# Quantum cryptography: from theory to practice

**Eleni Diamanti**

**Laboratoire Traitement et Communication de l'Information**

**CNRS – Télécom ParisTech**

1

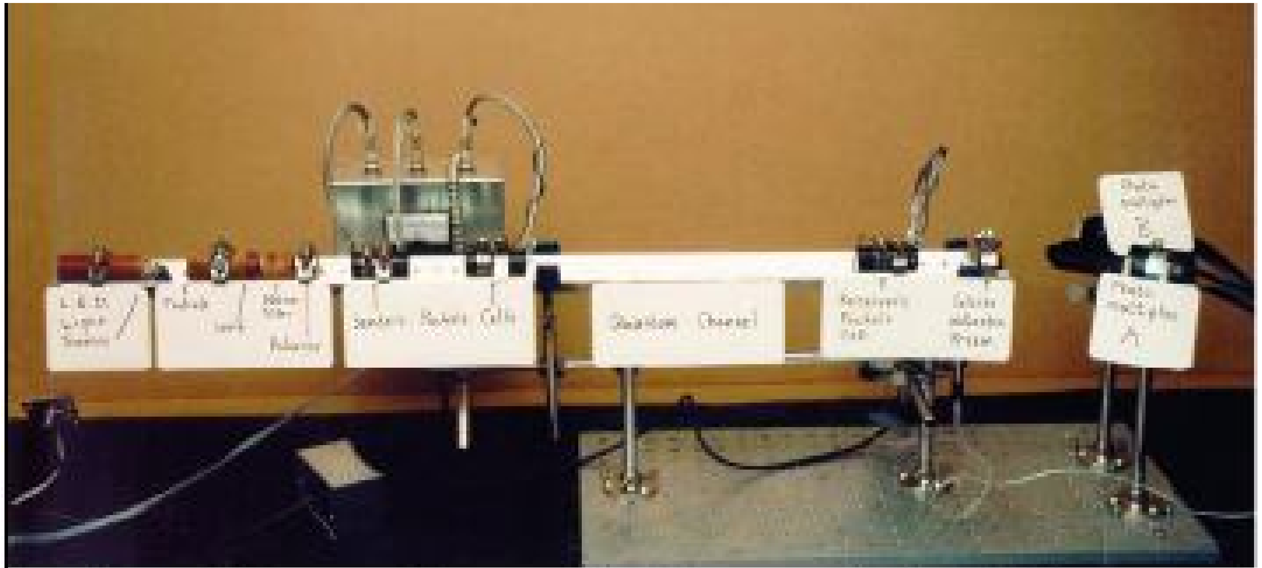
with

Anna Pappa, André Chailloux, Iordanis Kerenidis

# Two-party secure communications: QKD

Alice and Bob trust each other but not the channel
Primitive for message exchange: key distribution

