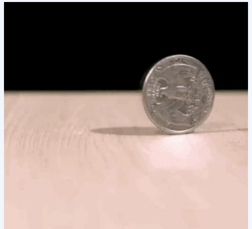
QCRYPT 2023

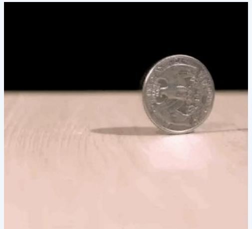
Experimental cheat-sensitive quantum weak coin flipping



Simon NEVES

LIP6 - QI team, Sorbonne Université

18th of August 2023



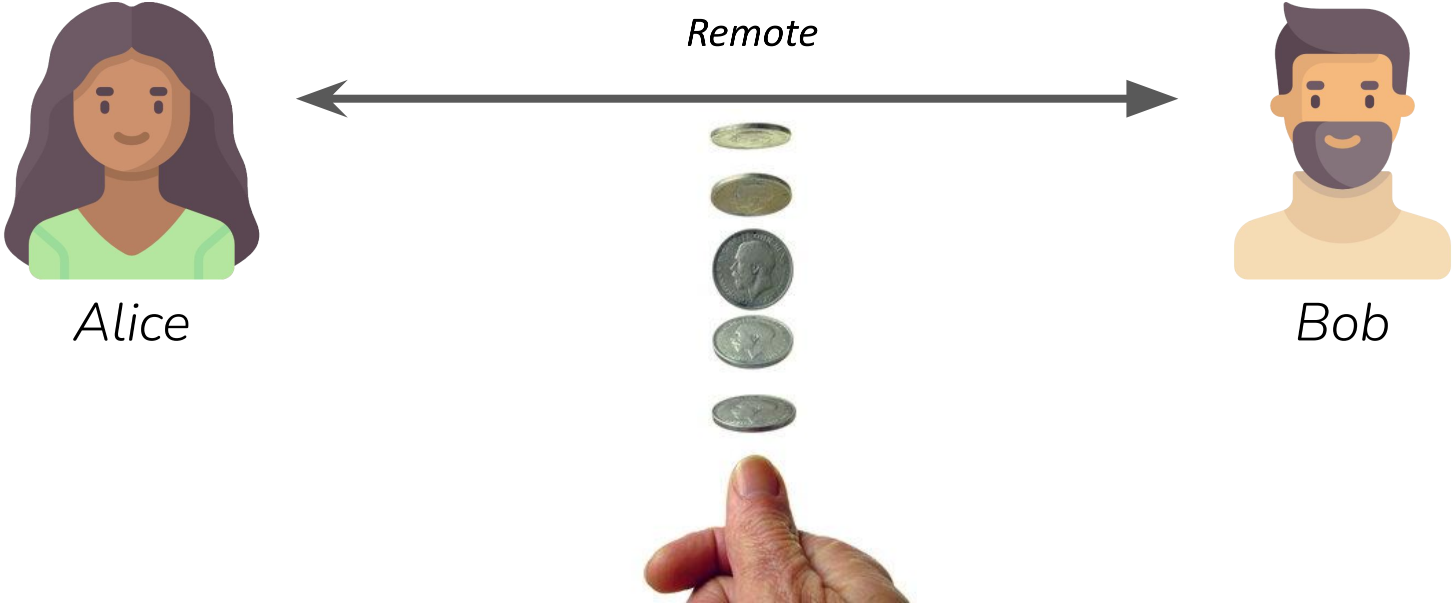
SORBONNE UNIVERSITÉ

ANR AGENCE NATIONALE DE LA RECHERCHE

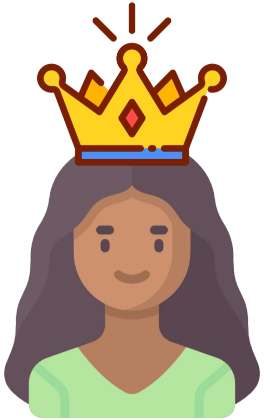
erc

cnrs

The Game



The Game

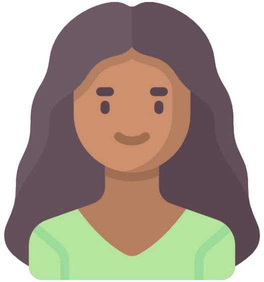


Alice

Head!

Bob

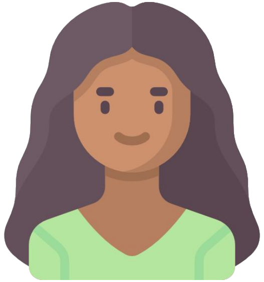
The Game



Alice

Bob

The Game

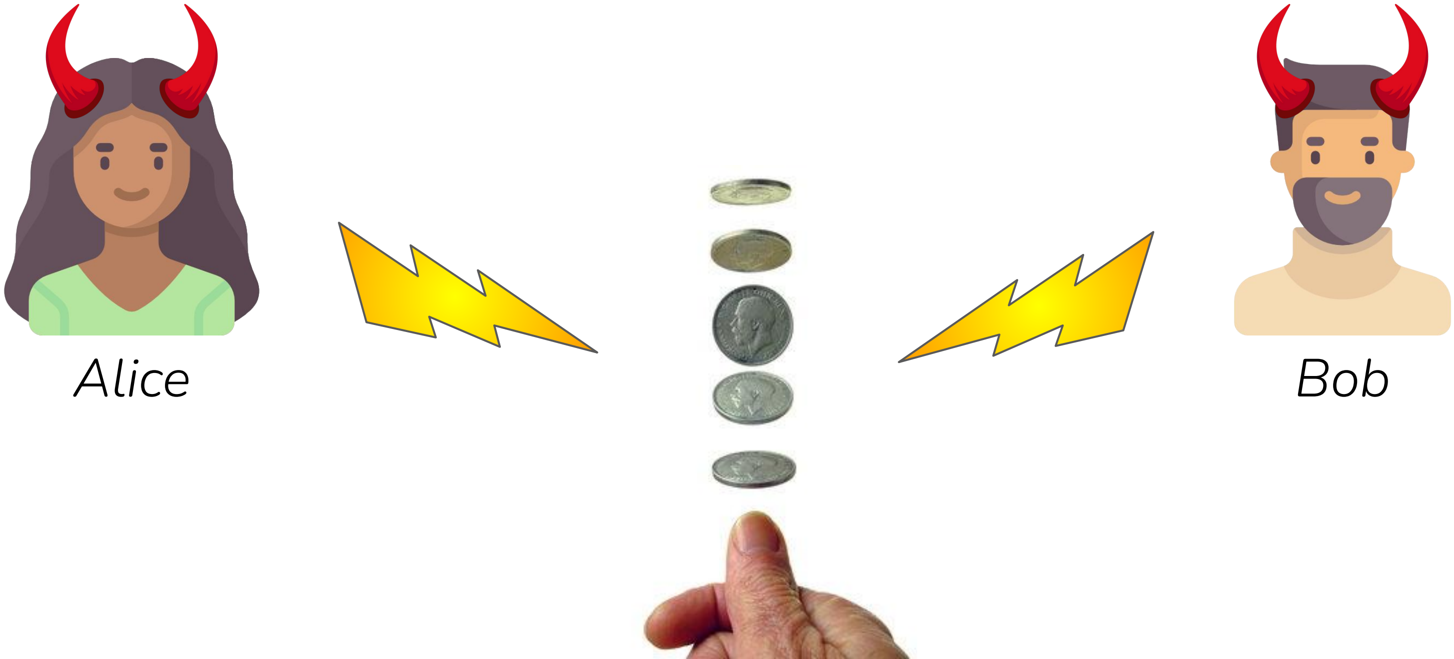


Alice

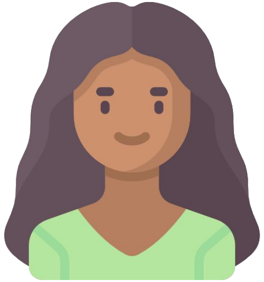
Tail!

Bob

The Game



The Game



Alice

Head

Bob

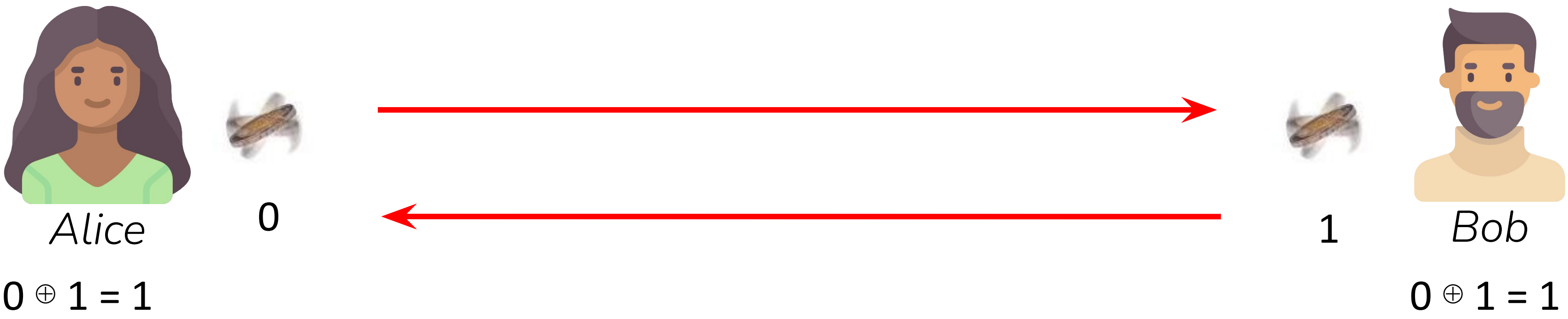
Tail

Preferred outcome

Important Cryptographic Primitive

- Multiparty computation

Classical Solutions



Quantum Protocol

PHYSICAL REVIEW A **102**, 022414 (2020)

Quantum weak coin flipping with a single photon

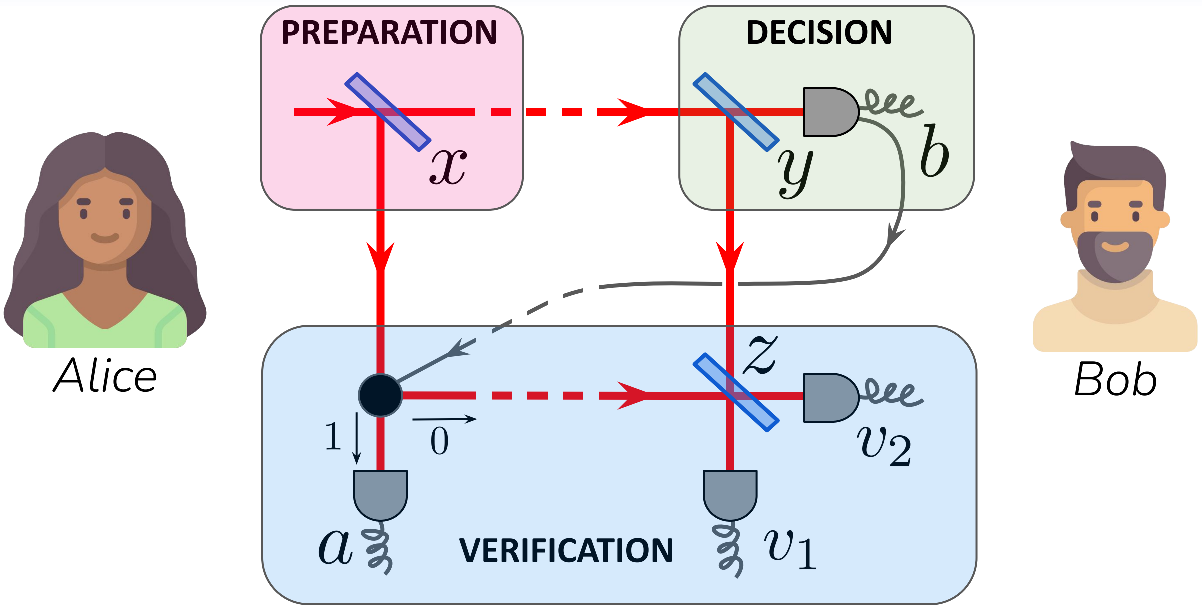
Mathieu Bozzio,[1,2] Ulysse Chabaud,[1] Iordanis Kerenidis,[3] and Eleni Diamanti[1]
[1]*Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, F-75005 Paris, France*
[2]*Institut Polytechnique de Paris, Télécom Paris, LTCI, 19 Place Marguerite Perey, 91129 Palaiseau, France*
[3]*Université de Paris, CNRS, IRIF, 8 Place Aurélie Nemours, 75013 Paris, France*

(Received 20 February 2020; accepted 30 July 2020; published 19 August 2020)

Weak coin flipping is among the fundamental cryptographic primitives which ensure the security of modern communication networks. It allows two mistrustful parties to remotely agree on a random bit when they favor opposite outcomes. Unlike other two-party computations, one can achieve information-theoretic security using quantum mechanics only: both parties are prevented from biasing the flip with probability higher than $1/2+\epsilon$, where ϵ is arbitrarily low. Classically, the dishonest party can always cheat with probability 1 unless computational assumptions are used. Despite its importance, no physical implementation has been proposed for quantum weak coin flipping. Here, we present a practical protocol that requires a single photon and linear optics only. We show that it is fair and balanced even when threshold single-photon detectors are used, and reaches a bias as low as $\epsilon = 1/\sqrt{2} - 1/2 \approx 0.207$. We further show that the protocol may display a quantum advantage over a few-hundred meters with state-of-the-art technology.

