# Private-Key Quantum Cryptography with Boson Sampling devices†

Zixin Huang[1], Peter P. Rohde, Dominic Berry,
Pieter Kok[1], Jonathan P. Dowling, Cosmo Lupo

[1] Center for Engineered Quantum Systems, Department of Physics and Astronomy, Macquarie University

Louisiana State University, May 2021

† Dedicated to the memory of Professor Jonathan P. Dowling

Quantum 5, 447

# Outline

Boson Sampling

Protocol

Quantum data locking

Sketch security proof

Quantum 5, 447

# A bit of cheek from Jon...

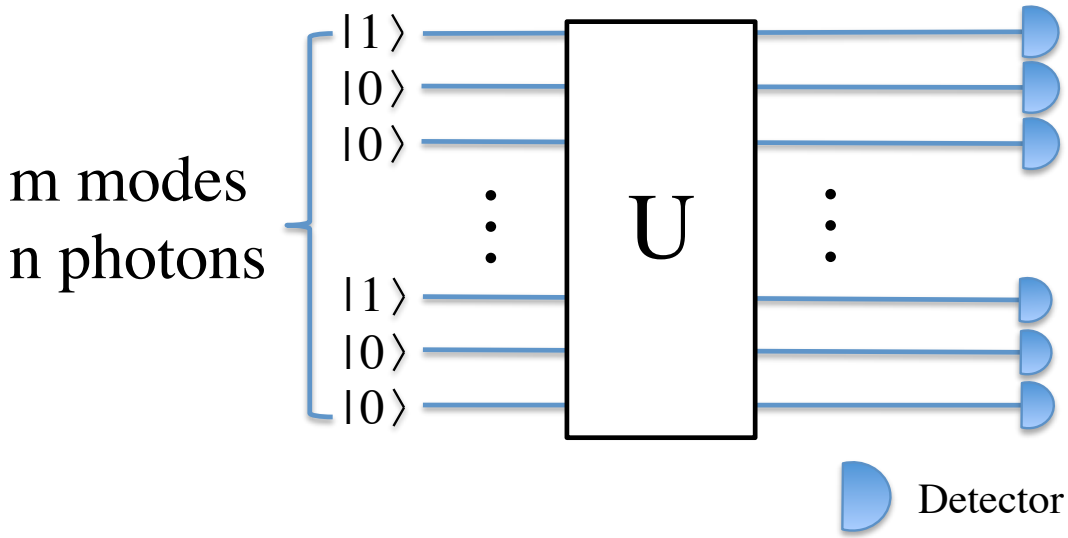
**Submission history**

From: Zixin Huang [view email]
[v1] Wed, 8 May 2019 11:40:39 UTC (92 KB)
[v2] Tue, 21 Jul 2020 12:13:07 UTC (110 KB)
**[v3]** Sat, 24 Apr 2021 08:54:37 UTC (123 KB)

As we outlined, we meet the acceptance criteria as followed:

- *Open a new research area, or a new avenue within an established area*:
  We show a deep and interesting connection between Boson sampling devices and cryptography.
- *Solve, or make essential steps towards solving, a critical problem:*
  We have an information theoretic security proof (i.e., the highest standard of proof) that uses multiphoton states in quantum communication.
- *Be of unusual intrinsic interest to PRL's broad audience*:
  We have taken ideas from Boson Sampling, which are inherently interesting to complexity theorists, and turned it into an information-theoretic proof for quantum cryptography. Therefore our work is "exceptionally pleasing science, aesthetically", having combined the two fields.

# Boson Sampling

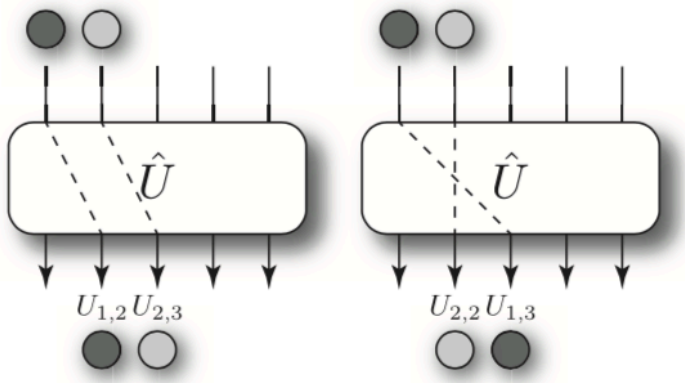



For an $n-$photon input Fock state, output photon distribution is proportional to the permanent of an $n \times n$ submatrix of $U$

