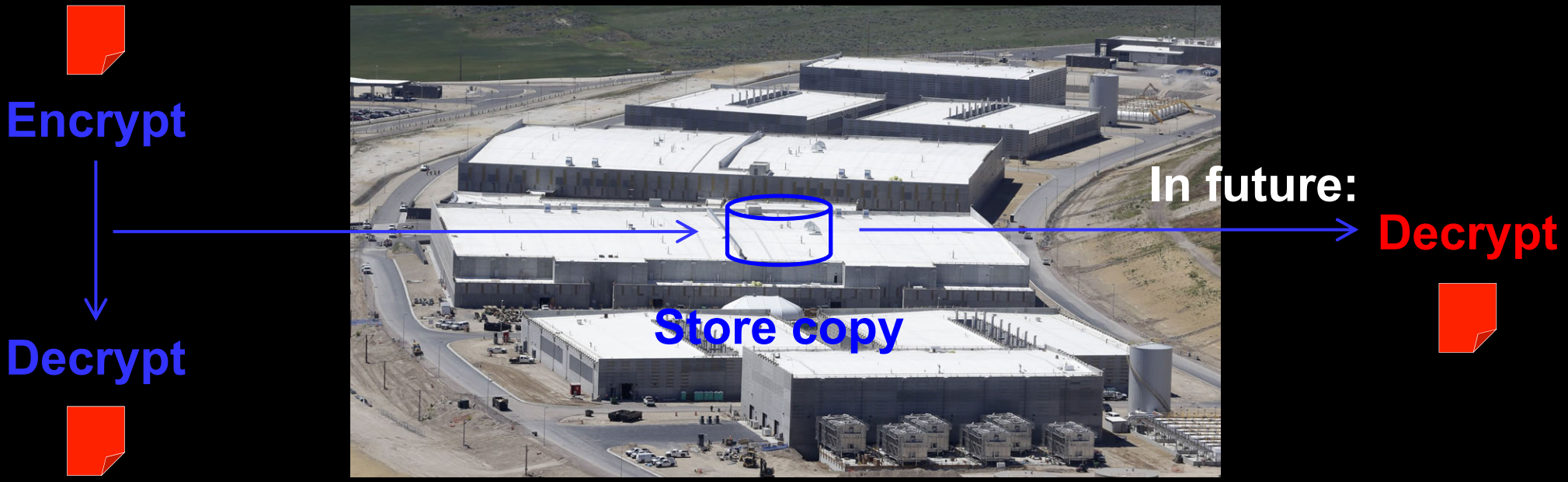
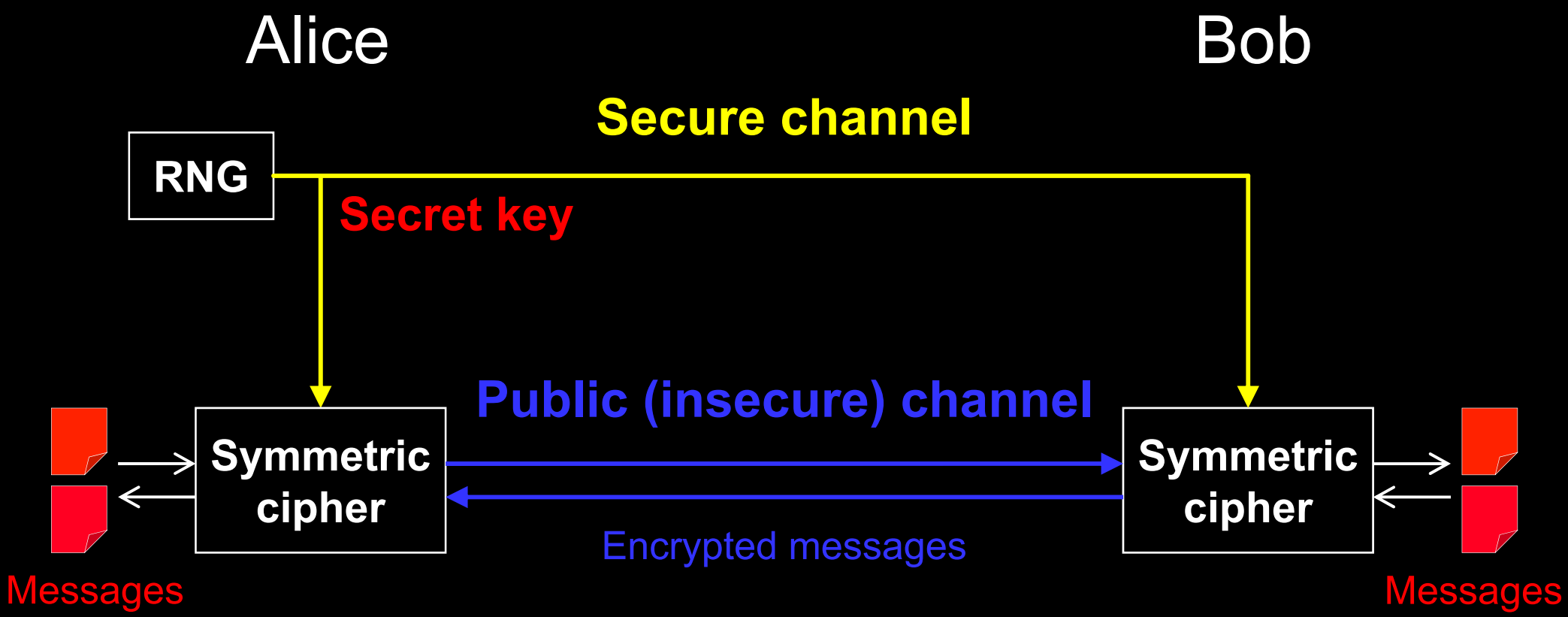


