

High-Dimensional Quantum Key Distribution with Structured Photons

Presented by:



Quantum Computing
and Communication
Technical Group

The OSA Quantum Computing and Communication Technical Group Welcomes You!



HIGH-DIMENSIONAL QUANTUM KEY DISTRIBUTION WITH STRUCTURED PHOTONS

16 January 2020 • 10:00 EST

OSA Quantum Computing
and Communication
Technical Group

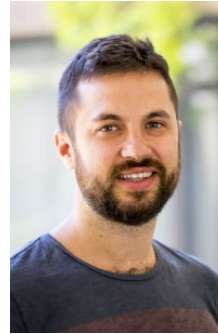
OSA Quantum Computing
and Communication
Technical Group

Technical Group Leadership 2020



Roberto de J. León-Montiel

Chair
UNAM, Mexico



Vito Giovanni Lucivero

ICFO, Spain



Veronica Vicuña-Hernandez

University of Naples "Federico II"



Ricardo Tellez-Limon

CICESE, Mexico



Jorge L. Domínguez-Juárez

UNAM, Mexico



Quantum Computing
and Communication
Technical Group

Technical Group at a Glance

•Focus

- Theoretical and experimental aspects of quantum computing
- Quantum communication systems - Cryptography
- Generation, detection and applications of non-classical light
- Quantum measurement and quantum control

•Mission

- To maximize the exchange of information and the creation of networking opportunities for our community
- Webinars, technical events (workshops, tutorials, poster sessions), outreach activities
- Interested in presenting your research? Have ideas for TG events? Contact us at TGactivities@osa.org.

•Find us here

- Website: www.osa.org/OC
- Facebook: <https://www.facebook.com/groups/OSAQuantumCC/>



Quantum Computing
and Communication
Technical Group

Today's Webinar

High-Dimensional Quantum Key Distribution with Structured Photons

Dr. Ebrahim Karimi

Group leader of Structural Quantum Optics (SQO) at the University of Ottawa.

ebrahim.karimi@sqogroup.ca

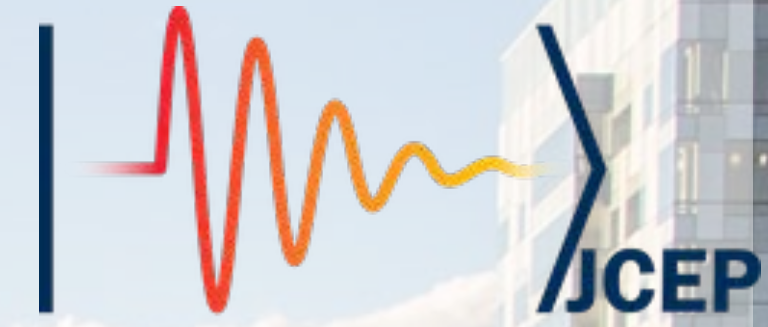
Speaker's Short Bio:

B. Sc. in Physics at Kerman University, Iran.

Ph.D. degree from the University of Naples "Federico II", Italy.

Postdoctoral fellow at Quantum Optics group, University of Ottawa.



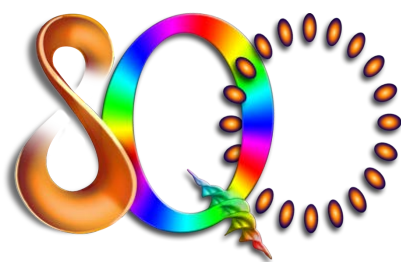


Quantum Cryptography with structured photons

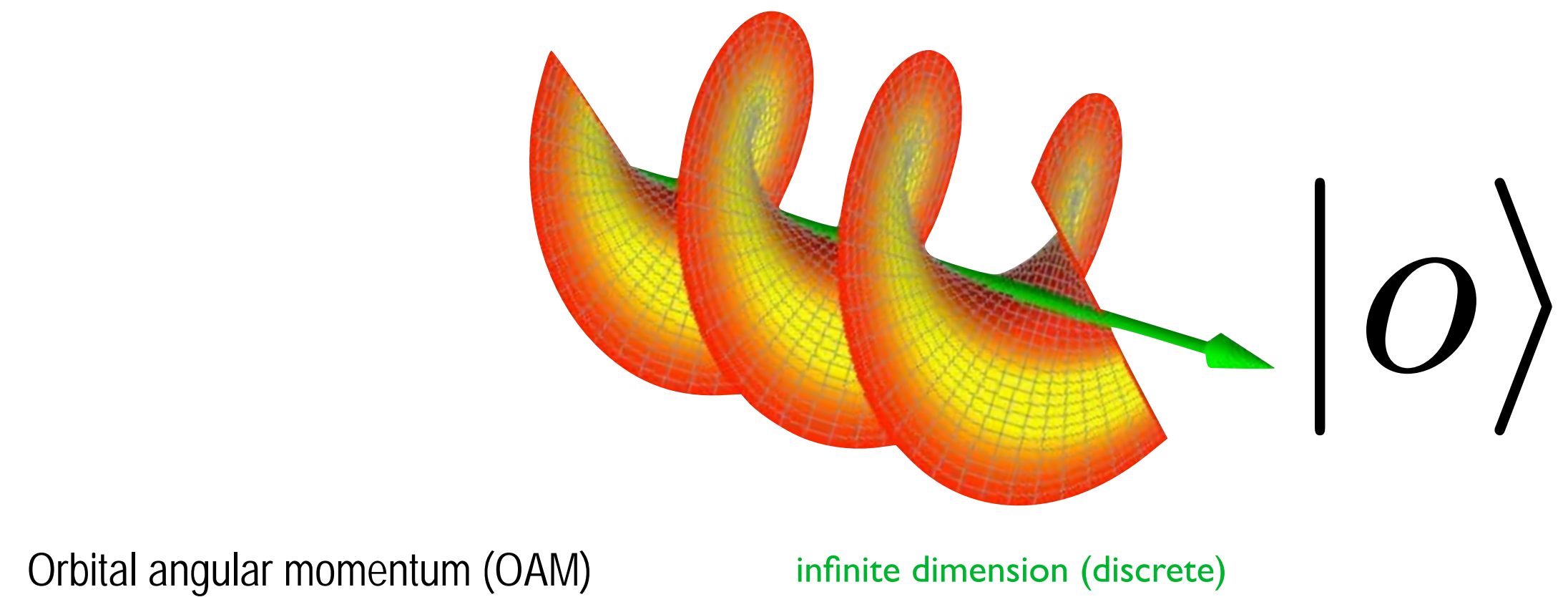
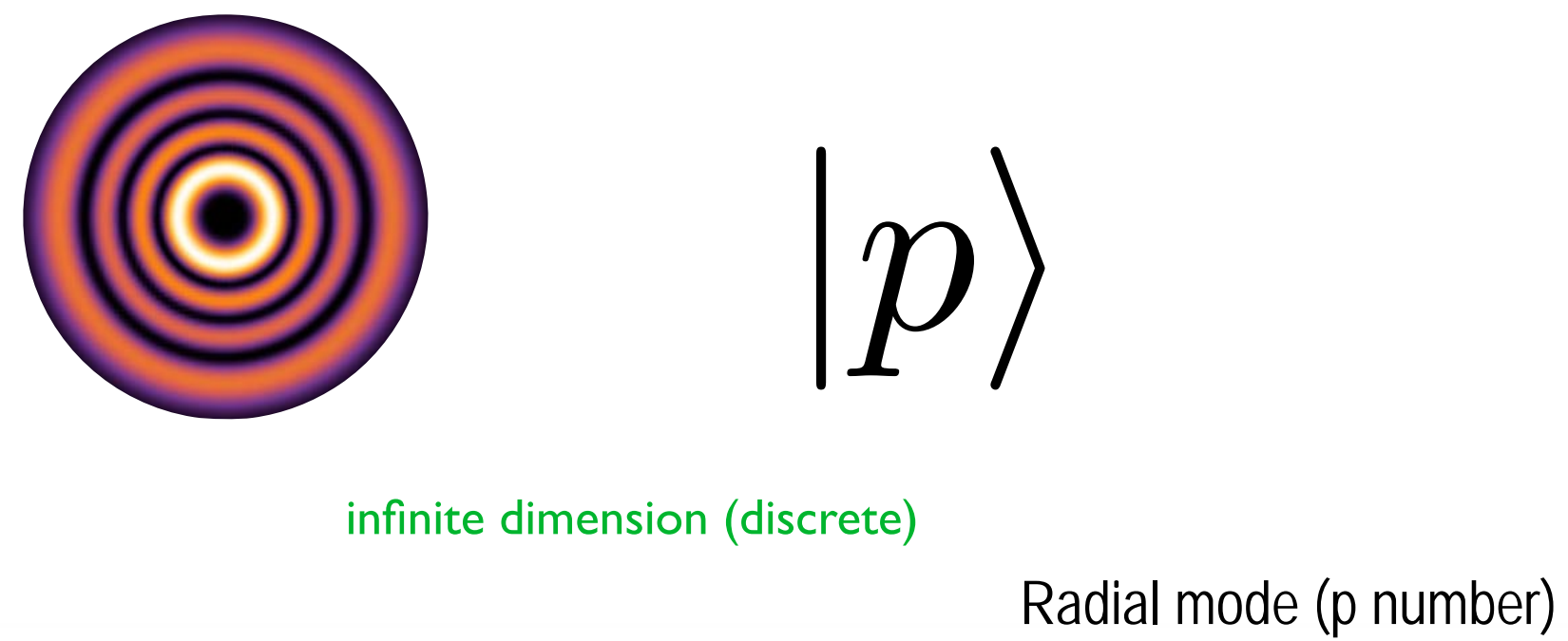
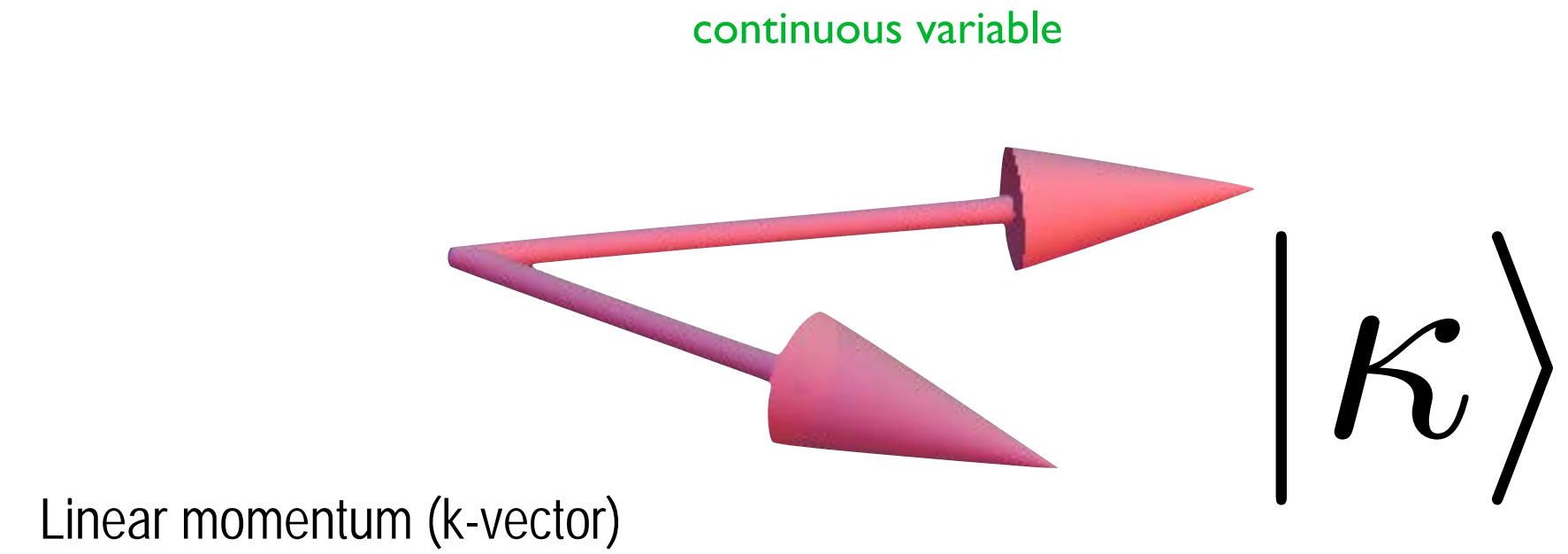
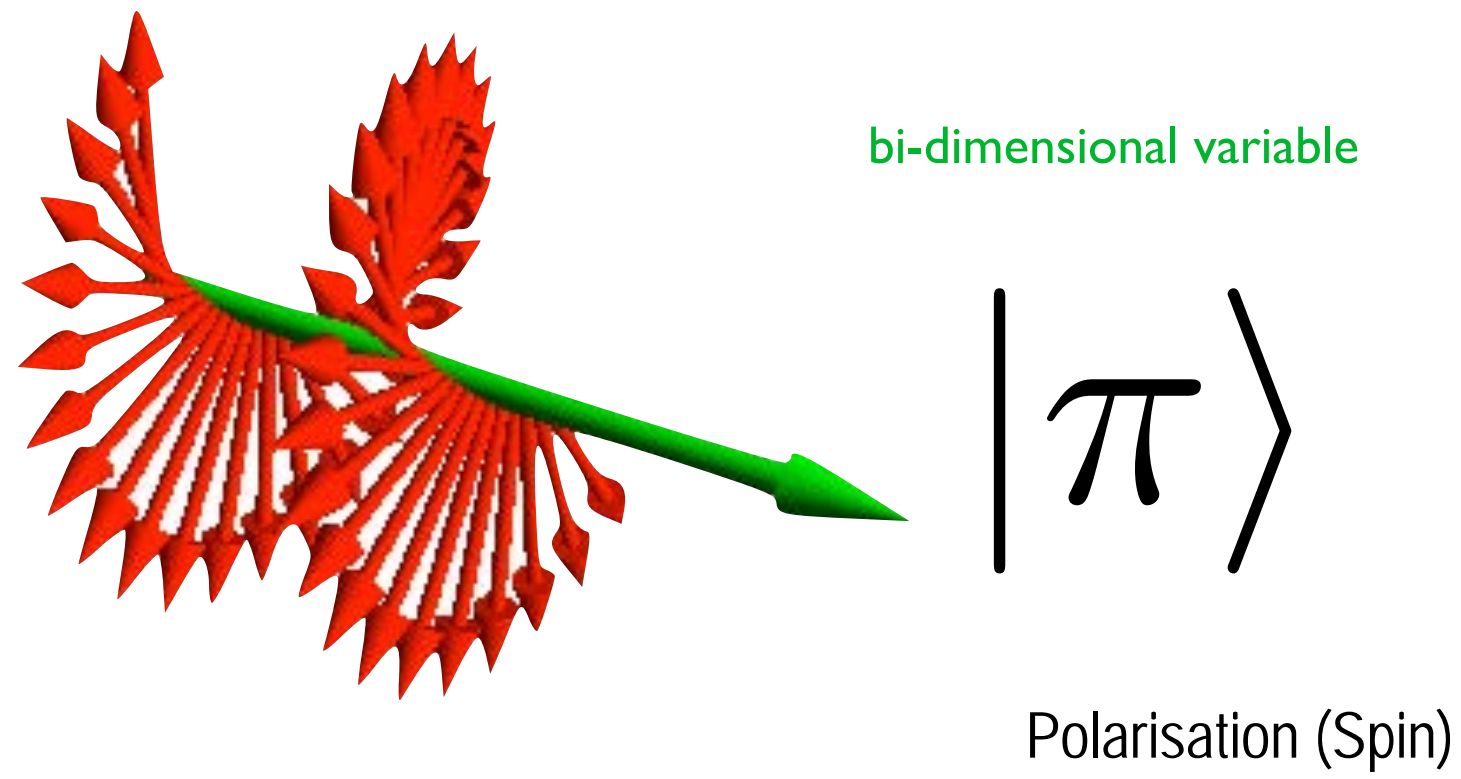
PRÉSENTÉ PAR : EBRAHIM KARIMI | PRESENTED BY: EBRAHIM KARIMI



Structured Photons



Photons Degrees of Freedom

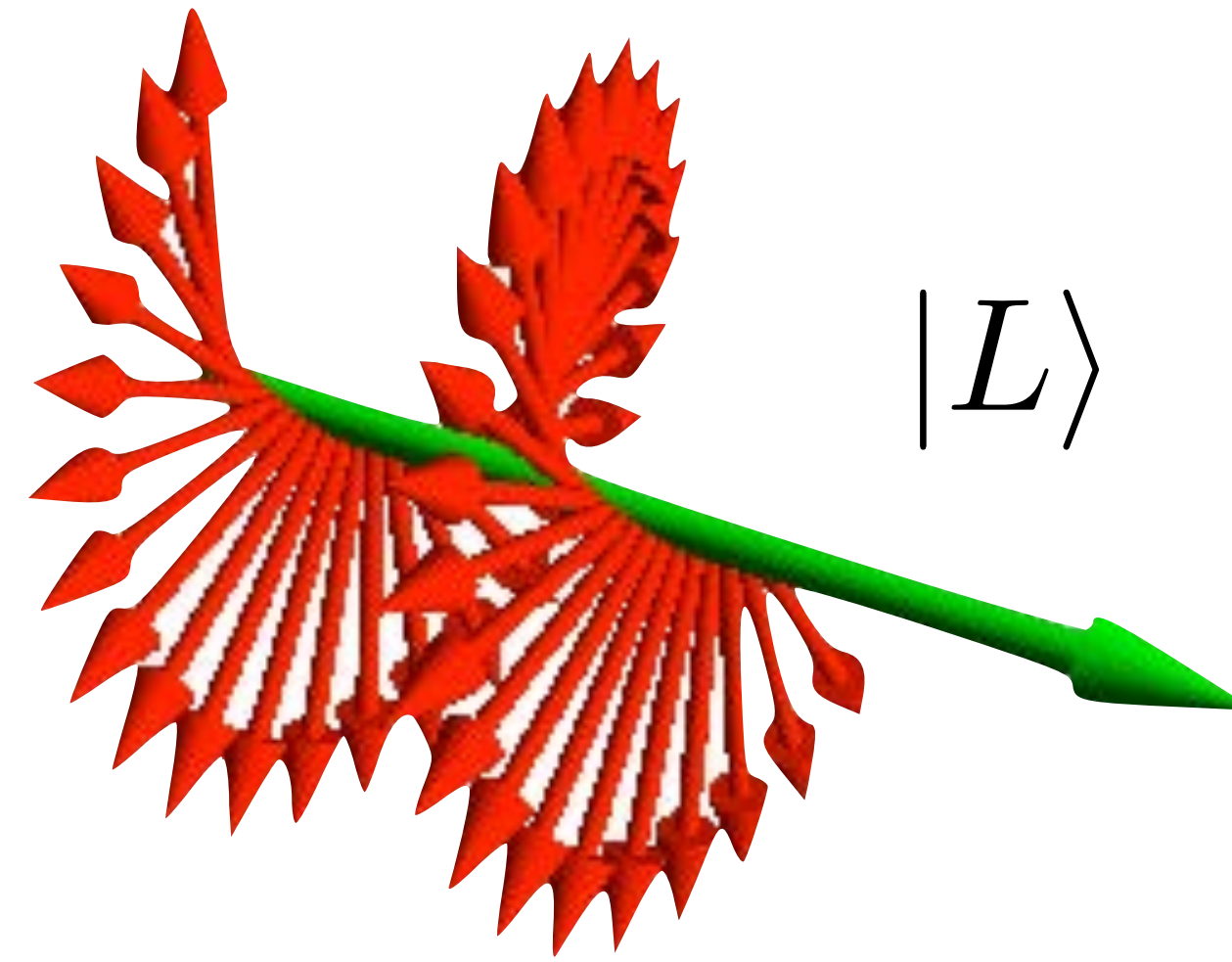


Spin Angular Momentum

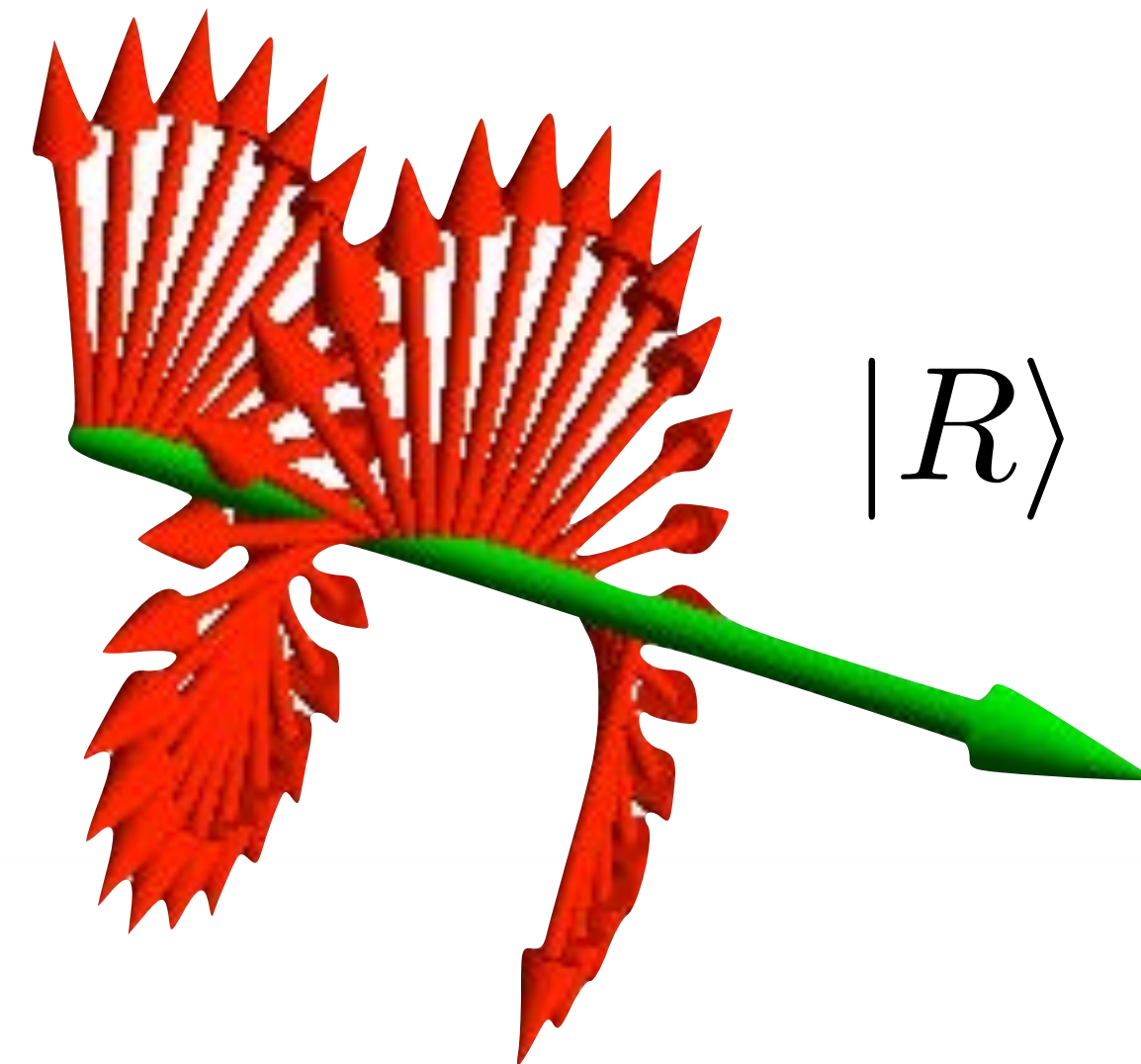
- Circular polarisations: (Left and Right)
- Spin angular momentum may take two values of $\pm \hbar$

$|L\rangle$ Left-handed circular polarisation
 $|R\rangle$ Right-handed circular polarisation

vectorial picture



$|L\rangle$



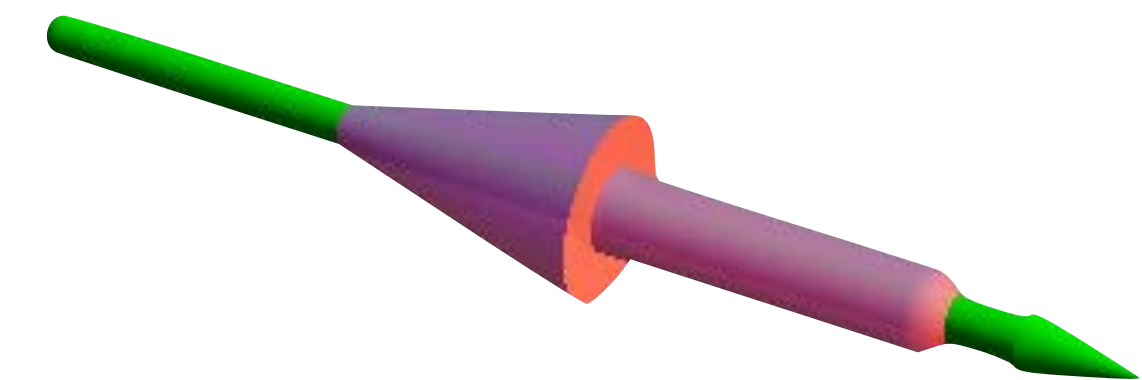
$|R\rangle$

angular momentum

$$J_z = +\hbar$$



$$J_z = -\hbar$$



Optical Angular Momentum

- Optical field expression in the cylindrical coordinate is

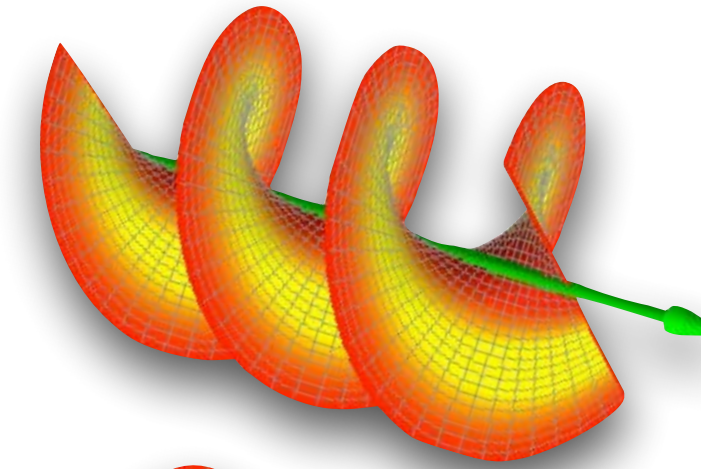
$$\hat{L}_z = -i\partial_\phi$$

$$E(r, \varphi, z, t) = E(r, z)e^{i\ell\varphi} e^{i(kz-\omega t)}$$

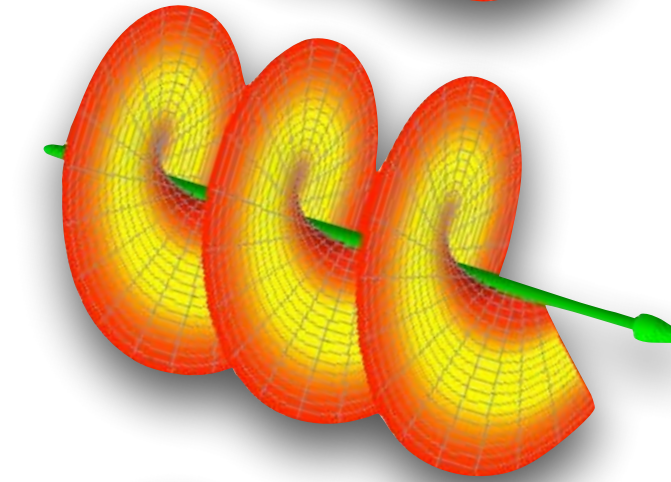
$$J_z = \ell\hbar$$

In the contrast to polarisation, orbital angular momentum may take any of the infinite values $\ell = \dots -2, -1, 0, 1, 2, \dots$

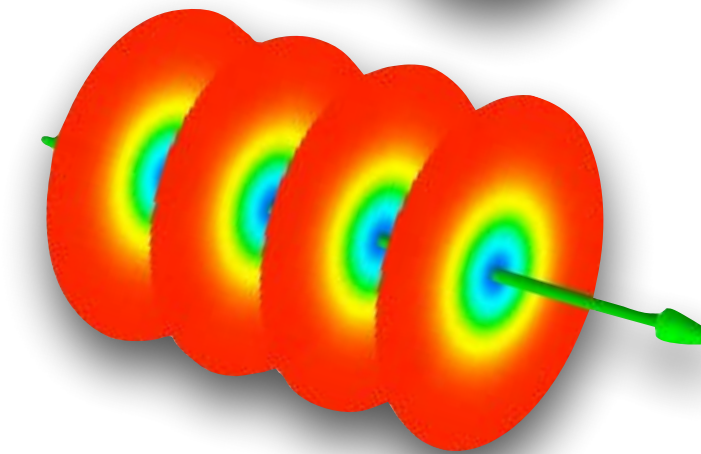
Laguerre-Gaussian modes are one set of paraxial wave mode which carry the OAM.



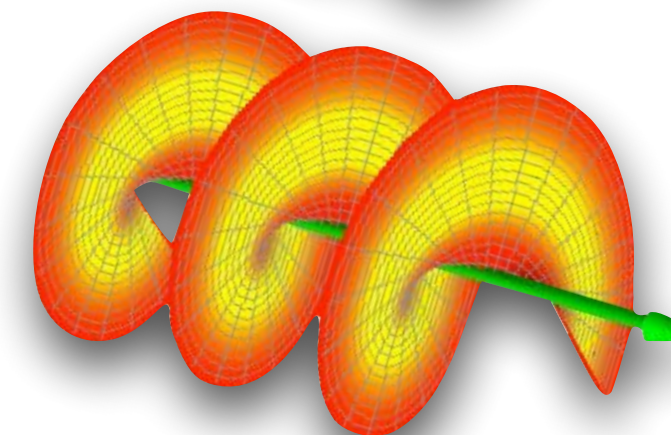
$$\ell = -2 \quad J_z = -2\hbar$$



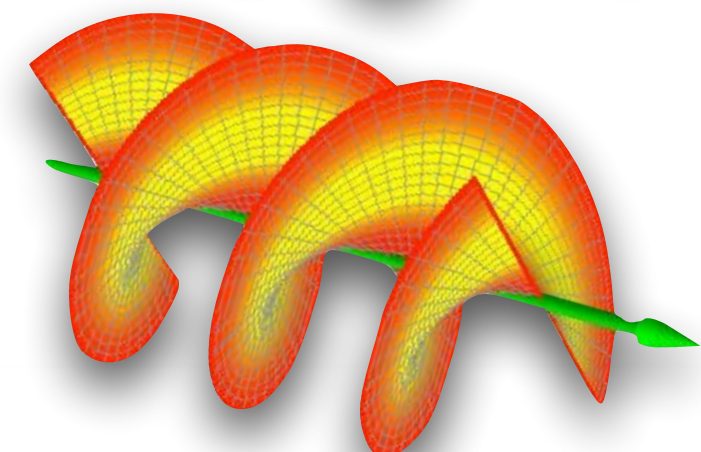
$$\ell = -1 \quad J_z = -\hbar$$



$$\ell = 0 \quad J_z = 0$$



$$\ell = +1 \quad J_z = +\hbar$$



$$\ell = +2 \quad J_z = +2\hbar$$



Optical Angular Momentum

$l = -3$

$l = -2$

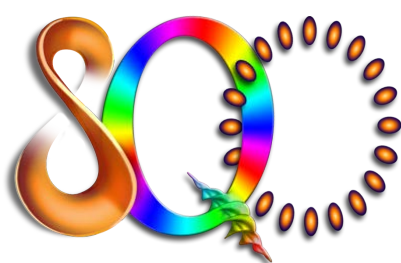
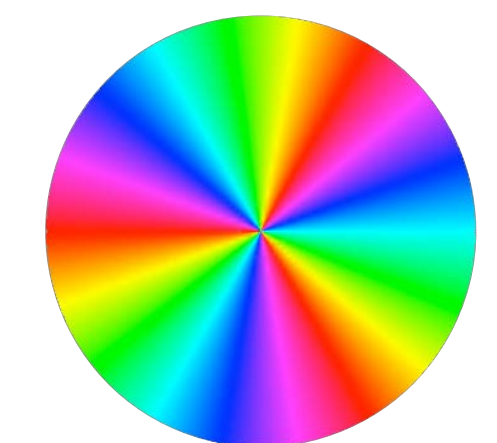
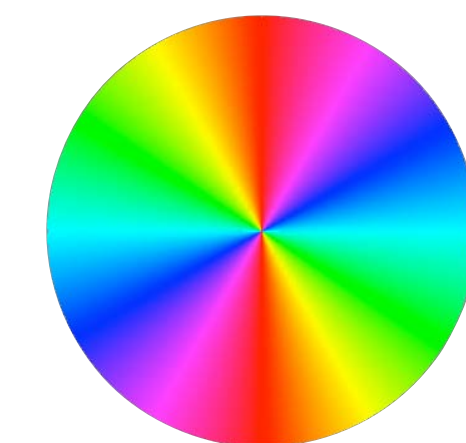
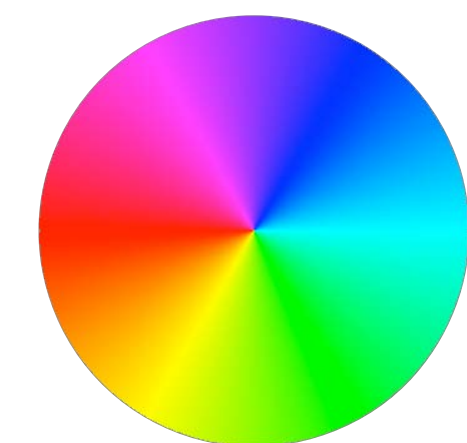
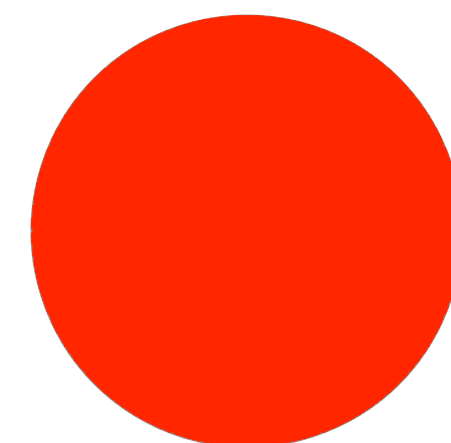
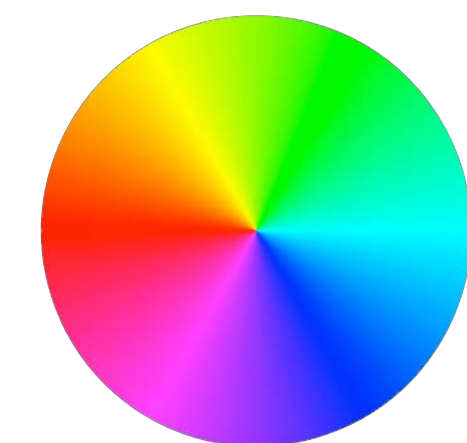
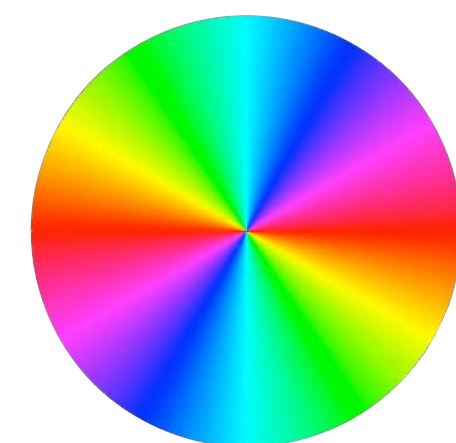
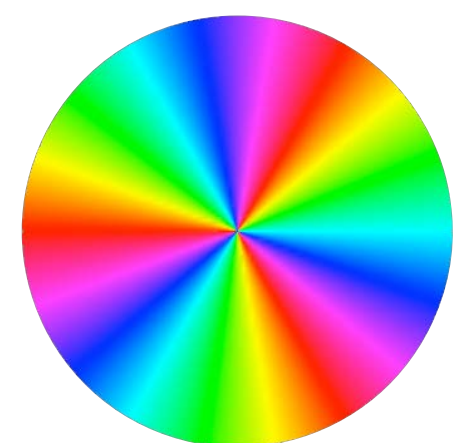
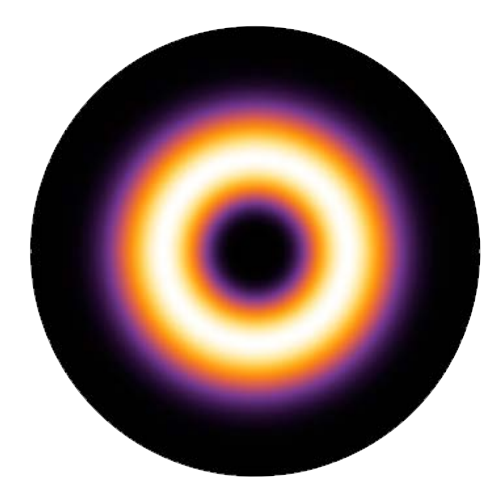
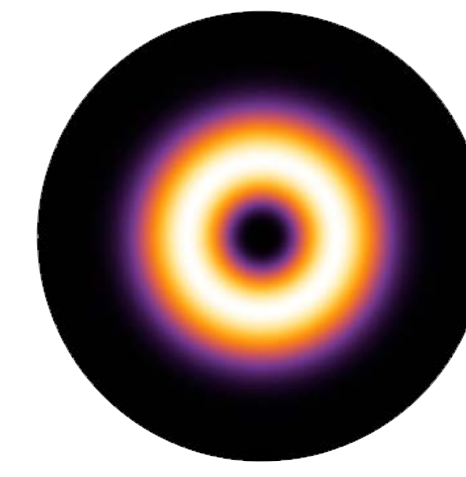
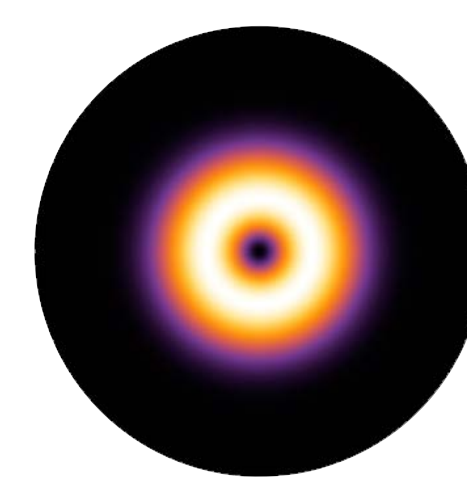
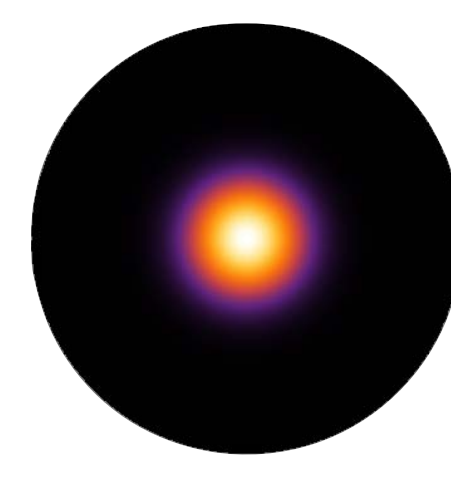
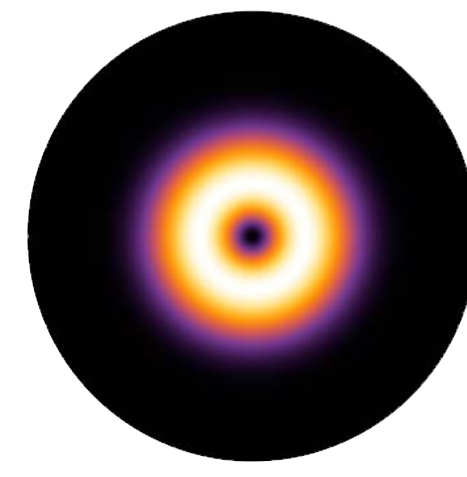
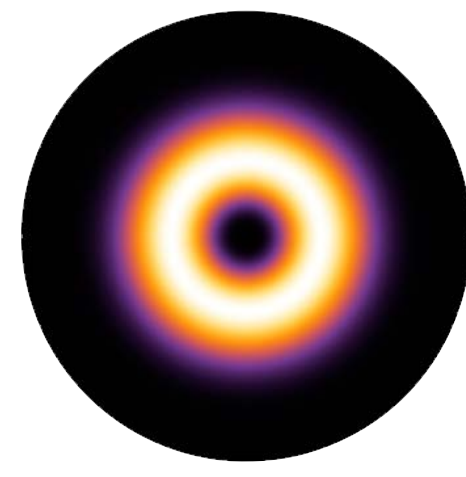
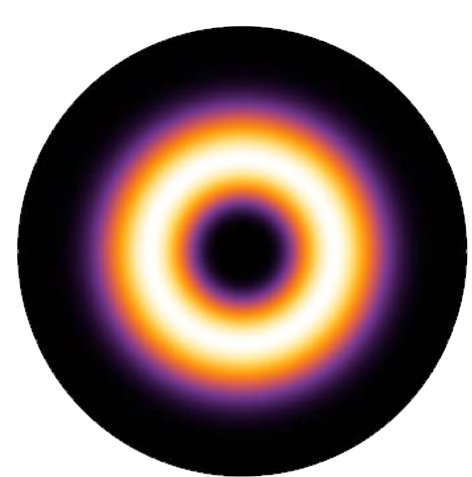
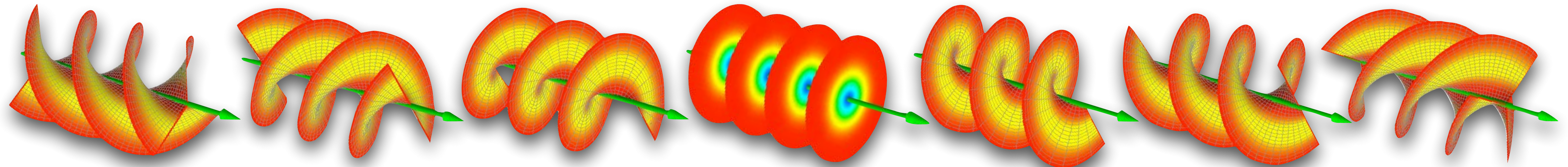
$l = -1$

$l = 0$

$l = +1$

$l = +2$

$l = +3$



Optical Angular Momentum

$$l = -3$$

$$l = -2$$

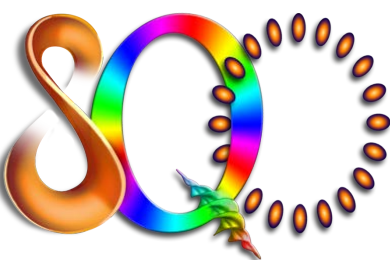
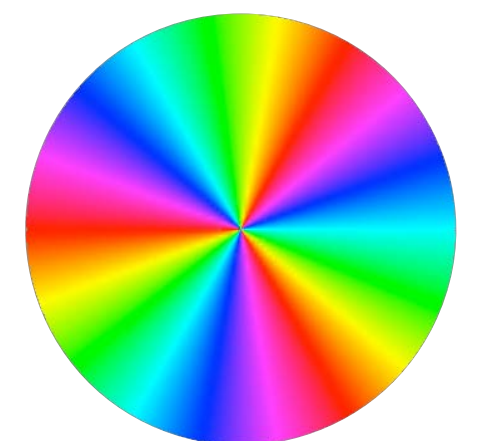
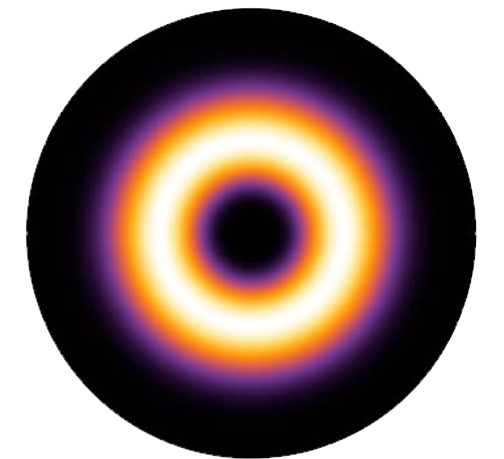
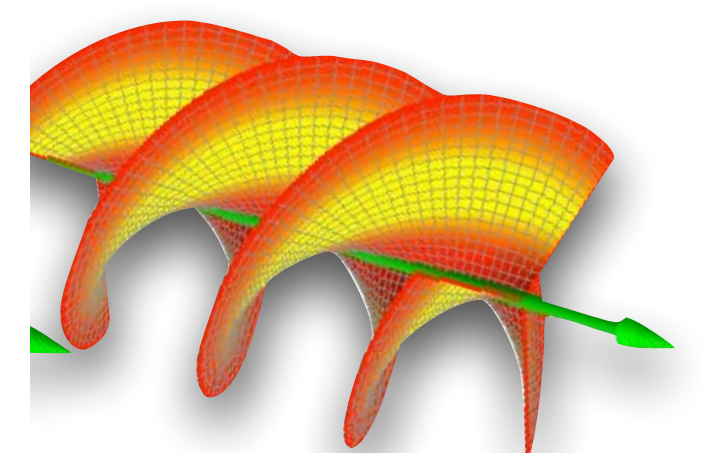
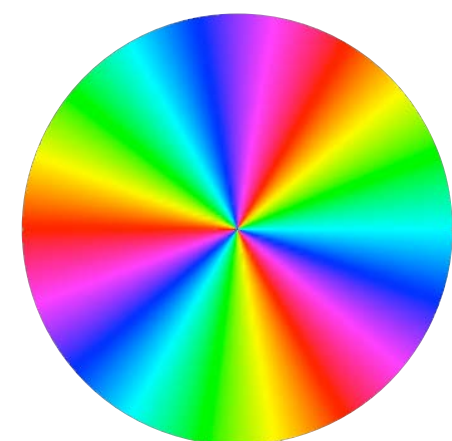
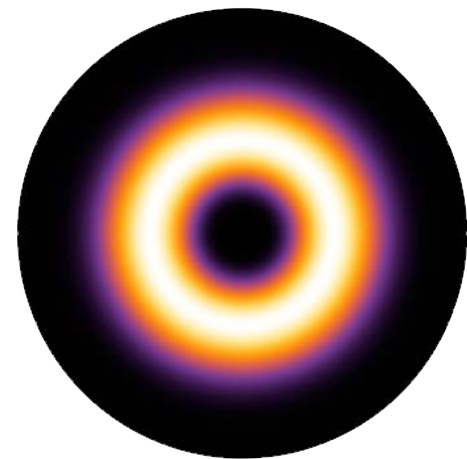
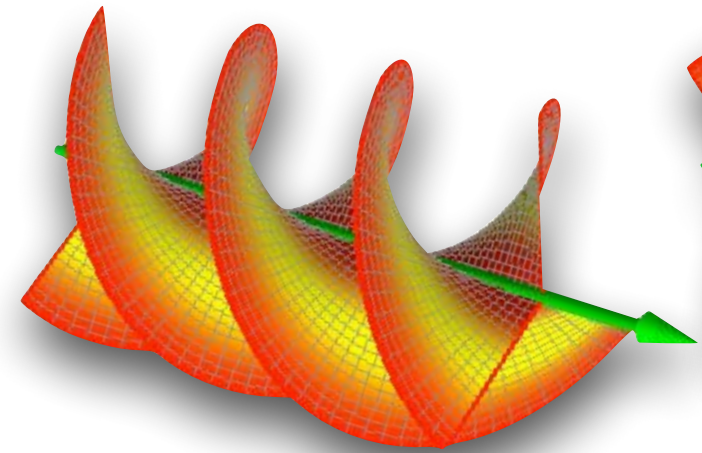
$$l = -1$$

$$l = 0$$

$$l = +1$$

$$l = +2$$

$$l = +3$$



Structured Photons

$$|\psi\rangle = \sum_{\omega, \sigma, n, p, \ell} c_{n,p,\ell}^{\omega, \sigma} |\omega, \sigma, n, p, \ell\rangle$$

