RESEARCH LABORATORY OF ELECTRONICS AT MIT
www.rle.mit.edu

September 1, 2014

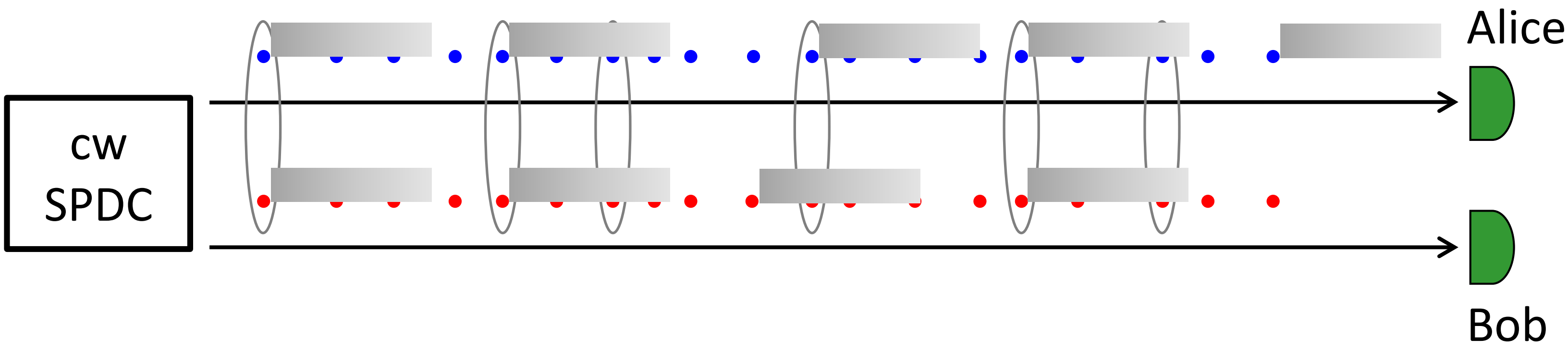
Entanglement-based High-Dimensional Quantum Key Distribution

Tian Zhong, Catherine Lee, Zheshen Zhang, Hongchao Zhou, Jake Mower, Greg Steinbrecher, Ligong Wang, Xiaolong Hu, Rob Horansky, Varun Verma, Adriana Lita, Rich Mirin, Thomas Gerrits, Alessandro Restelli, Josh Bienfang, Francesco Marsili, Matt Shaw, Sae Woo Nam, Greg Wornell, Dirk Englund, Jeff Shapiro, **Franco Wong**

MIT, NIST, JPL

OPTICAL AND QUANTUM COMMUNICATIONS GROUP

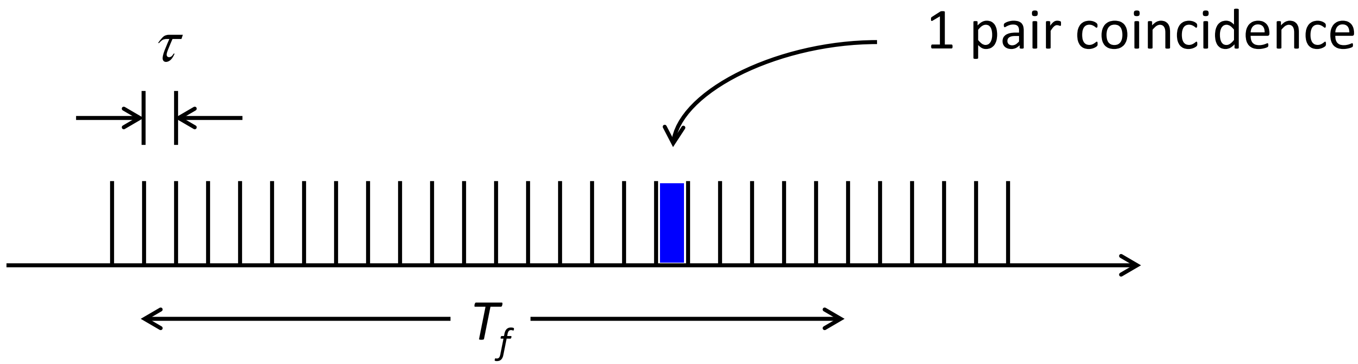
Motivation for high-dimensional encoding



- QKD typically operates under "photon-starved" conditions
  - component loss + propagation losses
  - long recovery times for detection system
  - low flux at receivers; few detected coincidences
  - $\Rightarrow$ many empty time periods between detection events

- High-dimensional encoding
  - maximize throughput with limited number of detection events
  - pack more bits per coincidence detection (multiple bits per photon)

