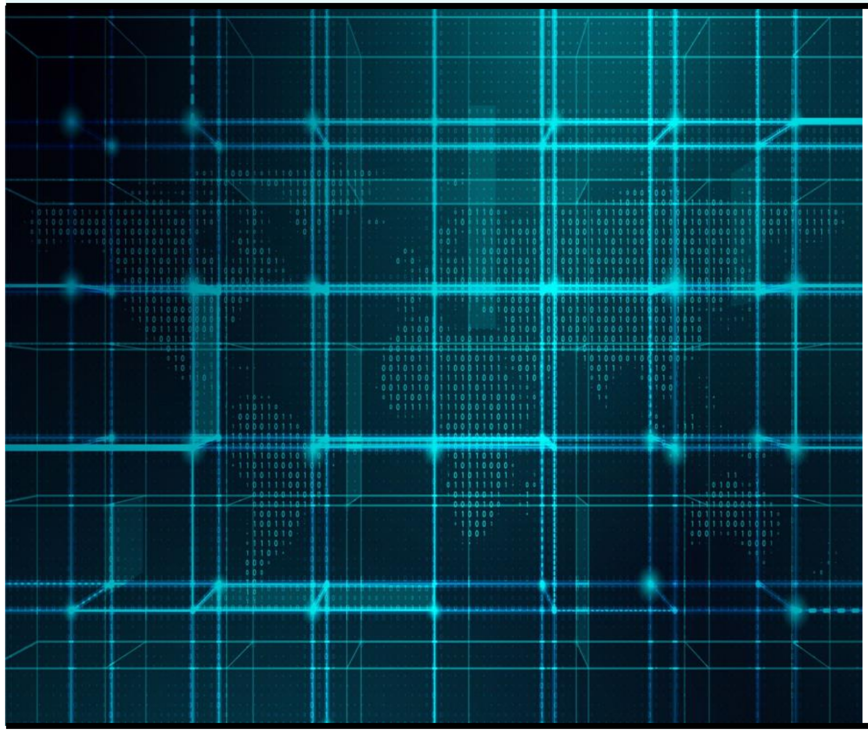
ICE-8 Quantum Information in Spain

Fully passive quantum key distribution

Víctor Zapatero[1,2,3] & Marcos Curty[1,2,3]

[1]Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain
[2]EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
[3]AtlanTTic Research Center, University of Vigo, Vigo E-36310, Spain



UNIVERSIDADE DE VIGO

atlanTTic research center for Telecommunication Technologies

29/05/2023

PUBLIC-KEY CRYPTOGRAPHY

1

Programming Techniques — S.L. Graham, R.L. Rivest* Editors

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R. L. Rivest, A. Shamir, and L. Adleman
MIT Laboratory for Computer Science and Department of Mathematics

- Private key, public key
- Computational security
- Ubiquitous example: RSA
- Weaknesses

2

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

3

Factoring integers with sublinear resources on a superconducting quantum processor

Bao Yan,[1,2,*] Ziqi Tan,[3,*] Shijie Wei,[4,*] Haocong Jiang,[5] Weilong Wang,[1] Hong Wang,[1] Lan Luo,[1] Qianheng Duan,[1] Yiting Liu,[1] Wenhao Shi,[1] Yangyang Fei,[1] Xiangdong Meng,[1] Yu Han,[1] Zheng Shan,[1] Jiachen Chen,[3] Xuhao Zhu,[3] Chuanyu Zhang,[3] Feitong Jin,[3] Hekang Li,[3] Chao Song,[3] Zhen Wang,[3,†] Zhi Ma,[1,‡] H. Wang,[3] and Gui-Lu Long[2,4,6,7,§]

POST-QUANTUM CRYPTOGRAPHY

NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

Federal agency reveals the first group of winners from its six-year competition.