BB84 QKD protocol: possibly the precursor of the entire field

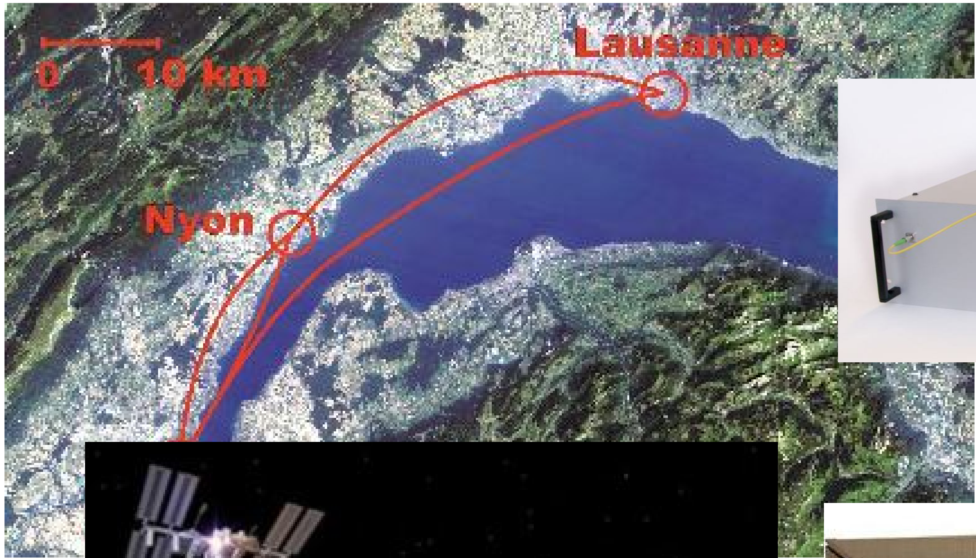


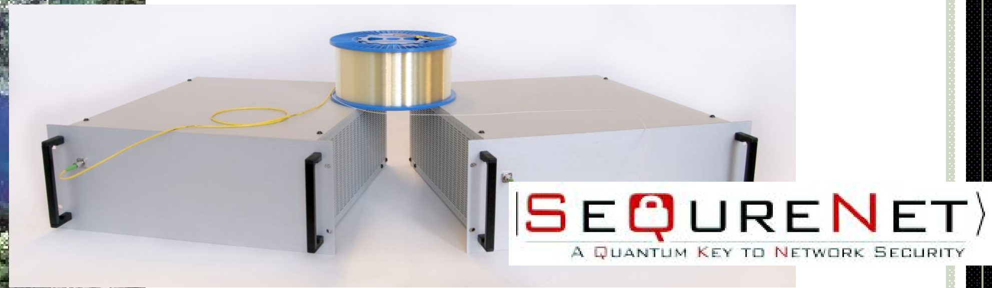
Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

Sender's side produces very faint green light pulses of 4 different polarizations.

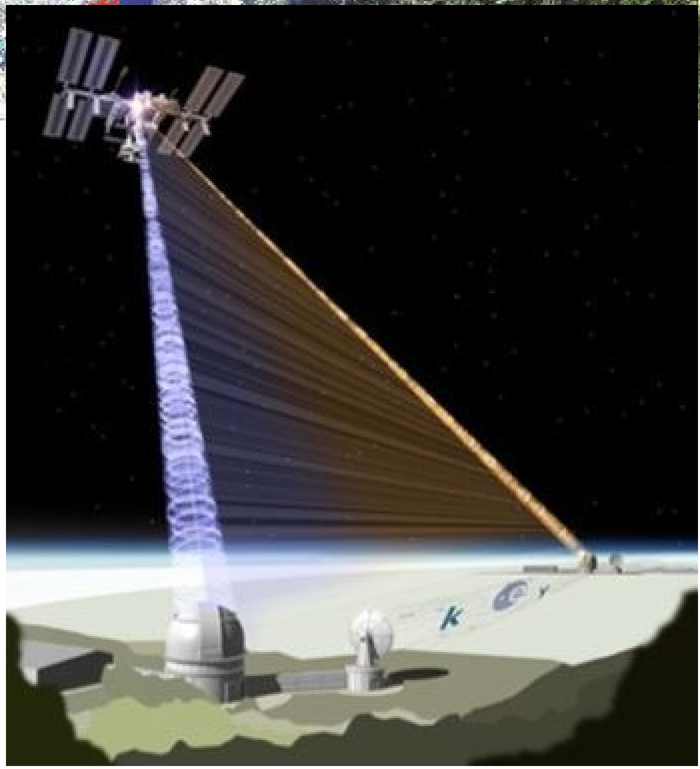
Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

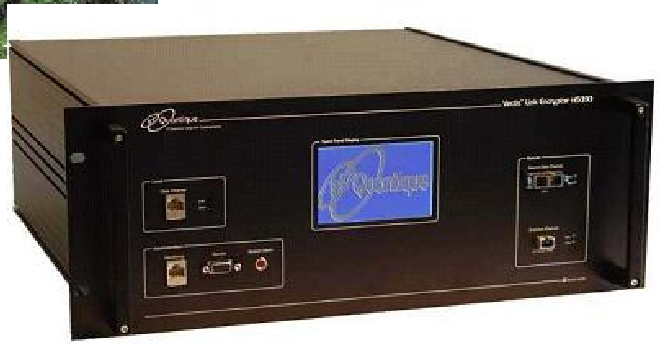
Calcite prism separates polarizations. Photomultiplier tubes detect single photons.