DOI: 10.1103/PhysRevA.102.022414

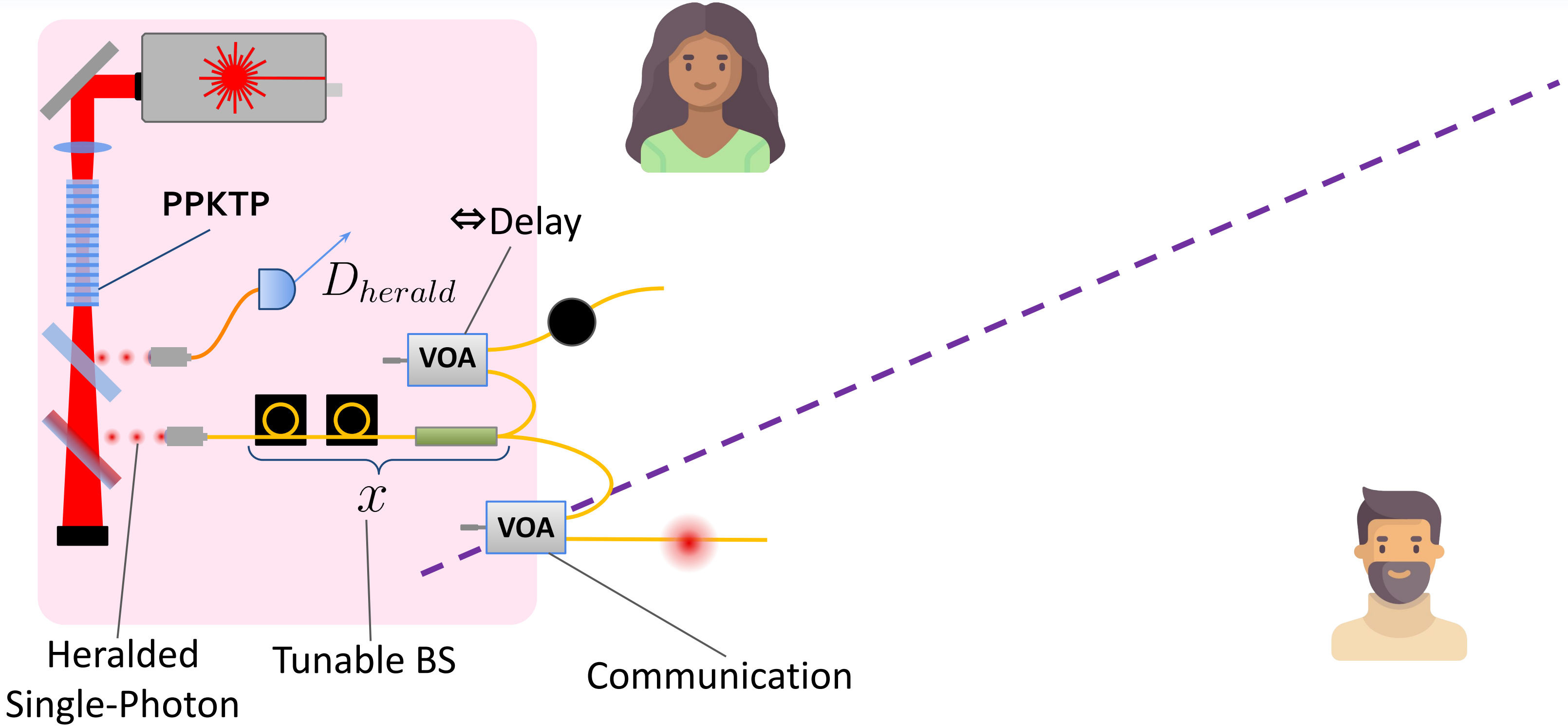
Quantum Protocol



Cheat-Sensitivity = Quantum advantage!