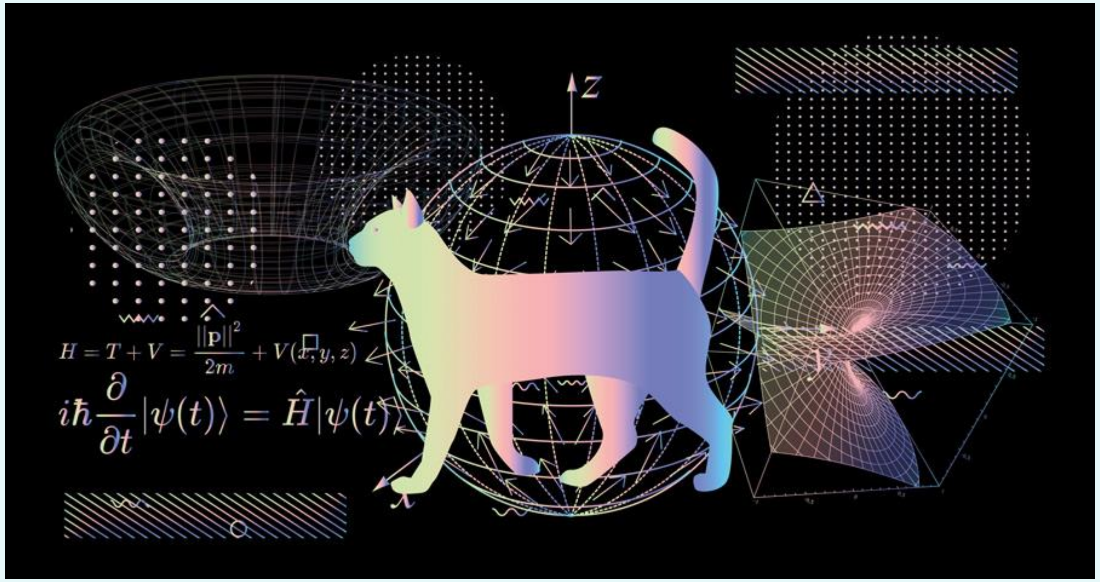
- Most popular approach
- Basic idea: quantum resistant public-key cryptography
- NIST standardization competition
- Fudamentally speculative

QUANTUM CRYPTOGRAPHY

- Radically different approach: take advantage of quantum mechanics (no cloning, monogamy)

- Private key-cryptography (key distribution, information-theoretic security)

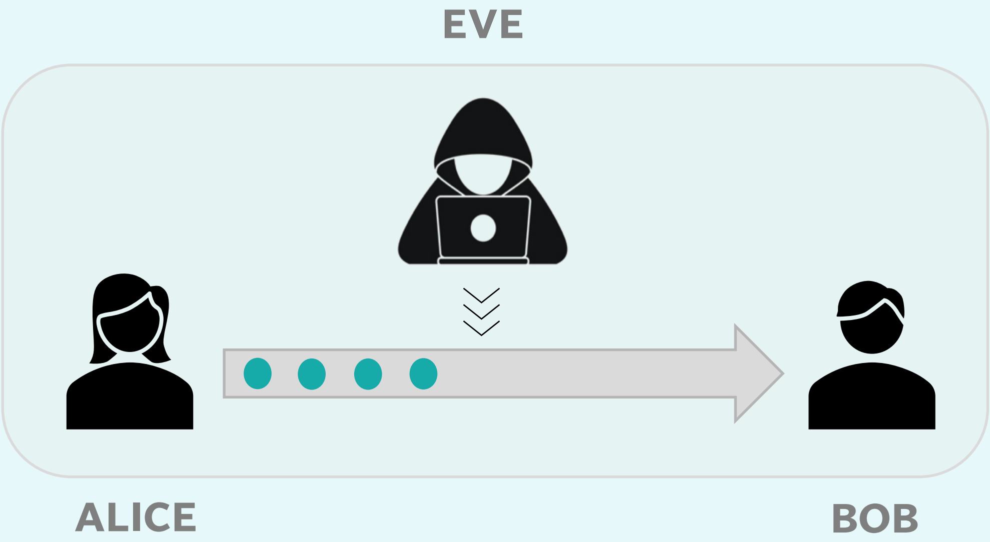
- Solving the key distribution problem: quantum key distribution (BB84 protocol)



QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

THE BB84 PROTOCOL



Rectilinear basis: $\{|H\rangle, |V\rangle\}$

Diagonal basis: $\left\{|+\rangle = \frac{|H\rangle+|V\rangle}{\sqrt{2}}, |-\rangle = \frac{|H\rangle-|V\rangle}{\sqrt{2}}\right\}$