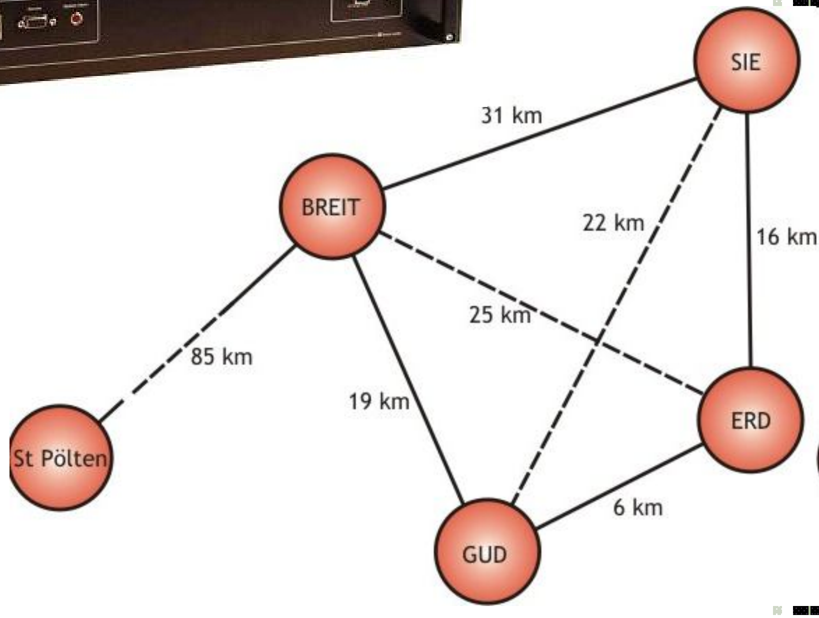



Jouguet, Kunz-Jacques, Leverrier, Grangier, D, Nature Photon. 2013








Scarani et al, Rev. Mod. Phys. 2009

# Two-party secure communications: QKD

**Information-theoretic security is possible and feasible!**

Theory adapted to experimental imperfections

- 2000: Using laser sources opens a disastrous security loophole in BB84

  $\rightarrow$ photon number splitting attacks

  Brassard, Lütkenhaus, Mor, Sanders, Phys. Rev. Lett. 2000

- Solution: Decoy state BB84 protocol, and other

  Lo, Ma, Chen, Phys. Rev. Lett. 2004

- 2010: Quantum hacking: setup vulnerabilities not taken into account in security proofs

  Lydersen et al, Nature Photon. 2010

- Solution: Exhaustive search for side channels and updated security proofs? Device independence? Measurement device independence?

# Two-party secure communications: beyond QKD

Alice and Bob do not trust each other
Primitives for joint operations: bit commitment, coin flipping, oblivious transfer

- Until recently relatively ignored by physicists

  → perfect unconditionally secure protocols are impossible,
  but imperfect protocols with information-theoretic security exist
  ideal framework to demonstrate quantum advantage

  → protocols require inaccessible resources, like quantum memories, generation of qutrits, perfect single photons,…

  → they are vulnerable to experimental imperfections (losses, noise, imperfect detectors and sources)

PHYSICAL REVIEW A **80**, 062321 (2009)

## Fair loss-tolerant quantum coin flipping

Guido Berlín,[1,*] Gilles Brassard,[1,†] Félix Bussières,[2,3,‡] and Nicolas Godbout[2,§]

Received 8 Jul 2011 | Accepted 27 Oct 2011 | Published 29 Nov 2011

DOI: 10.1038/ncomms1572

# Experimental loss-tolerant quantum coin flipping

Guido Berlín[1], Gilles Brassard[1], Félix Bussières[2,3,4], Nicolas Godbout[2], Joshua A. Slater[3] & Wolfgang Tittel[3]

