Quantum Cryptography with Structured photons

Présenté par : Ebrahim Karimi | Presented by: Ebrahim Karimi

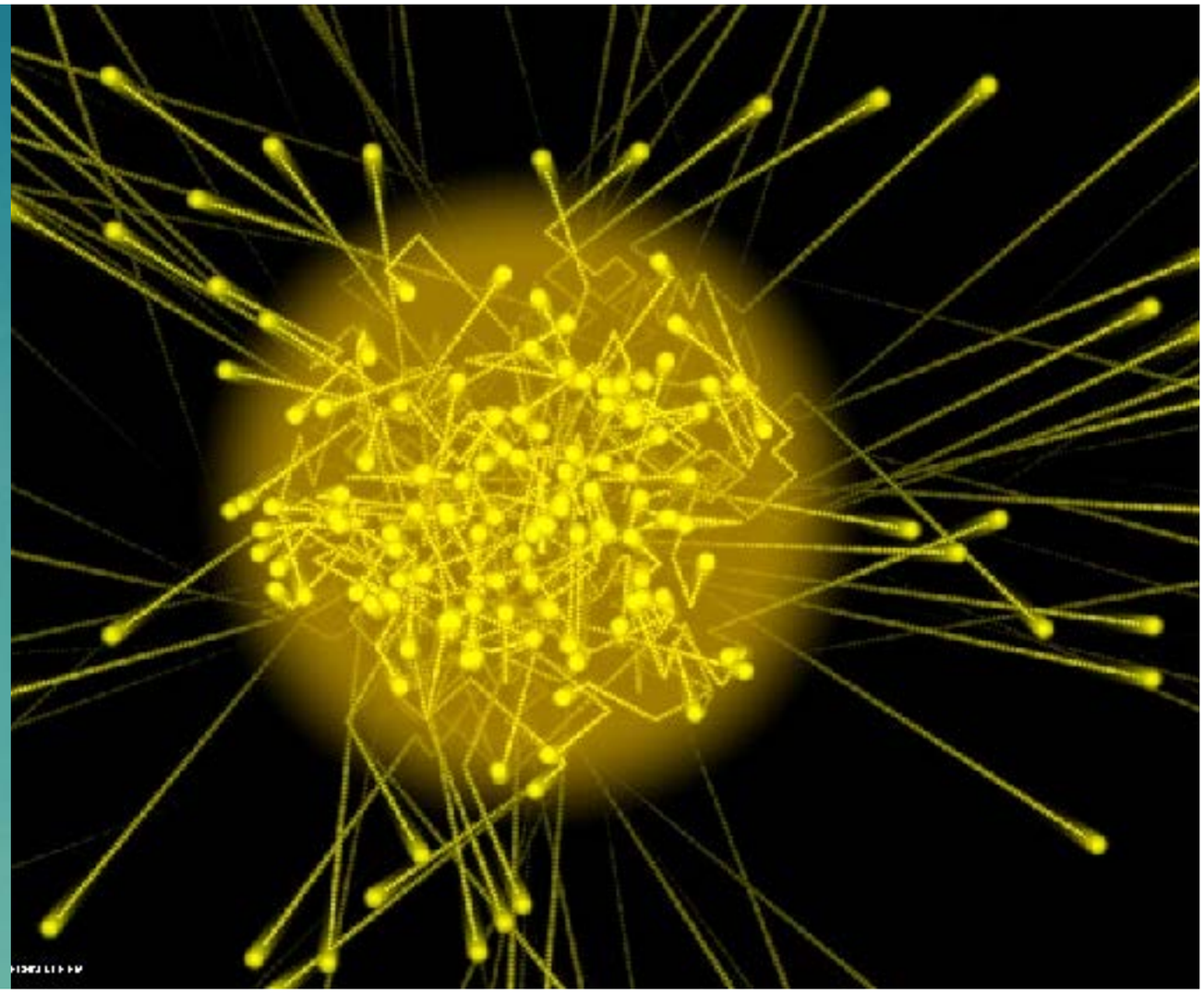
sqogroup.ca

uOttawa

Photon: The Quanta of Light

Photon: The Quanta of Light

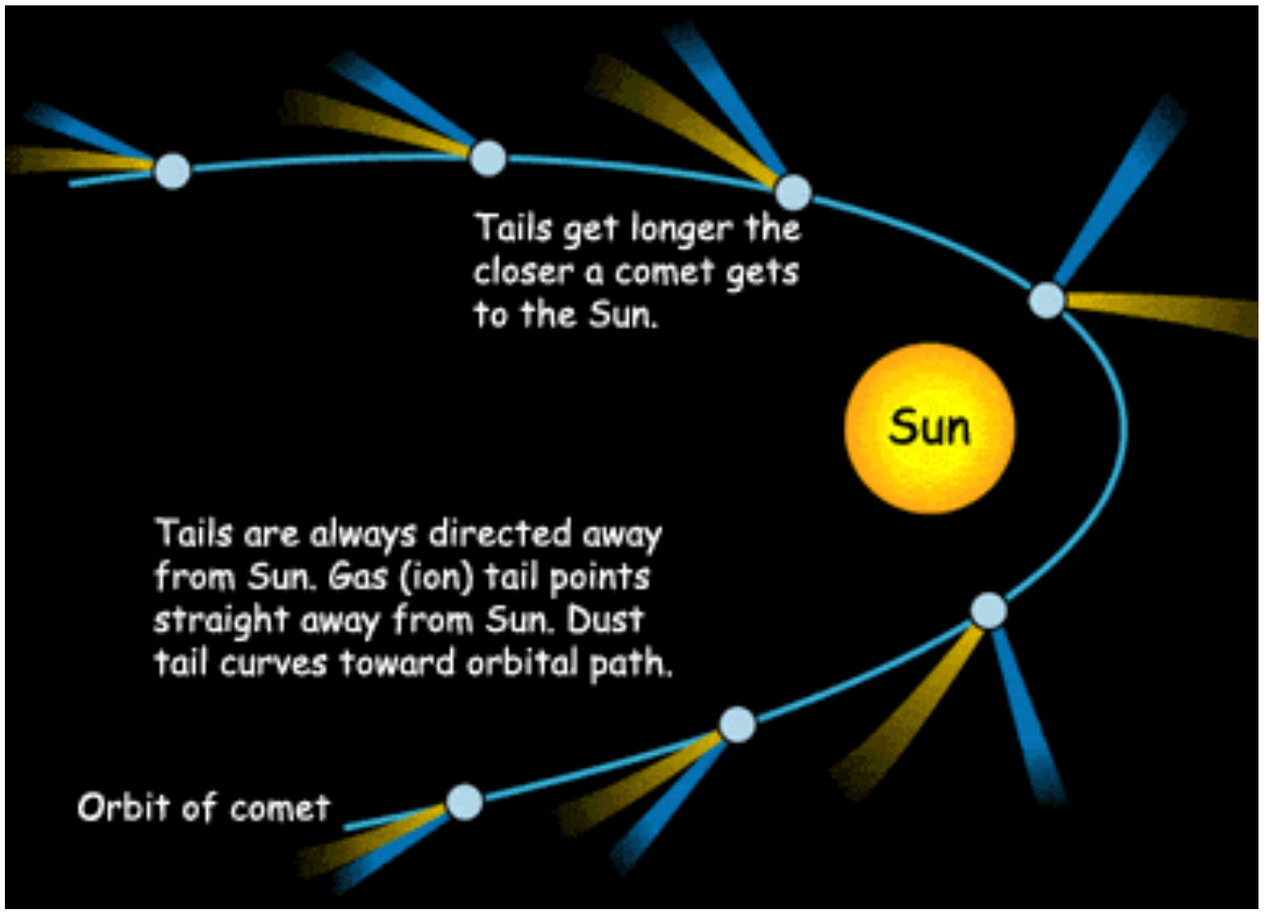
Photon: The Quanta of Light



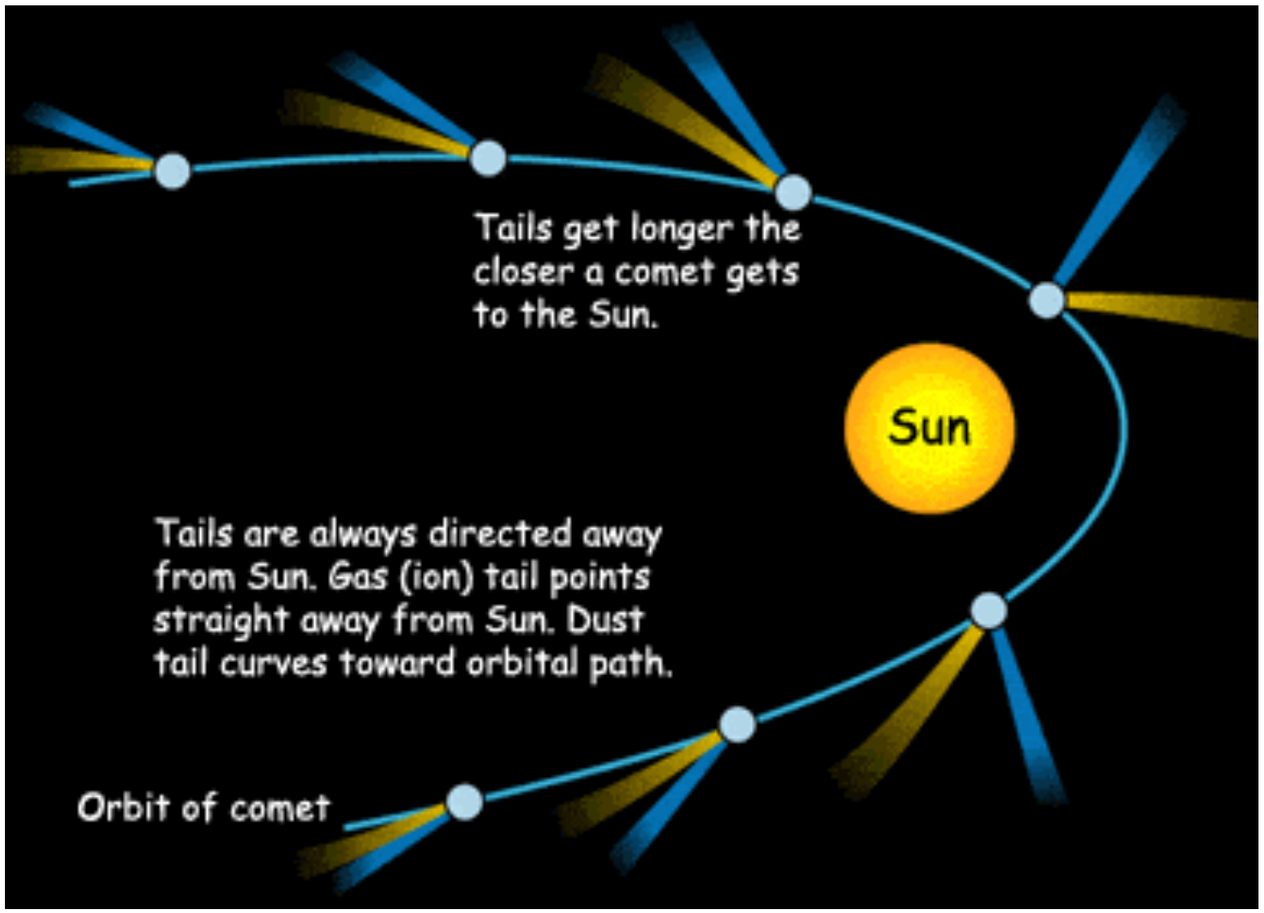
Photon: Linear Momentum

Photon: Linear Momentum

Photon: Linear Momentum



Photon: Linear Momentum



$$\tilde{p} \propto \left(\widetilde{E}^{\star} \times \widetilde{B} \right)$$

$$\tilde{p} = \hbar \tilde{k}$$

Photon: Optical Angular Momentum

Photon: Optical Angular Momentum

$$\tilde{j} = \frac{1}{2\mu_0}\left(\tilde{r} \times (\widetilde{E}^{\star} \times \widetilde{B})\right)$$

Photon: Optical Angular Momentum

$$\tilde{j} = \frac{1}{2\mu_0}\left(\tilde{r} \times (\widetilde{E}^{\star} \times \widetilde{B})\right)$$

$$\tilde{j} = \frac{-i}{2\mu_0\omega}\left(\tilde{r} \times (\widetilde{E}^{\star} \times (\widetilde{\nabla} \times \widetilde{E}))\right)$$

Photon: Optical Angular Momentum

$$\tilde{j} = \frac{1}{2\mu_0}\left(\tilde{r} \times (\widetilde{E}^{\star} \times \widetilde{B})\right)$$

$$\tilde{j} = \frac{-i}{2\mu_0\omega}\left(\tilde{r} \times (\widetilde{E}^{\star} \times (\widetilde{\nabla} \times \widetilde{E}))\right)$$

Angular momentum decomposition

$$\widetilde{J} = \widetilde{S} + \widetilde{L}$$

$$S_i = \frac{1}{2\mu_0\omega}\int d^3r E_j^{\star}(-i\epsilon_{i,j,k})E_k$$

$$L_i = \frac{1}{2\mu_0\omega}\int d^3r\, E_j^{\star}(-i\,\tilde{r} \times \widetilde{\nabla})_i E_j$$

Photon: Optical Angular Momentum

$$\tilde{j} = \frac{1}{2\mu_0}\left(\tilde{r} \times (\widetilde{E}^{\star} \times \widetilde{B})\right)$$

$$\tilde{j} = \frac{-i}{2\mu_0\omega}\left(\tilde{r} \times (\widetilde{E}^{\star} \times (\widetilde{\nabla} \times \widetilde{E}))\right)$$

Angular momentum decomposition

$$\widetilde{J} = \widetilde{S} + \widetilde{L}$$

Spin term

$$S_i = \frac{1}{2\mu_0\omega}\int d^3r E_j^{\star}(-i\epsilon_{i,j,k})E_k$$

$$L_i = \frac{1}{2\mu_0\omega}\int d^3r\, E_j^{\star}(-i\,\tilde{r} \times \widetilde{\nabla})_i E_j$$

Photon: Optical Angular Momentum

$$\tilde{j} = \frac{1}{2\mu_0}\left(\tilde{r} \times (\widetilde{E}^{\star} \times \widetilde{B})\right)$$

$$\tilde{j} = \frac{-i}{2\mu_0\omega}\left(\tilde{r} \times (\widetilde{E}^{\star} \times (\widetilde{\nabla} \times \widetilde{E}))\right)$$

Angular momentum decomposition

$$\widetilde{J} = \widetilde{S} + \widetilde{L}$$

Spin term

$$S_i = \frac{1}{2\mu_0\omega}\int d^3r E_j^{\star}(-i\epsilon_{i,j,k})E_k$$

OAM term

$$L_i = \frac{1}{2\mu_0\omega}\int d^3r\, E_j^{\star}(-i\,\tilde{r} \times \widetilde{\nabla})_i E_j$$

Photon: Optical Angular Momentum

Photon: Optical Angular Momentum

Longitudinal component of angular momentum

$$S_i = \frac{1}{2\mu_0\omega}\int d^3r E_j^\star(-i\epsilon_{i,j,k})E_k \qquad L_i = \frac{1}{2\mu_0\omega}\int d^3r\, E_j^\star(-i\,\tilde{r}\times\tilde{\nabla})_i E_j$$

$$\widehat{S}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \widehat{L}_z = -i\partial_\phi$$

Photon: Optical Angular Momentum

Longitudinal component of angular momentum

$$S_i = \frac{1}{2\mu_0\omega}\int d^3r E_j^\star(-i\epsilon_{i,j,k})E_k \qquad L_i = \frac{1}{2\mu_0\omega}\int d^3r\, E_j^\star(-i\,\tilde{r}\times\tilde{\nabla})_i E_j$$

$$\widehat{S}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \widehat{L}_z = -i\partial_\phi$$

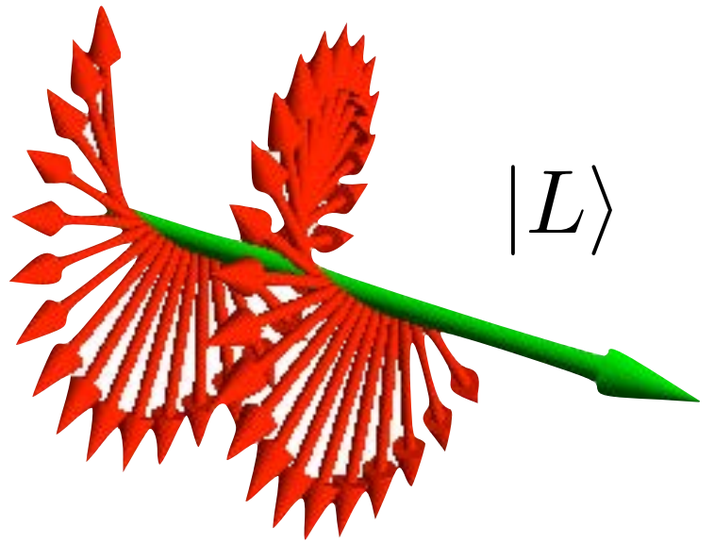
$$S_z = \hbar\int d\sigma_\perp(|E_L|^2 - |E_R|^2) \qquad L_z = \hbar\int d\sigma_\perp(E_L^*\partial_\phi E_L + E_R^*\partial_\phi E_R)$$

Photon: Spin Angular Momentum

vectorial picture

angular momentum

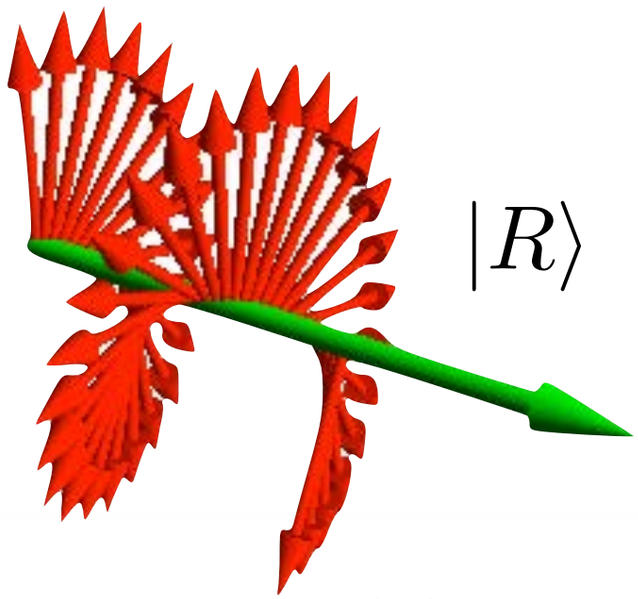
- Circular polarisations: (Left and Right)



$|L\rangle$

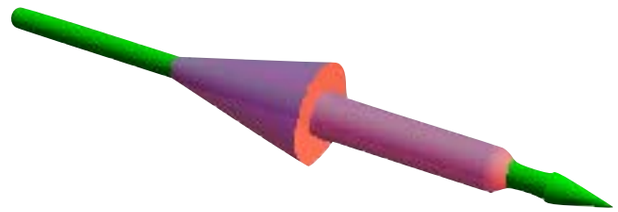
$J_z = +\hbar$

- Spin angular momentum may take two values of



$|R\rangle$

$J_z = -\hbar$



$|L\rangle$ Left-handed circular polarisation

$|R\rangle$ Right-handed circular polarisation

Photon: Optical Angular Momentum

- Optical field expression in the cylindrical coordinate is

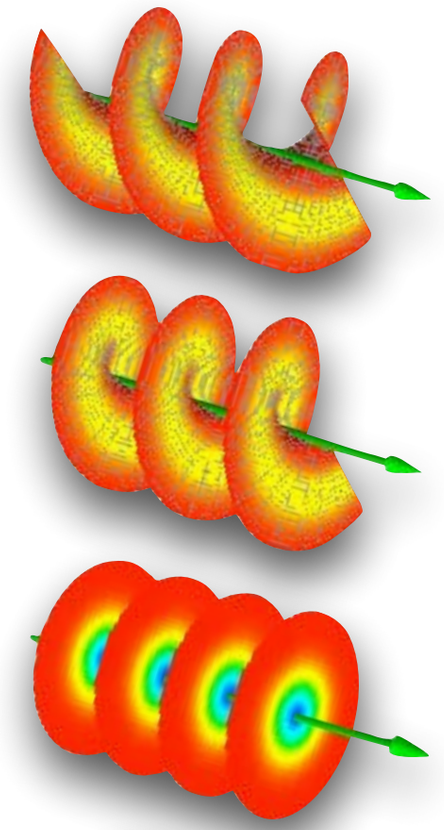
$$\widehat{L}_z = -i\partial_\phi$$

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

$$J_z = \ell\hbar$$

In the contrast, orbital angular momentum may take any of the infinite values ℓ =. .. - 2, -1, 0, 1, 2, ...