[1] S. Scheel, arXiv preprint quant-ph/0406127 (2004)
[2] S. Aaronson and A. Arkhipov, Quantum Information & Computation 14, 1383 (2014)

# Boson Sampling

$$U a_i^\dagger U^\dagger = \sum_{j=1}^{m} U_{i,j} a_j^\dagger \tag{1}$$




$$\gamma_{\{2,3\}} = \underbrace{U_{1,2}U_{2,3}}_{\text{walkers don't swap}} + \underbrace{U_{1,3}U_{2,2}}_{\text{walkers swap}}$$

$$= \text{Per}\begin{bmatrix} U_{1,2} & U_{2,2} \\ U_{1,3} & U_{2,3} \end{bmatrix},$$

Image taken from T. Gard et al., Gard, Bryan T., et al. "An introduction to boson-sampling." From atomic to mesoscale: The role of quantum coherence in systems of various complexities. 2015. 167-192.

# Boson Sampling

## Experimental validation of photonic boson sampling

Nicolò Spagnolo, Chiara Vitelli, Marco Bentivegna, Daniel J. Brod, Andrea Crespi, Fulvio Flamini, Sandro Giacomini, Giorgio Milani, Roberta Ramponi, Paolo Mataloni, Roberto Osellame ✉, Ernesto F. Galvão ✉ & Fabio Sciarrino ✉

*Nature Photonics* **8**, 615–620(2014) | Cite this article

REPORT

## Photonic Boson Sampling in a Tunable Circuit

Matthew A. Broome[1,2,*], Alessandro Fedrizzi[1,2], Saleh Rahimi-Keshari[2], Justin Dove[3], Scott Aaronso…

+ See all authors and affiliations

*Science* 15 Feb 2013:
Vol. 339, Issue 6121, pp. 794-798
DOI: 10.1126/science.1231440

Published: 01 May 2017

## High-efficiency multiphoton boson sampling

Hui Wang, Yu He, Yu-Huai Li, Zu-En Su, Bo Li, He-Liang Huang, Xing Ding, Ming-Cheng Chen, Chang Liu, Jian Qin, Jin-Peng Li, Yu-Ming He, Christian Schneider, Martin Kamp, Cheng-Zhi Peng, Sven Höfling, Chao-Yang Lu ✉ & Jian-Wei Pan ✉

*Nature Photonics* **11**, 361–365(2017) | Cite this article

**3062** Accesses | **168** Citations | **128** Altmetric | Metrics

Published: 12 May 2013

## Experimental boson sampling

Max Tillmann ✉, Borivoje Dakić, René Heilmann, Stefan Nolte, Alexander Szameit & Philip Walther ✉

*Nature Photonics* **7**, 540–544(2013) | Cite this article

**1413** Accesses | **369** Citations | **91** Altmetric | Metrics

REPORT

## Boson Sampling on a Photonic Chip

Justin B. Spring[1,*], Benjamin J. Metcalf[1], Peter C. Humphreys[1], W. Steven Kolthammer[1], Xian-Min Ji…

+ See all authors and affiliations

*Science* 15 Feb 2013:
Vol. 339, Issue 6121, pp. 798-801
DOI: 10.1126/science.1231692

Featured in Physics | Editors' Suggestion

## Boson Sampling with 20 Input Photons and a 60-Mode Interferometer in a $10^{14}$-Dimensional Hilbert Space

Hui Wang, Jian Qin, Xing Ding, Ming-Cheng Chen, Si Chen, Xiang You, Yu-Ming He, Xiao Jiang, L. You, Z. Wang, C. Schneider, Jelmer J. Renema, Sven Höfling, Chao-Yang Lu, and Jian-Wei Pan

Phys. Rev. Lett. **123**, 250503 – Published 18 December 2019

Physics See Synopsis: Quantum Computers Approach Milestone for Boson Sampling

# Cryptography using Boson Sampling

- Boson Sampling: photon number-path entanglement [3], difficult to crack classically – what about by a quantum computer?
- First information-theoretic proof that Boson Sampling is useful for cryptography.
- Move out of the no-collision regime – efficient scaling of Hilbert space
- "Quantum enigma machine" [4]

"Useful" – efficient QKD or can encrypt a message longer than the key.