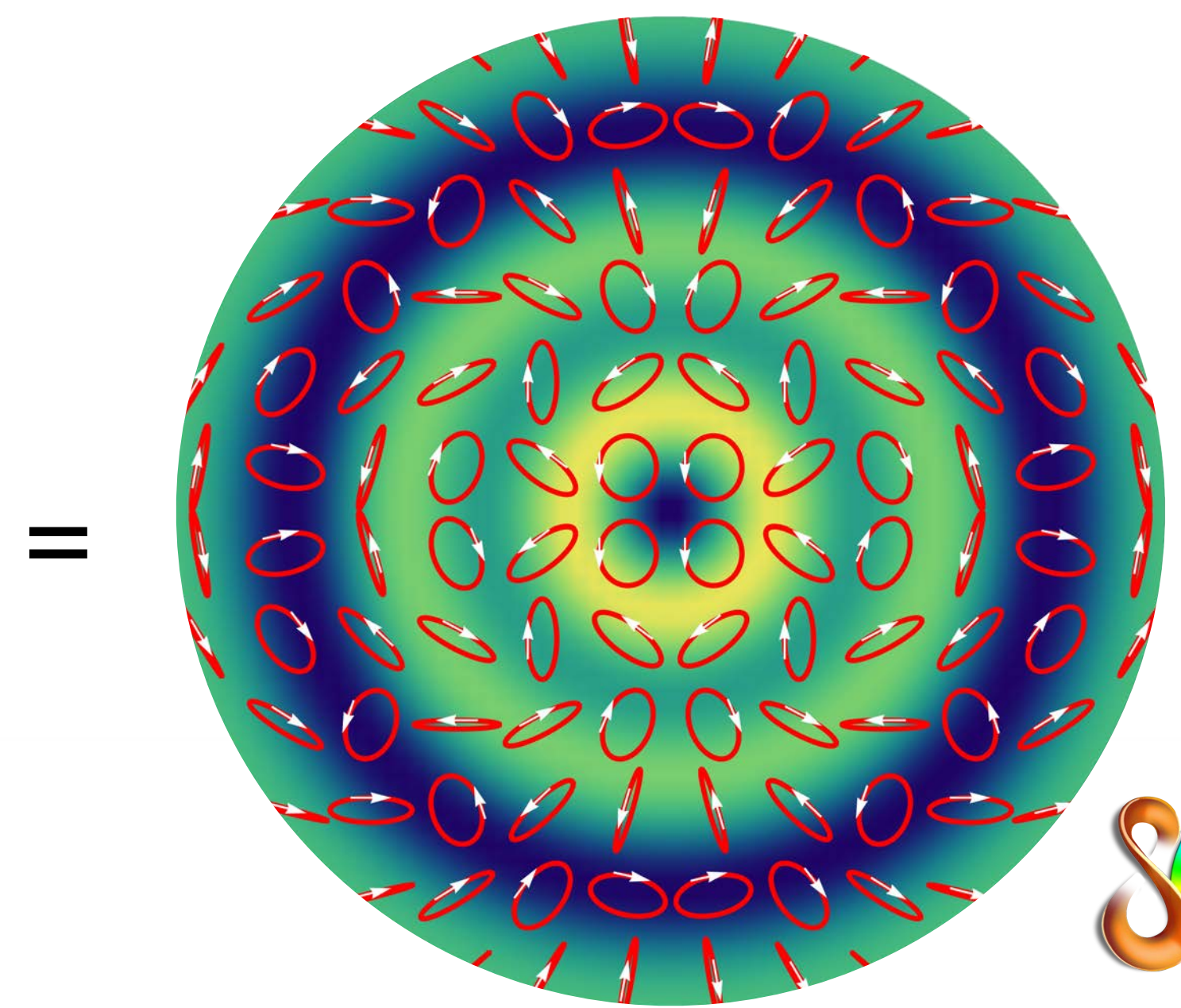
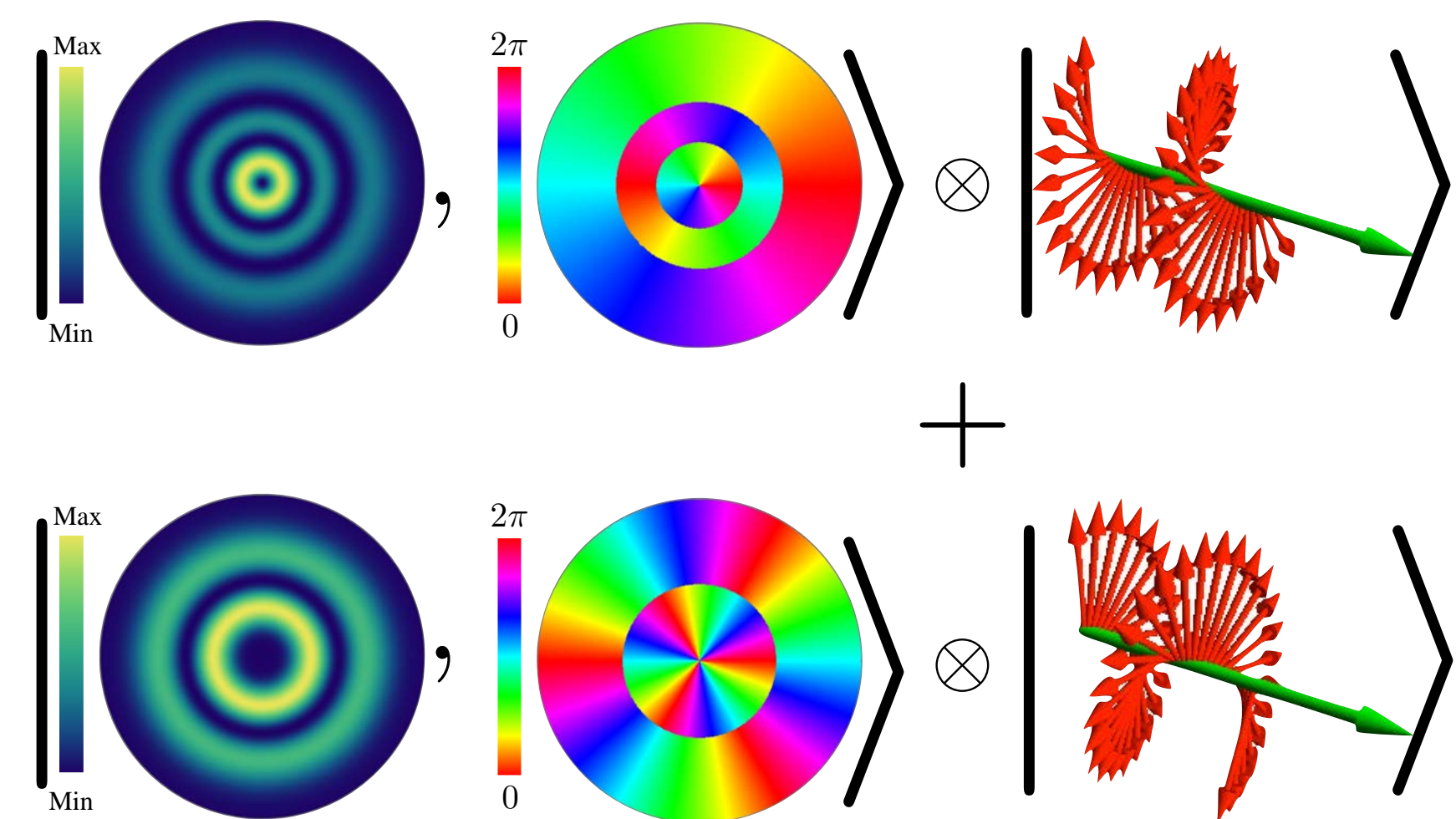
$\omega \in \mathbb{R}$

$\sigma \in \{-1, +1\}$

$n \in \mathbb{Z}^+$

$p \in \mathbb{Z}^+$

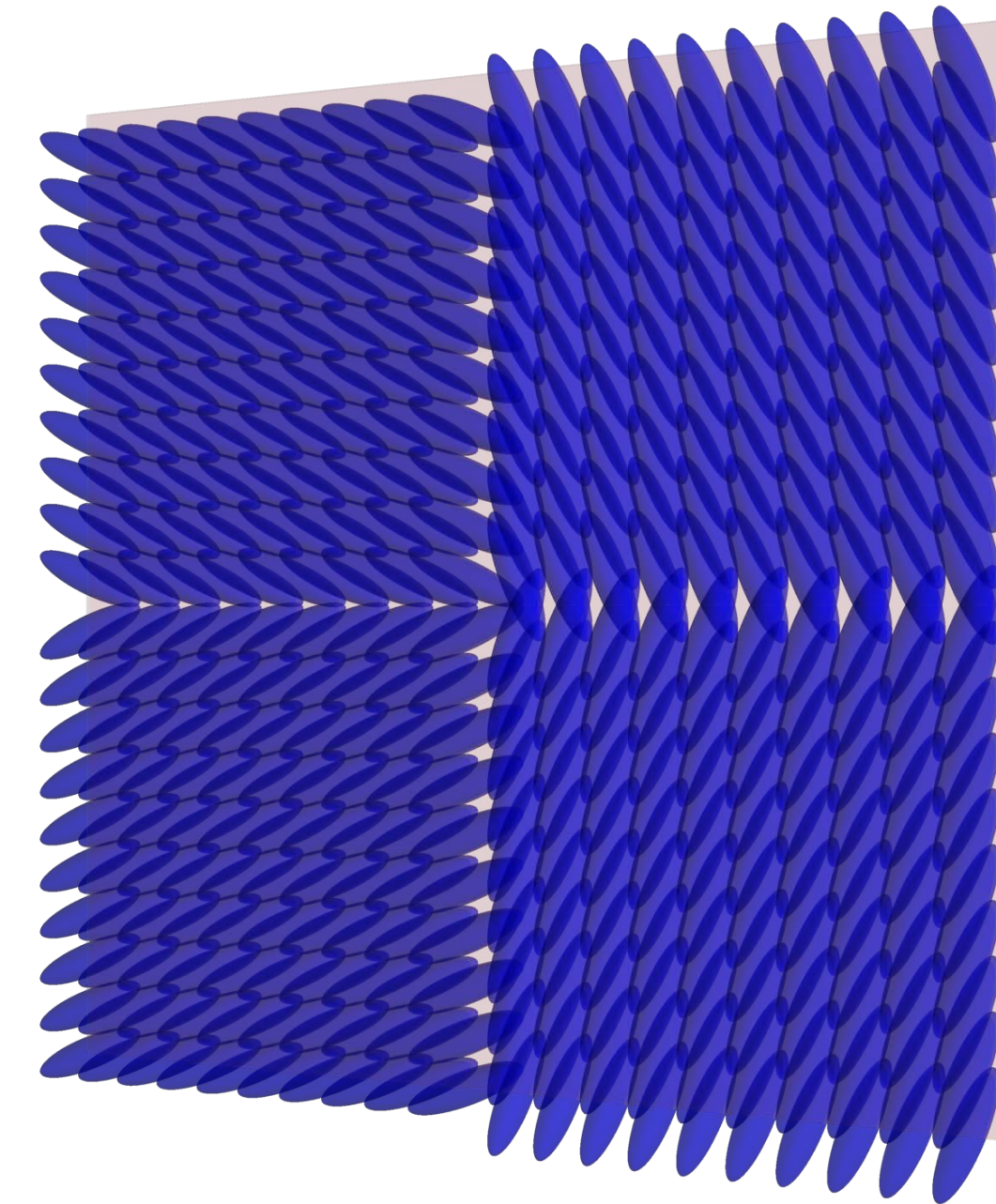
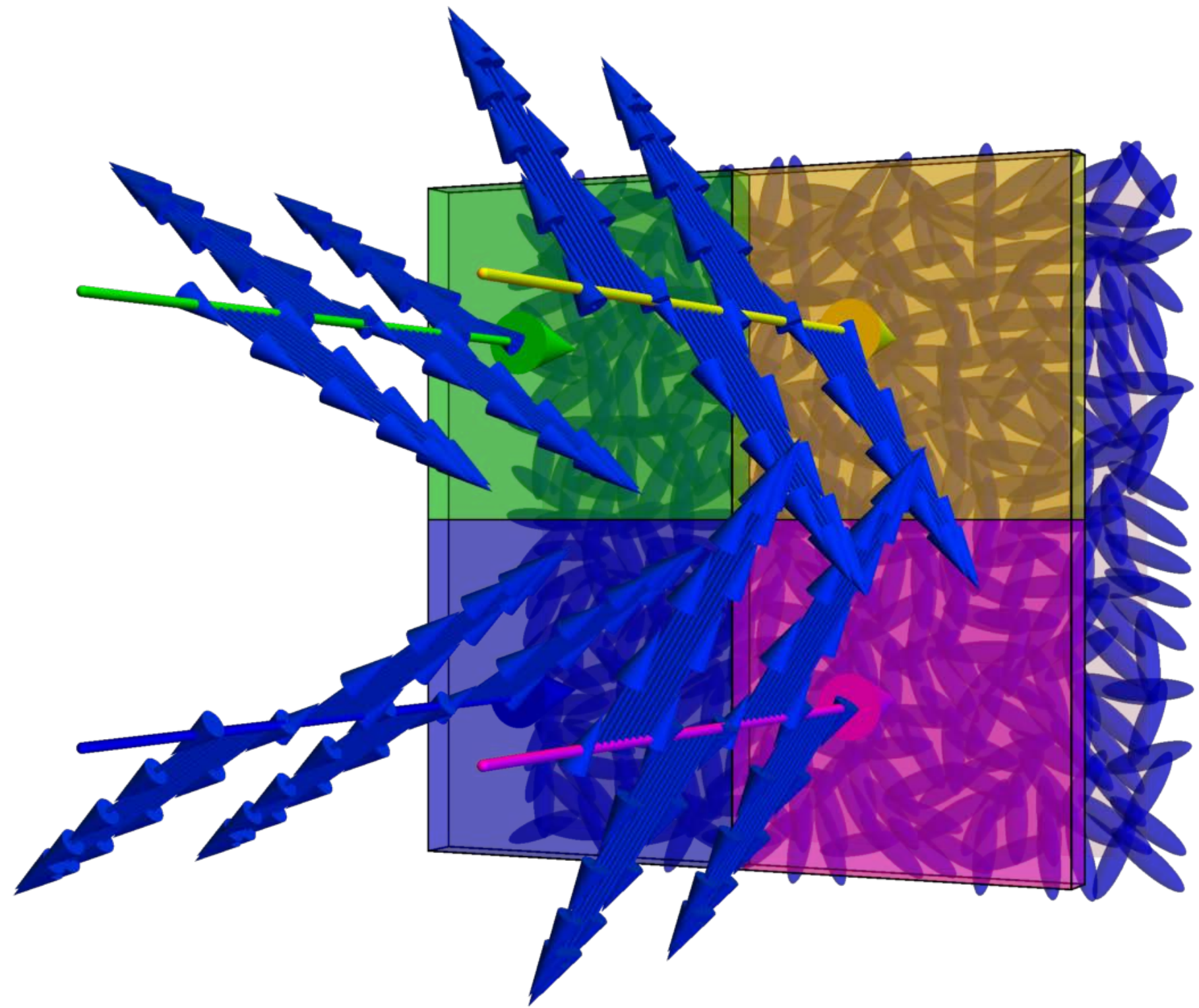
$\ell \in \mathbb{Z}$



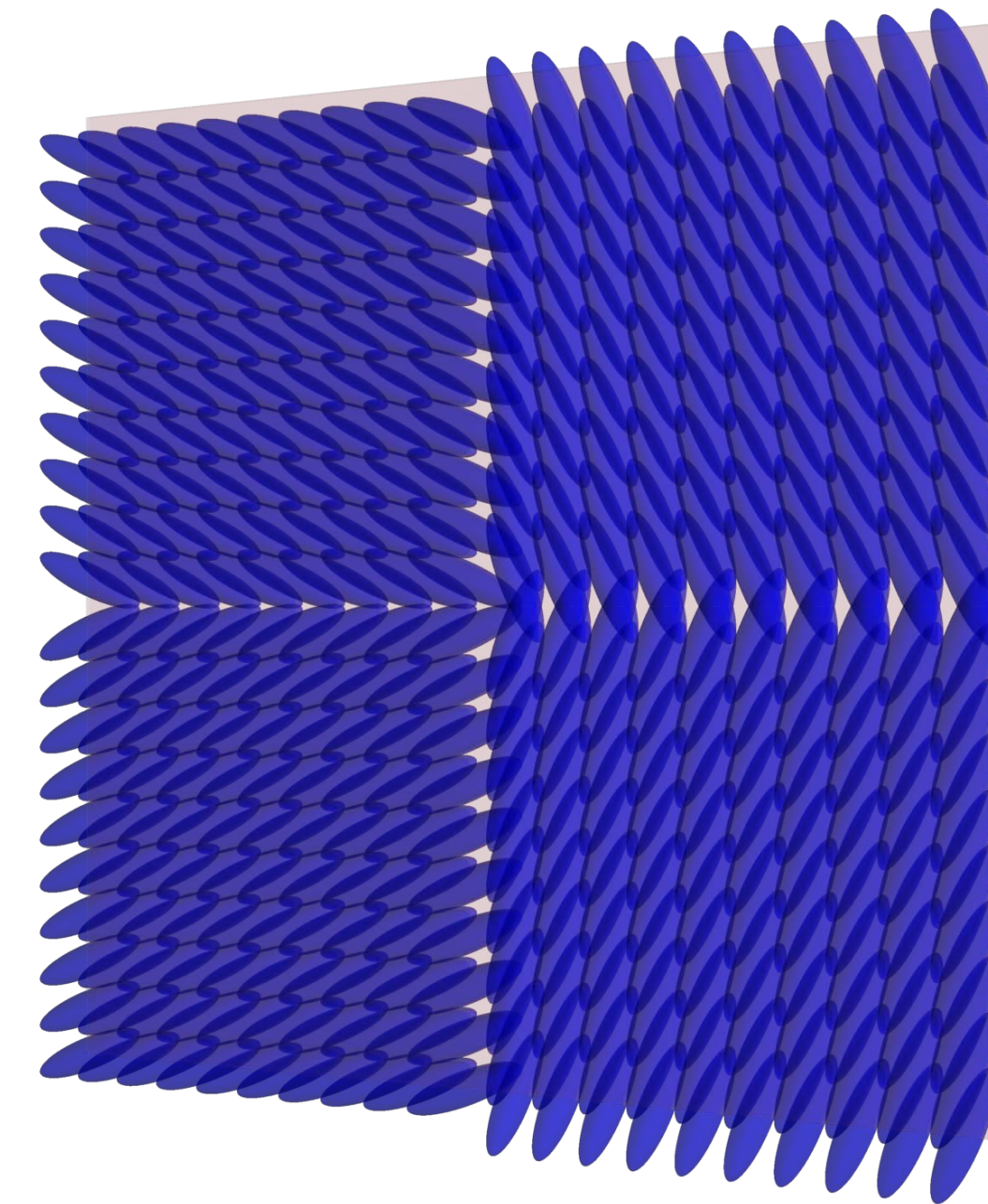
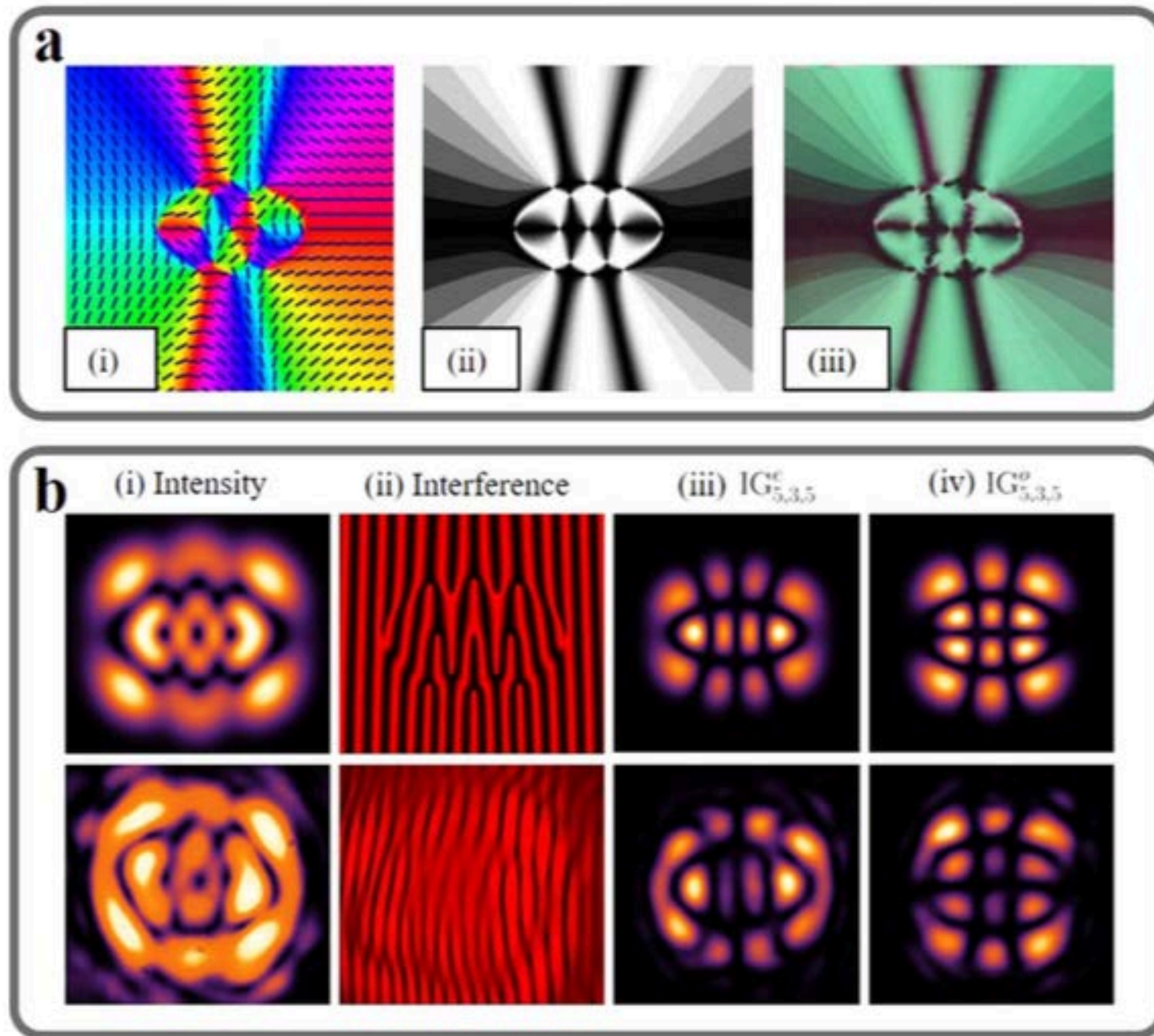
E. K. & E Santamato, *Optics Letters* **37**, 2484 (2012).

E. K., et al., *Phys. Rev. A* **89**, 063813 (2014).

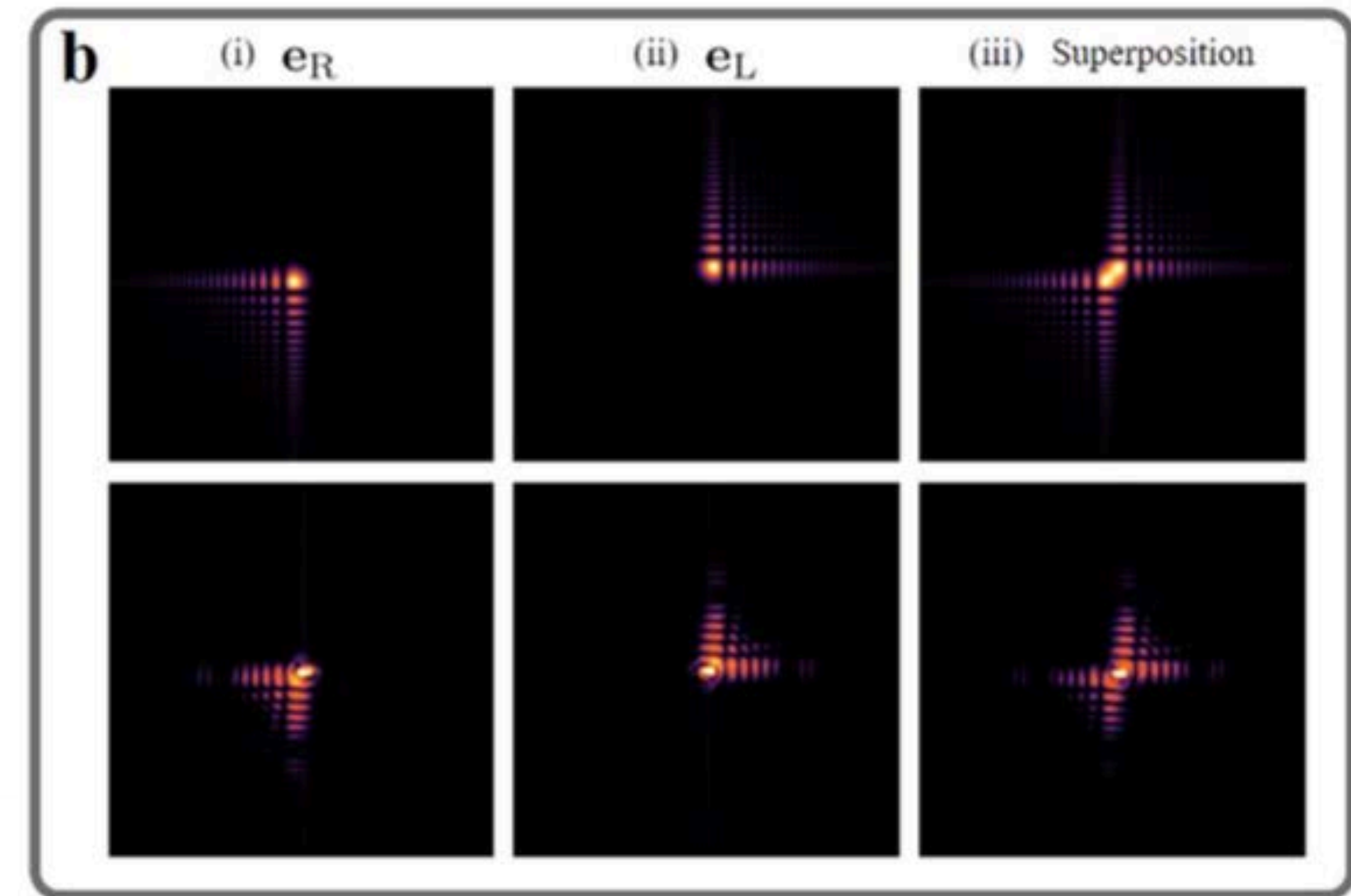
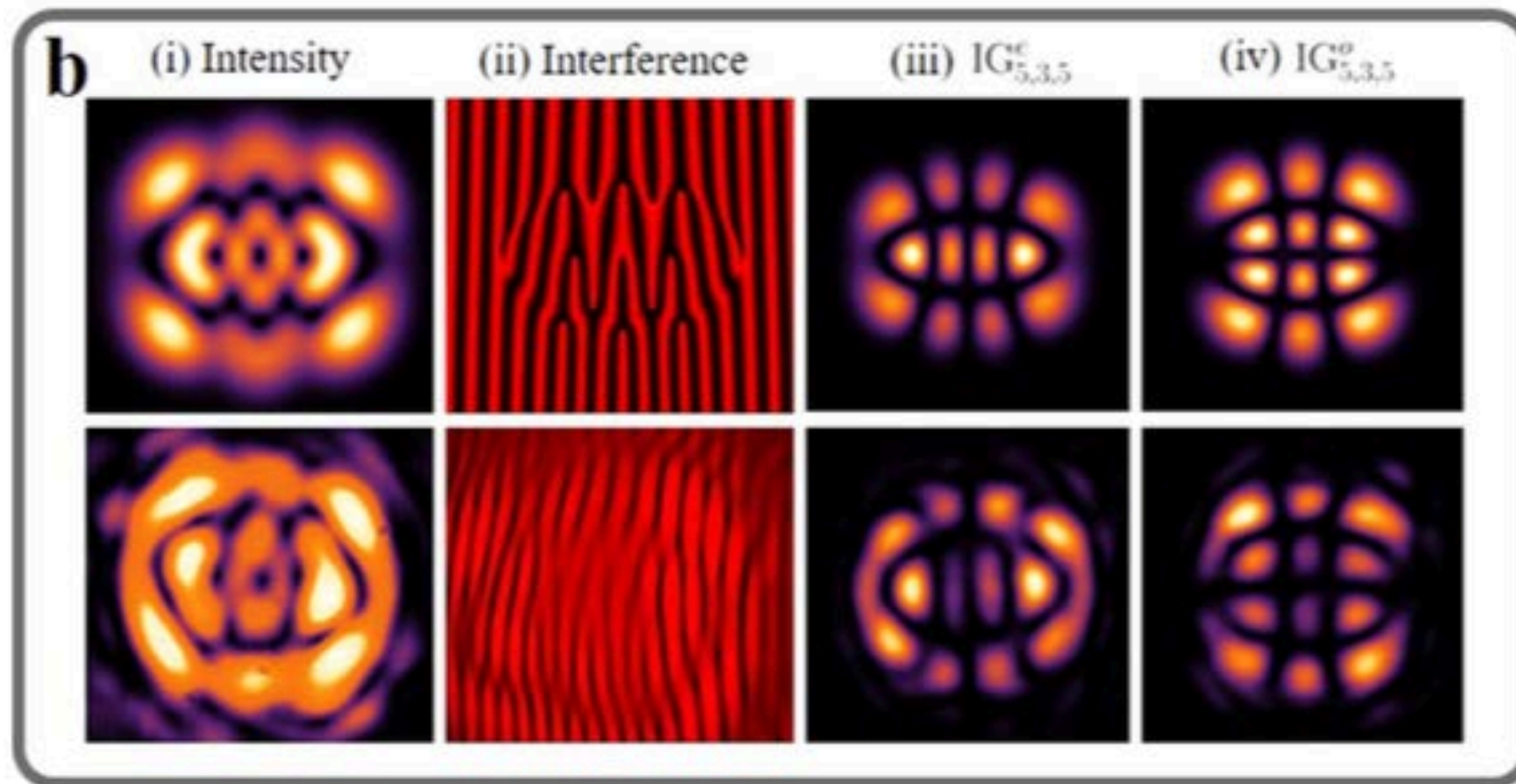
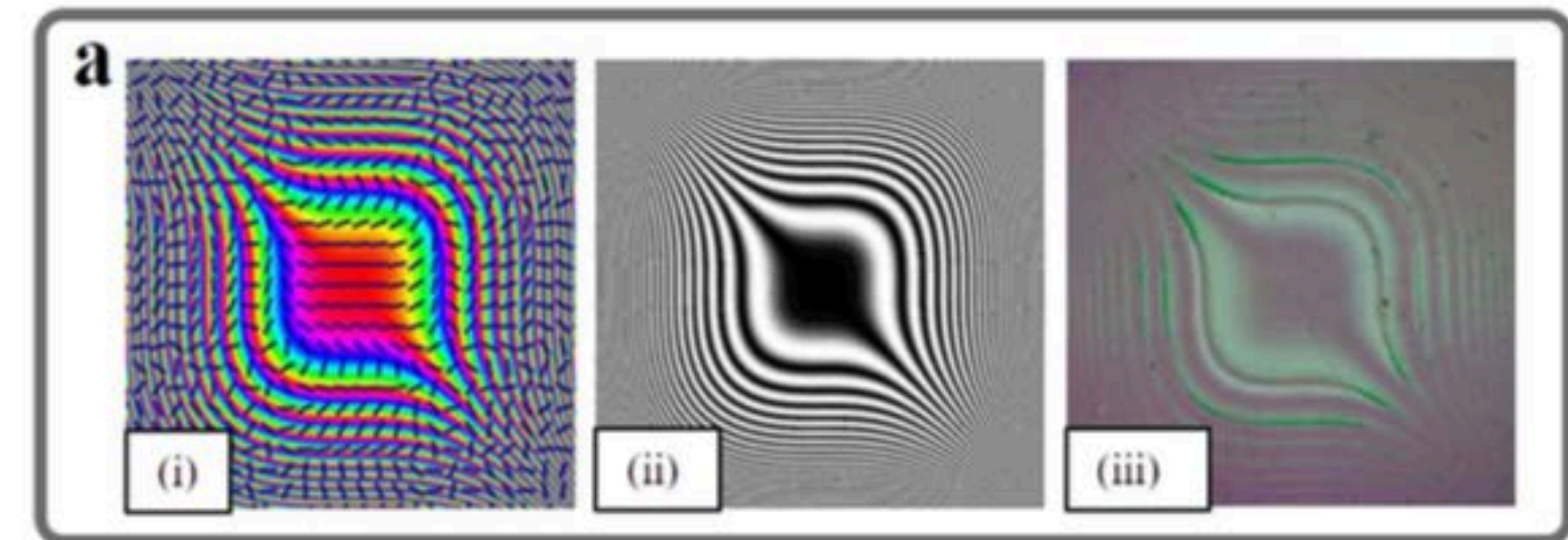
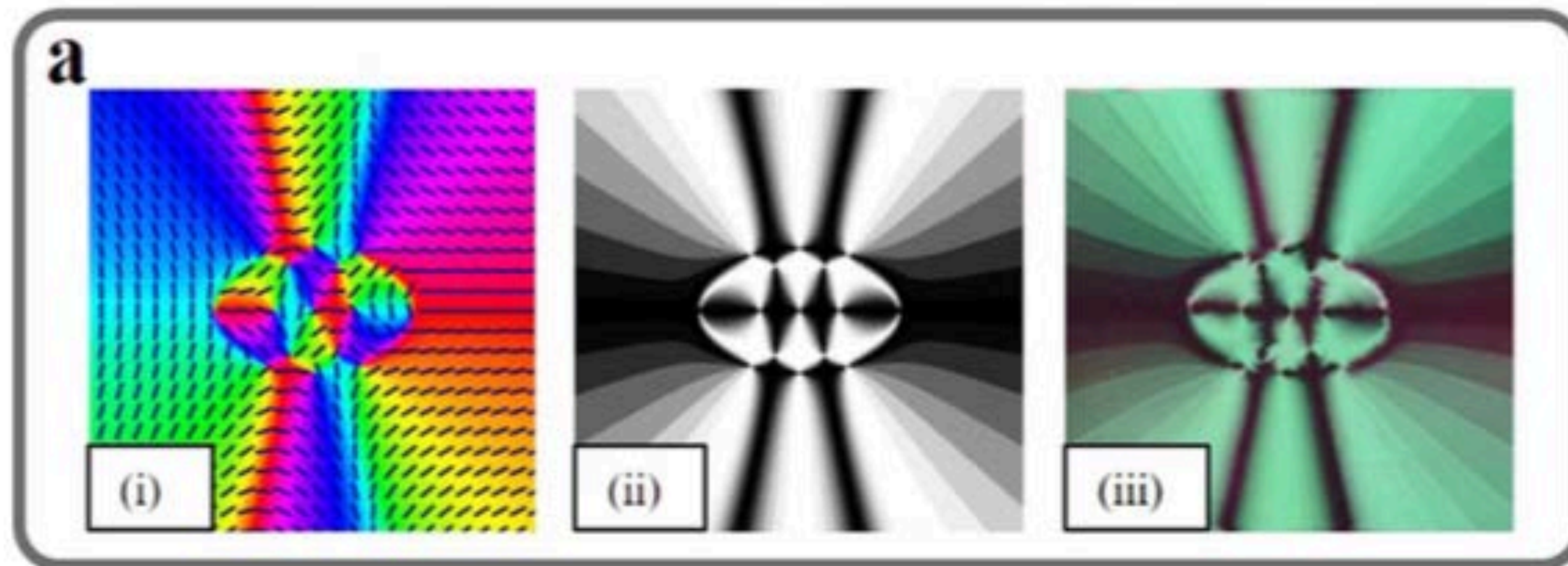
Liquid Crystal Facility