Multiple-bit time-of-arrival encoding



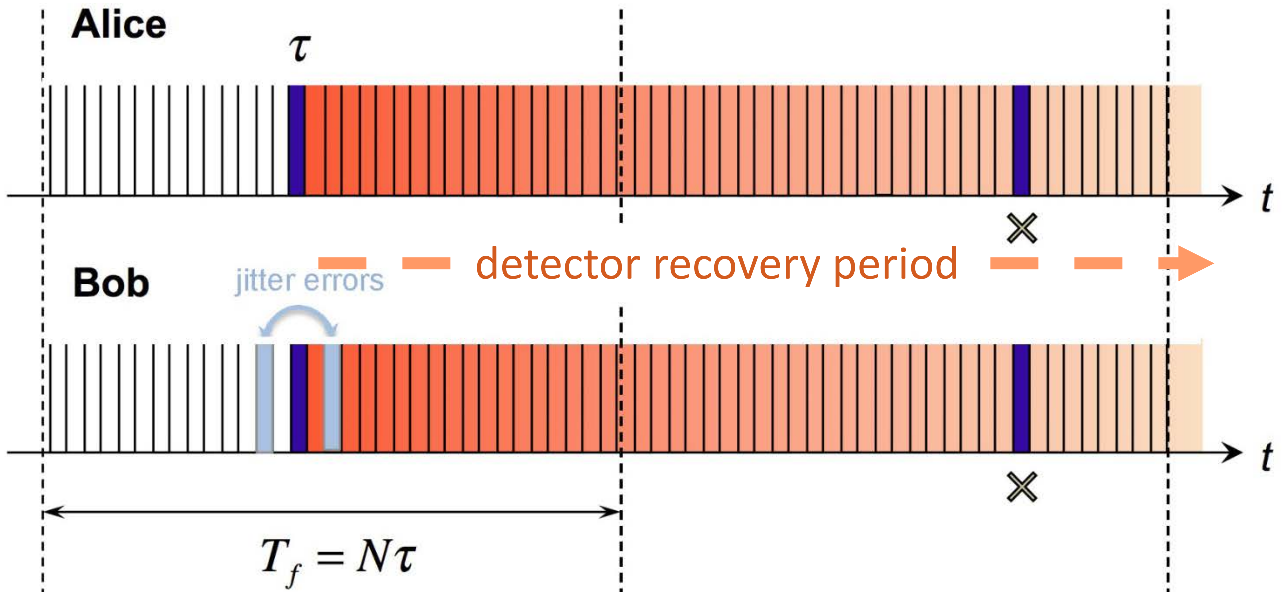
T_f/τ : N bins per frame

T_f = 10 ns, τ = 1 ps, N = 10^4 (~13 bits/photon-pair)
Potential raw key rates = 1.3 Gbps
(0.1 Gbps with binary encoding)

- Continuous-time encoding
- Discrete-energy measurement (photon counting)

Initial concept and demonstration of large alphabet encoding:
John Howell *et al*., PRL **98**, 060503 (2007)

HDQKD (time-of-arrival encoding)



- Time-energy entangled-photon source
  - high flux + single spatial mode + high entanglement quality
- WSi superconducting nanowire single-photon detectors
  - high efficiency + short reset time + low timing jitter
- Efficient error correction and privacy amplification
  - Multi-layer low-density parity check designed for HD encoding
- Security check against collective attacks
  - dispersive optics or Franson interferometer

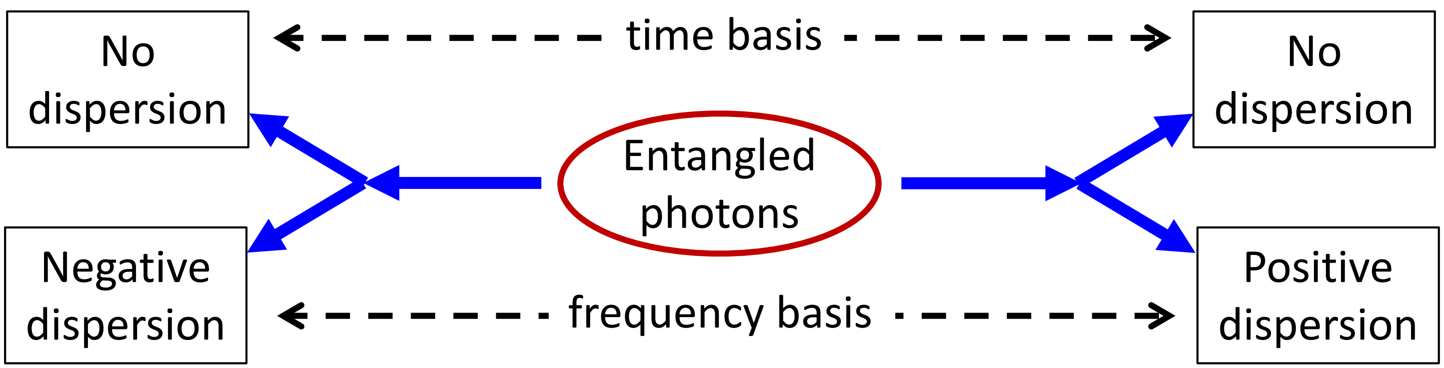
Security of HDQKD based on time-energy entanglement

Apply security analysis technique for CVQKD to HDQKD:

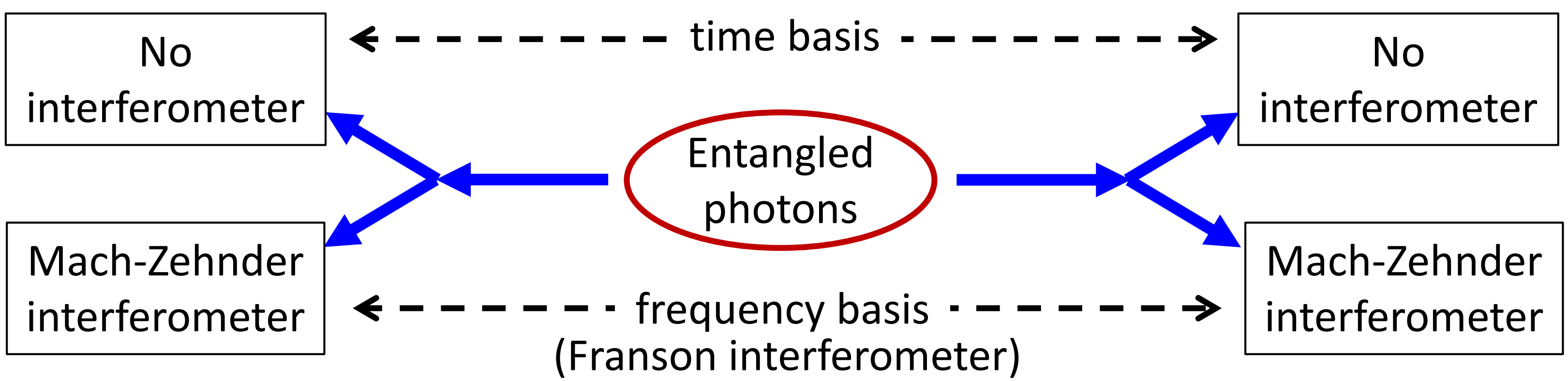
Continuous time (arrivals) and frequency (detunings) as conjugate bases