Photo ©2013 AP / Rick Bowmer

A (very) brief history of cryptography

		Broken?
Monoalphabetic cipher	invented ~50 BC (J. Caesar)	~850 (Al-Kindi)
Nomenclators (code books)	~1400 – ~1800	✓
Polyalphabetic (Vigenère)	1553 – ~1900	1863 (F. W. Kasiski)
…		
One-time pad	invented 1918 (G. Vernam)	**impossible** (C. Shannon 1949)
Polyalphabetic electromechanical (Enigma, Purple, etc.)	1920s – 1970s	✓
…		
DES	1977 – 2005	1998: 56 h (EFF)
Public-key crypto (RSA, elliptic-curve)	1977 –	will be once we have q. computer (P. Shor 1994)
AES	2001 –	?
Quantum cryptography	invented 1984, in development	**impossible**
Public-key crypto ('quantum-safe')	in development	?

Encryption and key distribution

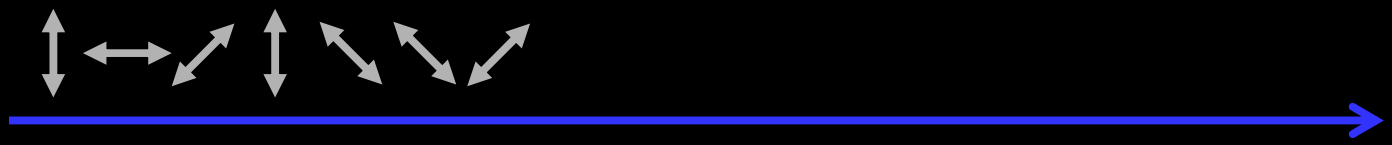


Quantum key distribution transmits secret key by sending quantum states over *open channel.*

Quantum key distribution (QKD)

Alice

Bob



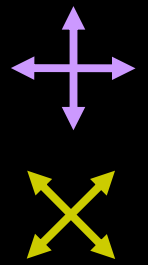
Prepares photons

(0), (1)

(0), (1)

Eavesdropping introduces errors

Measures photons



C. H. Bennett, G. Brassard (1984)

Commercial QKD

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)