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



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

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

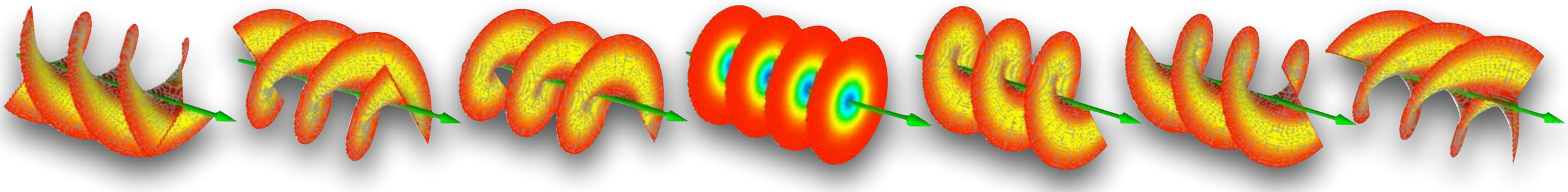
$\ell = 0$ $J_z = 0$

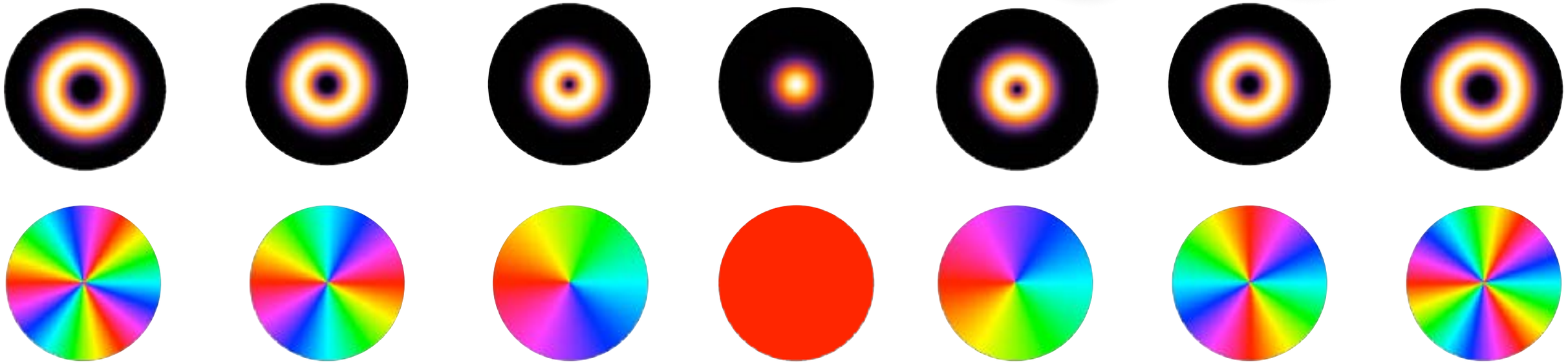
$\ell = +1$ $J_z = +\hbar$

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

Photon: Optical Angular Momentum

$\ell = -3$ $\ell = -2$ $\ell = -1$ $\ell = 0$ $\ell = +1$ $\ell = +2$ $\ell = +3$

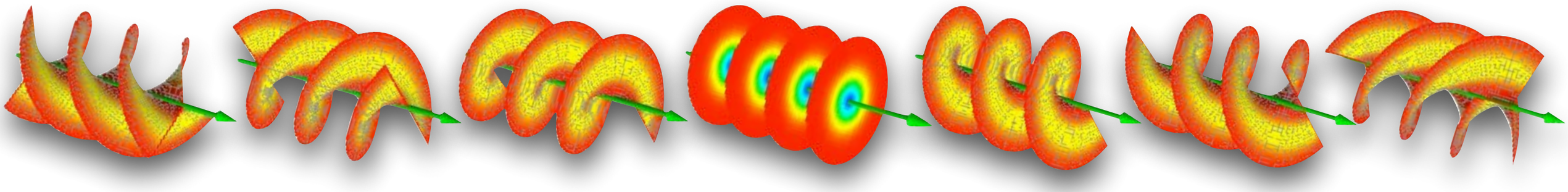


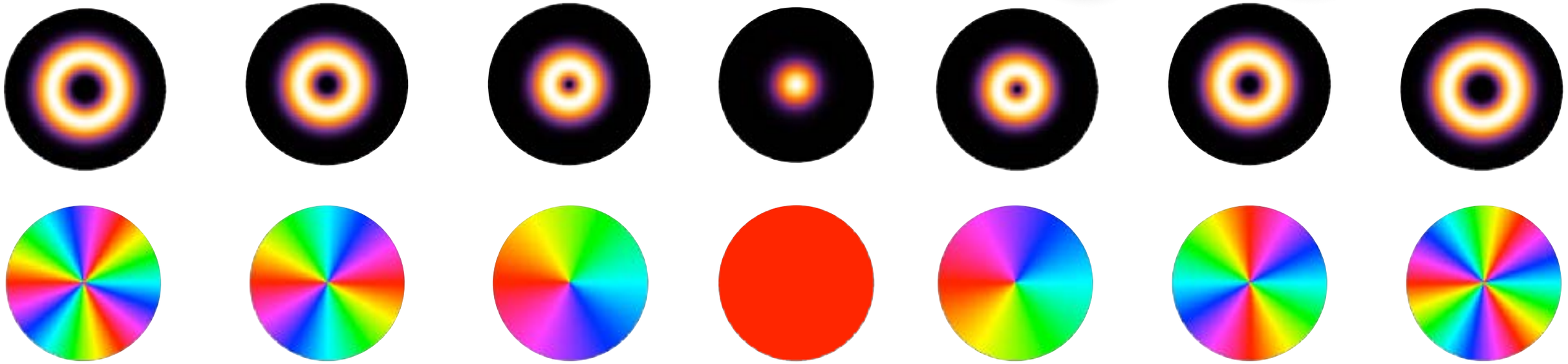


Interested: see WiKipedia pages on angular momentum of light

Photon: Optical Angular Momentum

$\ell = -3$ $\ell = -2$ $\ell = -1$ $\ell = 0$ $\ell = +1$ $\ell = +2$ $\ell = +3$





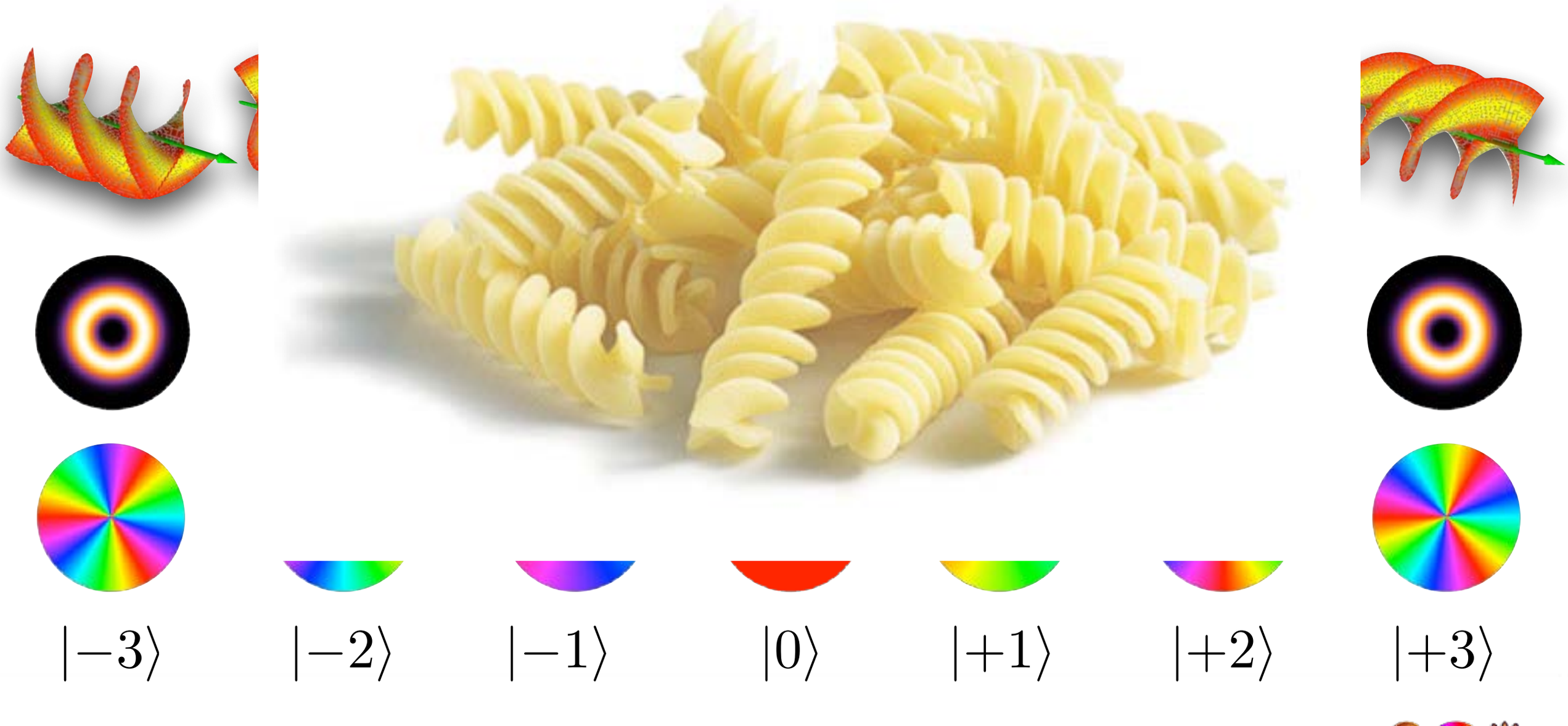
$|-3\rangle$ $|-2\rangle$ $|-1\rangle$ $|0\rangle$ $|+1\rangle$ $|+2\rangle$ $|+3\rangle$

Interested: see WiKipedia pages on angular momentum of light

Photon: Optical Angular Momentum

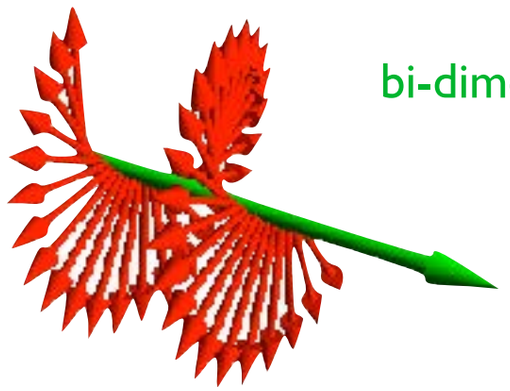
$\ell = -3$

$\ell = +3$



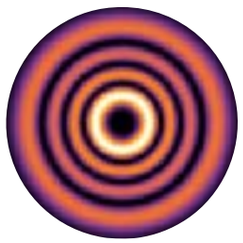
$|-3\rangle$ $|-2\rangle$ $|-1\rangle$ $|0\rangle$ $|+1\rangle$ $|+2\rangle$ $|+3\rangle$

Photon: Degrees of Freedom



bi-dimensional variable

$|\pi\rangle$ Polarisation (Spin)



$|p\rangle$ Radial mode (p number)

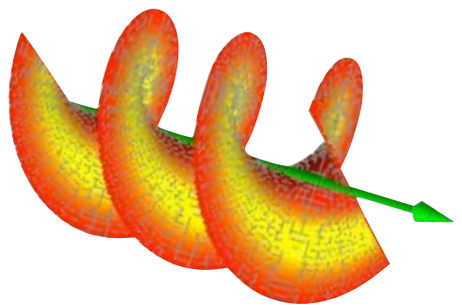
infinite dimension (discreet)

continues variable

Linear momentum (k-vector)

$|\kappa\rangle$

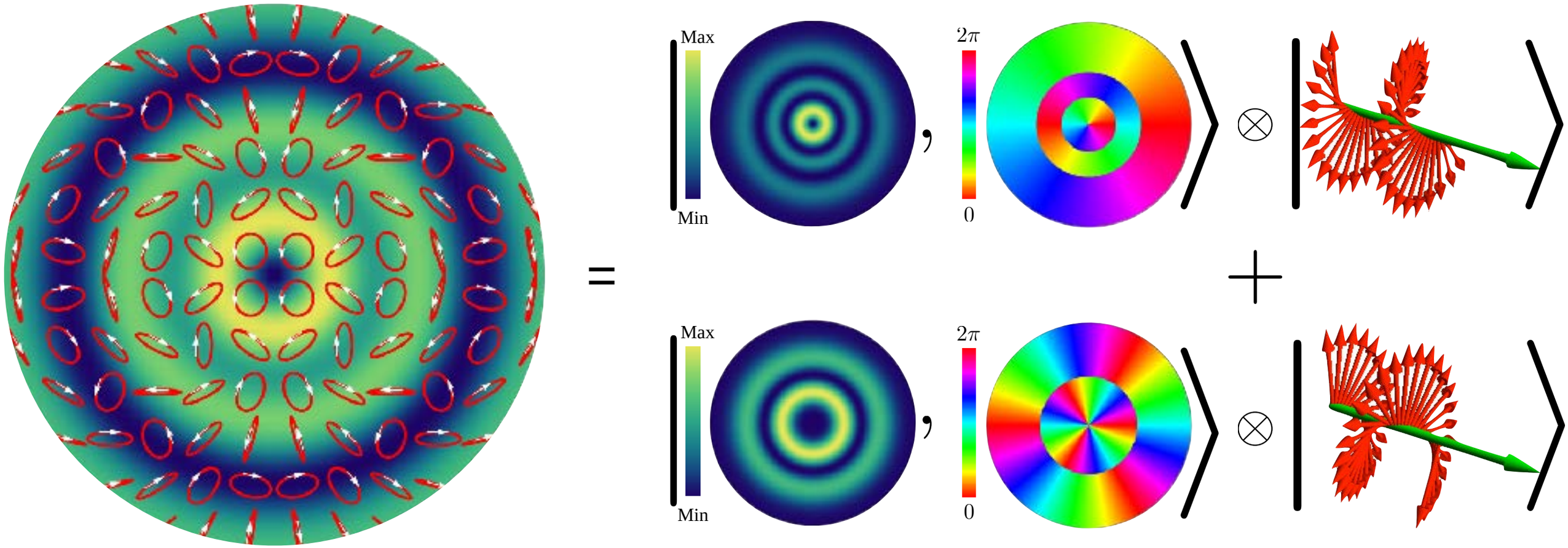
Orbital angular momentum (OAM)



$|o\rangle$

infinite dimension (discreet)

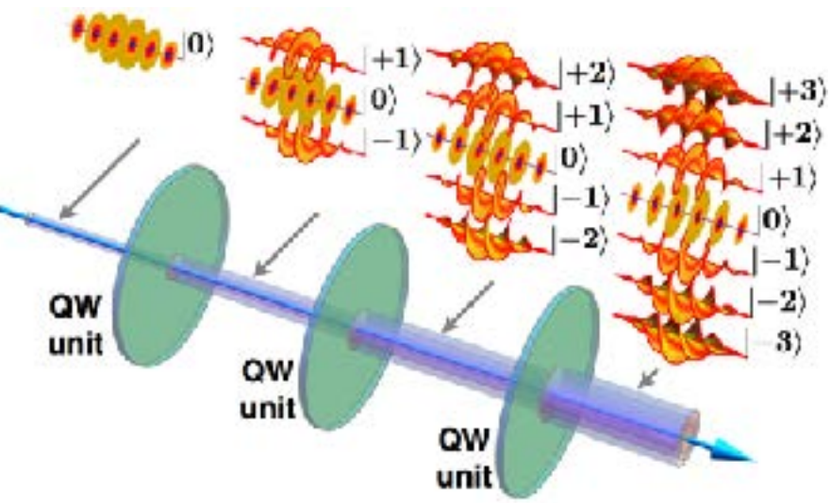
Structural Photons



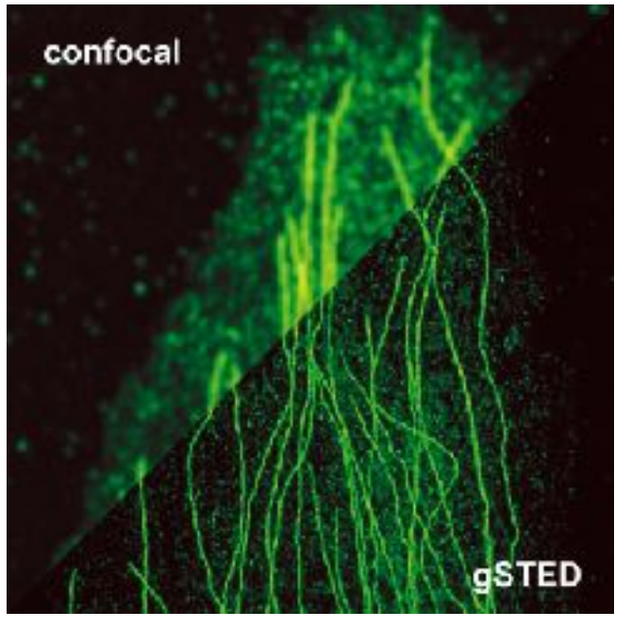
E Karimi, R W Boyd, *Science* 350, 1172 (2015)