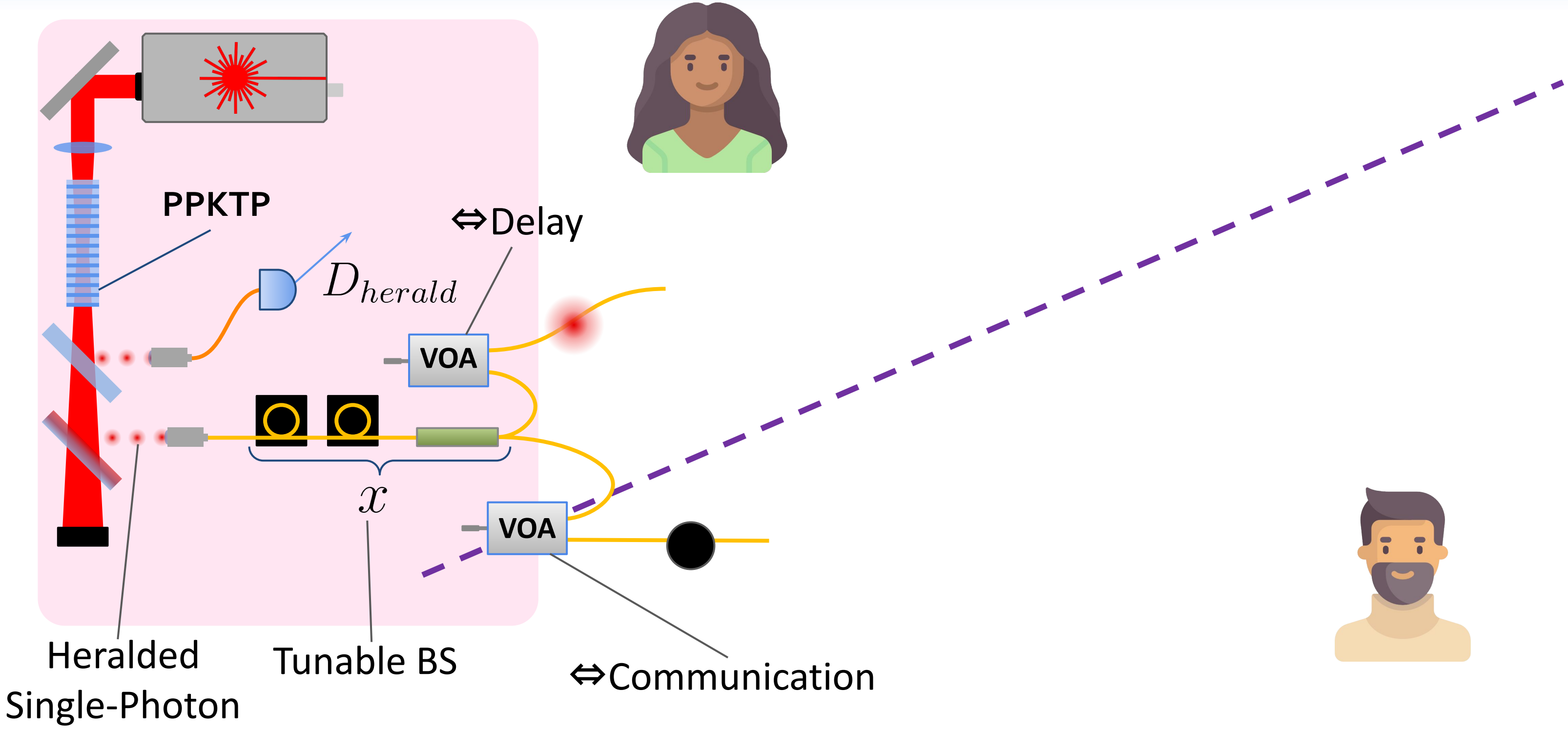
Quantum Protocol

Experimental Implementation



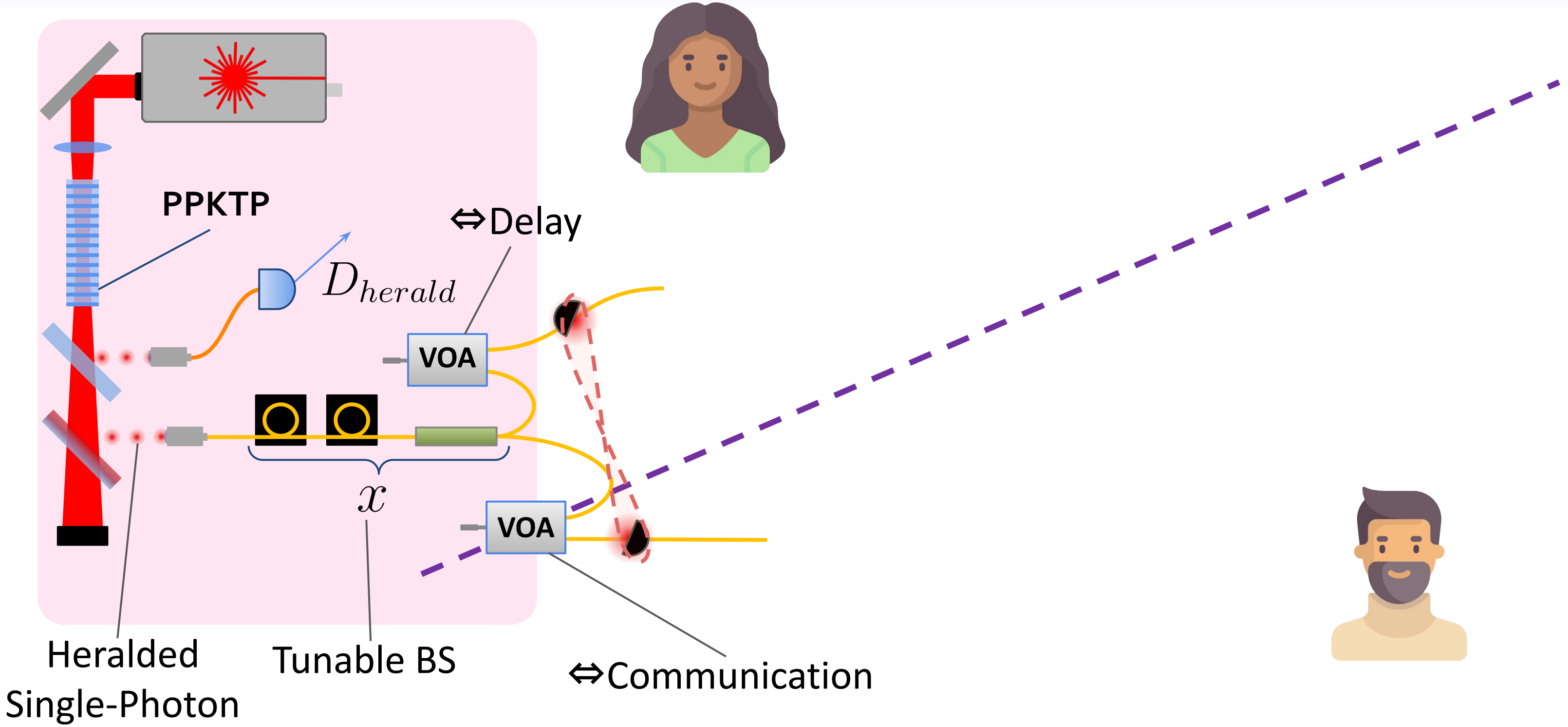
Quantum Protocol

Experimental Implementation



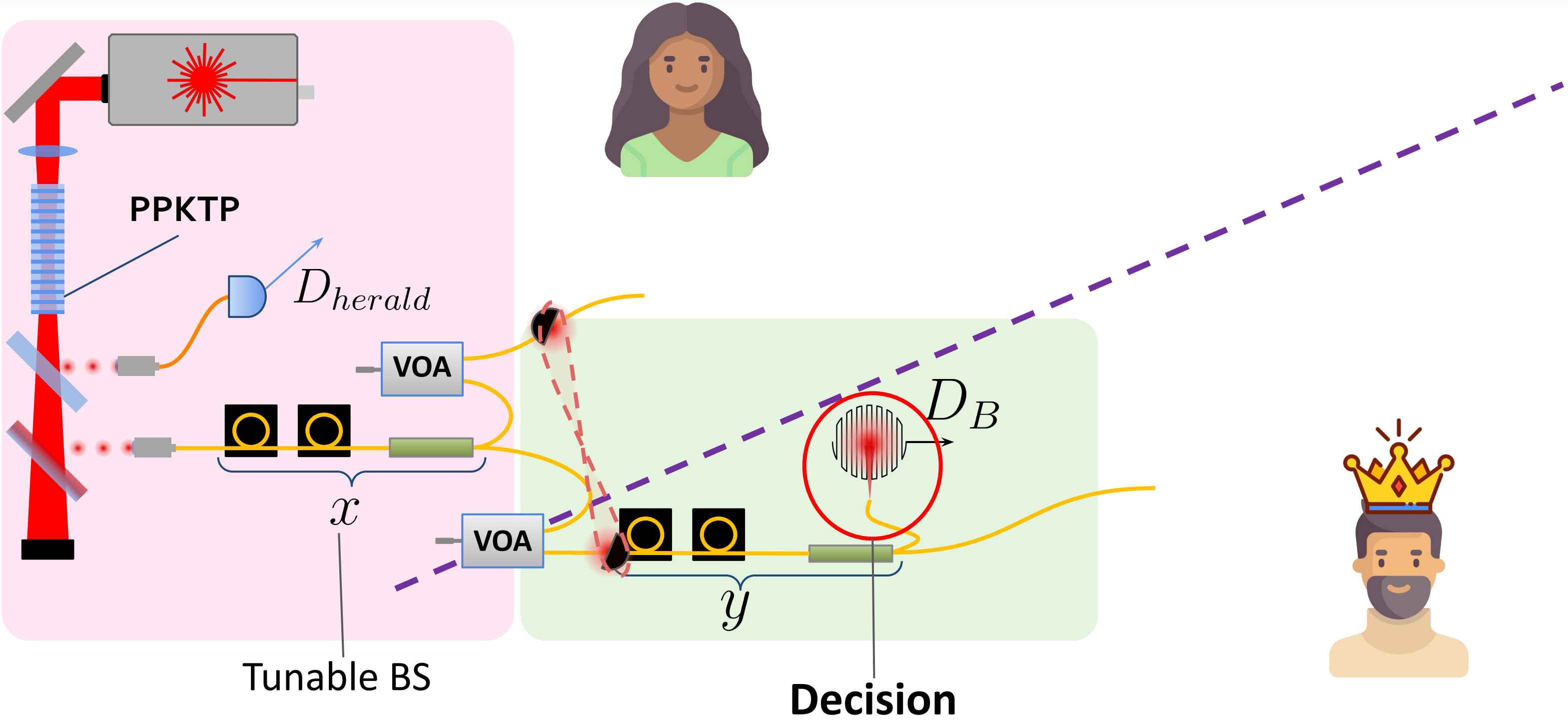
Quantum Protocol

Experimental Implementation



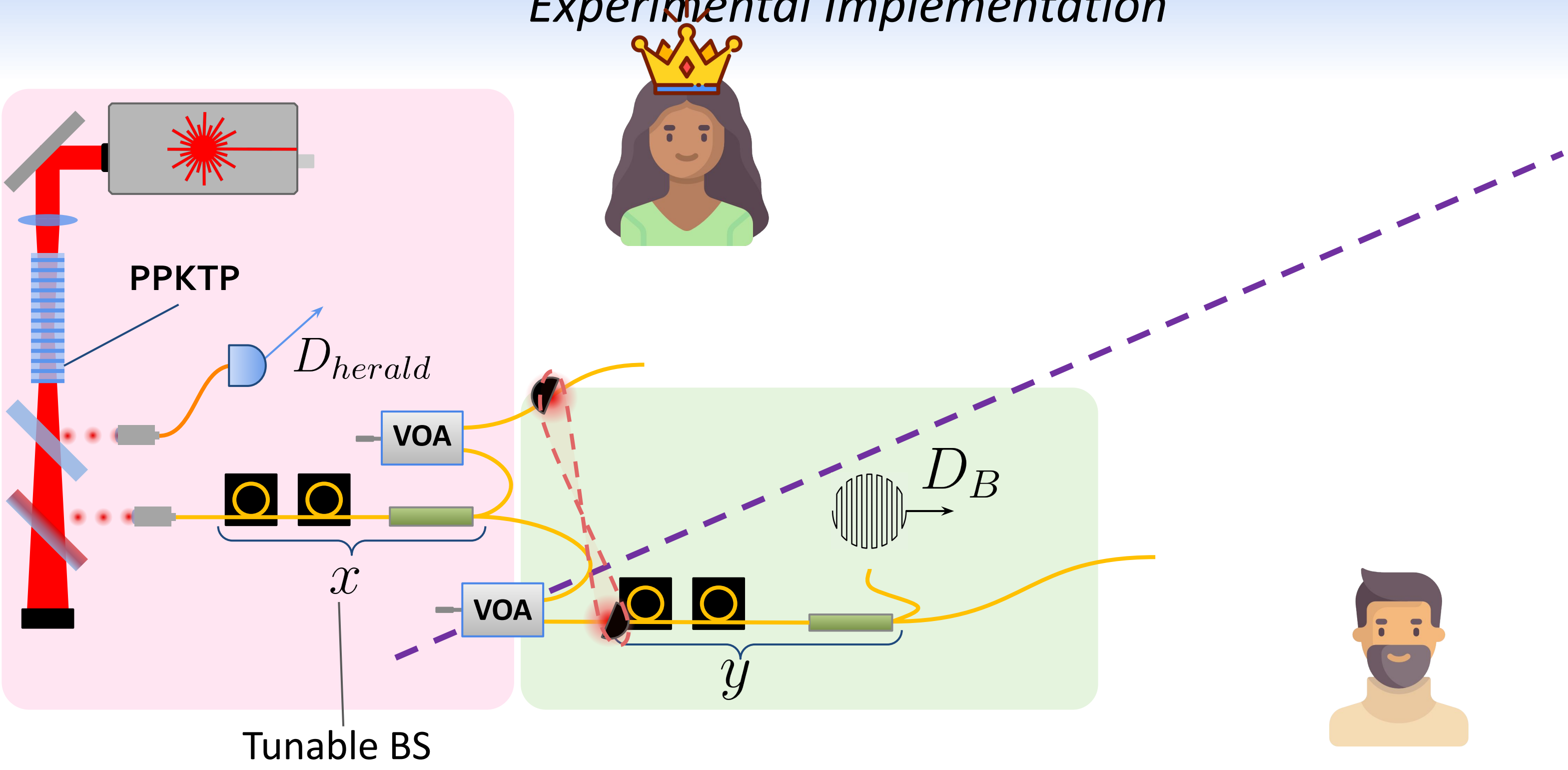
Quantum Protocol

Experimental Implementation



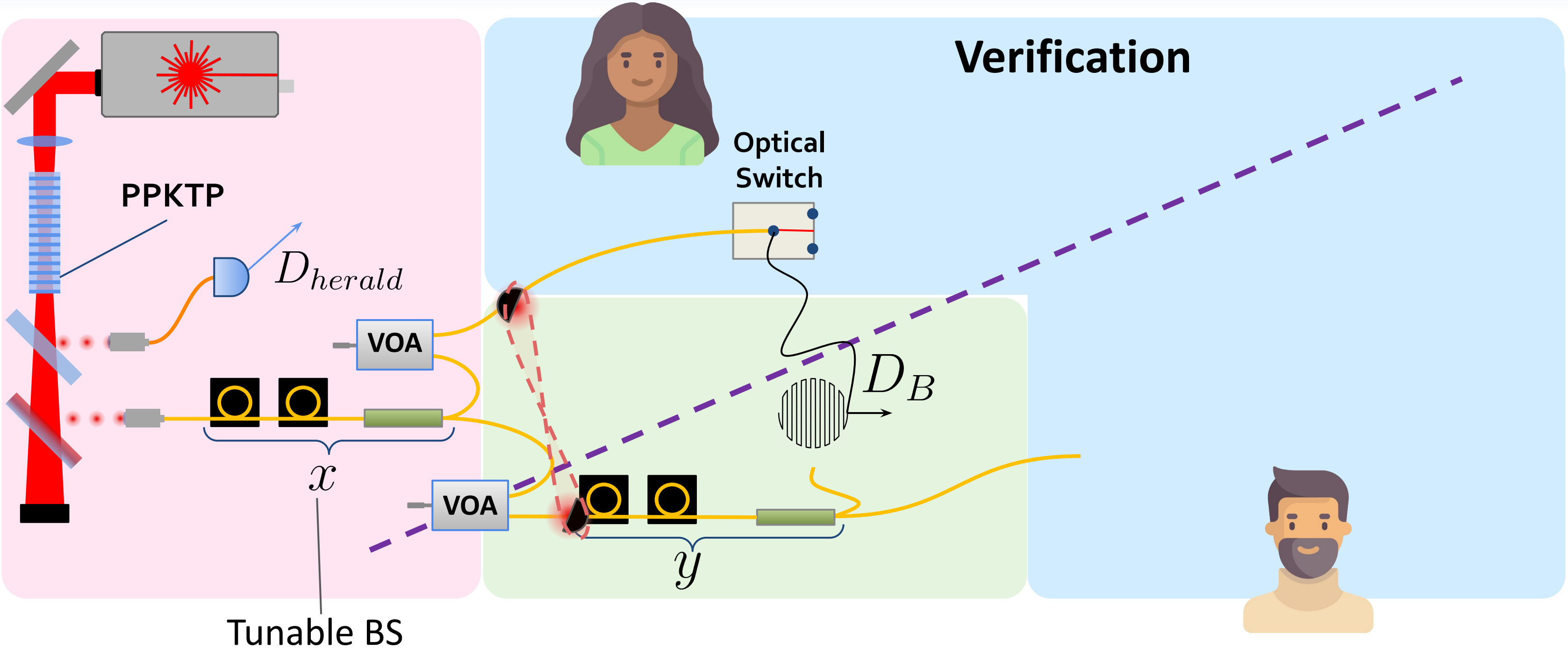
Quantum Protocol

Experimental Implementation



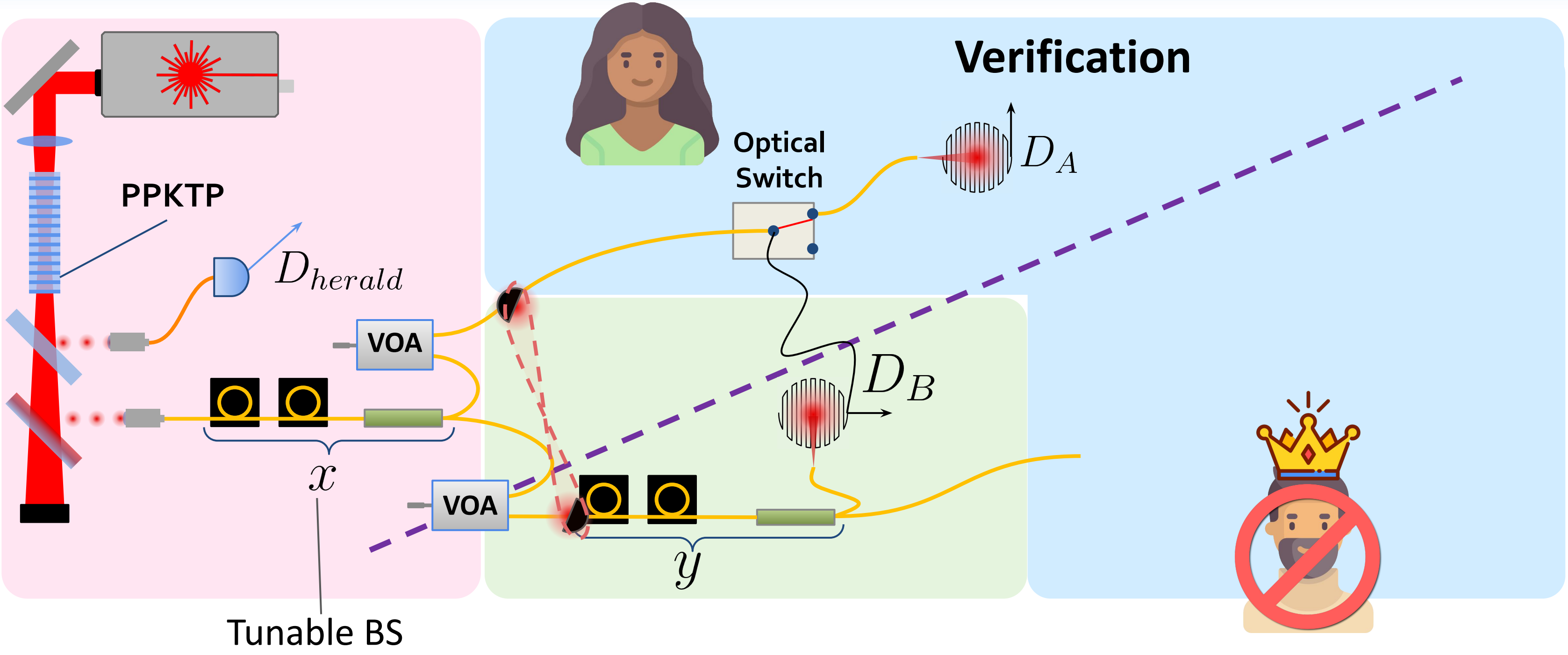