Relate measurements to time-frequency covariance matrix (TFCM)

Dispersive optics   Mower *et al.*, PRA **87,** 062322 (2013)

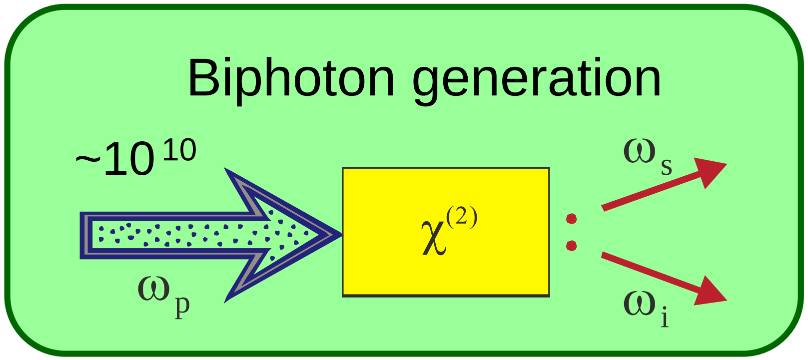


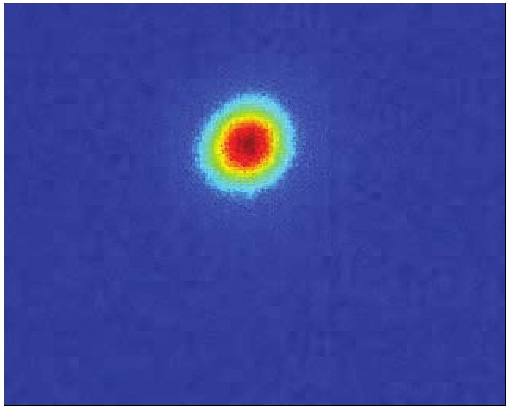
Franson interferometer   Zhang *et al.*, PRL **112,** 120506 (2014)

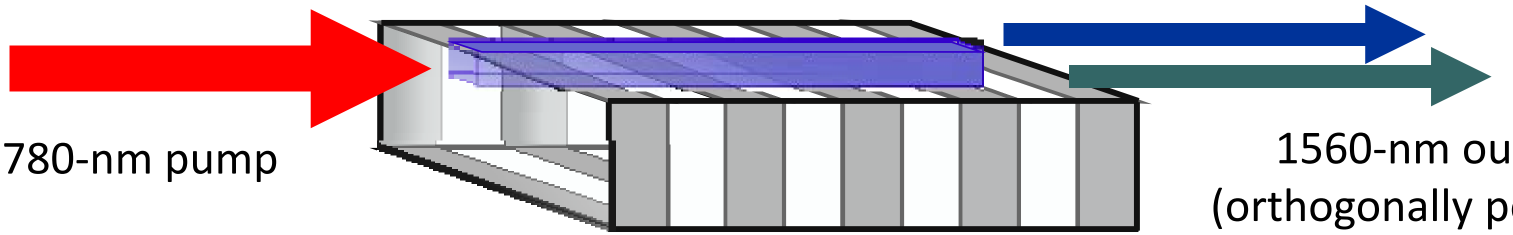


Time-energy entangled-photon source

Spontaneous parametric downconversion (SPDC)





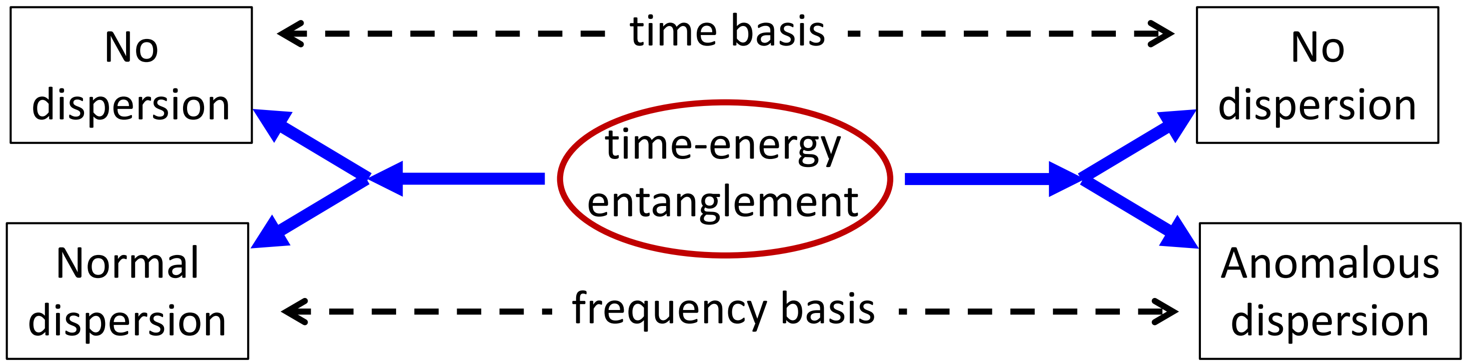


Type-II phase-matched PPKTP waveguide

- Efficient generation: 10^7 pairs/s/nm/mW (1.6 nm bandwidth)
- High extraction efficiency (~80%) into single-mode fibers
- Naturally time-energy entangled; very little fluorescence

Zhong *et al*., Opt. Express **28,** 26868 (2012)