Application of Structural Photons

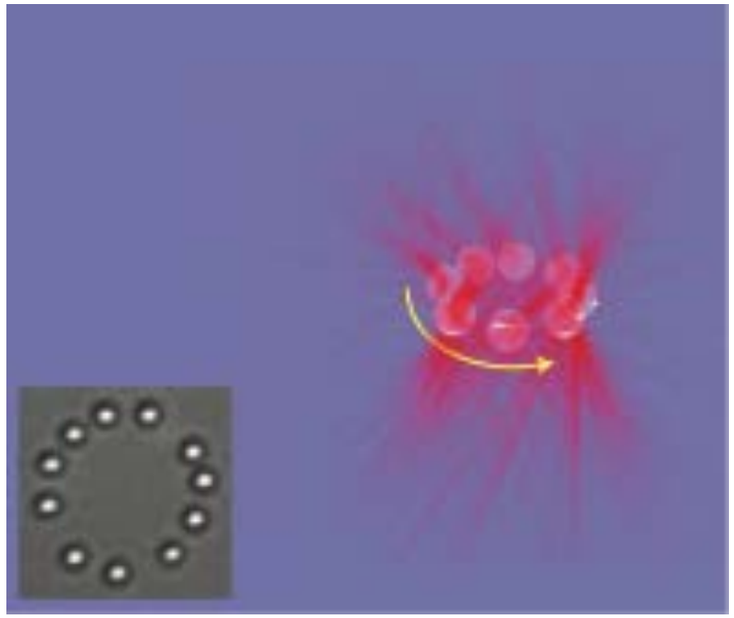
Quantum Computation



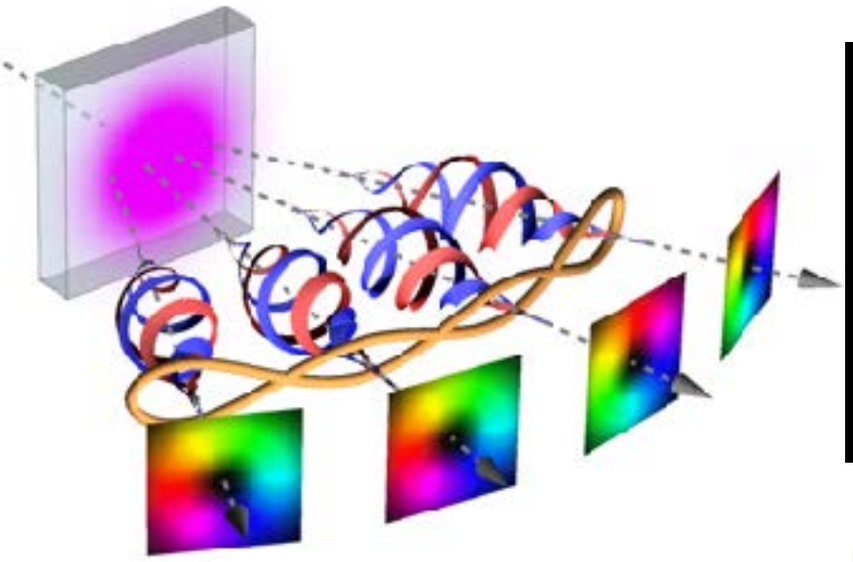
Optical Microscopy



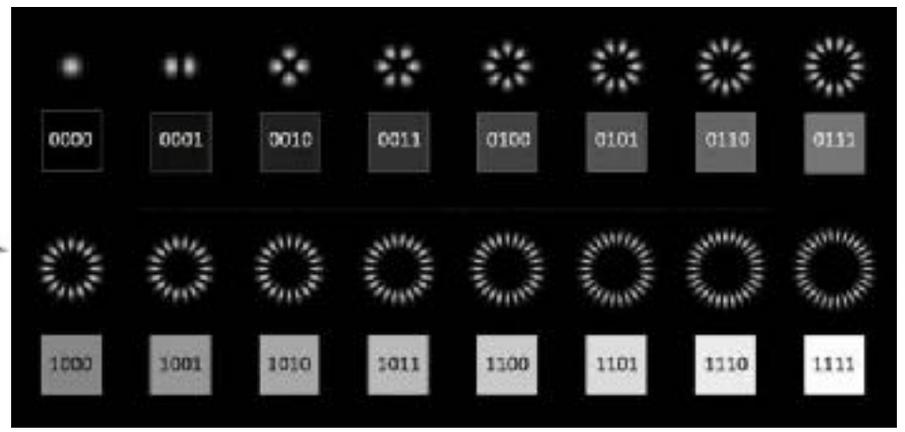
Optical Manipulation



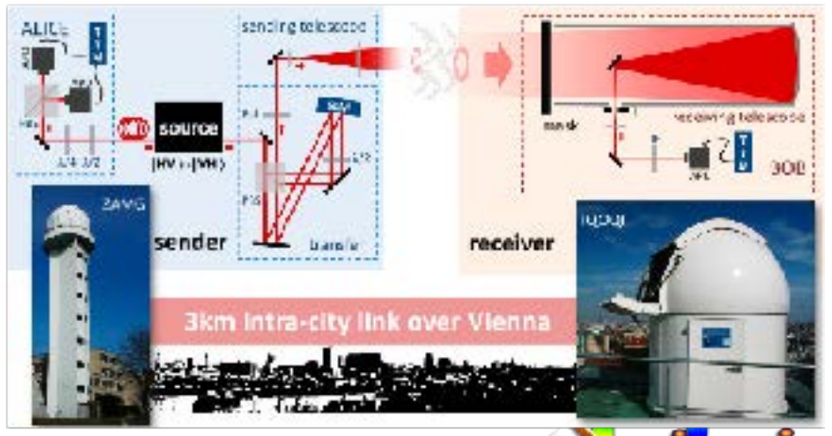
Hig-dimensional entengelement



Classical communication



Quantum Cryptography



The importance of Orbital Angular Momentum

The importance of Orbital Angular Momentum

Let us send letter **M**

The importance of Orbital Angular Momentum

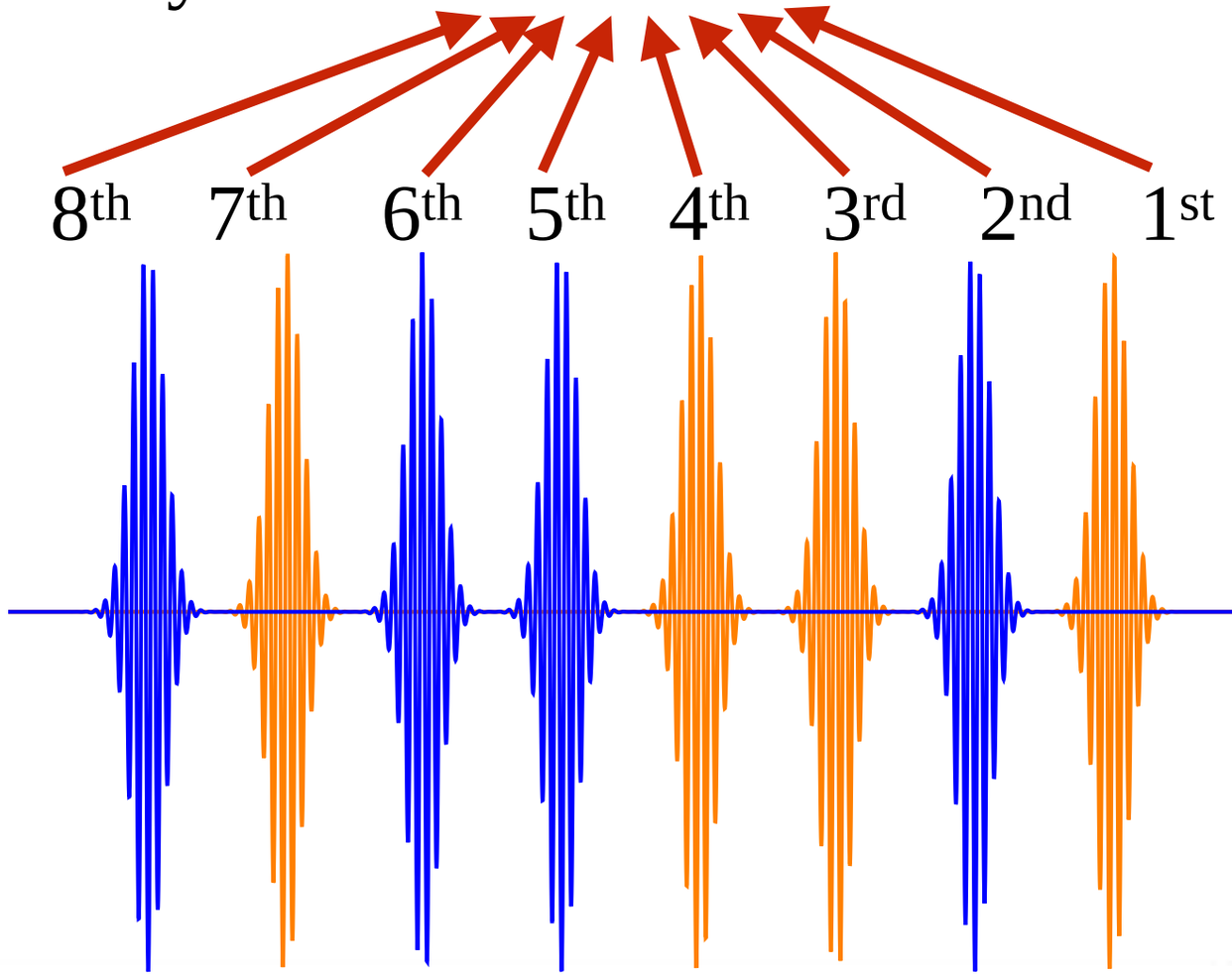
Let us send letter **M**

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

The importance of Orbital Angular Momentum

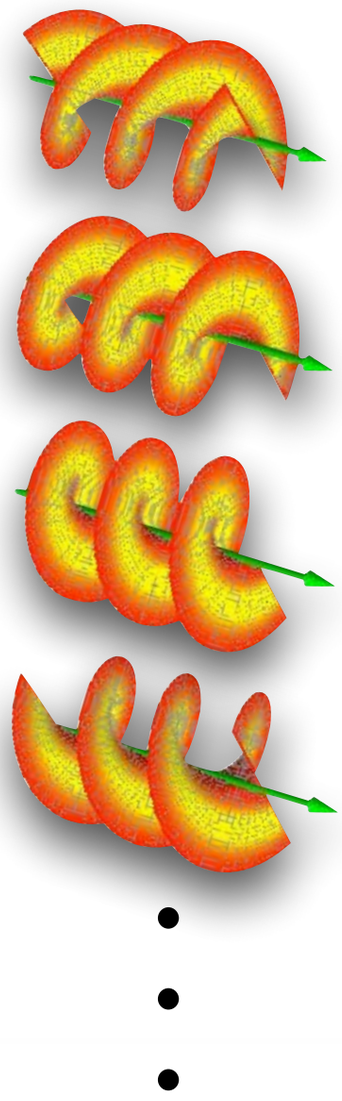
Let us send letter **M**

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



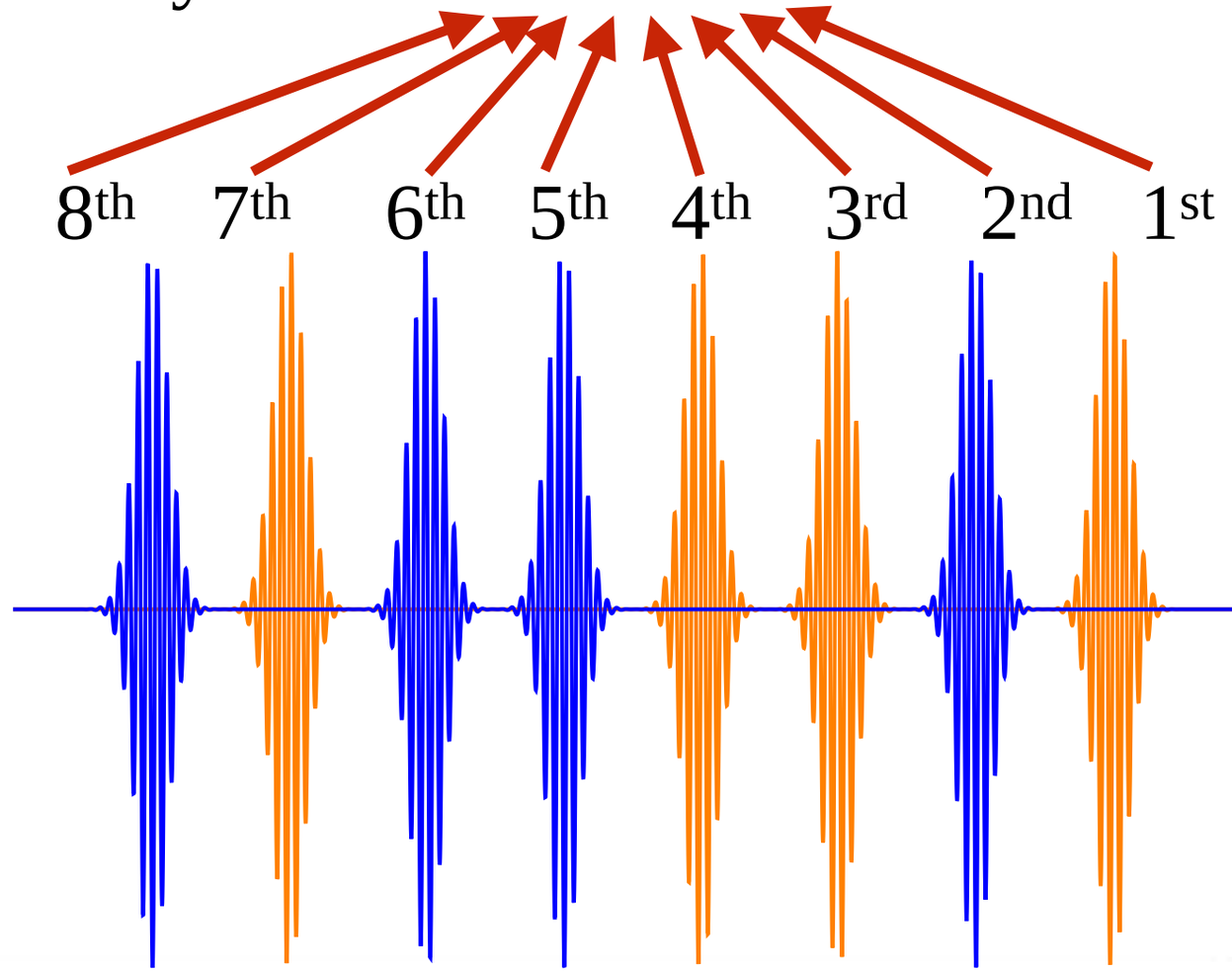
The importance of Orbital Angular Momentum

-
-
-



Let us send letter **M**

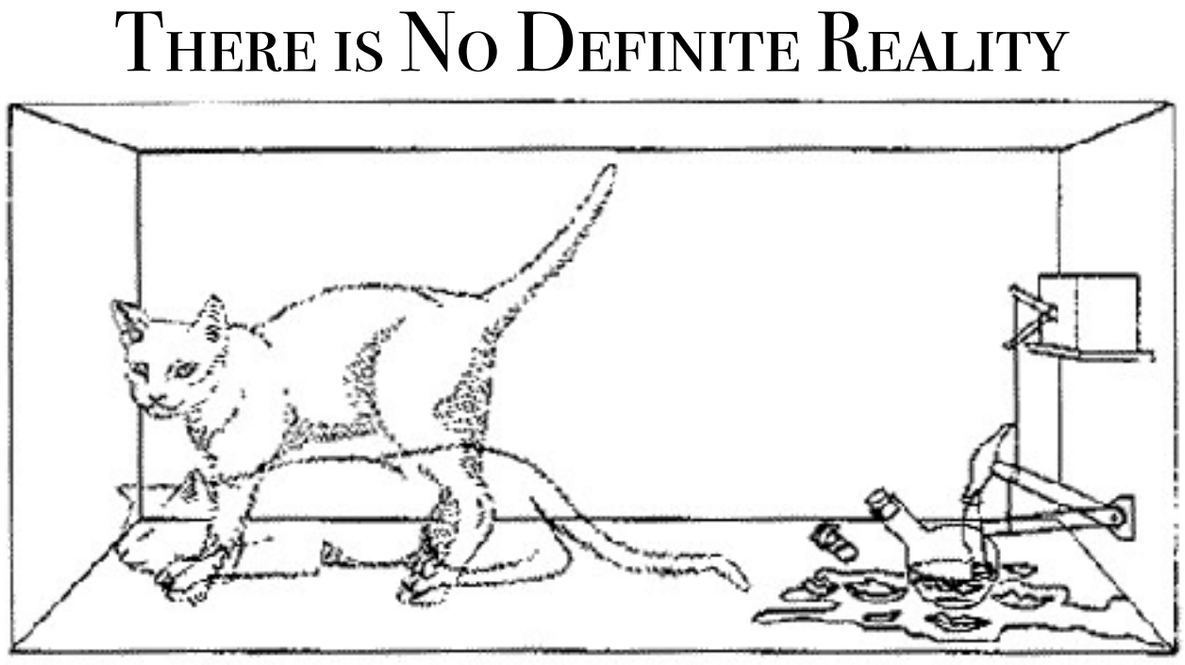
Letter **M** in the binary code is **01001101**



Quantum Cryptography

Quantum World

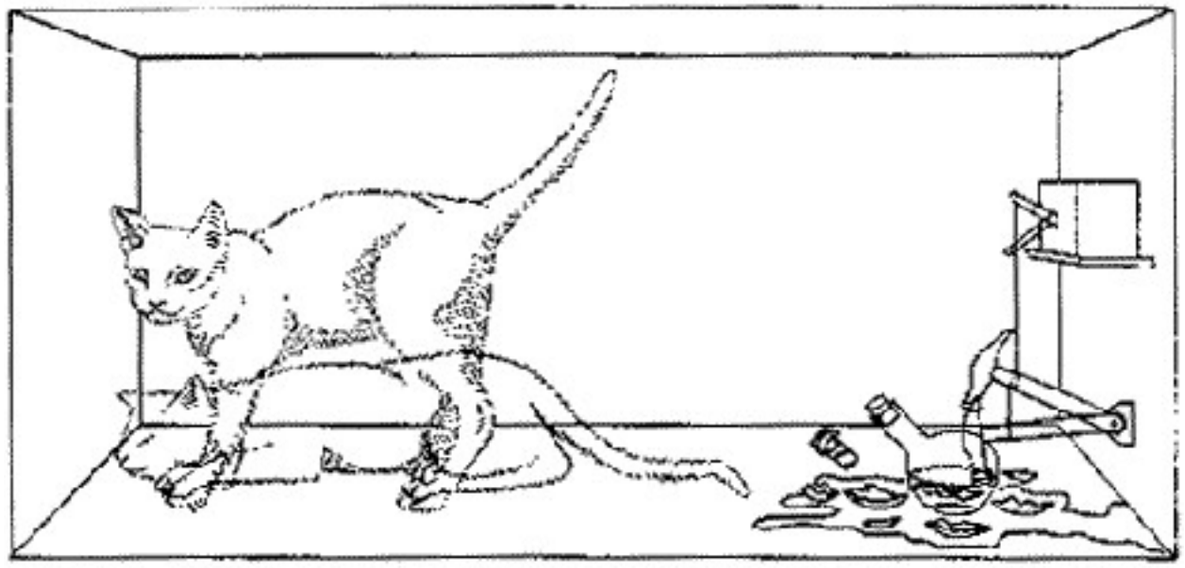
Quantum World



Quantum World

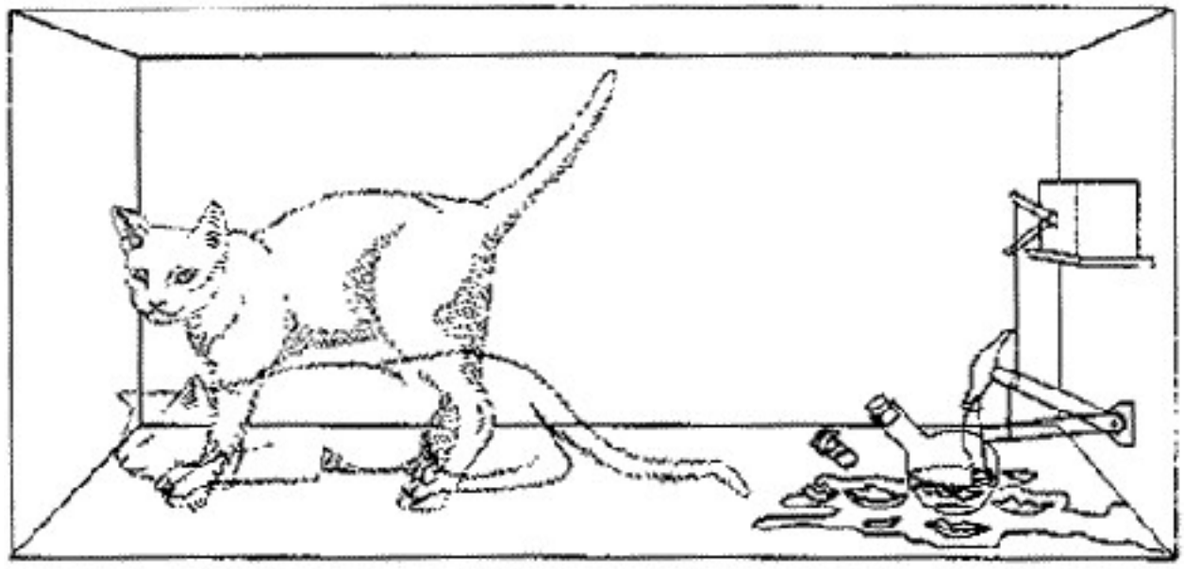
Conjugate Quantities Cannot Be Measured Simultaneously

