Characterising the behaviour of classical-quantum broadcast networks

arXiv: 1803.04796

Ignatius William Primaatmaja, Yukun Wang, Emilien Lavie, Antonios Varvitsiotis, Charles Ci Wen Lim

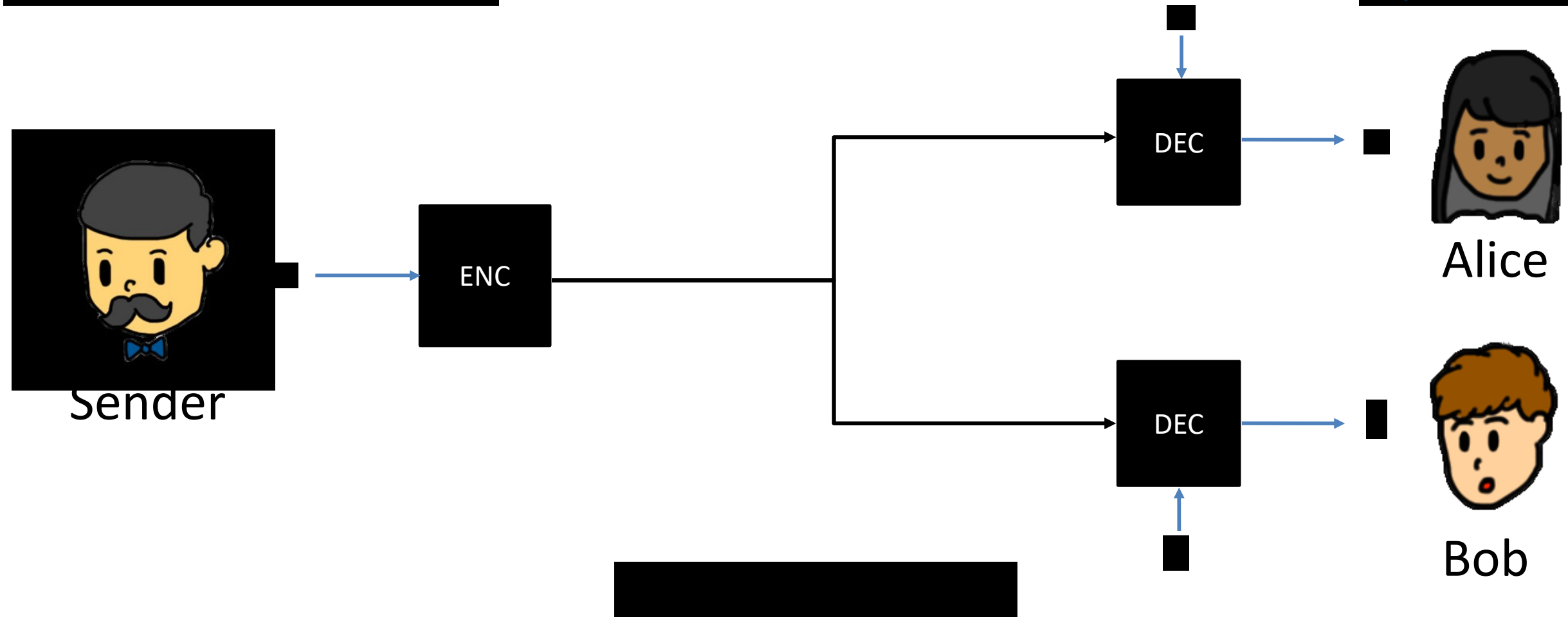
Outline

1. Numerical toolbox for characterisation of the behaviour of classical-quantum broadcast network
2. Application: analysis of security of quantum key distribution (QKD)
   - ✓ Phase encoding-BB84 protocol
   - ✓ Time-bin encoding three-state protocol with coherent states