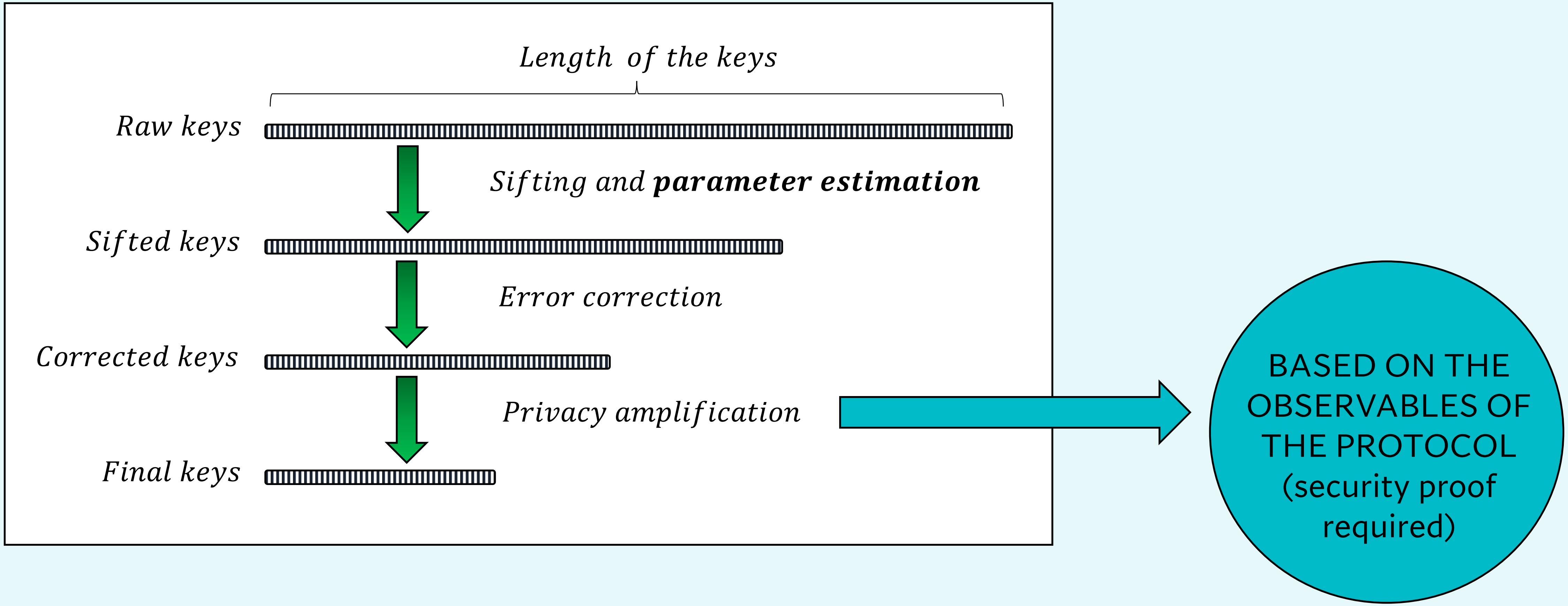
RECIPE
Only the basis-match events matter:
rectilinear basis match→ key round
diagonal basis match → test round

TRANSMITTER
Randomly prepare $|H\rangle$, $|V\rangle$, $|+\rangle$ or $|-\rangle$

RECEIVER
Randomly measure rectilinear basis or diagonal basis

29/05/2023

QKD POST-PROCESSING



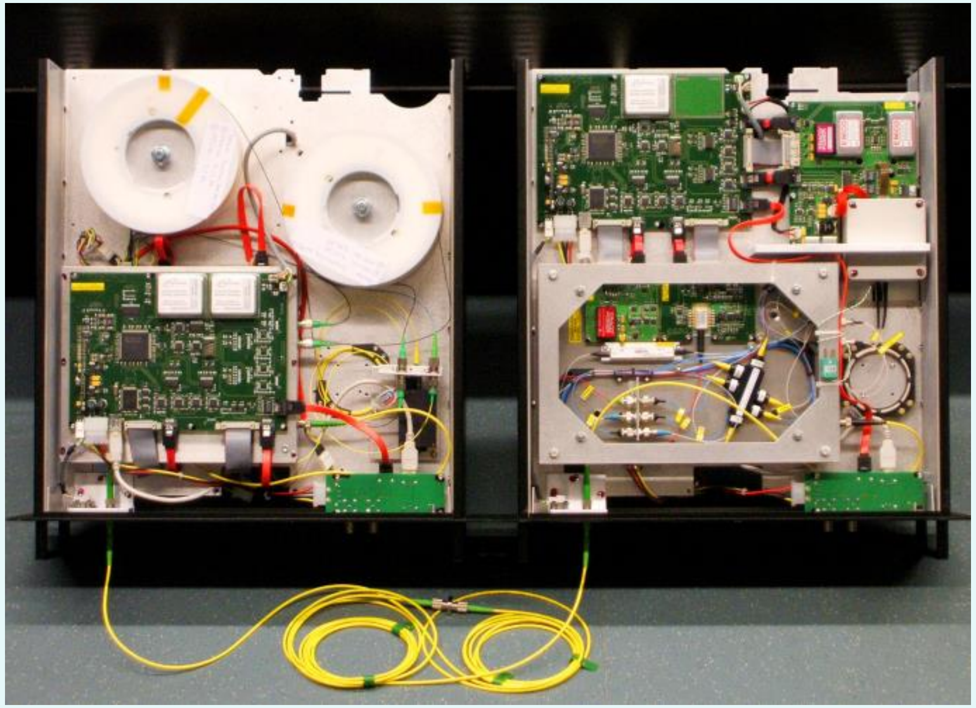
SUMMARY: QKD VERSUS POST-QUANTUM CRYPTO

PROS
✓ Fundamental security upgrade (long-term secuity warrant)

