Information Reconciliation in Higher-Dimensional Quantum Cryptography

Daniel Kumor[1], Bradley Christensen[1], Kevin McCusker[1,2], Venkat Chandar[3], Christoph Wildfeuer[4], Daniel Gauthier[4], Paul Kwiat[1]

(1) Department of Physics, University of Illinois at Urbana-Champaign, 1110 W Green St, Urbana IL 61801 USA
(2) Department of Physics & Astronomy, Northwestern University, Evanston, IL 60208 USA
(3) Department of EECS, Massachusetts Institute of Technology, Cambridge, MA 02139 USA
(4) Department of Physics, Duke University, Durham, NC 27708 USA

Hyperentanglement-enabled quantum cryptography allows unprecedented rates of key generation with multiple bits per photon. Information reconciliation needs to be modified to work in such systems.

Quantum Cryptography

- **Alice** and **Bob** want to share cat videos
- **Eve** wants to join on the fun
- Alice and Bob don't want Eve to see the videos
  (they don't trust Eve)
- Alice and Bob want provably secure encryption
  (they *really* don't trust Eve)
- What can they do?

Quantum Key Distribution (QKD) to the rescue!

It is impossible to clone an unknown quantum state, or to measure one without risking altering it → Alice and Bob can detect Eve's snooping.

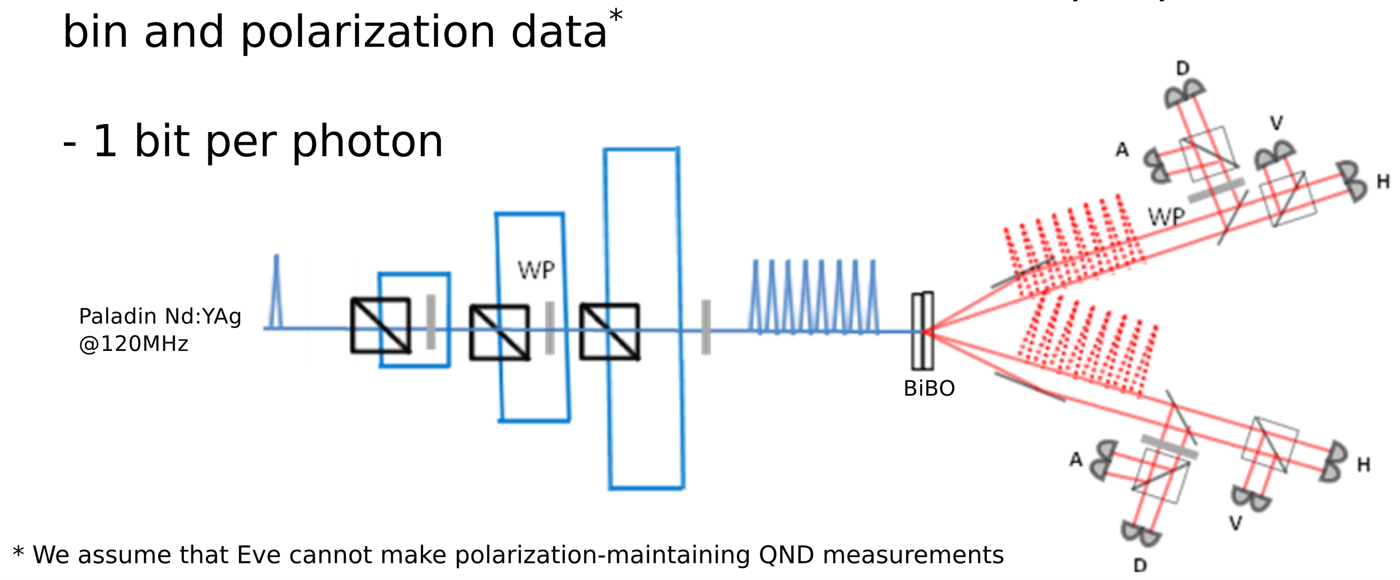
Most QKD systems use single qubits, generating at most 1 bit secret key per detection. We exploit timing degrees of freedom, giving up to 11 bits of information per photon. This allows us to create secret key fast enough for Bob to stream his cat videos to Alice!