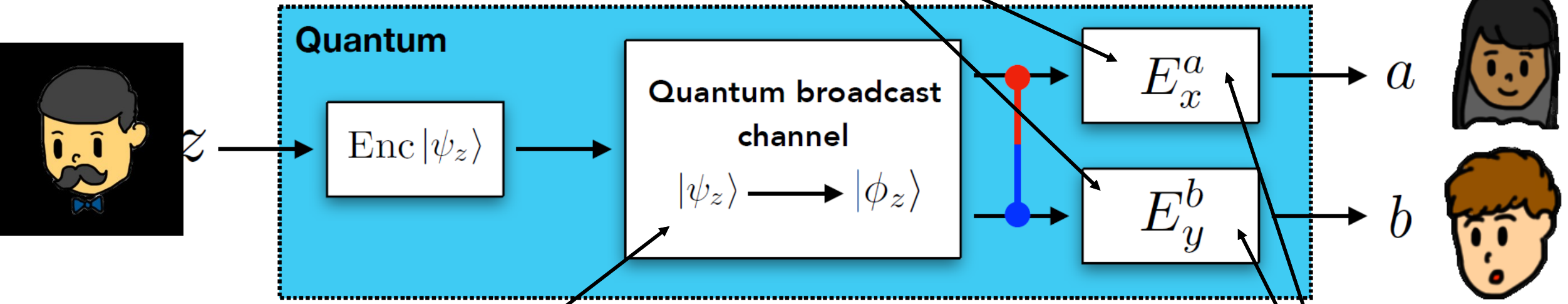
FIFA WORLD CUP RUSSIA 2018

beIN

OFFICIAL BROADCASTER

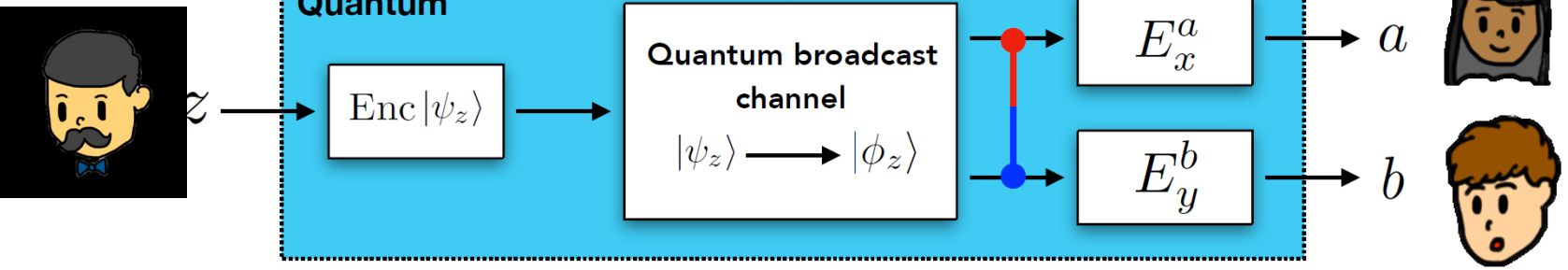

DEC
Alice
ENC
Sender
DEC
Bob
behaviour

separable measurements [redacted]



unitary operation [redacted]

projective measurements



What are the behaviour allowed by quantum physics?

No-cloning theorem
Wooters-Zurek, *Nature* (1982)

Information-disturbance trade-off
Fuchs & Peres, *PRA* (1996)
Horodecki et al, *Found. Phys*. (2005)

Indistinghuishability of non-orthogonal states
Holevo, *J. Multivariate Anal*. (1973)

Fundamental constraints on the correlations

Born's rule

Inner product

What are the allowed behaviour?

How do we do that when the dimension is unbounded?

Do we need to find all the states and measurements that satisfy the constraints?

We can consider semidefinite relaxations!

PRL 98, 010401 (2007) PHYSICAL REVIEW LETTERS week ending 5 JANUARY 2007

Bounding the Set of Quantum Correlations

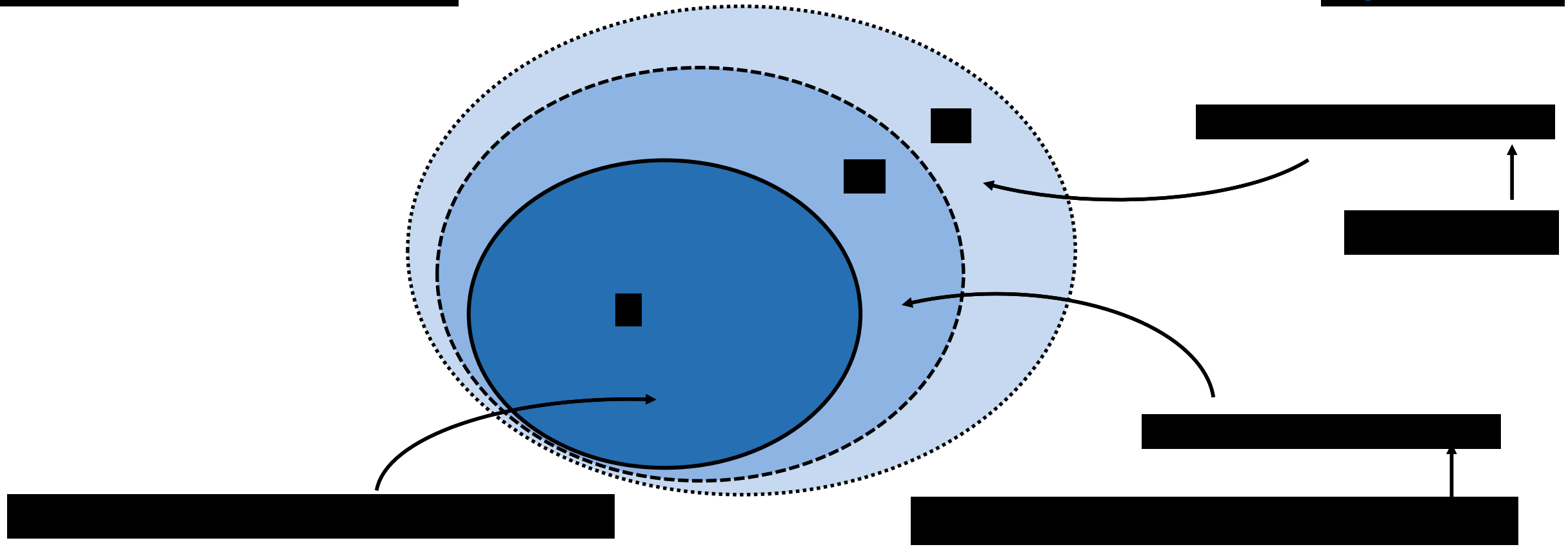
Miguel Navascués,* Stefano Pironio,† and Antonio Acín‡
ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain
(Received 18 July 2006; published 4 January 2007)