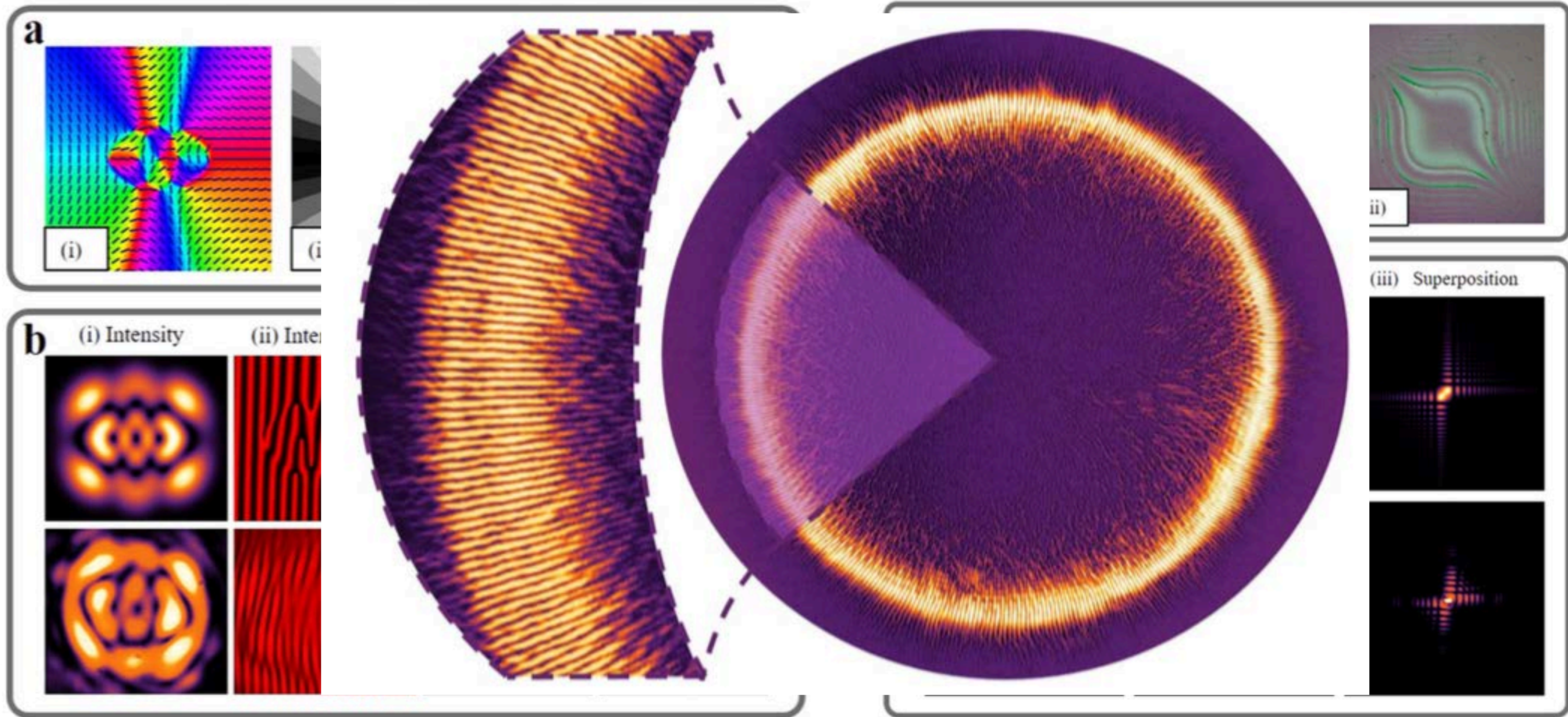
Liquid Crystal Facility



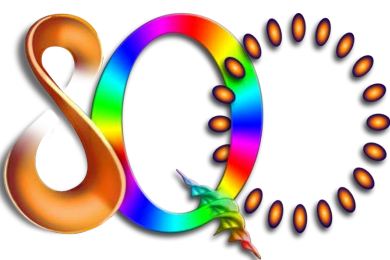
Liquid Crystal Facility



Liquid Crystal Facility



Application in Quantum Information

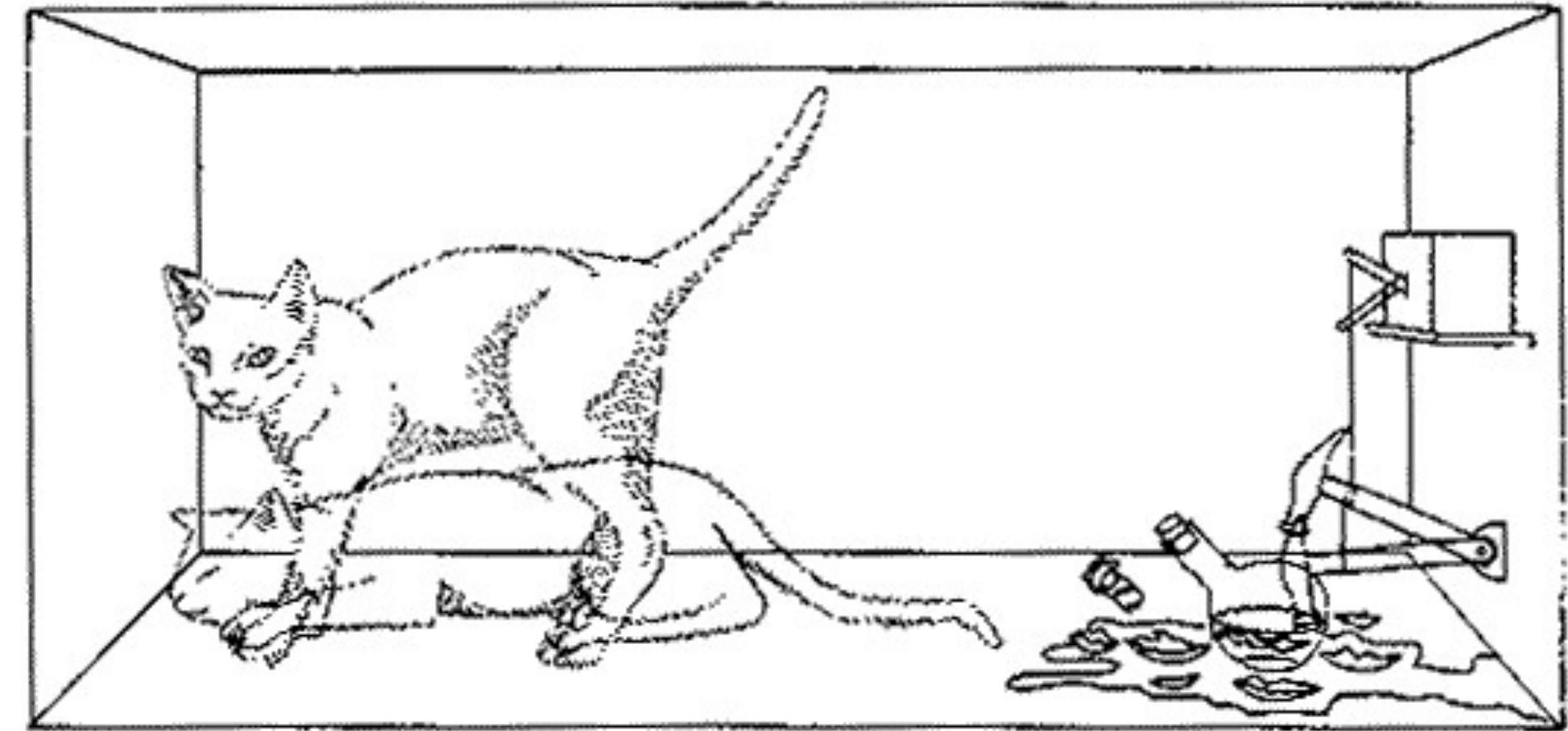


Application in Quantum Cryptography



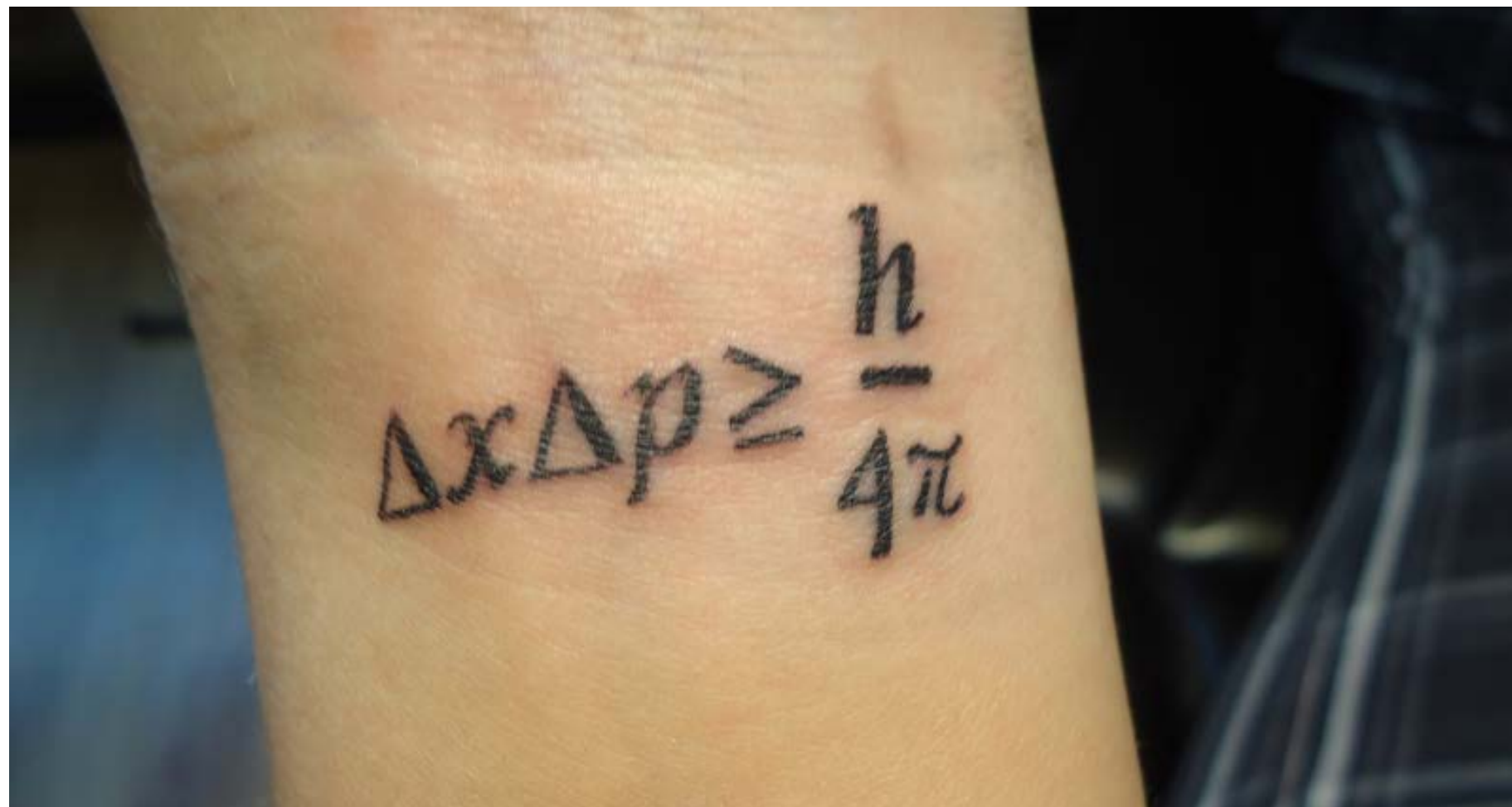
Application in Quantum Cryptography

THERE IS NO DEFINITE REALITY

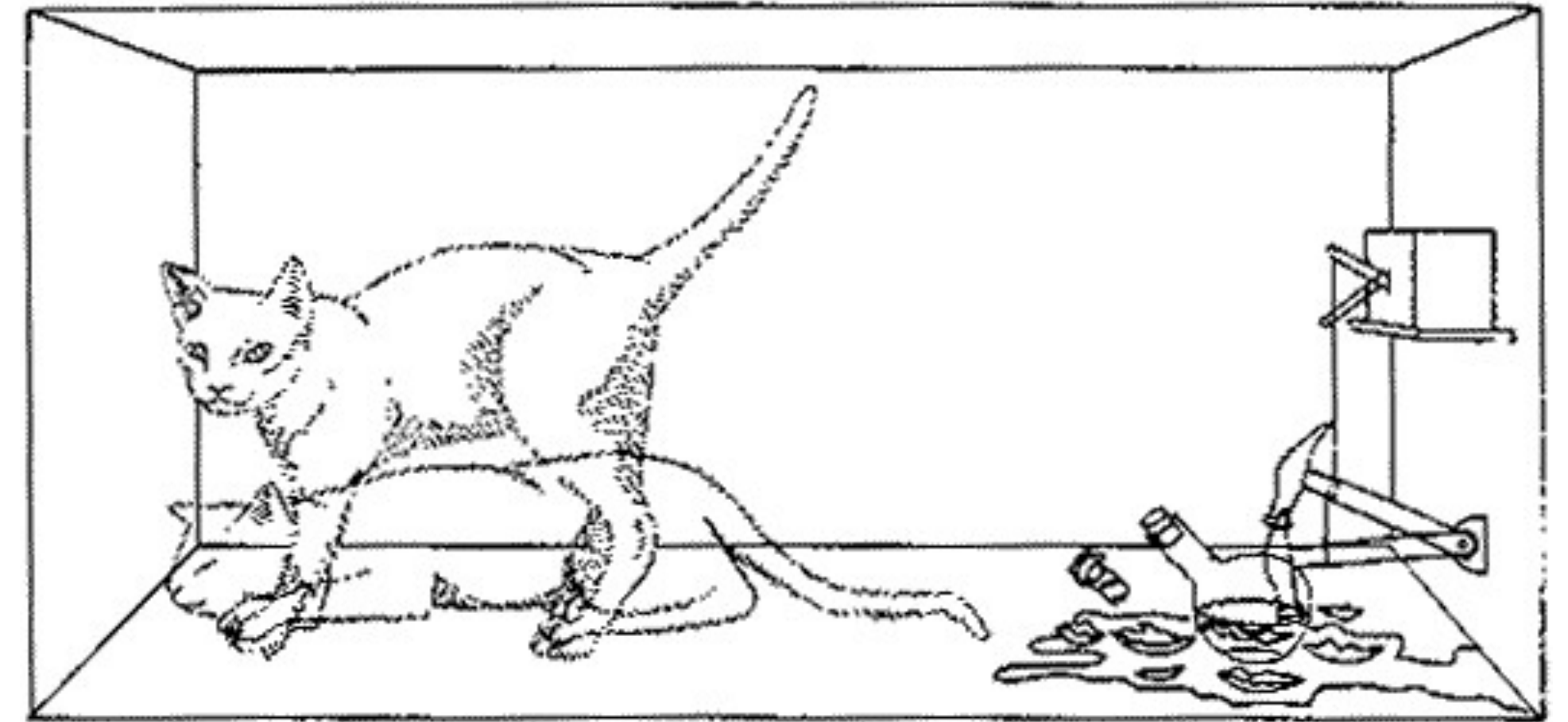


Application in Quantum Cryptography

CONJUGATE QUANTITIES CANNOT
BE MEASURED SIMULTANEOUSLY

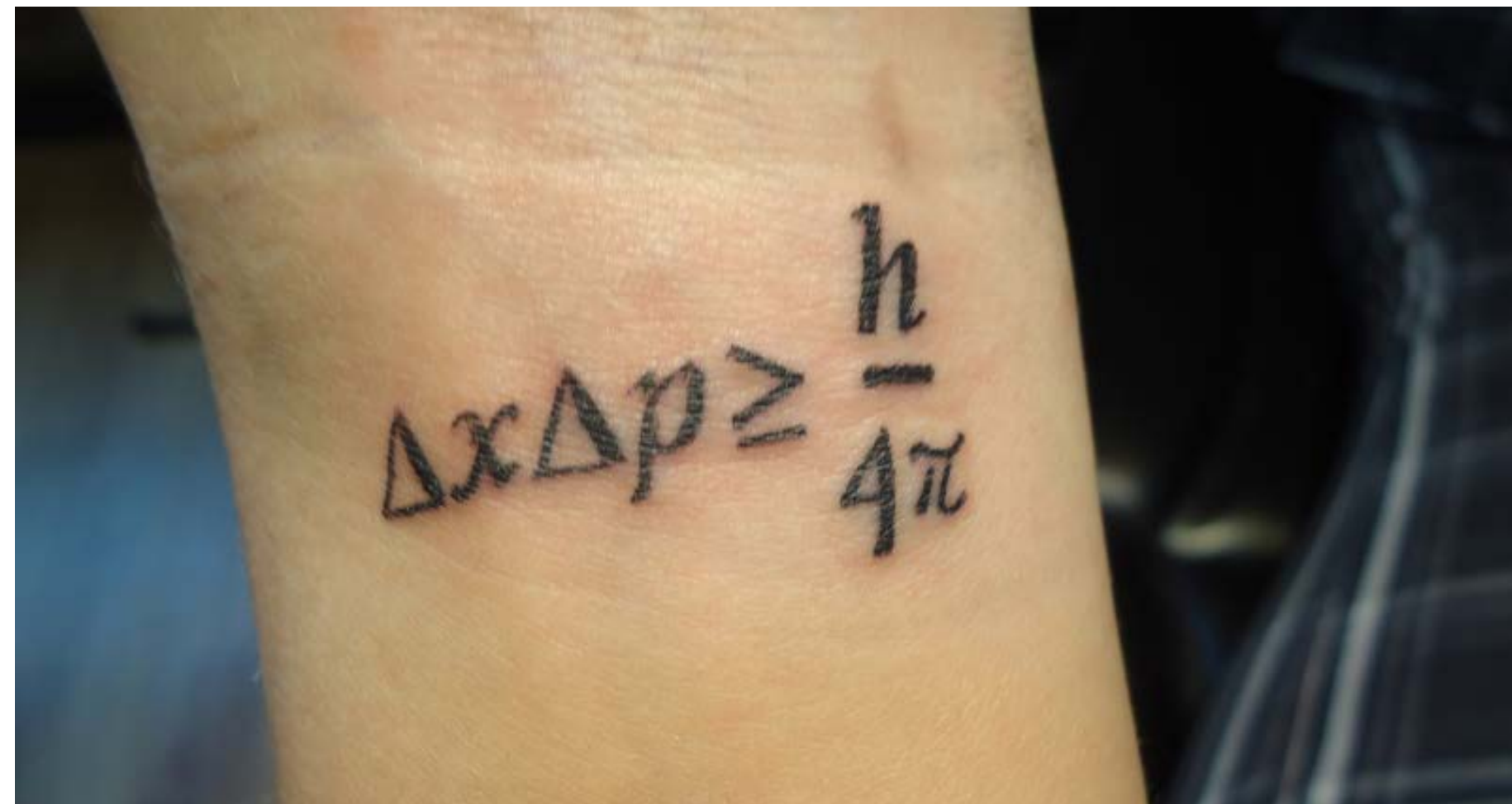


THERE IS NO DEFINITE REALITY

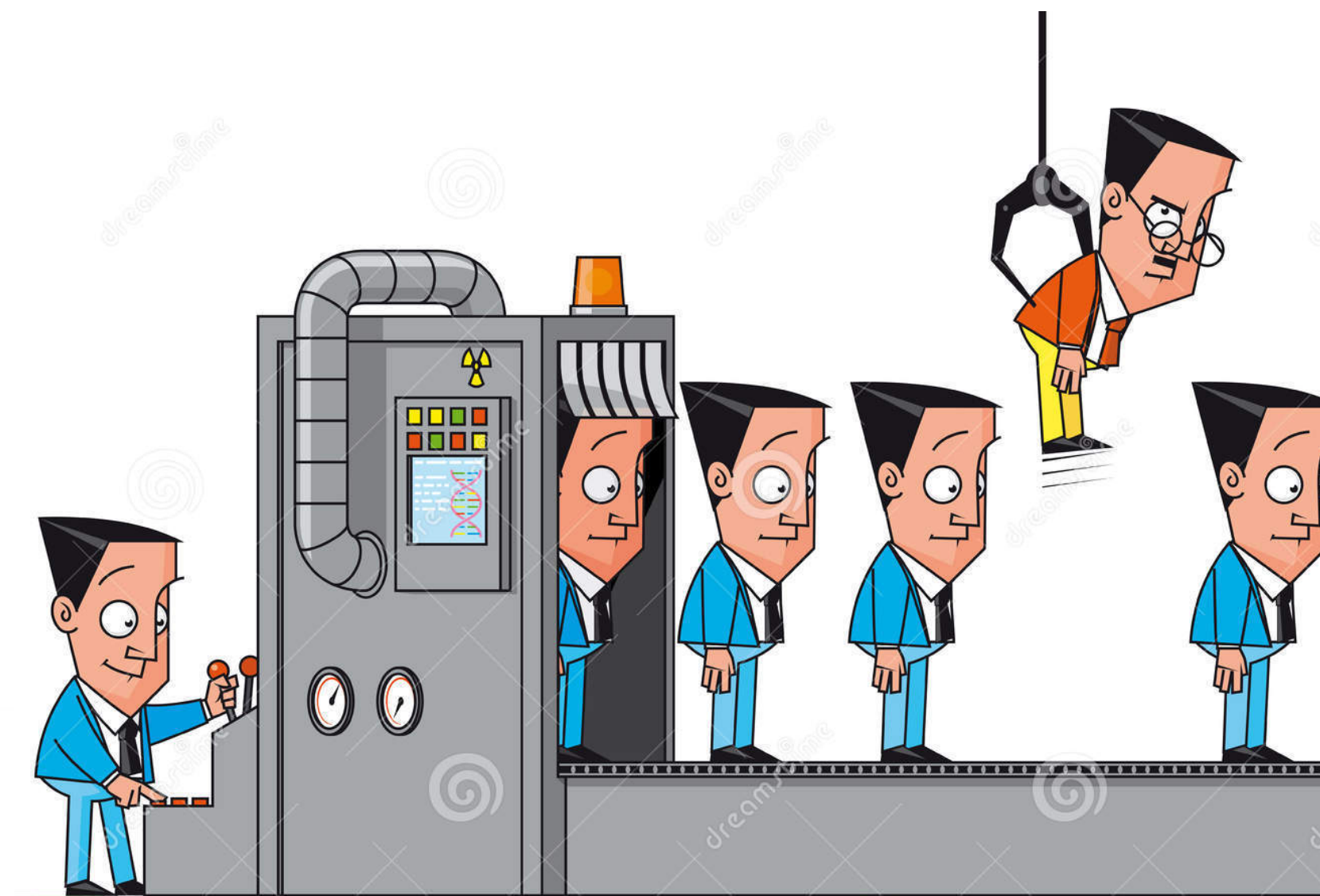
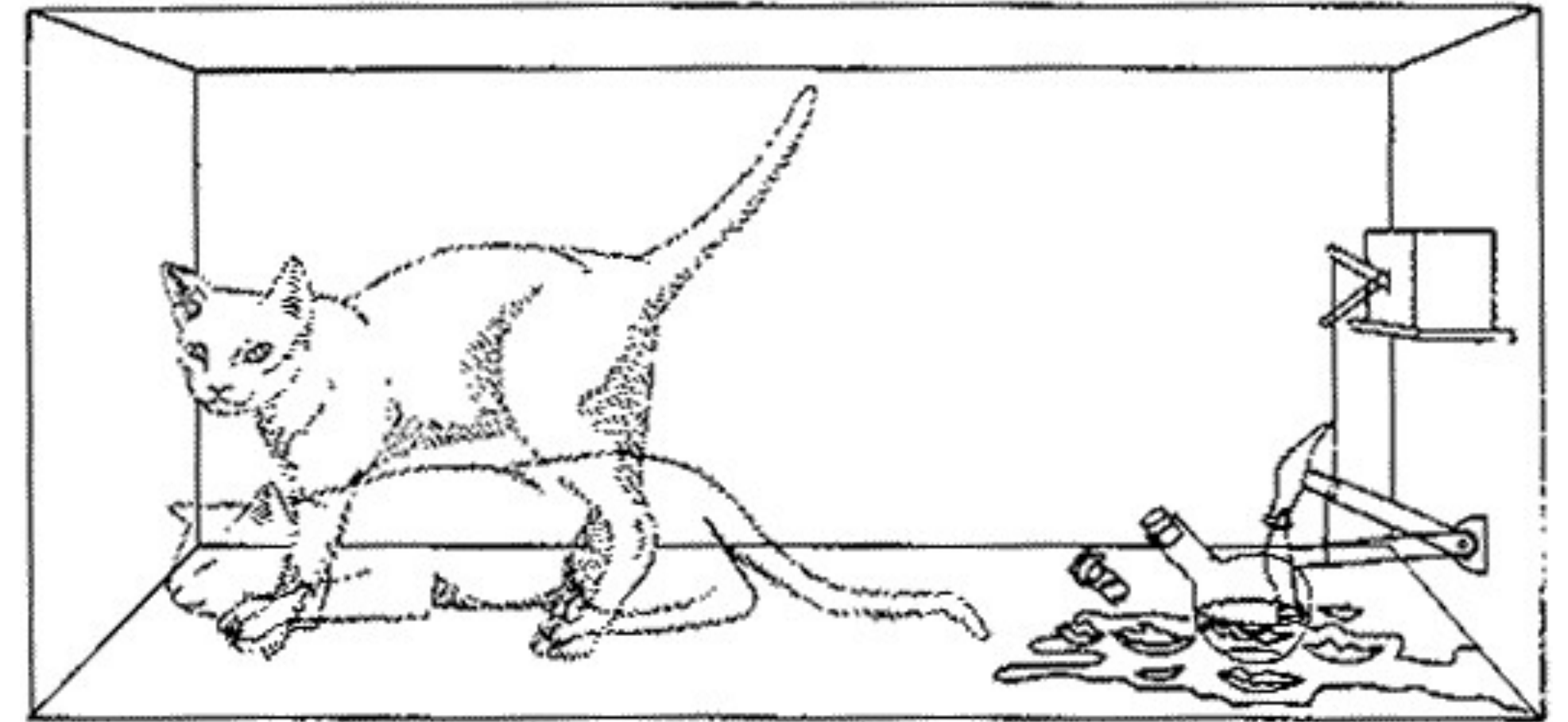


Application in Quantum Cryptography

CONJUGATE QUANTITIES CANNOT BE MEASURED SIMULTANEOUSLY



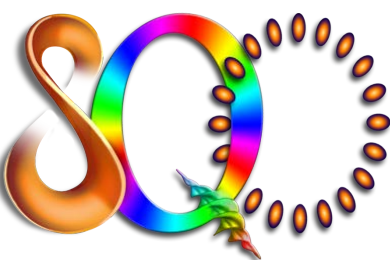
THERE IS NO DEFINITE REALITY



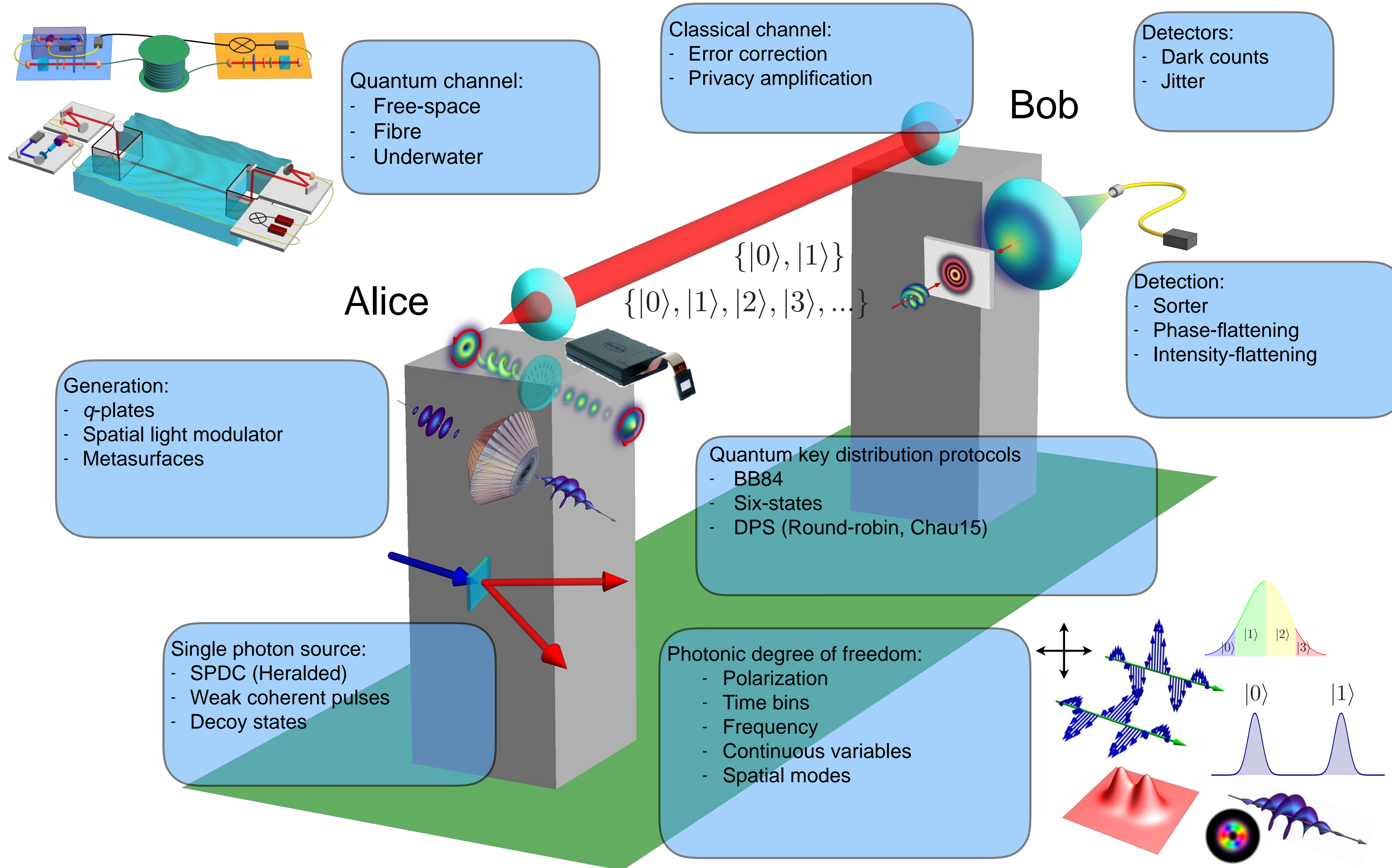
QUANTUM INFORMATION CANNOT BE CLONED WITHOUT INTRODUCING ERRORS

Download from Dreamstime.com

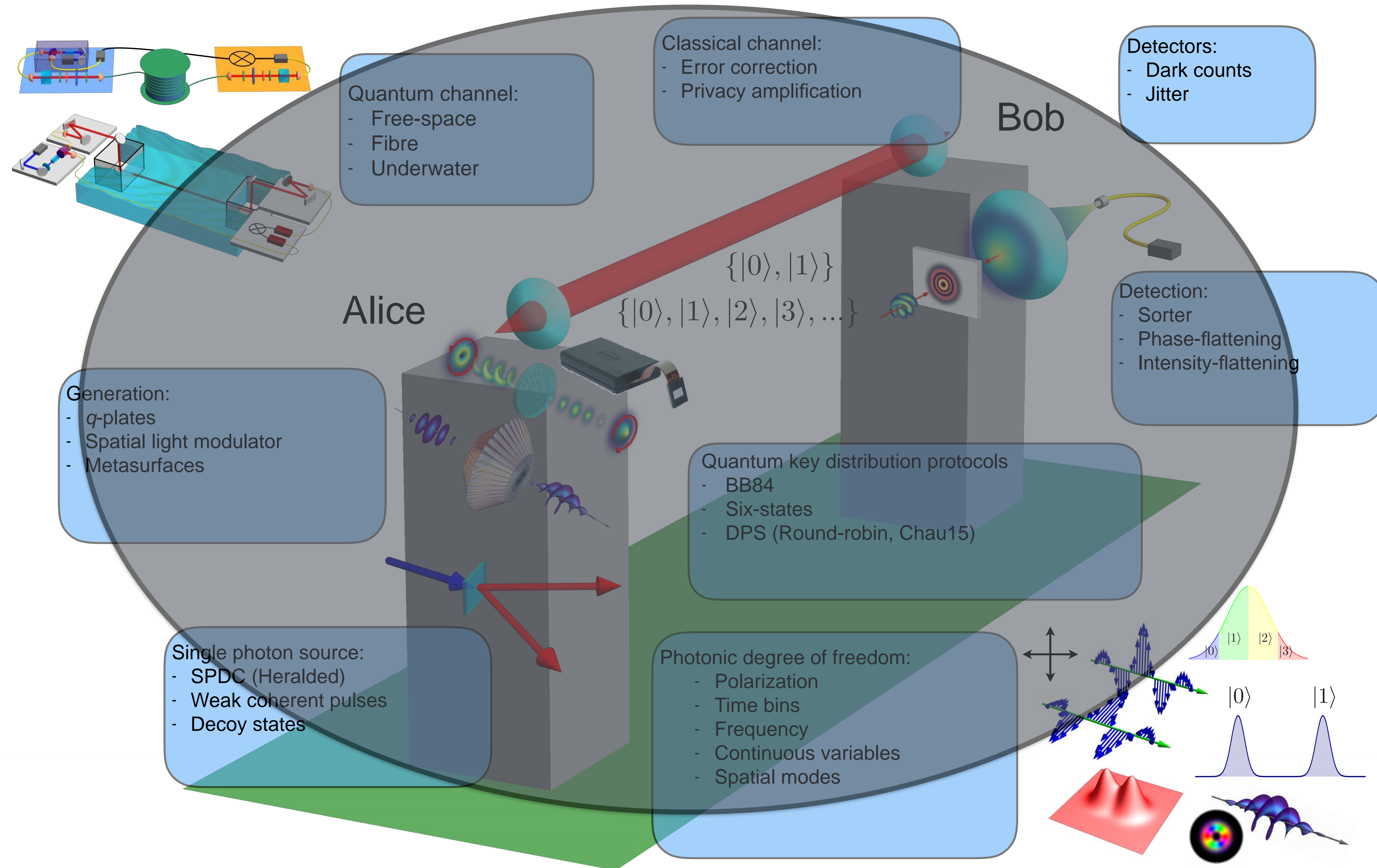
26808938 Carbouval | Dreamstime.com



QKD



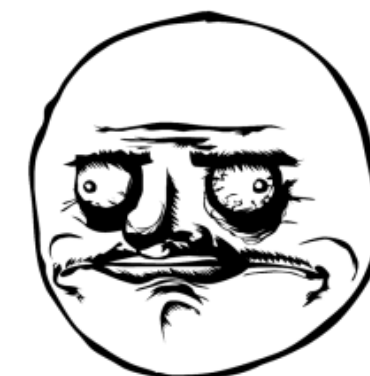
QKD



Cryptography



Alice



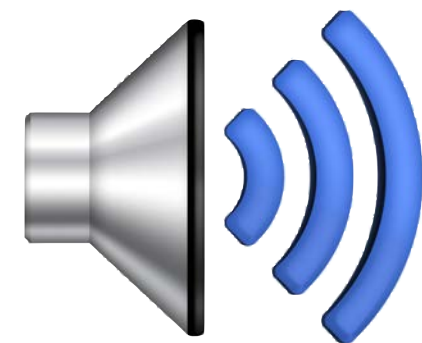
Bob



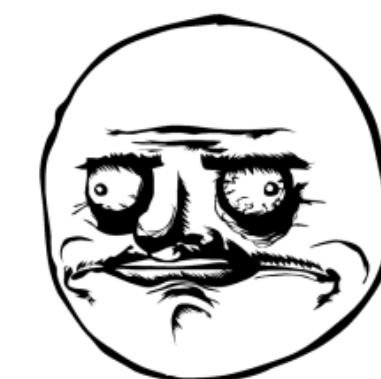
Cryptography



Alice



PUBLIC CHANNEL



Bob



Cryptography



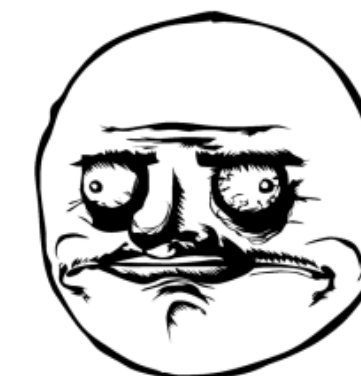
Alice



PUBLIC CHANNEL



Eve



Bob



Cryptography



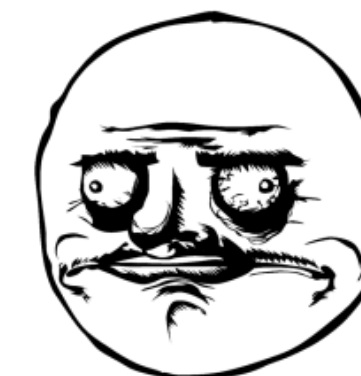
Alice



PUBLIC CHANNEL

**wsqi jsv xli kpsvmiw sj xlmw asvph; erh wsqi
wmkl jsv xli tvstlix'w tevehmwi xs gsqi;
el, xeoï xli gewl, erh pix xli gvihmx ks,
rsv liih xli vyqfpi sj e hmw xerx hvyq!**

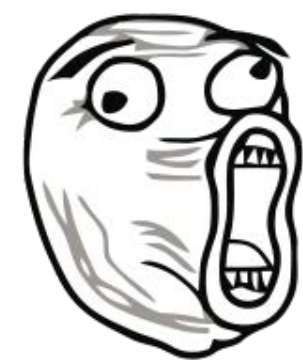
Eve



Bob



Cryptography



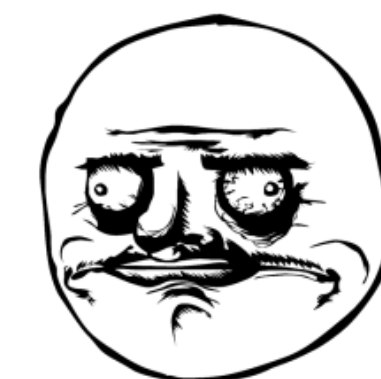
Alice



PUBLIC CHANNEL

wsqi jsv xli kpsvmiw sj xlmw asvph; erh wsqi
wmkl jsv xli tvstlix'w tevehmwi xs gsqi;
el, xeoï xli gewl, erh pix xli gvihmx ks,
rsv liih xli vyqfpi sj e hmw xerx hvyq!

Eve



Bob



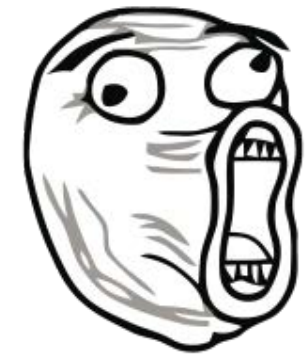
SECURE CHANNEL

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d

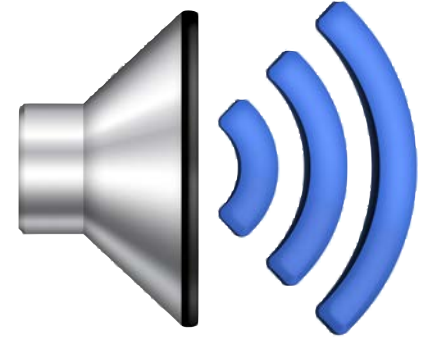
Key



Cryptography



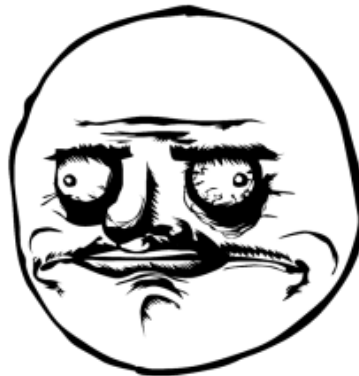
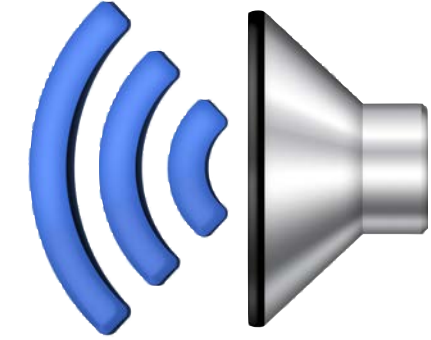
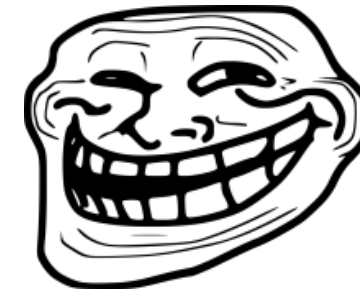
Alice



PUBLIC CHANNEL

wsqi jsv xli kpsvmiw sj xlmw asvph; erh wsqi
wmkl jsv xli tvstlix'w tevehmwi xs gsqi;
el, xeoï xli gewl, erh pix xli gvihmx ks,
rsv liih xli vyqfpi sj e hmw xerx hvyq!

Eve



Bob



SECURE CHANNEL

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d

Key

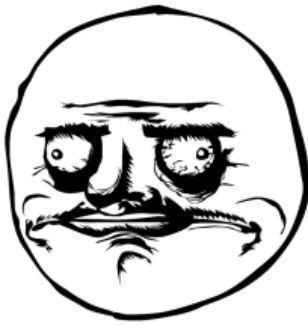


some for the glories of this world; and
some sigh for the prophet's paradise to come;
ah, take the cash, and let the credit go,
nor heed the rumble of a distant drum!



Quantum Cryptography

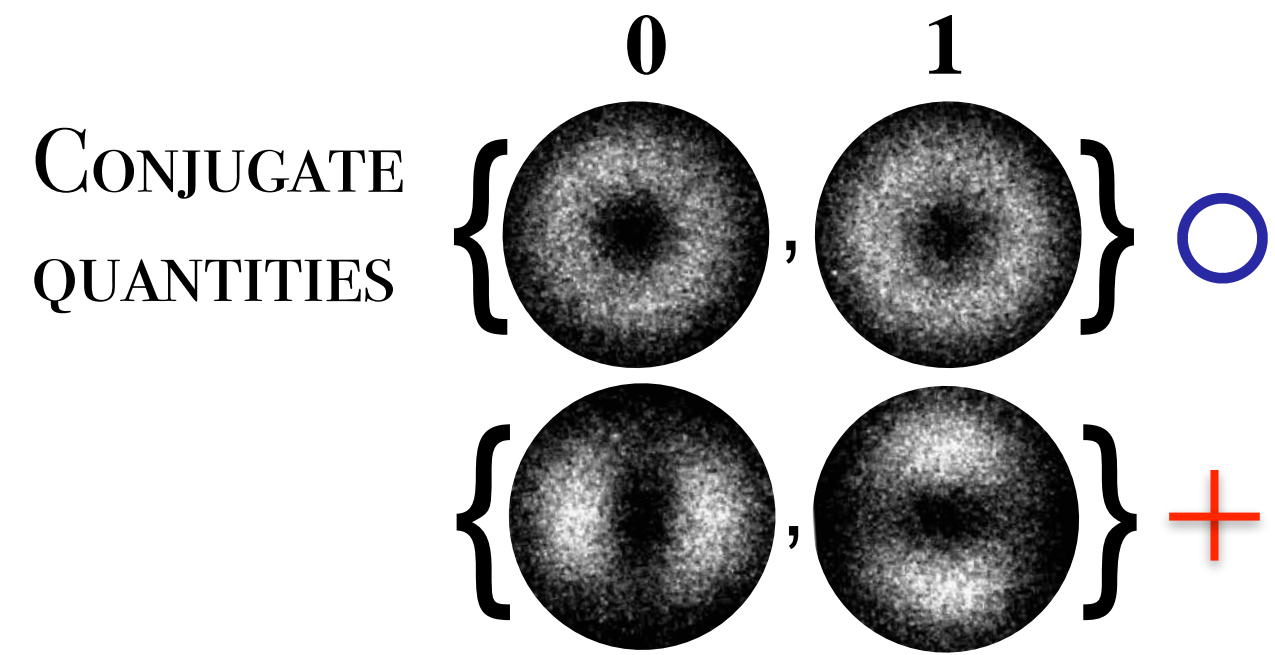
Eve



Bob



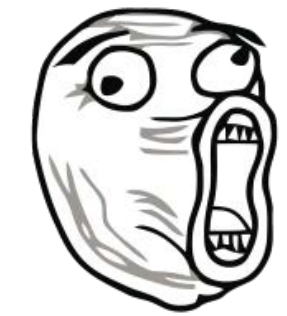
Alice



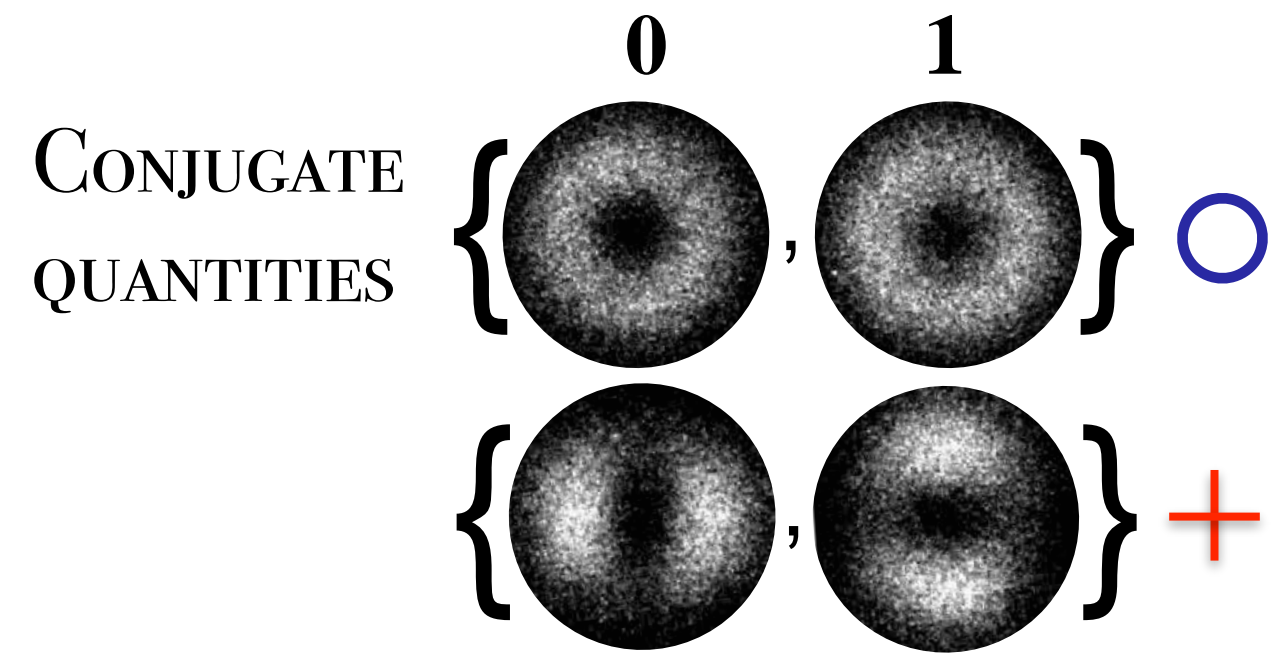
$$\Delta_{+} \cdot \Delta_{\circ} \geq \frac{\hbar}{2}$$



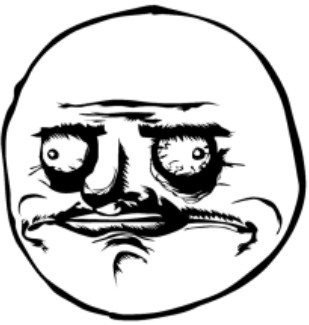
Quantum Cryptography



Alice



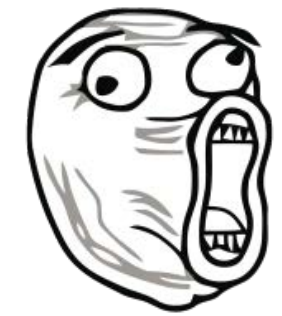
$$\Delta_{+} \cdot \Delta_{\circ} \geq \frac{\hbar}{2}$$