## Experimental implementation of bit commitment in the noisy-storage model

Nelly Huei Ying Ng,[1,2] Siddarth K. Joshi,[2] Chia Chen Ming,[2] Christian Kurtsiefer,[2,3] and Stephanie Wehner[2,4,*]

Nature Commun. 2012

## Experimental bit commitment based on quantum communication and special relativity

T. Lunghi,[1] J. Kaniewski,[2] F. Bussières,[1] R. Houlmann,[1]
M. Tomamichel,[2] A. Kent,[3,4] N. Gisin,[1] S. Wehner,[2] and H. Zbinden[1]

arXiv 1306.4801

## Experimental unconditionally secure bit commitment

Yang Liu[1,*], Yuan Cao[1,*], Marcos Curty[2,*], Sheng-Kai Liao[1], Jian Wang[1], Ke Cui[1], Yu-Huai Li[1], Ze-Hong Lin[1], Qi-Chao Sun[1], Dong-Dong Li[1], Hong-Fei Zhang[1], Yong Zhao[1,3], Cheng-Zhi Peng[1], Qiang Zhang[1], Adán Cabello[4], Jian-Wei Pan[1]

arXiv 1306.4413

## An Experimental Implementation of Oblivious Transfer in the Noisy Storage Model

C. Erven[1,2,*] N. Ng[3], N. Gigov[1], R. Laflamme[1,4], S. Wehner[3], and G. Weihs[1,5]

arXiv 1308.5098

PHYSICAL REVIEW A **84**, 052305 (2011)

## Practical quantum coin flipping

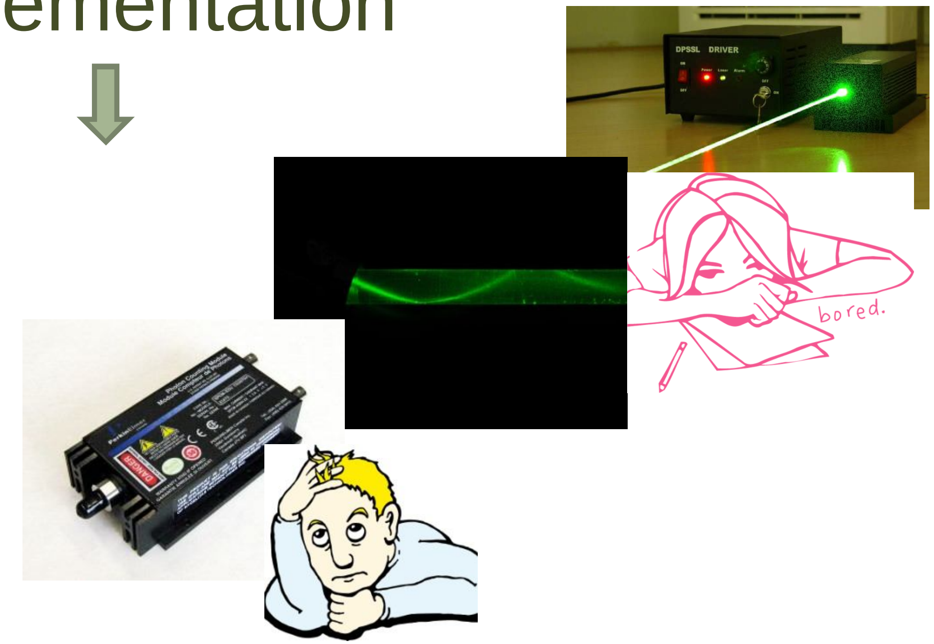
Anna Pappa,[1,*] André Chailloux,[2,†] Eleni Diamanti,[1,‡] and Iordanis Kerenidis[2,§]

## Experimental plug&play quantum coin flipping

Anna Pappa,[1,2] Paul Jouguet,[1,3] Thomas Lawson,[1] André Chailloux,[2,4] Matthieu Legré,[5] Patrick Trinkler,[5] Iordanis Kerenidis,[2,6] and Eleni Diamanti[1]

arXiv 1306.3368

# Adapting theory to implementation




**Strong quantum coin flipping**

Allows two spatially separated distrustful parties to agree on a random bit, whose value should not be biased