There is No Definite Reality



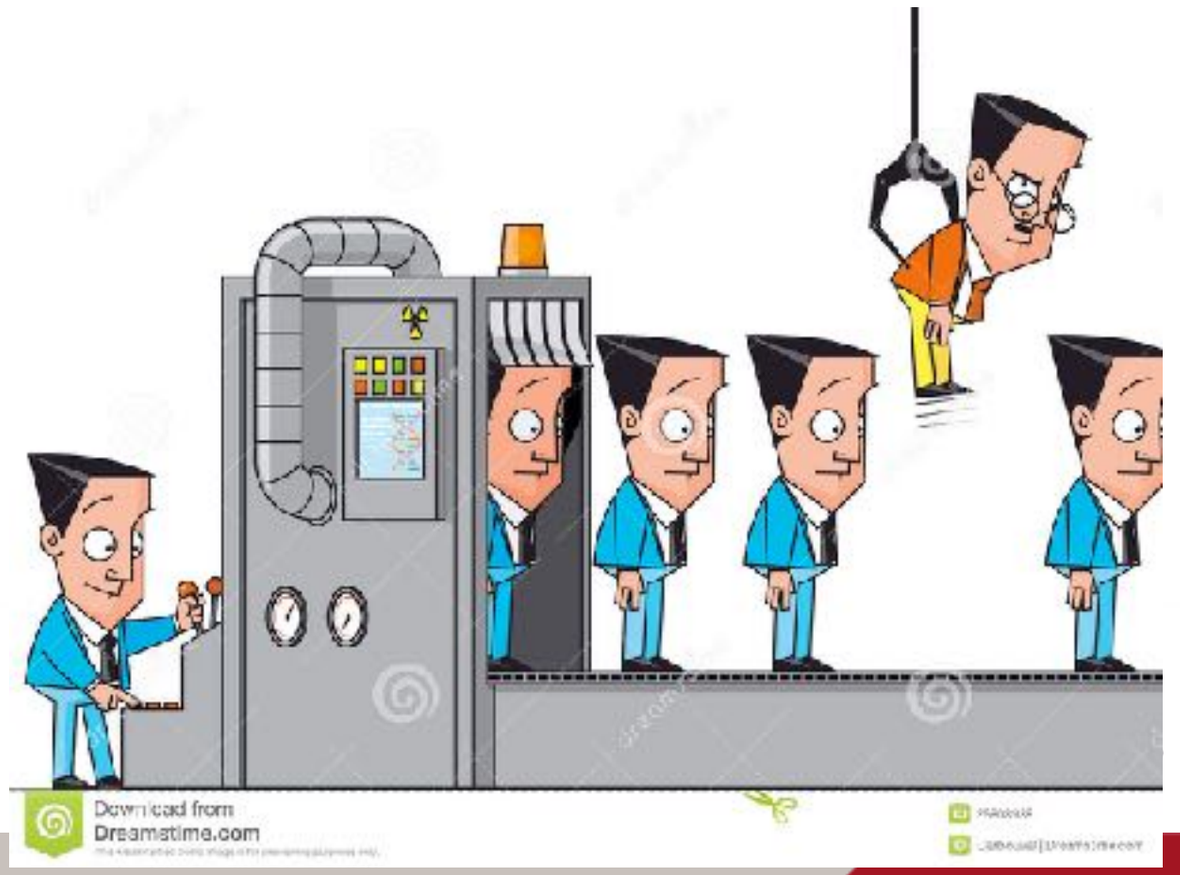
Quantum World

There is No Definite Reality



Conjugate Quantities Cannot Be Measured Simultaneously

Quantum Information Cannot Be Cloned without introducing errors



Cryptography

Alice

Bob

Cryptography

PUBLIC CHANNEL

Alice

Bob

Cryptography

Eve

PUBLIC CHANNEL

Alice

Bob

Cryptography

Eve

PUBLIC CHANNEL

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

Alice

Bob

Cryptography

Eve

PUBLIC CHANNEL

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

Alice

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

Eve

PUBLIC CHANNEL

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

Alice

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

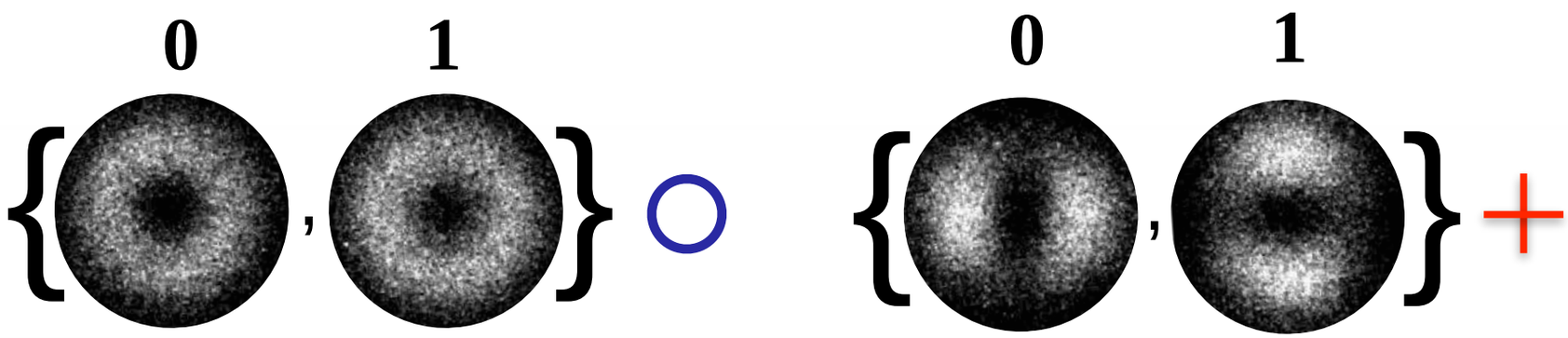
Key

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

Alice

Bob



Conjugate quantities

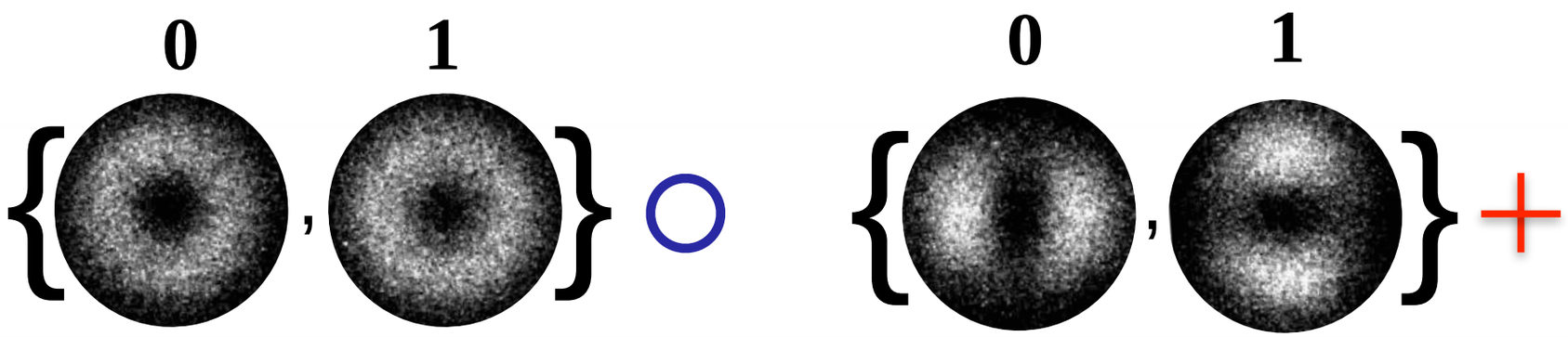
Quantum Cryptography

Alice

SECURE CHANNEL

Bob

CONJUGATE QUANTITIES



Quantum Cryptography

Alice

SECURE CHANNEL

Bob

ALICE + ○ + + + ○ ○ + + ○

0 0 0 1 0 1 1 1 1 0

CONJUGATE QUANTITIES

0 1 ○ 0 1 +

Quantum Cryptography

Alice

SECURE CHANNEL

Bob

ALICE + ○ + + + ○ ○ + + ○

0 0 0 1 0 1 1 1 1 0

○ ○ + ○ ○ + ○ ○ + +

BOB

CONJUGATE QUANTITIES

0 1 ○ 0 1 +

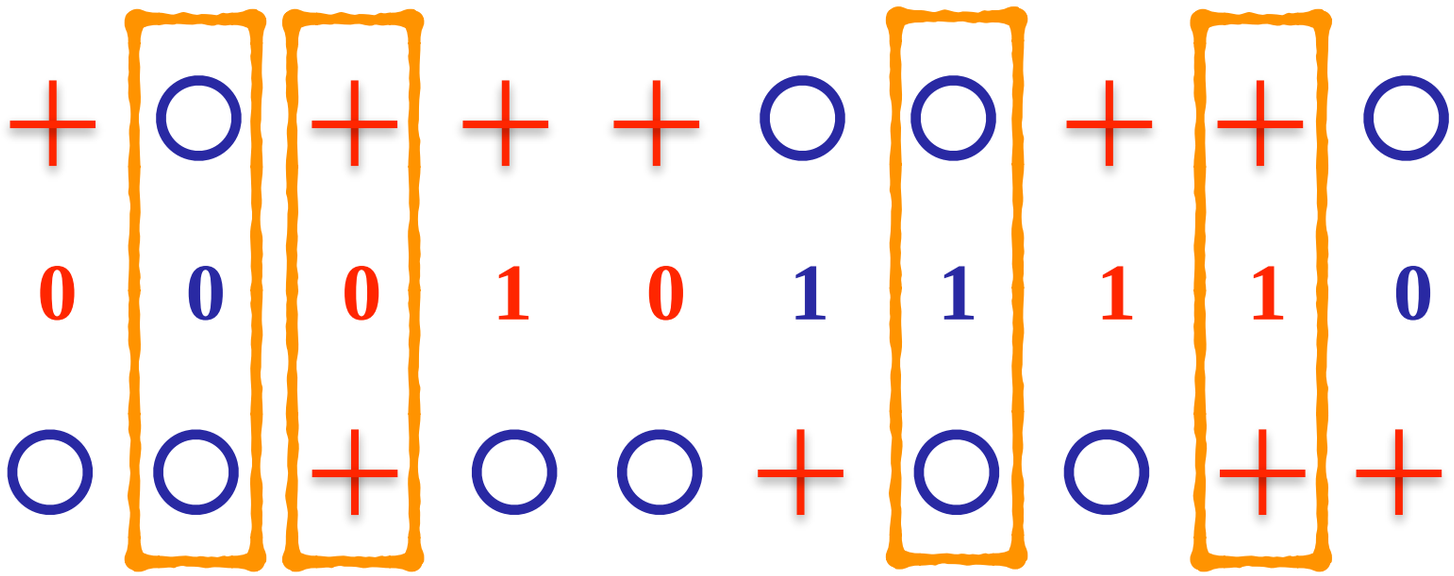
Quantum Cryptography

Alice

Bob

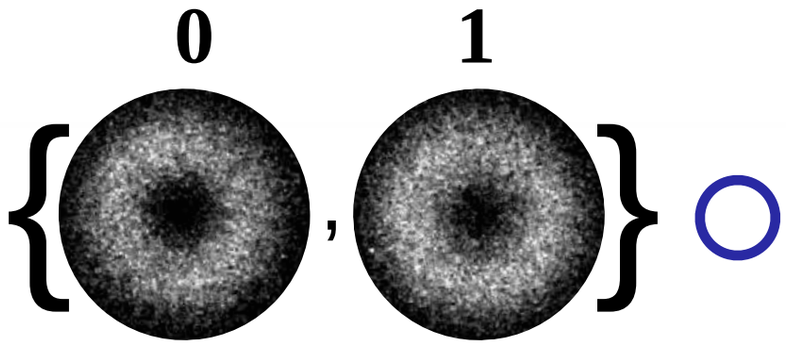
Secure Channel

Alice



Bob

Conjugate quantities

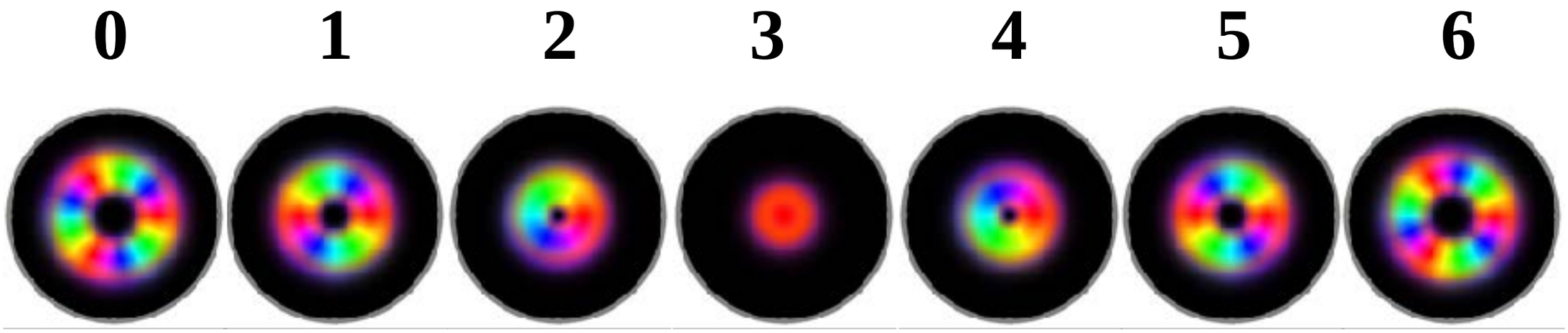


High-Dimensional QKD

0 1 2 3 4 5 6

F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

High-Dimensional QKD



F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

High-Dimensional QKD

	0	1	2	3	4	5	6
$\{\|\psi\rangle_i\}$							
$\{\|\phi\rangle_j\}$							

sqogroup.ca

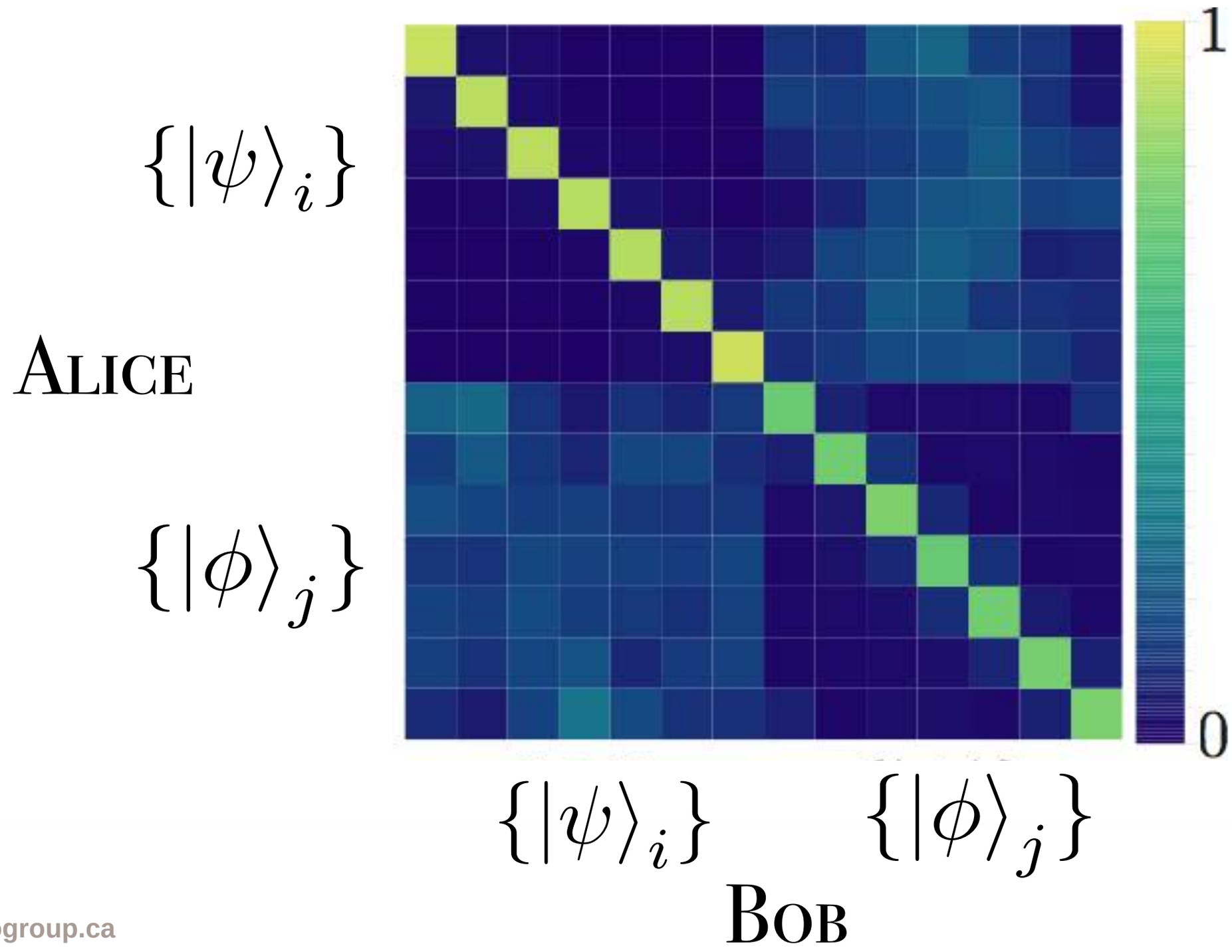
High-Dimensional QKD

	0	1	2	3	4	5	6
$\{\|\psi\rangle_i\}$							
$\{\|\phi\rangle_j\}$							

$$|\langle\psi|\phi\rangle|^2 = \frac{1}{7}$$

sqogroup.ca

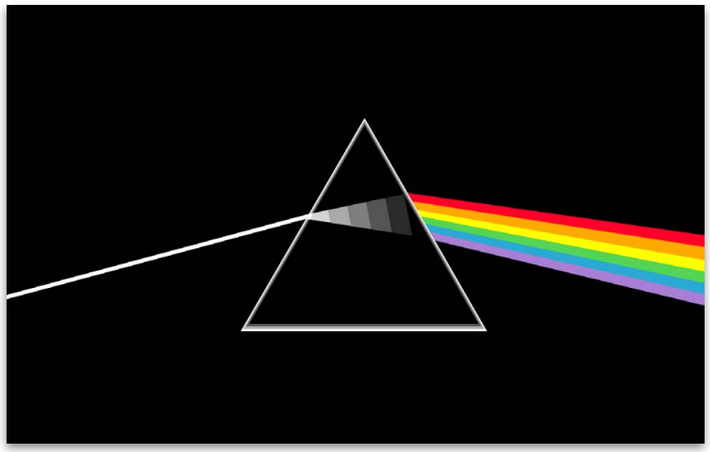
Experimental results



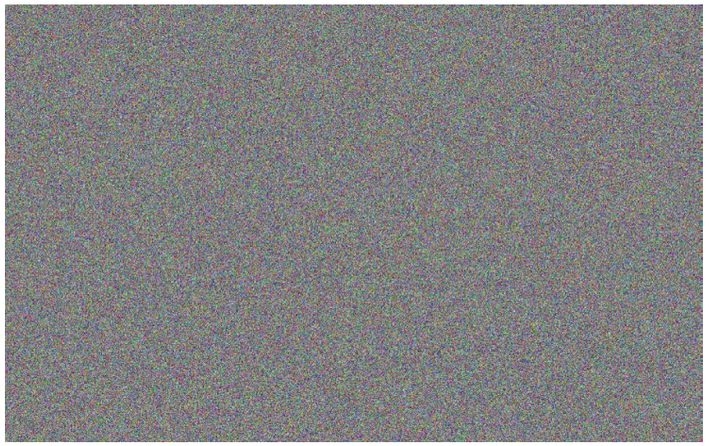
F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Encryption results

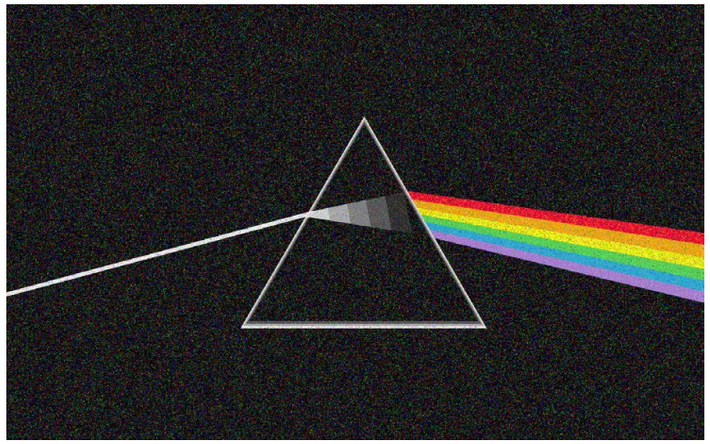
Sender (Alice)



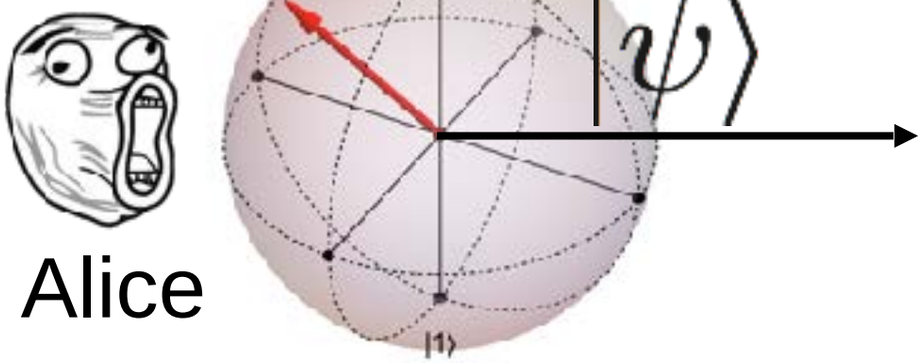
Encrypted message



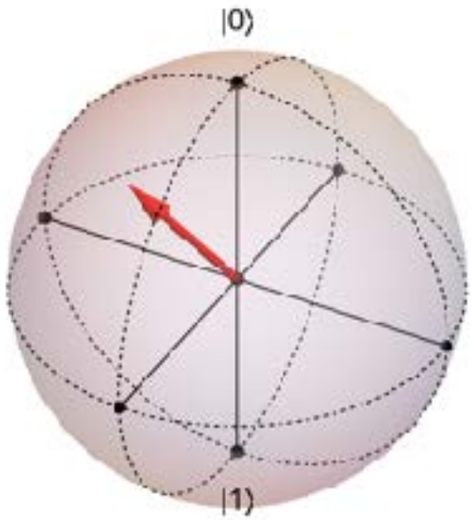
Receiver (Bob)

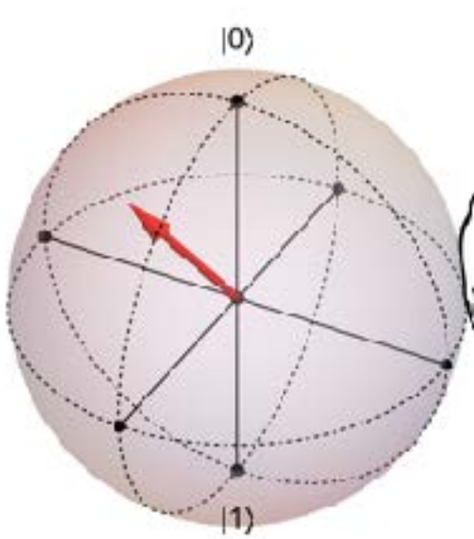


Cloning Attack



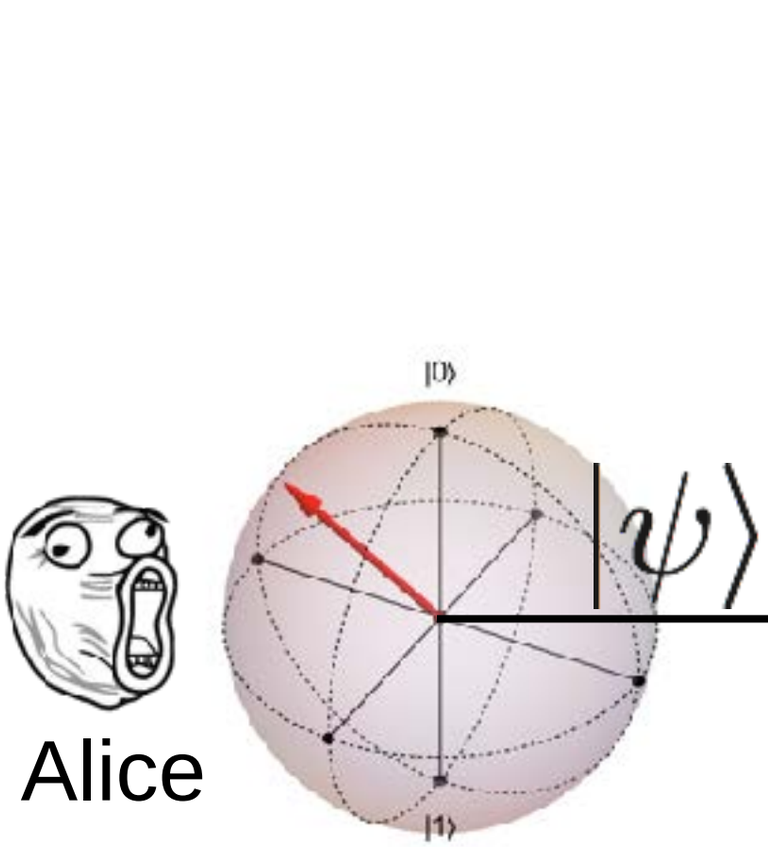
Alice



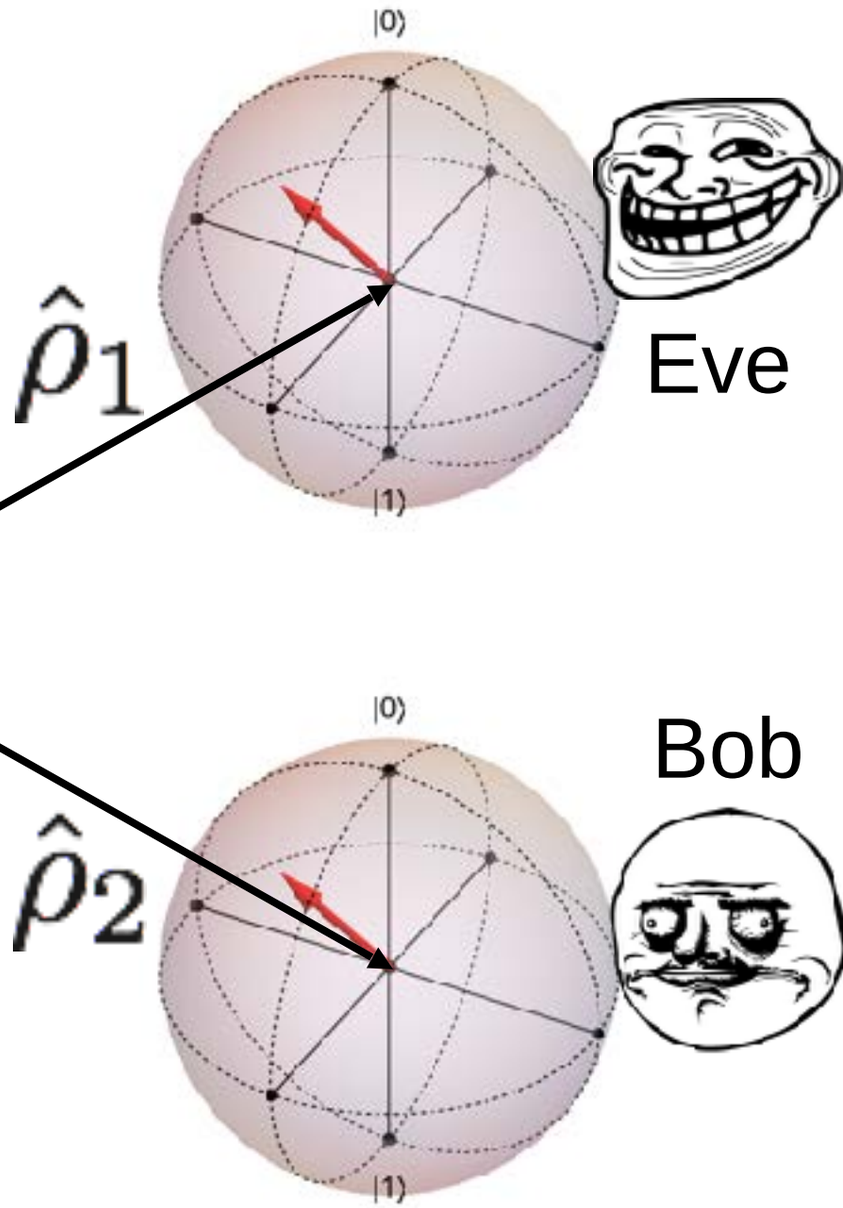


Bob

Cloning Attack



Optimal quantum cloning machine

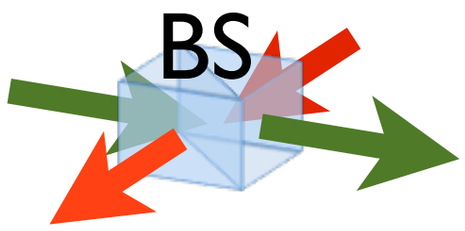


F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Optimal Cloning Attack: Hong-Ou-Mandel