[3] Motes et. al., PRL 114, 170802 (2015)
[4] Guha et. al., Phys. Rev. X 4, 011016 (2014)
[6] Motes et al., Phys. Rev. Lett. 114, 170802 (2015)
[7] Huh et al., Nat. Photon. 9, 615 (2015)

# The enigma machine

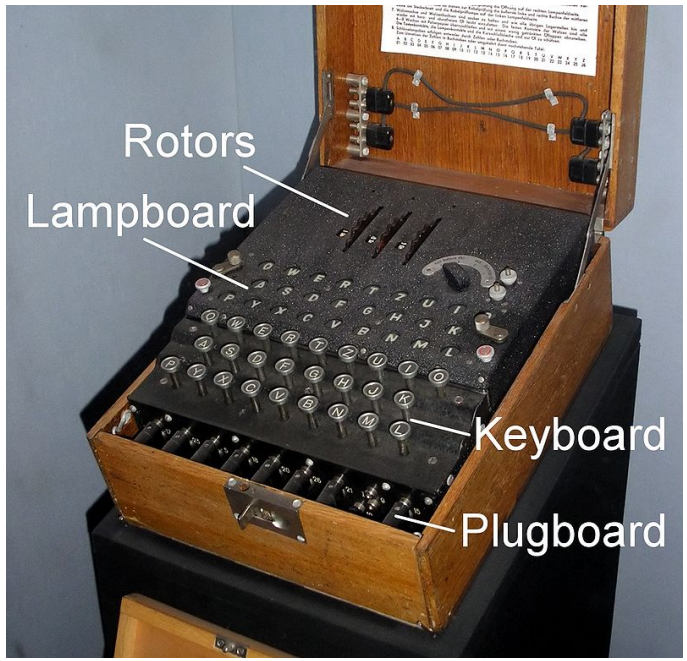


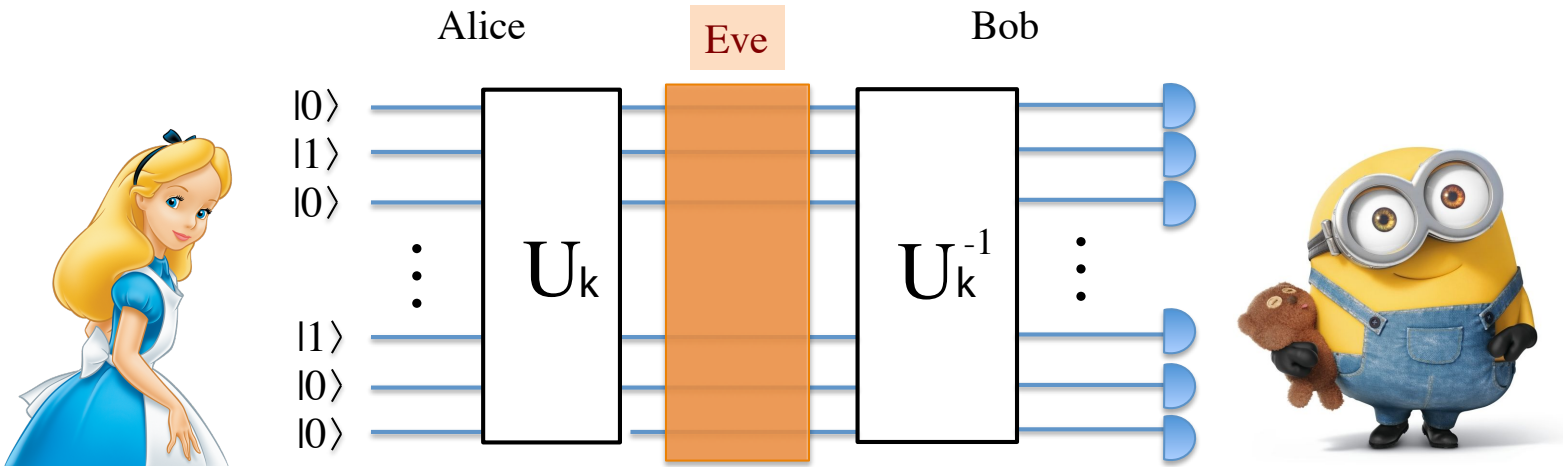

Figure: Image taken from Wikipedia

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: LUSHQOXDMZNAIKFREPCYBWVGTJ

Quantum state: you get one measurement.