For unbounded adversaries: $\varepsilon > 0$

But better than classical protocols exist : lower bound $\varepsilon = \dfrac{1}{\sqrt{2}} - \dfrac{1}{2} \approx 0.21$

Aharonov, Ta-Shma, Vazirani, Yao, STOC 2000
Spekkens and Rudolph 2001
Kitaev 2003, Ambainis 2004
Chailloux and Kerenidis, FOCS 2009

# Ambainis protocol

Alice　　　　　　　　　　　　　　　　　Bob

*Step 1*　Randomly picks $\alpha, c \in \{0,1\}$　Prepares $\left|\Phi_{\alpha,c}\right\rangle$ →

$$\left|\Phi_{0,c}\right\rangle = \left(\left|0\right\rangle + (-1)^c \left|1\right\rangle\right) / \sqrt{2}$$
$$\left|\Phi_{1,c}\right\rangle = \left(\left|0\right\rangle + (-1)^c \left|2\right\rangle\right) / \sqrt{2}$$
$$(\rho_0 \neq \rho_1)$$

*Step 2*　Bob stores qutrit in quantum memory

*Step 3*　← Random bit $b$

*Step 4*　$\alpha$ , $c$ →

*Step 5*　Randomly picks $\beta \in \{0,1\}$, measures on the $B_\beta = \left\{\left|\Phi_{\beta,0}\right\rangle, \left|\Phi_{\beta,1}\right\rangle, \left|2-\beta\right\rangle\right\}$ basis

Bob checks if his measurement result is $c$ otherwise he aborts

Optical fibers, components, detectors, memories have losses…

Coin value $x = \alpha \oplus b$

# Vulnerability to losses

- All possible strategies to take losses into account break the protocol
- Bob must measure in Step 2, increases Alice's bias a bit but still ok

  $\rightarrow$ great!

- But then Bob can discriminate $\rho_0, \rho_1$ conclusively with positive probability

  $\rightarrow$ protocol completely broken

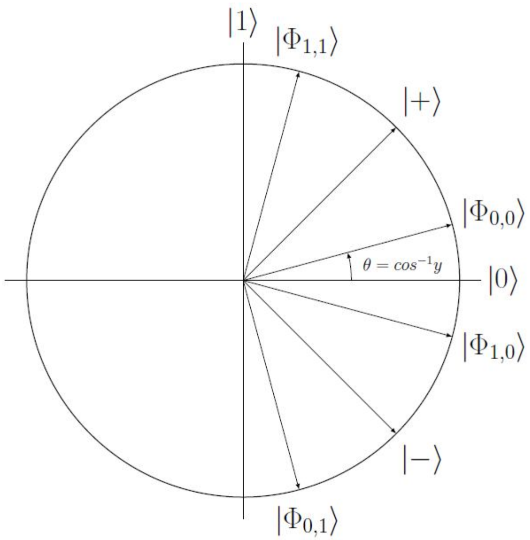
# First step: achieving loss tolerance

Alice | Bob

*Step 1* — Randomly picks $\alpha, c \in \{0,1\}$ — Prepares $|\Phi_{\alpha,c}\rangle$ →

$$|\Phi_{\alpha,0}\rangle = \sqrt{y}\,|0\rangle + (-1)^{\alpha}\sqrt{1-y}\,|1\rangle$$

$$|\Phi_{\alpha,1}\rangle = \sqrt{1-y}\,|0\rangle - (-1)^{\alpha}\sqrt{y}\,|1\rangle$$




*Step 2* — Randomly picks $\beta \in \{0,1\}$, measures on the $B_\beta = \{|\Phi_{\beta,0}\rangle, |\Phi_{\beta,1}\rangle\}$ basis; if no output asks to start again, otherwise Step 3

*Step 3* — ← Random bit $b$

*Step 4* — $\alpha$ , $c$ →

*Step 5* — If $\alpha = \beta$, Bob checks if his measurement result is $c$, otherwise he aborts

If $\alpha \neq \beta$, he cannot verify and accepts

Coin value $x = c \oplus b$

Berlin et al, Phys. Rev. A 2009

# Vulnerability to noise and multi-photon pulses

- Bob can ask to restart the protocol if he gets no detection $\rightarrow$ crucial for loss tolerance (for any value of loss!)
- Alice chooses a bit $c = 0,1$, for which $\rho_0 \neq \rho_1$ and there is no conclusive discrimination measurement
- Protocol fair for $y = 0.9$, for which $\varepsilon = 0.4$

But what about practical imperfections other than loss?