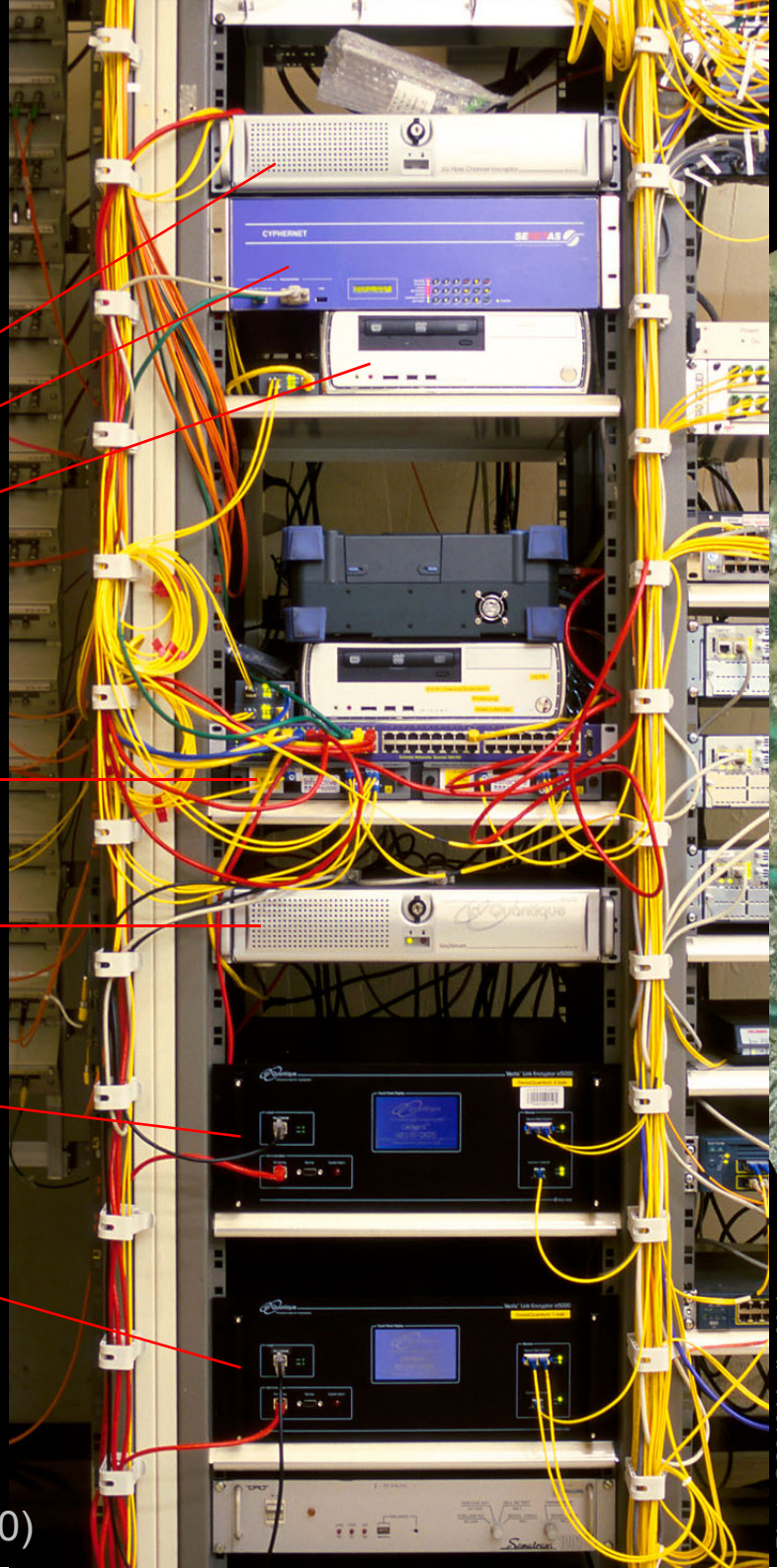