Bob



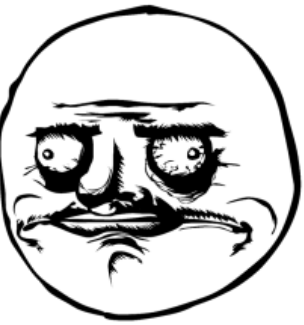
Quantum Cryptography



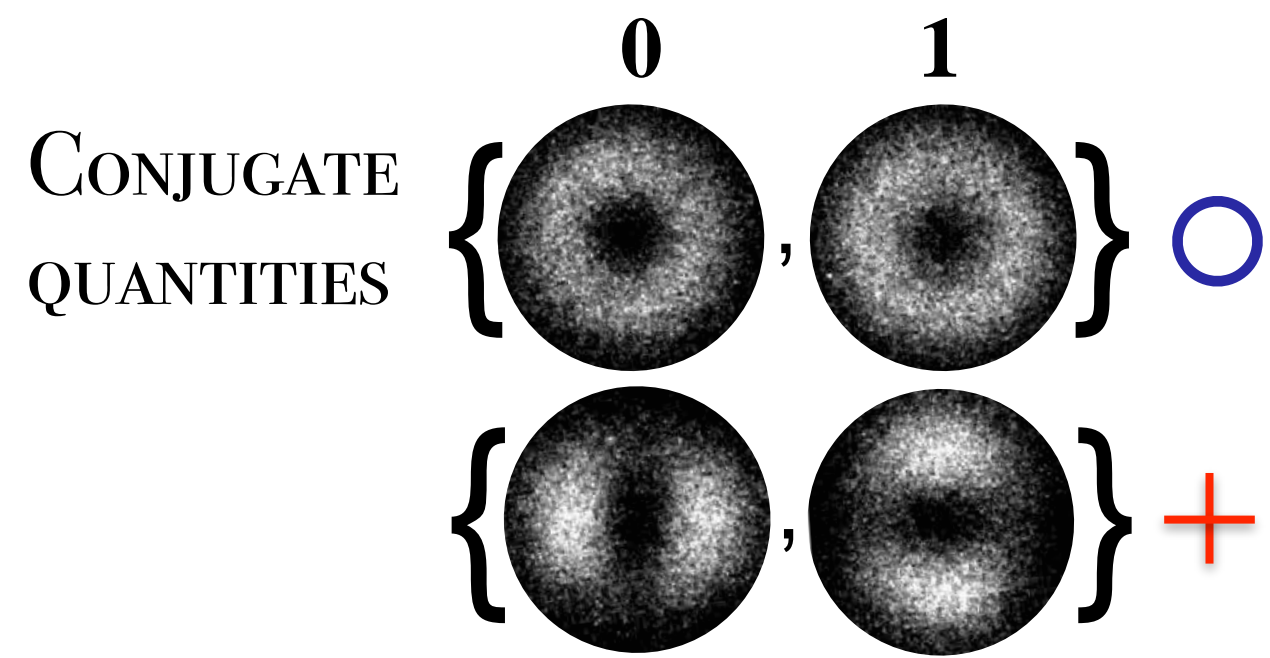
Alice



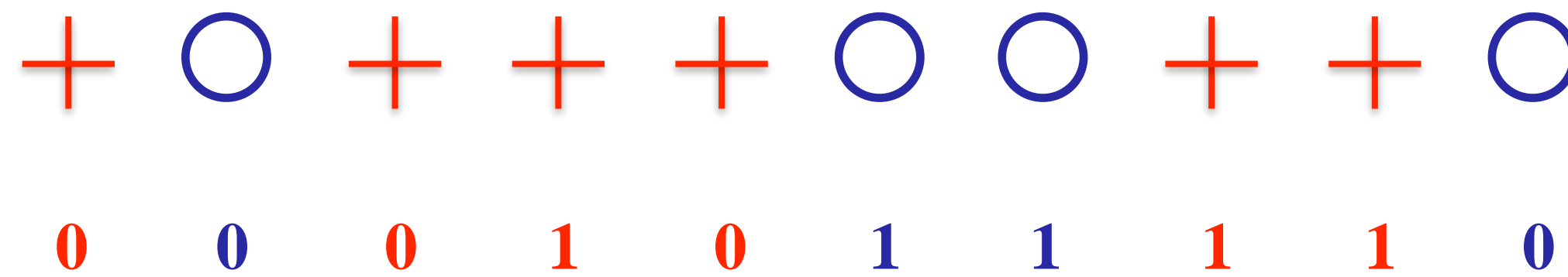
Eve



Bob



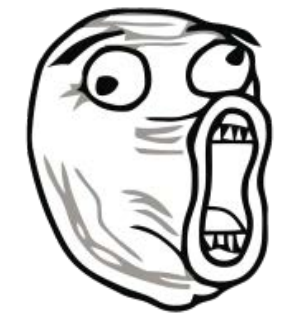
ALICE



$$\Delta_{+} \cdot \Delta_{\circ} \geq \frac{\hbar}{2}$$



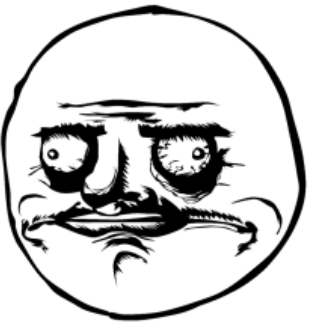
Quantum Cryptography



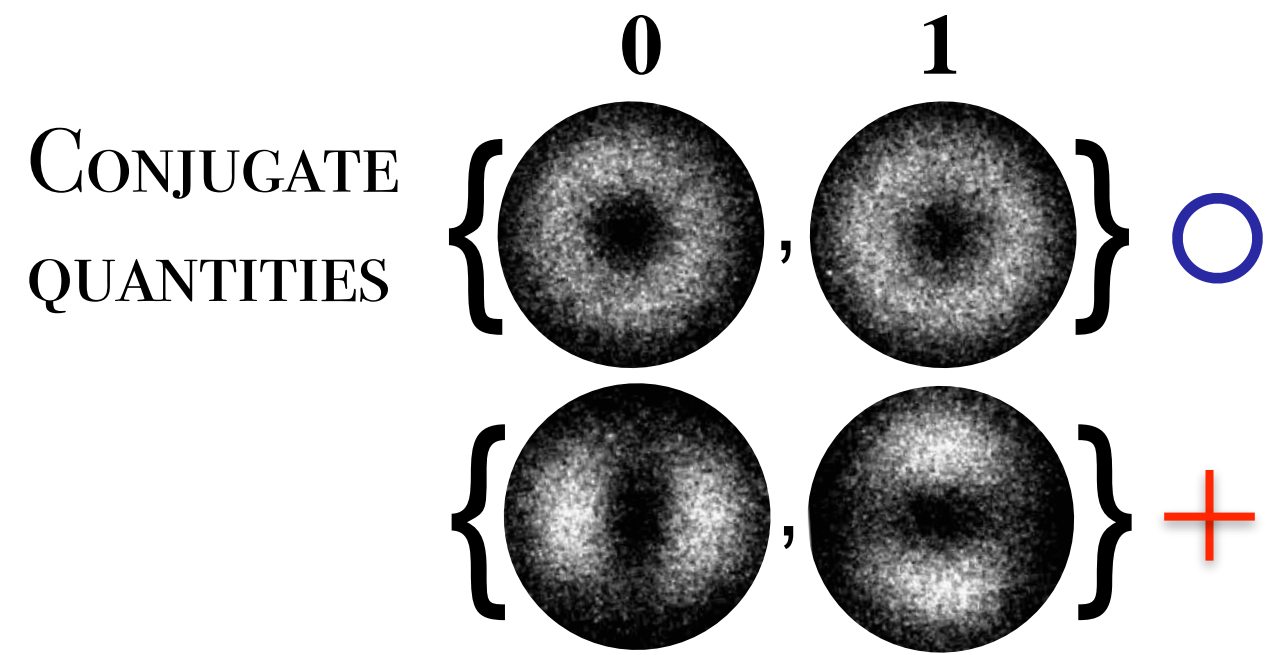
Alice



Eve

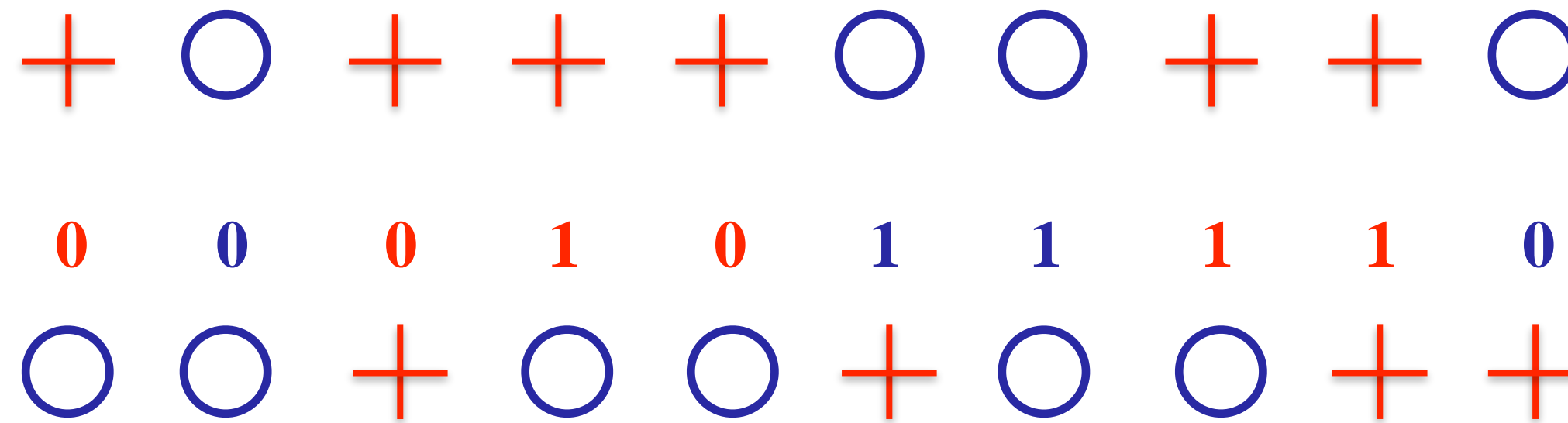


Bob



$$\Delta_{+} \cdot \Delta_{\circ} \geq \frac{\hbar}{2}$$

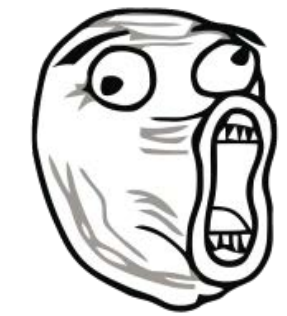
ALICE



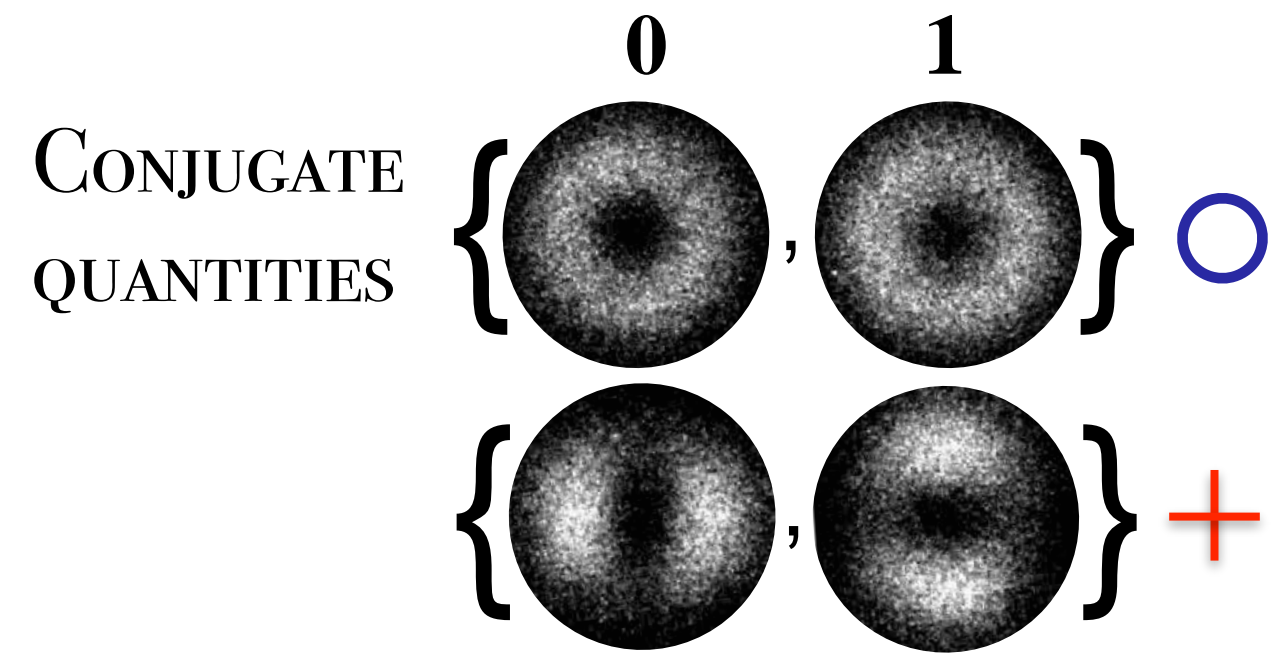
BOB



Quantum Cryptography



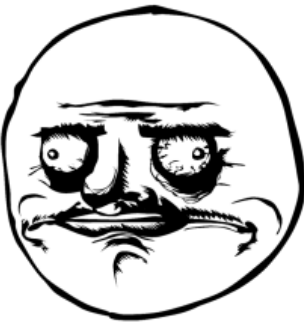
Alice



$$\Delta_{+} \cdot \Delta_{\circ} \geq \frac{\hbar}{2}$$

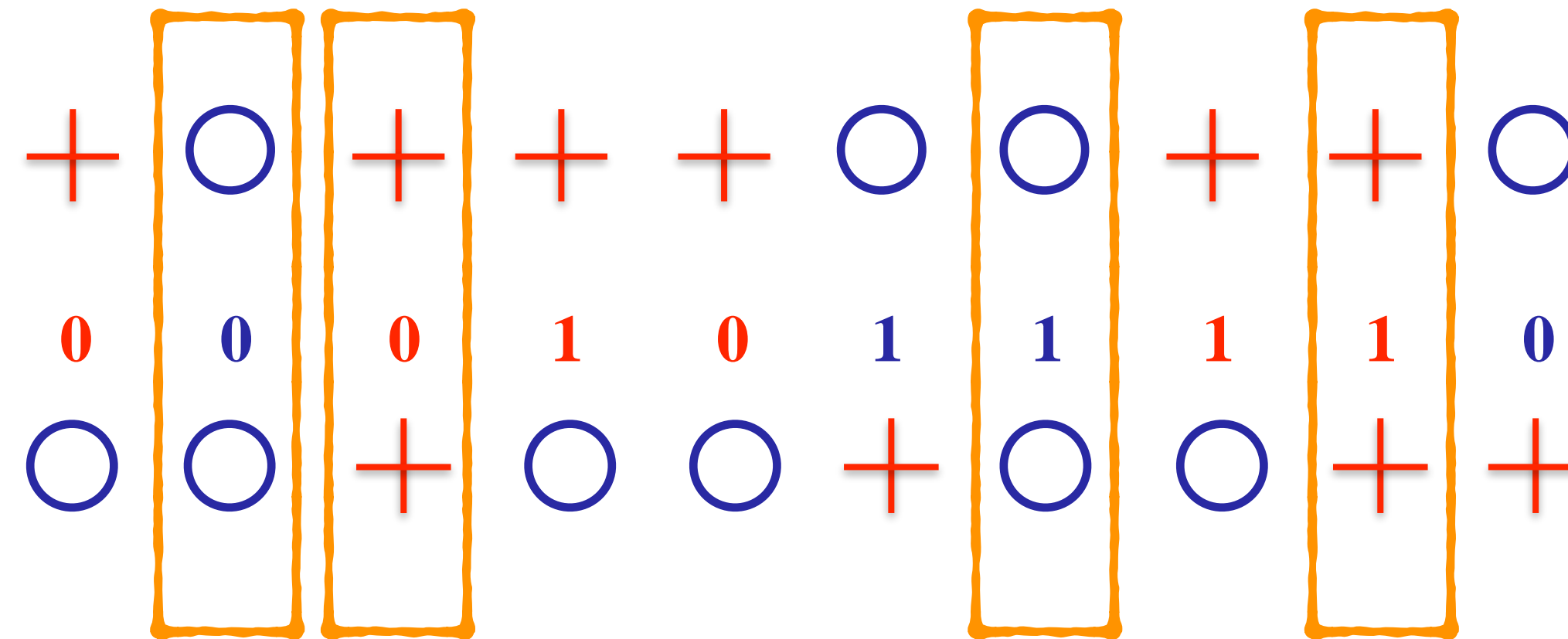


Eve



Bob

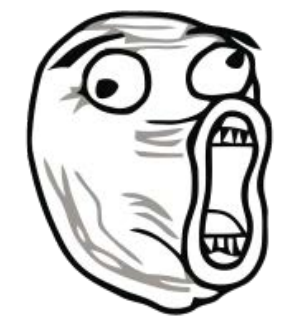
ALICE



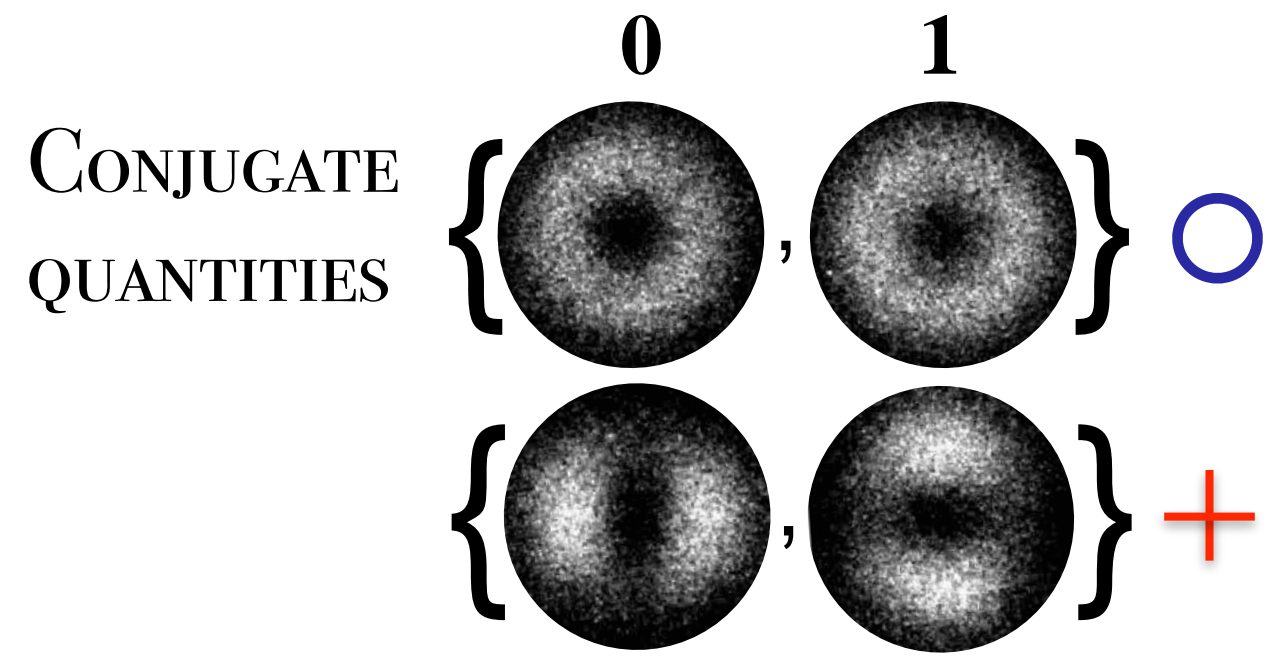
BOB



Quantum Cryptography



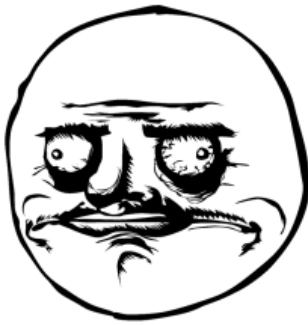
Alice



$$\Delta_{+} \cdot \Delta_{\circ} \geq \frac{\hbar}{2}$$

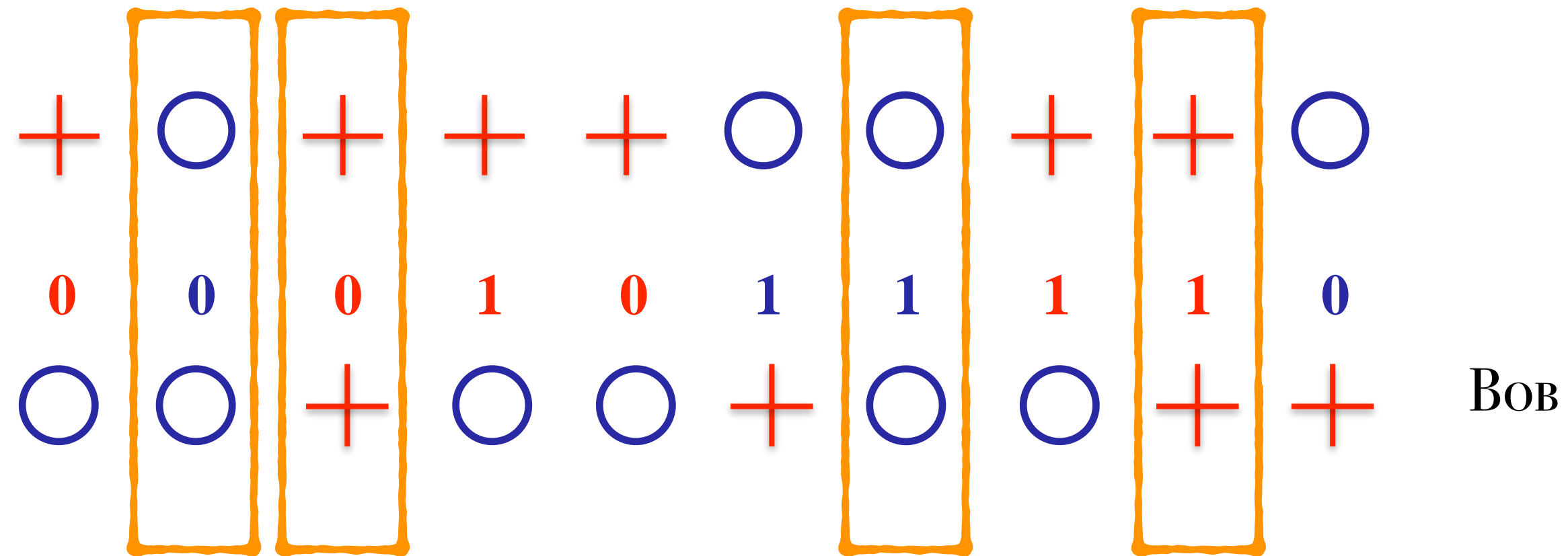


Eve



Bob

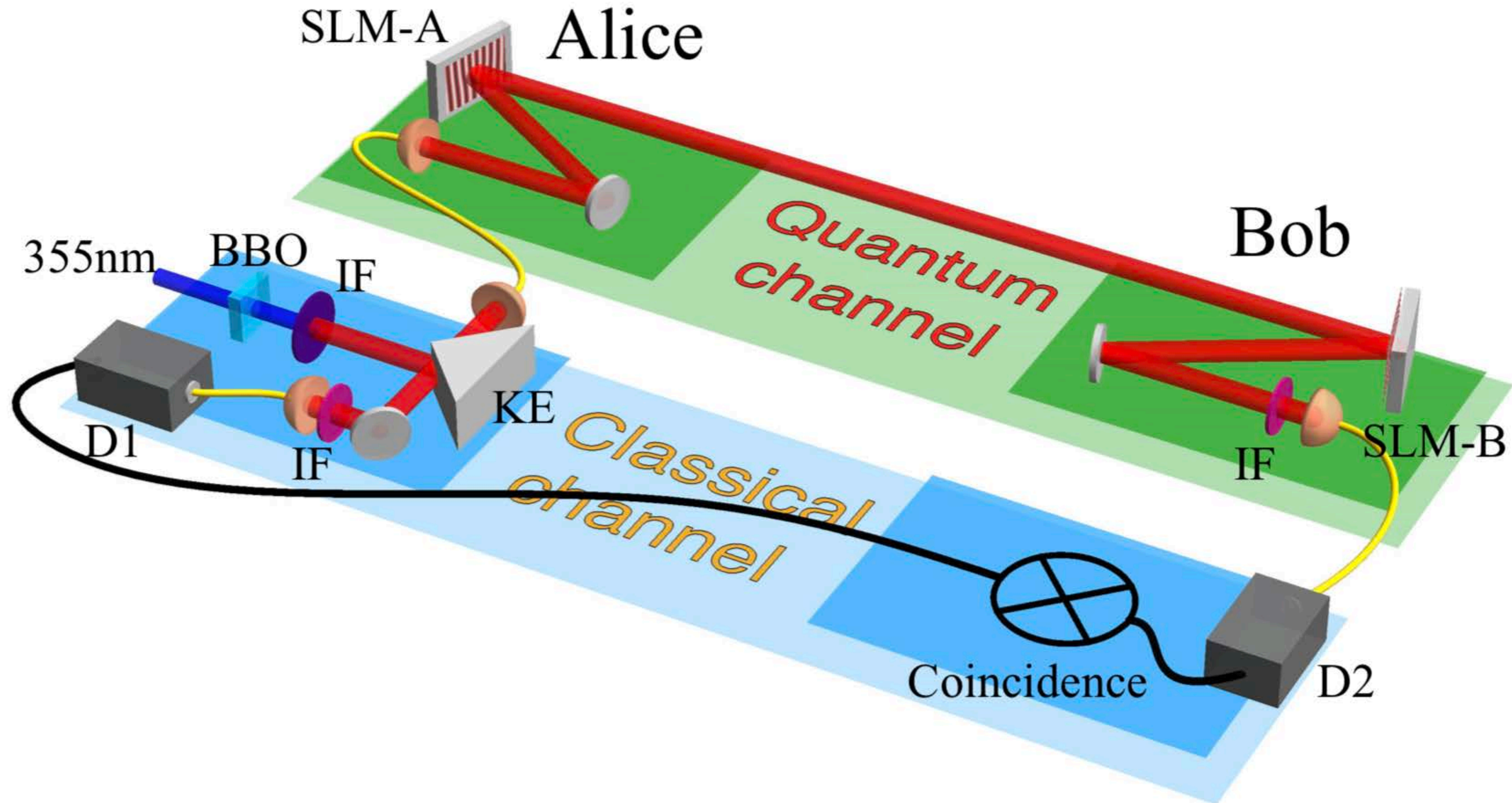
ALICE



0 0 1 1 Secret Key



Quantum Cryptography: Setup



High-Dimensional "alphabet"

Classically:

$$\begin{aligned}
 &00101011001100110101001101000110 \\
 &= \\
 &223030311031012 \\
 &= \\
 &5314651506 \\
 &= \\
 &724783942
 \end{aligned}$$

Quantum:

$$\begin{aligned}
 &(\alpha_1|0, 0\rangle + \beta_1|1, 1\rangle) \otimes (\alpha_2|0, 0\rangle + \beta_2|1, 1\rangle) \\
 &\neq \\
 &\alpha|0, 0\rangle + \beta|1, 1\rangle + \gamma|2, 2\rangle + \delta|3, 3\rangle
 \end{aligned}$$



High-Dimensional "alphabet"

Let us send letter **M**

Classically:

$$\begin{aligned}
 &00101011001100110101001101000110 \\
 &= \\
 &223030311031012 \\
 &= \\
 &5314651506 \\
 &= \\
 &724783942
 \end{aligned}$$

Quantum:

$$\begin{aligned}
 &(\alpha_1|0, 0\rangle + \beta_1|1, 1\rangle) \otimes (\alpha_2|0, 0\rangle + \beta_2|1, 1\rangle) \\
 &\neq \\
 &\alpha|0, 0\rangle + \beta|1, 1\rangle + \gamma|2, 2\rangle + \delta|3, 3\rangle
 \end{aligned}$$



High-Dimensional "alphabet"

Let us send letter **M**

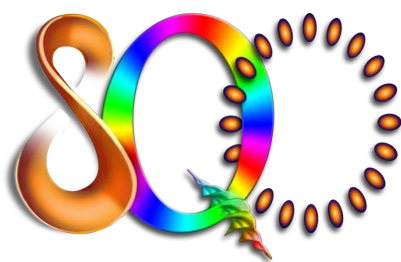
Letter **M** in the binary code is **01001101**

Classically:

$$\begin{aligned}
 &00101011001100110101001101000110 \\
 &= \\
 &223030311031012 \\
 &= \\
 &5314651506 \\
 &= \\
 &724783942
 \end{aligned}$$

Quantum:

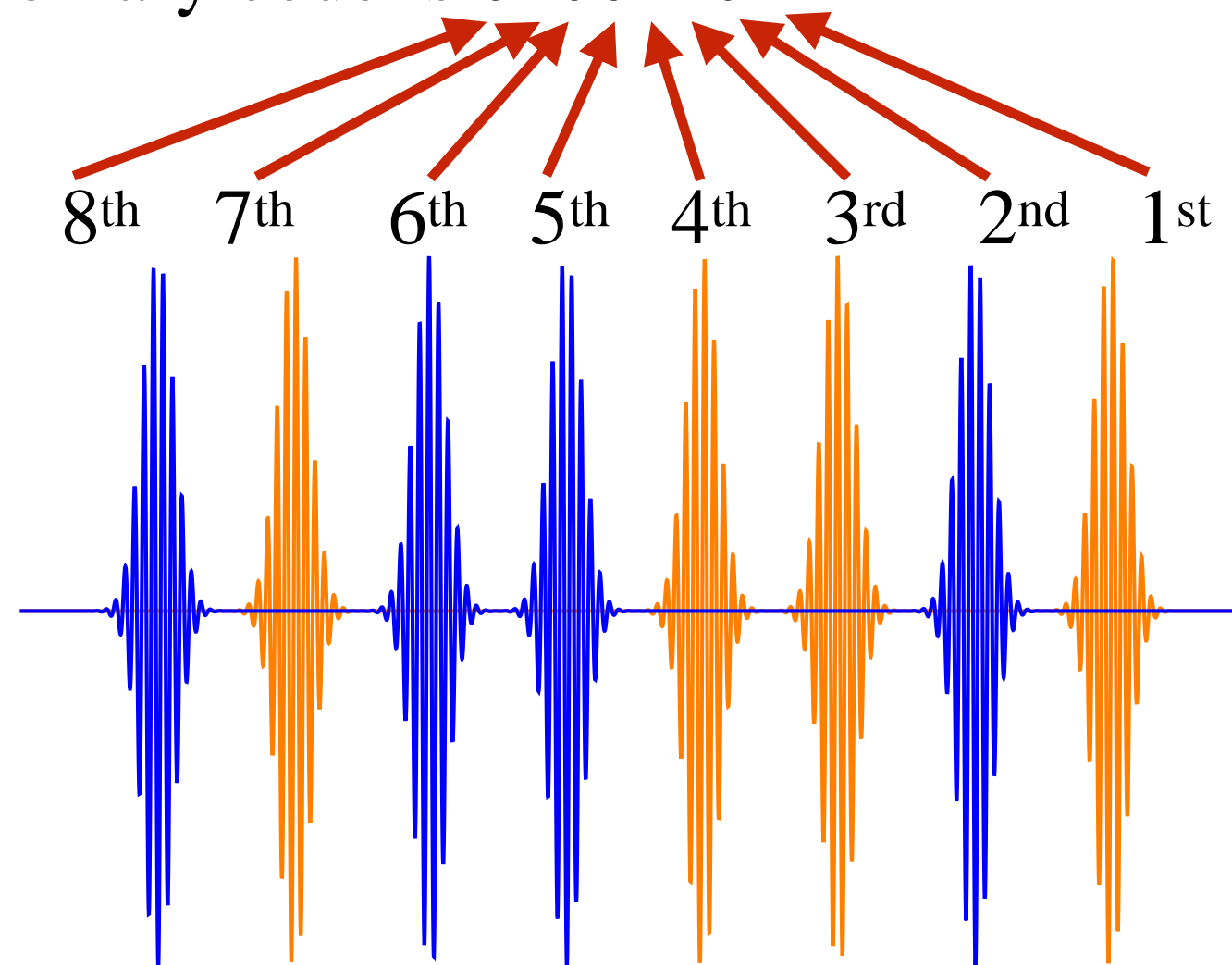
$$\begin{aligned}
 &(\alpha_1|0, 0\rangle + \beta_1|1, 1\rangle) \otimes (\alpha_2|0, 0\rangle + \beta_2|1, 1\rangle) \\
 &\neq \\
 &\alpha|0, 0\rangle + \beta|1, 1\rangle + \gamma|2, 2\rangle + \delta|3, 3\rangle
 \end{aligned}$$



High-Dimensional "alphabet"

Let us send letter **M**

Letter **M** in the binary code is **01001101**



Classically:

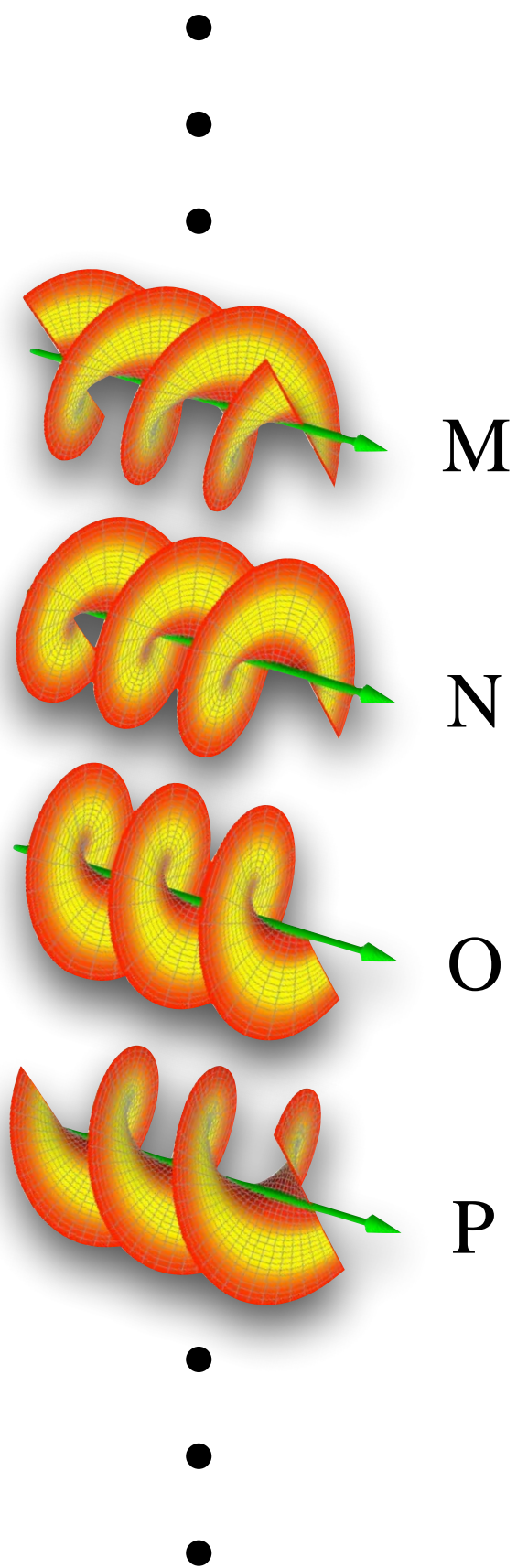
$$\begin{aligned}
 &00101011001100110101001101000110 \\
 &= \\
 &223030311031012 \\
 &= \\
 &5314651506 \\
 &= \\
 &724783942
 \end{aligned}$$

Quantum:

$$\begin{aligned}
 &(\alpha_1|0, 0\rangle + \beta_1|1, 1\rangle) \otimes (\alpha_2|0, 0\rangle + \beta_2|1, 1\rangle) \\
 &\neq \\
 &\alpha|0, 0\rangle + \beta|1, 1\rangle + \gamma|2, 2\rangle + \delta|3, 3\rangle
 \end{aligned}$$

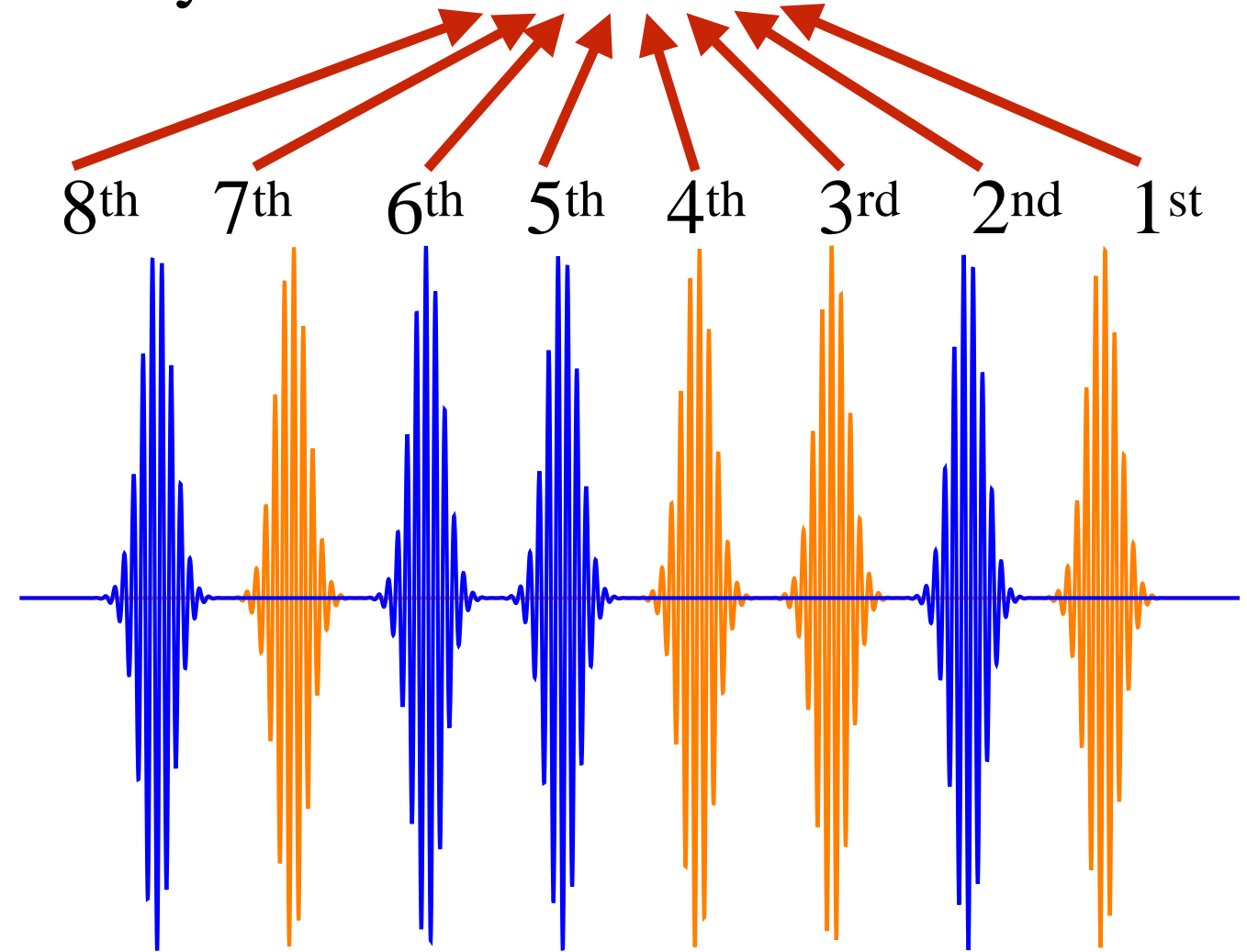


High-Dimensional "alphabet"



Let us send letter **M**

Letter **M** in the binary code is **01001101**



Classically:

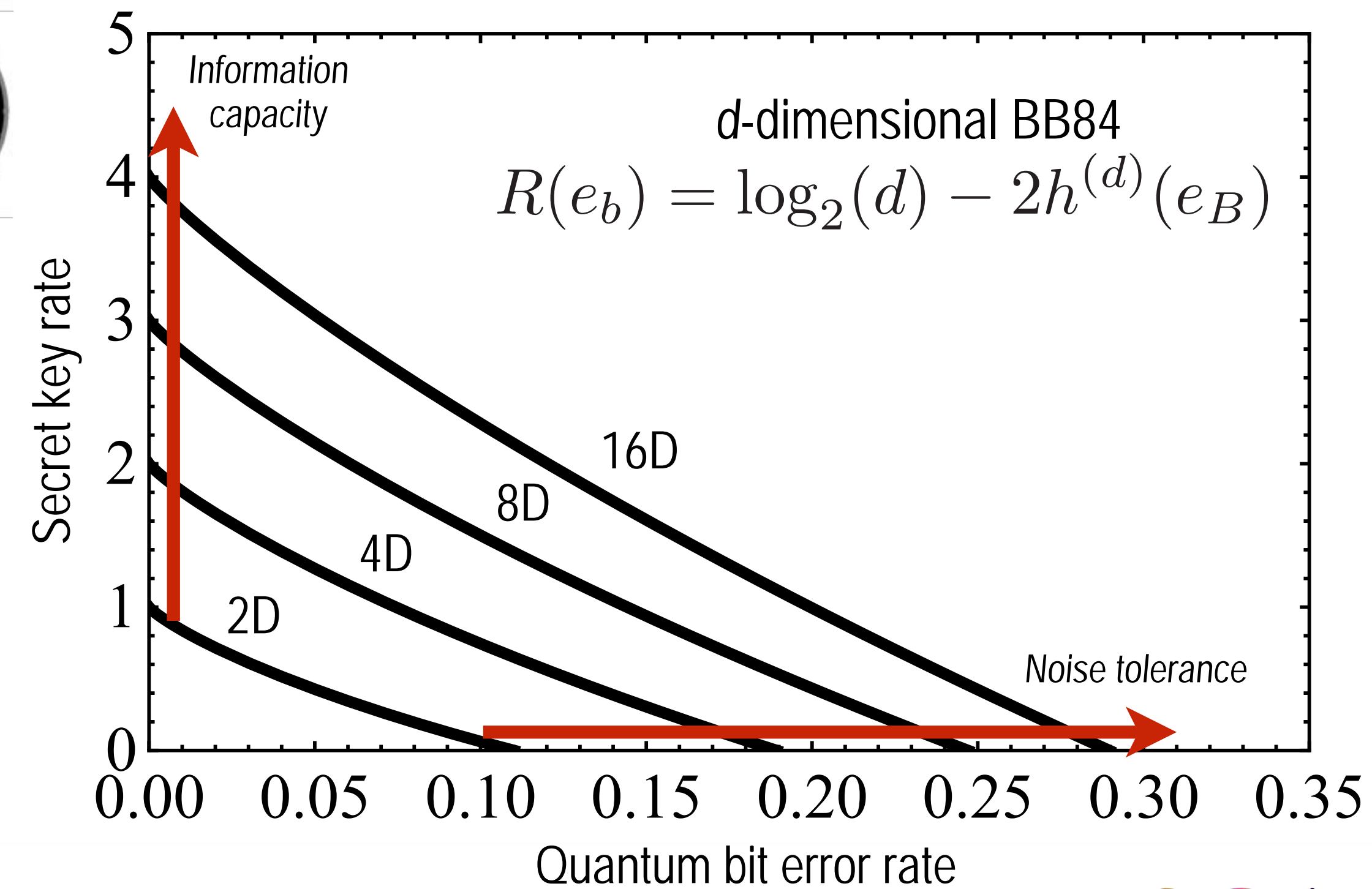
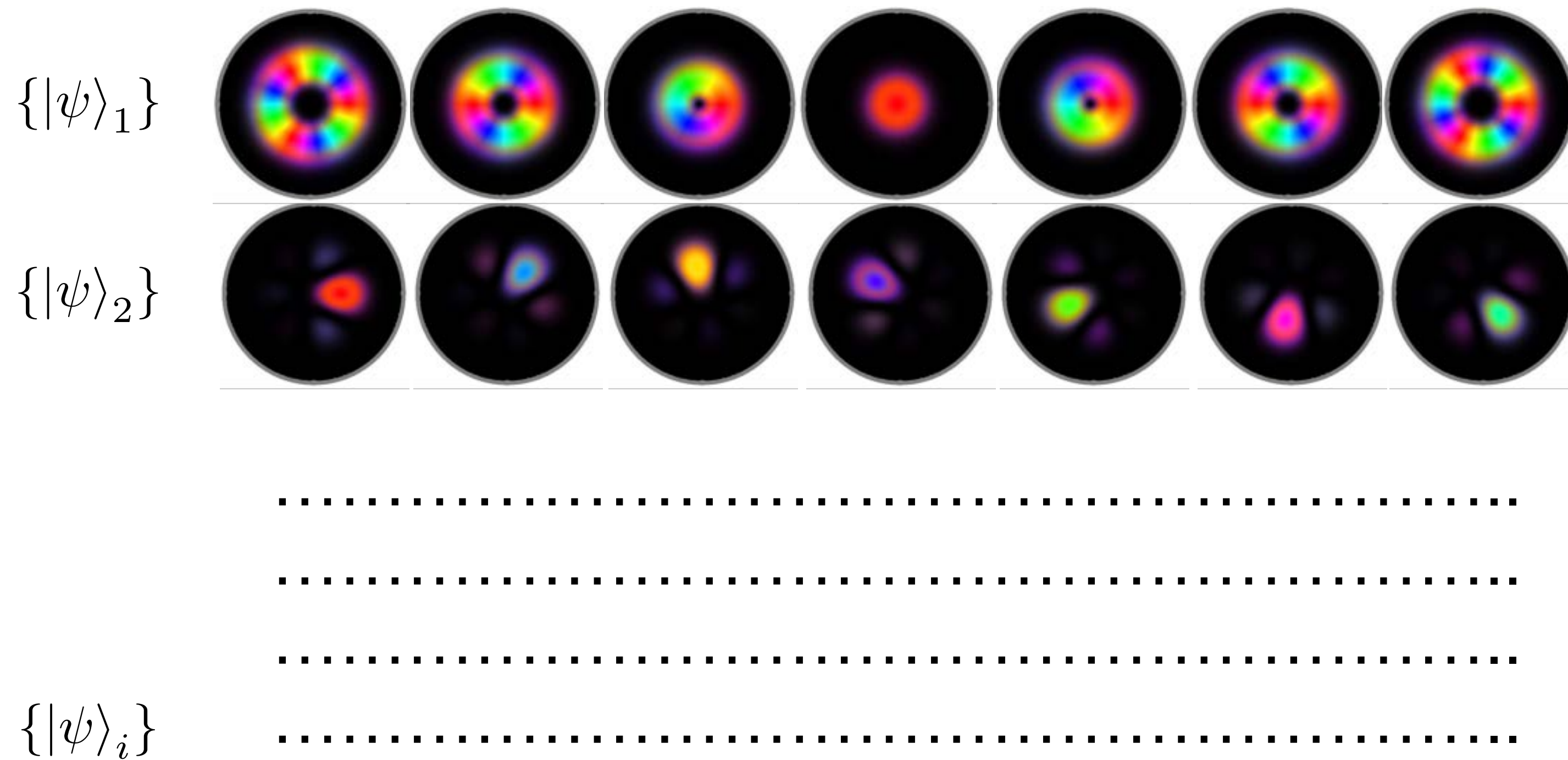
$$\begin{aligned}
 &00101011001100110101001101000110 \\
 &= \\
 &223030311031012 \\
 &= \\
 &5314651506 \\
 &= \\
 &724783942
 \end{aligned}$$

Quantum:

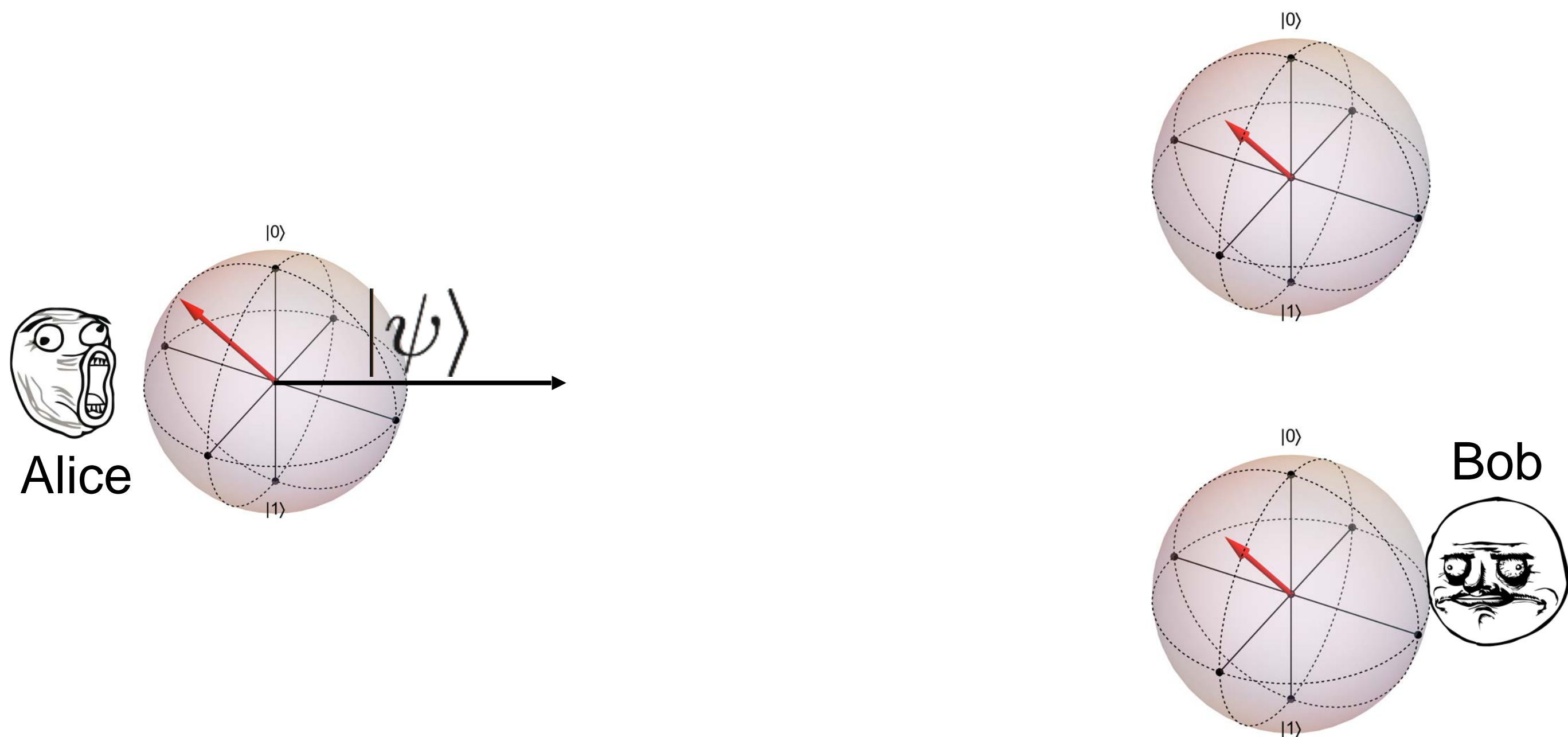
$$\begin{aligned}
 &(\alpha_1|0, 0\rangle + \beta_1|1, 1\rangle) \otimes (\alpha_2|0, 0\rangle + \beta_2|1, 1\rangle) \\
 &\neq \\
 &\alpha|0, 0\rangle + \beta|1, 1\rangle + \gamma|2, 2\rangle + \delta|3, 3\rangle
 \end{aligned}$$