We introduce a hierarchy of conditions necessarily satisfied by any distribution $P_{\alpha\beta}$ representing the probabilities for two separate observers to obtain outcomes α and β when making local measurements on a shared quantum state. Each condition in this hierarchy is formulated as a semidefinite program. Among other applications, our approach can be used to obtain upper bounds on the quantum violation of an arbitrary Bell inequality. It yields, for instance, tight bounds for the violations of the Collins *et al.* inequalities.

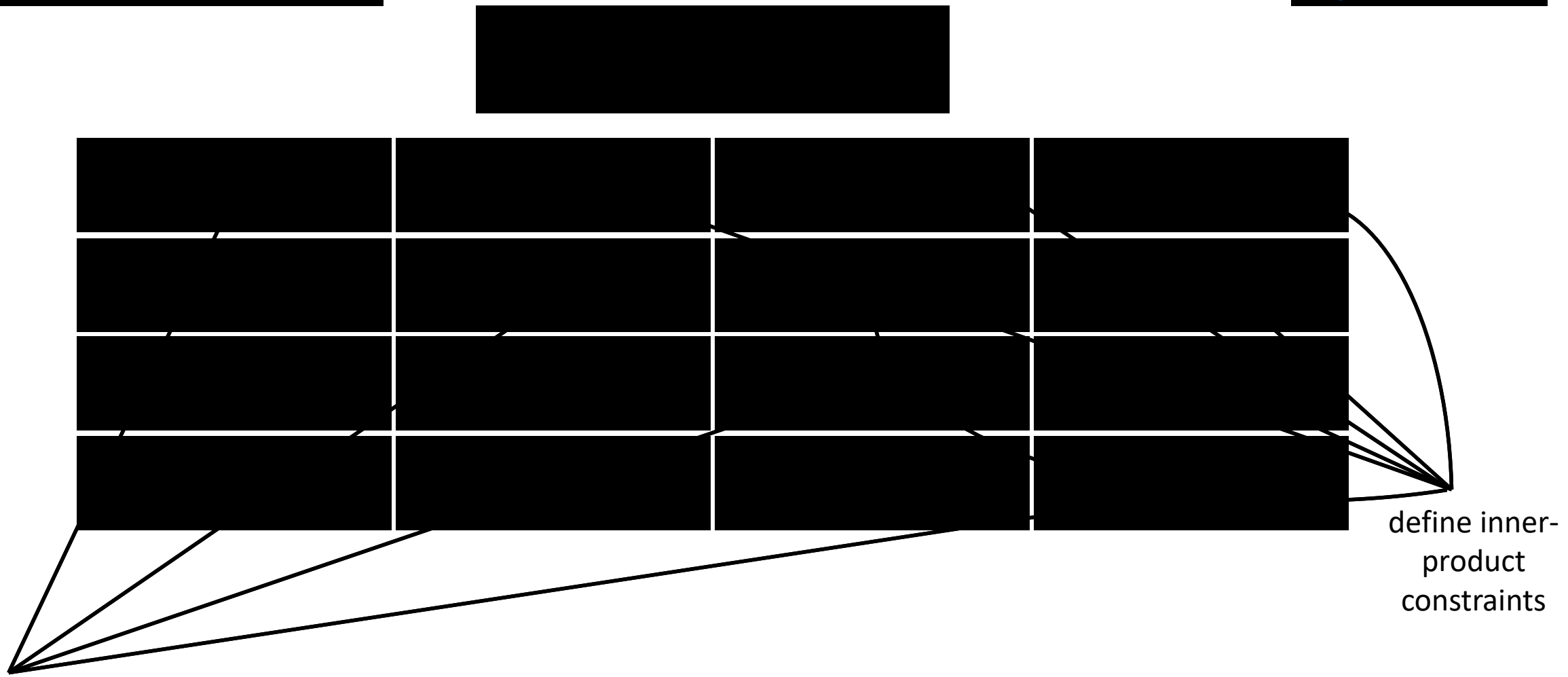
DOI: 10.1103/PhysRevLett.98.010401 PACS numbers: 03.65.Ud, 03.67.−a