Dispersive-optics QKD protocol



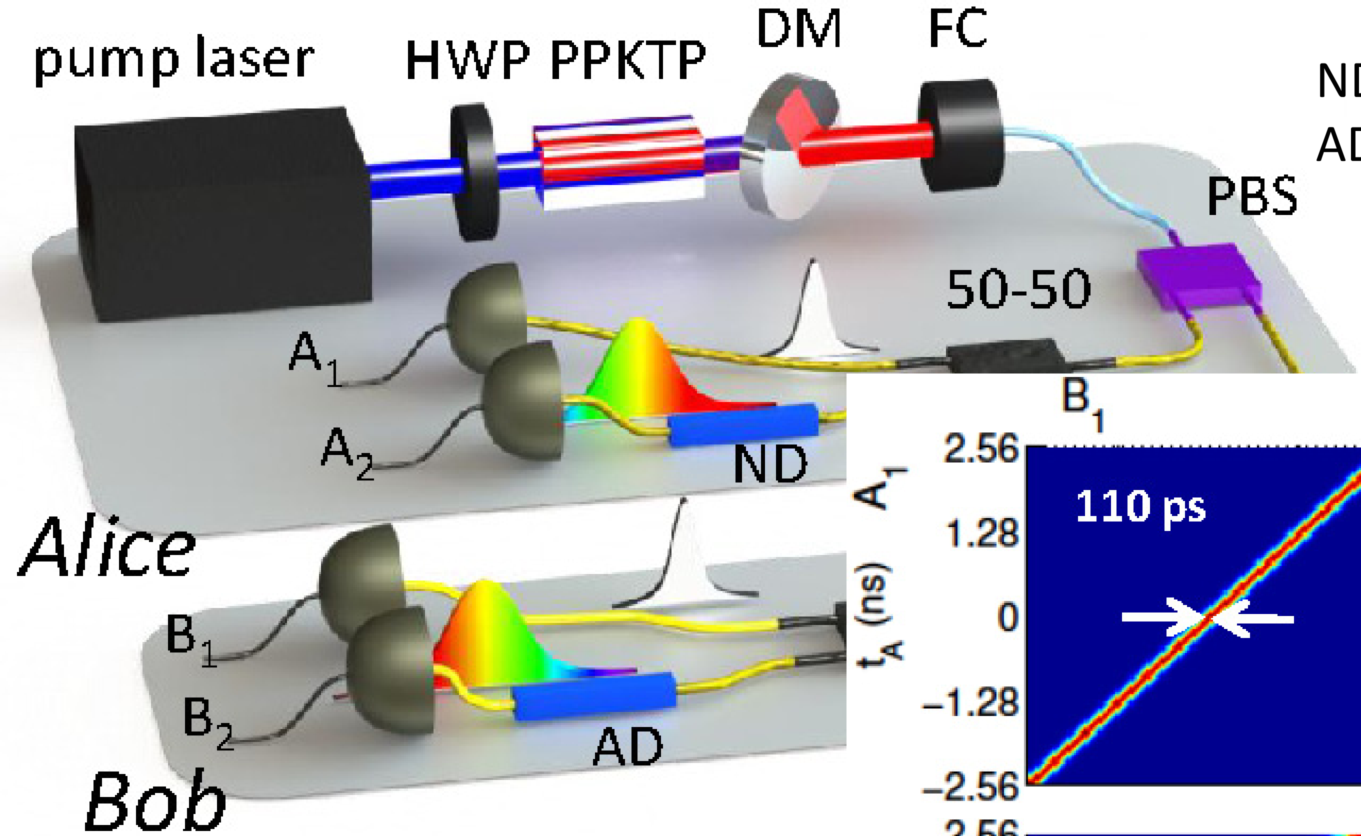
Nonlocal cancellation of dispersion: J. D. Franson, PRA (1992)

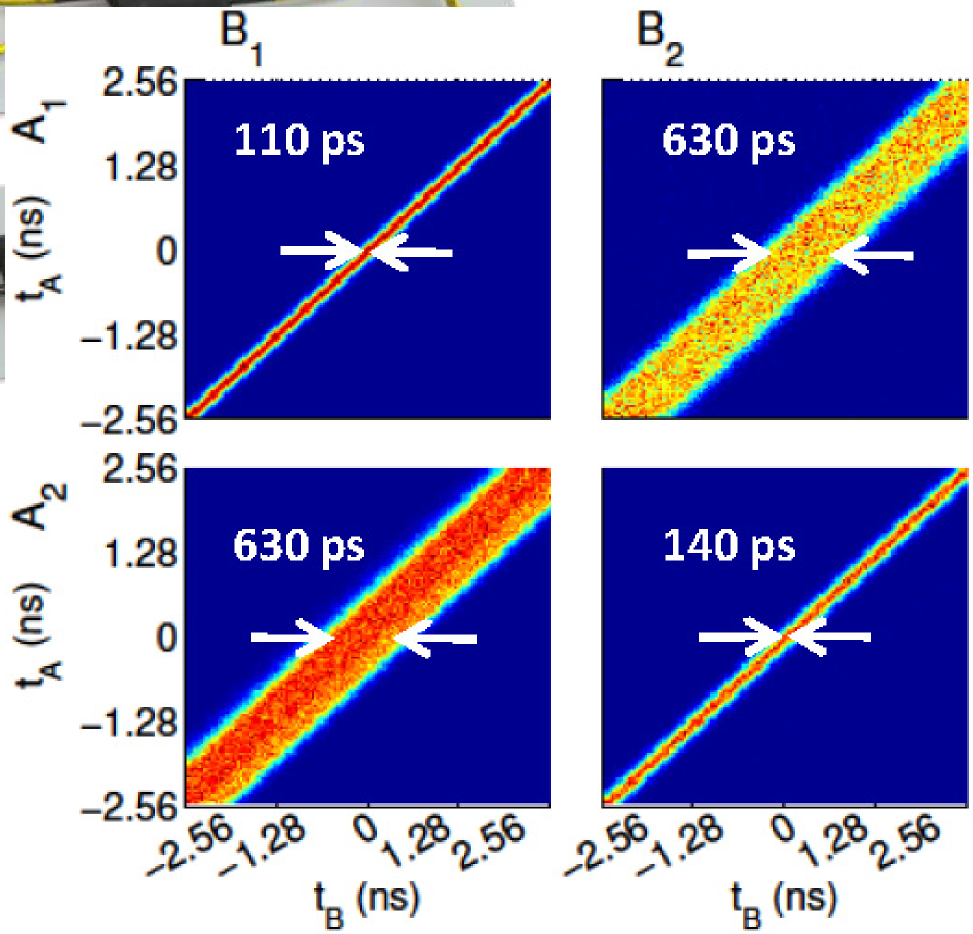
- Dispersive-optics QKD (DO-QKD)
  - two dispersive conjugate measurement bases
  - correct bases yield narrow time coincidence for key generation
  - security check: correct bases, timing errors indicate eavesdropping
  - choose frame size and bin duration in software; adjust dynamically
  - retain frames with 1 detection event by Alice and Bob
  - apply error correction and privacy amplification, finite key correction
  - obtainsecure key capacity and secure key rate