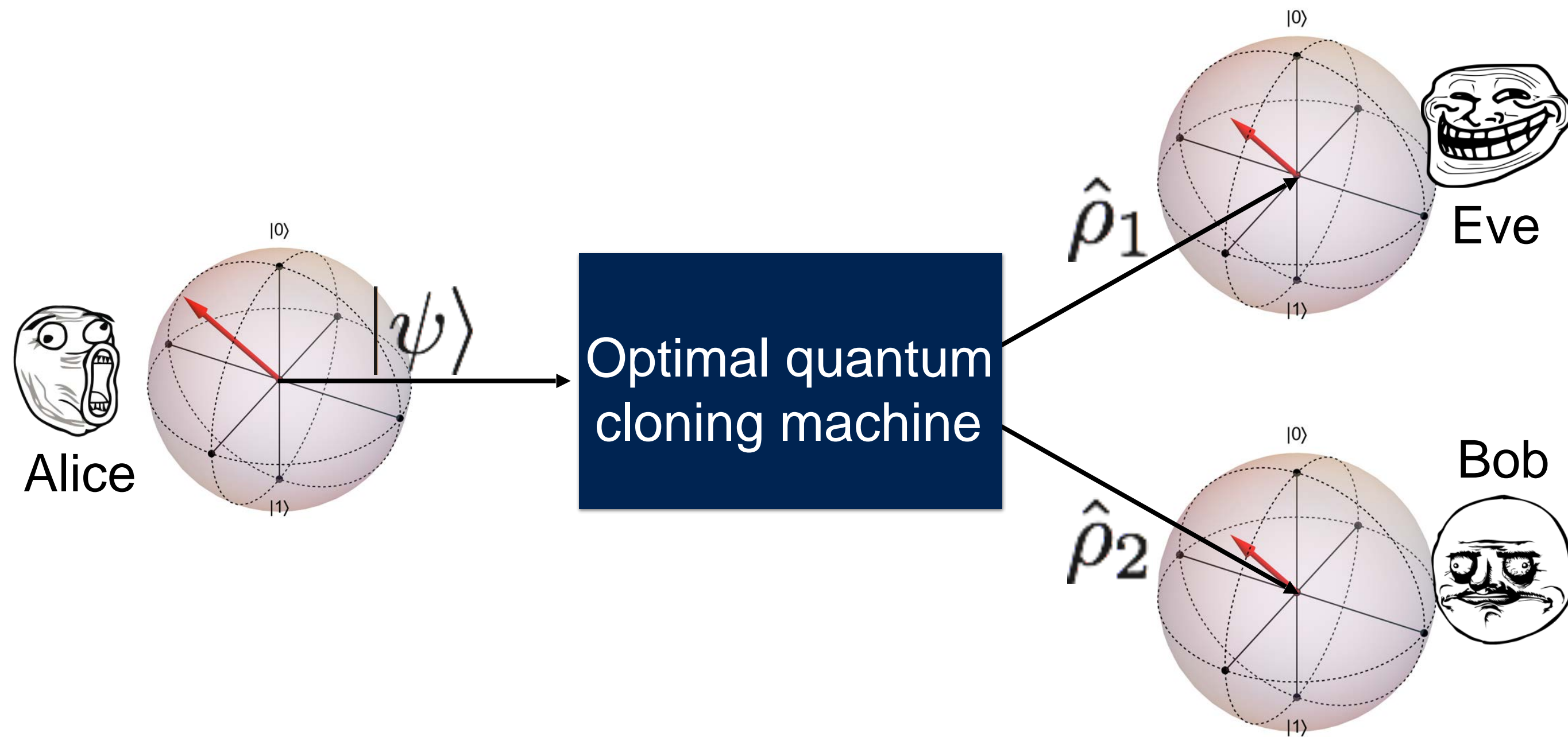
Application in High-Dimensional Quantum Key Distribution



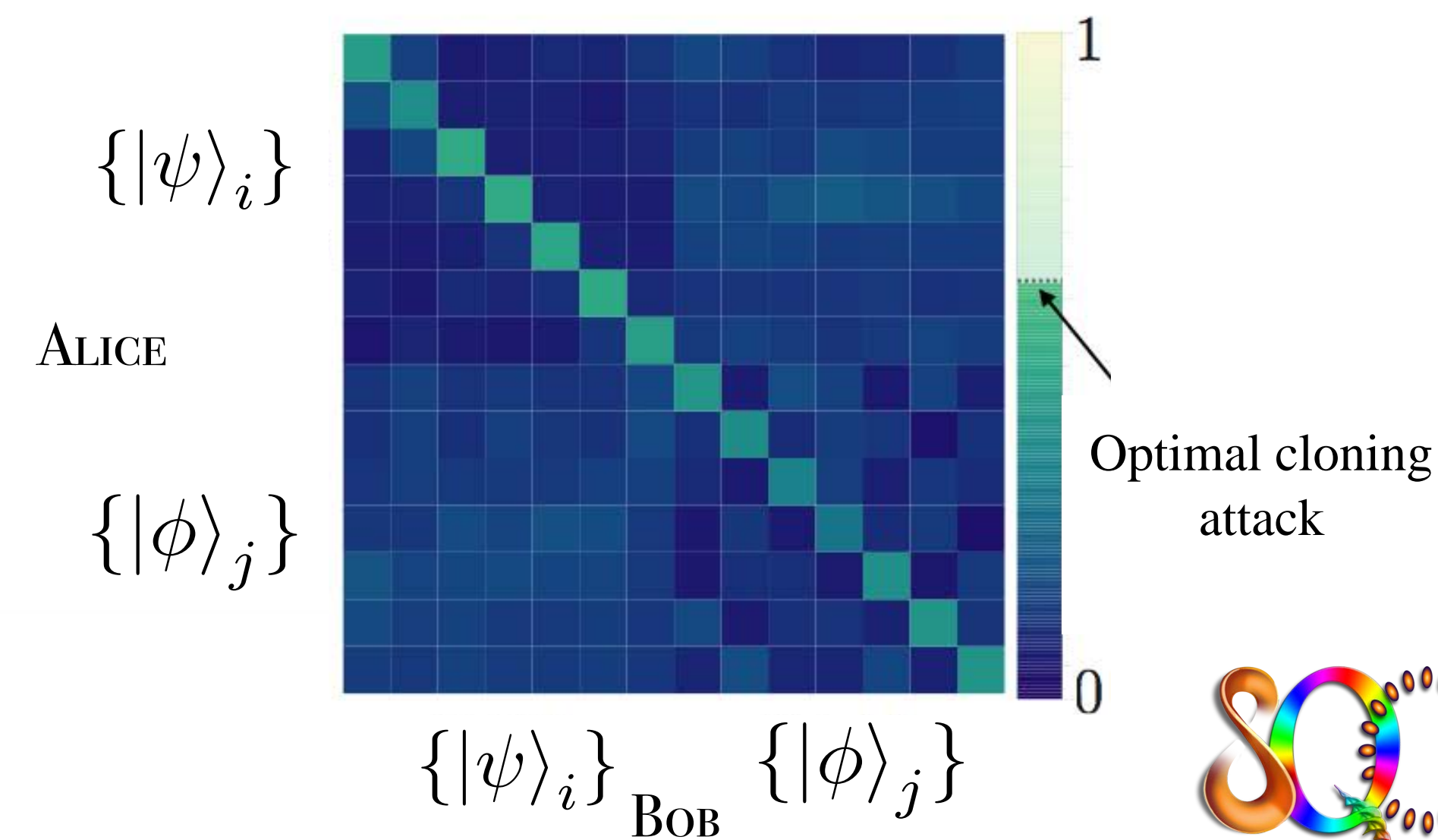
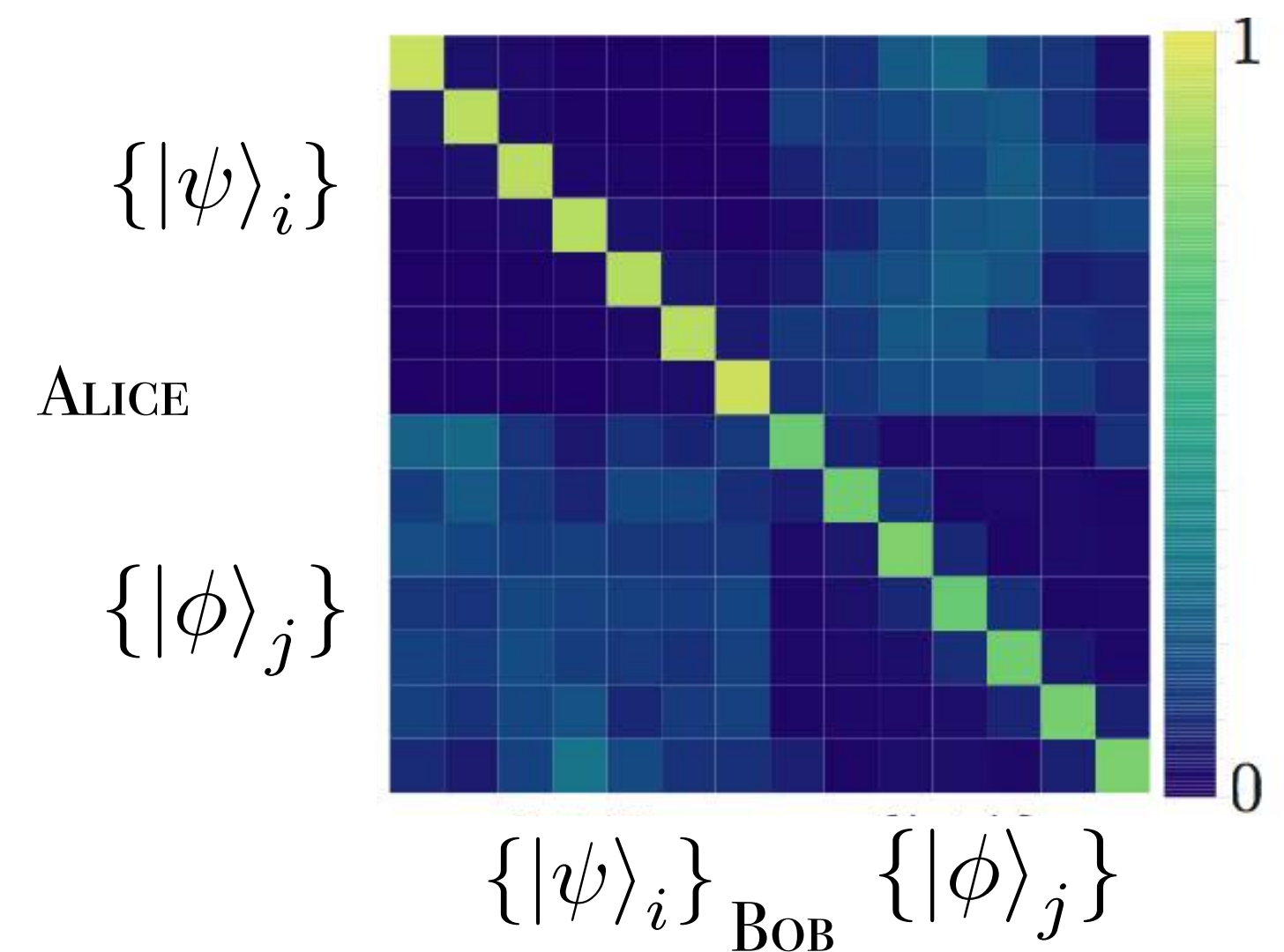
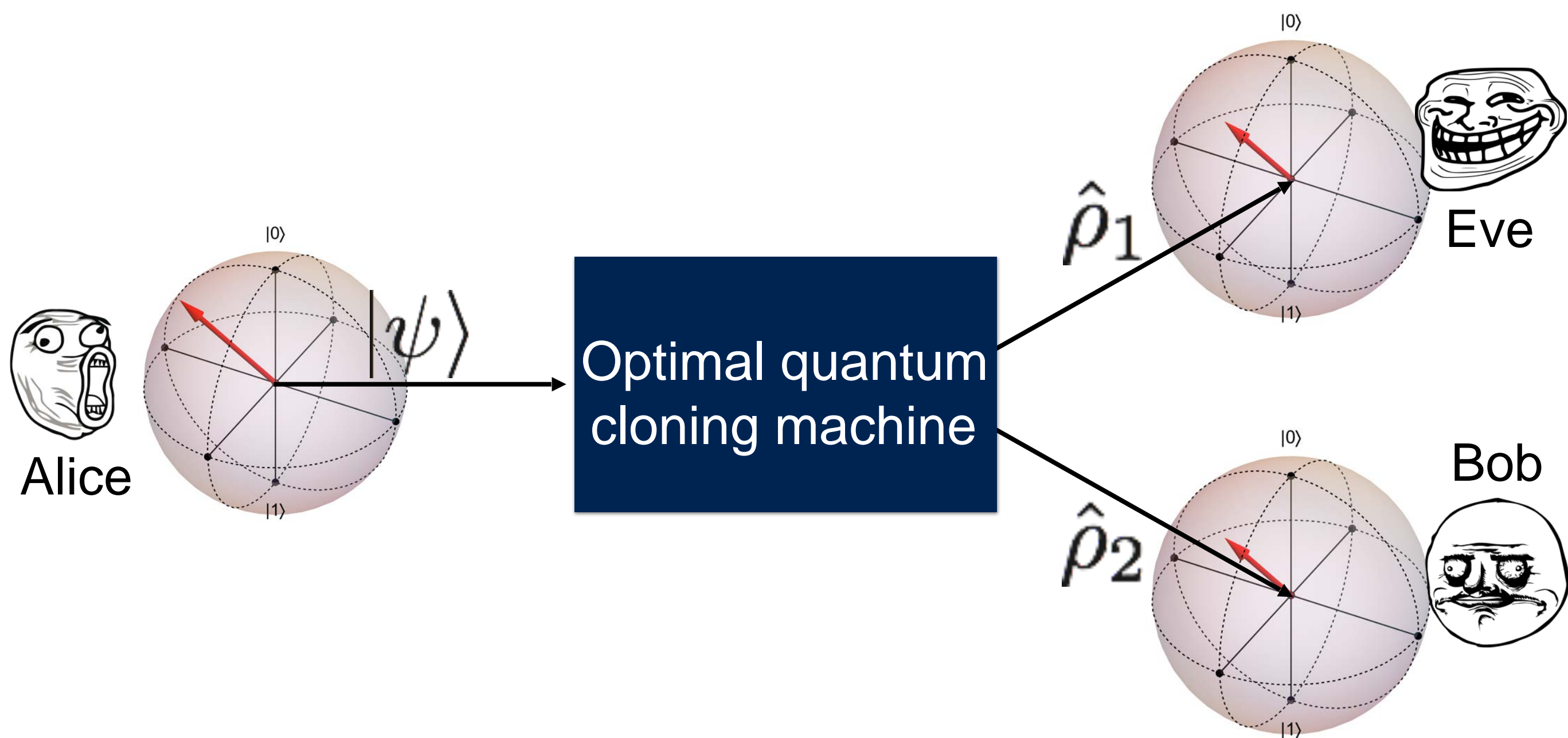
High-Dimensional Quantum Key Distribution: Security threshold



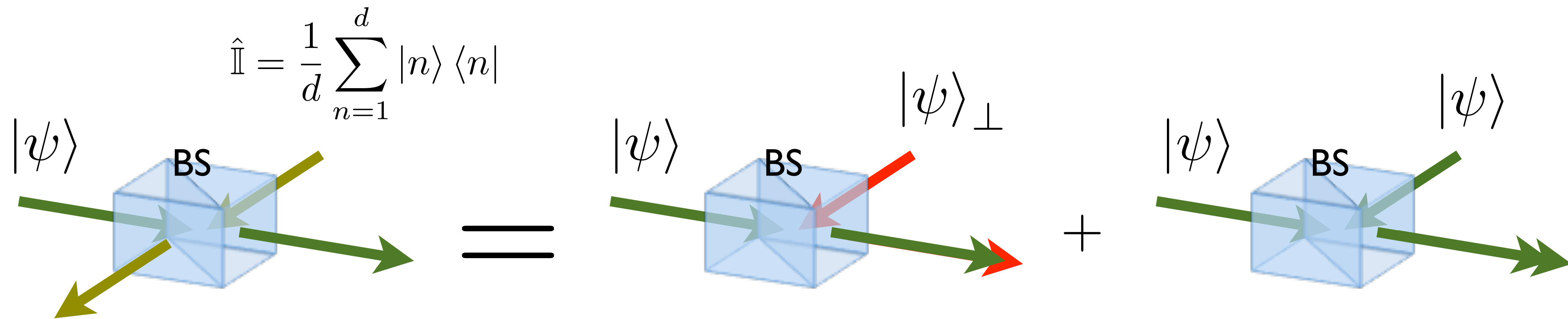
High-Dimensional Quantum Key Distribution: Security threshold



High-Dimensional Quantum Key Distribution: Security threshold



High-Dimensional Quantum Key Distribution: Security threshold



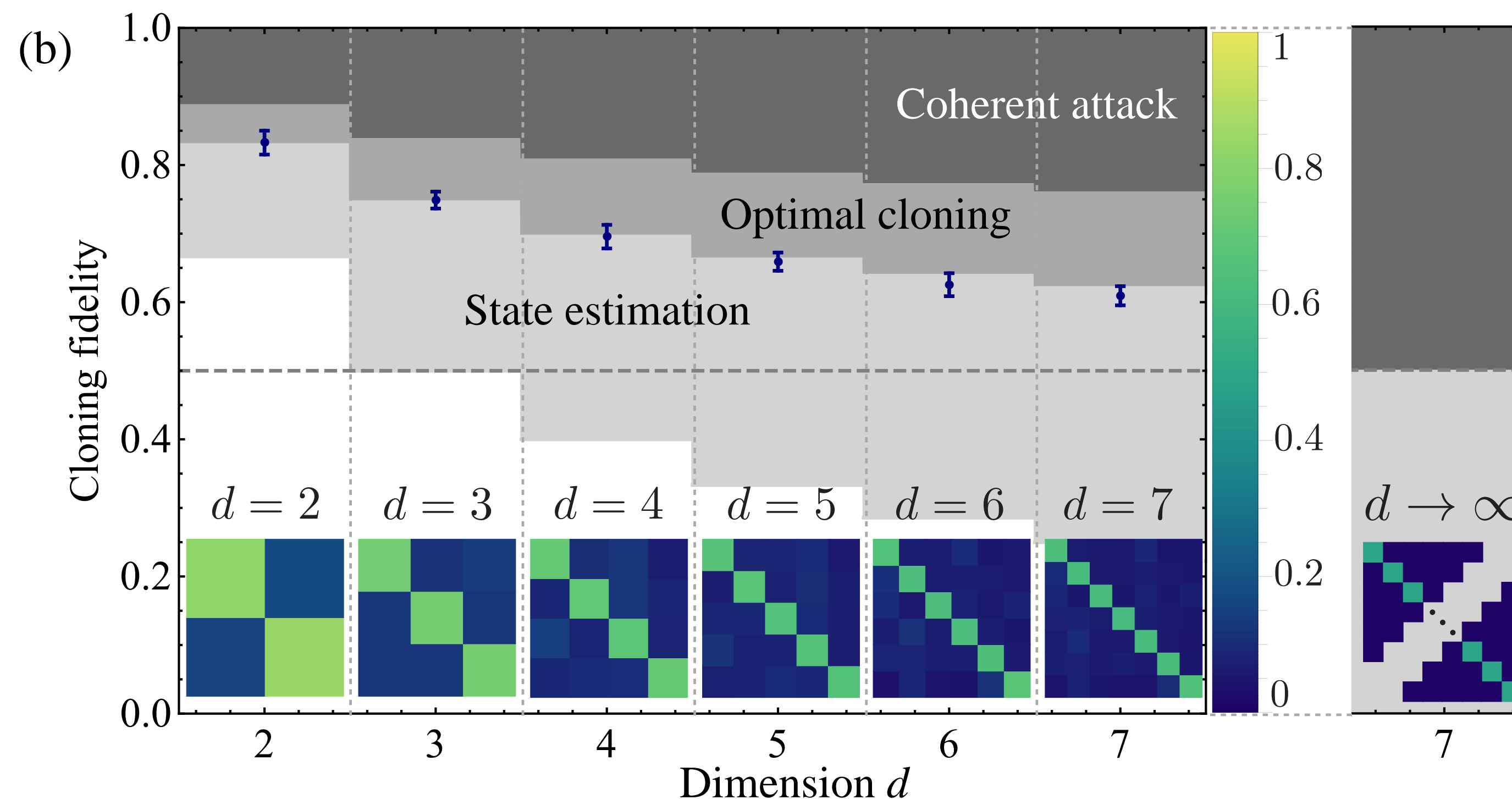
$$\mathcal{F} = \frac{d-1}{d+1} \times \frac{1}{2} + \frac{2}{d+1} \times 1$$

$$\mathcal{F} = \frac{1}{2} + \frac{1}{d+1}$$

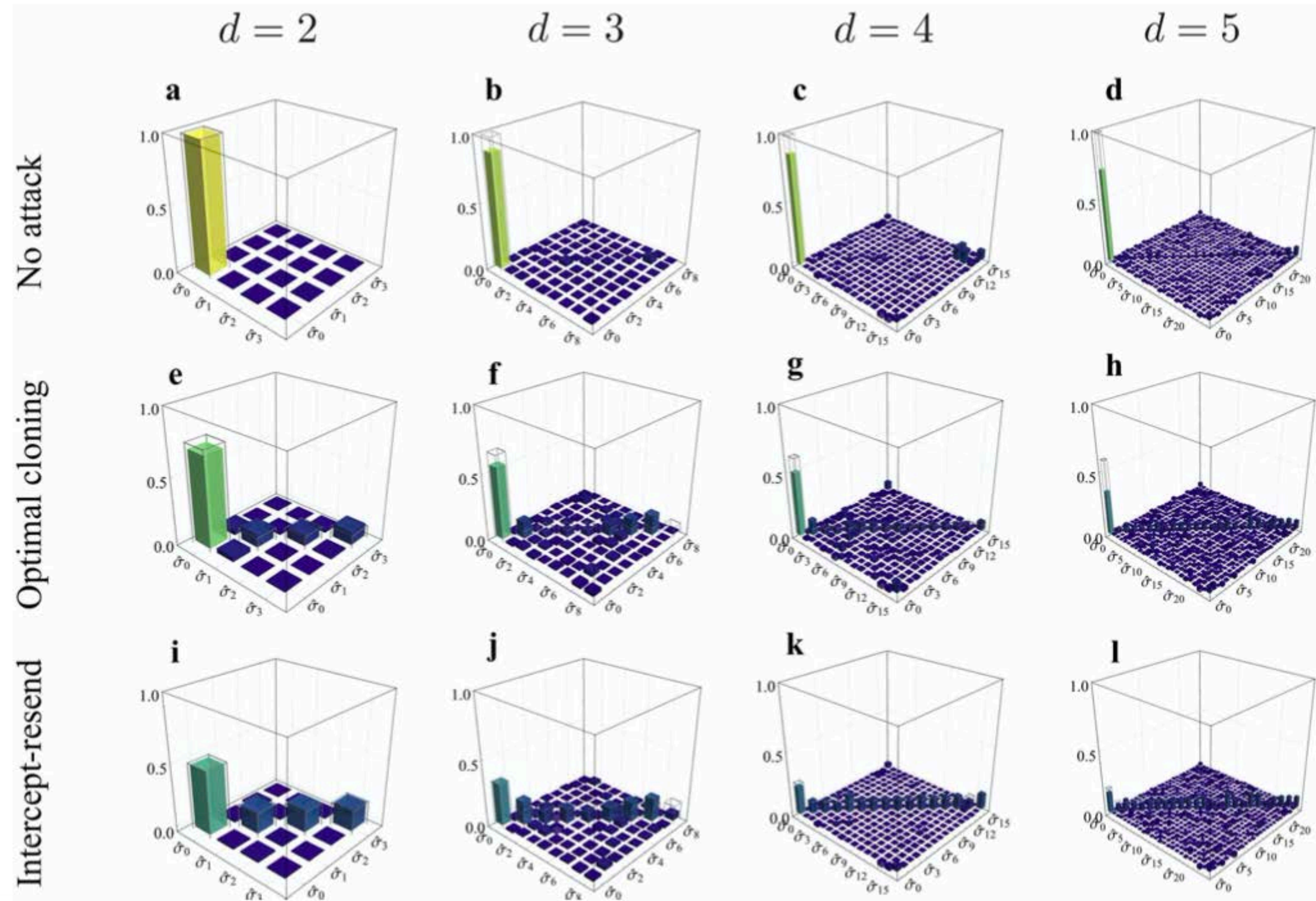
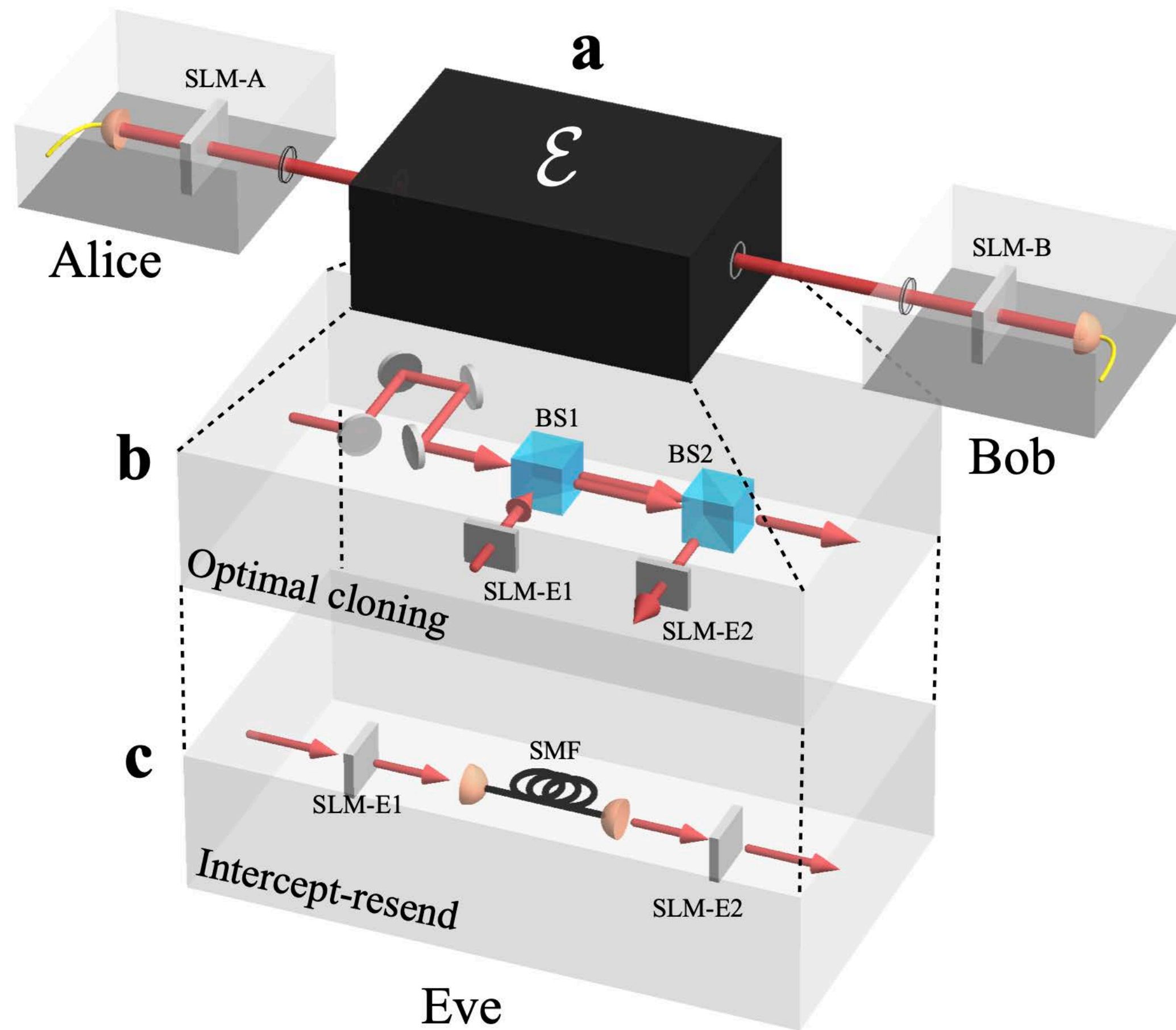


High-Dimensional Quantum Key Distribution: Security threshold

Dimension	$d = 2$	$d = 3$	$d = 4$	$d = 5$	$d = 6$	$d = 7$	$d \rightarrow \infty$
Theory	0.833	0.75	0.7	0.667	0.643	0.625	0.5
Experimental	0.82 ± 0.01	0.75 ± 0.01	0.70 ± 0.02	0.66 ± 0.01	0.64 ± 0.02	0.62 ± 0.02	
	0.84 ± 0.02	0.75 ± 0.01	0.70 ± 0.01	0.67 ± 0.01	0.62 ± 0.01	0.61 ± 0.01	
		0.75 ± 0.01	0.68 ± 0.01	0.65 ± 0.08	0.62 ± 0.01	0.61 ± 0.01	
			0.70 ± 0.02	0.66 ± 0.01	0.62 ± 0.01	0.60 ± 0.01	
				0.65 ± 0.02	0.62 ± 0.01	0.61 ± 0.01	
Average	0.83 ± 0.02	0.75 ± 0.01	0.70 ± 0.02	0.66 ± 0.01	0.63 ± 0.02	0.61 ± 0.01	

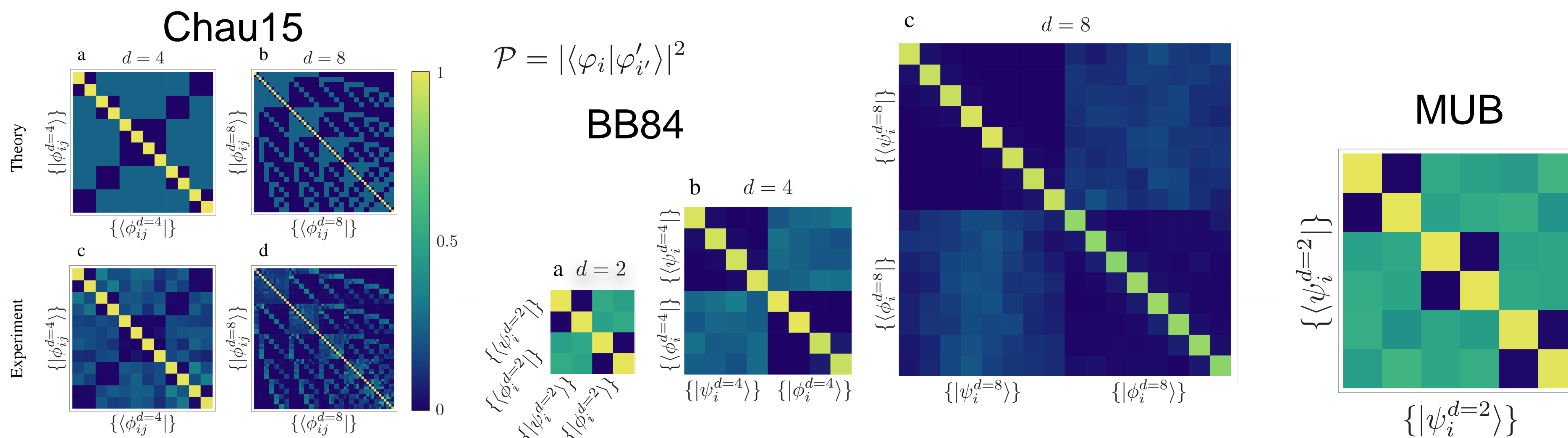


High-Dimensional Quantum Key Distribution: Security threshold

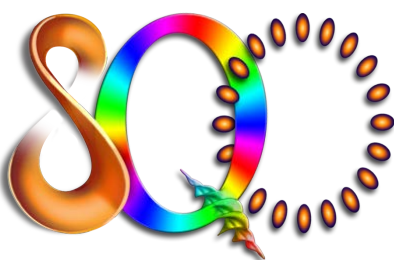
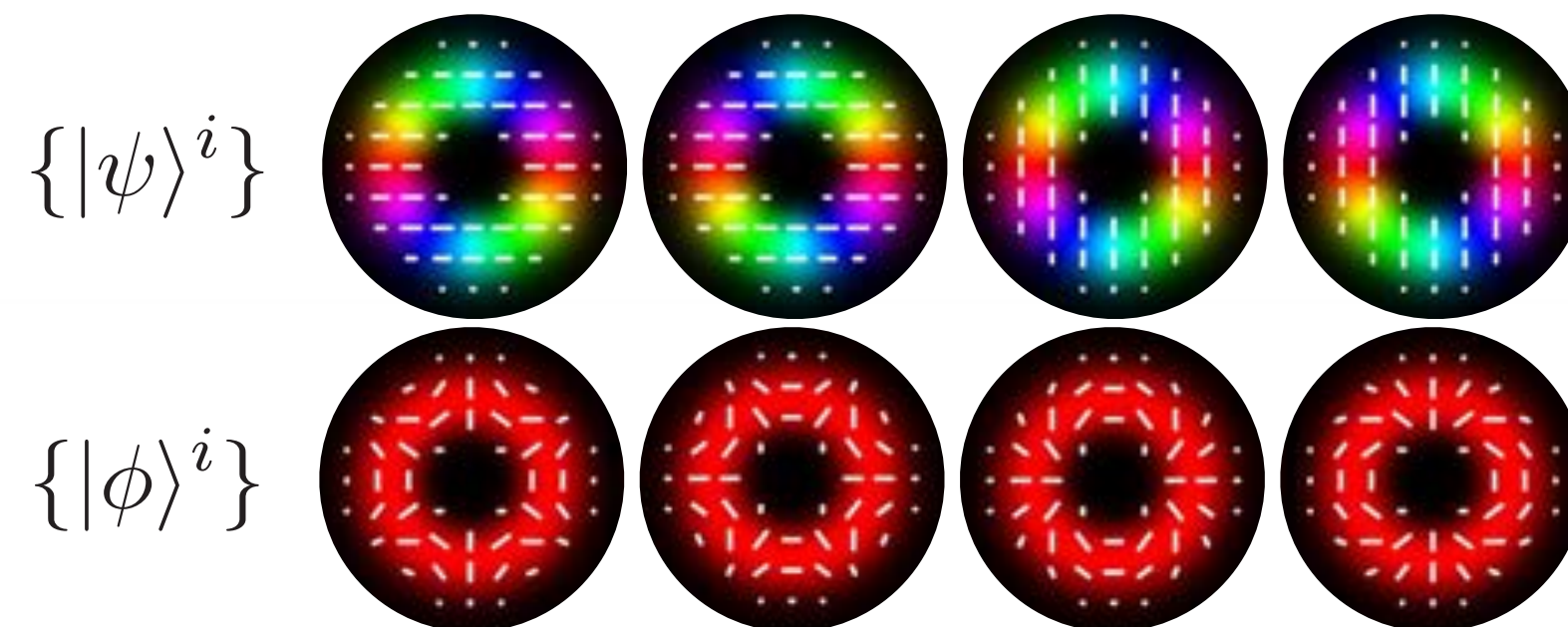
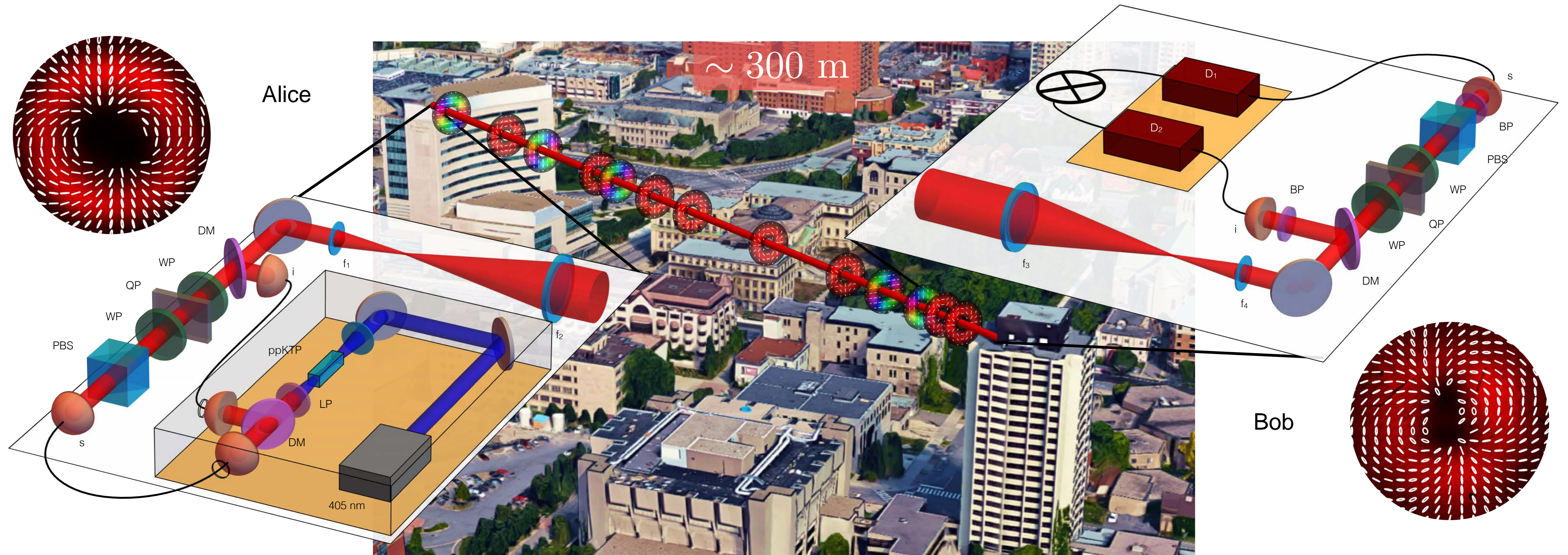


Is there any optimal spaces or protocols for QKD?

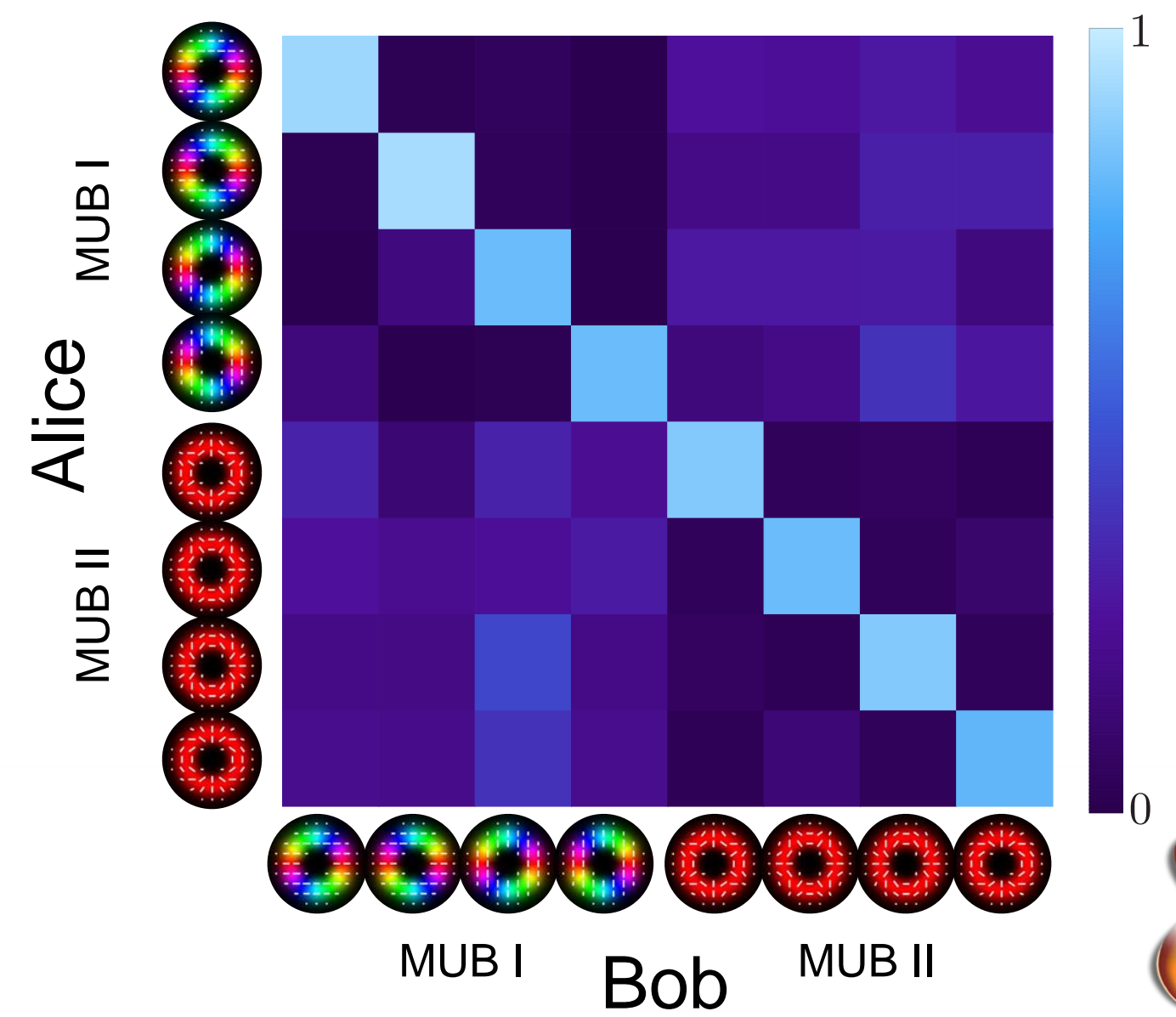
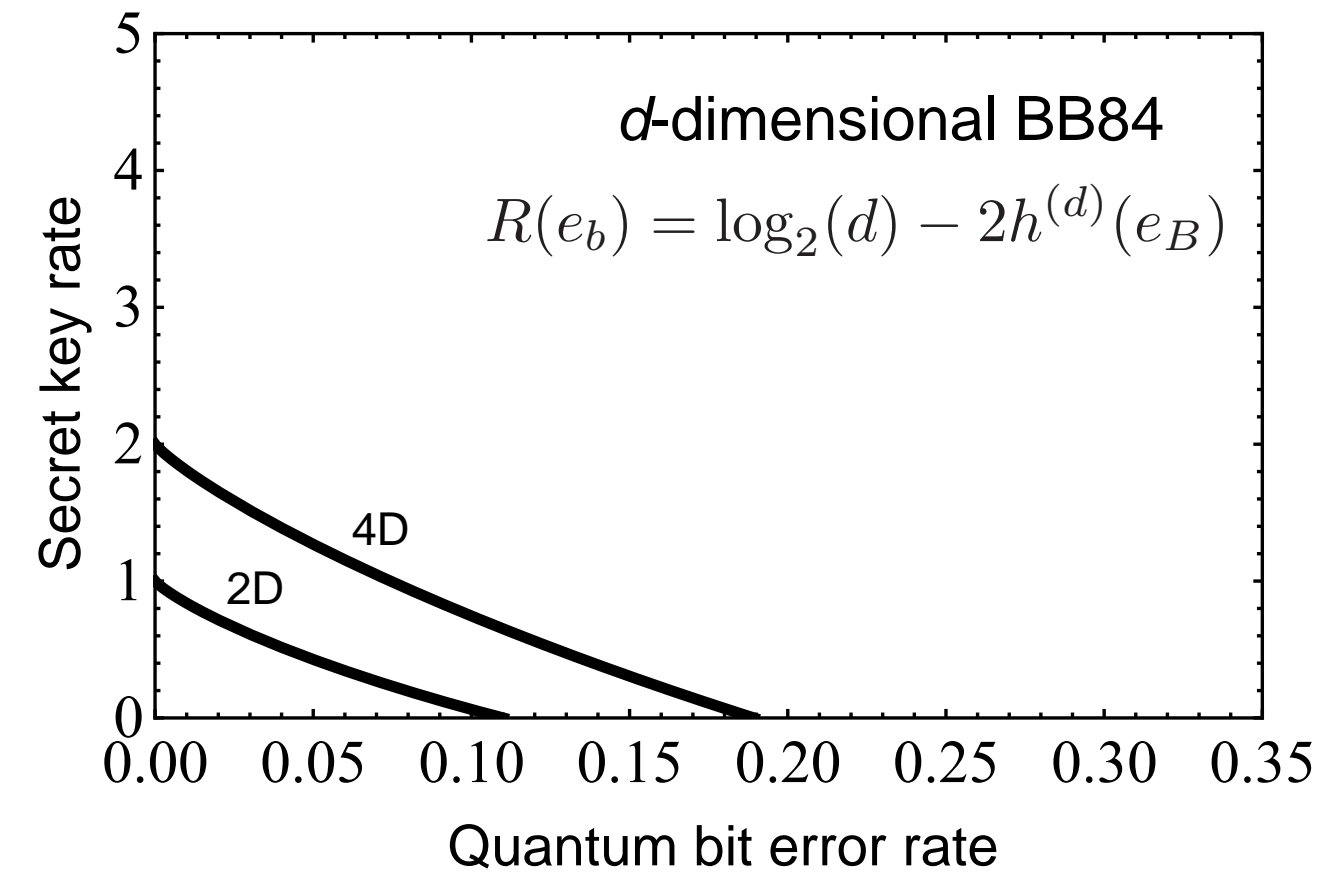
Protocol	d	e_b^{\max}	e_b^{\exp}	$R(0)$	R^{\exp}	Sifting	$R^{\exp} \times$ Sifting
Chau15	4	50 %	0.778 %	1	0.8170	1/6	0.1362
	8	50 %	3.11 %	1	0.8172	1/28	0.0292
BB84	2	11.00 %	0.628 %	1	0.8901	1/2 - 1*	0.4451 - 0.8901
	4	18.93 %	3.51 %	2	1.4500	1/2 - 1*	0.7250 - 1.4500
	8	24.70 %	10.9 %	3	1.3942	1/2 - 1*	0.6971 - 1.3942
MUB	2	12.62 %	0.923 %	1	0.8727	1/3 - 1*	0.2909 - 0.8727
	4	23.17 %	3.87 %	2	1.5316	1/5 - 1*	0.3063 - 1.5316
Singapore	2	38.93 %	1.23 %	0.4	0.374**	1	0.374**