Quantum Protocol

Experimental Implementation



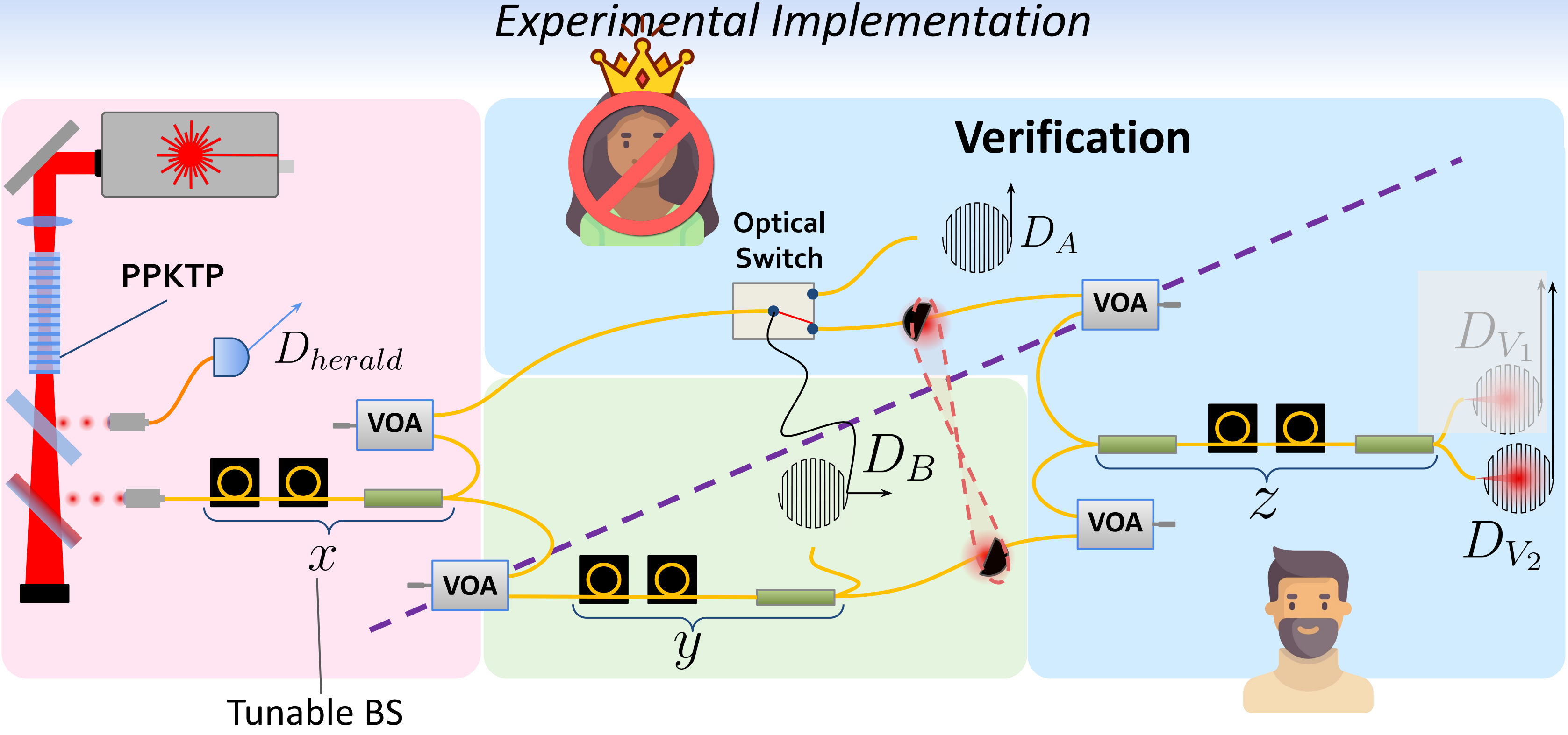
Quantum Protocol

Experimental Implementation



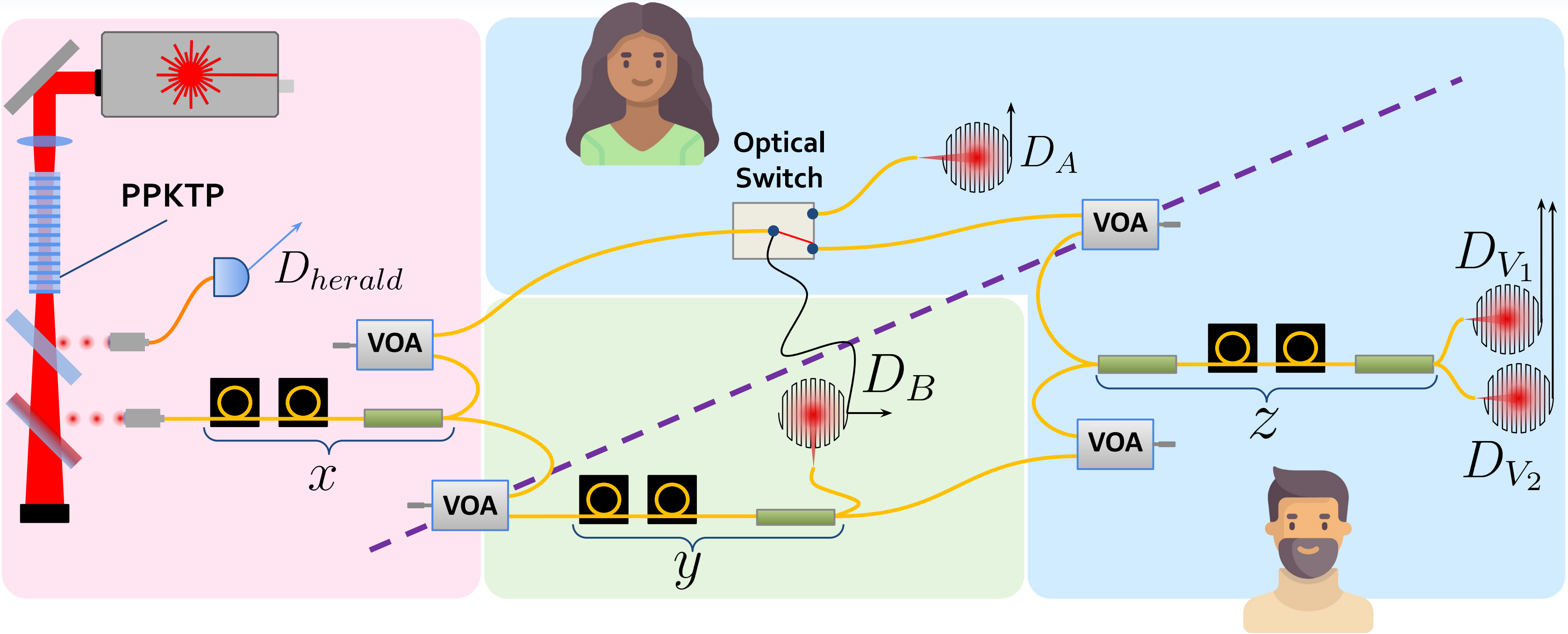
Quantum Protocol

Experimental Implementation



Quantum Protocol

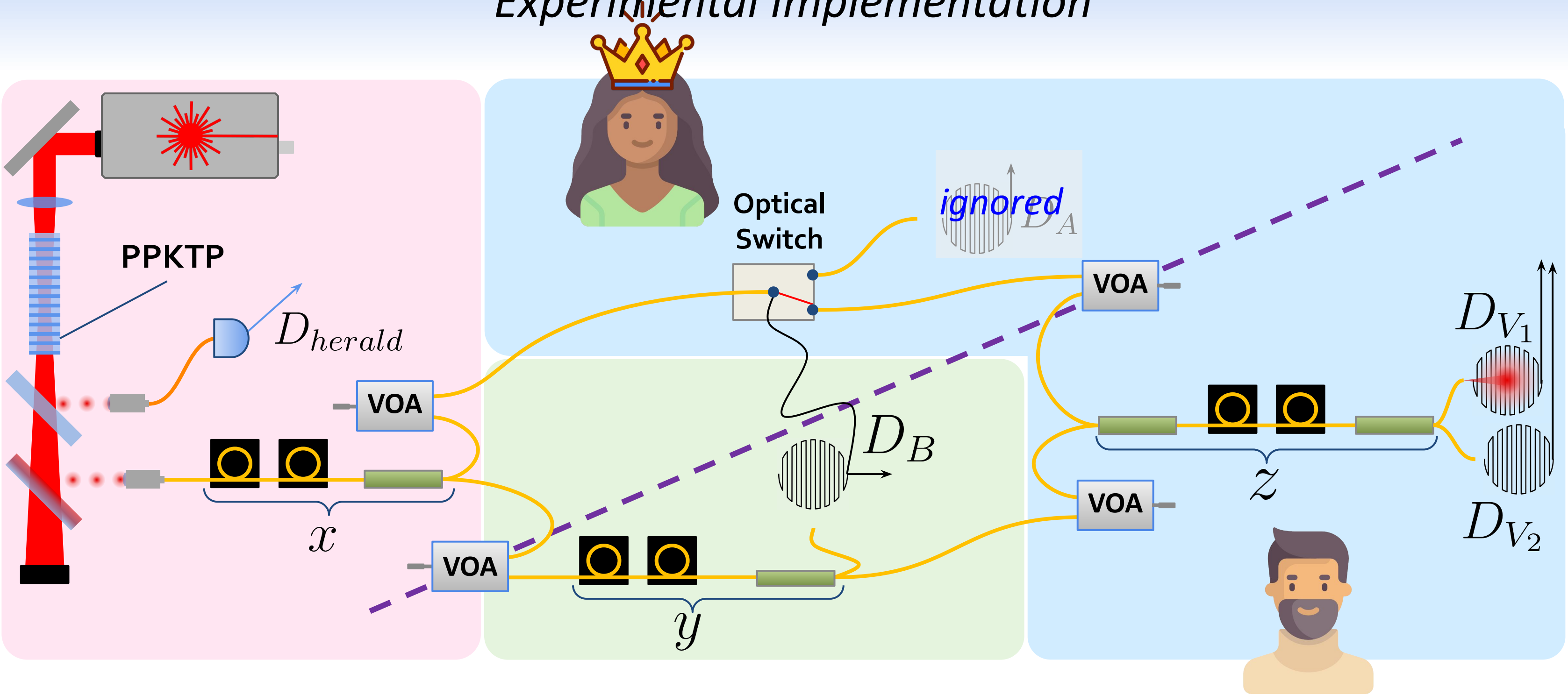
Experimental Implementation



5 Outcomes

Quantum Protocol

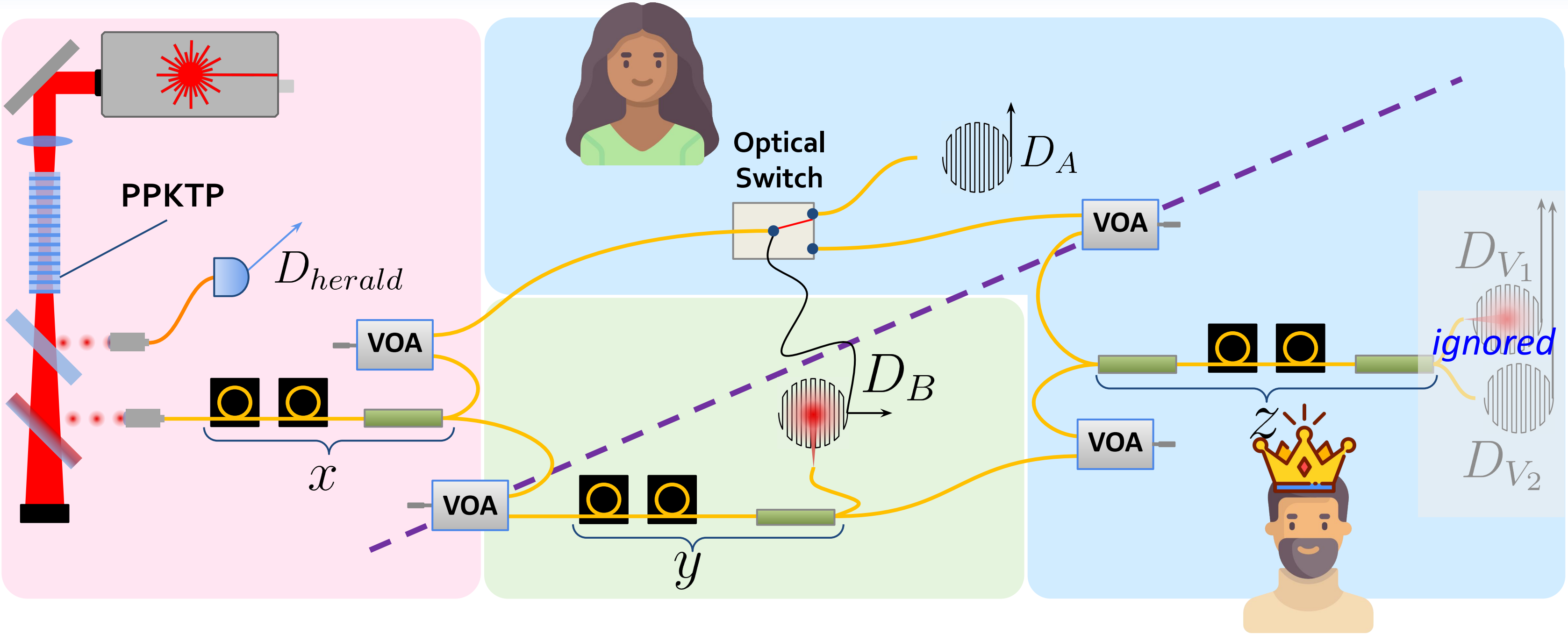
Experimental Implementation



Alice Wins

Quantum Protocol