Mower, Zhang, Desjardins, Lee, Shapiro, Englund, PRA **87,** 062322 (2013)

Dispersive optics HDQKD experimental demonstration

ND: normal dispersion
AD: anomalous dispersion





6 WSi SNSPDs:
~100 ps jitter
~1 MHz max count rate
~80-90% efficiency

DOQKD secure key capacity > 3 bpc

$$r = \beta I(A;B) - \chi(A;E) - \Delta_{FK}$$

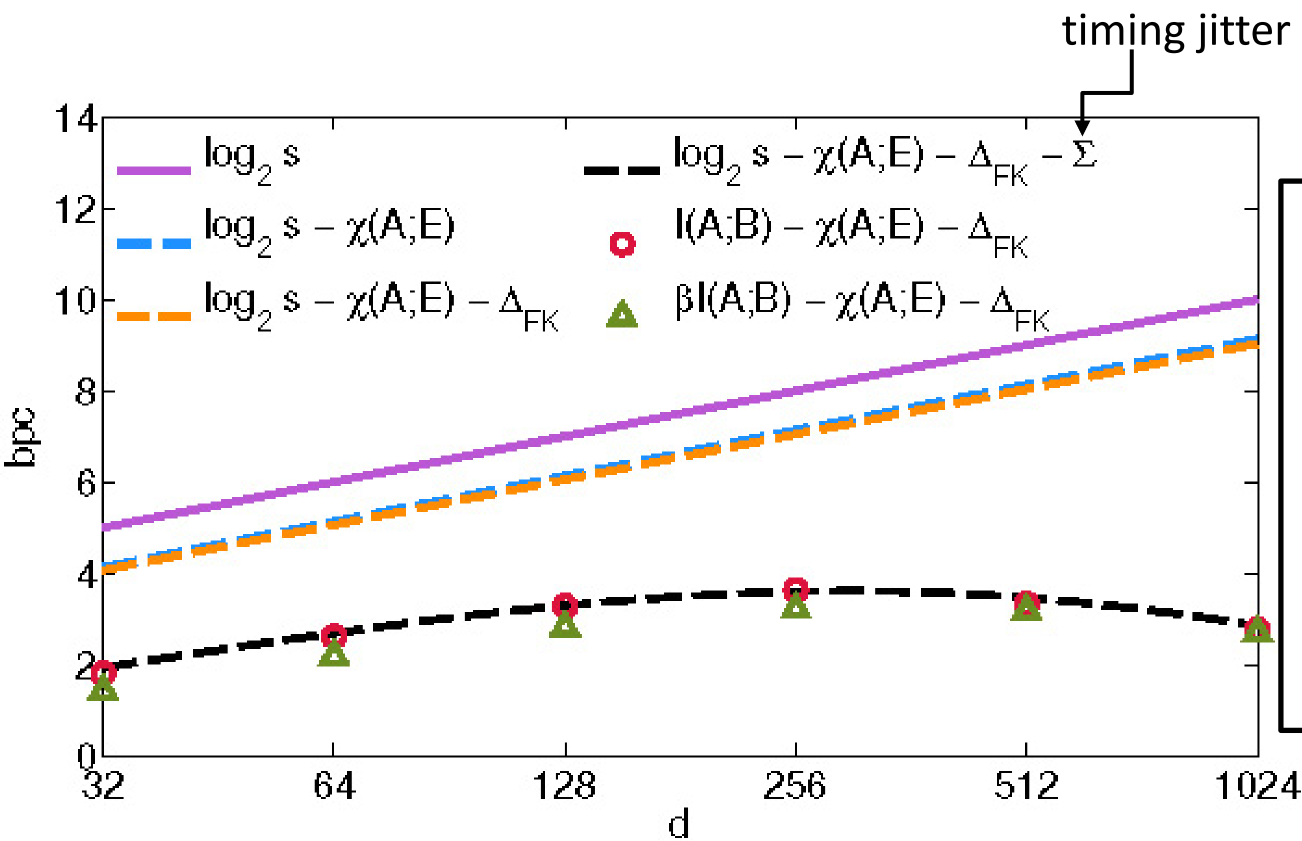
Secure key capacity

Reconciliation efficiency

Mutual information between Alice, Bob

Alice, Eve shared Holevo information

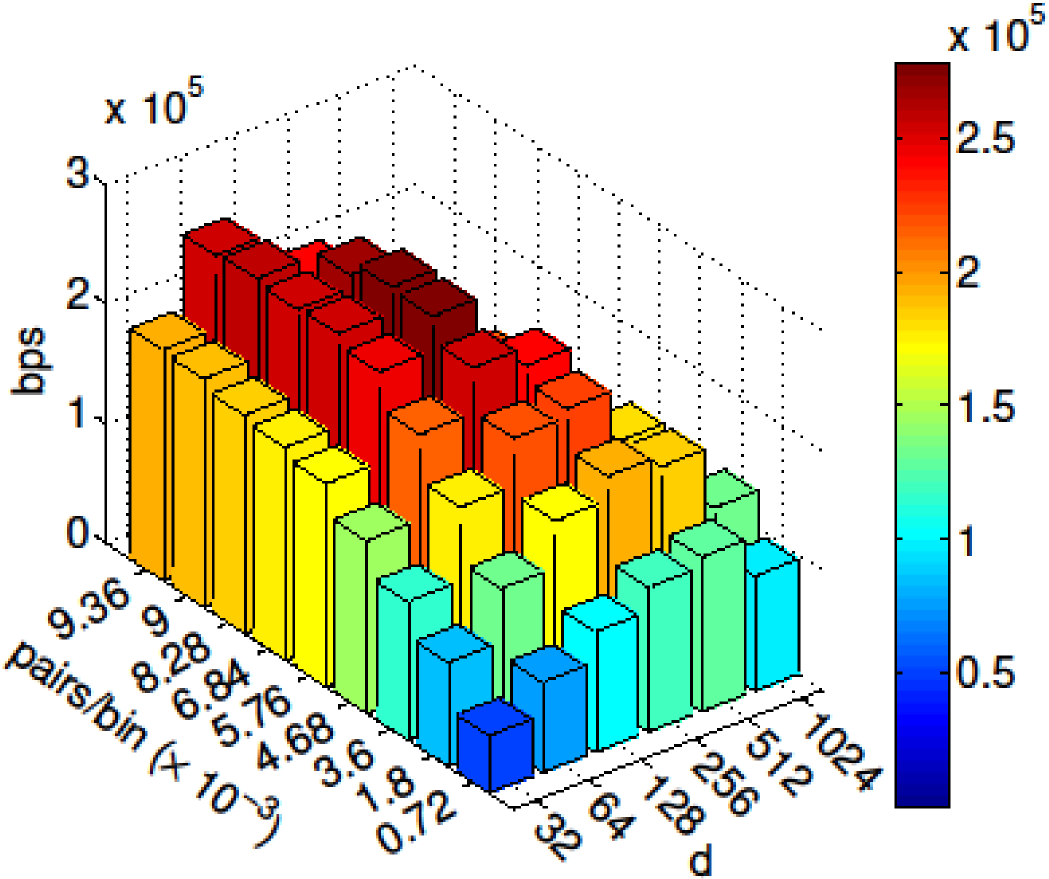