CONS
× Limited performance (keyrate, distance)

× More complex and costly (new infrastructure)

× Implementation security issues (quantum hacking)

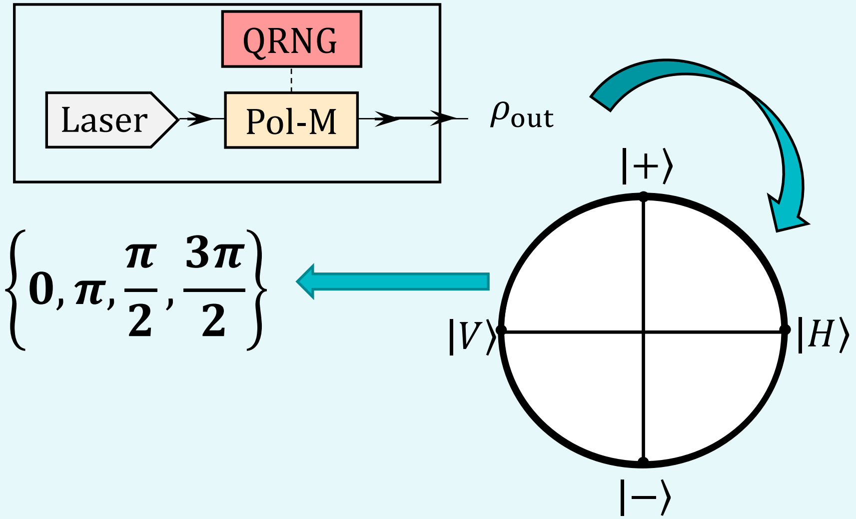


Complex hardware inside a commercial QKD system.

AN ALTERNATIVE TO EXPLORE: PASSIVE QKD

ACTIVE QKD

Standard approach: active modulation (seeded by RNGs)

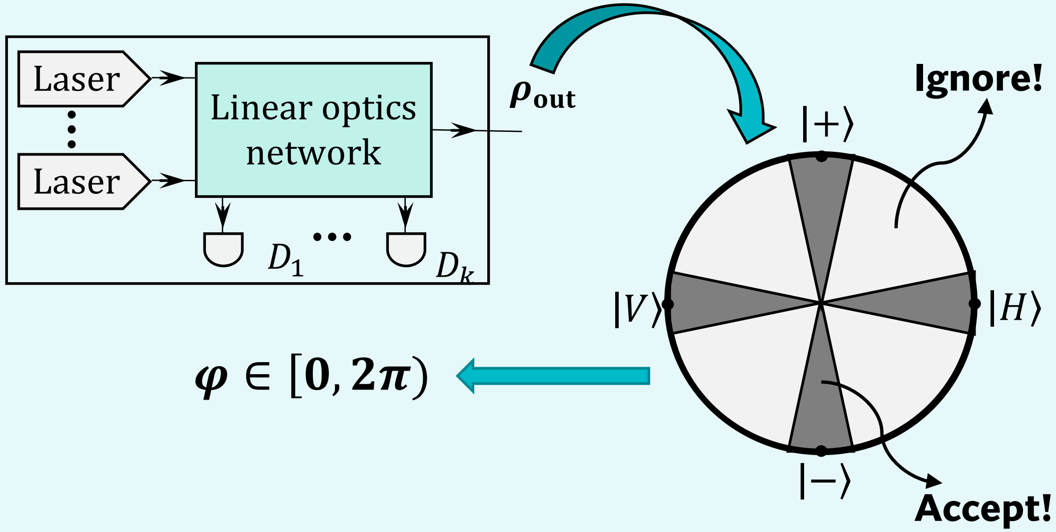


$$\varphi \in \left\{0, \pi, \frac{\pi}{2}, \frac{3\pi}{2}\right\}$$

- × Vulnerable to modulator side-channels (e.g. mode-dependencies, THAs)
- × More complex (hardware-wise)
- × Lower frequency of operation
- ✓ Higher secret key rate per pulse

PASSIVE QKD

Alternative approach: replace active modulation by a fixed "quantum mechanism" and a post-selection step