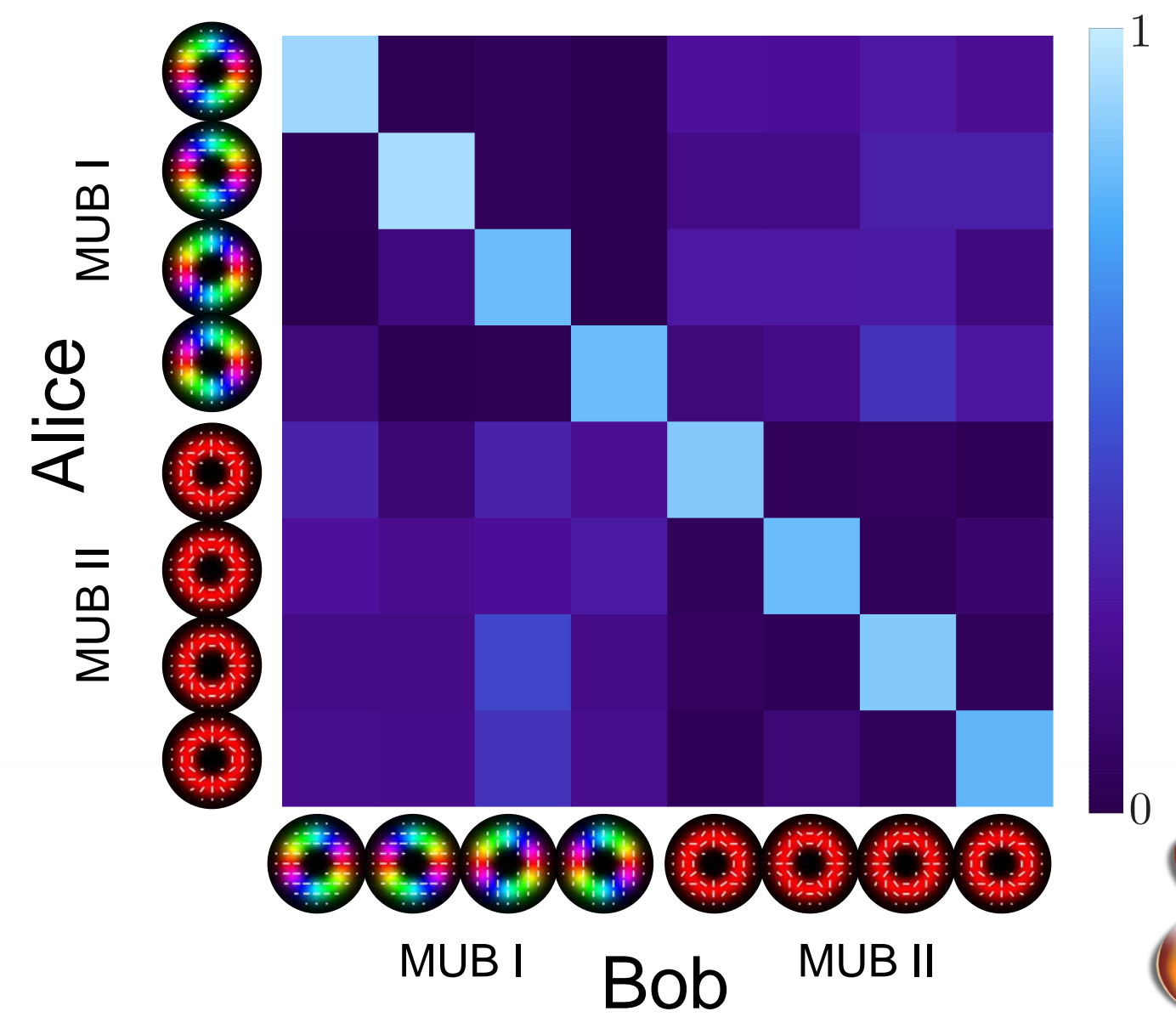
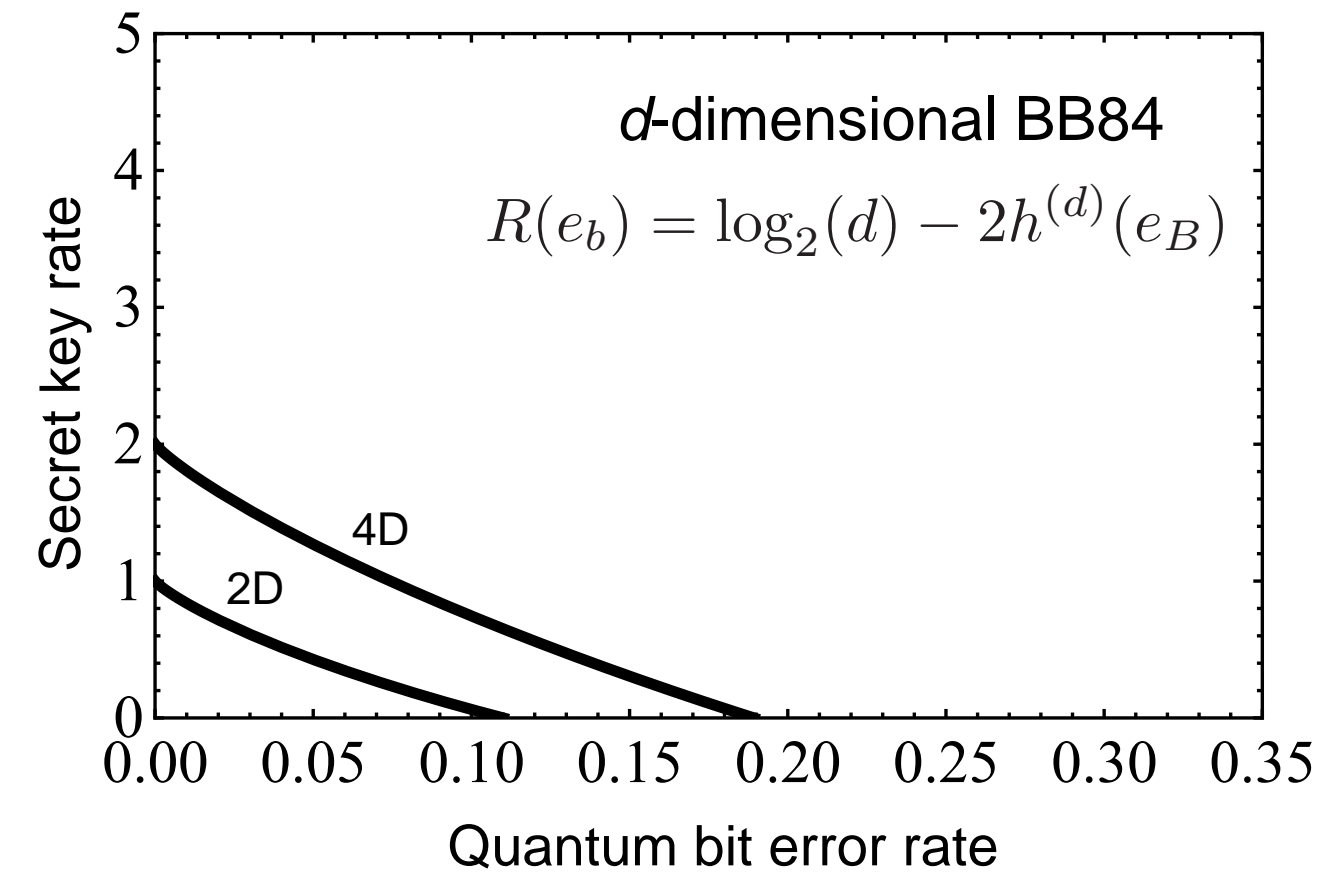
Free Space Quantum Key Distribution



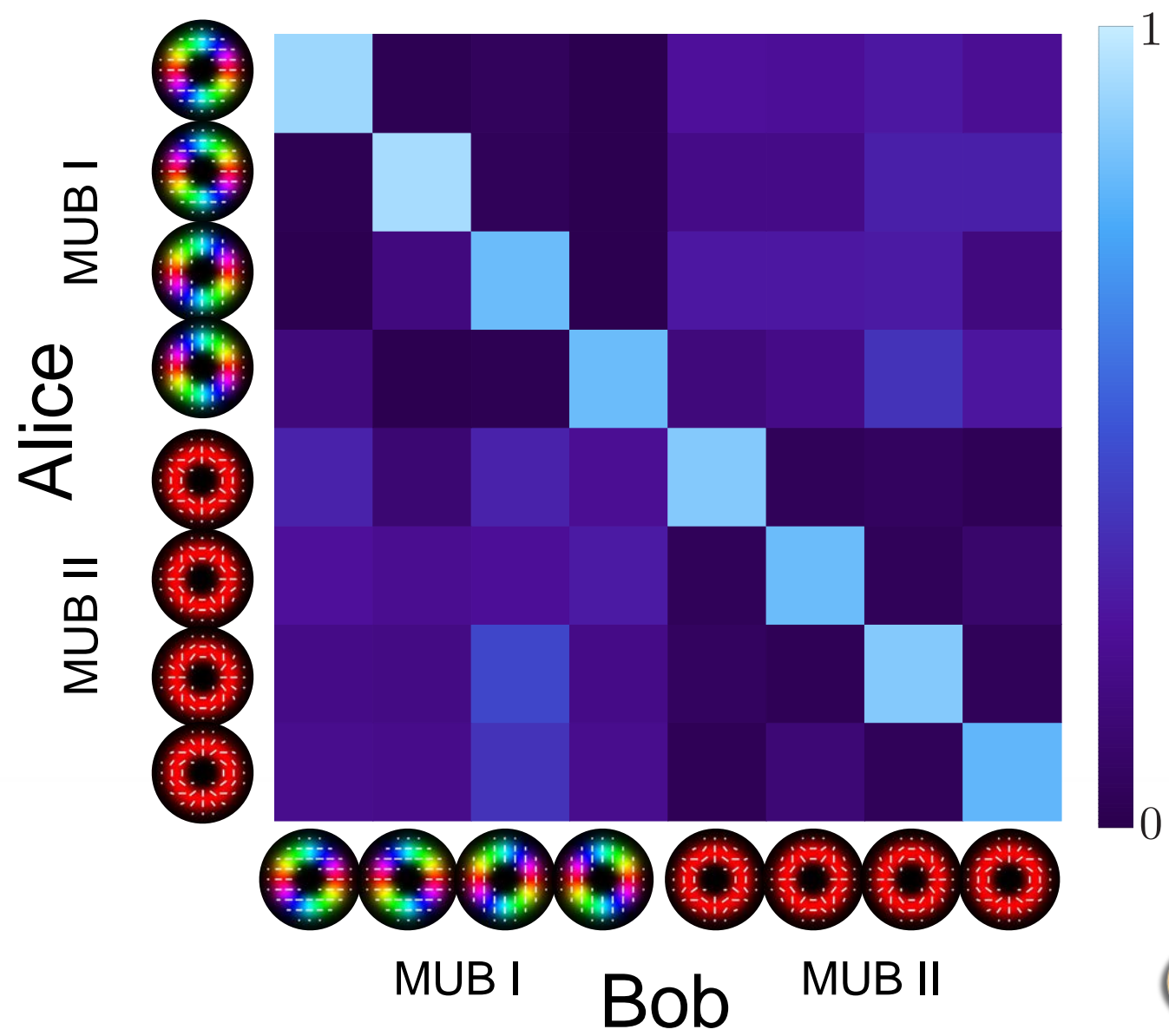
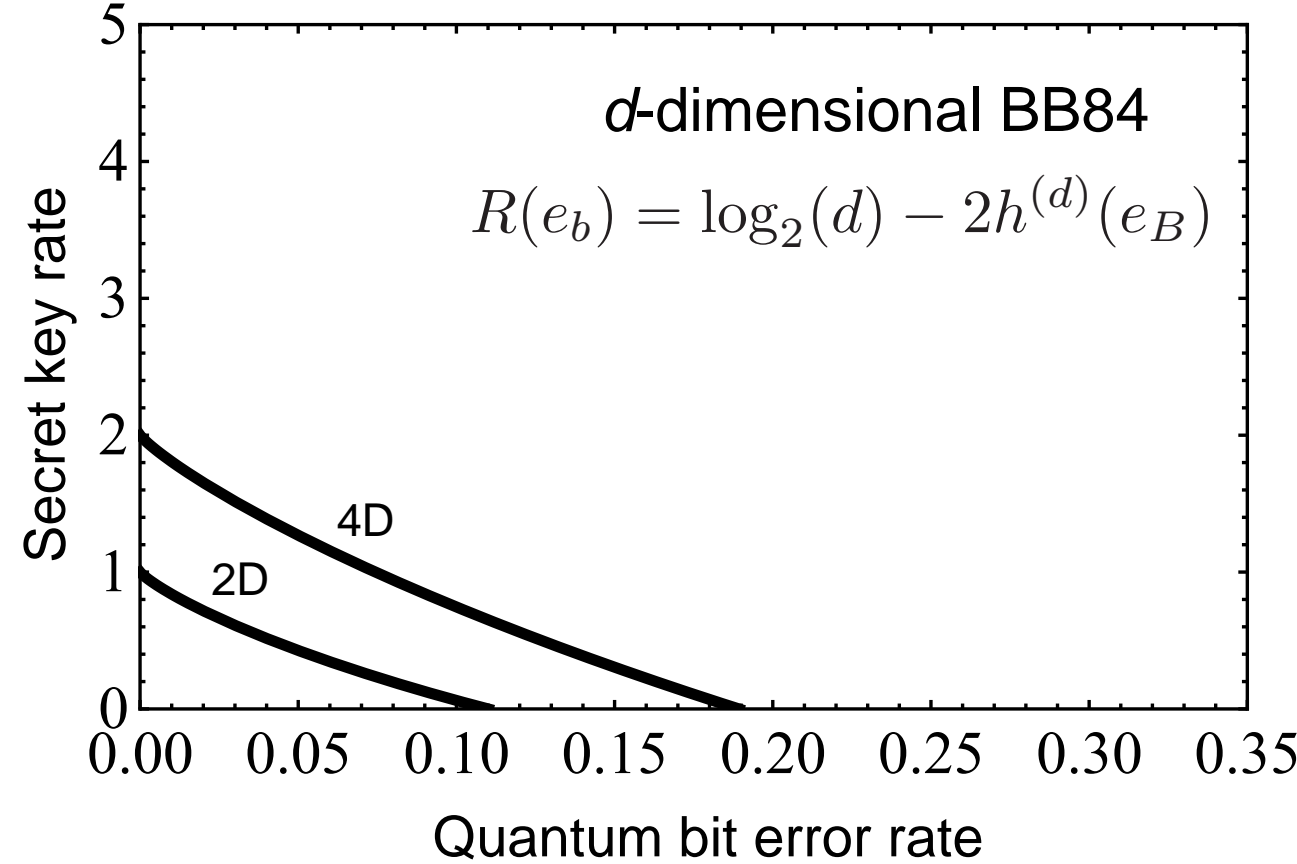
Free Space Quantum Key Distribution



Free Space Quantum Key Distribution



Free Space Quantum Key Distribution

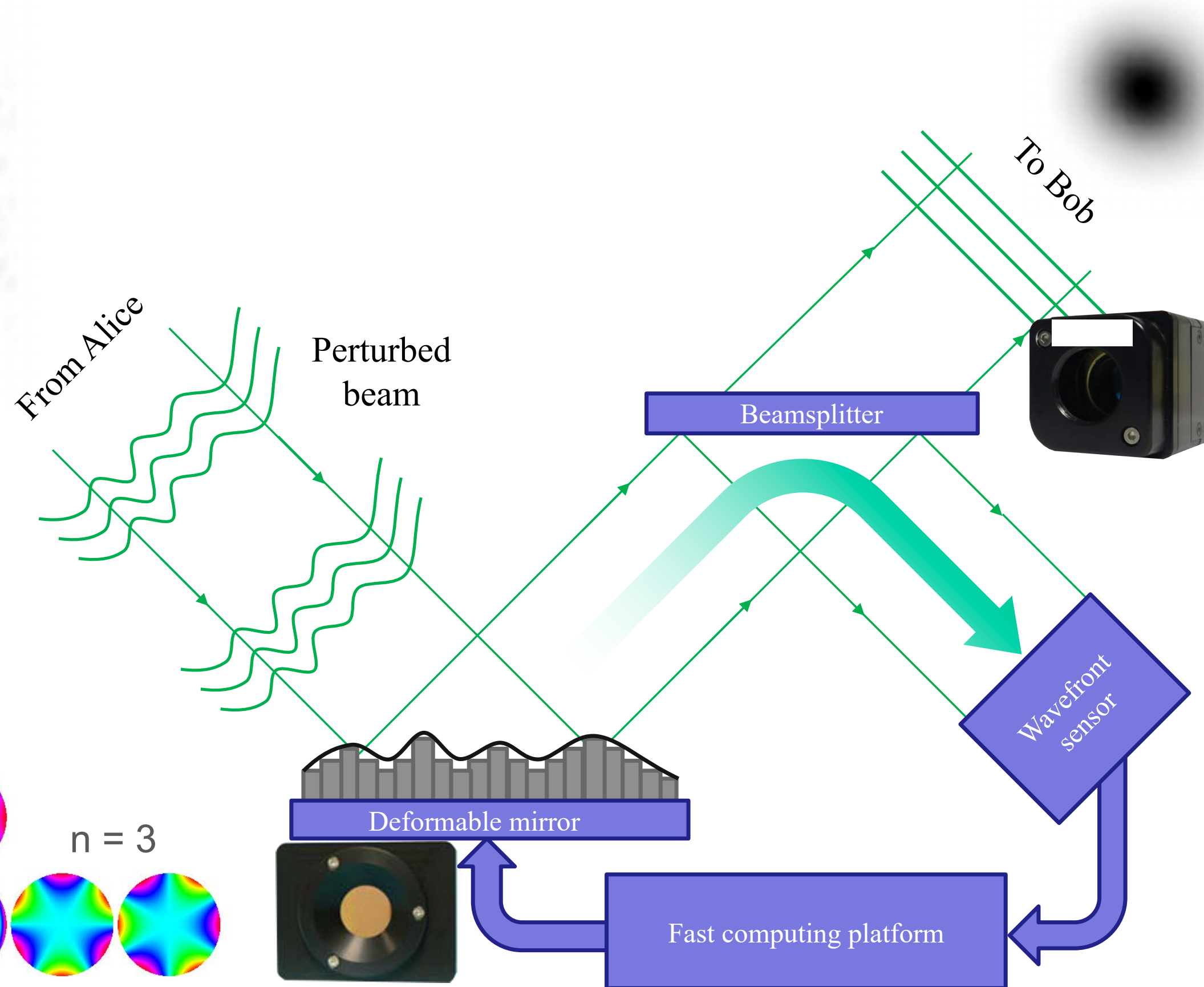
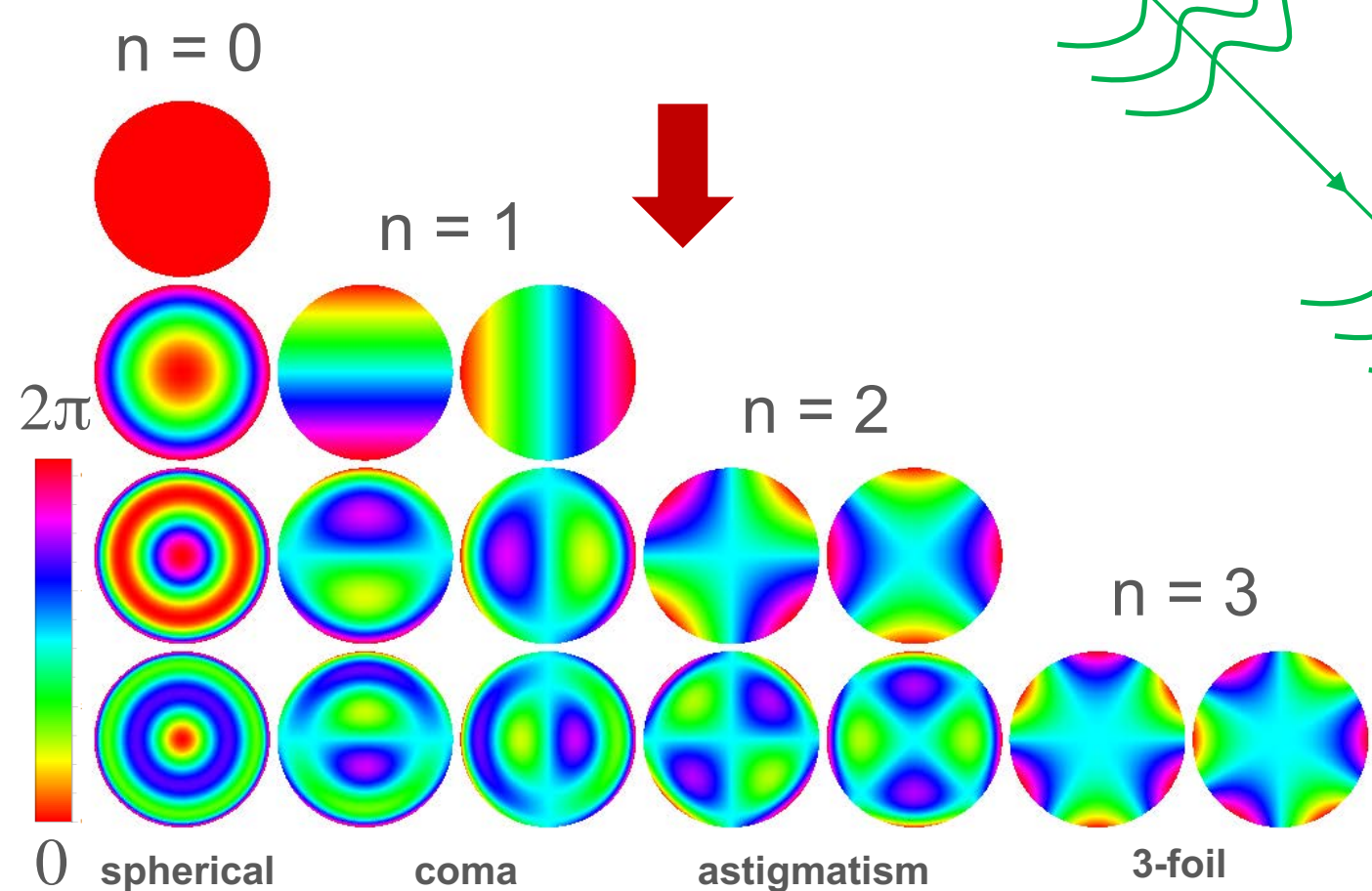
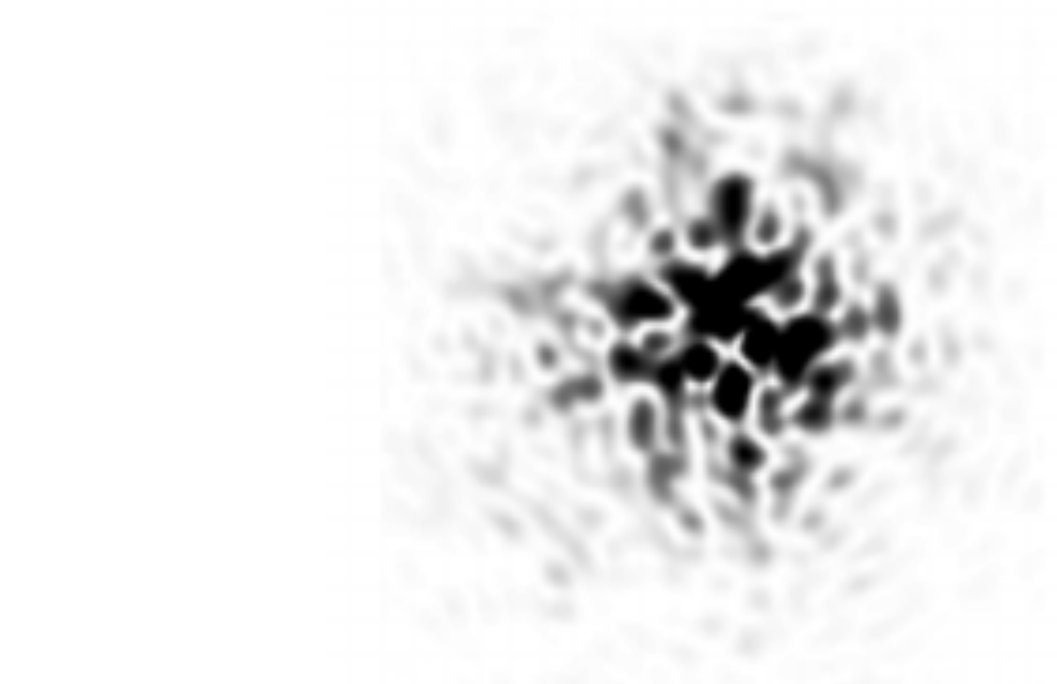
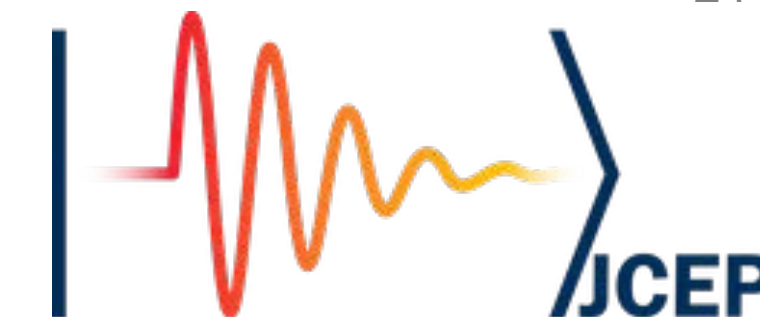




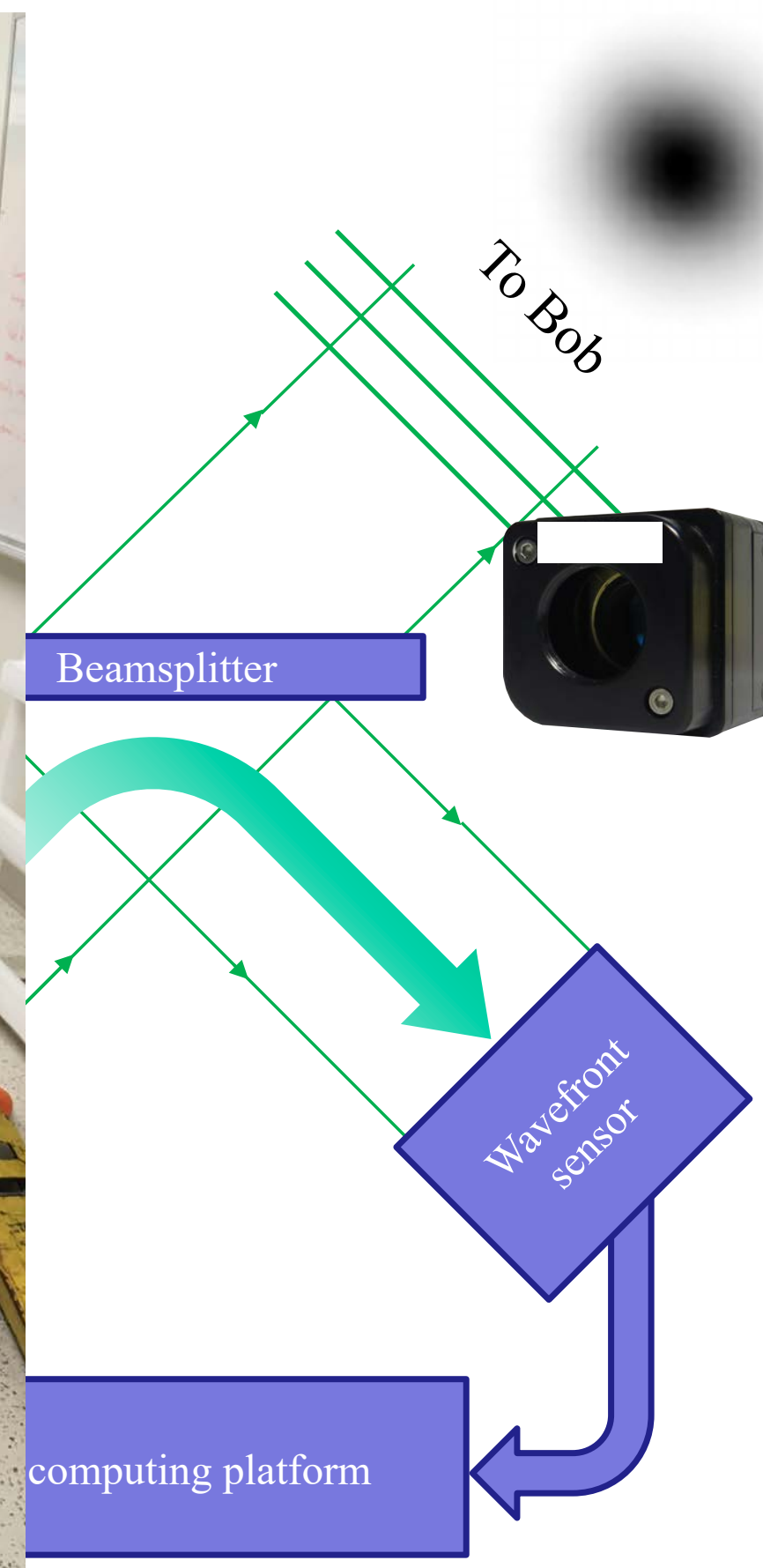
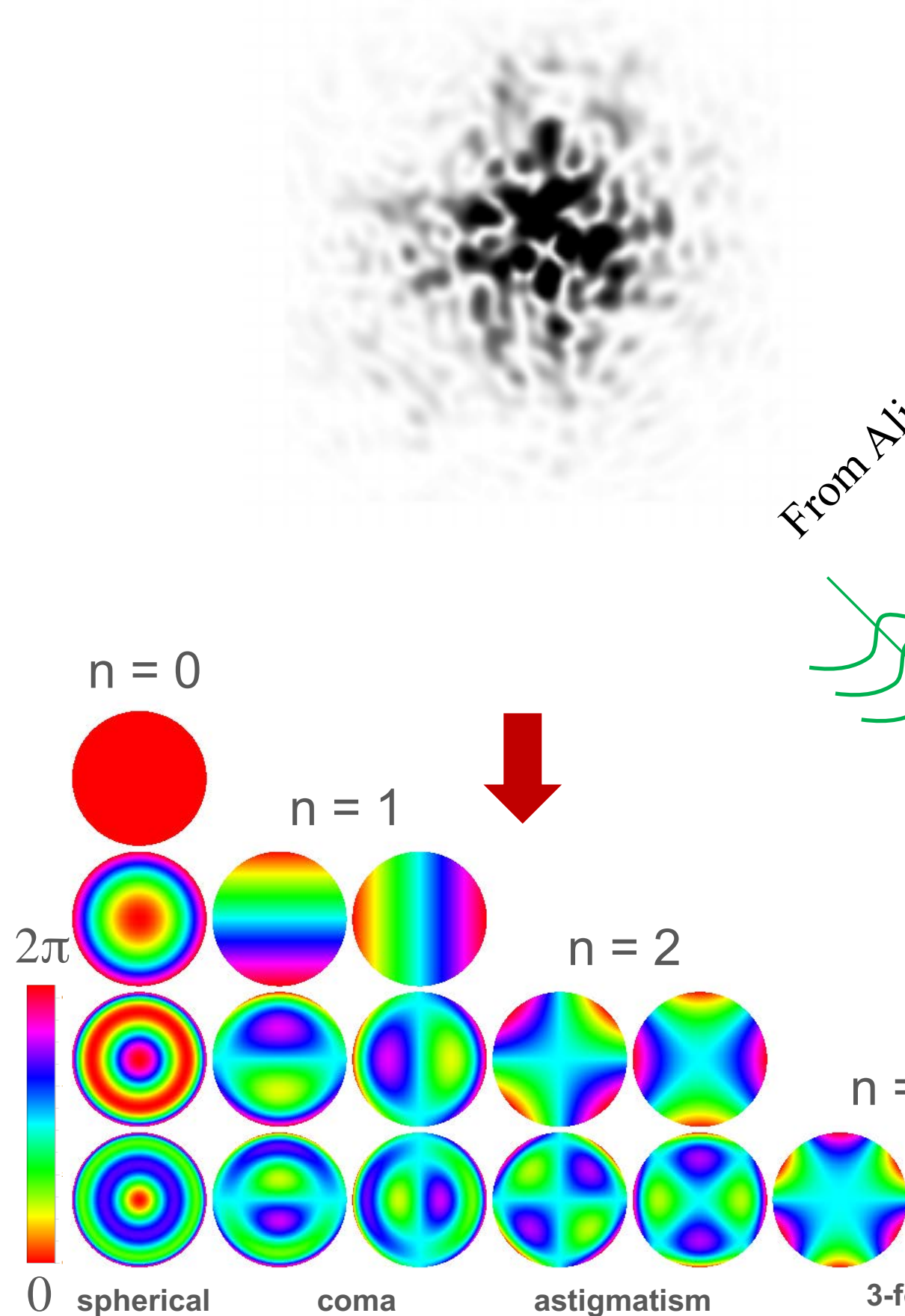
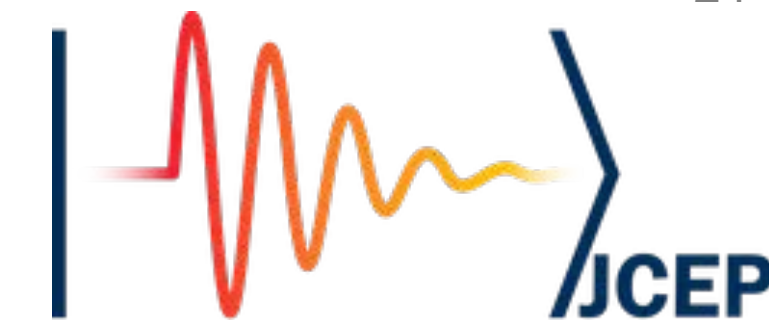
NRC-uOttawa Free-Space Quantum Communication link



NRC-uOttawa Free-Space Quantum Communication link



NRC-uOttawa Free-Space Quantum Communication link



Quantum Key Distribution through Underwater Channel



Quantum Key Distribution through Underwater Channel



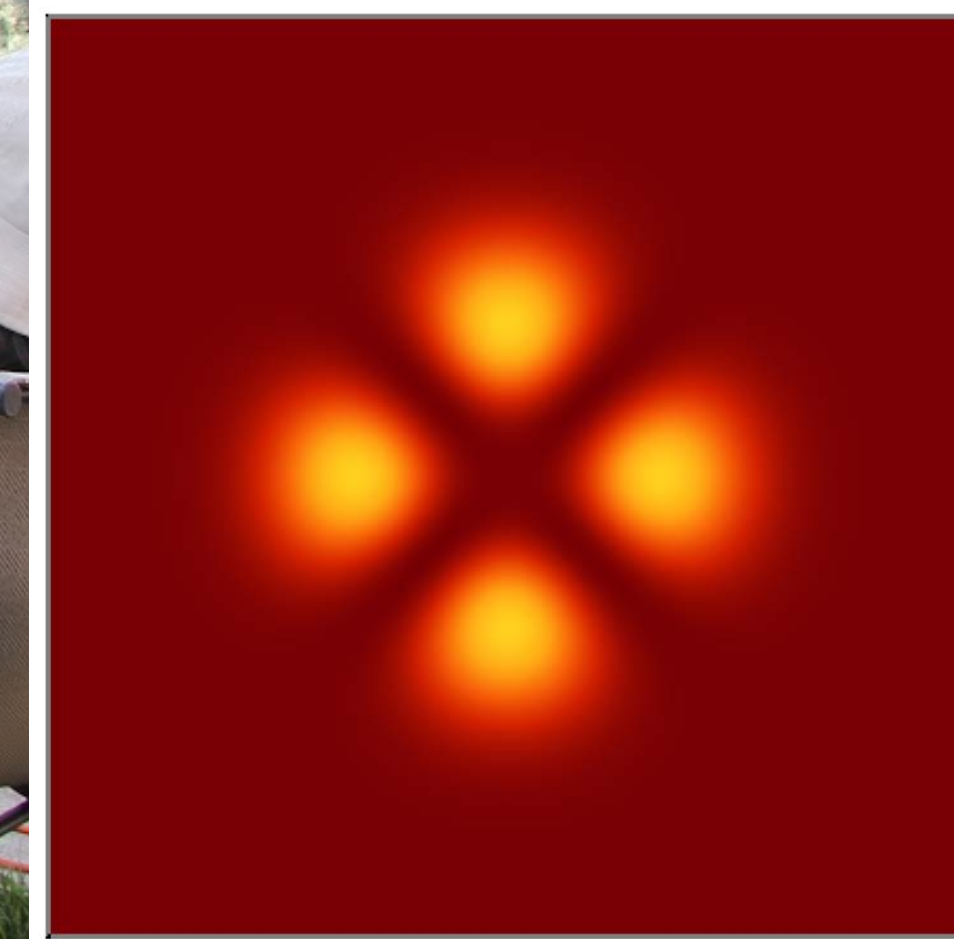
Quantum Key Distribution through Underwater Channel



sqogroup.c



Quantum Key Distribution through Underwater Channel



sqogroup.c

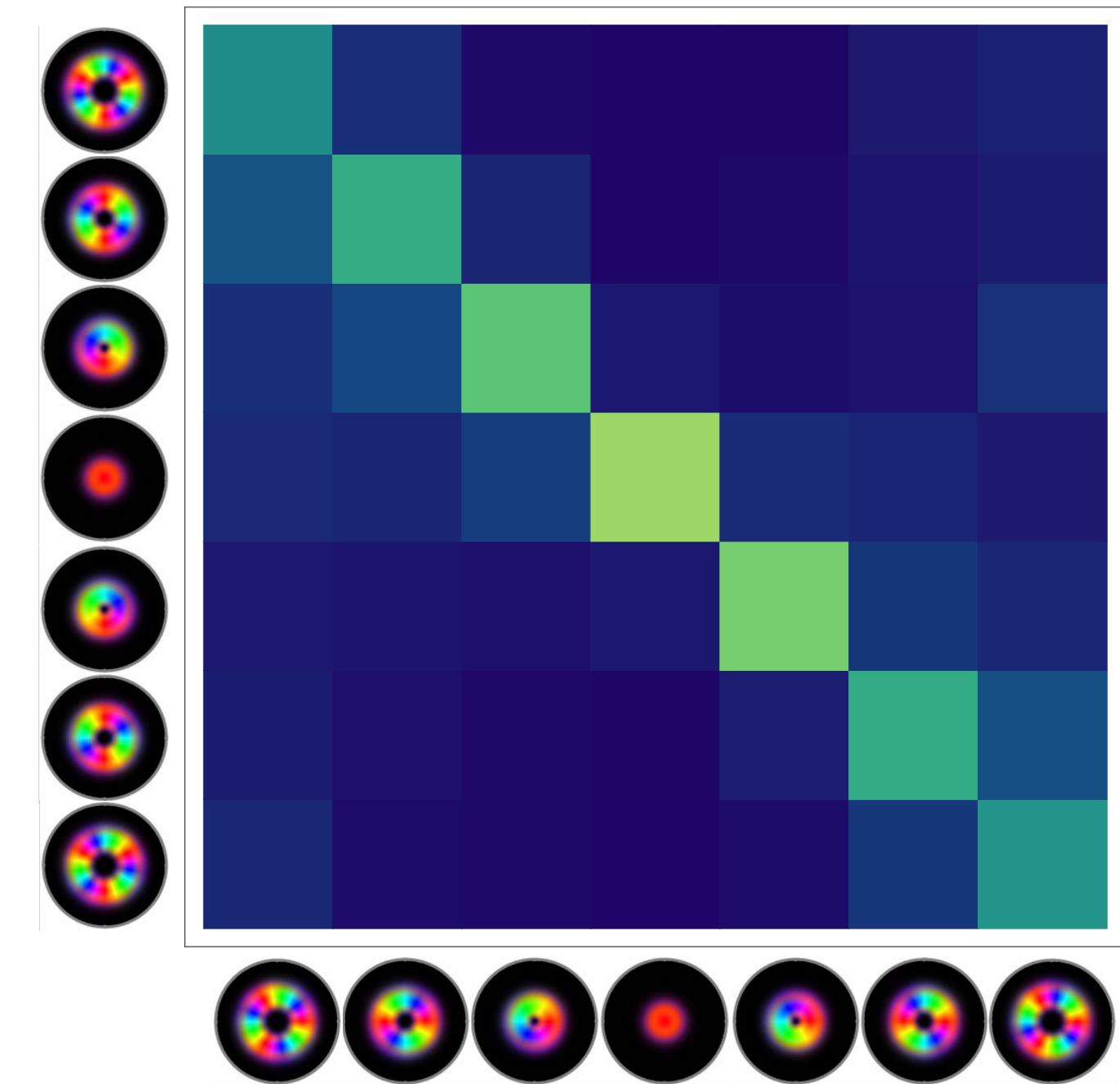
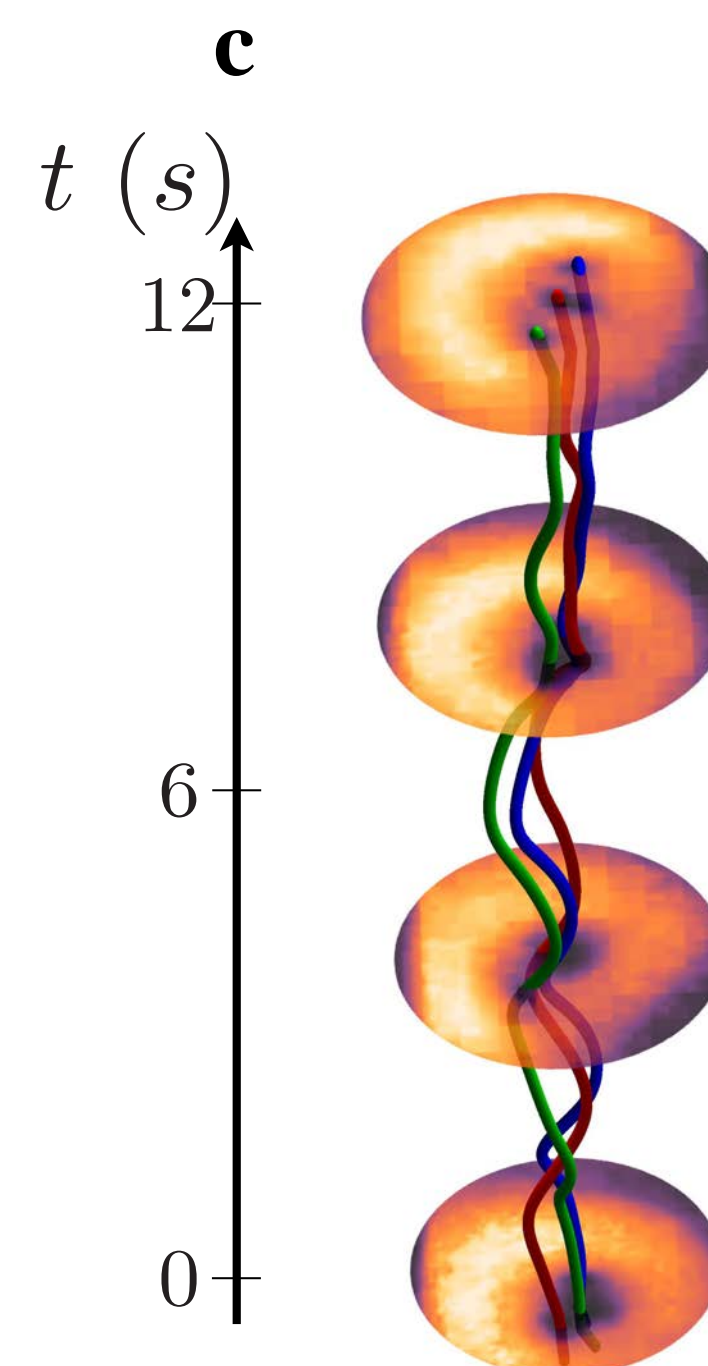
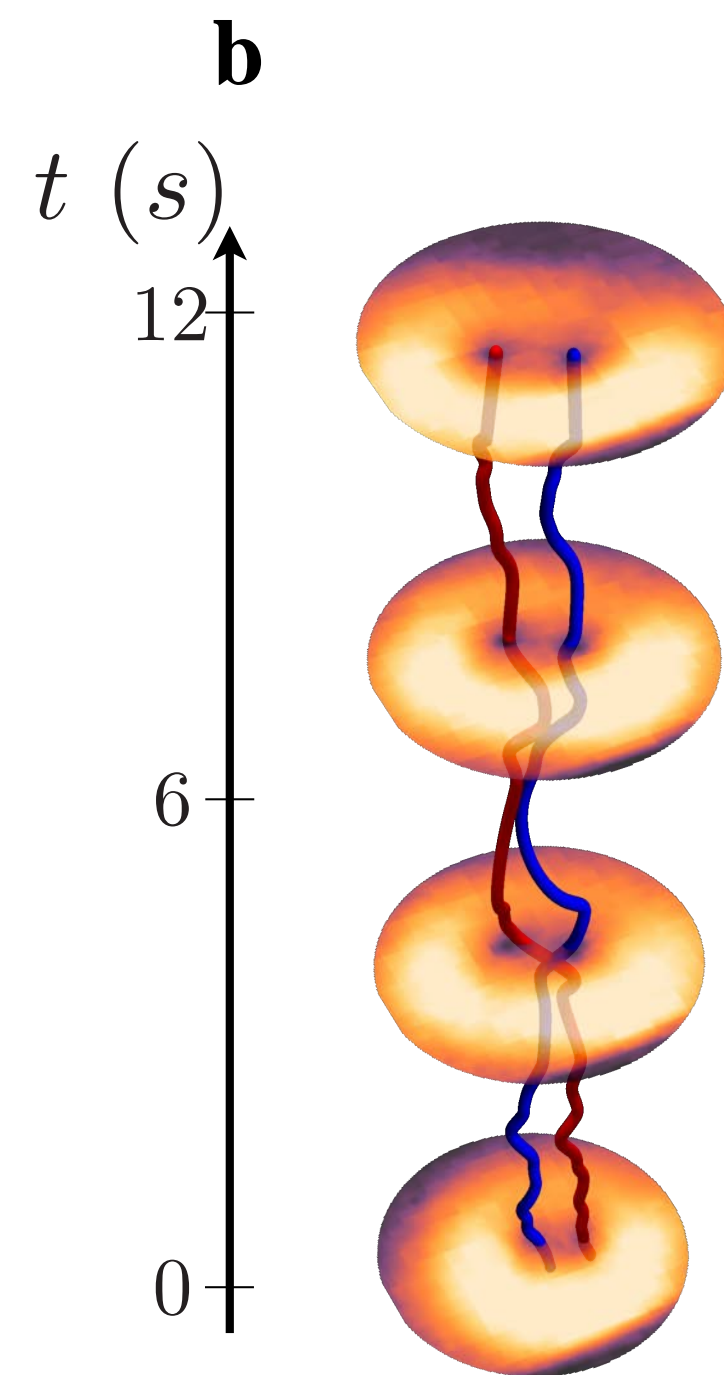
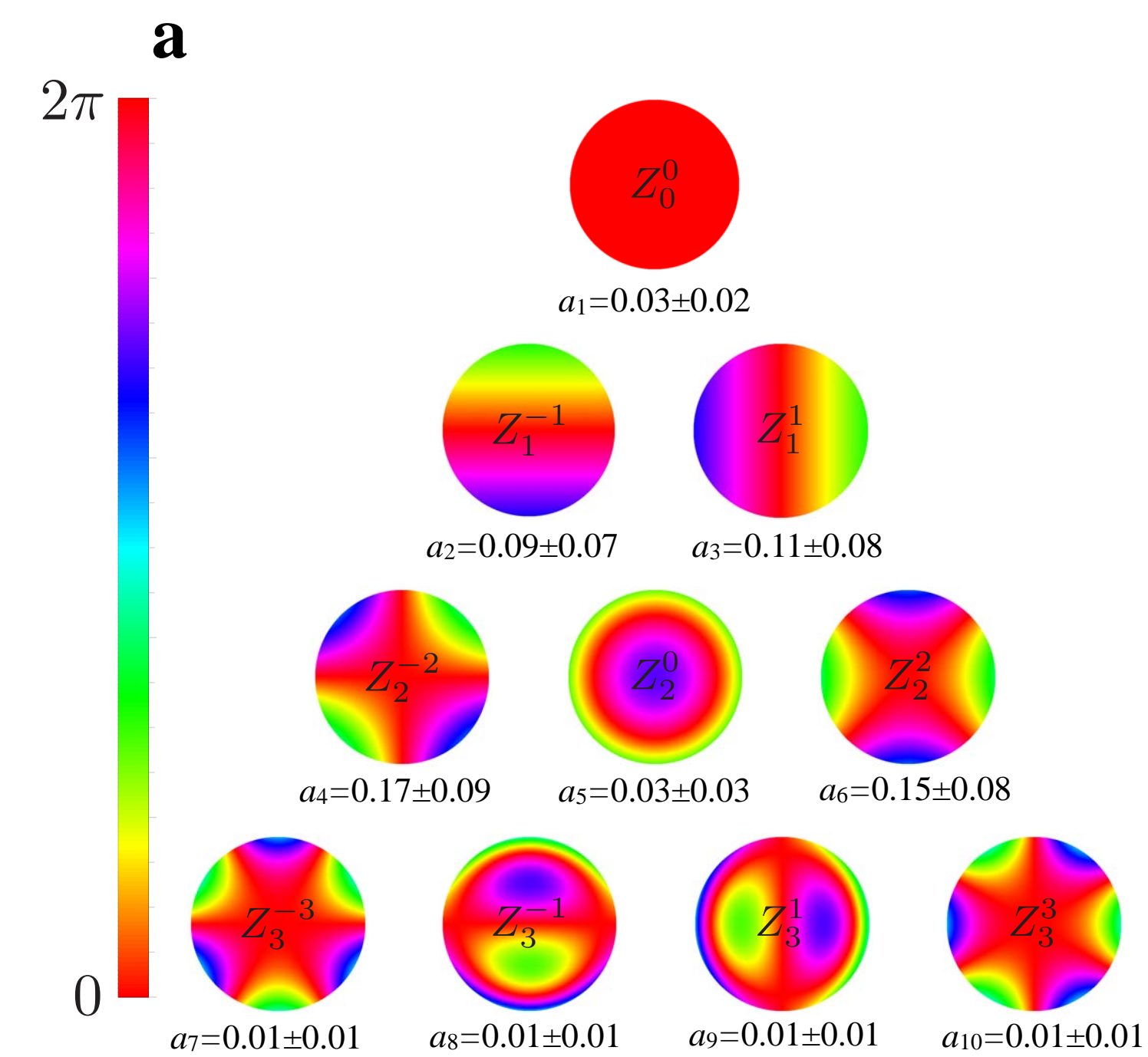
Quantum Key Distribution through Underwater Channel