Problem solved for the special case of fixed source

Navascués-Pironio-Acín (NPA) method
PRL (2007)
NJP (2008)



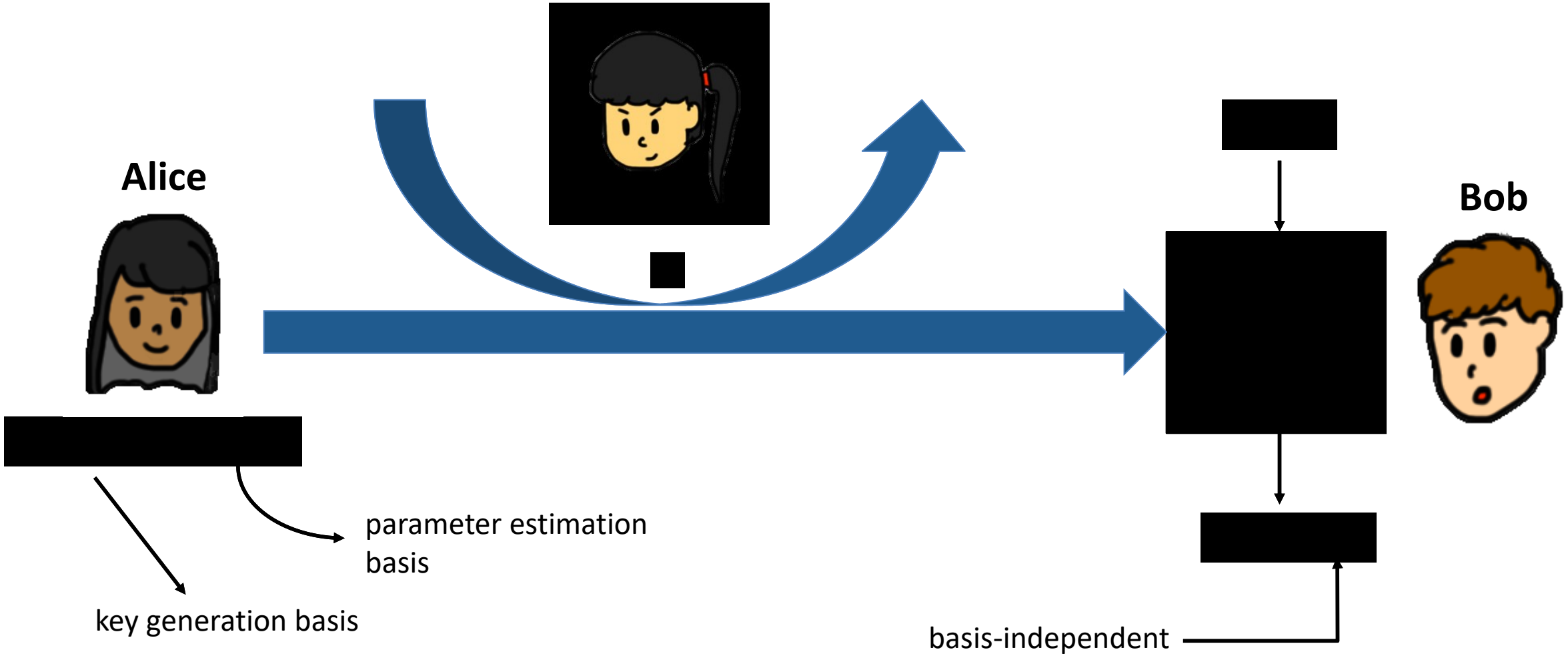
Use a hierarchy of semidefinite relaxations with increasing number of constraints to obtain an outer approximation of the quantum set


define inner-product constraints
define probabilities constraints

Application: security analysis of quantum key distribution

Phase-encoding BB84

Huttner, Imoto, Gisin & Mor, *PRA* (1995)



Apply the unitary transformation on the signal states

[redacted]

[redacted]

Use Devetak-Winter bound and entropic uncertainty relation

[redacted]