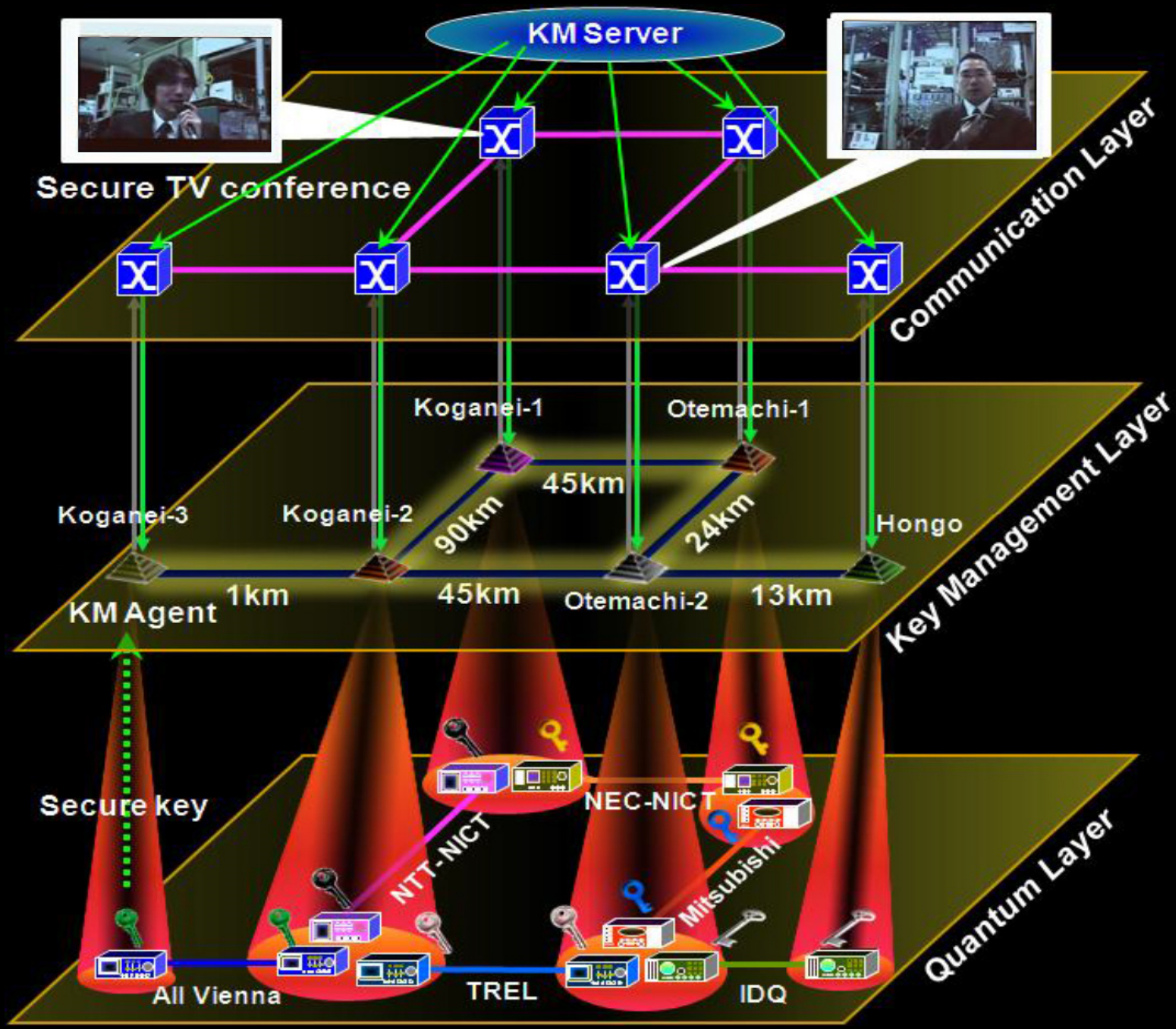