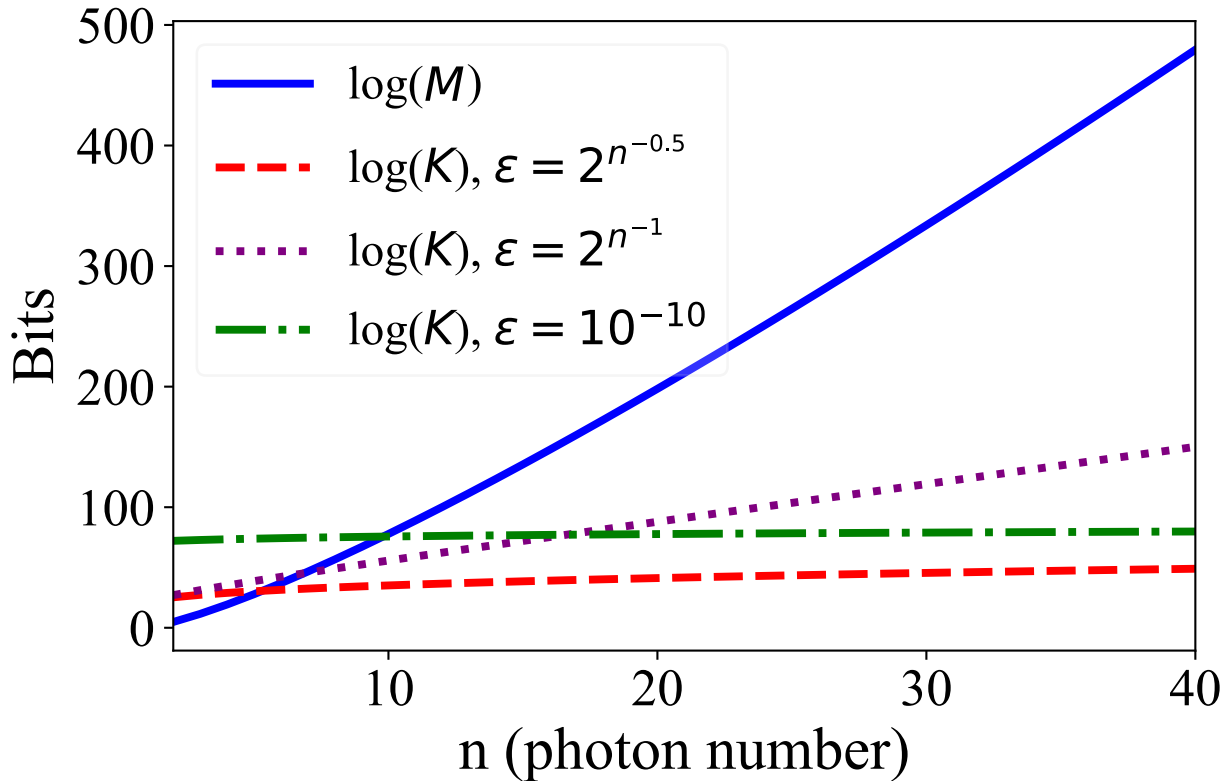
# Boson Sampling inspired cryptography




1. The code words $|\psi_x\rangle$ are chosen from the $M = \binom{m}{n}$ possible configurations, $\log \binom{m}{n}$ bits transmitted.
2. Alice and Bob pre-share a $K$-bit secret key
3. In advance, Alice and Bob agree upon a set of $K$ Haar-random $m \times m$ unitary matrices, $U_k$.
4. Alice encrypts the quantum state $|\psi_x\rangle$ by applying $U_k$ associated with the key, she sends this state.
5. Bob decrypts using $U_k^\dagger$.

# Boson Sampling inspired cryptography

Net secure communication rate $= \log M - \log K$




Asymptotic communication and secret key rates, $m = n^3$.

Quantum 5, 447

# Framework & Relation to Boson Sampling

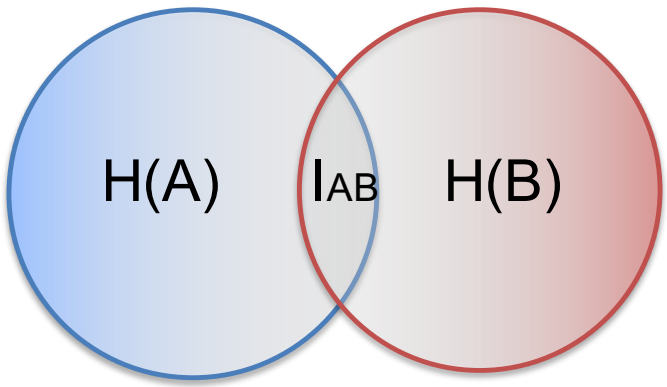
- Technical results from Aaronson & Arkhipov are crucial in calculating the key consumption, but the classical computation complexity of Boson Sampling is not required.
- We go beyond the no-collision regime
- Use accessible information as security quantifier — quantum data locking [8,9].
- Bounded quantum memories: Eve can store quantum information for no longer than a limited (known) time.