F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Optimal Cloning Attack: Hong-Ou-Mandel

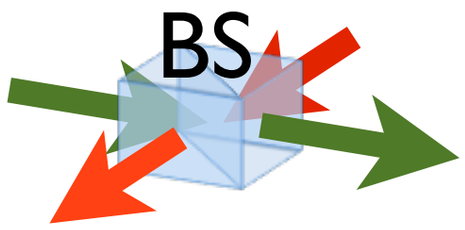


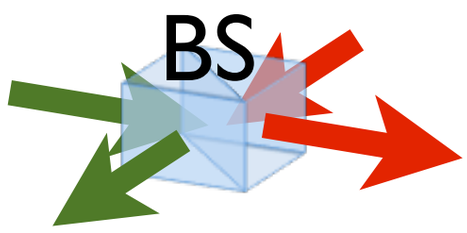
F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

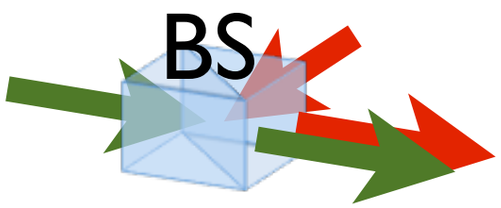
Optimal Cloning Attack: Hong-Ou-Mandel

F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Optimal Cloning Attack: Hong-Ou-Mandel

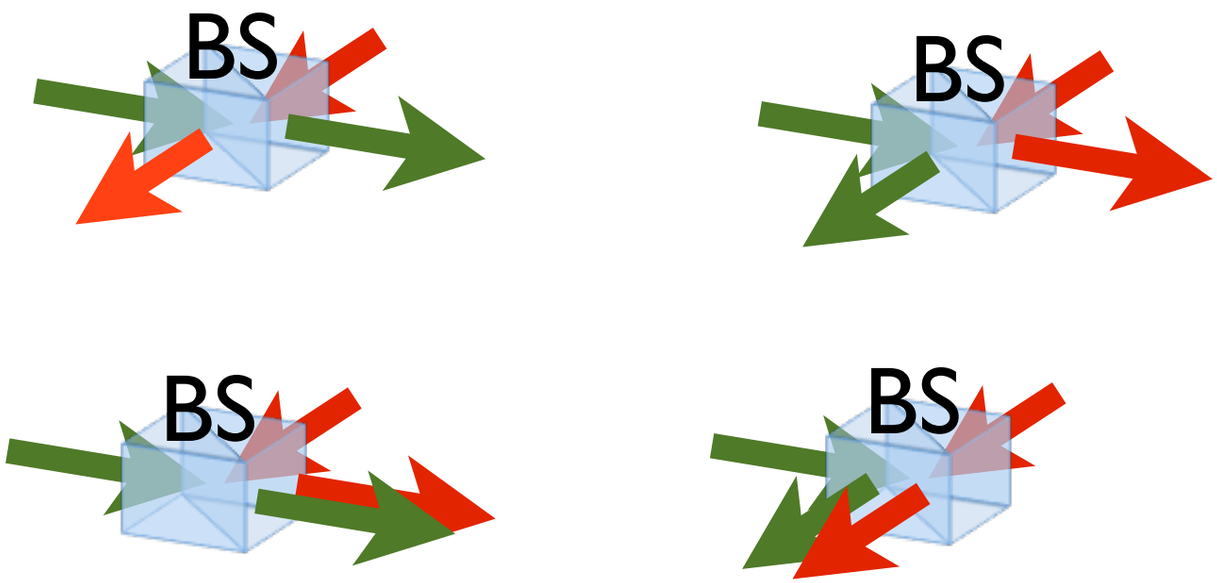






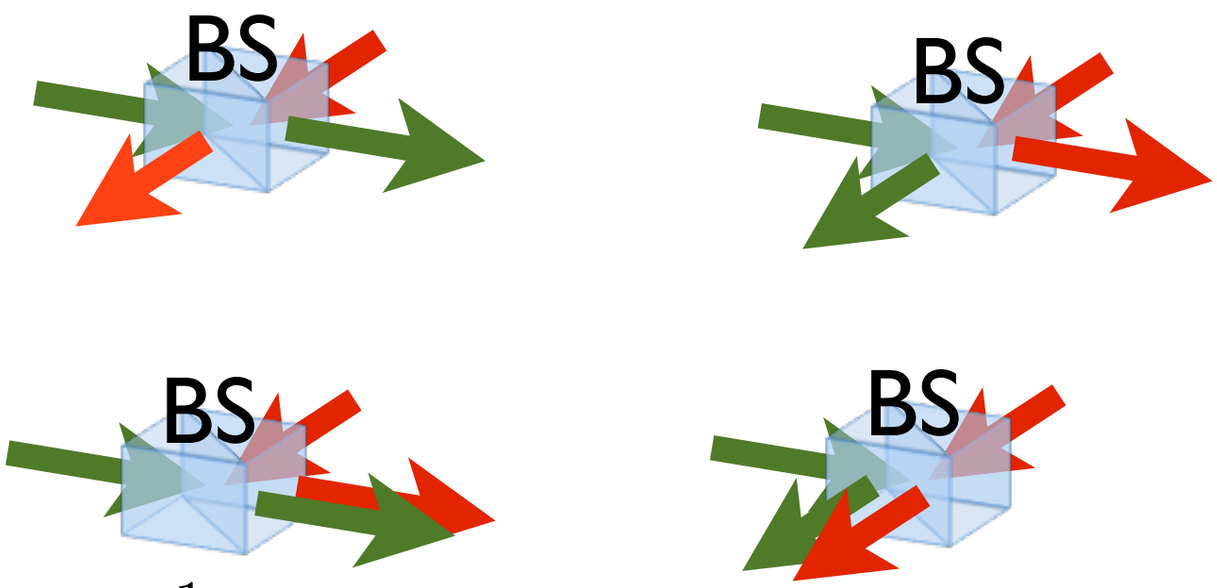
F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Optimal Cloning Attack: Hong-Ou-Mandel



F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

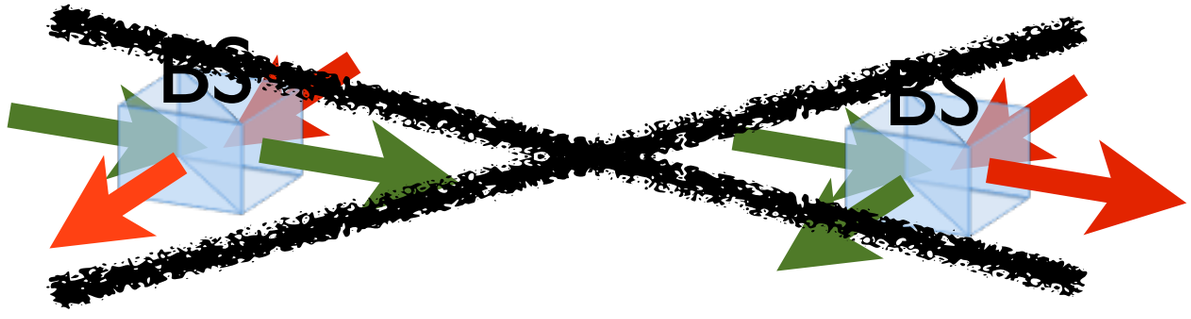
Optimal Cloning Attack: Hong-Ou-Mandel

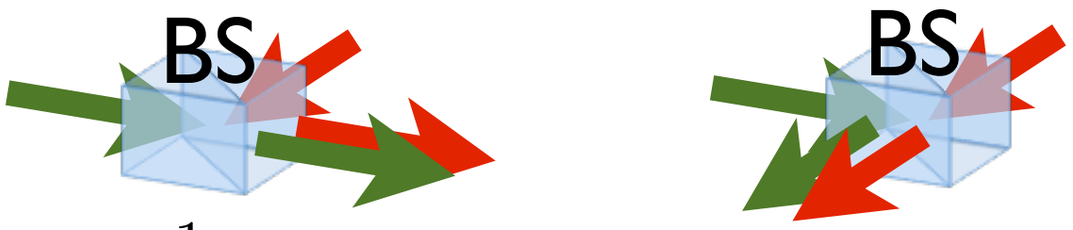


$$|\psi\rangle_{12,out} = \frac{1}{2}\left(i|c\rangle_1|c\rangle_2 + |c\rangle_1|d\rangle_2 - |d\rangle_1|c\rangle_2 + i|d\rangle_1|d\rangle_2\right)$$

F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Optimal Cloning Attack: Hong-Ou-Mandel

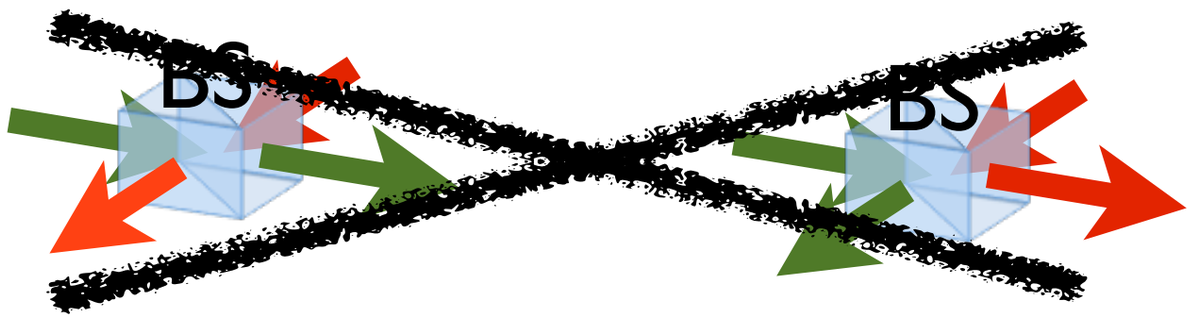


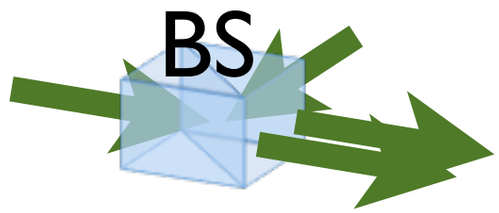


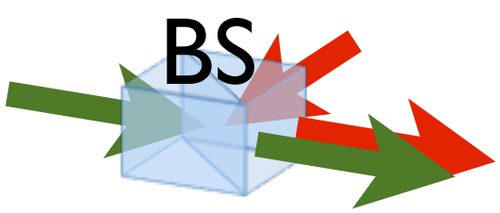
$$|\psi\rangle_{12,out} = \frac{1}{2}\left(i|c\rangle_1|c\rangle_2 + |c\rangle_1|d\rangle_2 - |d\rangle_1|c\rangle_2 + i|d\rangle_1|d\rangle_2\right)$$

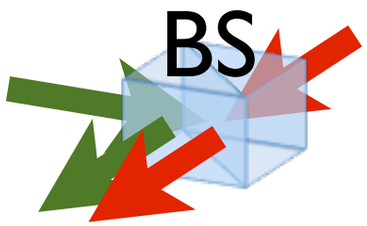
F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

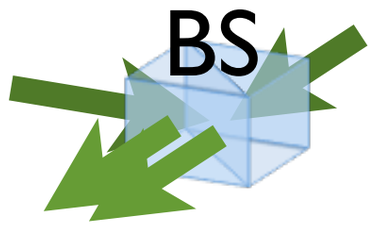
Optimal Cloning Attack: Hong-Ou-Mandel







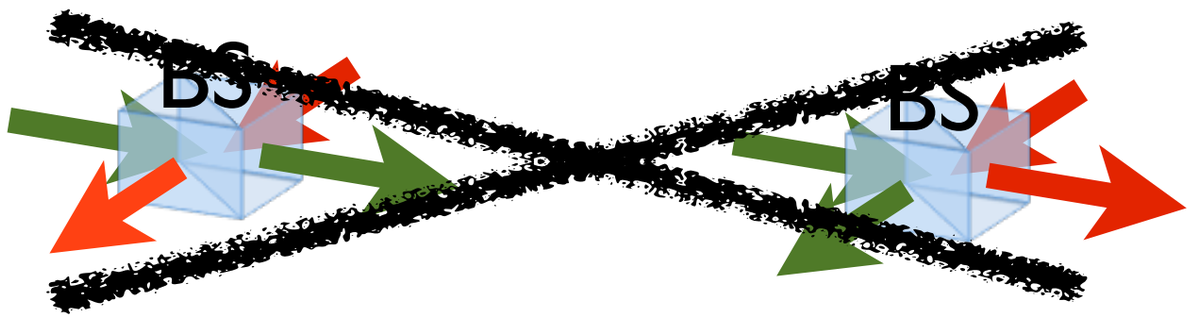


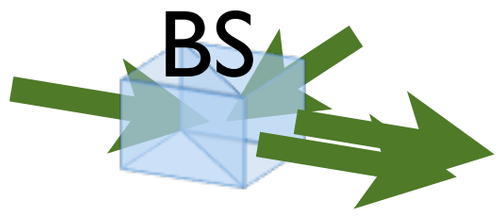


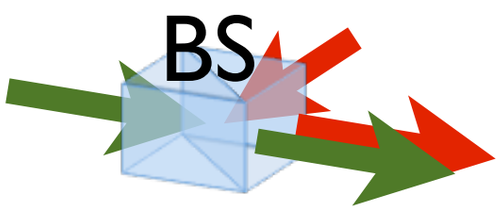
$$|\psi\rangle_{12,out} = \frac{1}{2}\left(i|c\rangle_1|c\rangle_2 + |c\rangle_1|d\rangle_2 - |d\rangle_1|c\rangle_2 + i|d\rangle_1|d\rangle_2\right)$$

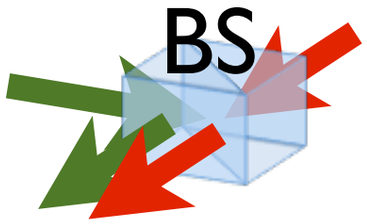
F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

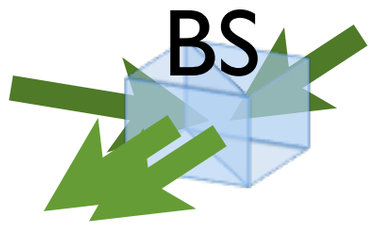
Optimal Cloning Attack: Hong-Ou-Mandel











$$|\psi\rangle_{12,out} = \frac{1}{2}\left(i|c\rangle_1|c\rangle_2 + |c\rangle_1|d\rangle_2 - |d\rangle_1|c\rangle_2 + i|d\rangle_1|d\rangle_2\right)$$

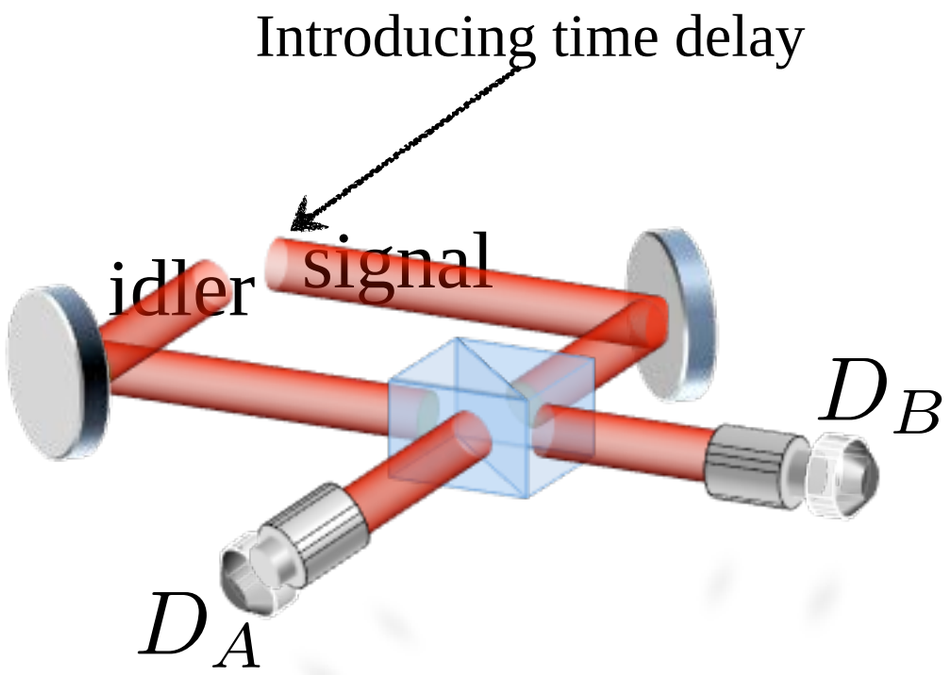
$$|\psi\rangle_{out} = \frac{1}{\sqrt{2}}\left(|c\rangle^2 + |d\rangle^2\right)$$

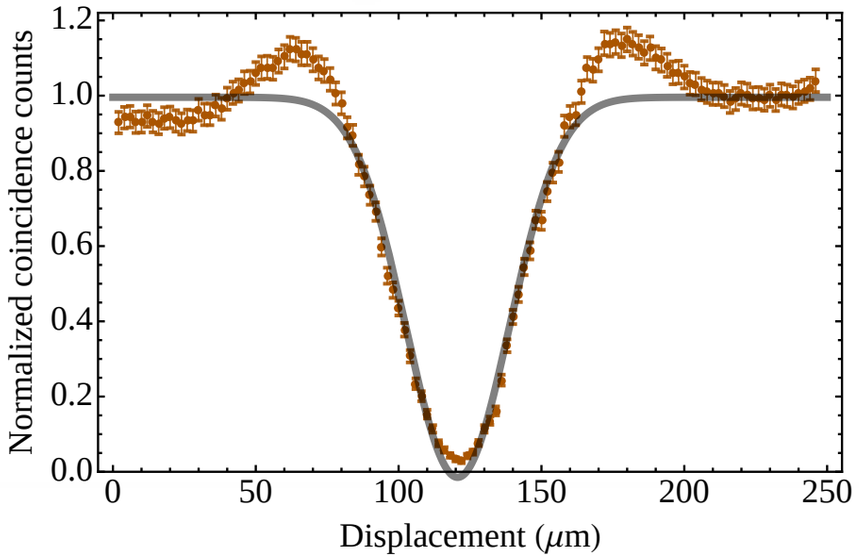
F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Optimal Cloning Attack: Hong-Ou-Mandel