- Theoretical analysis does not take into account noise (errors, dark counts,…)
  $\rightarrow$ probability for honest abort is always zero

- Protocol becomes completely insecure in the presence of multi-photon pulses
  $\rightarrow$ there is a conclusive measurement to distinguish between $\rho_0, \rho_1$ when two identical states are in a pulse, Bob can measure in both bases $B_0, B_1$
  recall the photon number splitting attacks in QKD!

# Second step: taking into account imperfections

Alice | Bob

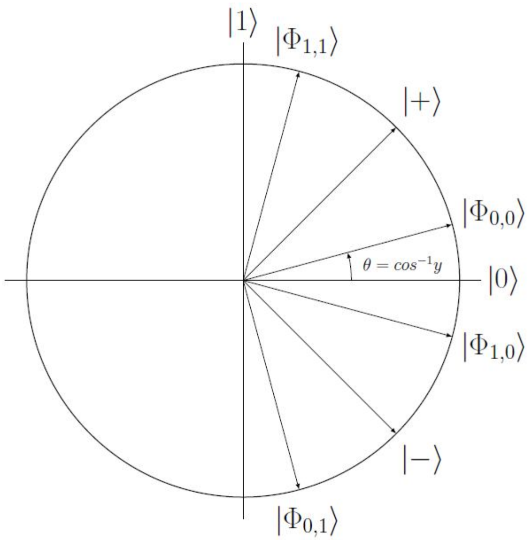
**Step 1**

Randomly picks $\alpha_i, c_i \in \{0,1\}, \quad i = 1,\ldots,K$

Pulse mean photon number follows $p_i = e^{-\mu}\mu^i / i!$

$$\left|\Phi_{\alpha_i,0}\right\rangle = \sqrt{y}\,|0\rangle + (-1)^{\alpha_i}\sqrt{1-y}\,|1\rangle$$
$$\left|\Phi_{\alpha_i,1}\right\rangle = \sqrt{1-y}\,|0\rangle - (-1)^{\alpha_i}\sqrt{y}\,|1\rangle$$

Prepares $\left|\Phi_{\alpha_i,c_i}\right\rangle$ $\longrightarrow$




**Step 2**

Randomly picks $\beta_i \in \{0,1\}$ for every pulse;
if his detectors do not click he aborts,
otherwise $j$ is first detected pulse

**Step 3**

$\longleftarrow$ $b, j$

**Step 4**

$\alpha_j, c_j$ $\longrightarrow$

**Step 5**

If $\alpha_j = \beta_j$, Bob checks if his measurement result is $c_j$, otherwise he aborts