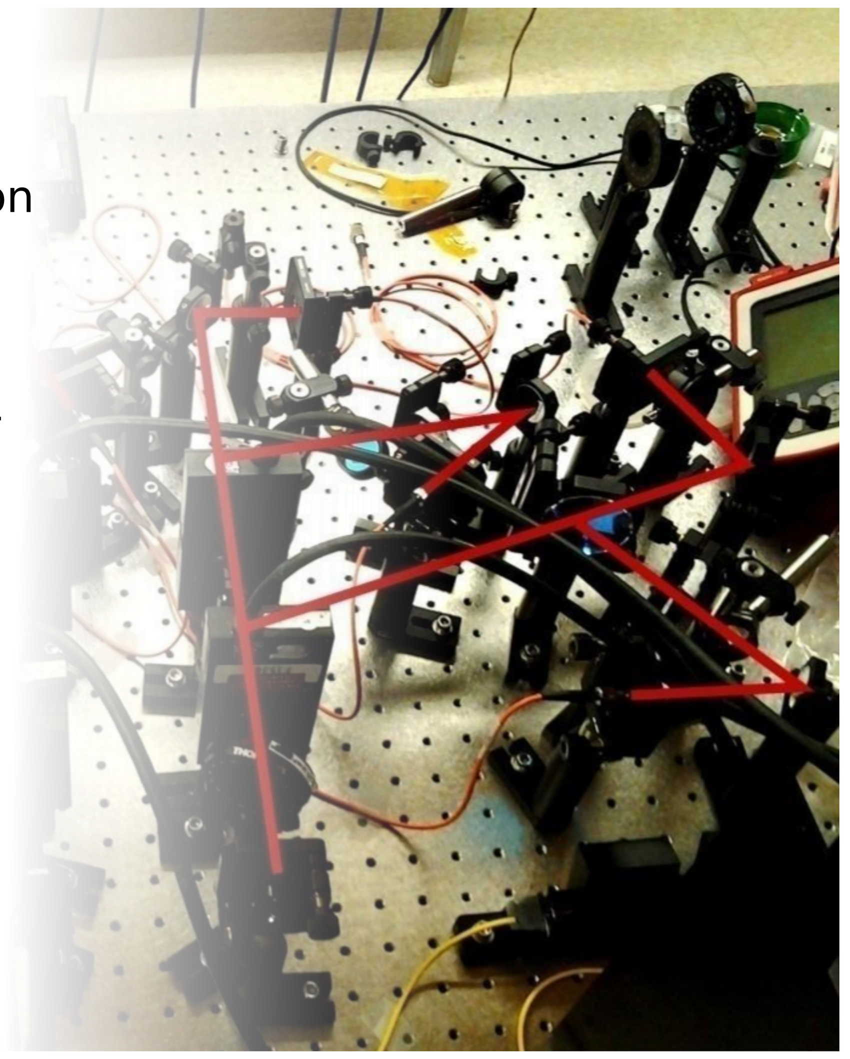
Setup

How do we distribute those 11 bits per photon?

Polarization Entanglement:
- Created by pumping orthogonal nonlinear crystals with pulsed laser
- Measured randomly in H/V or D/A basis
- MUBs used to secure both time-bin and polarization data*
- 1 bit per photon

Time-Bin Entanglement:
- Pairs produced in superposition of many different pump pulses
- Outputs from single photon counting modules sent to time-to-digital converters
- 5-10 bits per photon





* We assume that Eve cannot make polarization-maintaining QND measurements

Results

- First system to achieve secure multi-dimensional QKD
- Practical implementation of information-reconciliation algorithms for multi-dimensional QKD

	Low Power	High Power
Singles	150 kHz	5.8 Mhz
Coincidences	45 kHz	1.9 MHz
Polarization BER	0.4%	0.8%
Entropy bits/ coincidence	10.4 bits	5.5 bits
Expected Secure bits/second	290 kbits	4.2 Mbps