[8] D. P. DiVincenzo et al., Phys. Rev. Lett. 92, 067902 (2004).
[9] S. Guha et al., Phys. Rev. X 4, 011016 (2014).

# Mutual information

$X$ is a random variable with $M$ outcomes, each occuring with probability $\{p_x\}$

$$H(X) = -\sum_{x}^{M} p_x \log_2(p_x) \tag{2}$$




$$I(A;B) = H(A) + H(B) - H(A,B)$$
$$I_{\text{acc}}(A;B) = \max_{M_B}\{I(A;B)\} \tag{3}$$

# Quantum data locking

Alice to Bob:

$$\rho = \frac{1}{M}\sum_{x=1}^{M} |\psi_x\rangle\langle\psi_x| \qquad \rightarrow I(X;YK) = \log_2 M$$

Alice to Eve: ($\log K$ bits of information missing)

$$\rho = \frac{1}{M}\sum_{x=1}^{M}\sum_{t=1}^{K} U_t |\psi_x\rangle\langle\psi_x| U_t^\dagger \qquad \rightarrow I(X;Y) = ??$$

Classically

$$I(X;YK) - I(X;Y) = I(X;K|Y) \leq H(K) \leq \log_2 K \qquad (4)$$

Quantum data locking

$$I_{\text{acc}}(X;YK) - I_{\text{acc}}(X;Y) \gg \log_2 K \qquad (5)$$

# Boson Sampling inspired cryptography

The goal is to upper bound $I_{acc}(X;E)$, with high probability.

$$I_{acc}(X;E) \leq 2\epsilon \log M, \qquad M \sim \binom{m}{n} \tag{6}$$

Accessible information (Eve with finite-time quantum memory)

$$I_{acc}(X;E) = \max_{\mathcal{M}_E} [H(X) + H(E) - H(X,E)] \tag{7}$$

Bob:

$$\rho_A = \frac{1}{M} \sum_{x=1}^{M} |\psi_x\rangle \langle\psi_x| \tag{8}$$

Eve:

$$\rho_{AE} = \frac{1}{M} \sum_{x=1}^{M} |x\rangle \langle x| \otimes \frac{1}{K} \sum_{t}^{K} U_t |\psi_x\rangle \langle\psi_x| U_t^\dagger. \tag{9}$$

Quantum 5, 447

# Sketch security proof

$$\rho_{AE} = \frac{1}{M}\sum_{x=1}^{M} |x\rangle\langle x| \otimes \underbrace{\frac{1}{K}\sum_{t}^{K} U_t |\psi_x\rangle\langle\psi_x| U_t^\dagger}_{\rho_E^x}. \qquad (10)$$

Eve's POVM elements

$$\{\alpha_y |\phi\rangle\langle\phi|\}, \qquad \sum_y \alpha_y |\phi\rangle\langle\phi| = \mathbb{1} \qquad (11)$$

$$I(X;Y) = \sum_y \alpha_y \Big\{ - \langle\phi_y|\rho_{AE}|\phi_y\rangle \log \langle\phi_y|\rho_{AE}|\phi_y\rangle + \frac{1}{M'}\sum_{x=1}^{M'} \langle\phi_y|\rho_E^x|\phi_y\rangle \log \langle\phi_y|\rho_E^x|\phi_y\rangle \Big\}. \qquad (12)$$

# Matrix Chernoff bound

**Theorem**

*Let $\{X_t\}_{t=1,\ldots,T}$ be $T$ i.i.d. $d$-dimensional Hermitian-matrix-valued random variables, with $\mathbb{E}[X] = \mu\mathbb{1}$ Then, for $\delta \geq 0$ [10]:*

$$\Pr\left\{\frac{1}{T}\sum_{t=1}^{T} X_t \not\leq (1+\delta)\mathbb{E}[X]\right\} \leq d\exp\left\{-\frac{T\delta^2\mu}{4\ln 2}\right\}. \tag{13}$$

The matrix Chernoff bound implies

$$\frac{1}{M'}\sum_{x=1}^{M'} \rho_E^x \leq (1+\epsilon)\bar{\rho}_E \tag{14}$$

holds true with almost unit probability.

[10] R. Ahlswede and A. Winter, IEEE Transactions on Information Theory 48, 569 (2002).