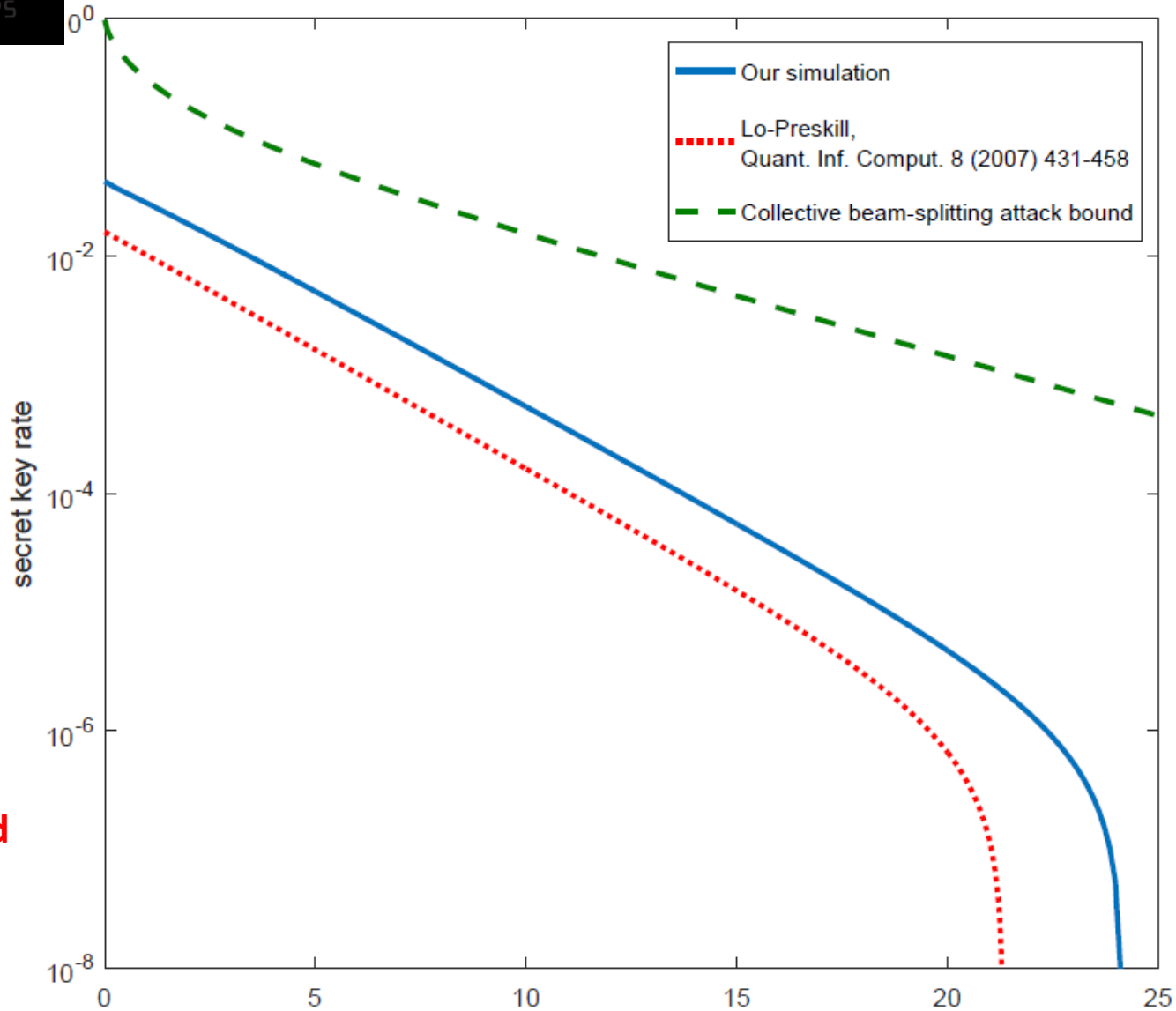
Devetak-Winter, *Proc. R. Soc. Lond. A* (2005)
Berta et al, *Nat. Phys.* (2010)

Maximise the phase error rate subject to the observed probabilities

[redacted]