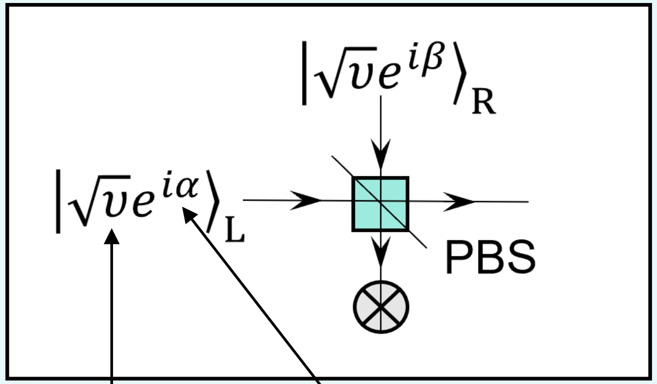
$$\varphi \in [0, 2\pi)$$

- ✓ Immune to modulator side-channels
- ✓ Presumably simpler and cheaper
- ✓ Higher frequency of operation
- × Lower secret key rate per pulse

AN ALTERNATIVE TO EXPLORE: PASSIVE QKD

PASSIVE IDEAL-BB84 ENCODING

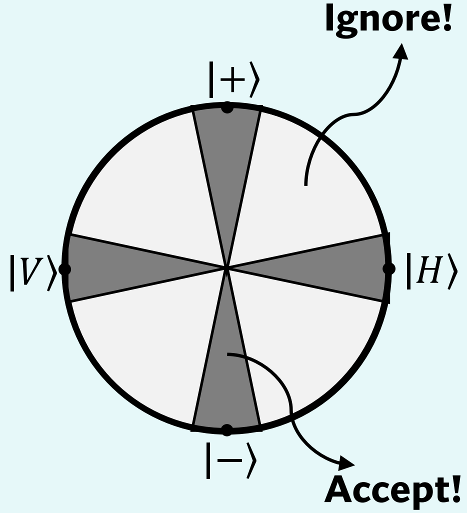
Curty, M., Ma, X., Qi, B., & Moroder, T. Physical Review A 81, 022310 (2010)



v = intensity of the coherent pulse (**e.g.** $v \approx 10^8$ **photons**)

α = phase of the coherent pulse

$\boldsymbol{\varphi = (\beta - \alpha) \sim U[0, 2\pi]}$



DIGRESSION: THE DECOY-STATE METHOD

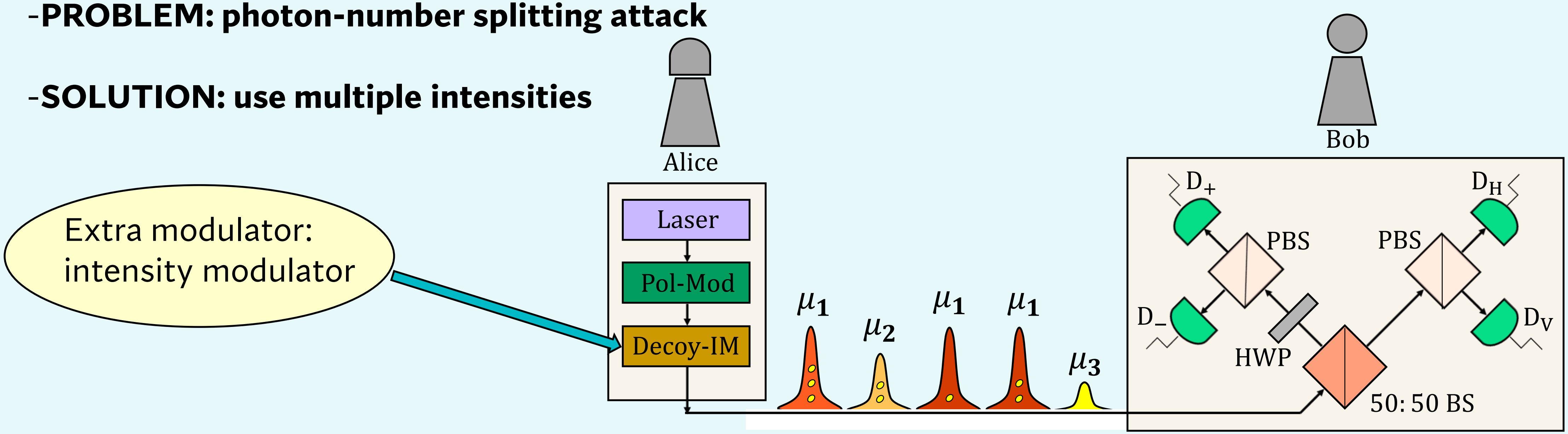
-IDEAL SOURCE : $|\mathbf{1}\rangle\langle\mathbf{1}|$

-REAL LASER SOURCE (phase-randomized coherent state) :

$$\int_0^{2\pi} d\alpha \left|\sqrt{v}e^{i\alpha}\right\rangle\left\langle\sqrt{v}e^{i\alpha}\right| = p_0|0\rangle\langle 0| + p_1|1\rangle\langle 1| + p_2|2\rangle\langle 2| + \cdots, \qquad p_k = \frac{e^{-\mu}\mu^k}{k!} \ (\mu = \text{"intensity"})$$