# Sketch security proof

2. We apply a tail bound from A. Maurer to show that

$$\langle\phi|\rho_E^x|\phi\rangle \geq (1-\epsilon)\langle\phi|\bar{\rho}_E|\phi\rangle\,, \tag{15}$$

**Theorem**

*[11] Let $\{X_k\}_{k=1,\ldots,K}$ be $K$ i.i.d. non-negative real-valued random variables, with $X_k \sim X$ and finite first and second moments, $\mathbb{E}[X], \mathbb{E}[X^2] < \infty$. Then, for any $\tau > 0$ we have that*

$$\Pr\left\{\frac{1}{K}\sum_{k=1}^{K} X_k < (1-\tau)\mathbb{E}[X]\right\} \leq \exp\left(-\frac{K\tau^2\mathbb{E}[X]^2}{2\mathbb{E}[X^2]}\right). \tag{16}$$

$$\gamma = \frac{\mathbb{E}[X^2]}{\mathbb{E}[X]^2} \rightarrow \text{(Photon bunching modifies } \gamma\text{)}$$

[11] Maurer, J. Inequalities in Pure and Applied Mathematics 4, 15 (2003)

# Boson Sampling inspired cryptography

How it relates to Boson Sampling: calculate the key consumption $\gamma$, we need:

$$\begin{aligned} X =& |\langle\phi|U|\psi_x\rangle|^2, \\ =& \mathrm{Perm}[A]^* \mathrm{Perm}[A]. \end{aligned} \tag{17}$$

$$\mathbb{E}_U[X] = \frac{n!}{m^n} \tag{18}$$

The fourth moment of the permanent can be computed as [2]

$$\mathbb{E}_U[X^2] = \mathbb{E}_U[\mathrm{Perm}[A]^2 \mathrm{Perm}[A^*]^2] = \frac{n!(n+1)!}{m^{2n}}$$

$$\gamma = \frac{\mathbb{E}[X^2]}{\mathbb{E}[X]^2} \leq 2(n+1) \tag{19}$$

[2] S. Aaronson and A. Arkhipov, Quantum Information & Computation 14, 1383 (2014)

# sketch security proof

Then:

- Account for photon bunching
- Extend to all codewords $x$
- Extend to all vectors (Eve's) $|\phi\rangle$

Putting the above results together

$$I(X;Y) \leq 2\epsilon \log M \tag{20}$$

Provided

$$\log K \geq \log \gamma + \log \frac{d}{M} + O(\log 1/\epsilon)\,. \tag{21}$$

Quantum 5, 447

# Probability of failure

$$P_{\text{fail}} = \exp\left(\log 2d - \frac{\epsilon}{4}\sqrt{\frac{M' K c_{\min}}{2}}\right) + \exp\left[2d \log\left(\frac{20}{\epsilon c_{\min}}\right) + \frac{\epsilon M'}{4}\log M' - \frac{K M' \epsilon^3}{128\gamma}\right]. \quad (22)$$

This probability is exponentially suppressed if

$$K > 128\gamma\left[\frac{2}{\epsilon^3}\frac{d}{M'}\log\left(\frac{20}{\epsilon c_{\min}}\right) + \frac{1}{4\epsilon^2}\log M'\right]$$

$$\log K \sim \log\gamma + \log\frac{d}{M} + O(\log 1/\epsilon)\,. \quad (23)$$

# Scaling up the protocol

Consider a train of $\nu \gg 1$ signal transmissions. Alice encodes information in code words of the form

$$|\boldsymbol{\psi}_{\boldsymbol{x}}\rangle = |\psi_{x_1}\rangle \otimes |\psi_{x_2}\rangle \otimes \dots |\psi_{x_\nu}\rangle \,, \tag{24}$$

This in particular implies

$$\bar{\rho}_E^{(\nu)} := \mathbb{E}_{\boldsymbol{U}}[\boldsymbol{U}_{\boldsymbol{k}}|\boldsymbol{\psi}_{\boldsymbol{x}}\rangle\langle\boldsymbol{\psi}_{\boldsymbol{x}}|\boldsymbol{U}_{\boldsymbol{k}}^\dagger] = \bar{\rho}_E^{\otimes\nu} \,, \tag{25}$$

and therefore

$$c_{\min}^{(\nu)} := \min_\phi \langle\phi|\bar{\rho}_E^{(\nu)}|\phi\rangle = \min_\phi \langle\phi|\bar{\rho}_E^{\otimes\nu}|\phi\rangle = c_{\min}^{\nu} \tag{26}$$

$$\gamma^{(\nu)} := \max_\phi \frac{\mathbb{E}_{\boldsymbol{U}}[|\langle\phi|\boldsymbol{U}_{\boldsymbol{k}}|\boldsymbol{\psi}_{\boldsymbol{x}}\rangle|^4]}{\mathbb{E}_{\boldsymbol{U}}[|\langle\phi|\boldsymbol{U}_{\boldsymbol{k}}|\boldsymbol{\psi}_{\boldsymbol{x}}\rangle|^2]^2} \,. \tag{27}$$