F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

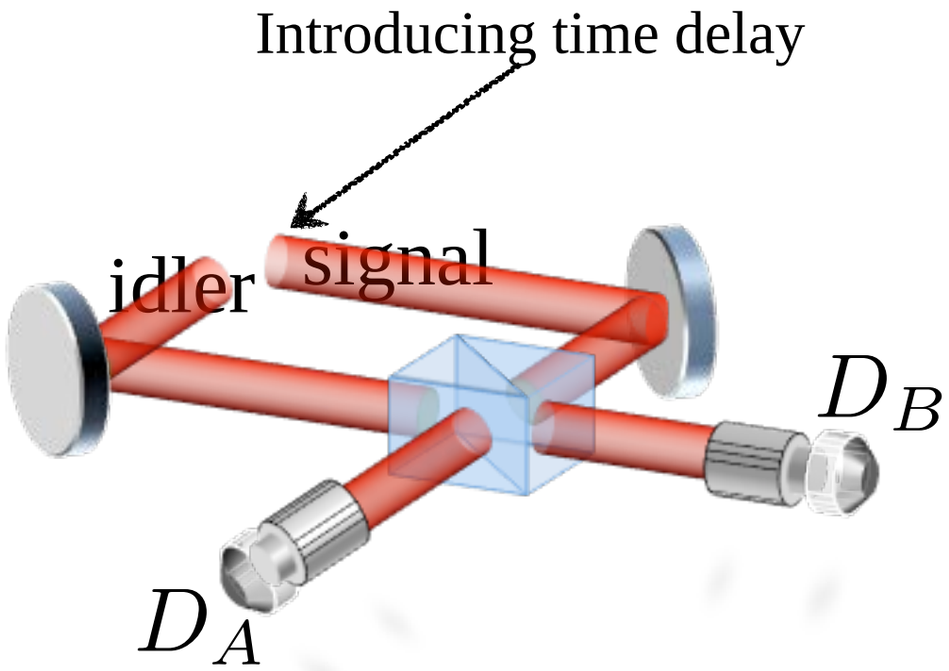
Optimal Cloning Attack: Hong-Ou-Mandel

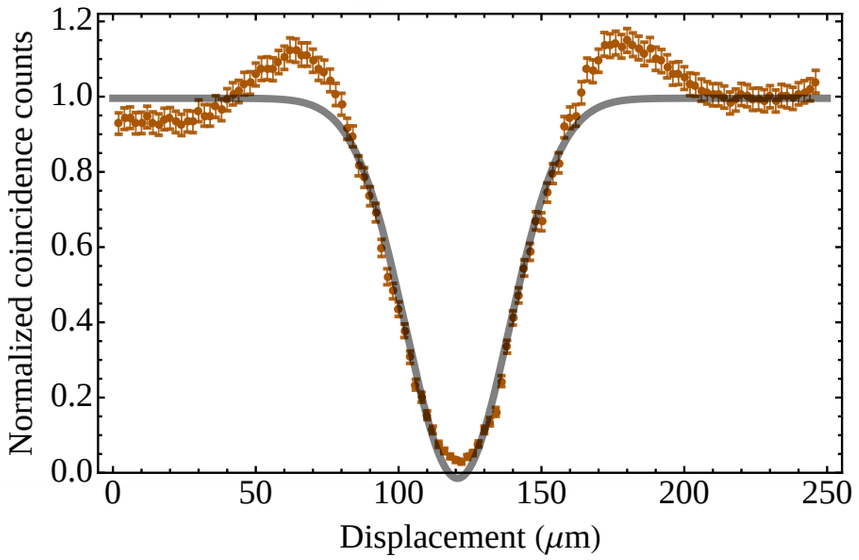


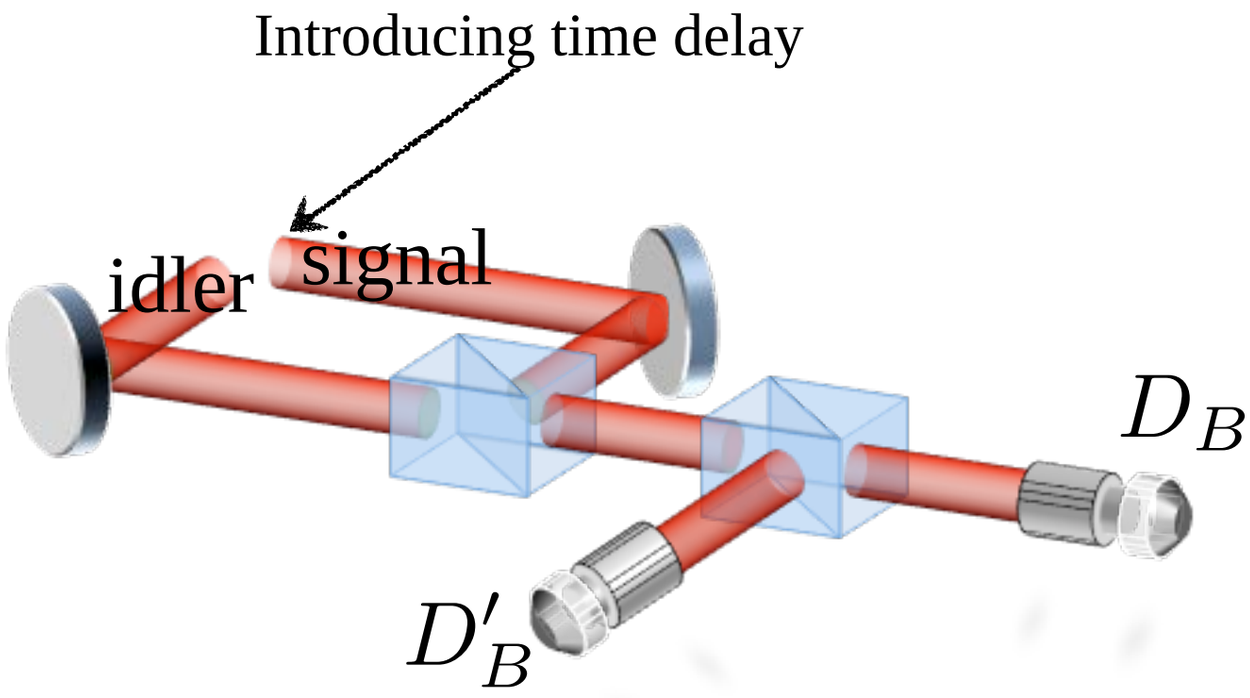


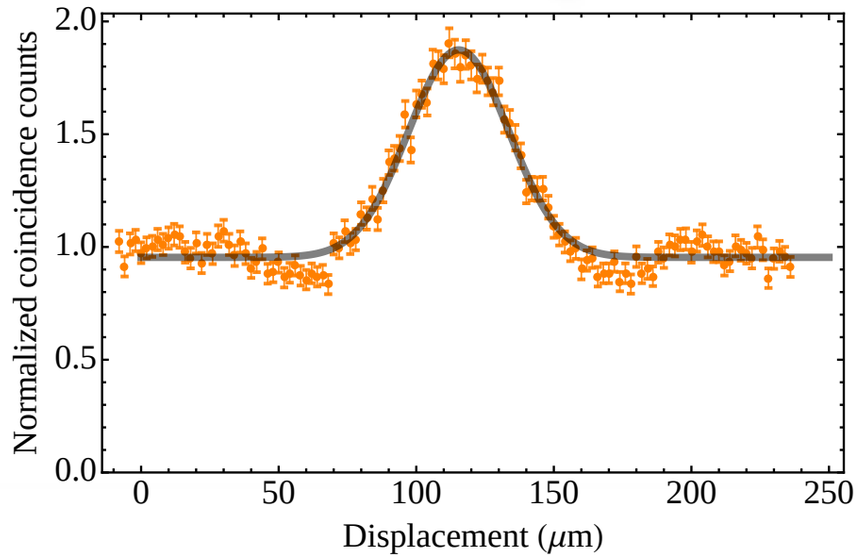
F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Optimal Cloning Attack: Hong-Ou-Mandel



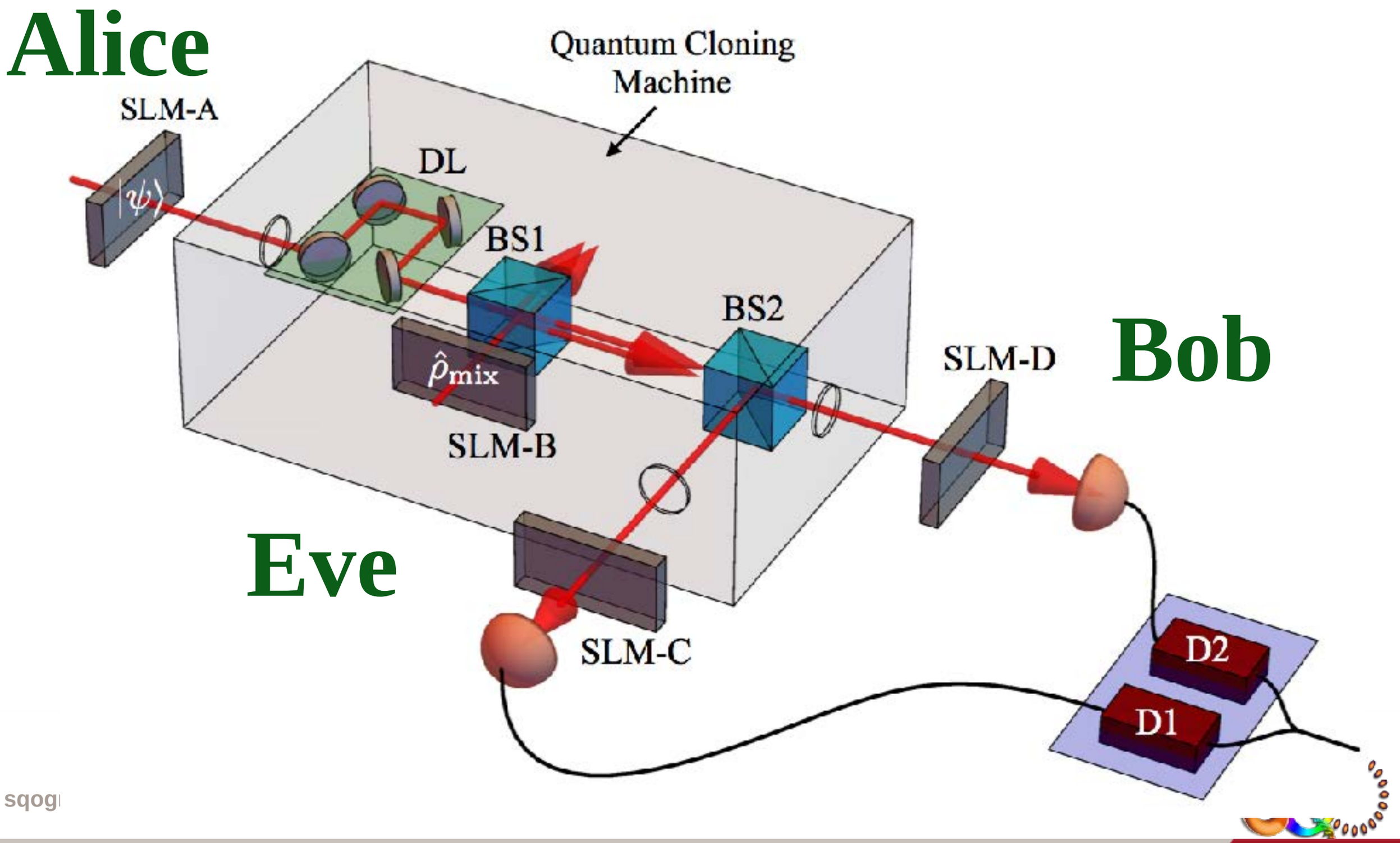






F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Optimal Cloning Attack: Experimental Setup



F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Optimal Cloning Attack: Experimental Setup

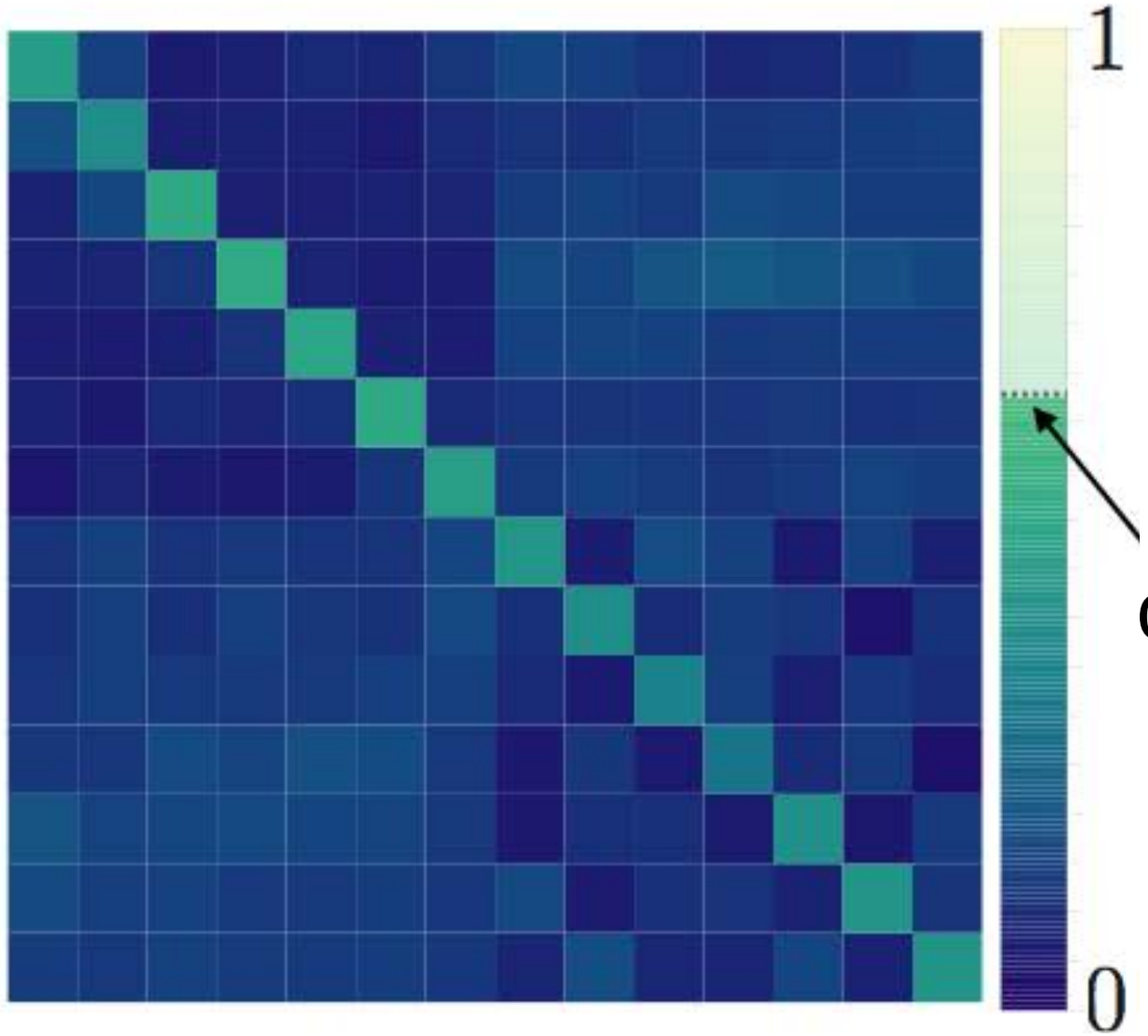
F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Optimal Cloning Attack: Experimental Results

$\{|\psi\rangle_i\}$

ALICE

$\{|\phi\rangle_j\}$

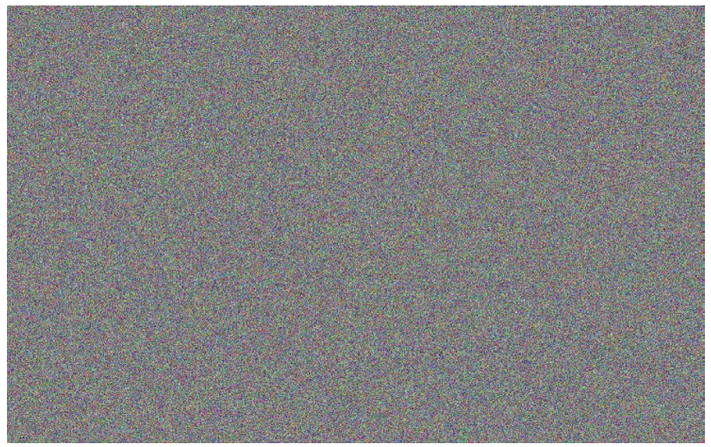


Optimal cloning attack

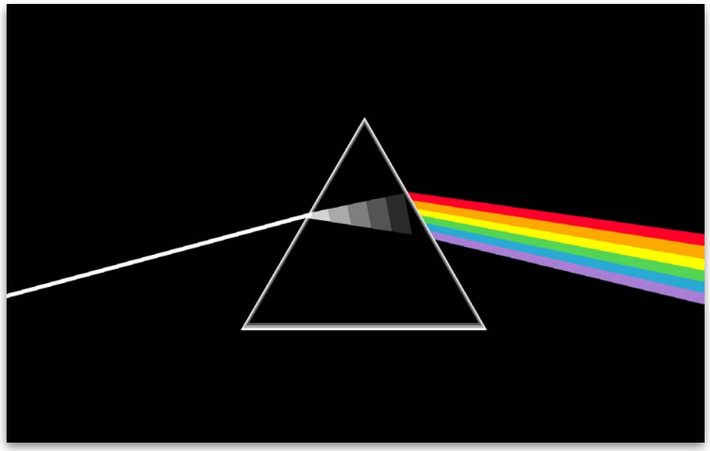
F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Secure Channel under Cloning Attack

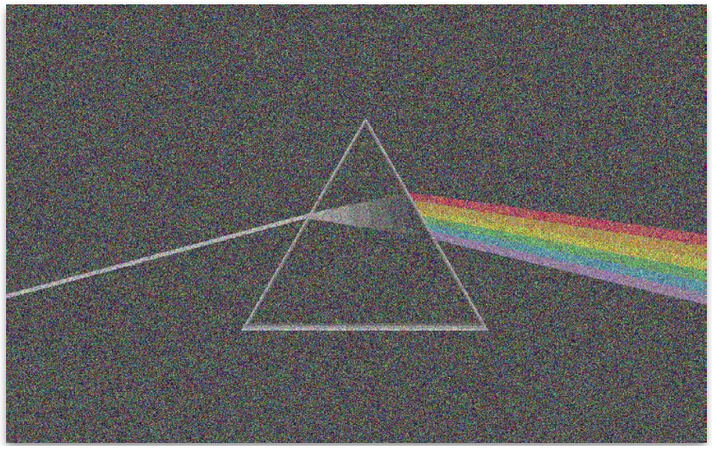
Encrypted message



Sender (Alice)

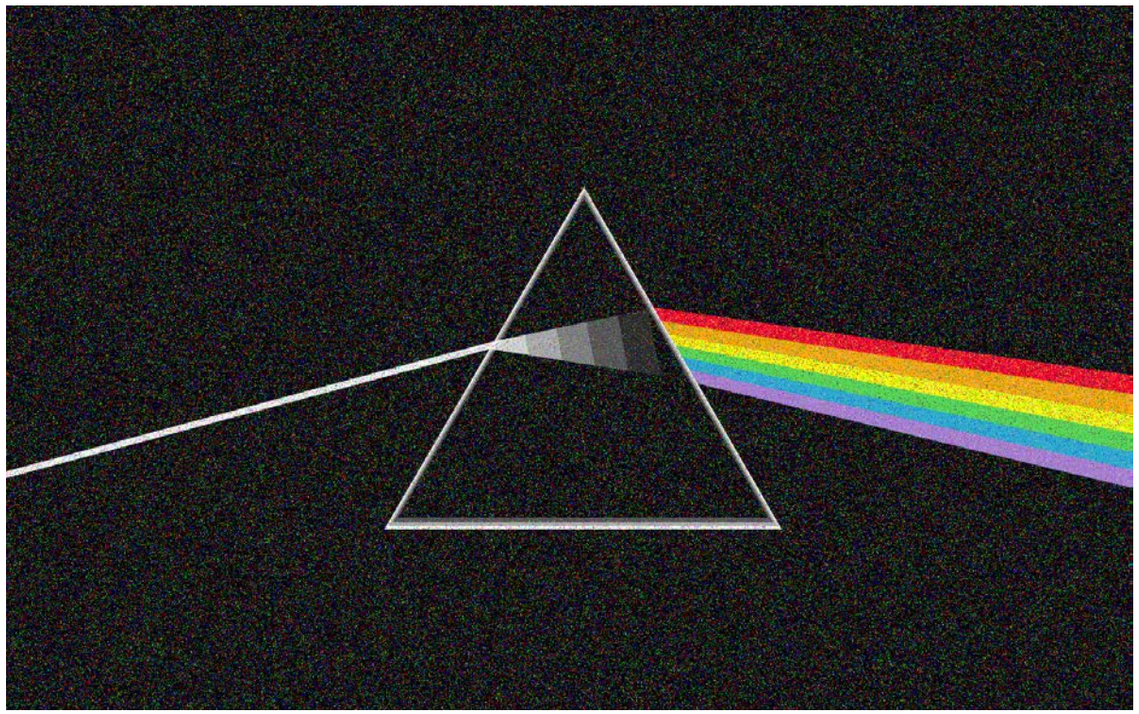


Receiver (Bob)