Finite-key corrections



Parameters:

- pair generation rate ~9 MHz
- detector jitter 100 ps
- bin duration 80 ps
- propagation loss 0.2 dB/km
- detector efficiency 90%
- Alice's system efficiency 10%
- Bob's system efficiency 7%
- dark count rate 1 kHz

Secure key rate > 270 kbps

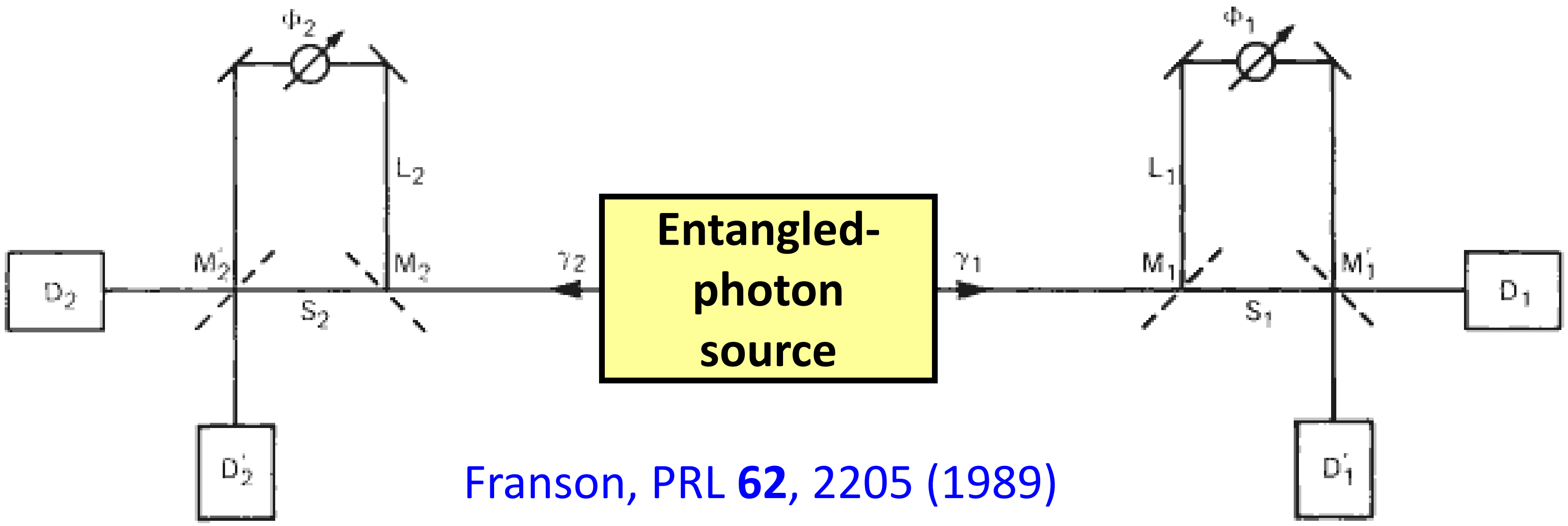


Parameters:

- pair generation rate ~9 MHz
- detector jitter 100 ps
- bin duration 80 ps
- propagation loss 0.2 dB/km
- detector efficiency 90%
- Alice's system efficiency 10%
- Bob's system efficiency 7%
- dark count rate 1 kHz