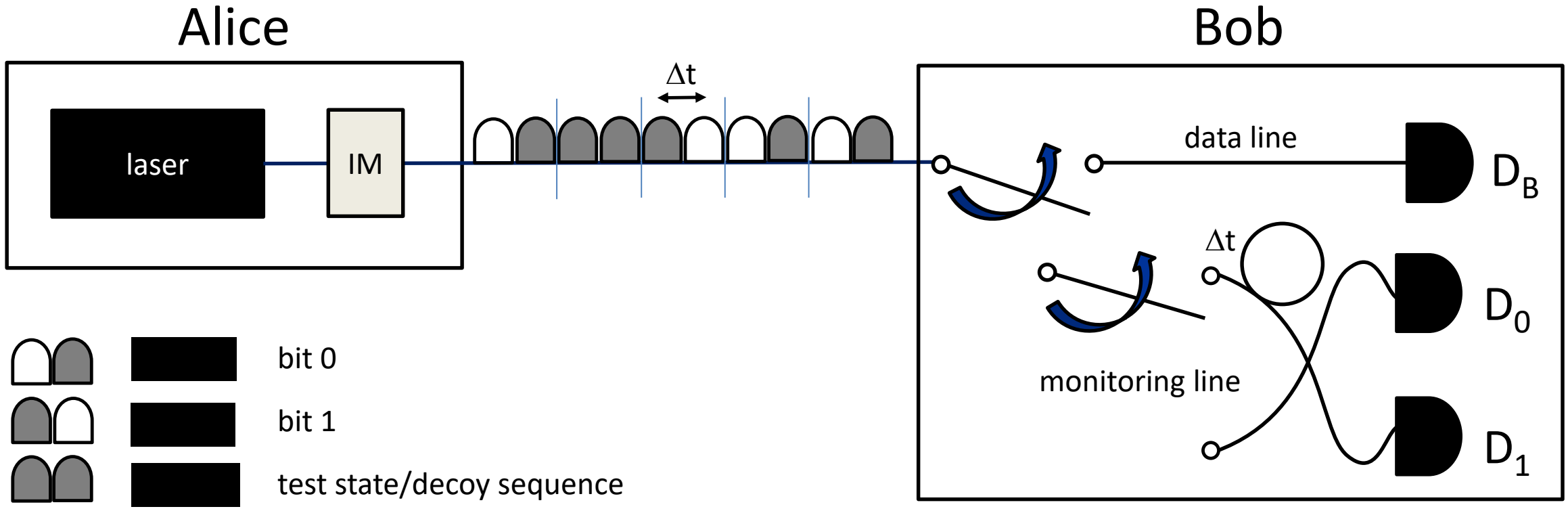
Parameters:

Intrinsic optical error rate = 2%
Dark count rate = 1E-7



Results using Lo-Preskill's bound
Lucamarini et al, *PRX* (2015)
Sibson et al, *Optica* (2017)