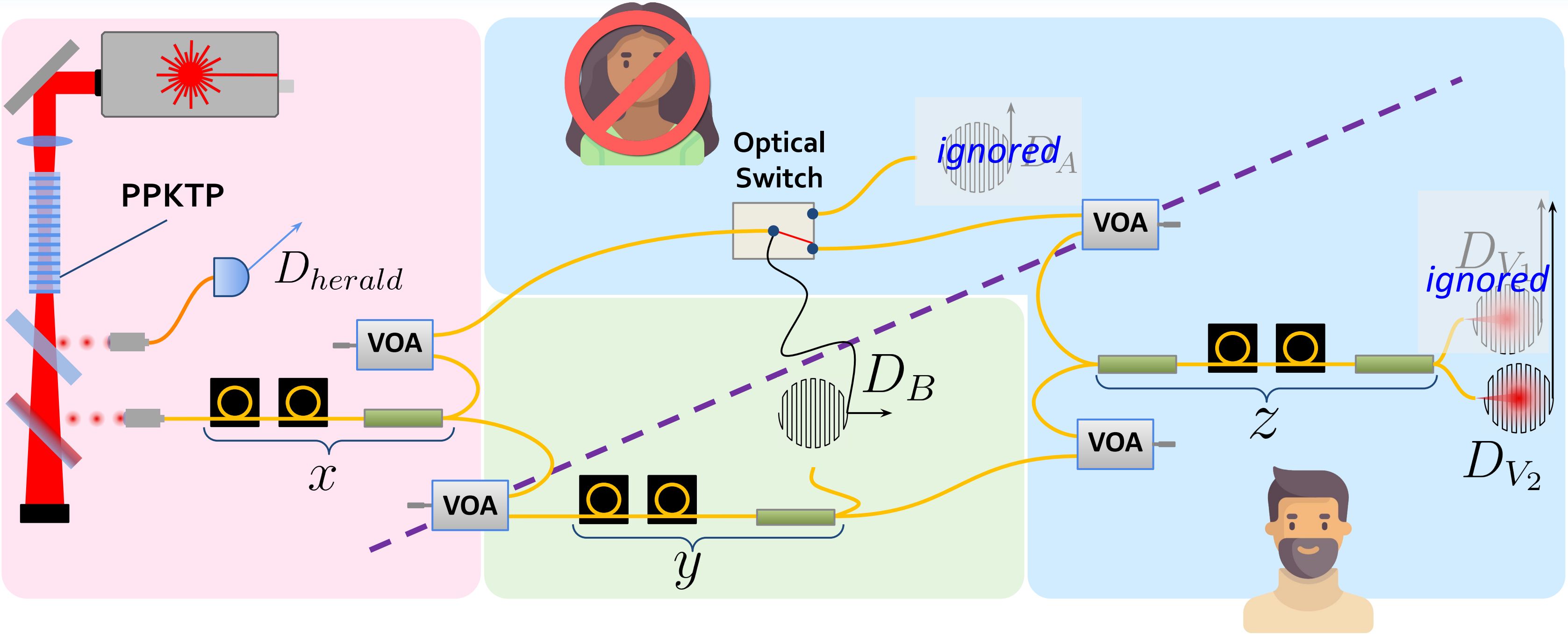
Experimental Implementation



Bob Wins

Quantum Protocol

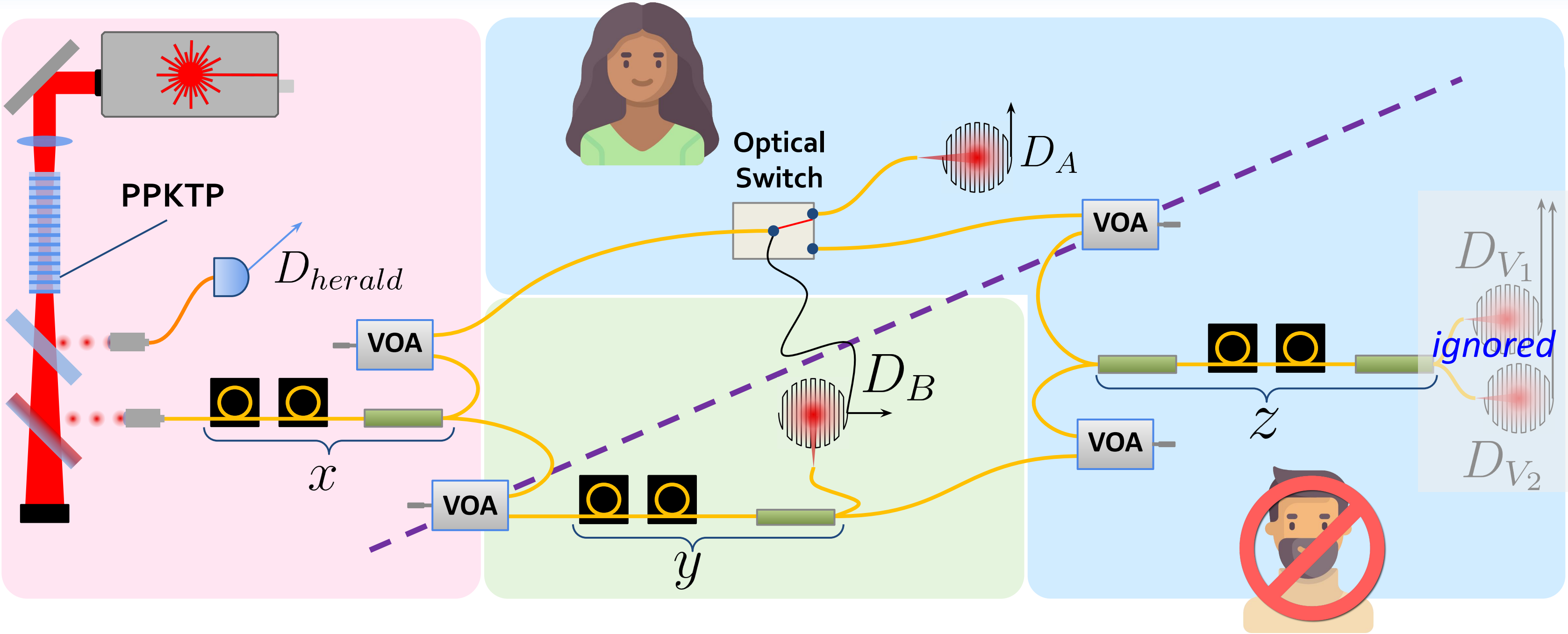
Experimental Implementation



Alice is Sanctioned

Quantum Protocol

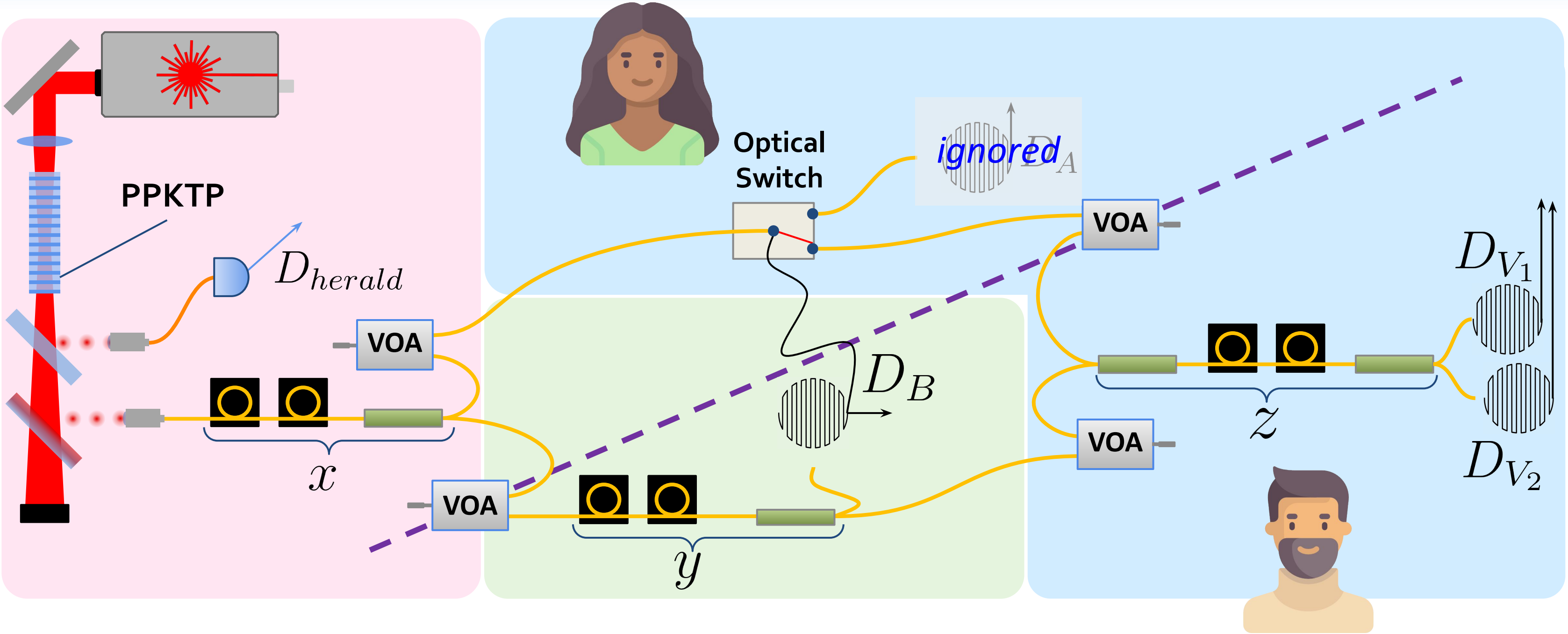
Experimental Implementation



Bob is Sanctioned

Quantum Protocol

Experimental Implementation



Abort

Quantum Protocol

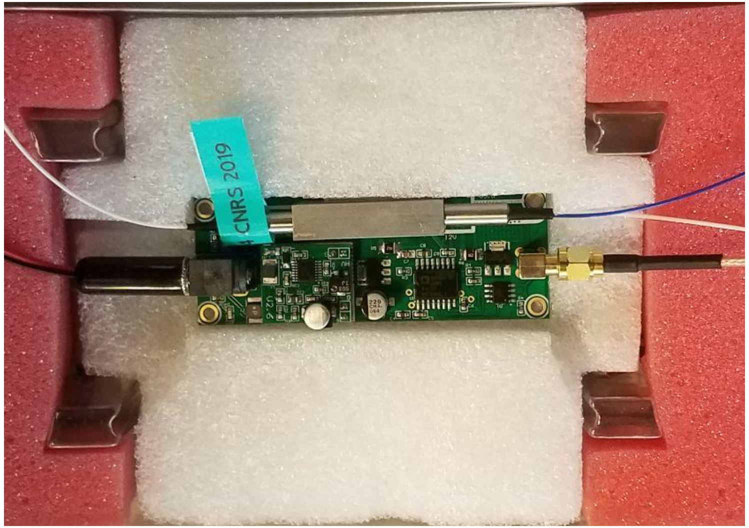
Requirements

When players are **honest**:

- Minimize P(Abort)