Photo ©2010 Vadim Makarov

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

Trusted-node network



M. Sasaki *et al.*, Opt. Express **19**, 10387 (2011)

Quantum Backbone

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

  31 fiber links
- Metropolitan networks

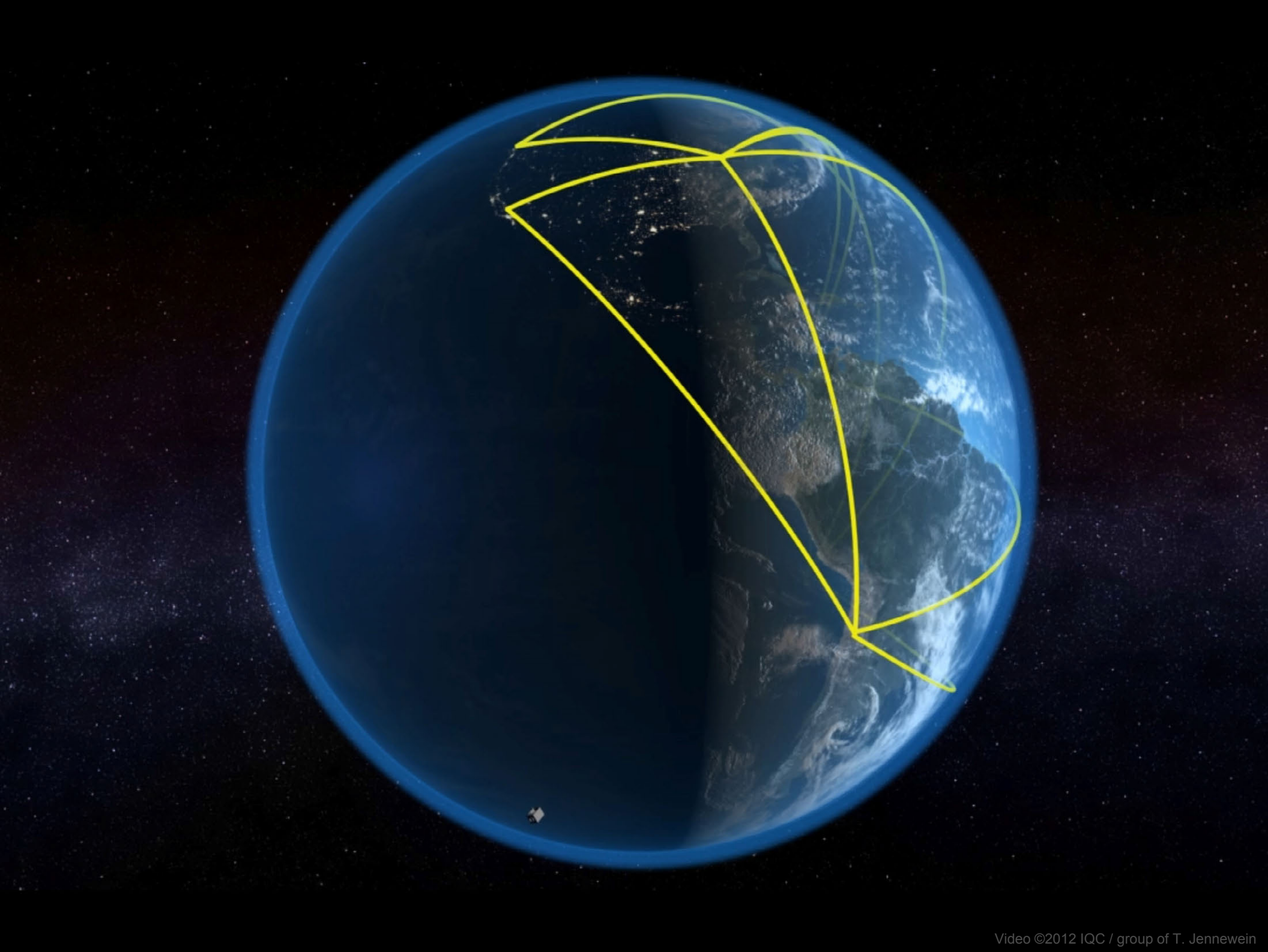
  Existing: Hefei, Jinan

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

Q. Zhang, talk at QCrypt 2014

Shanghai control center of the Chinese quantum key distribution network and satellite