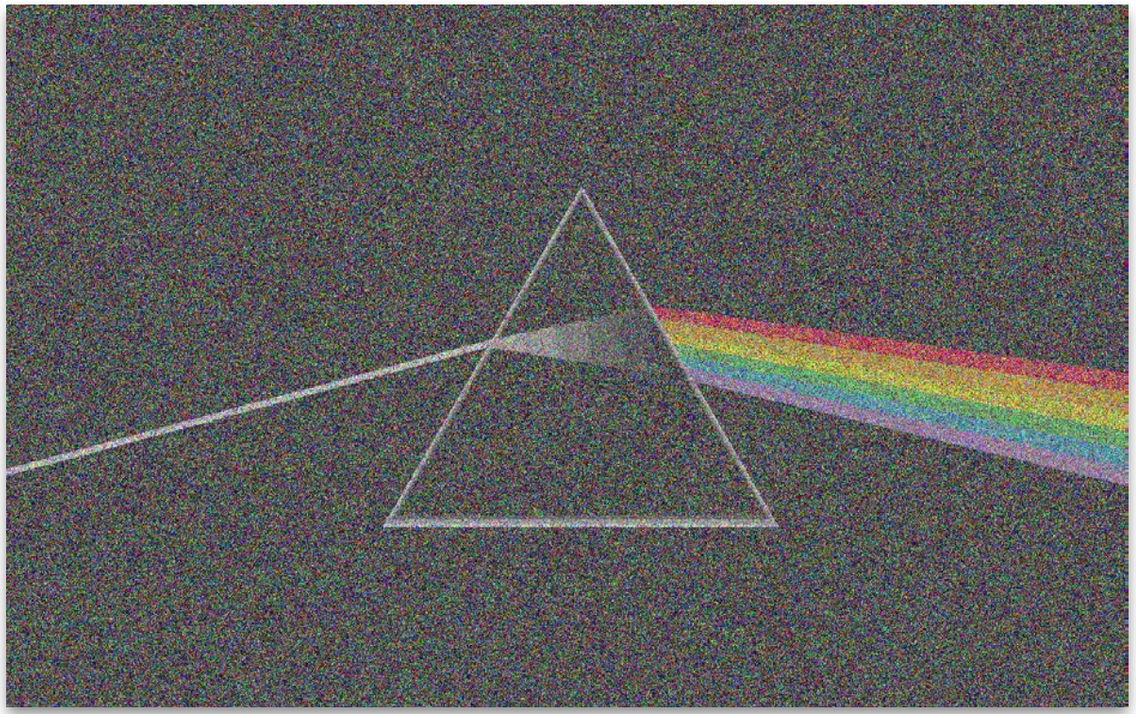


F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

Secure link

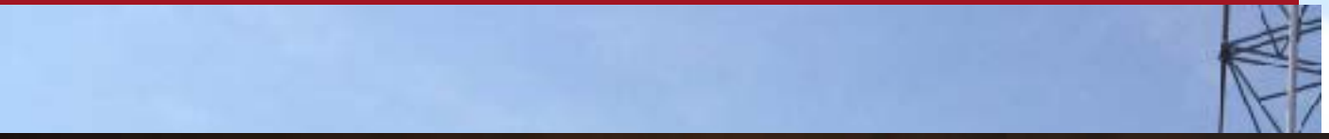


Cloning attack

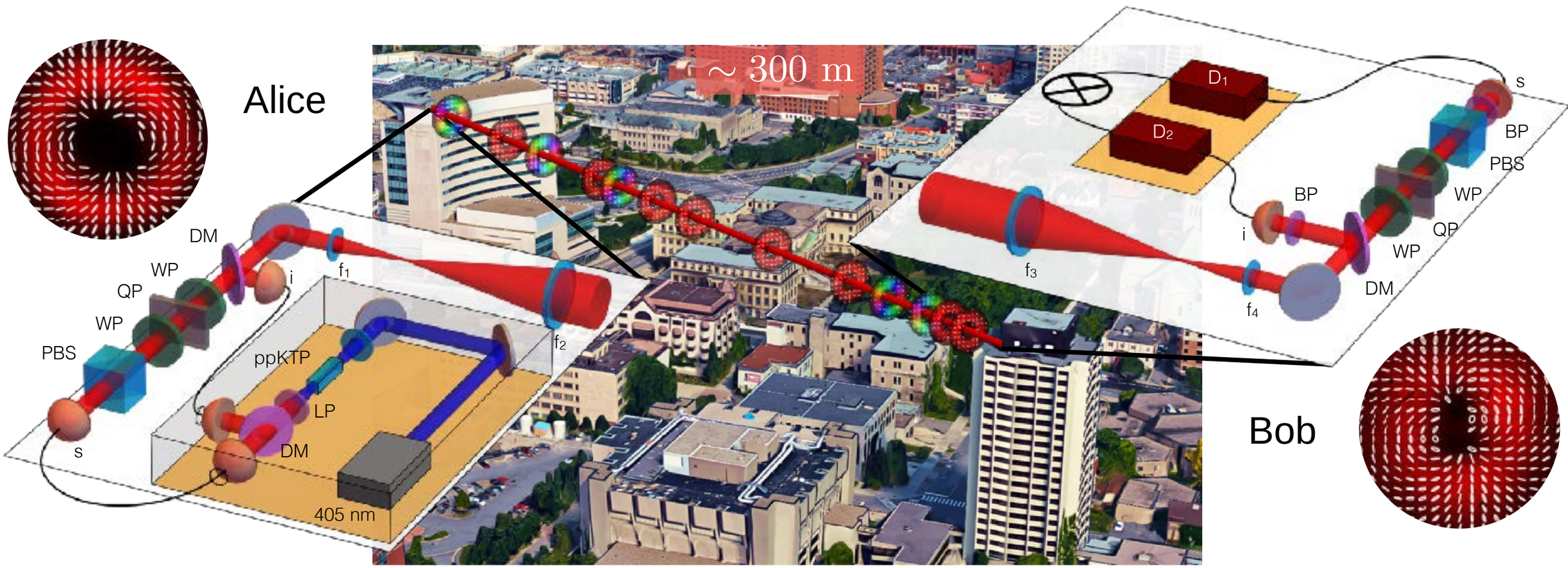


F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, *in press*

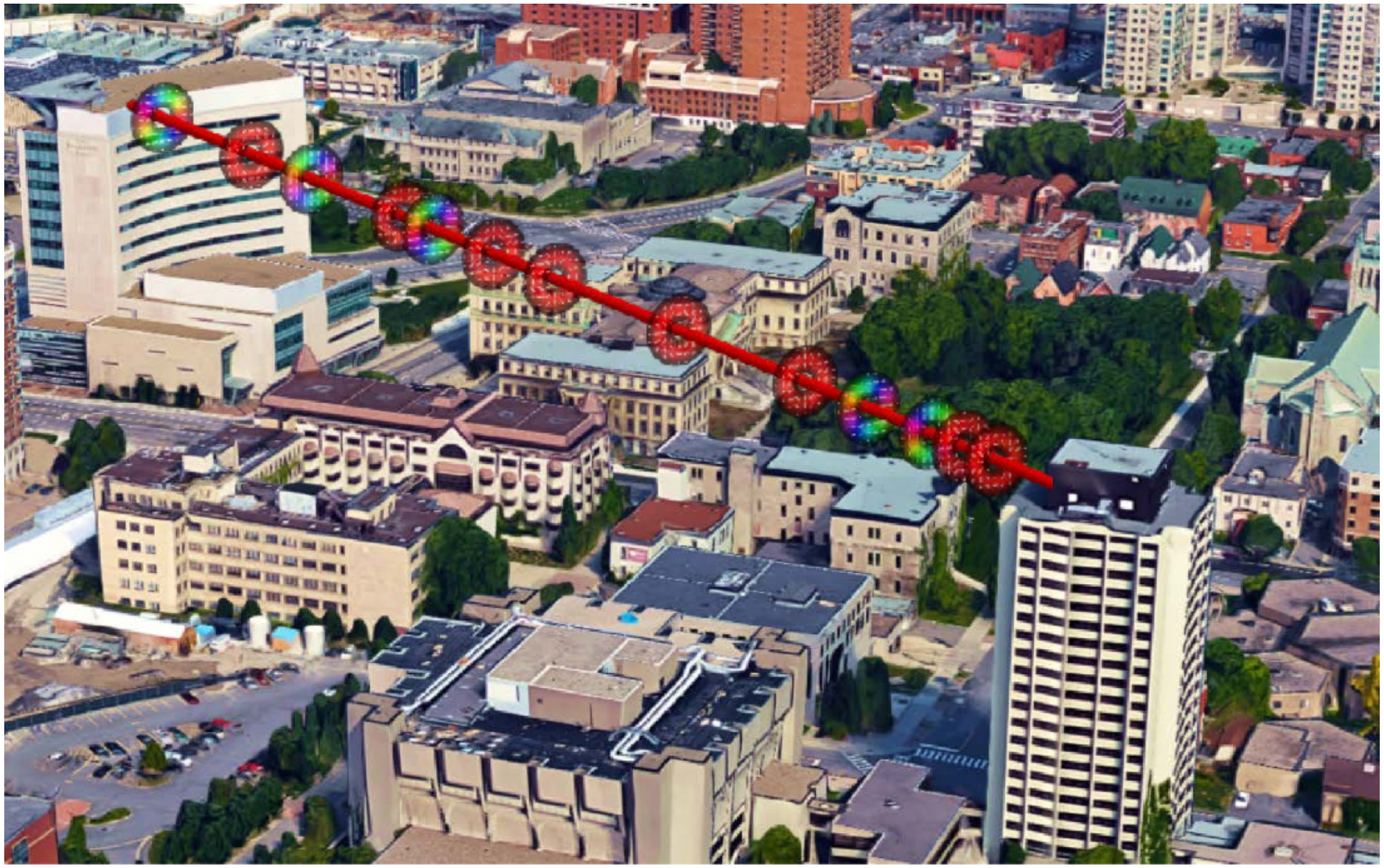
QKD over the city of Ottawa

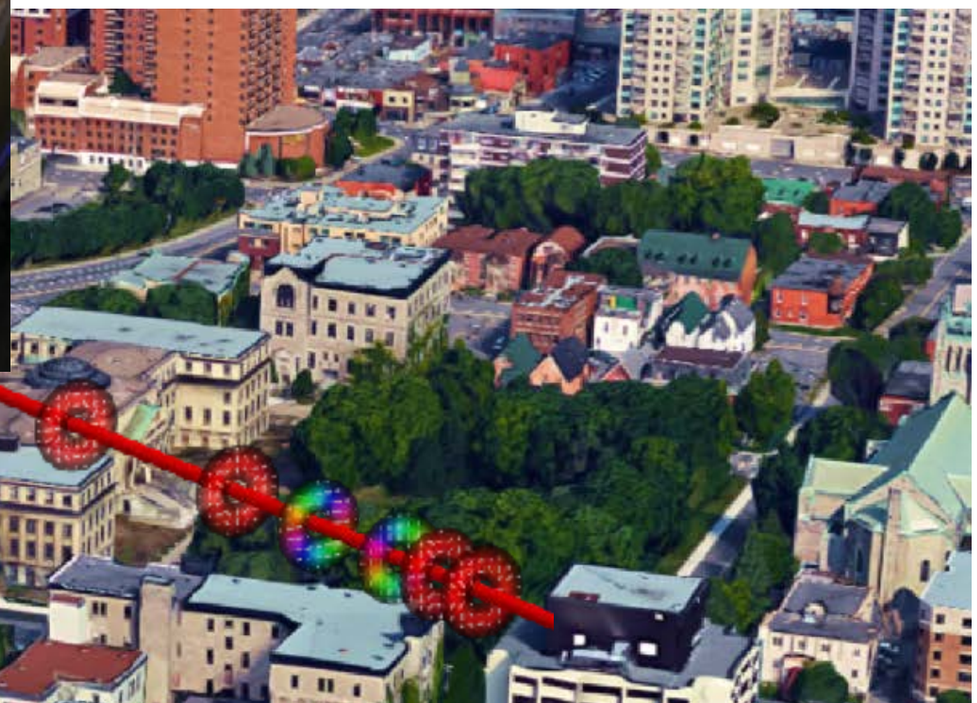


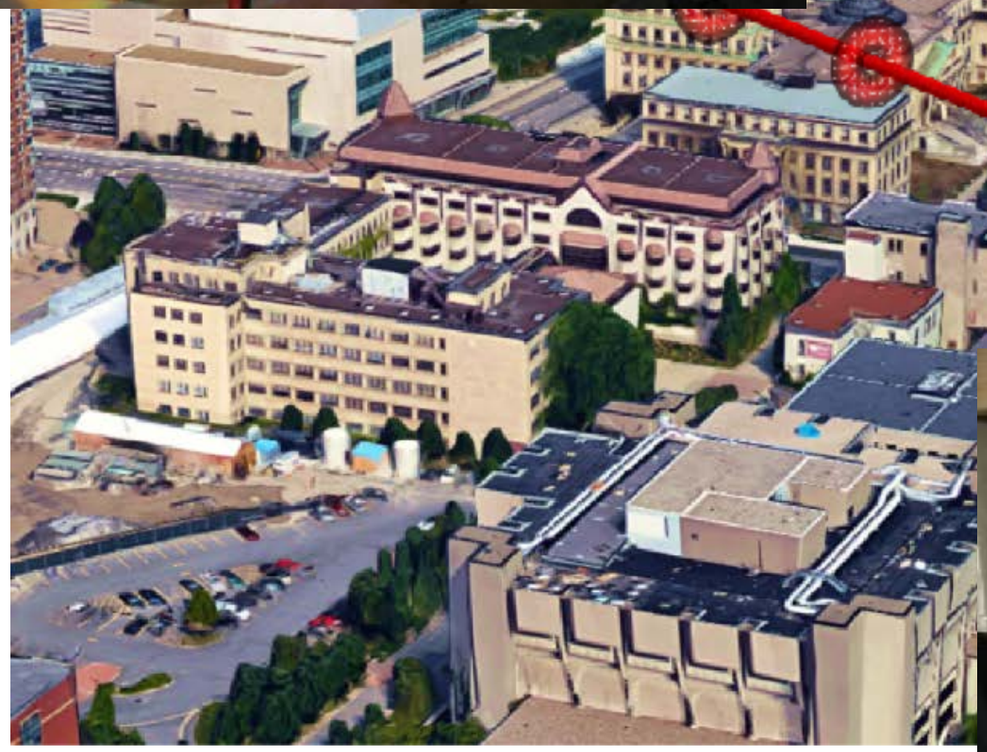
Intra-city QKD experiment



A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, arXiv:1612.05195.

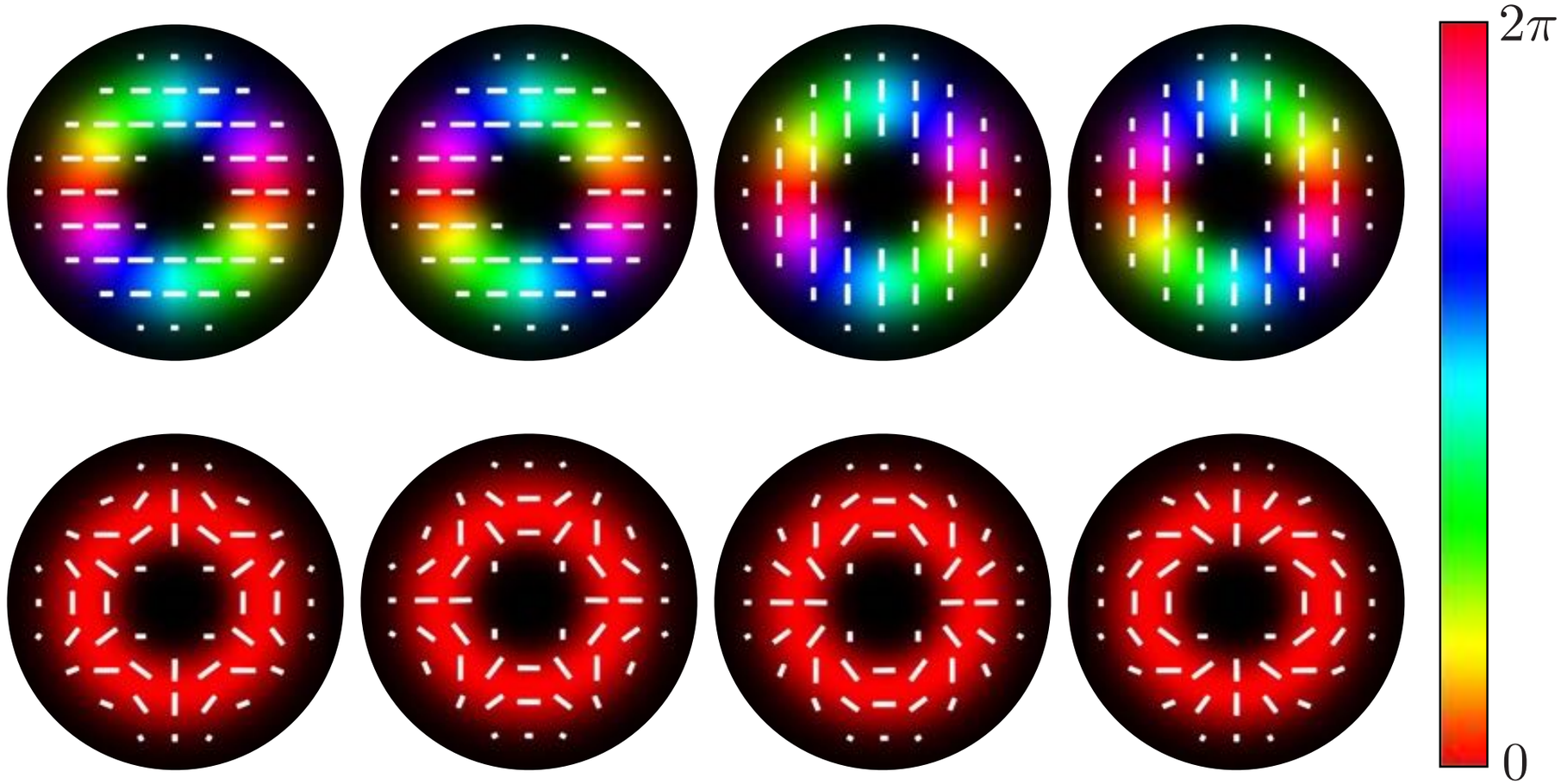






Degrees of freedom of light

$\{|\psi\rangle^i\}$

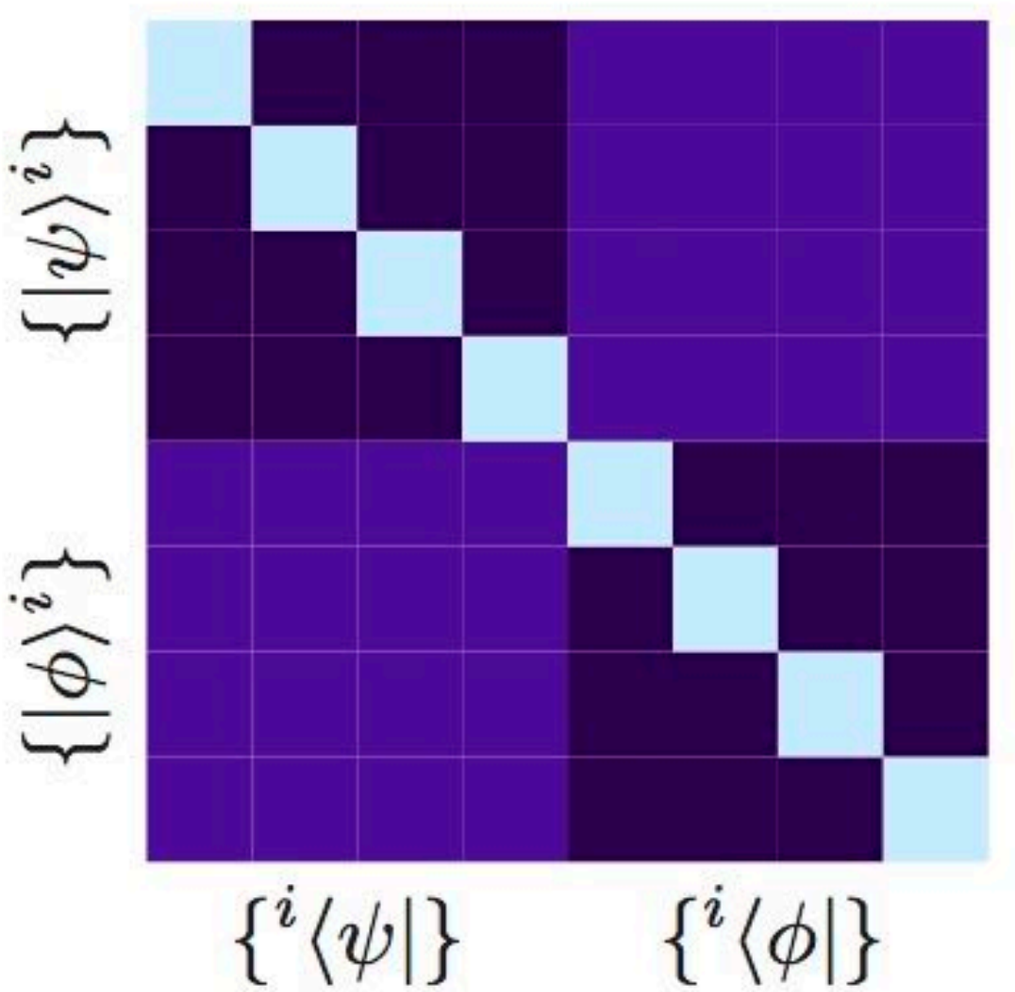


$\{|\phi\rangle^i\}$

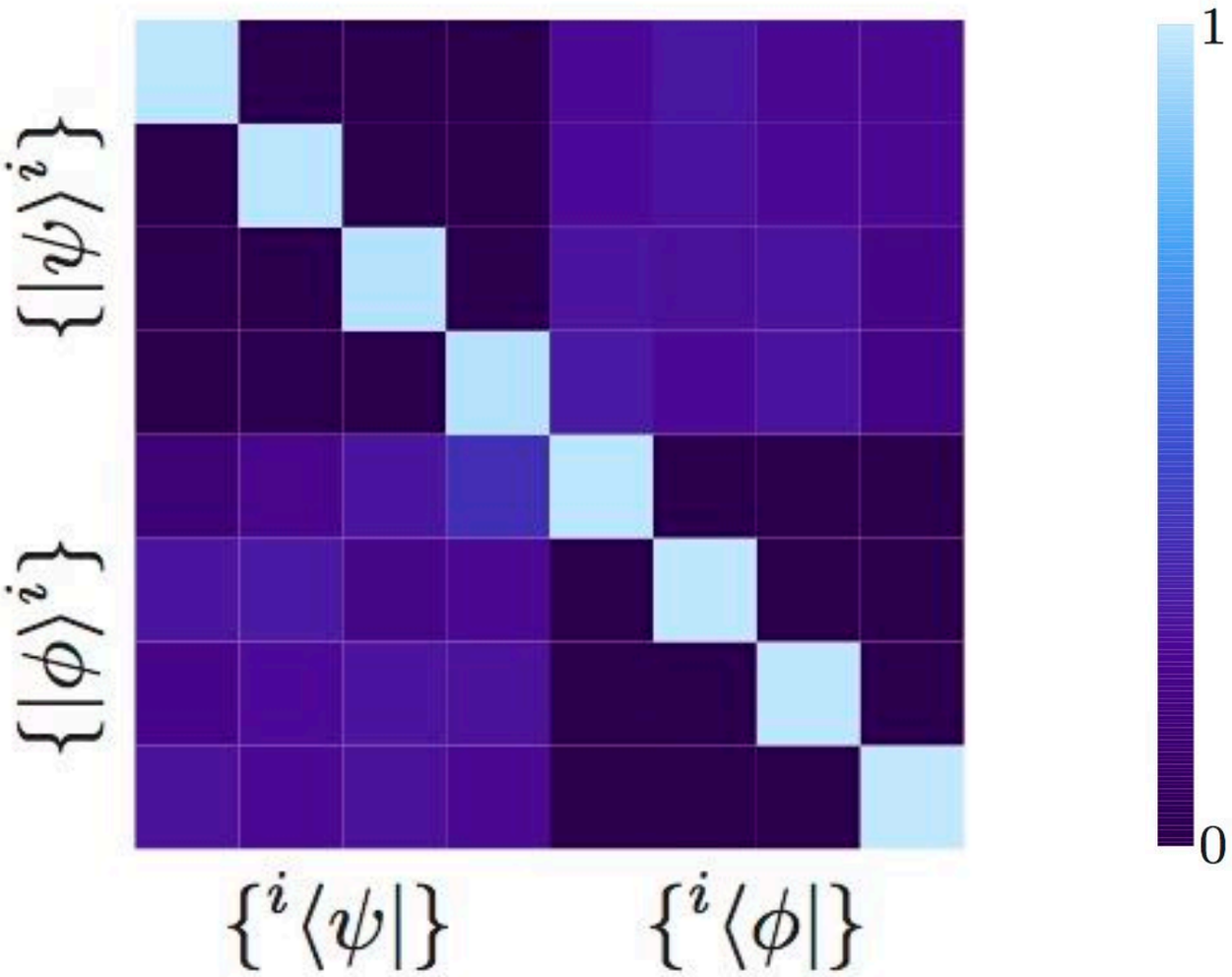
A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, arXiv:1612.05195.