Experimental Implementation

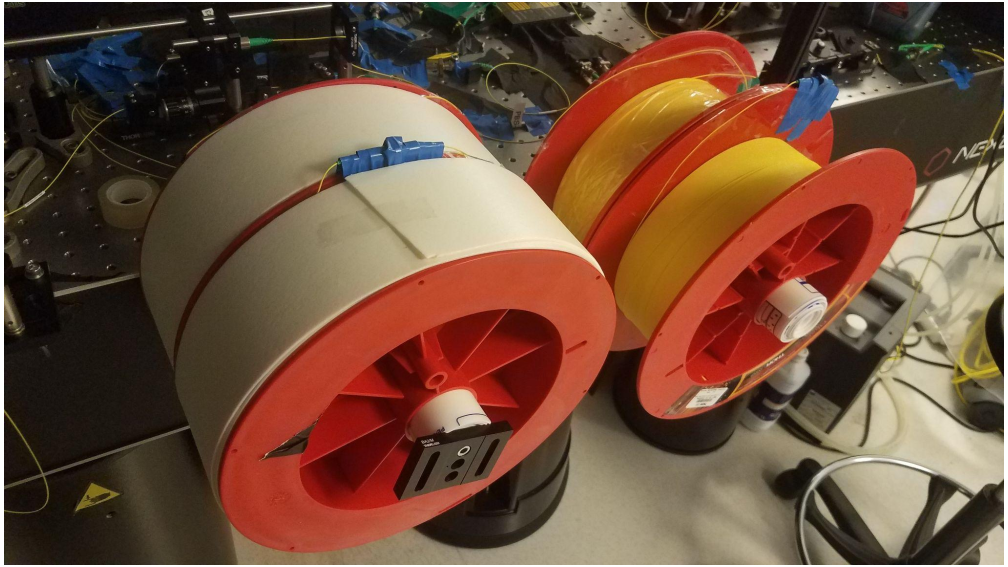
Switch & Delay



400ns reaction time

Experimental Implementation

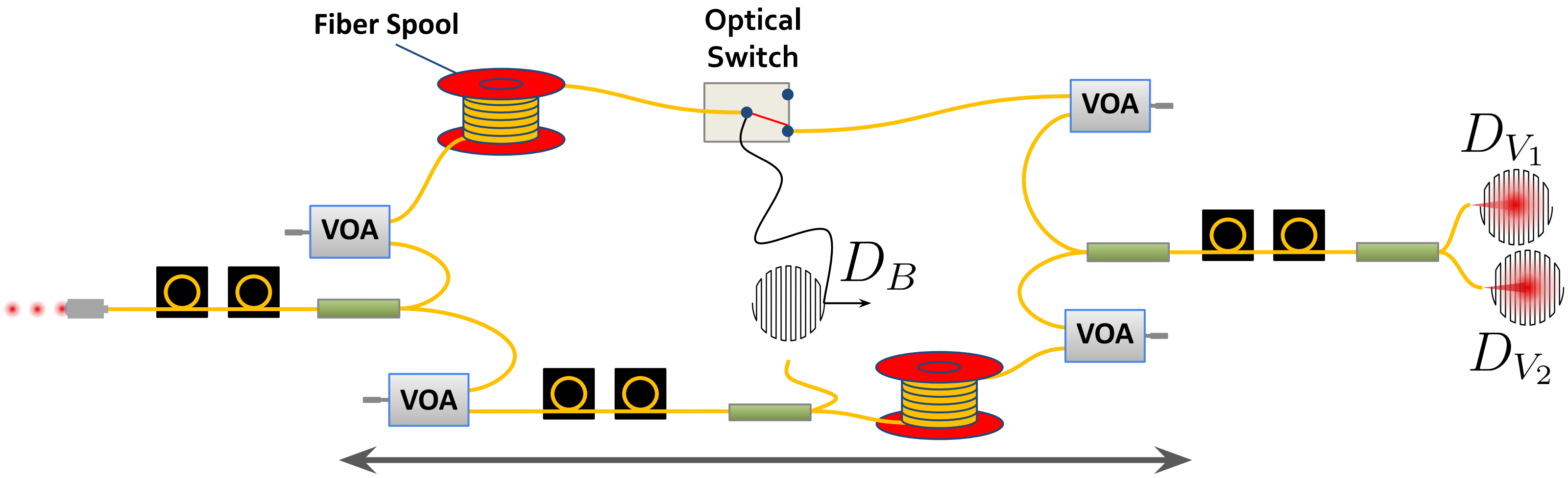
Switch & Delay



2x 300m fiber spools

Experimental Implementation

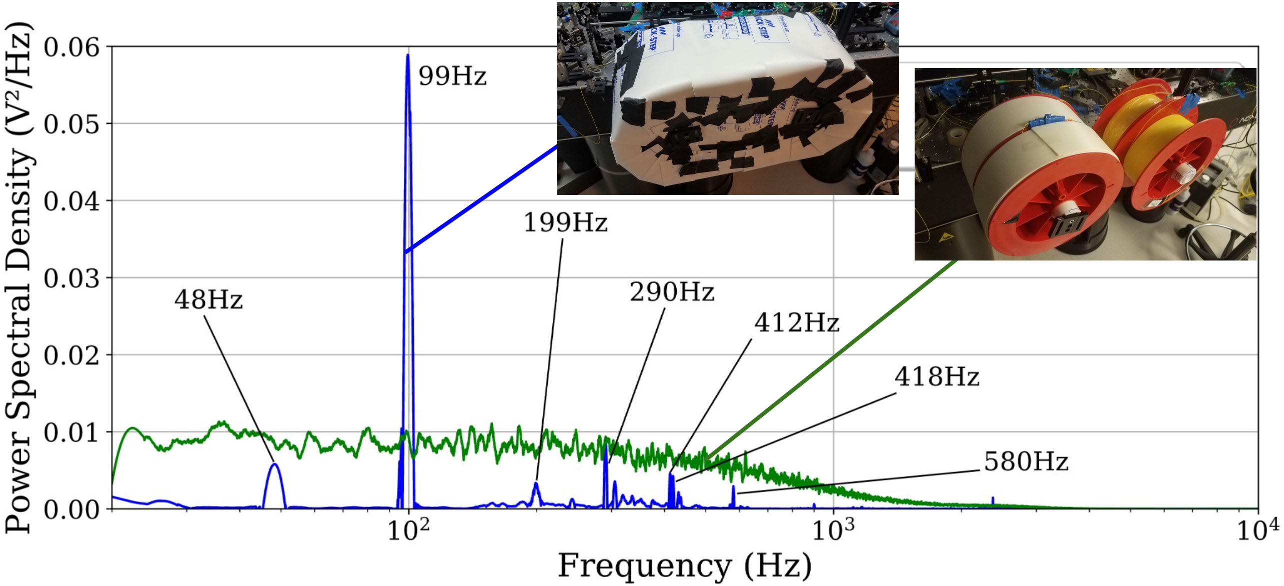
Switch & Delay



> 300m fibered interferometer

Experimental Implementation

Noise Recording - Spools Insulation

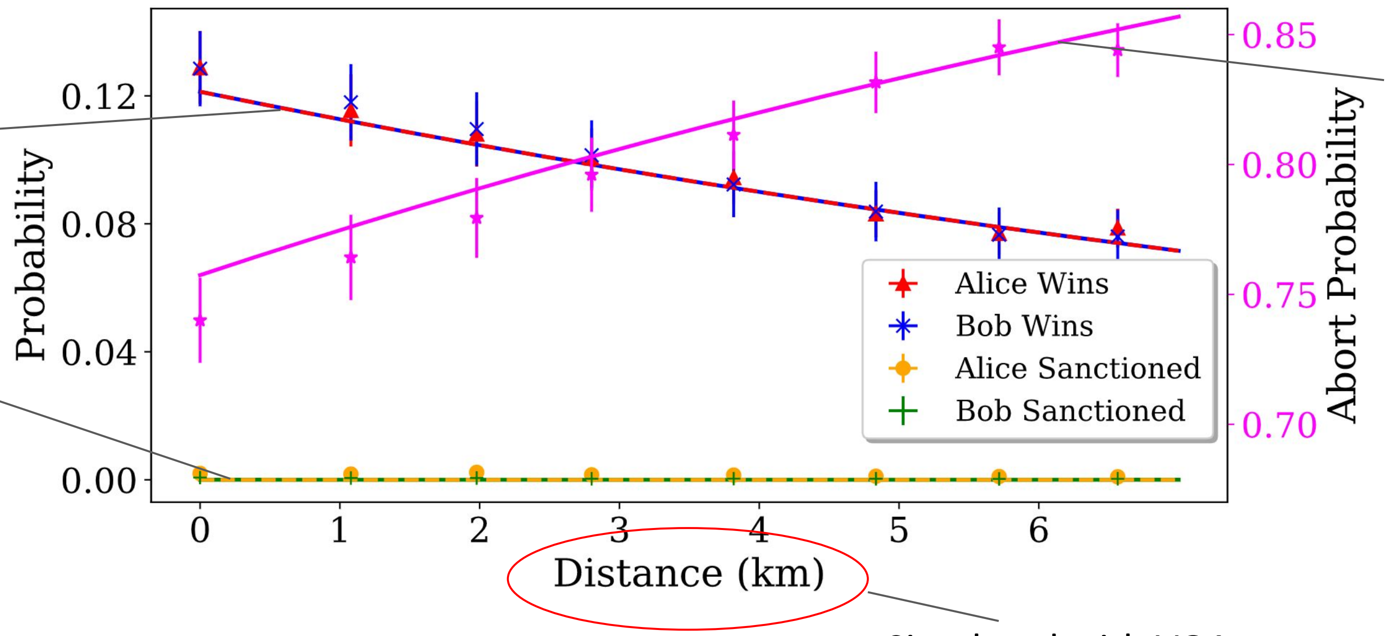


Results with Honest Players

Outcomes Probabilities VS Communication Distance

Fair protocol

Correct protocol



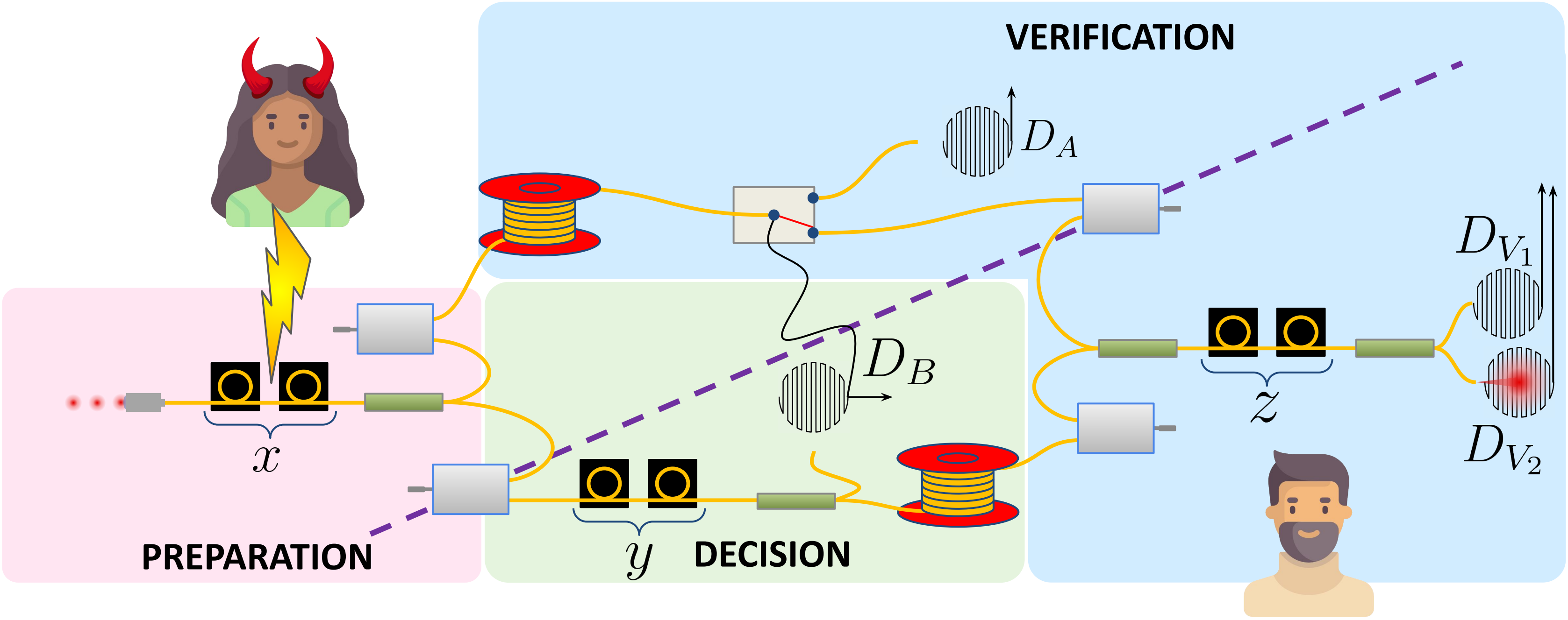
High abort… but goes to 0 if less losses

Simulated with VOAs

Cheat-Sensitivity

Quantum advantage!

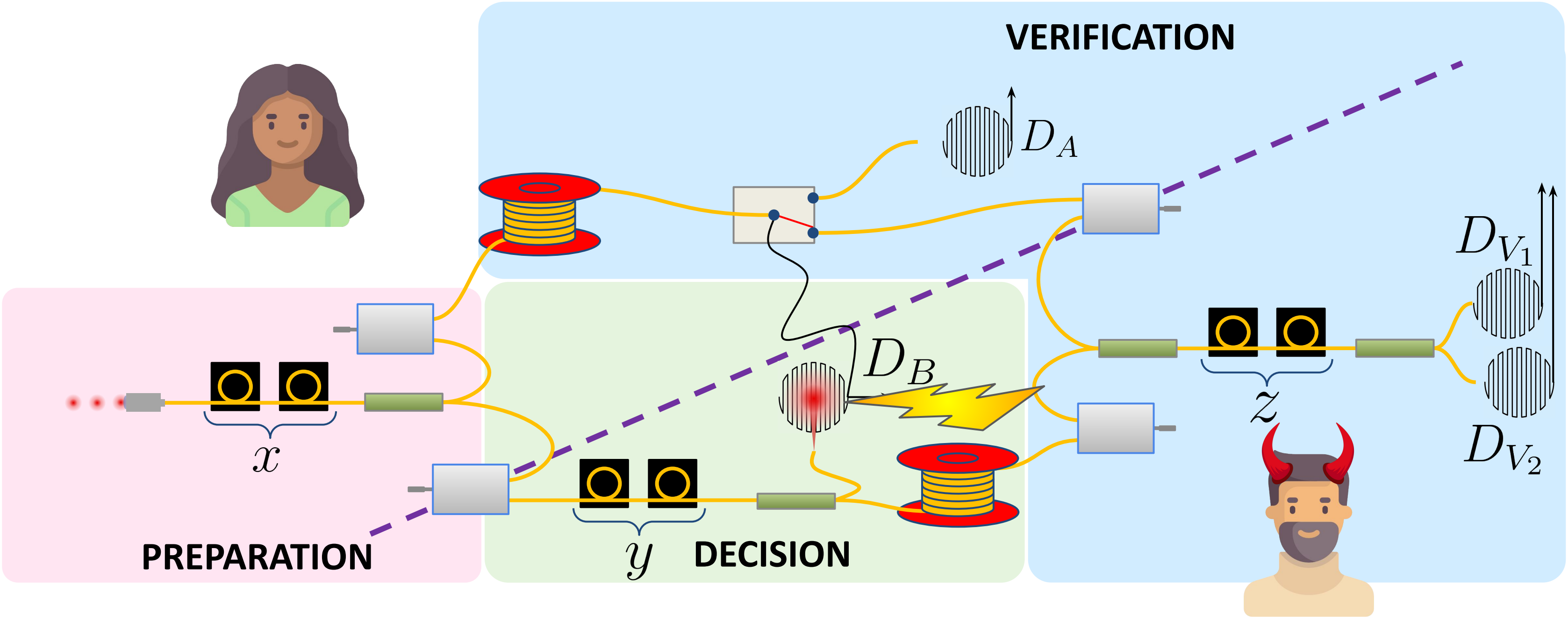
Possible Cheating Strategies



Cheat-Sensitivity

Quantum advantage!