If $\alpha_j \neq \beta_j$ he cannot verify and accepts

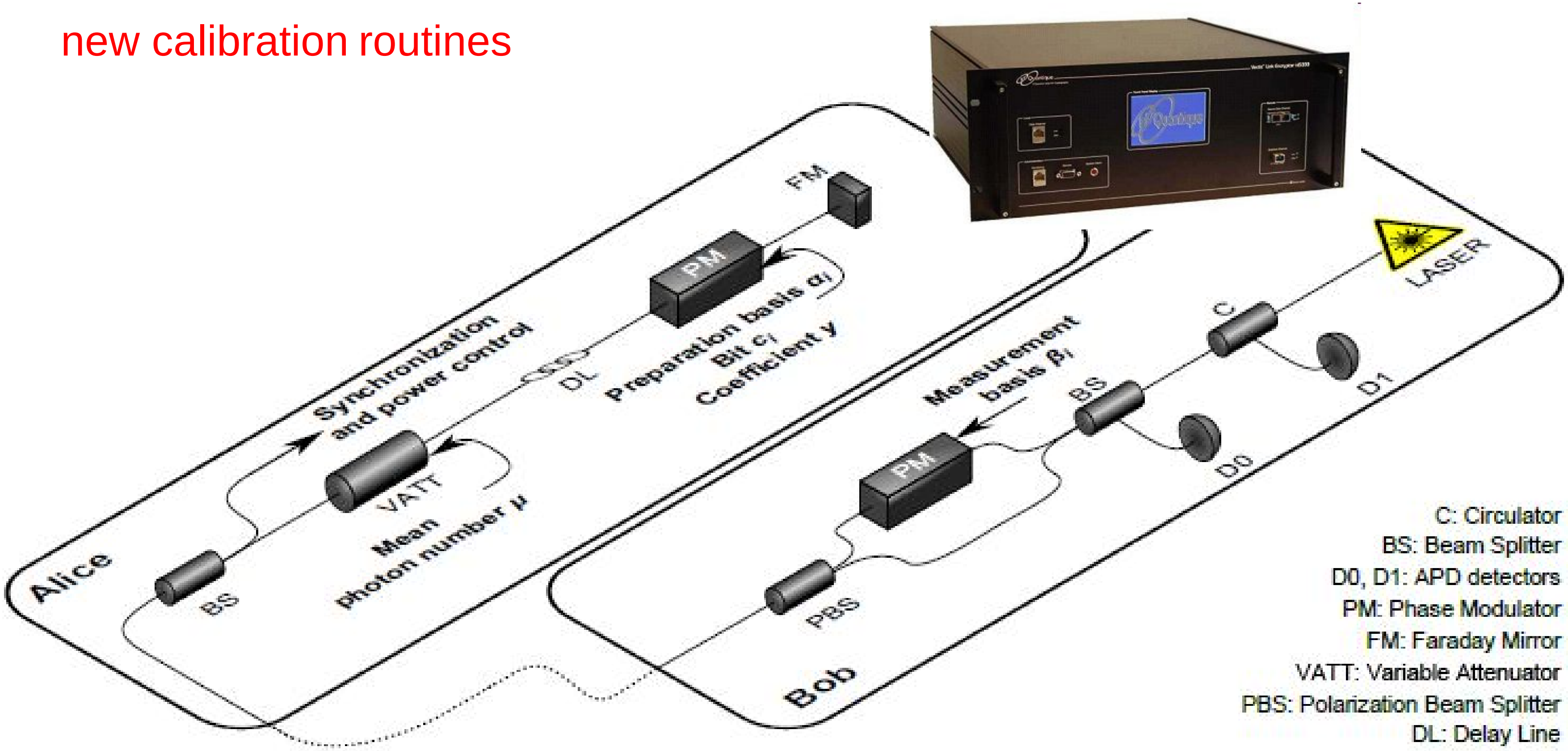
Pappa et al, Phys. Rev. A 2011

Coin value $x = c_j \oplus b$

# Experimental implementation

Experiment based on a commercial plug&play QKD system

- high-quality single-photon detectors
- rotated BB84 states
- very low mean photon number regime
- new calibration routines



# Security of the implementation

- Our system has losses, single-photon detectors with dark counts and finite quantum efficiency, multi-photon pulses, noise

  $\rightarrow$ these all lead to a probability of honest abort

- By setting a target honest abort probability, we can minimize the cheating probability for a fair protocol by finding optimal values of $\mu, K, y$

Is this enough to claim security?

- Are the basis and bit values chosen by Alice and Bob really independently and randomly?
- Might it be possible that Bob detects one state much more often than another?
- Security proof does not hold if security assumptions are not satisfied in practice!