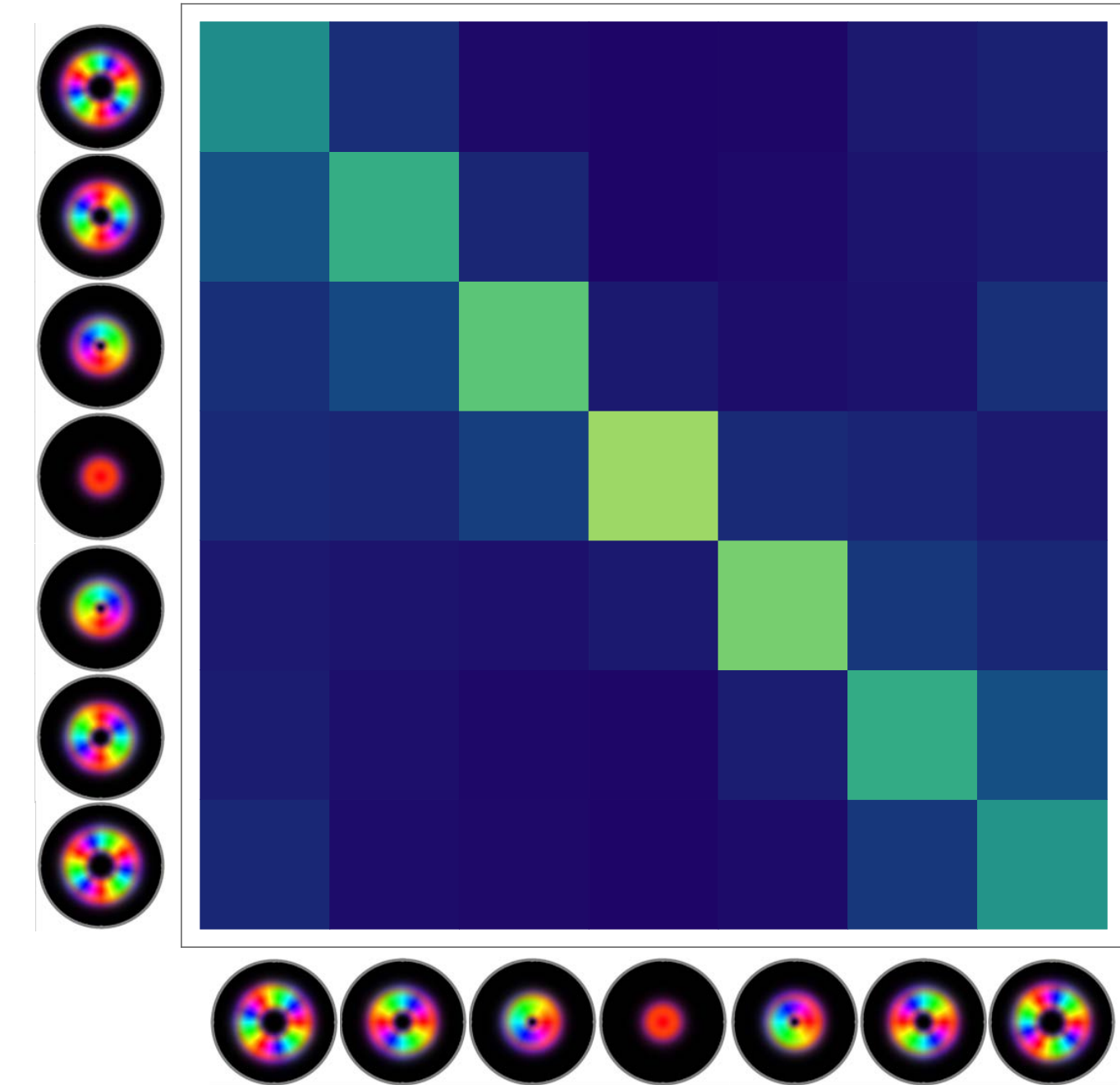
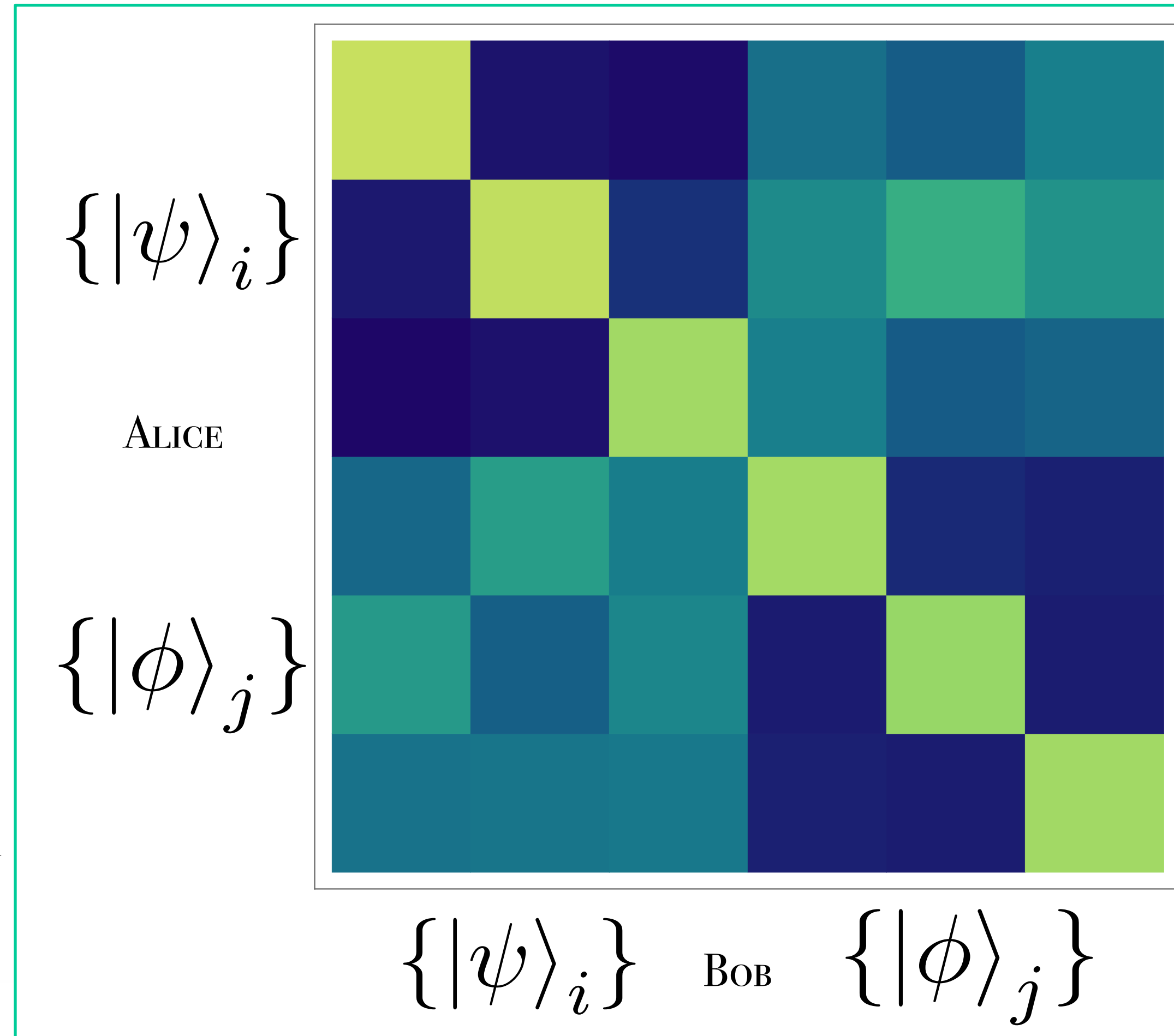
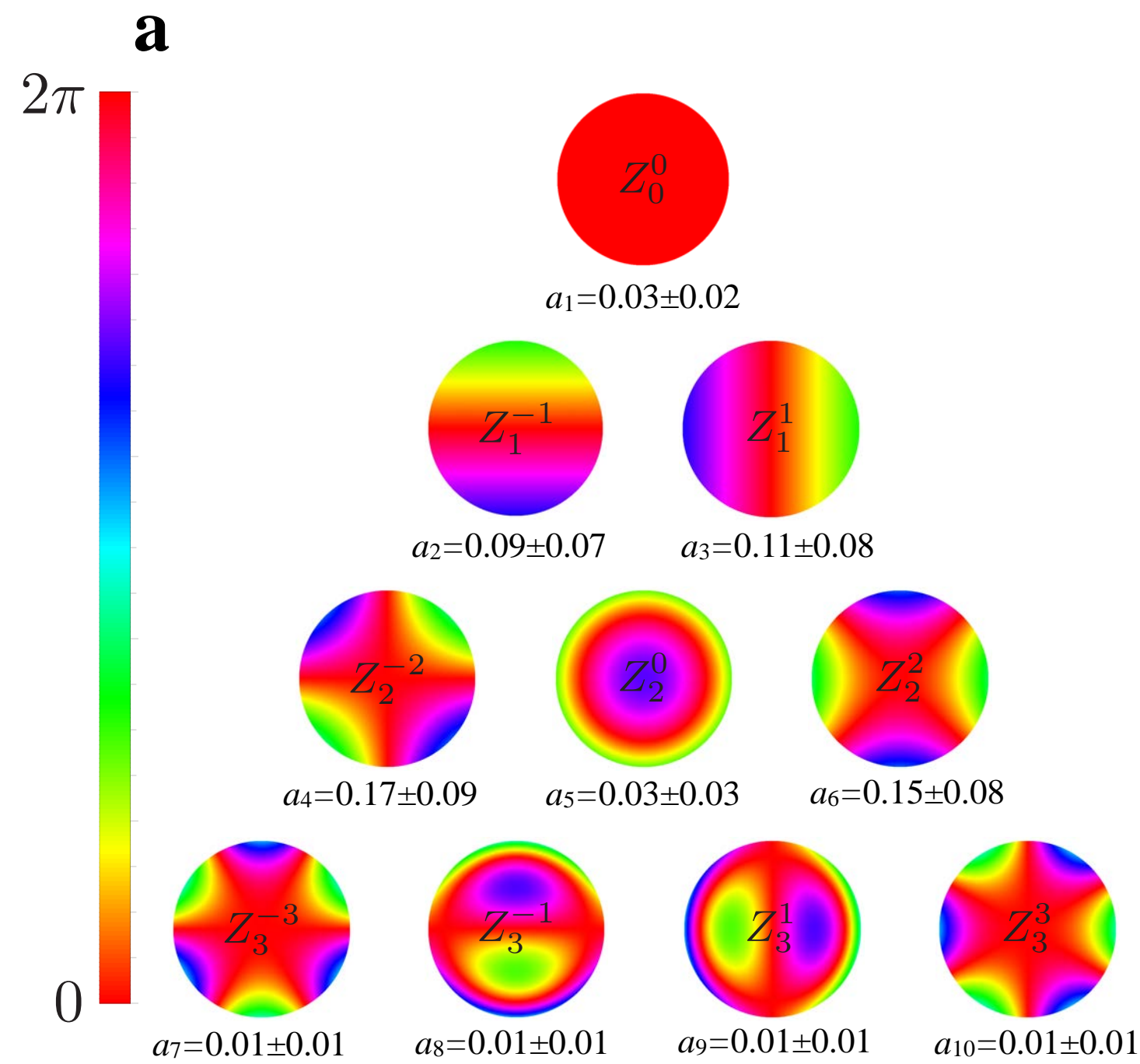
sqogroup.c



Quantum Key Distribution through Underwater Channel



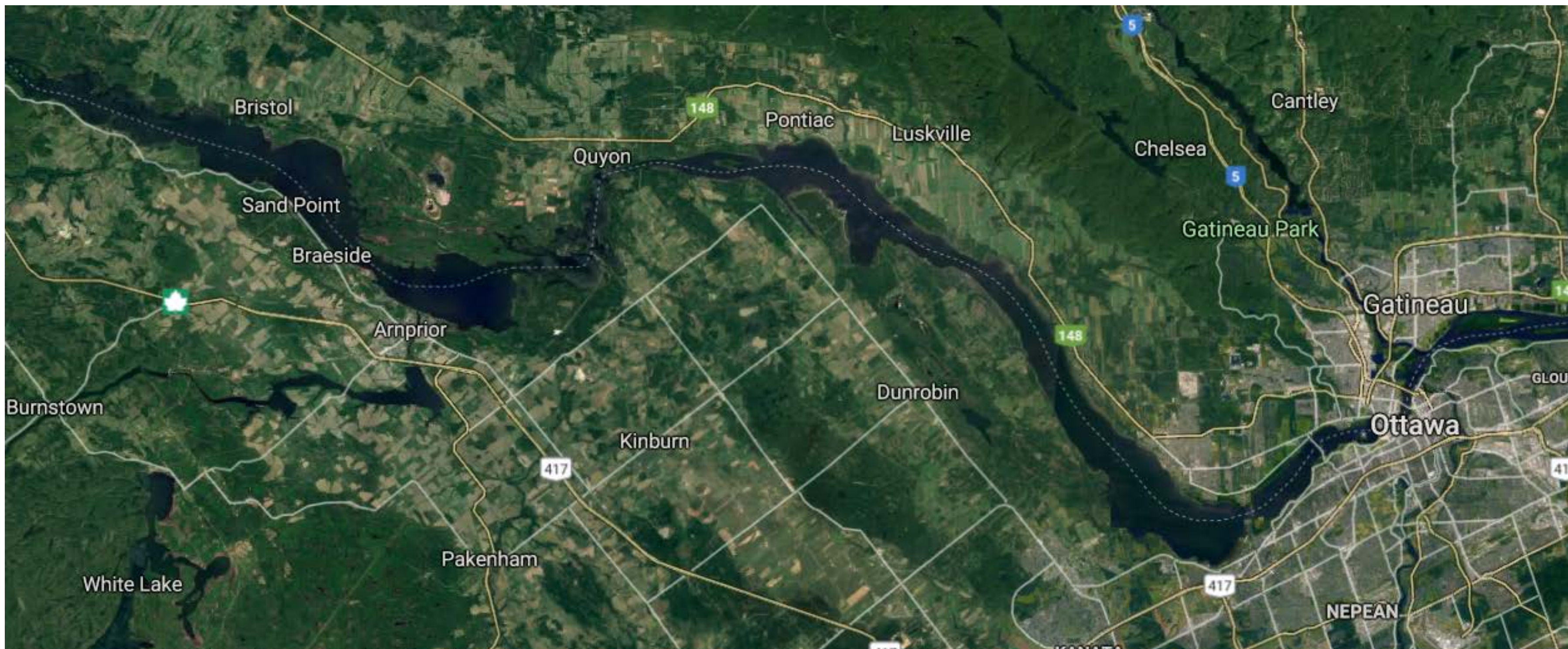
Quantum Key Distribution through Underwater Channel



3D 0.302 Bits per Photon
11.7% Quantum Bit Error Rate



Underwater Quantum Cryptography in the Ottawa River

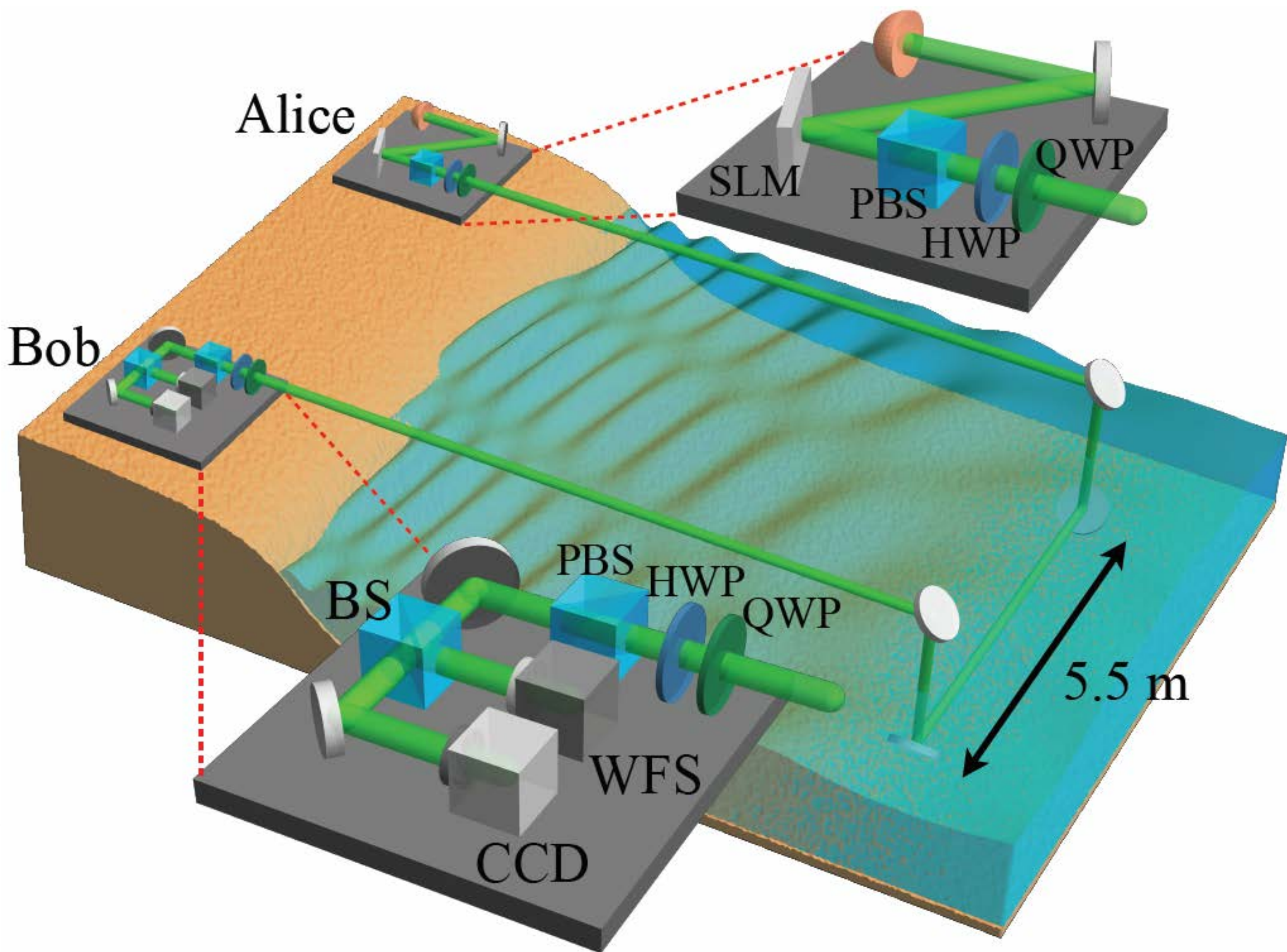


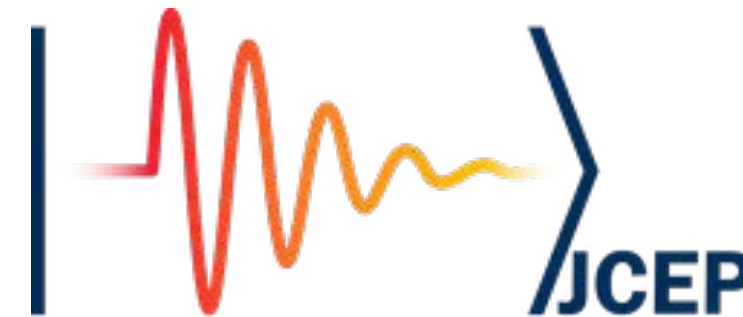
Underwater Quantum Cryptography in the Ottawa River



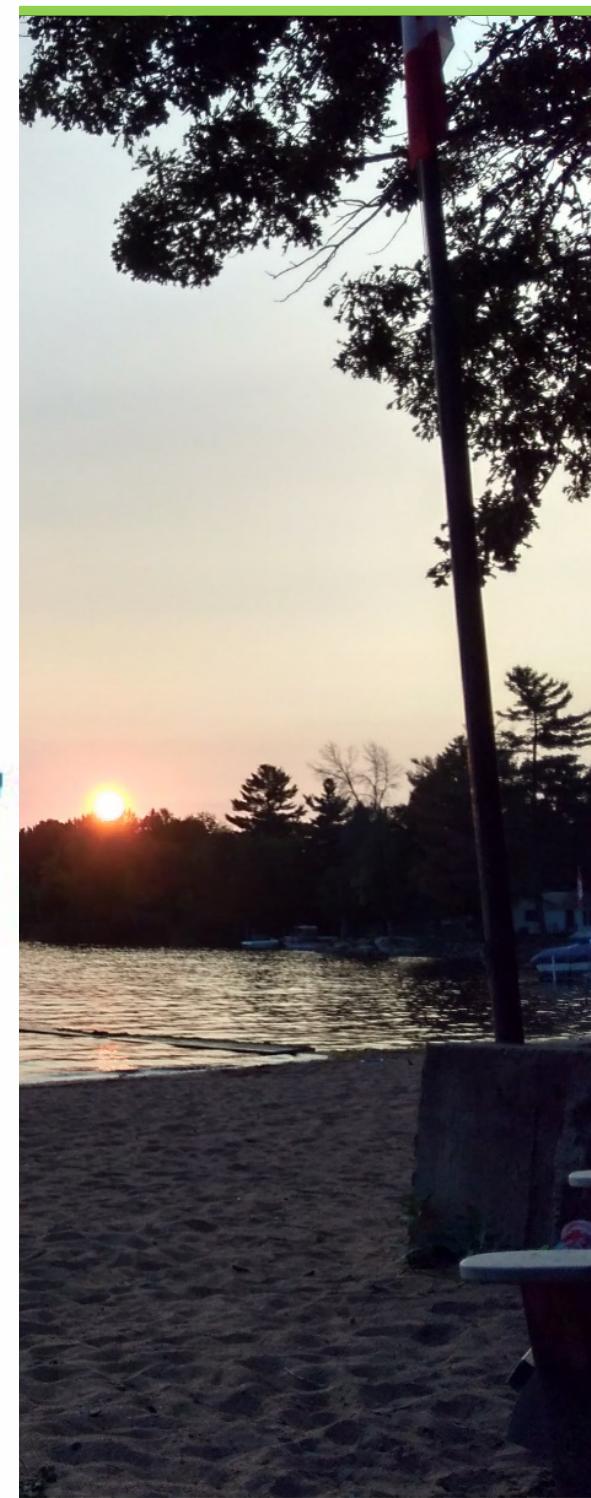
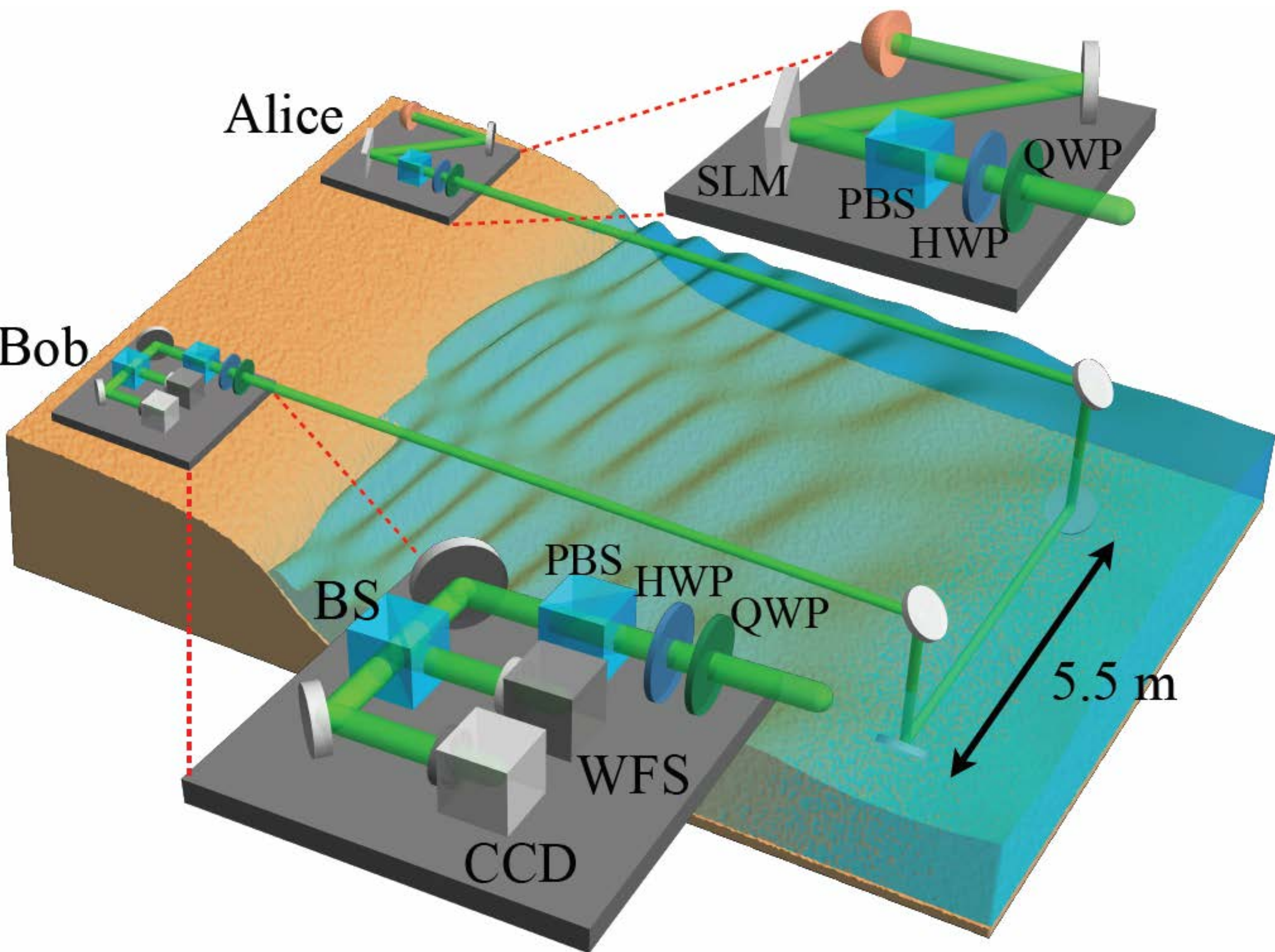


Underwater Quantum Cryptography in the Ottawa River





Underwater Quantum Cryptography in the Ottawa River

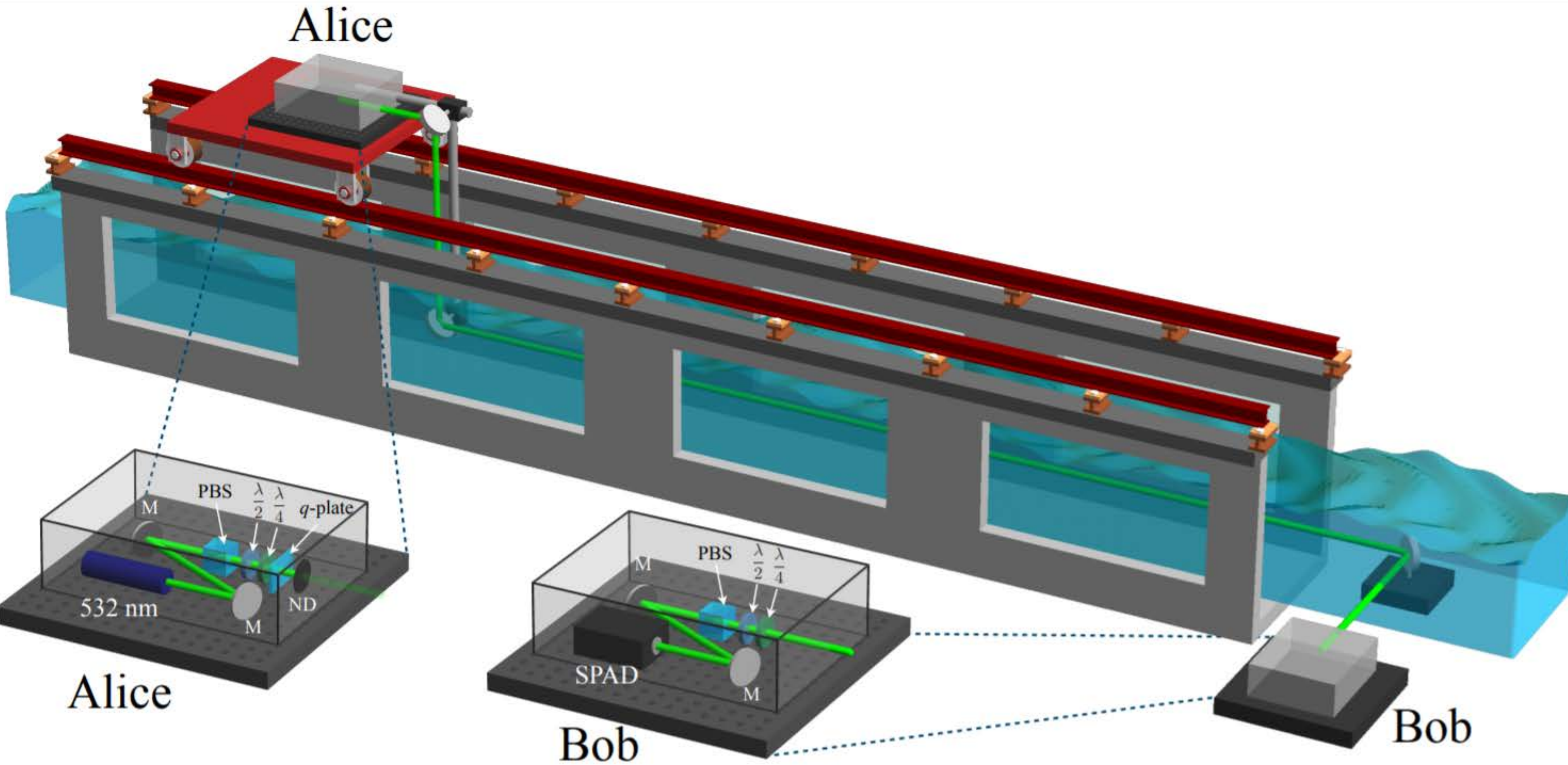


$ H\rangle$	0.93	0.06	0.40	0.59
$ V\rangle$	0.02	0.97	0.45	0.54
$ A\rangle$	0.49	0.50	0.97	0.03
$ D\rangle$	0.53	0.47	0.04	0.96
	$ H\rangle$	$ V\rangle$	$ A\rangle$	$ D\rangle$



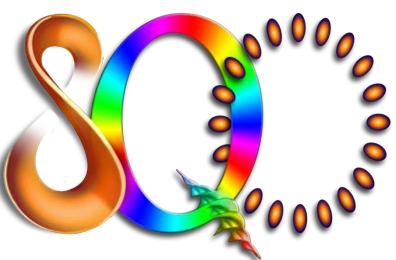
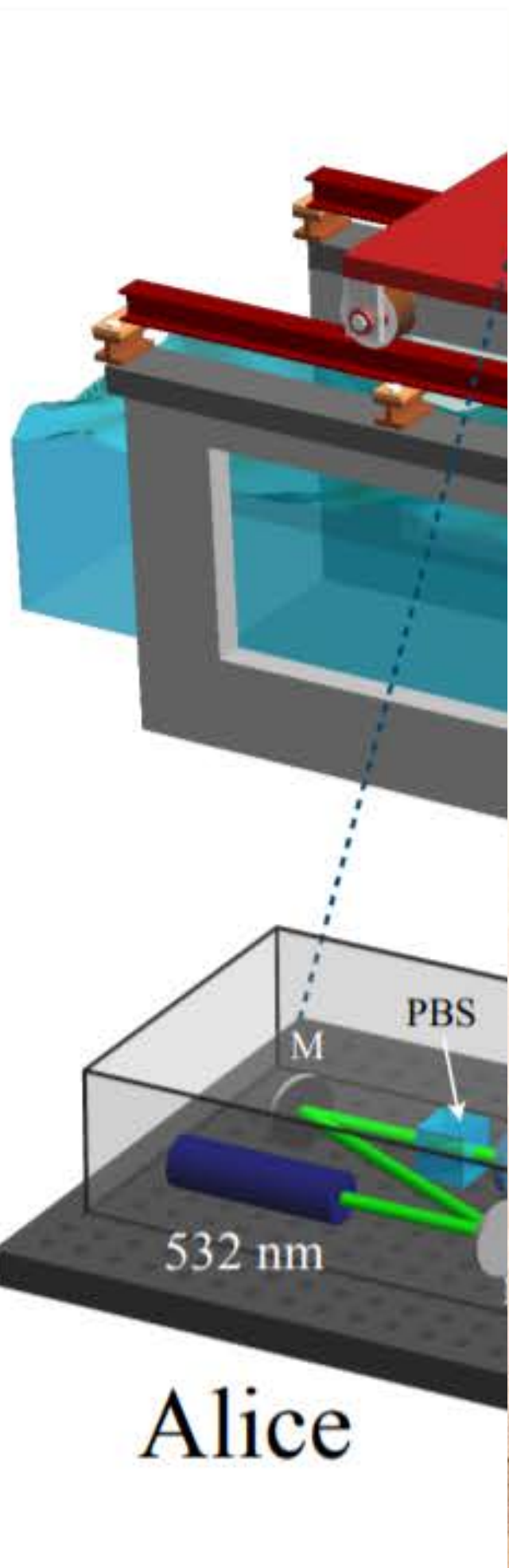


Underwater Quantum Cryptography in the NRC Flumes



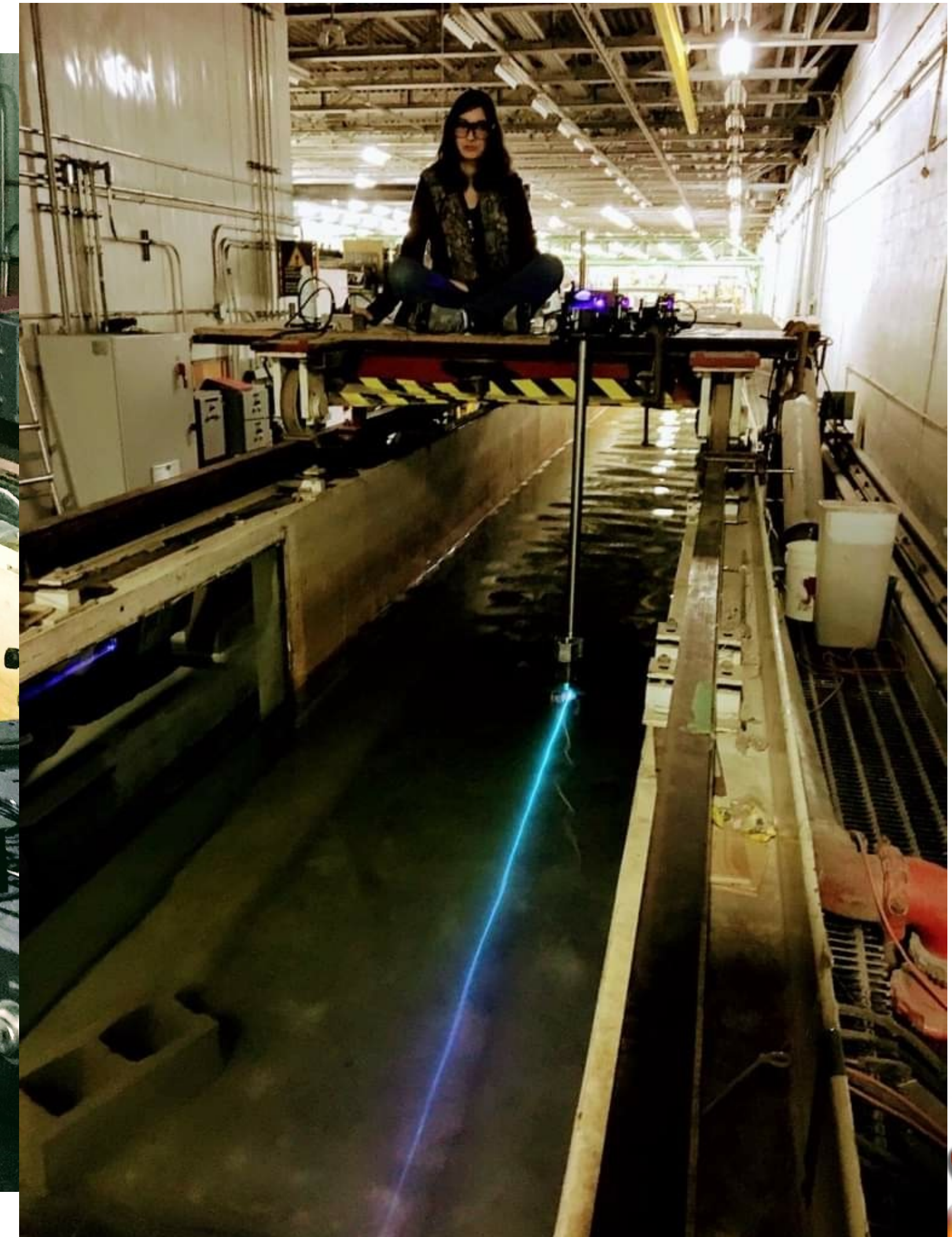
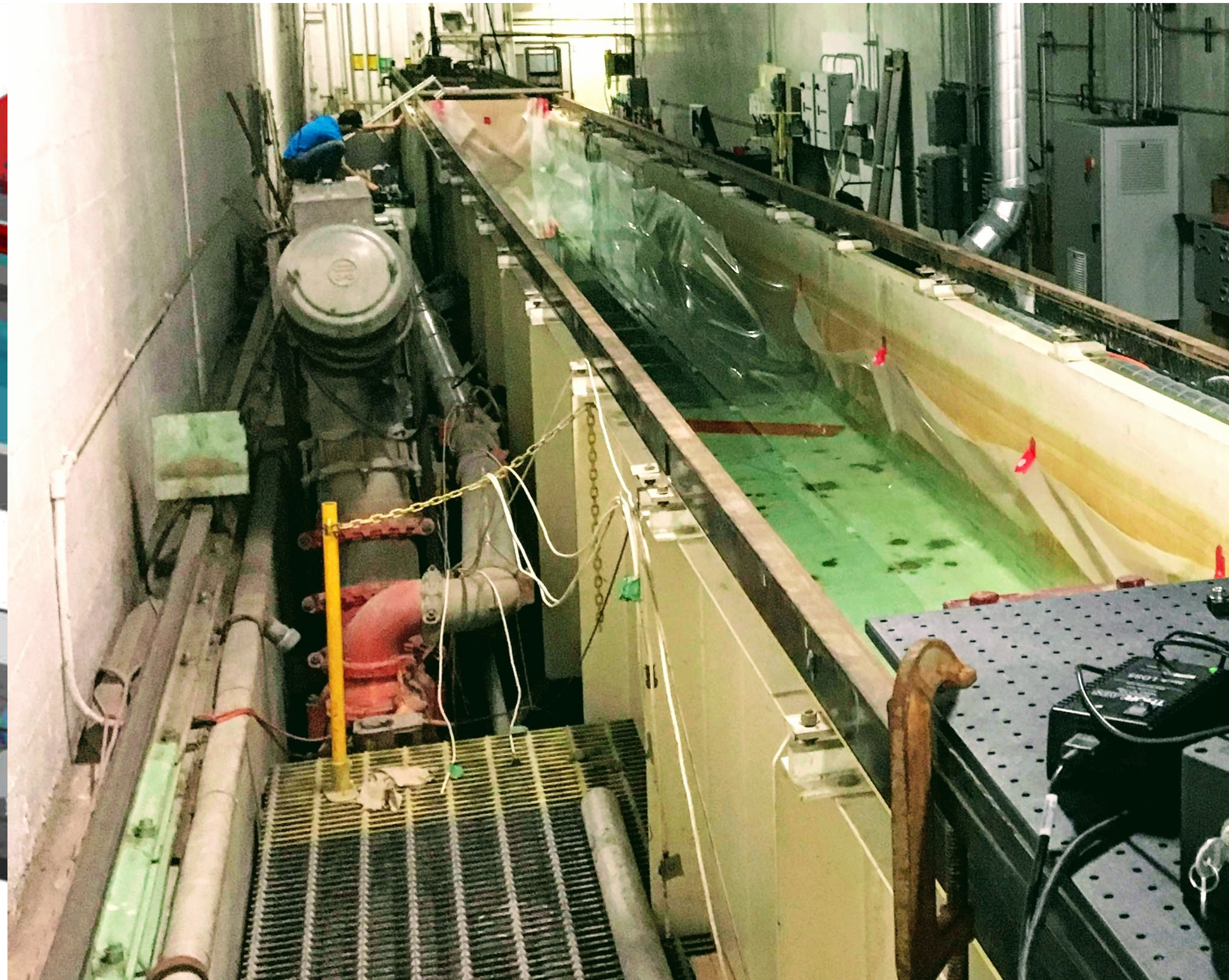
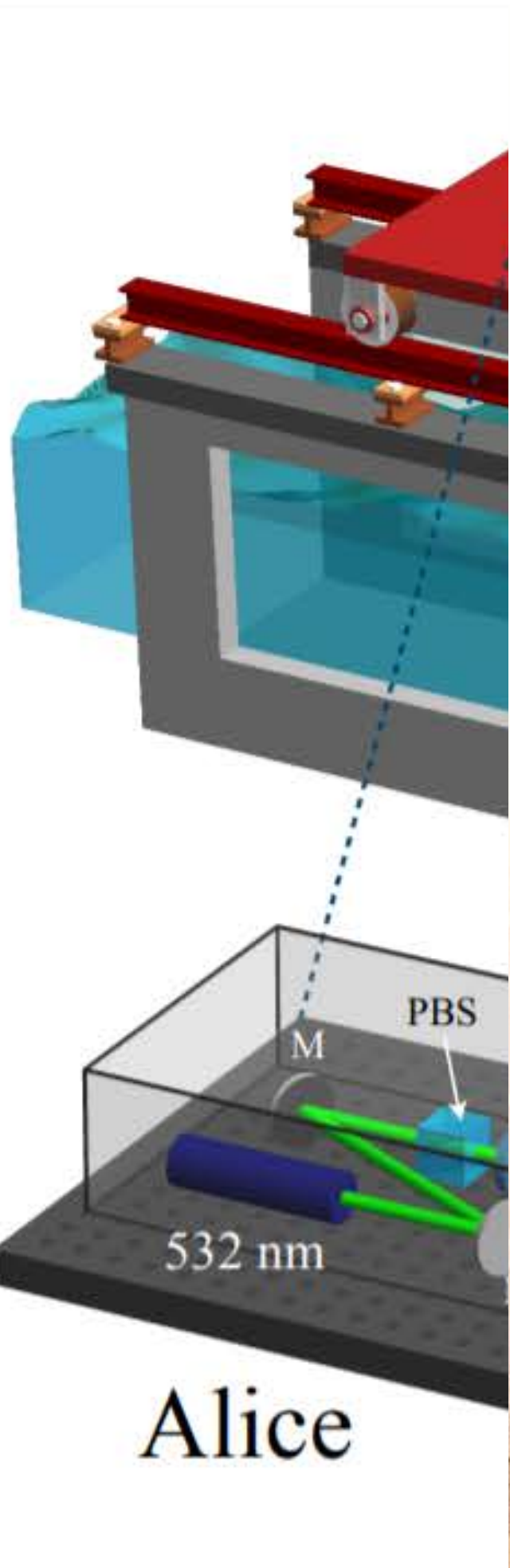