-**PROBLEM: photon-number splitting attack**

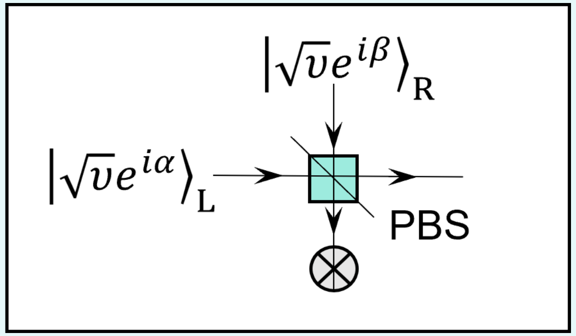
-**SOLUTION: use multiple intensities**



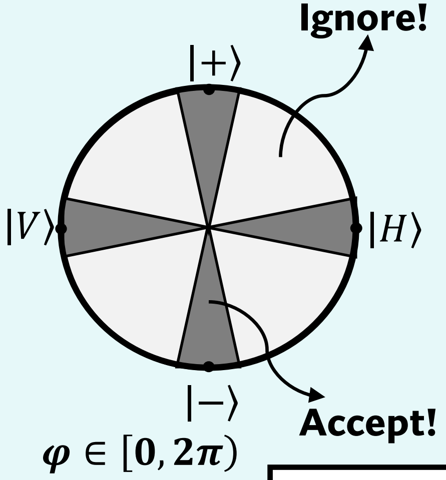
PASSIVE DECOY-STATE METHOD

PASSIVE IDEAL-BB84 ENCODING

Curty, M., Ma, X., Lo, H. K., & Lütkenhaus, N. Physical Review A 82, 052325 (2010)

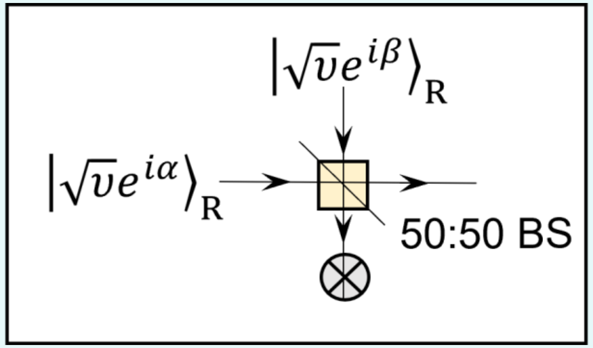


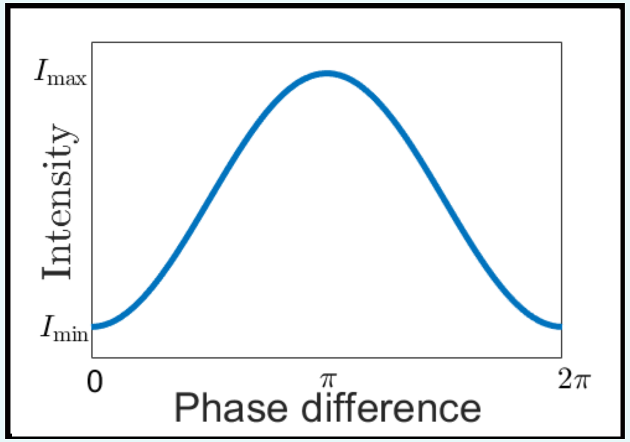
$\varphi = (\beta - \alpha) \sim U[0, 2\pi)$



PASSIVE DECOY-STATE METHOD

Curty, M., Ma, X., Qi, B., & Moroder, T. Physical Review A 81, 022310 (2010)