Maximum throughput does not occur where key capacity is maximum

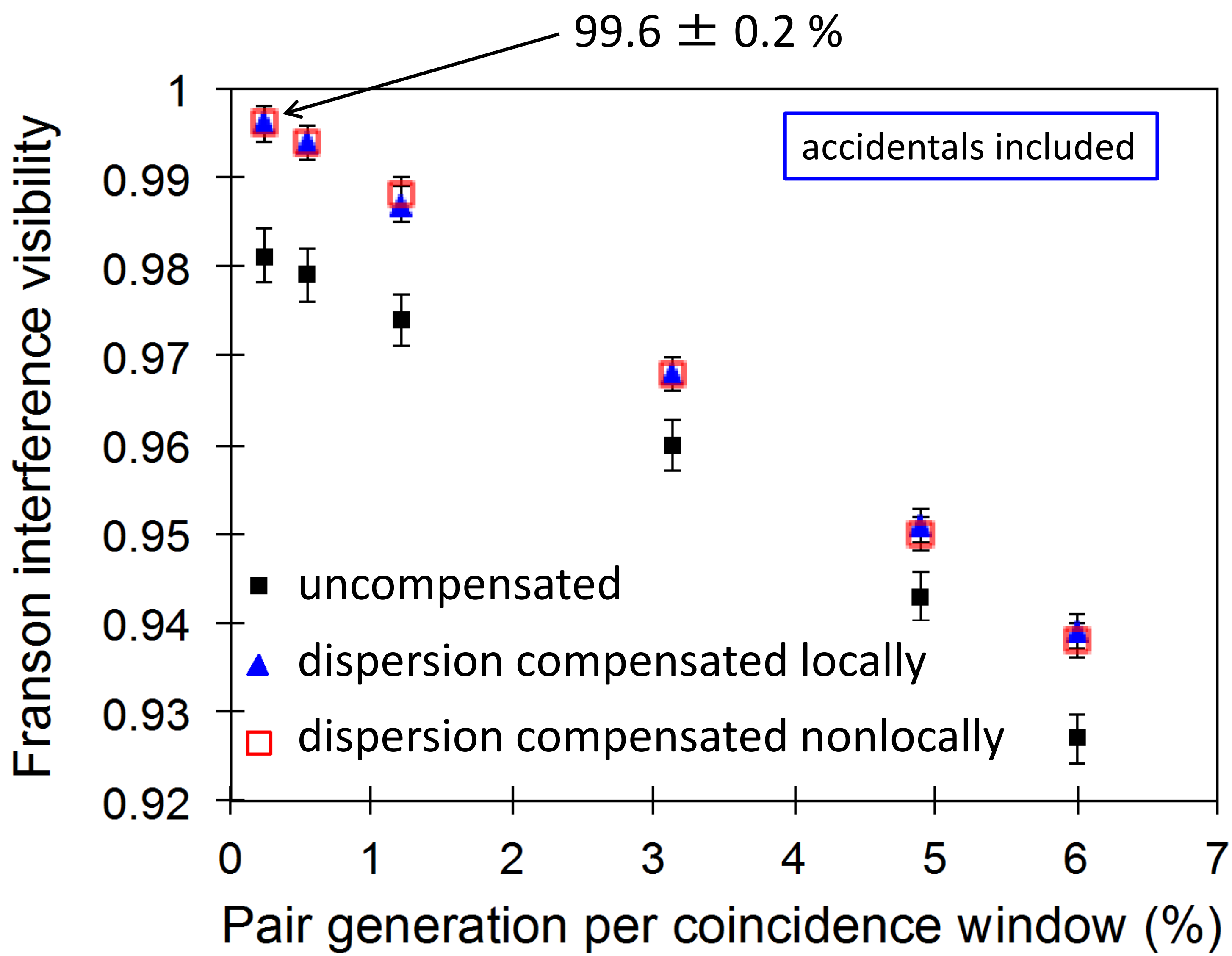
Security based on high-visibility Franson interferometer



Franson, PRL **62**, 2205 (1989)