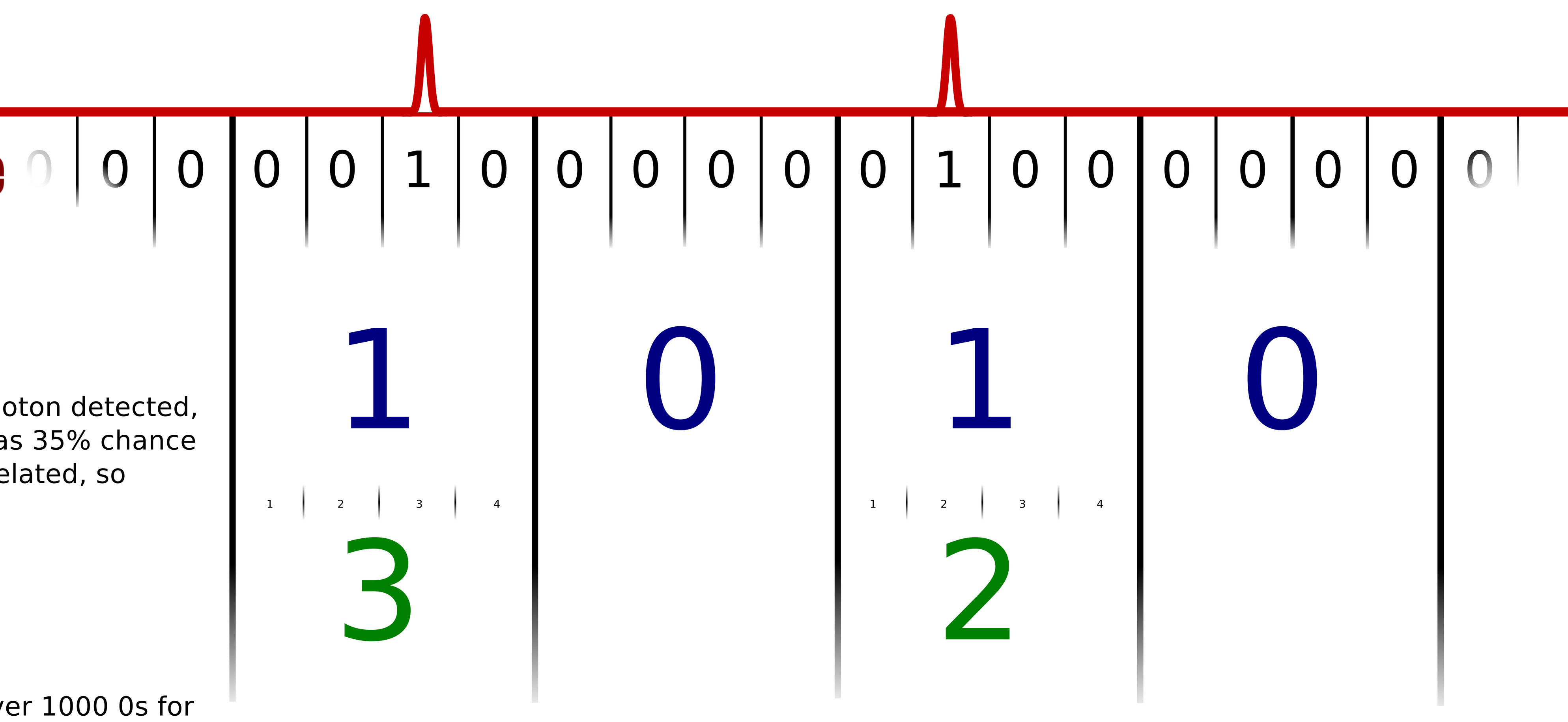
Future Work

Hardware:	**Secret Key Rate**
- Two spatial channels	12.8 Mbps
- Fix time-tagger saturation	25.4 Mbps
- Lower jitter detectors (700ps → 250ps)	37.0 Mbps
- 3 spectral channels	111 Mbps
- 10 spatial x 3 spectral channels	555 Mbps
- Few-mode fiber collection	>3Gbps
Software:	**% Improvement**
- Addition of frames with multiple photons	~20-40%
- Better LDPC codes	~8-30%
- Real-time decoding (GPU)	