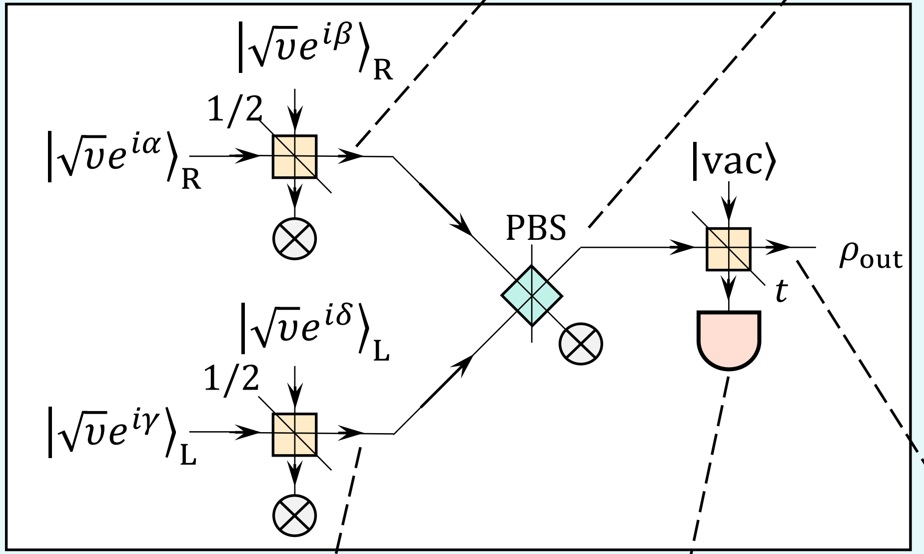
29/05/2023

PASSIVE DECOY-STATE BB84

e.g. $v \approx 10^8$ photons

passive BB84 encoding

passive decoy (R)



passive decoy (L)

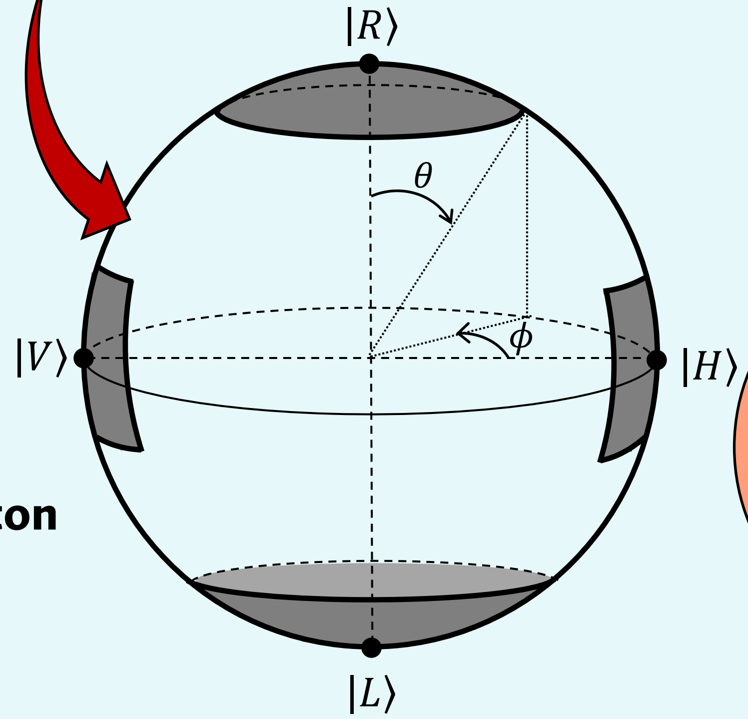
CLASSICAL
MEASUREMENT
(for post-selection)

$vt \approx$ 1 photon

DIFFICULTIES

-arbitrary polarization (not in a circle)

-polarization-decoy coupling



DECOY-STATE METHOD INVALIDATED!

DECOY-STATE LINEAR PROGRAMS

ACTIVE QKD → decoy-independent Fock states

"Yields" LP → **TARGET: y_1**

$$Q_j = \sum_n p_{n|j} y_n$$

- Q_j: Detection rates of the different decoys (observed)
- $p_{n|j}$: Known photon-number probabilities
- y_n: Detection rates of the different photon-numbers (unknowns)

"Error yields" LP → **TARGET: e_1**

$$E_j = \sum_n p_{n|j} e_n$$

- E_j: Detection-and-error rates of the different decoys
- e_n: Detection-and-error rates of the different photon-numbers