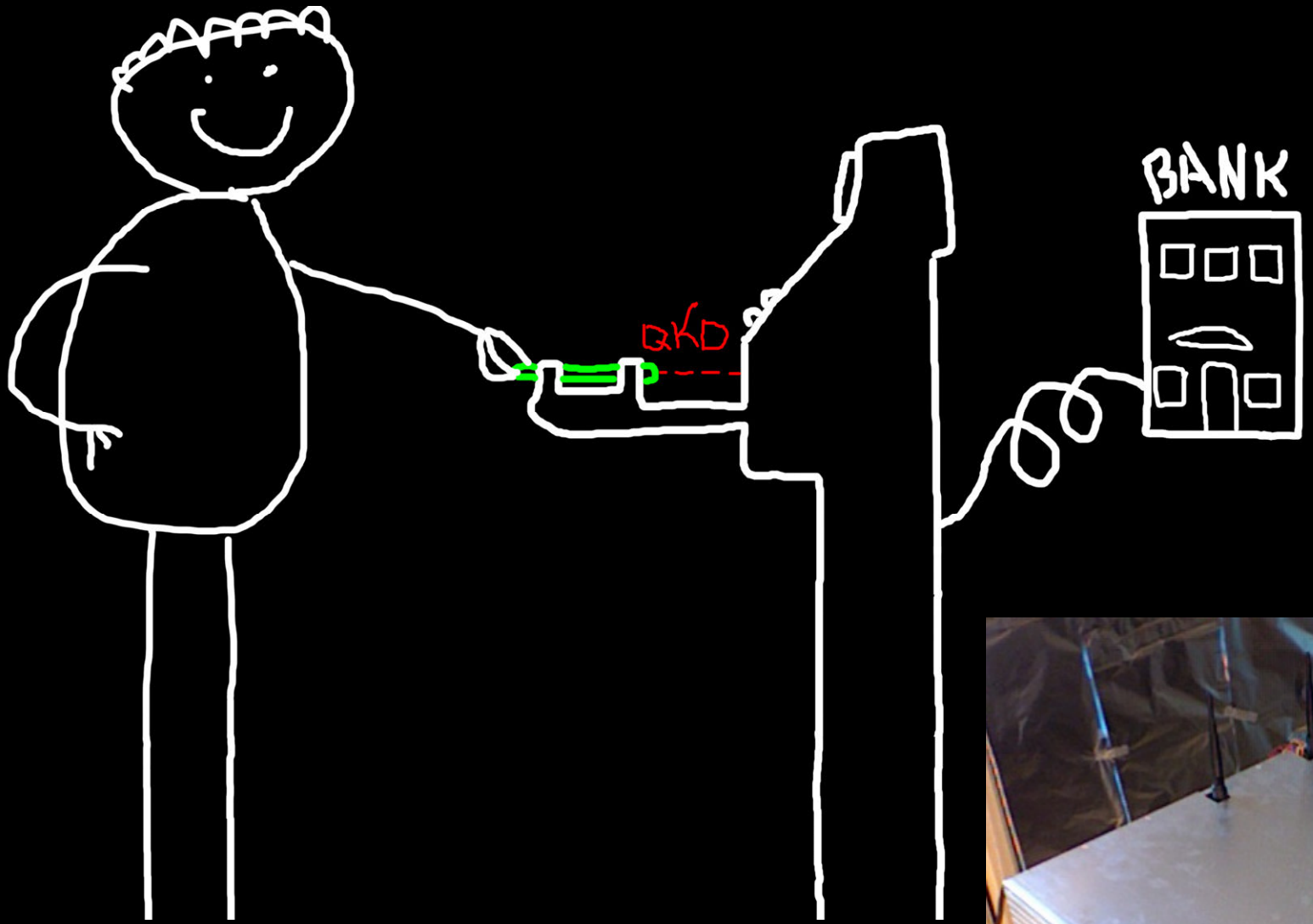

Global
quantum key distribution
Video ©2012 IQC / group of T. Jennewein

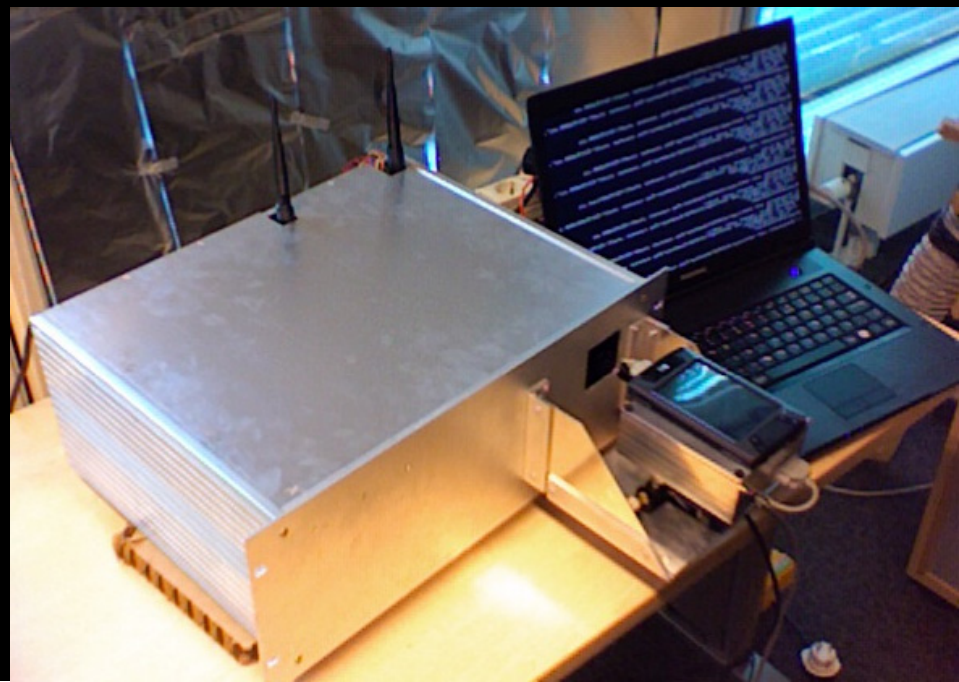


Video ©2012 IQC / group of T. Jennewein

False ATM front

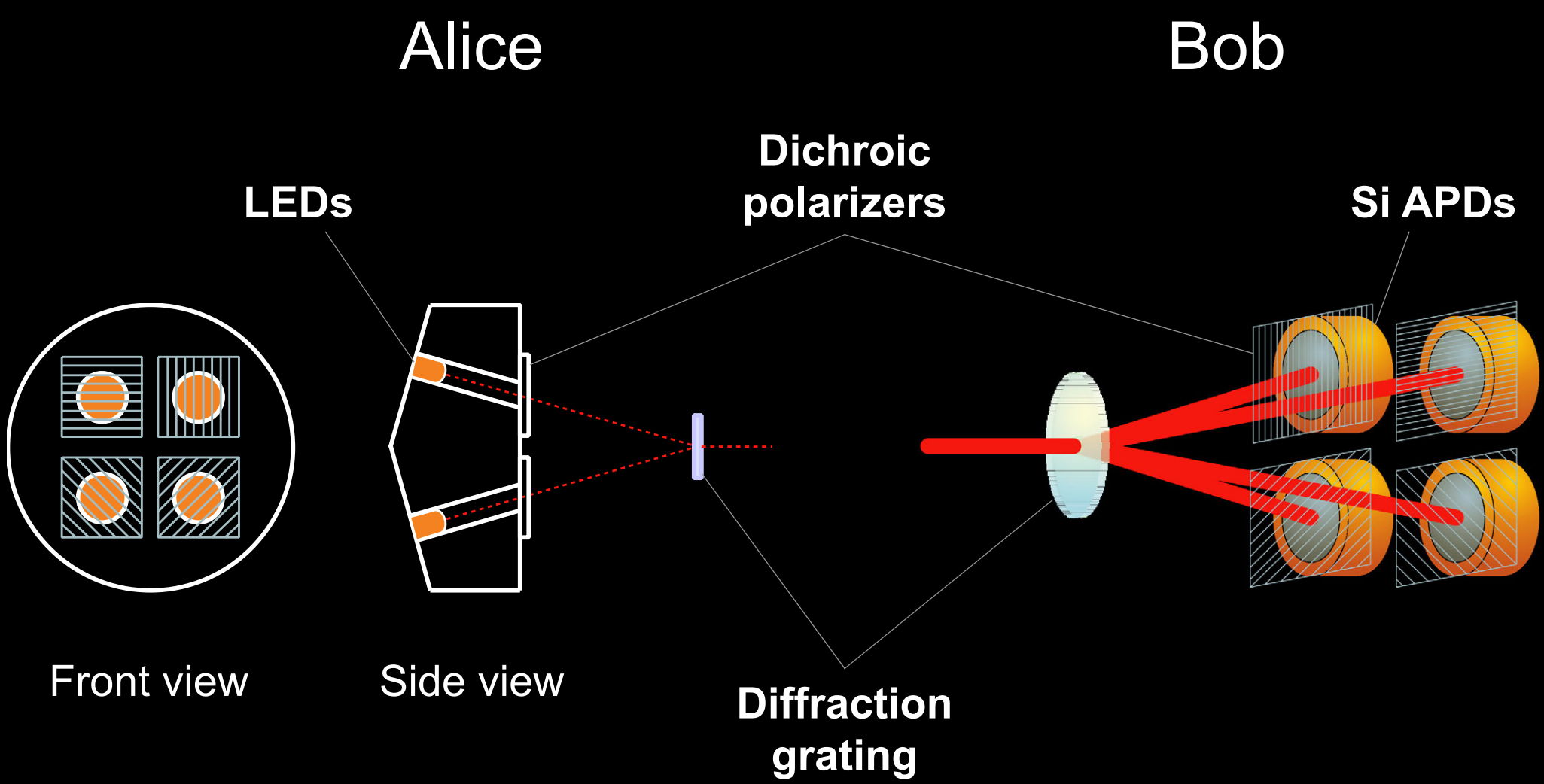
Solution: quantum ATM





J. L. Duligall *et al.,* New J. Phys. **8**, 249 (2006)

Solution: quantum ATM



Key rate: ~4 Kbit/s

J. L. Duligall *et al.*, New J. Phys. **8**, 249 (2006)

UNIVERSITY OF WATERLOO

Quantum hacking lab

vad1.com/lab

UNIVERSITY OF WATERLOO

Quantum hacking lab

vad1.com/lab