References

[1] Bennett, C. H., Brassard, *G., Quantum Cryptography: Public Key Distribution and Coin Tossing* Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179, 1984
[2] Kochman, Y.; Wornell, Gregory W., *On high-efficiency optical communication and key distribution*, Information Theory and Applications Workshop (ITA), 2012 , vol., no., pp.172,179, 5-10 Feb. 2012
[3] Ali-Khan, I, Broadbent, C.J., Howell, J.C., *Large-alphabet quantum key distribution using energy-time entangled bipartite states* Phys Rev Lett 98 (6):060503, 2007
[4] Liveris, A.D.; Zixiang Xiong; Georghiades, C.N., *Compression of binary sources with side information at the decoder using LDPC codes* Communications Letters, IEEE , vol.6, no.10, pp.440,442, Oct. 2002

Decoding Procedure



Step 1

Bin photons by laser pulse

For each laser pulse, assign 0 if no photon detected, and 1 otherwise. If Alice has 1, Bob has 35% chance of having 1. Their sequences are correlated, so shared entropy can be extracted!

Step 2

Frame binary sequence

Step 1's binary sequence can have over 1000 0s for every 1, making entropy extraction difficult. "Framing" lowers data's asymmetry and makes efficient decoding easier.
The "original" (Step 1) sequence of 1s and 0s is divided up into frames (=4 bins here). A sequence is generated from framing, containing **number of photons detected in frame**. In frames with occupancy 1, **location of photon within frame** is also used.

Step 3

Extract entropy from photon number sequence

Using a Slepian-Wolf code, Bob can find Alice's photon number sequence without revealing all the entropy it contains.
Bob sends Alice locations of frames with different occupancy, and both create their final frame location sequences.

```
Alice: ...10001010101100101111010...
       ...1   3 2 4 42  1 2241 3 ...
Bob:   ...10001010101010001101010...
       ...1   3 1 4 4 1   12 1 3 ...
```

Step 4

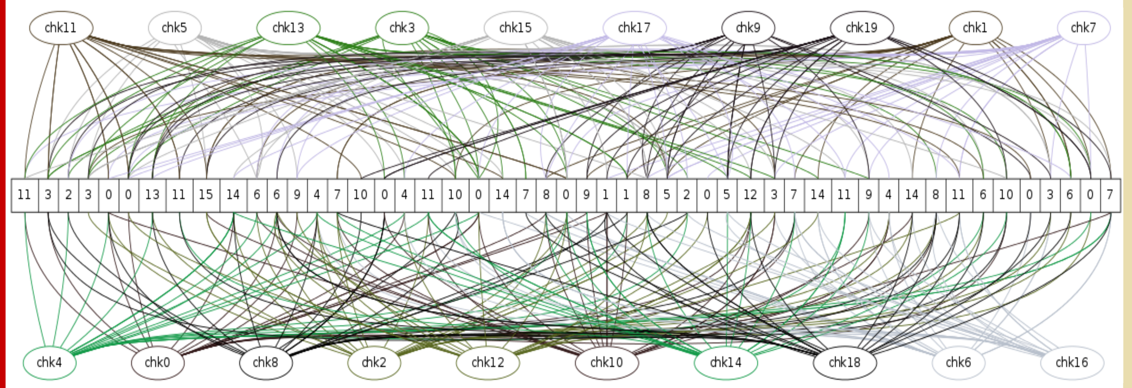
Extract shared entropy from frame location sequence

Alice and Bob use a special non-binary Slepian-Wolf code for Bob to find Alice's frame location sequence without giving all of its entropy to Eve.

```
A: ...132442213...
B: ...131441213...
```

Step 5

Apply Privacy Amplification → Eve has no part of secret key[1]