PASSIVE QKD → decoy-dependent Fock states

$$Q_j = \sum_n p_{n|j} y_{n,j} \qquad E_j = \sum_n p_{n|j} e_{n,j}$$

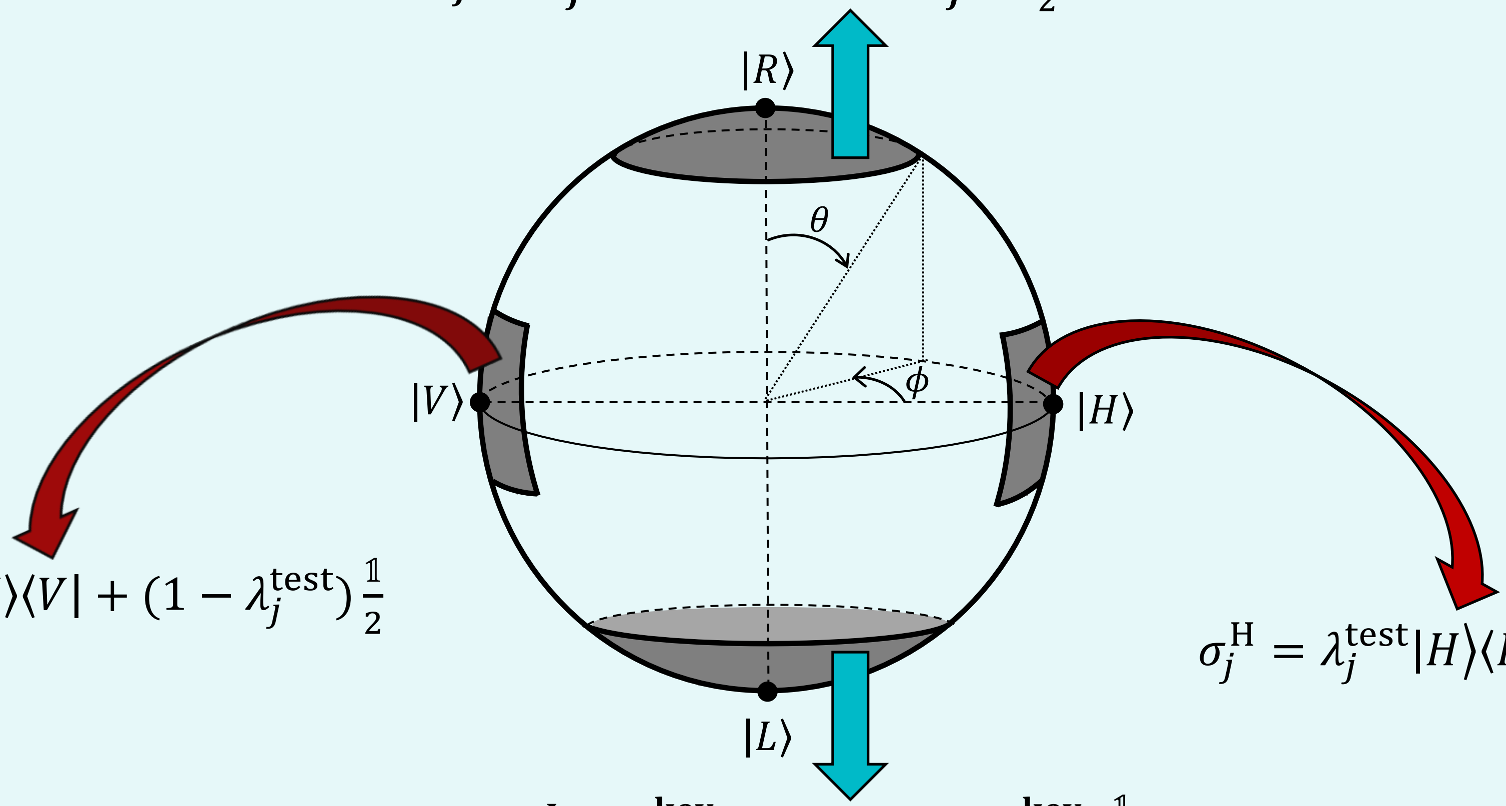
-**PROBLEM**: lack of constraints

-**SOLUTION**: additional trace-distance constraints

$$\left\{ |y_{n,j} - y_{n,k}| < \Delta_{j,k,n}, \qquad |e_{n,j} - e_{n,k}| < \tilde{\Delta}_{j,k,n} \right\}_{j,k,n}$$

NEW IDEA: NOISE-SUPPRESSING CONSTRAINTS

$\boldsymbol{\sigma_j^{\mathrm{R}}} = \lambda_j^{\mathbf{key}}|\boldsymbol{R}\rangle\langle\boldsymbol{R}| + (\mathbf{1} - \lambda_j^{\mathbf{key}})\frac{\mathbb{1}}{2}$ (i.e. "ideal state" + "white noise")



$\sigma_j^{\mathrm{V}} = \lambda_j^{\mathrm{test}}|V\rangle\langle V| + (1 - \lambda_j^{\mathrm{test}})\frac{\mathbb{1}}{2}$

$\sigma_j^{\mathrm{H}} = \lambda_j^{\mathrm{test}}|H\rangle\langle H| + (1 - \lambda_j^{\mathrm{test}})\frac{\mathbb{1}}{2}$

$\boldsymbol{\sigma_j^{\mathrm{L}}} = \lambda_j^{\mathbf{key}}|\boldsymbol{L}\rangle\langle\boldsymbol{L}| + (\mathbf{1} - \lambda_j^{\mathbf{key}})\frac{\mathbb{1}}{\mathbf{2}}$

PERFORMANCE OF PASSIVE QKD

KEY-RATE DECREASE (~1 o.m.)

(1) Additional sifting

(2) Inherent noise of the mixtures