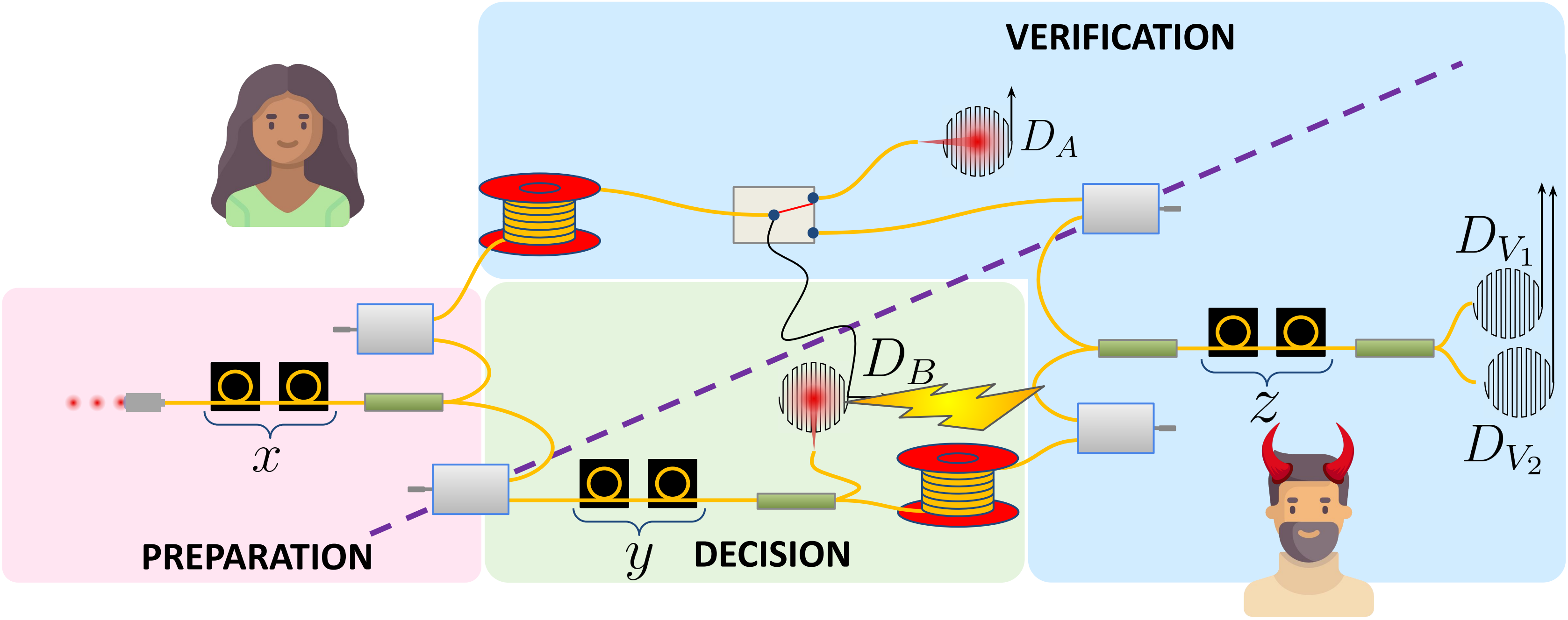
Possible Cheating Strategies



Cheat-Sensitivity

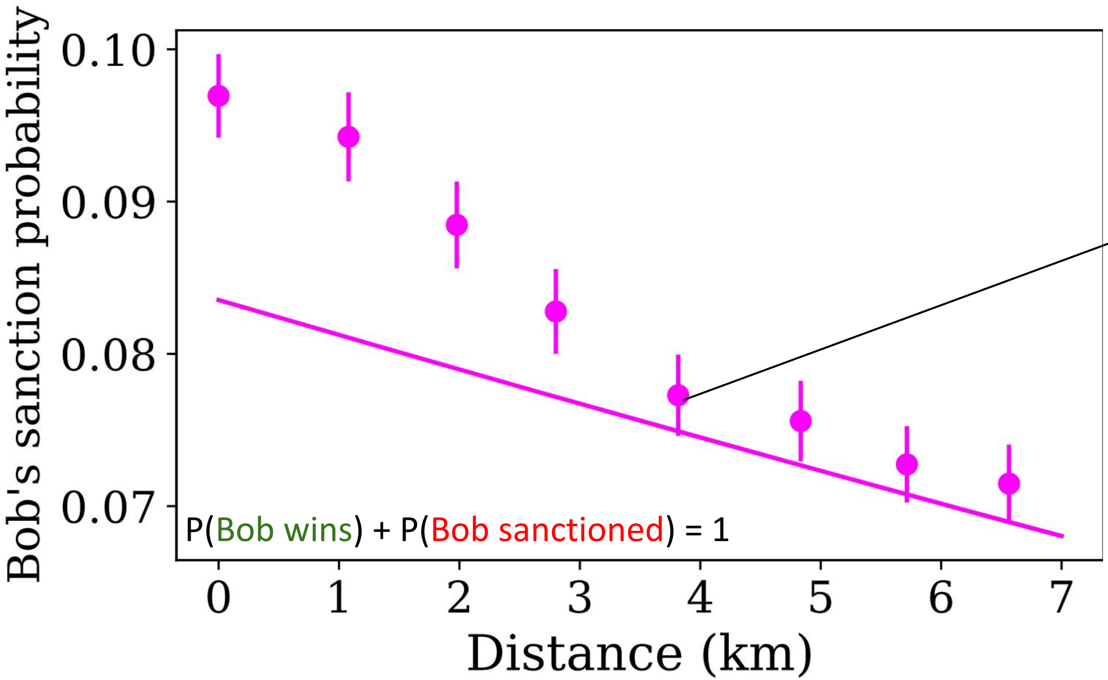
Quantum advantage!

Possible Cheating Strategies



Cheat-Sensitivity

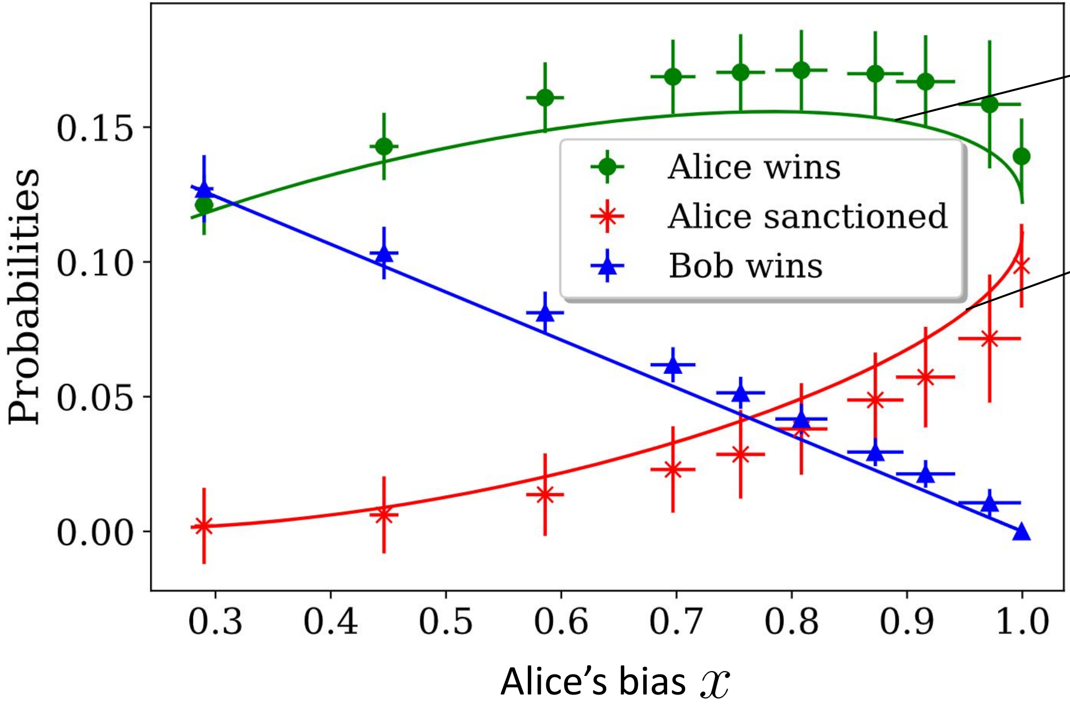
Dishonest Bob



Cheat-sensitivity decreases with losses and communication distance

Cheat-Sensitivity

Dishonest Alice



Winning probability peaks for a bias $x < 1$

Sanction probability increases with bias

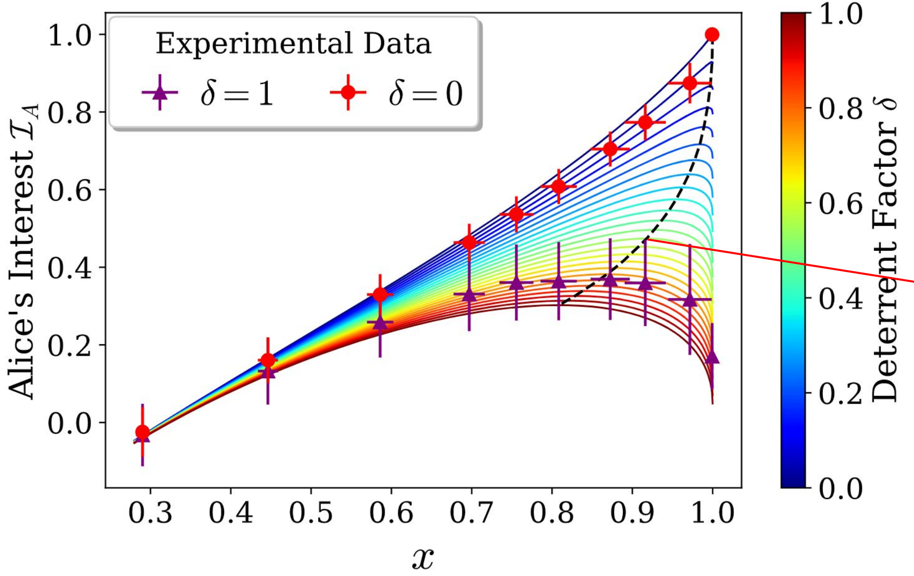
Cheat-sensitivity limits Alice's cheating strategies

Cheat-Sensitivity

Dishonest Alice

Alice's interest in cheating: $\mathcal{I}_A(\delta) = \dfrac{\mathbb{P}(\text{A. wins}) - \mathbb{P}(\text{B. wins}) - \delta\,\mathbb{P}(\text{A. sanctioned})}{\mathbb{P}(\text{A. wins}) + \mathbb{P}(\text{B. wins}) + \delta\,\mathbb{P}(\text{A. sanctioned})}$

deterrent factor = *strength of the sanction*



The interest peaks thanks to cheat-sensitivity!

nature communications

Article https://doi.org/10.1038/s41467-023-37566-x

Experimental cheat-sensitive quantum weak coin flipping

Received: 9 November 2022

Accepted: 22 March 2023

Published online: 03 April 2023

Check for updates

Simon Neves[1], Verena Yacoub[1], Ulysse Chabaud[2,3], Mathieu Bozzio[4], Iordanis Kerenidis[5] & Eleni Diamanti[1]

As in modern communication networks, the security of quantum networks will rely on complex cryptographic tasks that are based on a handful of fundamental primitives. Weak coin flipping (WCF) is a significant such primitive which allows two mistrustful parties to agree on a random bit while they favor opposite outcomes. Remarkably, perfect information-theoretic security can be achieved in principle for quantum WCF. Here, we overcome conceptual and practical issues that have prevented the experimental demonstration of this primitive to date, and demonstrate how quantum resources can provide cheat sensitivity, whereby each party can detect a cheating opponent, and an honest party is never sanctioned. Such a property is not known to be classically achievable with information-theoretic security. Our experiment implements a refined, loss-tolerant version of a recently proposed theoretical protocol and exploits heralded single photons generated by spontaneous parametric down conversion, a carefully optimized linear optical interferometer including beam splitters with variable reflectivities and a fast optical switch for the verification step. High values of our protocol benchmarks are maintained for attenuation corresponding to several kilometers of telecom optical fiber.