# Bit rates with losses

In the limit $\nu \gg 1$:

$$\frac{1}{\nu} \log K^{(\nu)} \approx \log \gamma + \log \frac{d}{M}, \qquad d = \binom{n+m-1}{n} \tag{28}$$

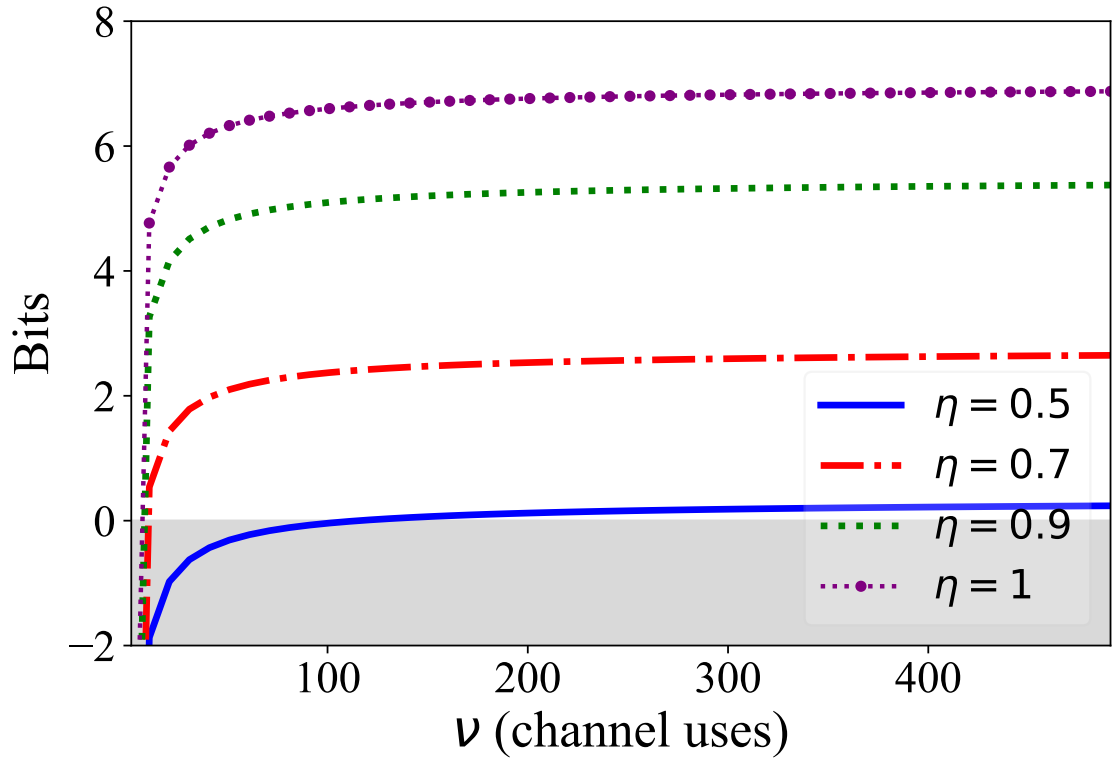



Figure: Net number of bits transmitted, 20 modes and 4 photons.
Quantum 5, 447

# Bit rates with losses

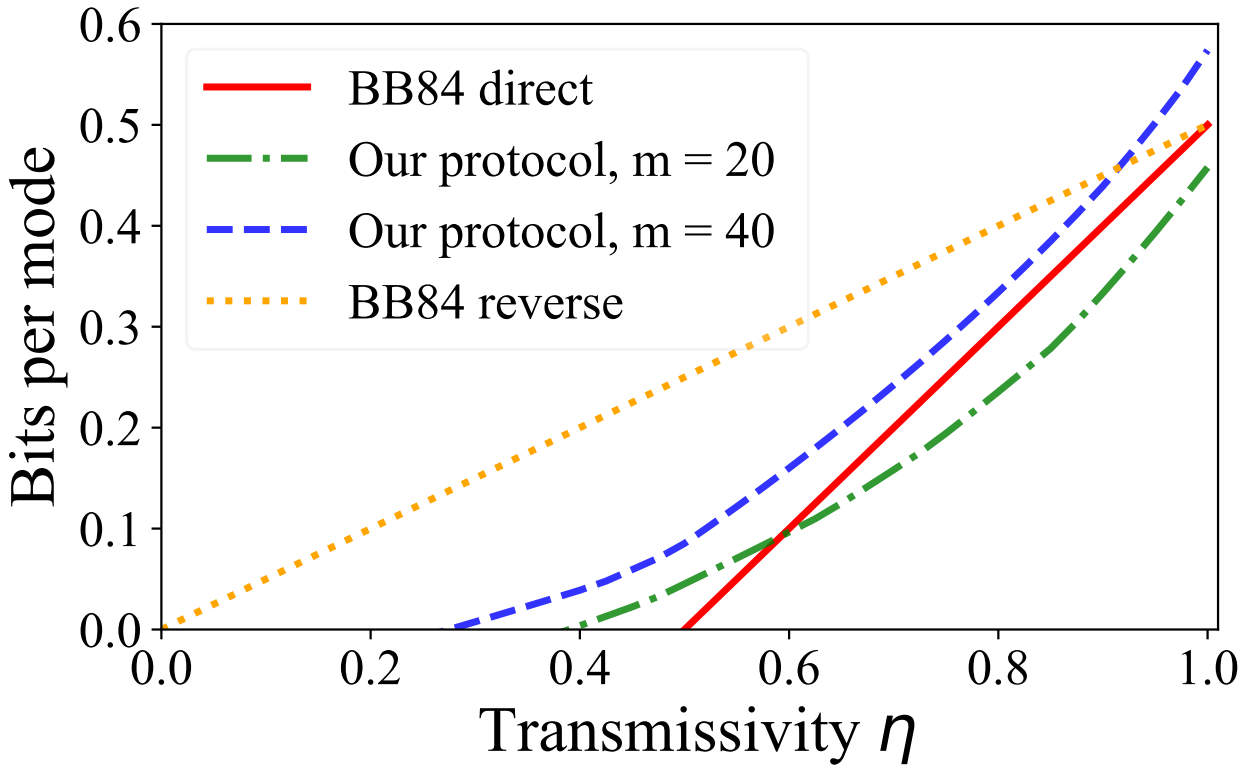



Figure: Net number of bits transmitted per optical mode in the presence of loss. We use *strictly* less photons than $n = m/2$ as per BB84.

"Boson Sampling" cryptography - $\log \binom{m}{n}/m$ bit per mode
BB84 - at most 0.5 bit per mode

# Boson-Samping crypto: summary

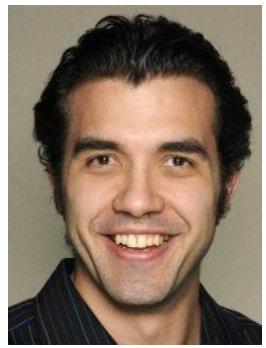
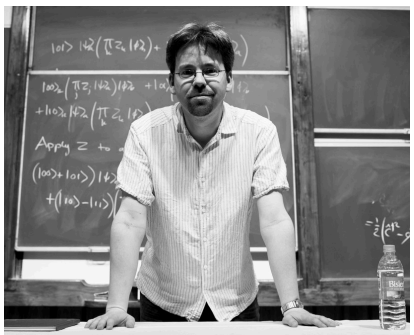
- A quantum private-key encryption protocol, first *actual* application of Boson Sampling
- Information-theoretic security proof – holds for any number of modes $m$ and number of photons $n$.

Future work:

- Removing the need for the bounded storage model
- Scattershot, weak coherent states
- Error-correcting code, privacy amplification
- Time-bin encoding for long distance communication

# Acknowledgements

Photonic quantum data locking
Quantum 5, 447

*zixin.huang@mq.edu.au
†c.lupo@sheffield.ac.uk

# Acknowledgements

"I DON'T CARE IF YOU HAVE A F*CKING NOBEL PRIZE, FRIENDSHIP IS FOREVER!"
– Jonathan P. Dowling, August 2018

ZH would like to thank Professor Jonathan P. Dowling for his encouragement and enthusiastic support throughout the years. PK would like to thank Jon Dowling for being a great mentor.

# Acknowledgements

Thank you for your attention. Questions?

Research presented in this talk is funded in part by EPSRC Quantum Communications Hub, Grant No. EP/M013472/1.