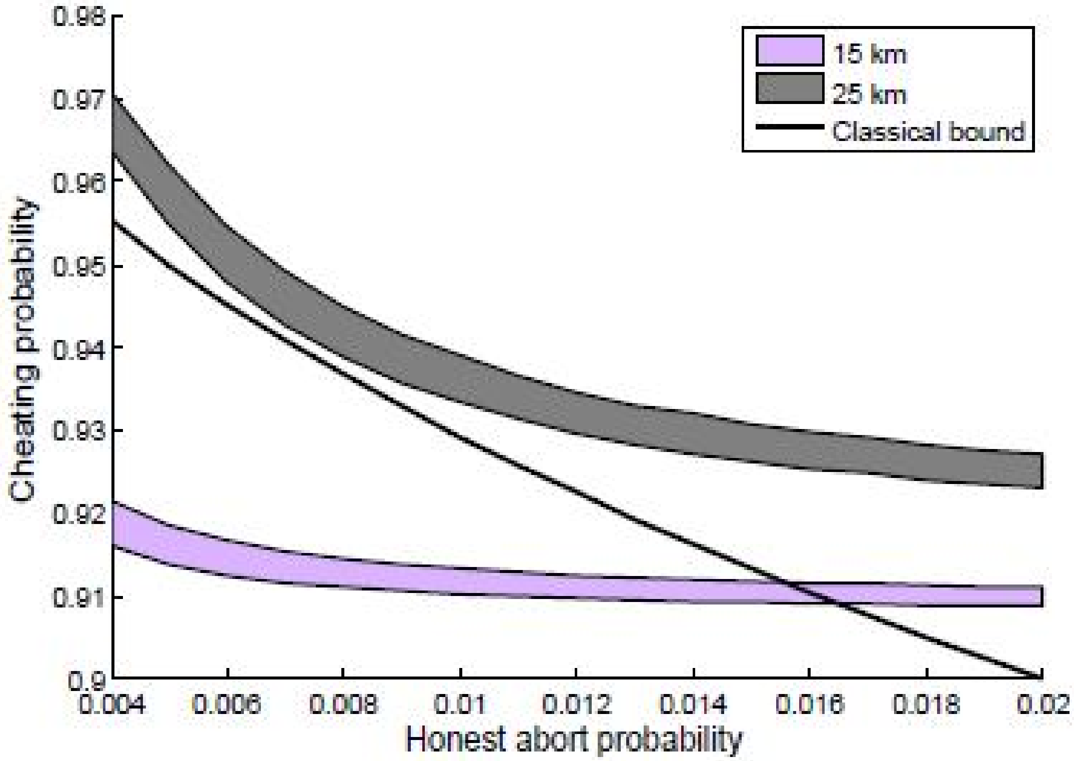
# Third step: satisfying the security assumptions

- From analysis of experimental detection events and characteristics of random number generators and phase modulators used for bit and basis choices :
  - Alice's state distribution probability away from uniform $\leq \varepsilon_A$
  - Bob's basis and bit distribution probability (for pulse used for coin) away from uniform $\leq \varepsilon_B$
  - Bob's outcomes very biased due to significant detector efficiency asymmetry $\rightarrow$ important security loophole!

    Solution: symmetrization of losses

    after this procedure, efficiency ratio away from 1 $\leq \varepsilon_{B'}$
- Optimal cheating strategies depend on security parameters $\varepsilon_A, \varepsilon_B, \varepsilon_{B'}$

# Showing quantum advantage in practice




- Comparison with classical bound: $p_c \leq 1 - \sqrt{H/2}, \quad H \leq 1/2$

  Hanggi and Wullschleger, TCC 2011

- Maximum communication distance smaller than in QKD



Pappa et al, arXiv 1306.3368

# Conclusions and open questions

- Flipping a single coin with security guarantees better than in any classical protocol is possible with present quantum technology

- Quantum information can be used beyond key distribution to achieve in practice cryptographic tasks in the distrustful model

- Is it possible to systematically find explicit, efficient and implementable protocols and adapt them to realistic conditions?

- Can we use current methods and techniques to a wide range of quantum games and protocols?

Pappa, Chailloux, Wehner, D, Kerenidis, Phys. Rev. Lett. 2012

- Roadmap to truly useful quantum information technology, even before a quantum computer becomes available

**Demonstrating quantum gap in practice is challenging, rewarding, and of both fundamental and applied interest**