Underwater Quantum Cryptography in the NRC Flumes



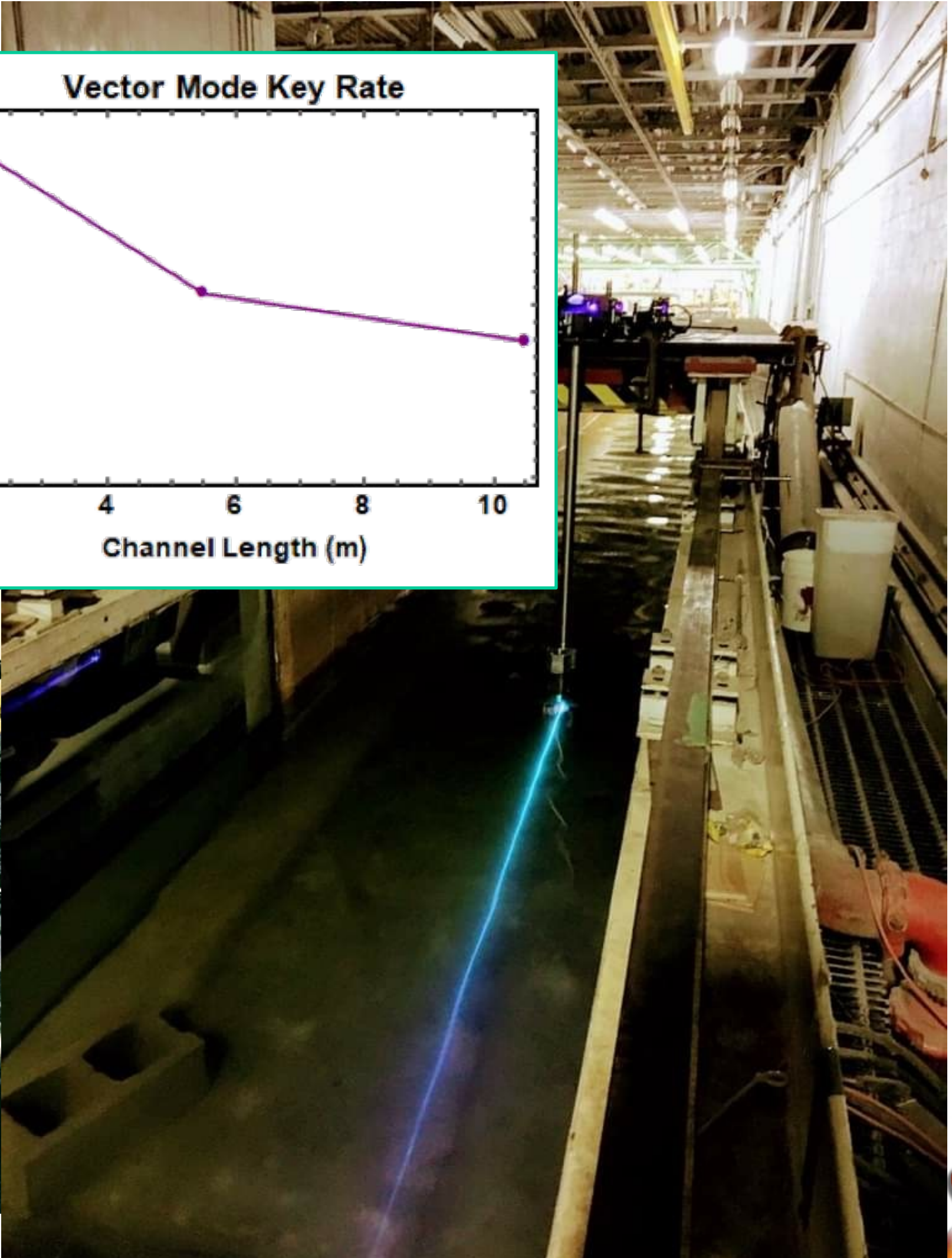
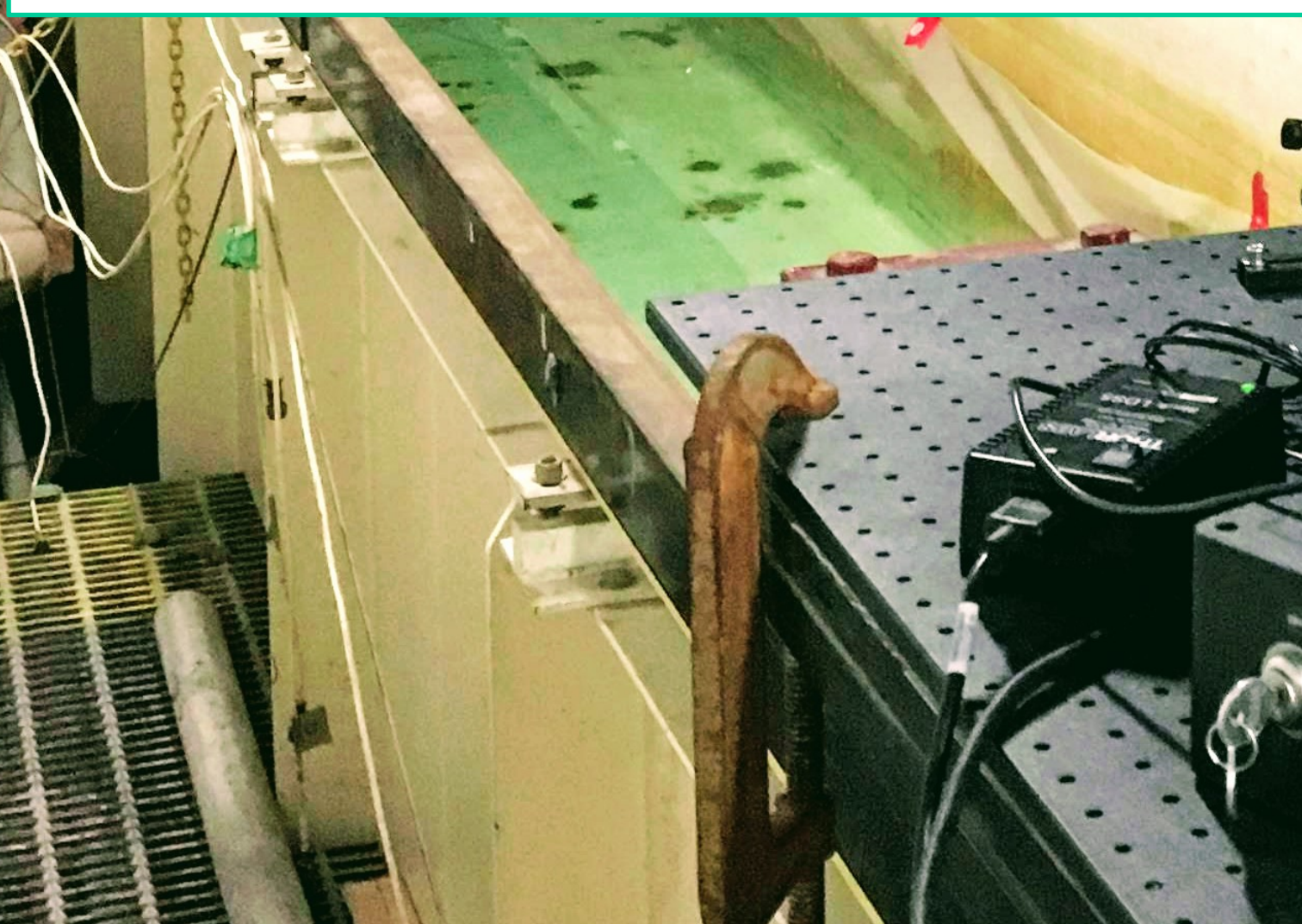
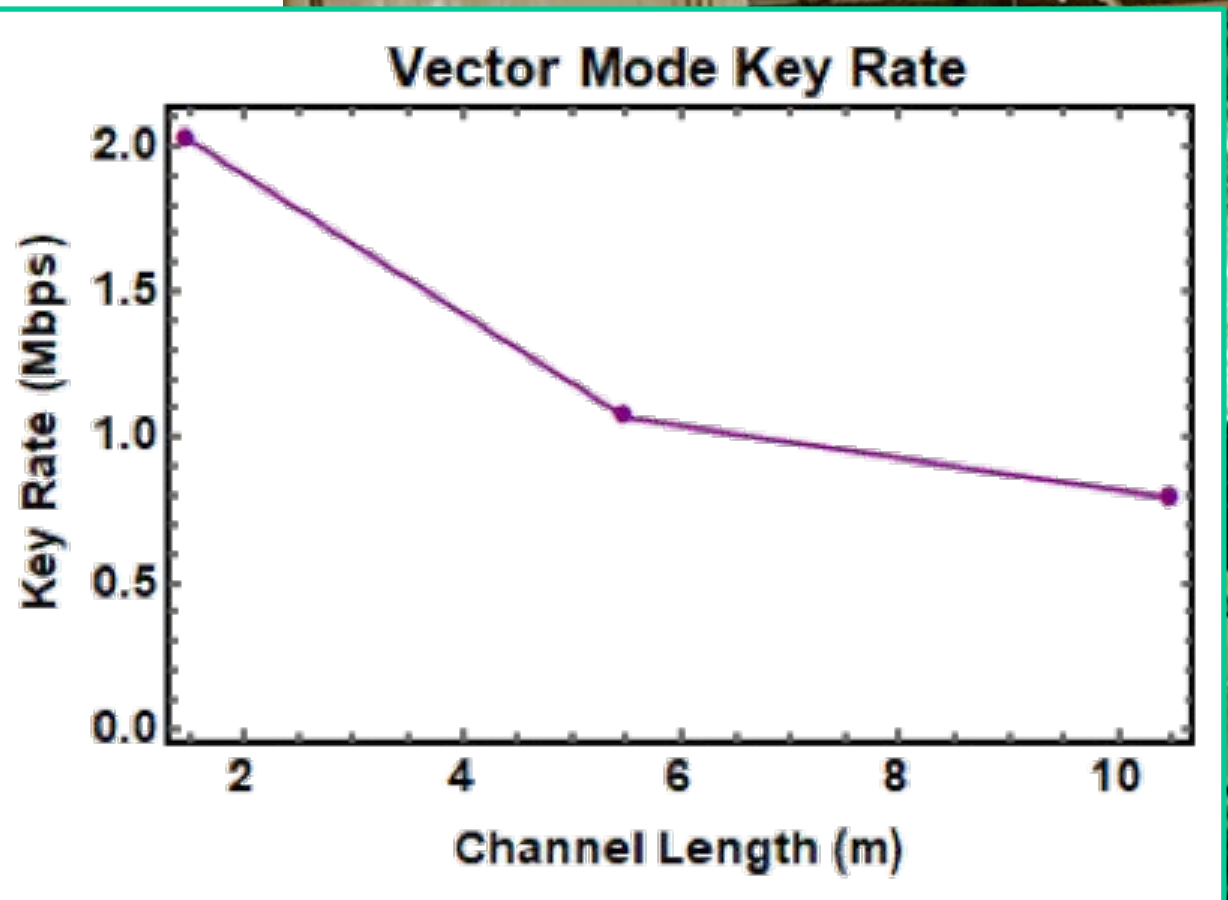
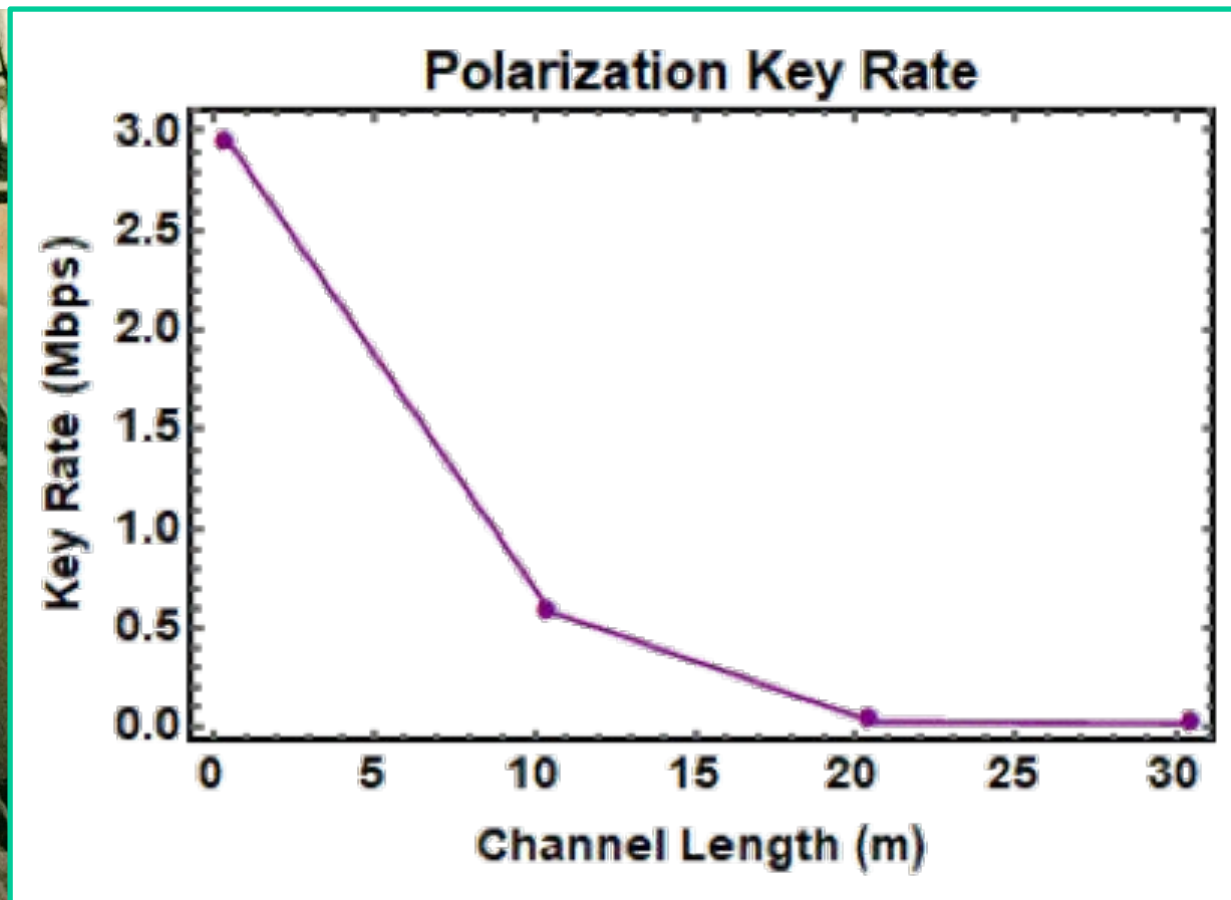
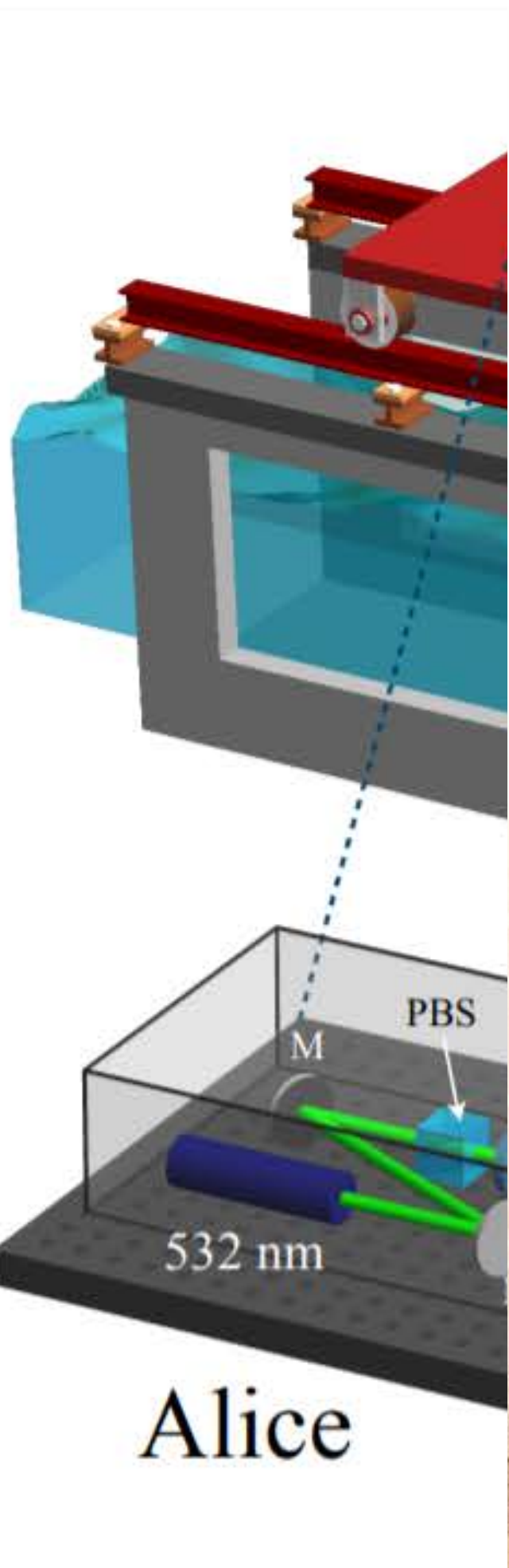


Underwater Quantum Cryptography in the NRC Flumes



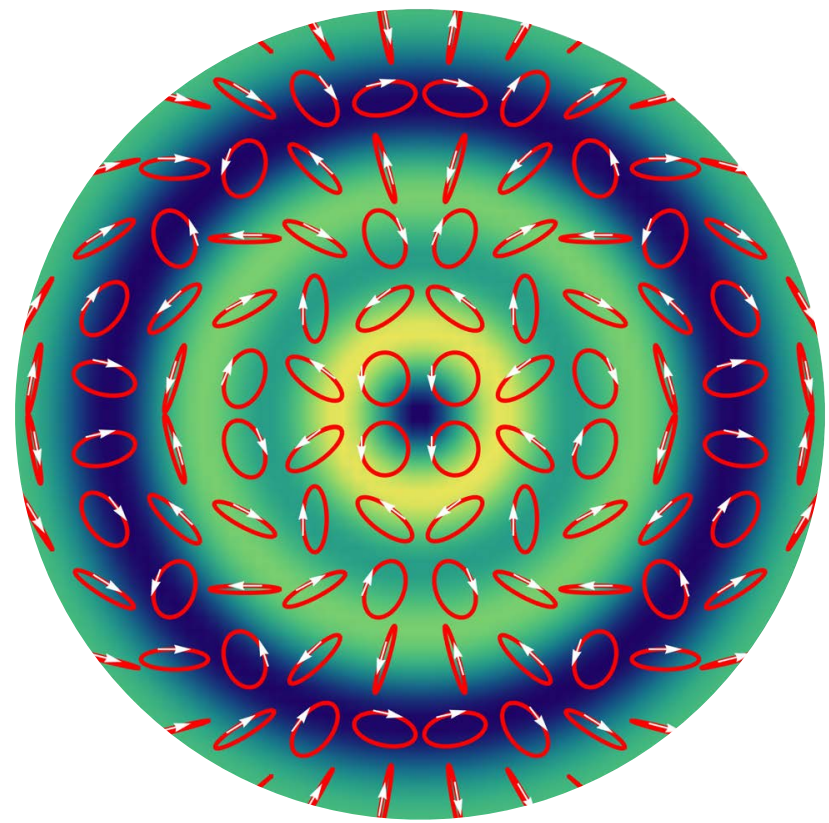


Underwater Quantum Cryptography in the NRC Flumes

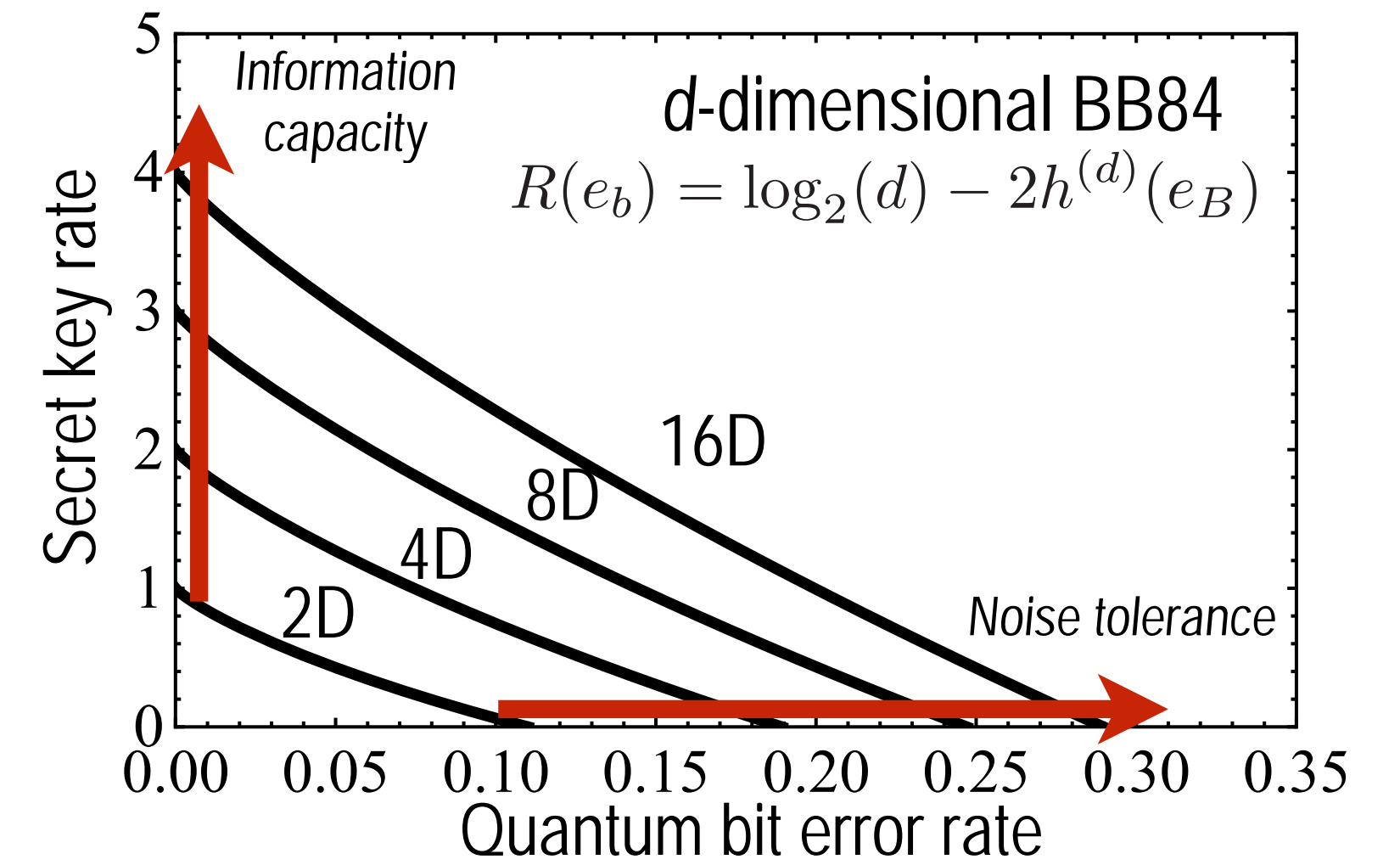


Summary

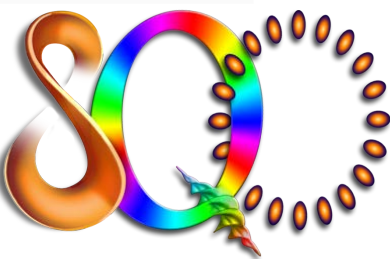
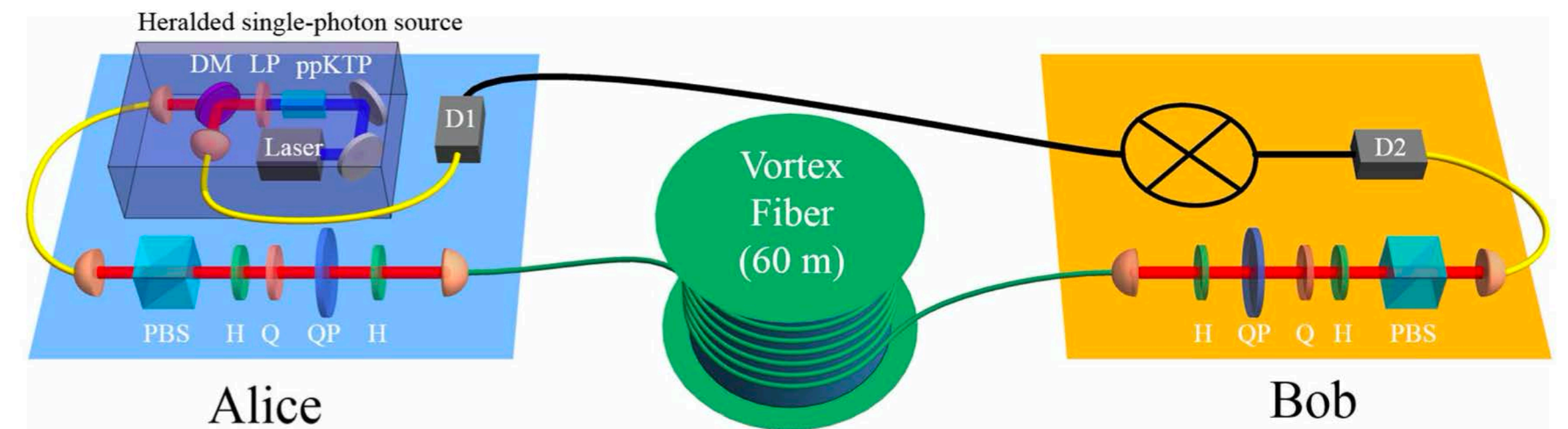
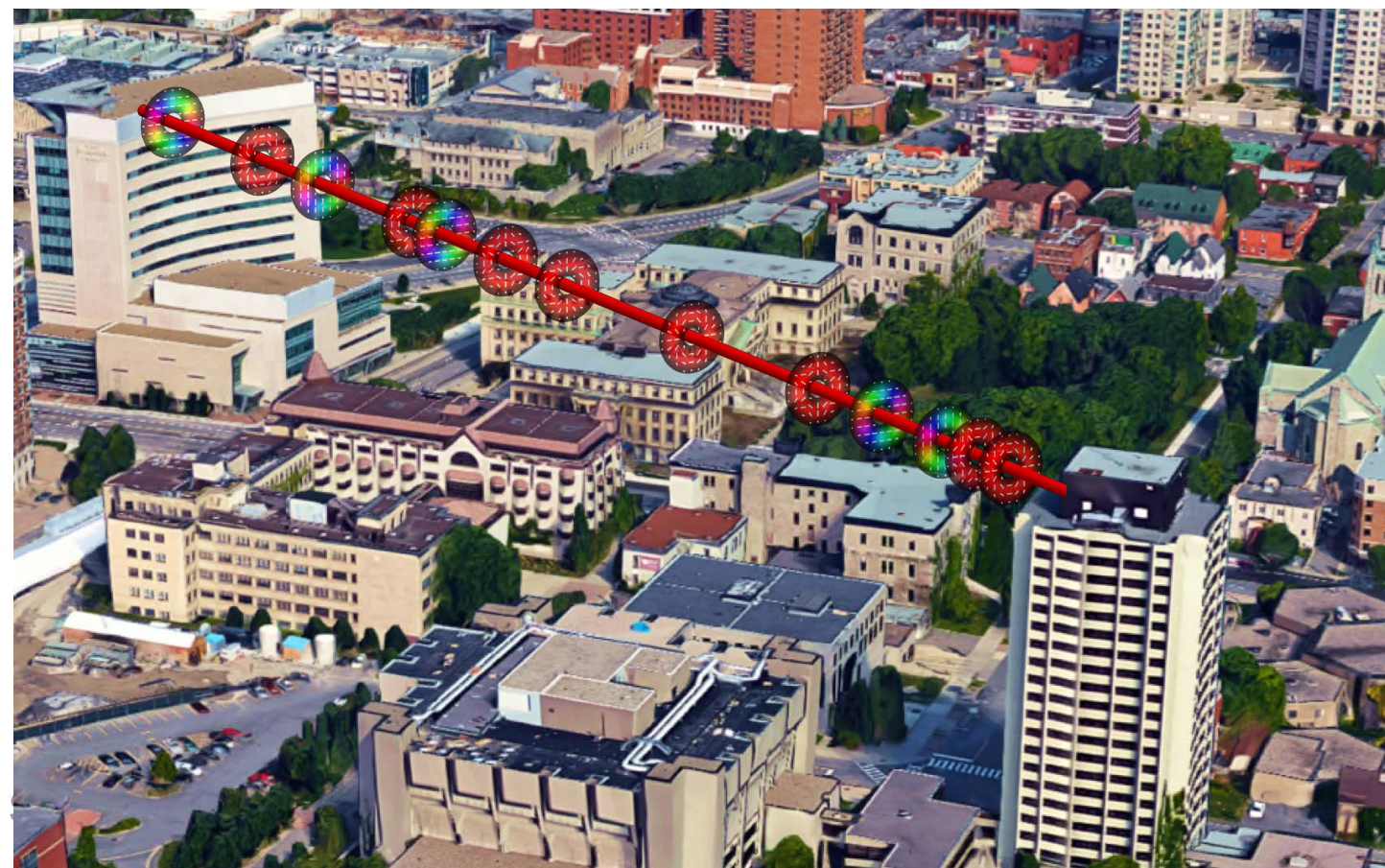
More information per carrier



They are robust in a noisier channel

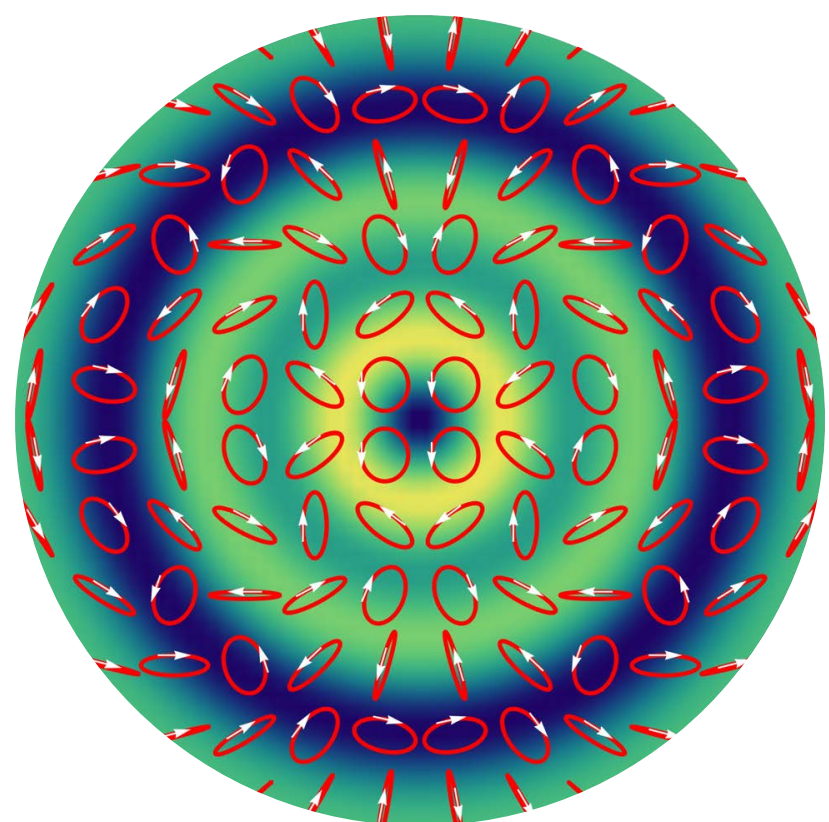


Different quantum channels



Summary

More information per carrier

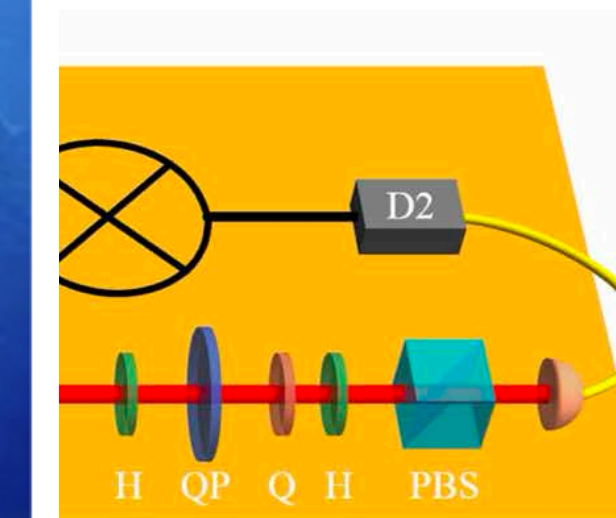
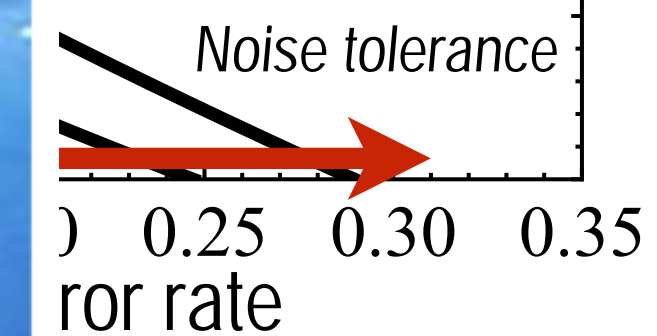


Different quantum channels



er channel

$$C(d) = 2h^{(d)}(e_B)$$



Bob



Funding agencies



Canada Research Chairs

www.chairs-chaire.gc.ca

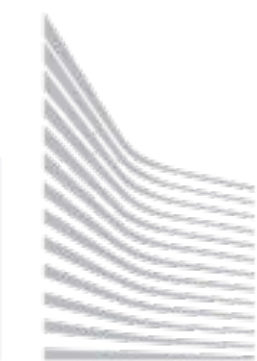


uOttawa

INNOVATION.CA

CANADA FOUNDATION FOR INNOVATION

FONDATION CANADIENNE POUR L'INNOVATION



European Commission

Horizon 2020
European Union funding for Research & Innovation



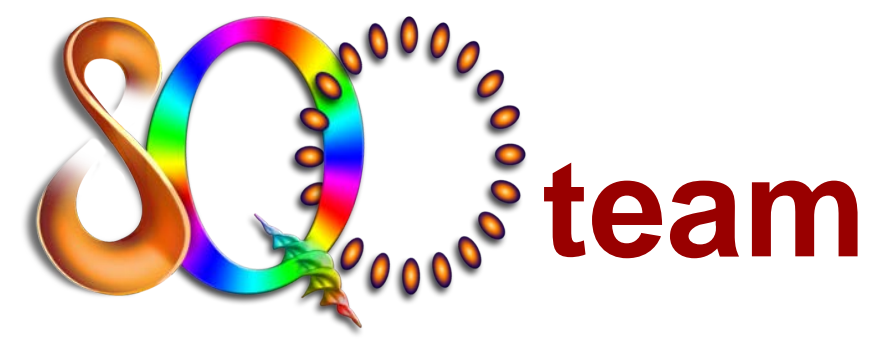
CANADA FIRST
RESEARCH EXCELLENCE FUND

APOGÉE CANADA
FONDS D'EXCELLENCE EN RECHERCHE



NSERC
CRSNG





Prof Ebrahim Karimi
Canada Research Chair



Dr Farshad Nejadiattari
Postdoctoral Fellow



Dr Sergey Nechayev
Postdoctoral Fellow



Alicia Sit
PhD student - Vanier Scholar



Fatimah Alsaiari
PhD student



Sajedah Shahbazi
PhD student



Dr Mohammadreza Rezaee
Postdoctoral Fellow (Mitacs)



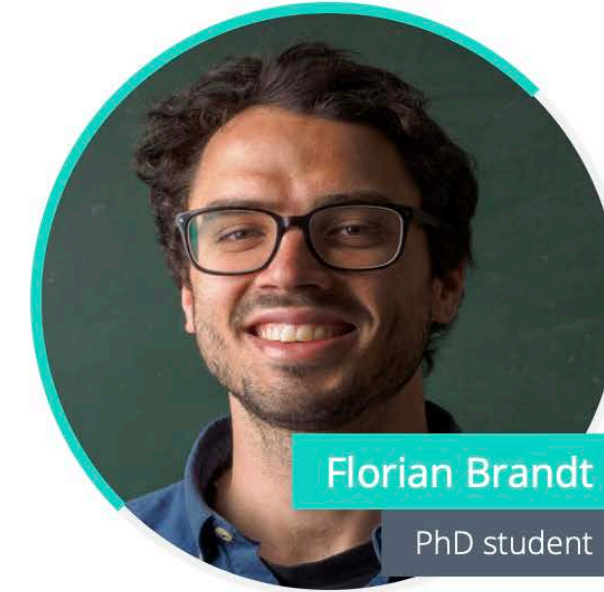
Dr Alessio D'Errico
Postdoctoral Fellow



Dr Qasem Exirifard
Visiting Researcher



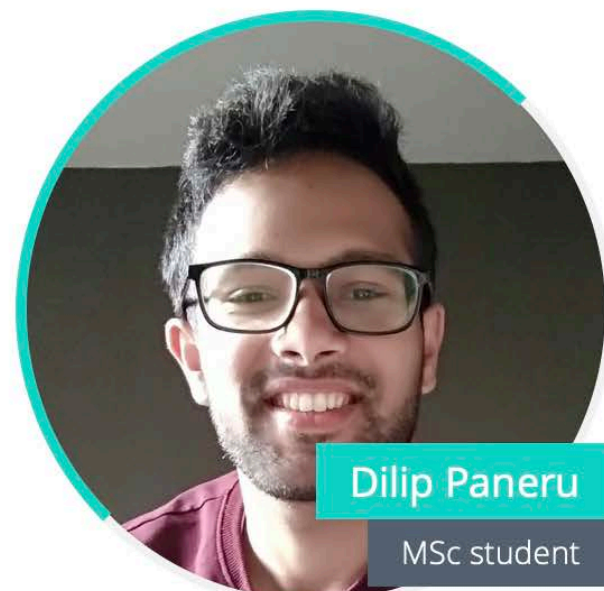
Manuel Ferrer
PhD student



Florian Brandt
PhD student



Felix Hufnagel
MSc student



Dilip Paneru
MSc student



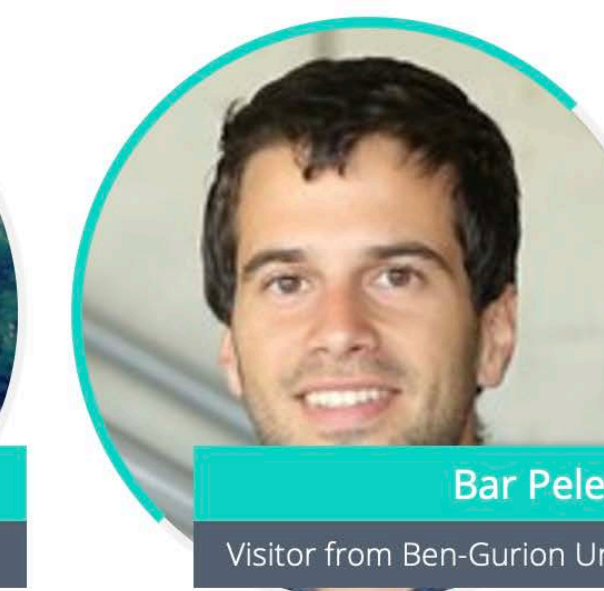
Kevin Mannix
MSc student



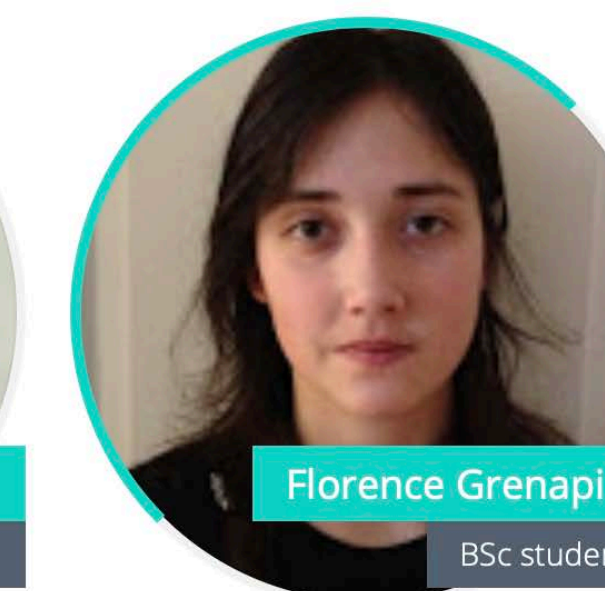
Youesf Alvandi
IASBS-uOttawa PhD student



Sana Booghdachi
IASBS-uOttawa MSc student

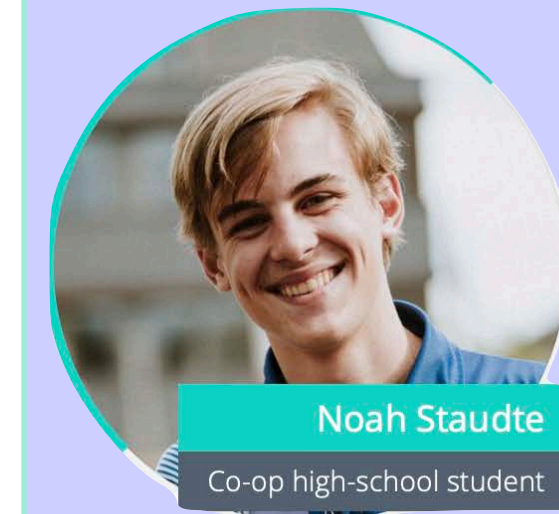


Bar Peled
Visitor from Ben-Gurion Uni.

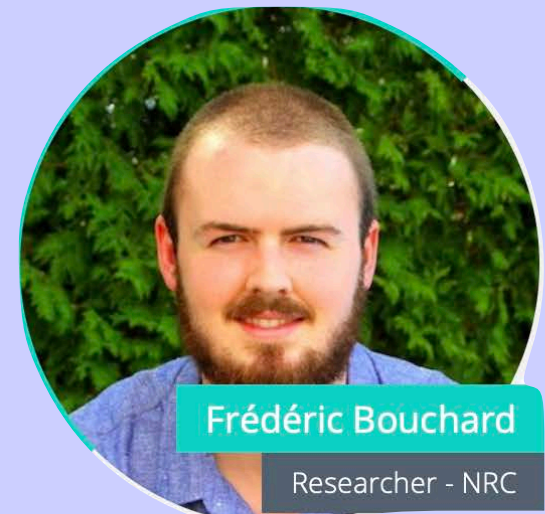


Florence Grenapin
BSc student

last year alumni



Noah Staudte
Co-op high-school student



Frédéric Bouchard
Researcher - NRC



Dr Robert Fickler
Assistant Prof in Tampere University



Hugo Larocque
PhD student MIT



Dr Yingwen Zhang
Researcher - NRC



Dr Eliahu Cohen
Assistant Prof in Bar-Ilan

Collaborators