Acknowledgement


Verena Yacoub

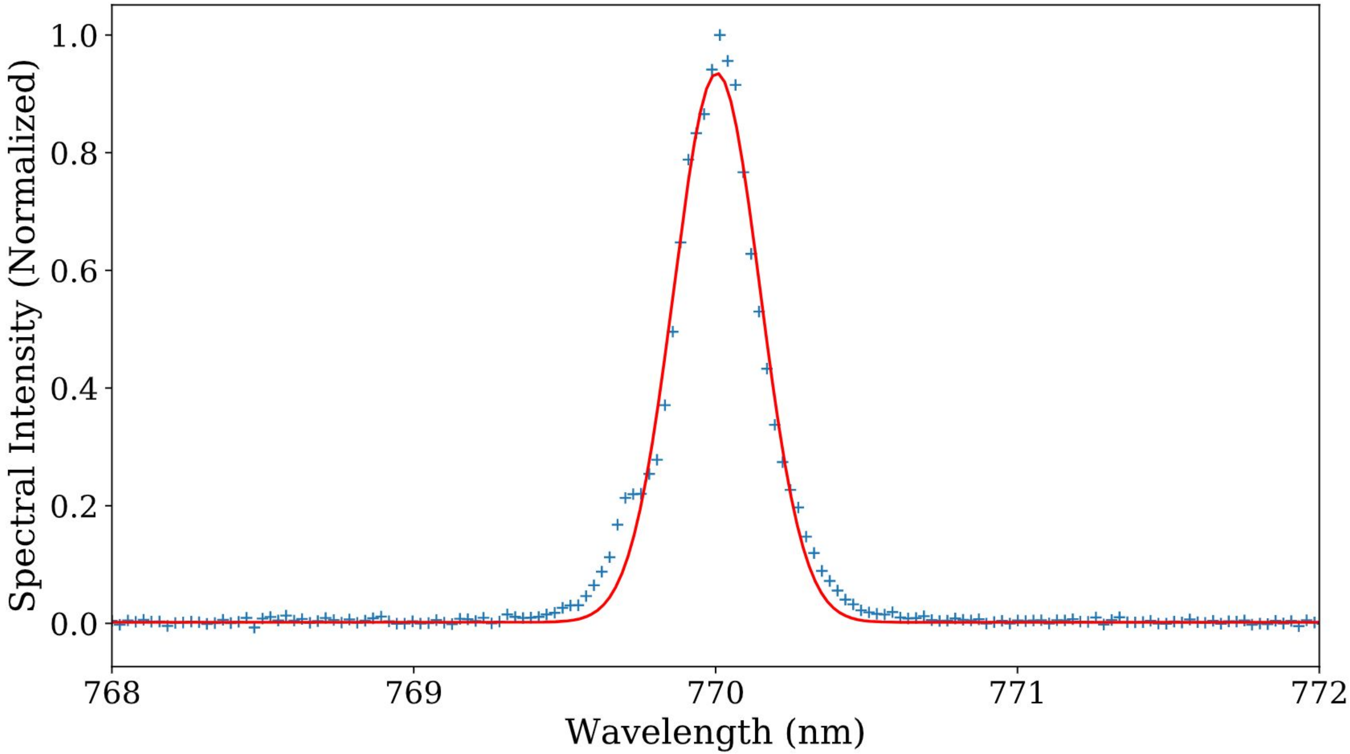

Ulysse Chabaud


Mathieu Bozzio

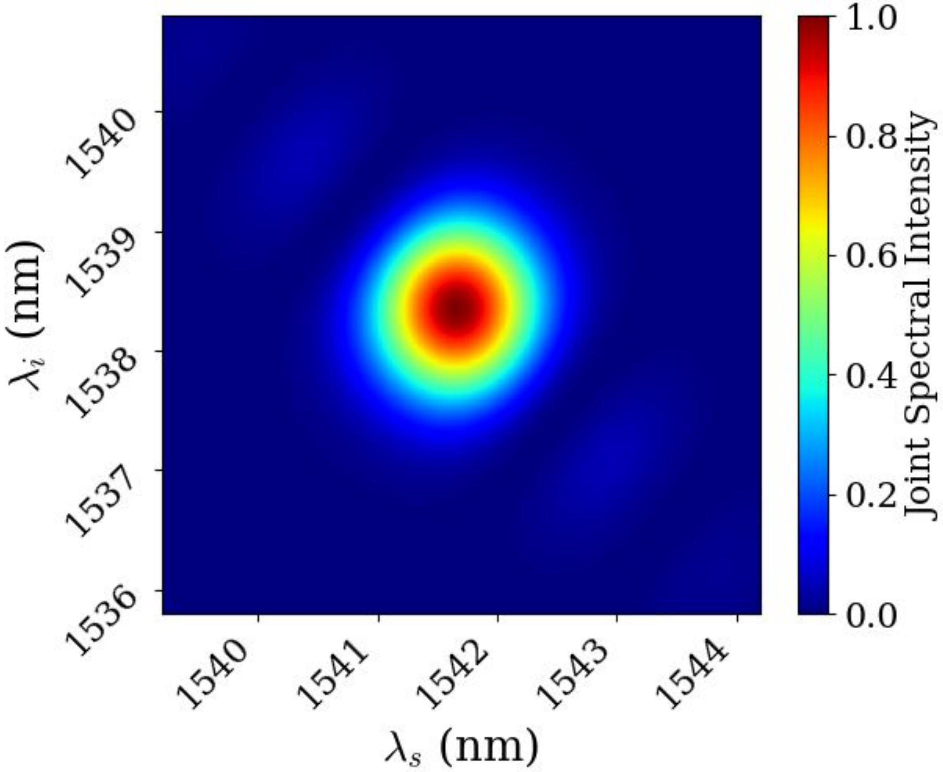

Iordanis Kerenidis


Eleni Diamanti

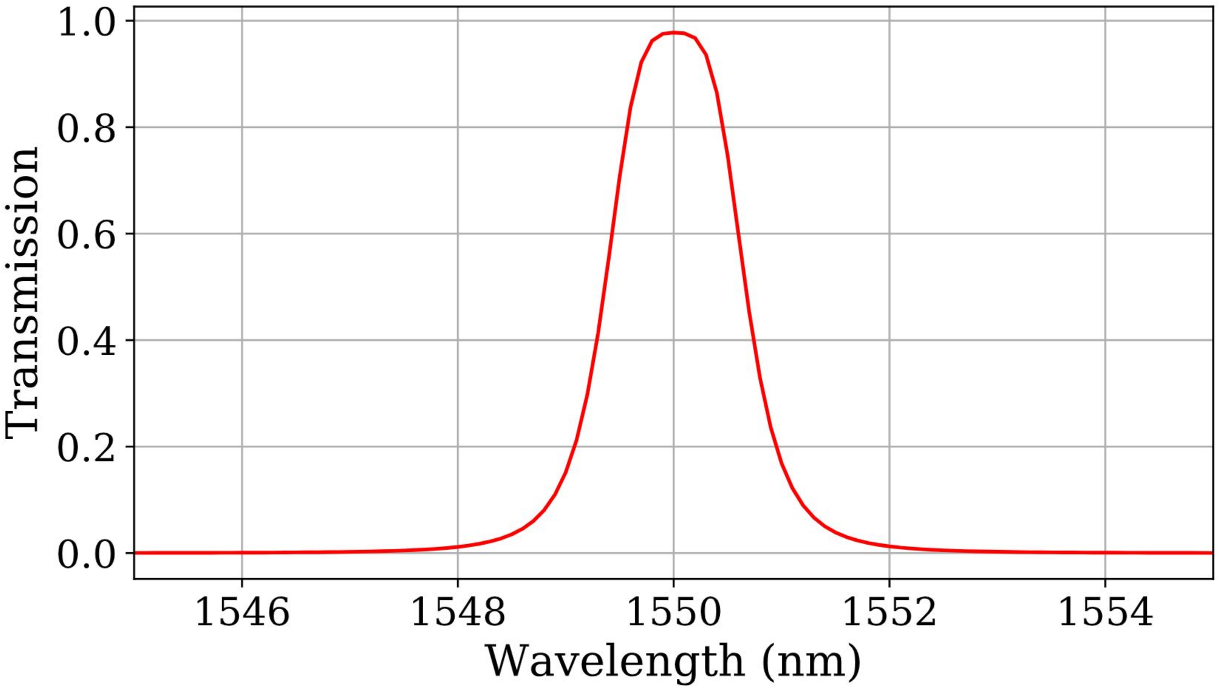
Pump Spectrum



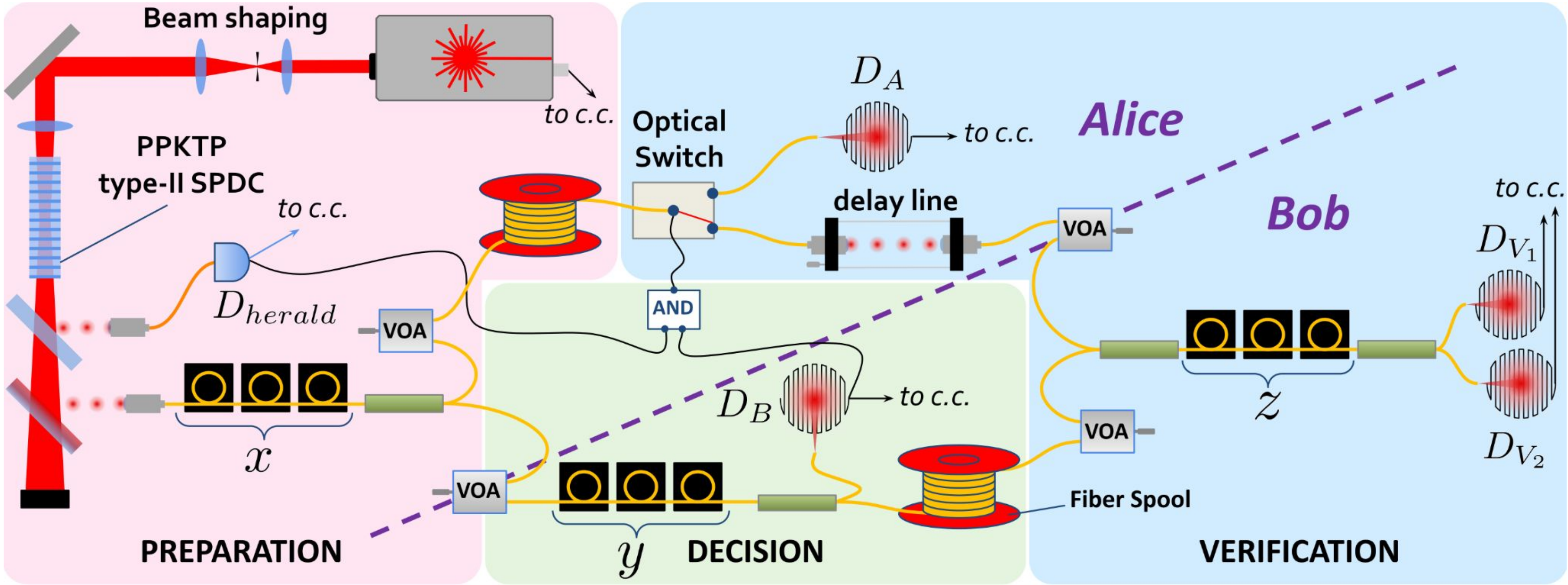
Photon Pair Spectral State



Photon Spectral Filtering



Full Setup


Beam shaping
to c.c.
PPKTP
type-II SPDC
to c.c.
D_{herald}
VOA
x
PREPARATION
Optical Switch
D_A
to c.c.
Alice
delay line
VOA
Bob
to c.c.
D_{V_1}
D_{V_2}
AND
D_B
to c.c.
VOA
y
DECISION
z
VOA
Fiber Spool
VERIFICATION

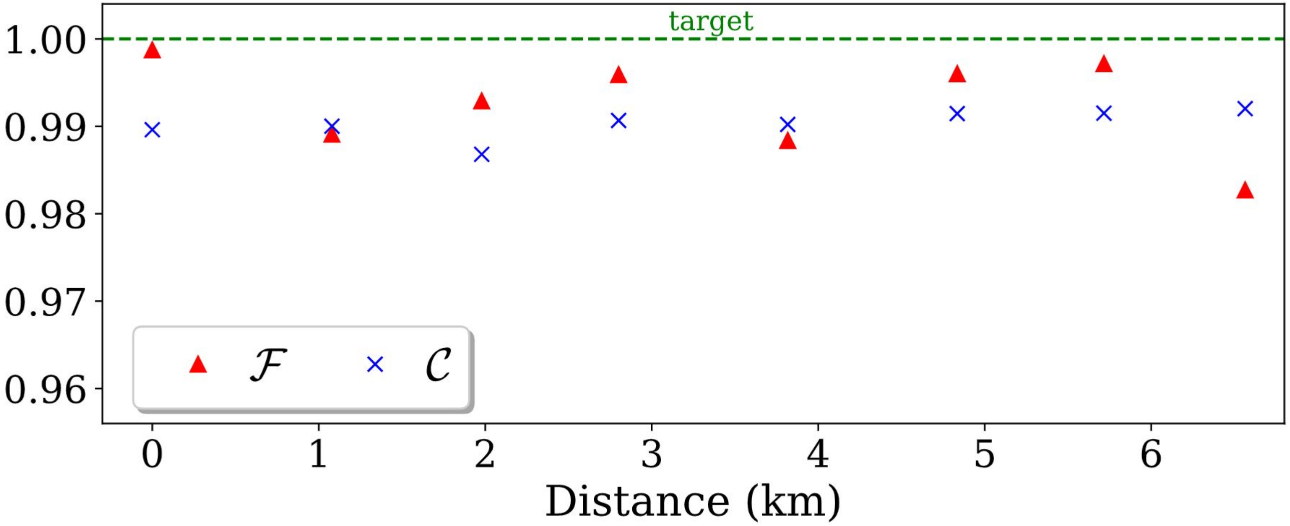
Detection Efficiencies

Notation	Path	x	y	z	s	Efficiency
η_A^s	$x \rightarrow \text{switch} \rightarrow D_A$	1			1	0.315 ± 0.008
η_B^y	$x \rightarrow y \rightarrow D_B$	0	0			0.303 ± 0.008
$\eta_A^{V_1}$	$x \rightarrow \text{switch} \rightarrow z \rightarrow D_{V_1}$	1		1	0	0.231 ± 0.008
$\eta_A^{V_2}$	$x \rightarrow \text{switch} \rightarrow z \rightarrow D_{V_2}$	1		0	0	0.219 ± 0.008
$\eta_B^{V_1}$	$x \rightarrow y \rightarrow z \rightarrow D_{V_1}$	0	1	0		0.184 ± 0.008
$\eta_B^{V_2}$	$x \rightarrow y \rightarrow z \rightarrow D_{V_2}$	0	1	1		0.175 ± 0.008

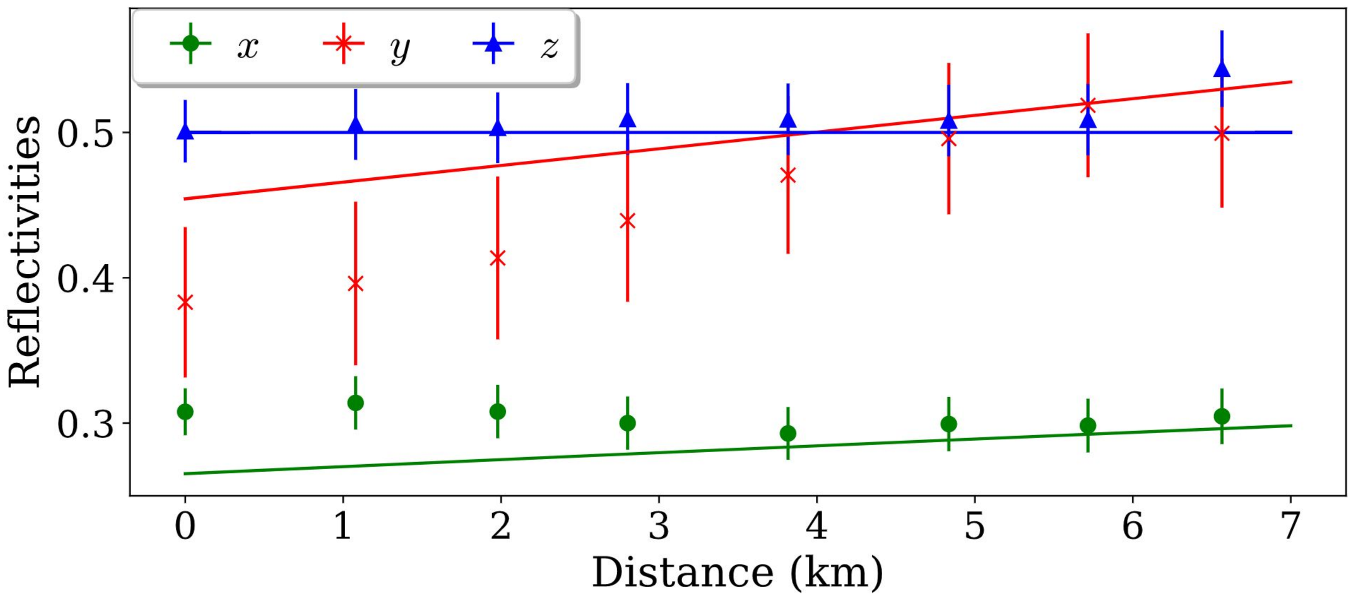
Fairness & Correctness

$$\mathcal{F} = 1 - \left| \frac{\mathbb{P}_h(\text{A. wins}) - \mathbb{P}_h(\text{B. wins})}{\mathbb{P}_h(\text{A. wins}) + \mathbb{P}_h(\text{B. wins})} \right|$$

$$\mathcal{C} = 1 - \frac{\mathbb{P}_h(\text{A. sanctioned}) + \mathbb{P}_h(\text{B. sanctioned})}{\mathbb{P}_h(\text{A. wins}) + \mathbb{P}_h(\text{B. wins})}$$



Reflectivities, Honest Players



Reflectivities, Honest Players

Theoretical Formulas

$$x_h = \left[1 + \frac{\eta_A^{V_1}}{\eta_B^{V_1}} + \frac{\eta_A^{V_1}}{\eta_B^{y}}(1+v)\right]^{-1}$$

$$y_h = \left[1 + \frac{\eta_B^{V_1}}{\eta_B^{y}}(1+v)\right]^{-1}$$

$$z_h = \frac{1}{2}$$