Simplified LDPC Slepian-Wolf code visualization

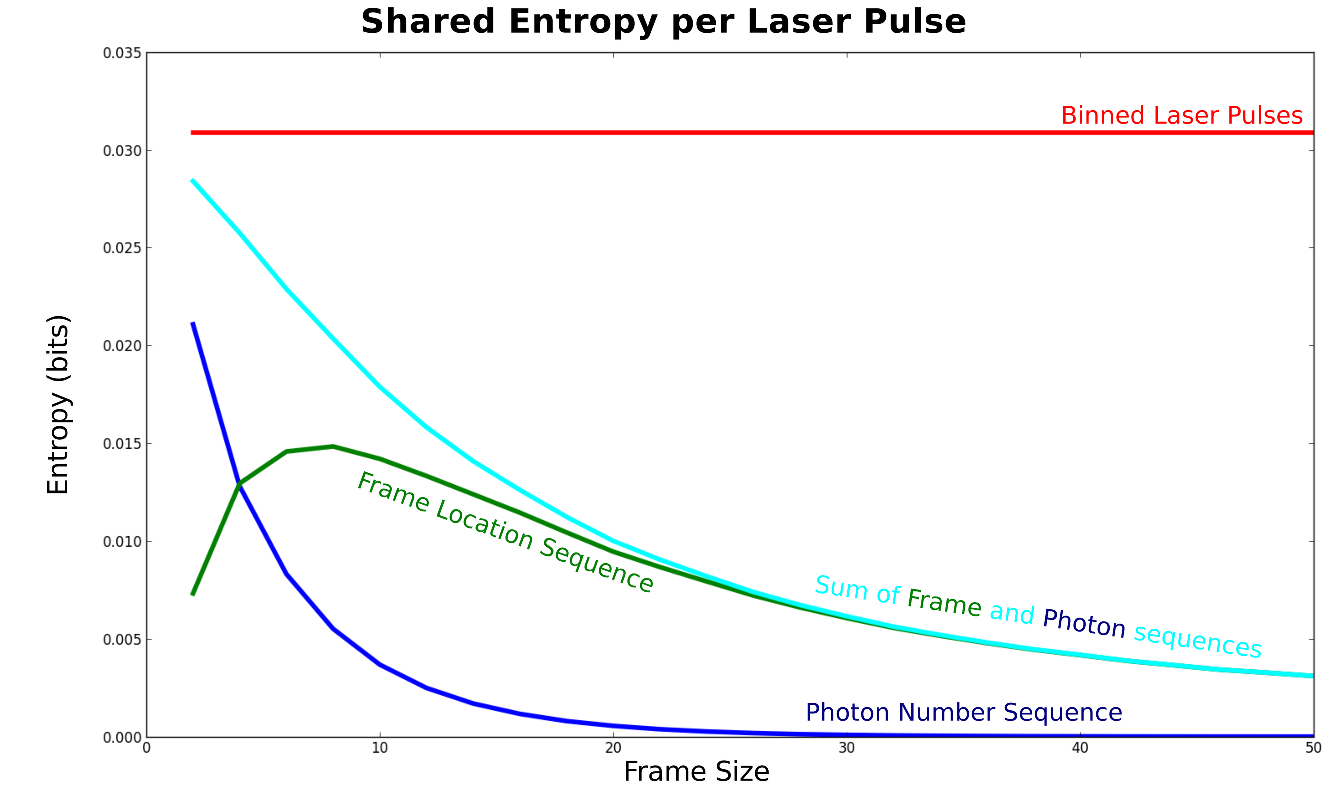
Entropy Extraction

Error correction codes used in wireless communication can be retrofitted to act as Slepian-Wolf codes[4]. Here we used LDPC (Low Density Parity Check) codes modified into Slepian-Wolf codes.

Specialized LDPC codes running on test data extracted:

- 90% of possible shared entropy from frame location sequence.
- 42-60% of total shared entropy within binned photon sequence (sequence of laser pulses)

Shared Entropy per Laser Pulse



Effect of framing on entropy content of sample sequence
At larger frame sizes, frames with multiple photons must be considered.

Information Entropy:

Uncertainty associated with a random variable.

Translated: The amount of information something contains, in bits. A computer with 1TB of memory can hold 1TB of entropy.

Slepian-Wolf code:

Algorithm that can compress and decompress correlated sequences

Translated: Alice and Bob have similar sequences of numbers. This algorithm can compress Alice's sequence such that it can be fully decompressed only by someone with access to a similar sequence (like Bob).