Time-bin encoding three-state protocol



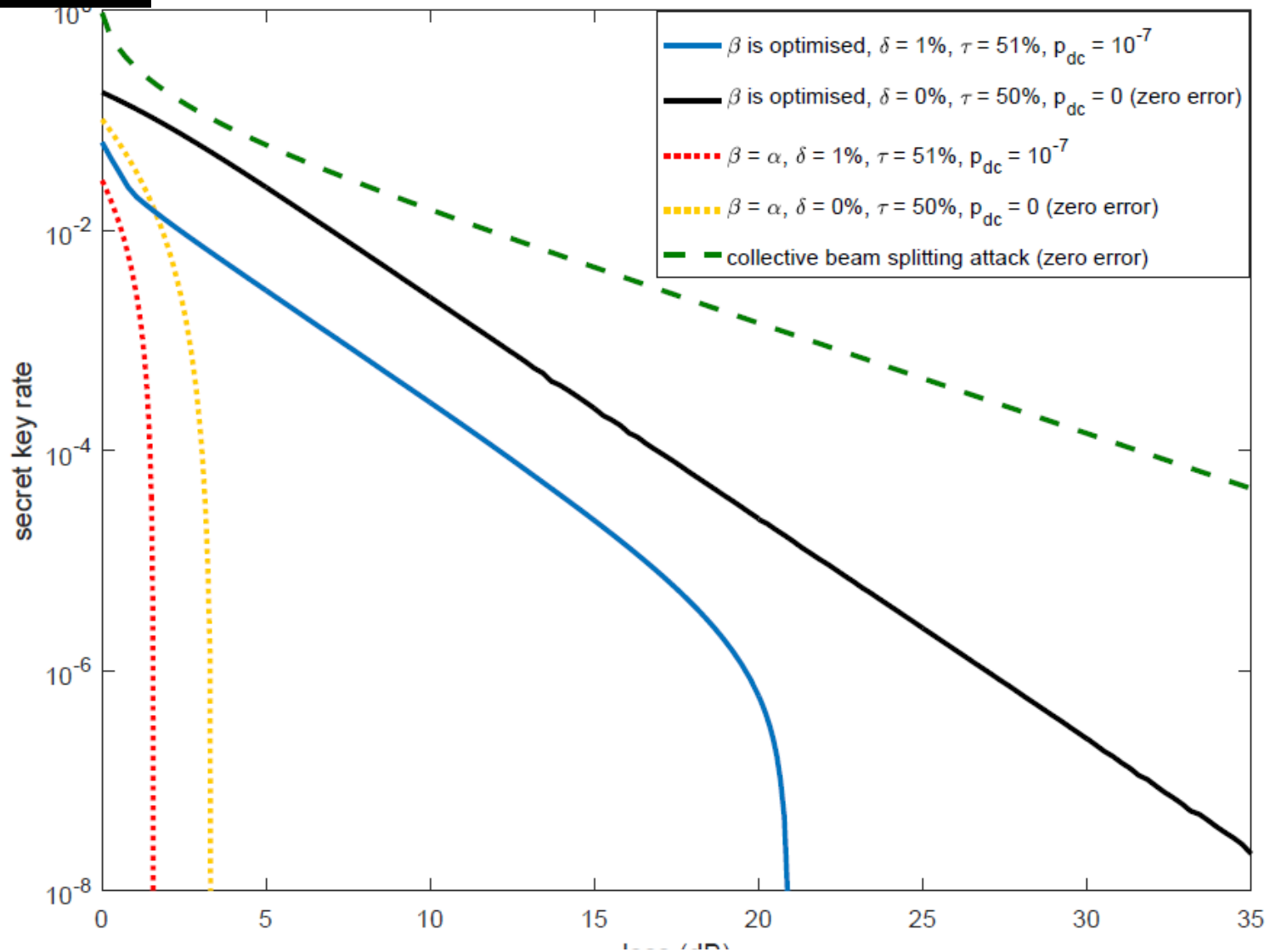
Coherent-one-way protocols

Stucki, Brunner, Gisin, Scarani & Zbinden, *Appl. Phys. Letter* (2005)

Moroder, Marcos, Lim, Thinh, Zbinden & Gisin, *PRL* (2012)

Parameters:

Extinction ratio = δ
Dark count rate = p_{dc}
Beam-splitter transmittivity = τ



Summary

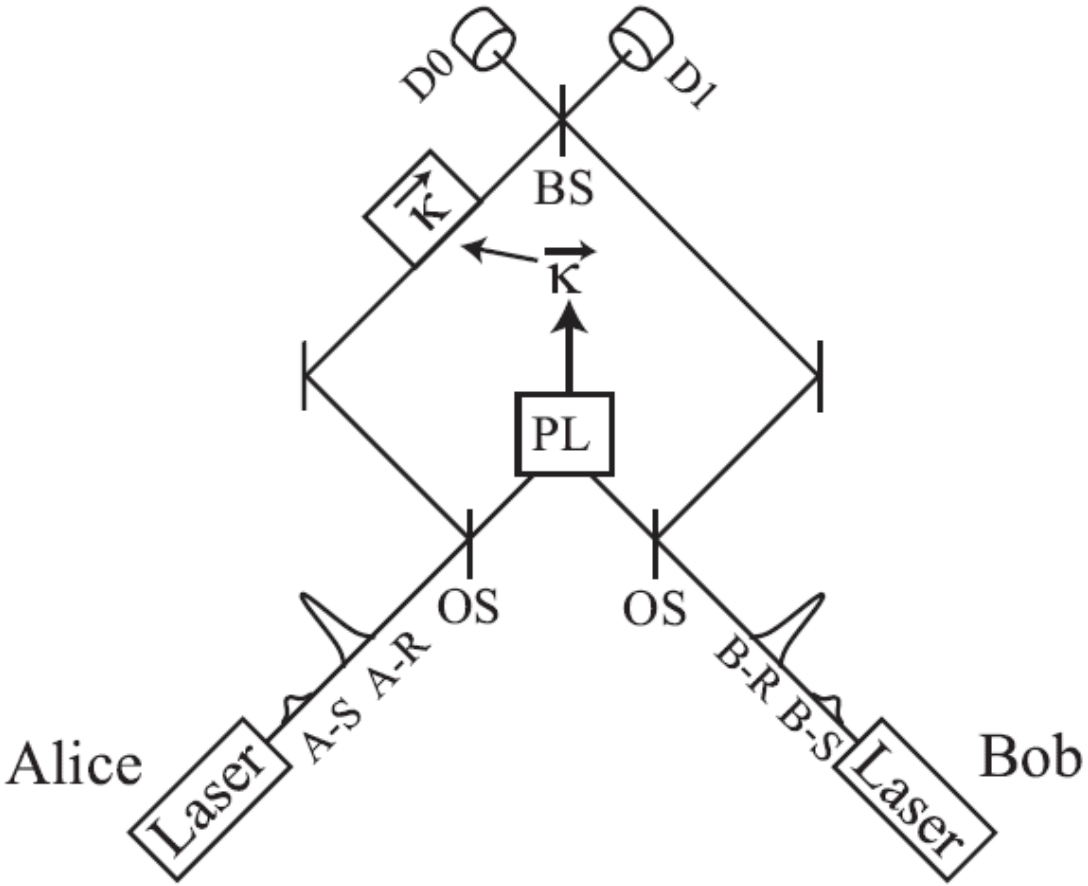
- We propose an efficient SDP-based numerical toolbox to characterise quantum correlations in a broadcast network
  - ✓ Independent of the dimension of system (thus, also works for coherent state encodings)
  - ✓ Minimal assumptions about the measurement devices
  - ✓ Applicable to any discrete prepare-and-measure protocols (not only in QKD)
- We apply our method to analyse the security of quantum key distribution
  - ✓ Higher secret key rate compared to previous results
  - ✓ Highly versatile, can be used to analyse non-standard QKD protocol