Laboratory results

Theory

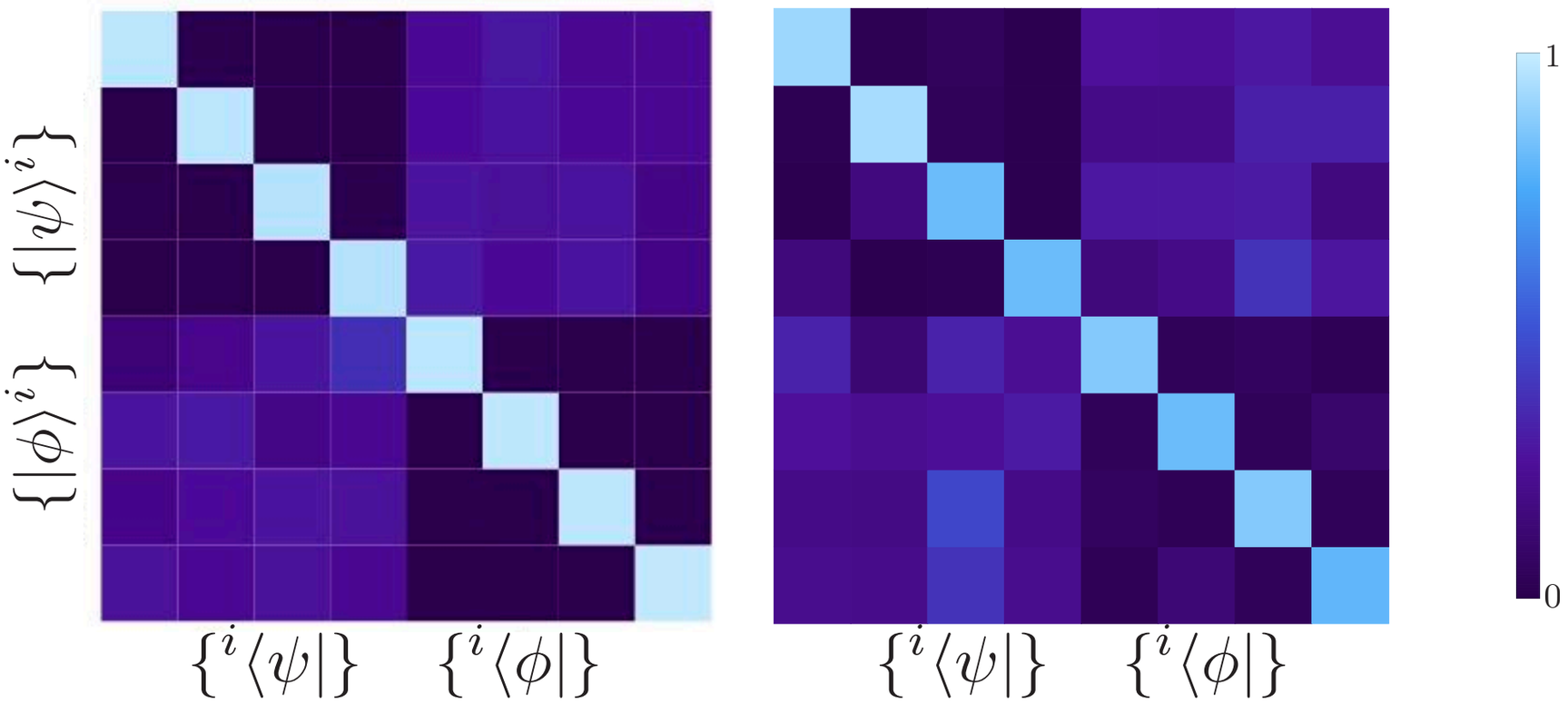


Experiment



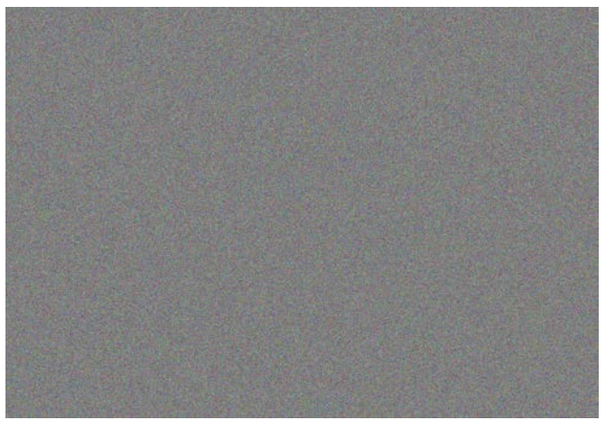
A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, arXiv:1612.05195.

Experimental results of intra-city QKD



Alice

Encrypted

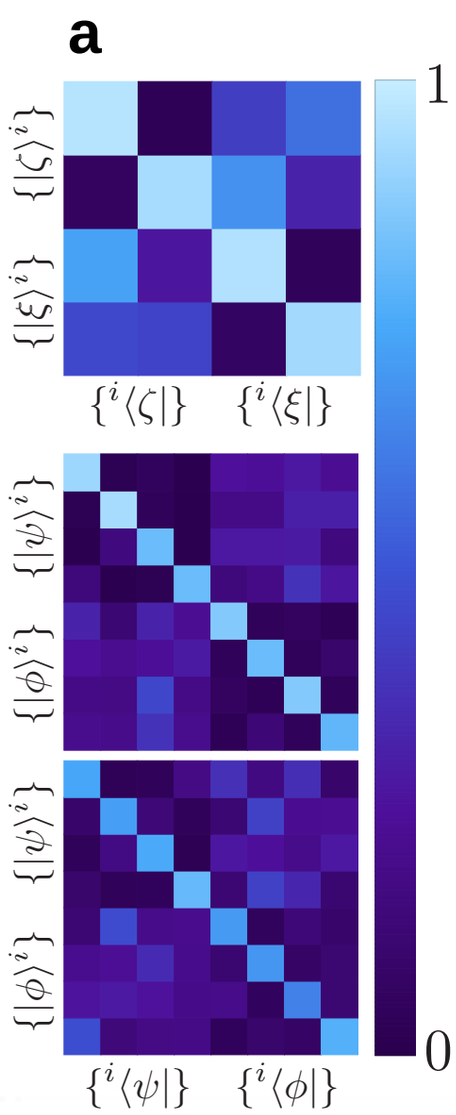


Bob

sqogroup.ca

A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, arXiv:1612.05195.

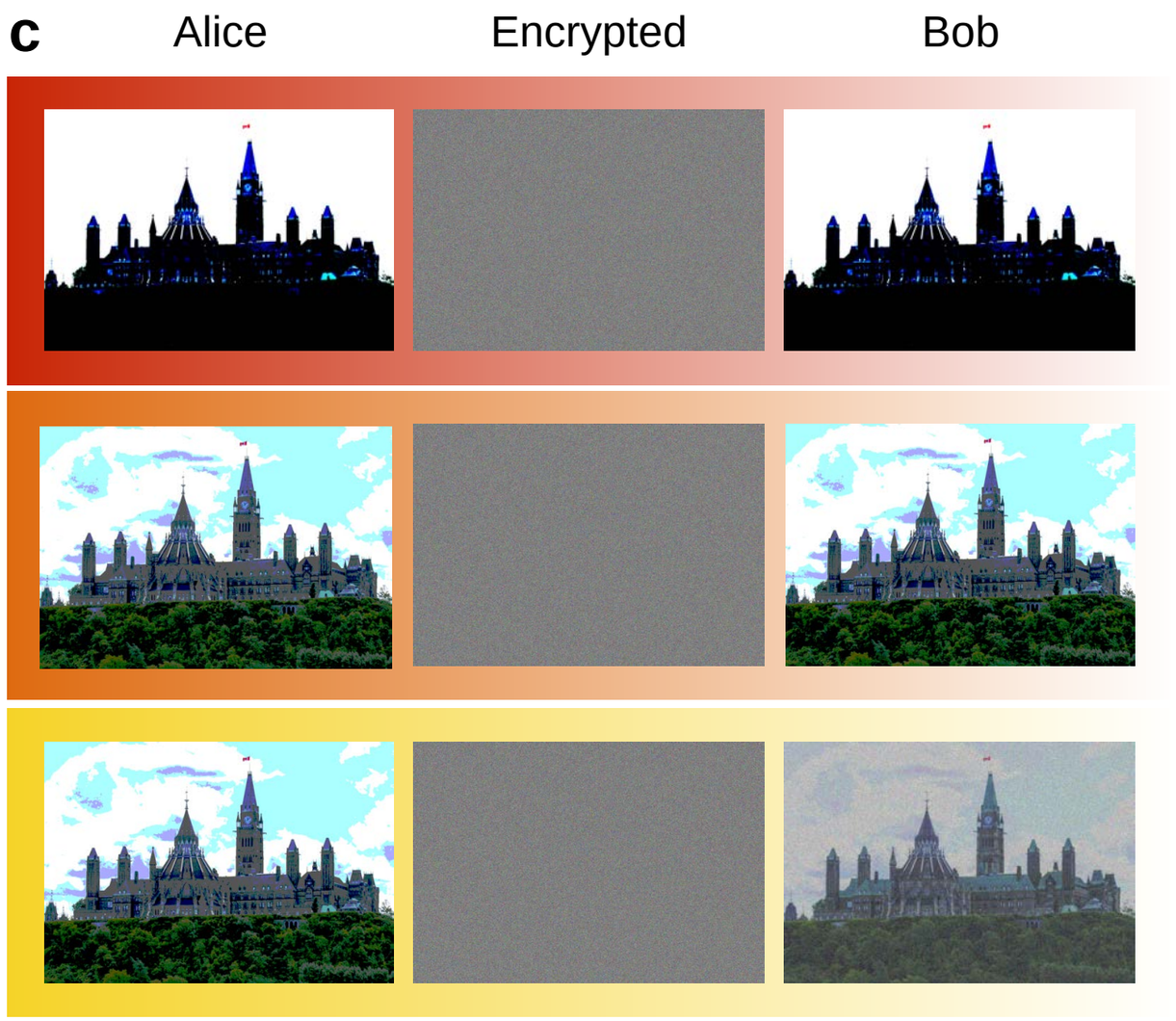
Experimental results of intra-city QKD



2D

4D

4D with errors

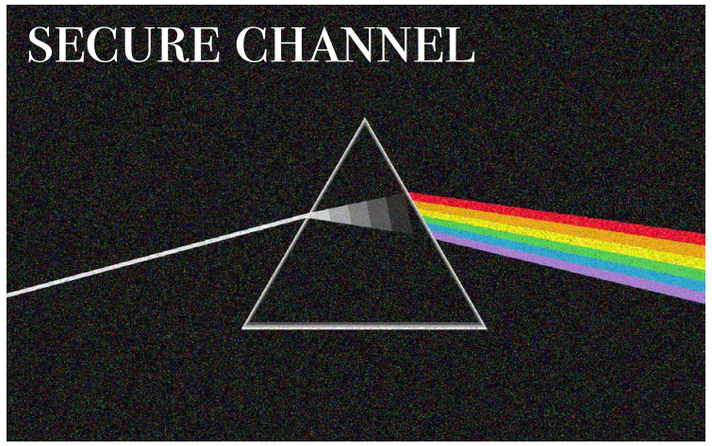


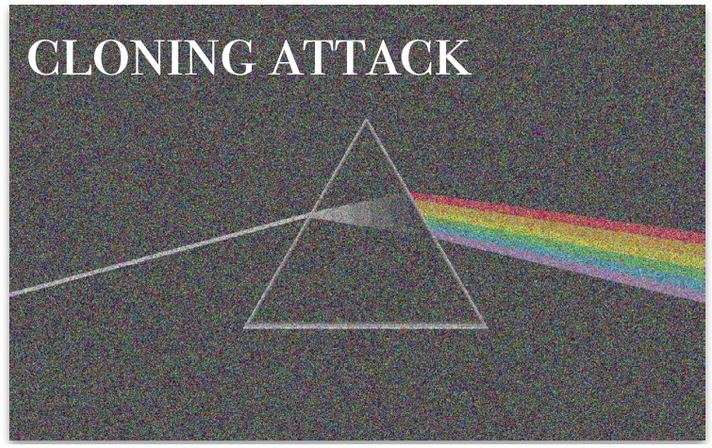
sqogroup.ca

A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, arXiv:1612.05195.

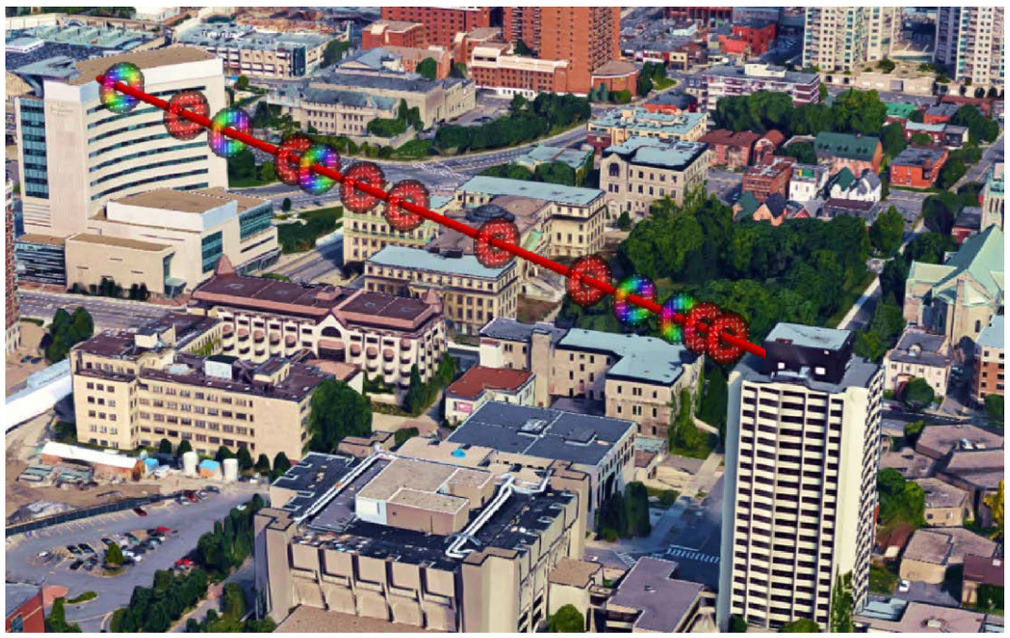
QKD

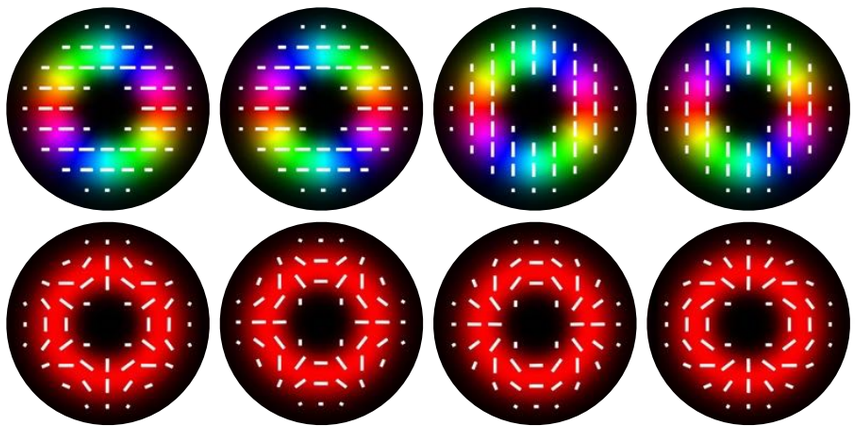
More information per carrier





They are robust in a noisier channel





SQ team


LE SYMPOSIUM SCHAWLOW-TOWNES SUR LA PHOTONIQUE - 2016
THE SCHAW TOWNES SYMPOSIUM ON PHOTONICS - 2016

Funding agencies

Canada Excellence Research Chairs

Chaires d'excellence en recherche du Canada

Canada Research Chairs

www.chairs-chaires.gc.ca

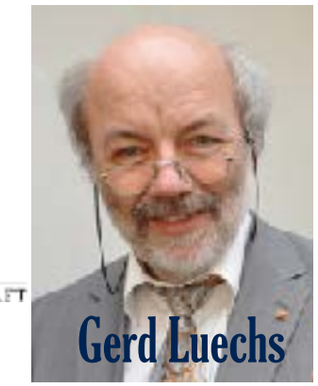
NSERC CRSNG

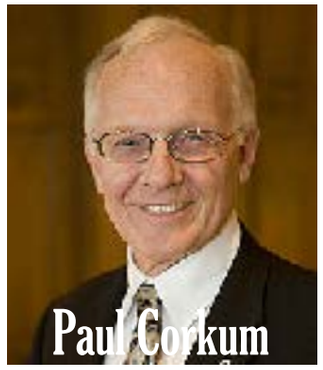
uOttawa

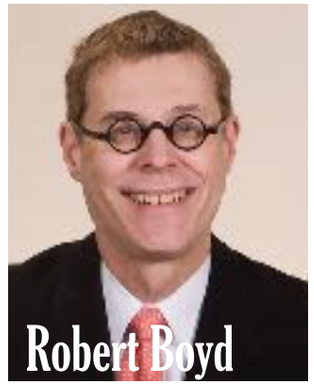
INNOVATION.CA

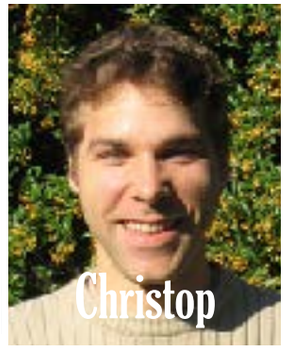
CANADA FOUNDATION FOR INNOVATION | FONDATION CANADIENNE POUR L'INNOVATION

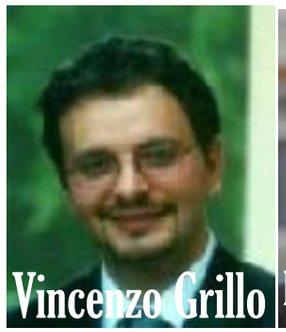
Collaborators

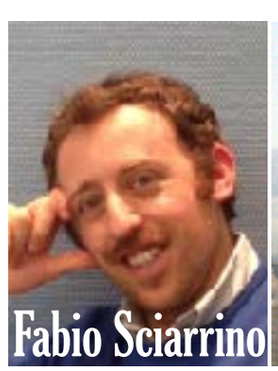












…, and many junior members of these research teams