On-going work and open problems

- Analyse the security of distributed-phase-reference QKD protocols and discrete-modulated QKD protocols with homodyne/heterodyne detection

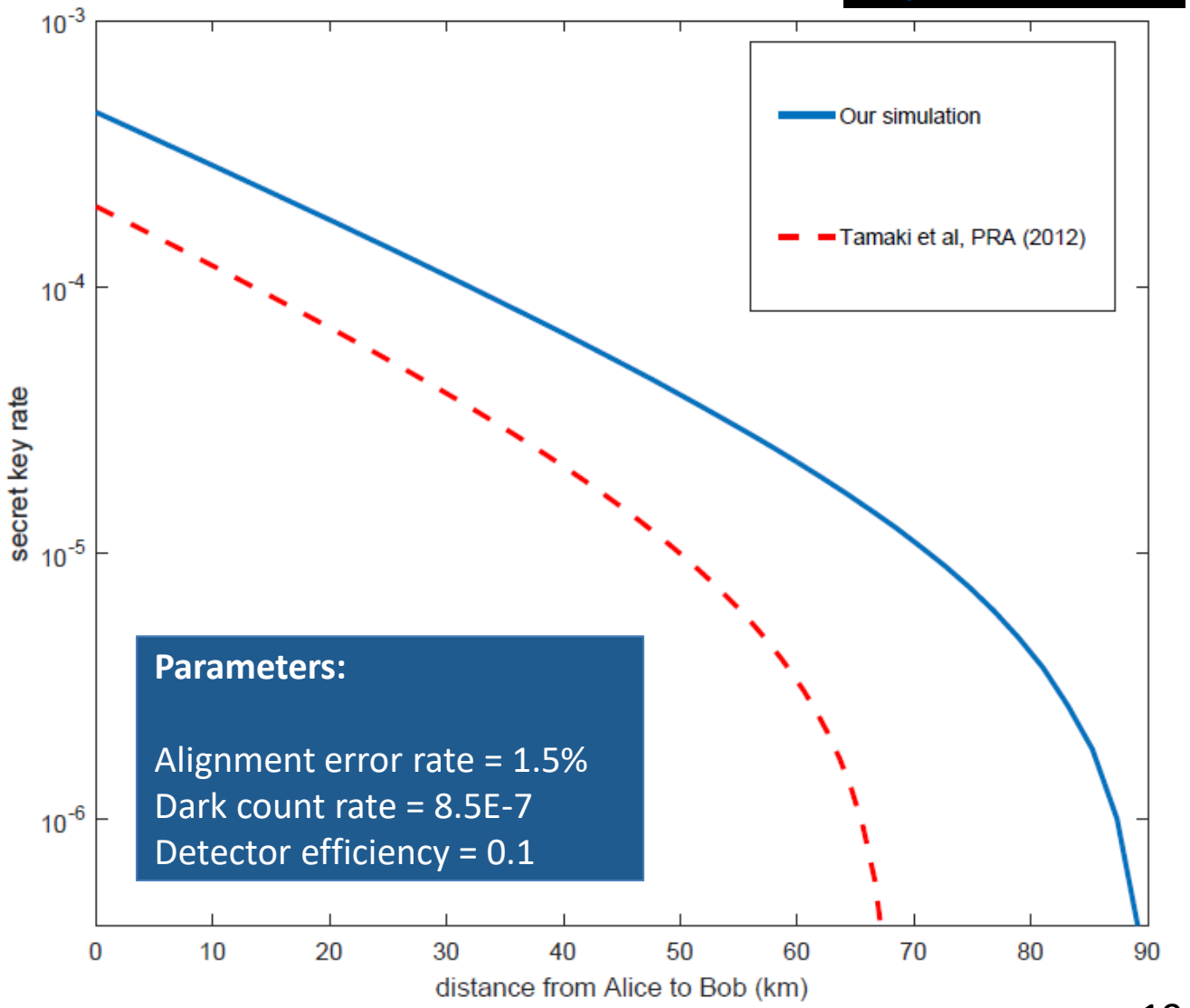
- Consider different constraints (e.g. energy constraint) other than the inner-product constraints

- Extend to measurement-device-independent (MDI) setups



Phase-encoding MDIQKD

Tamaki et al, *PRA* (2012)



Full paper can be found here