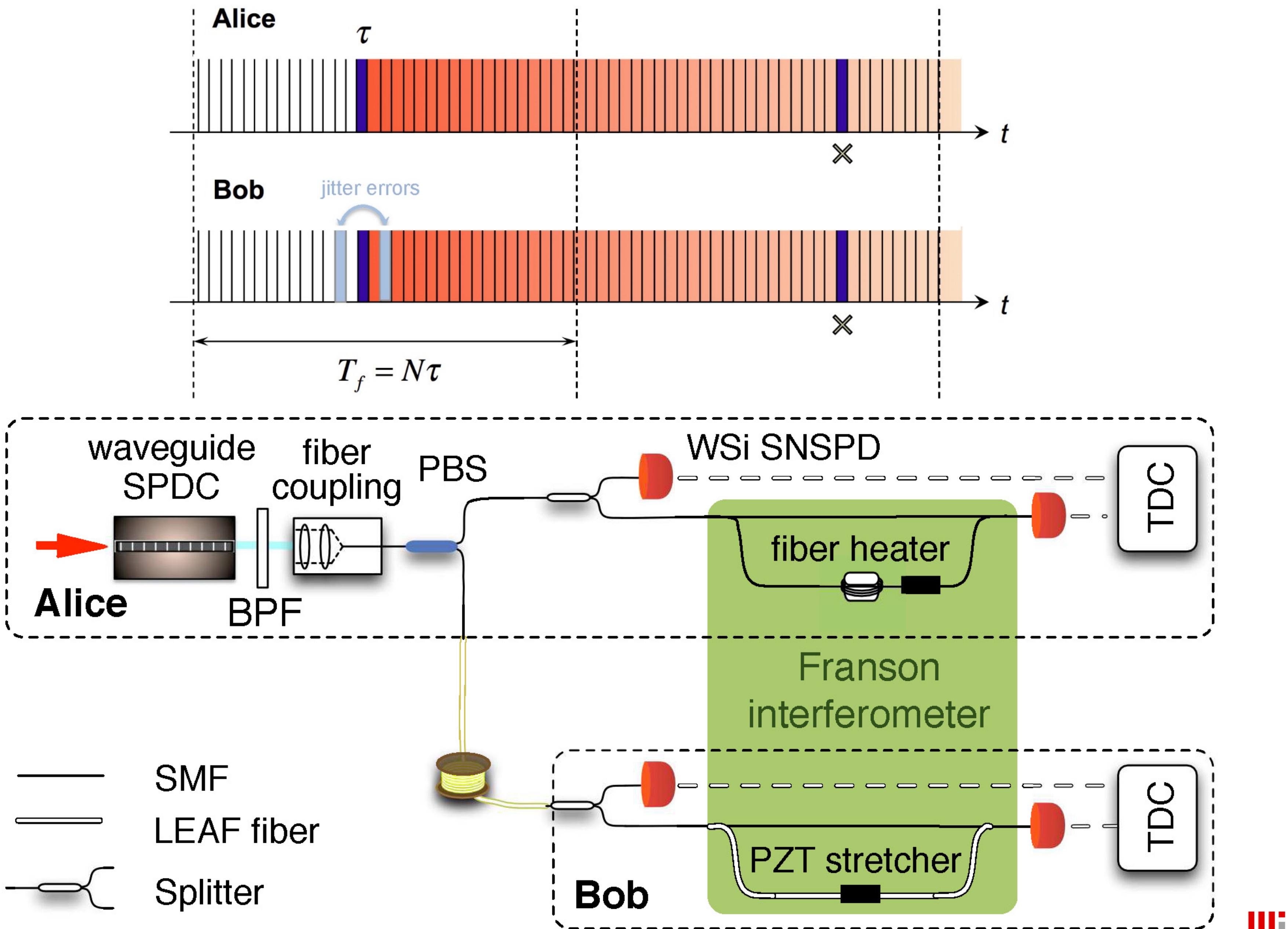
- Franson interferometer measures quality of time-energy (or time-bin) entanglement and its frequency correlation
  - frequency correlation degradation ε ➔ $V_{\text{Franson}} \leq 1 - \varepsilon$
- High visibility => small amount of frequency disturbance (by Eve)
  - Franson measurements bound Eve's Holevo information
  - visibility limited by multi-pair emission and differential dispersion between long and short paths of each arm

Dispersion-compensated Franson measurements

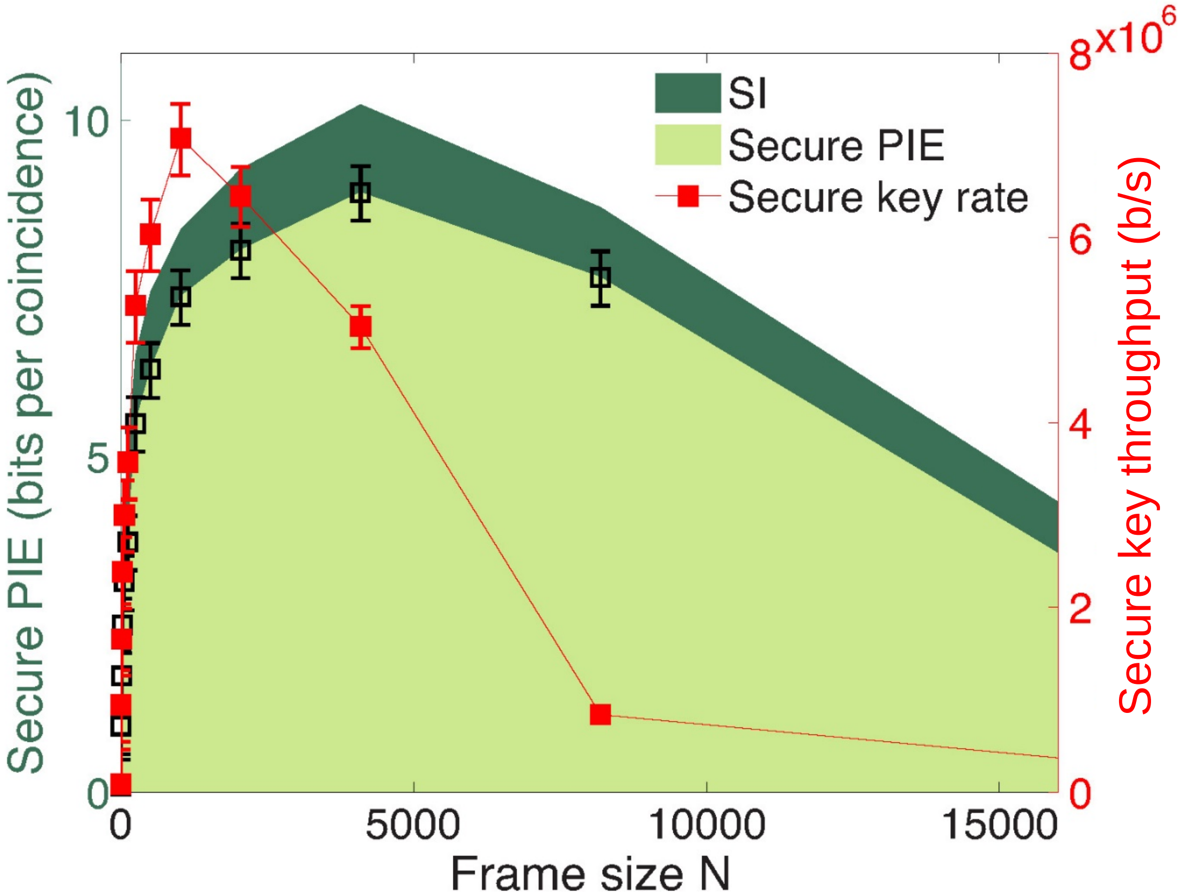


PRA **88,** 020103(R) (2013)

HDQKD with Franson security check



Franson-based HDQKD results



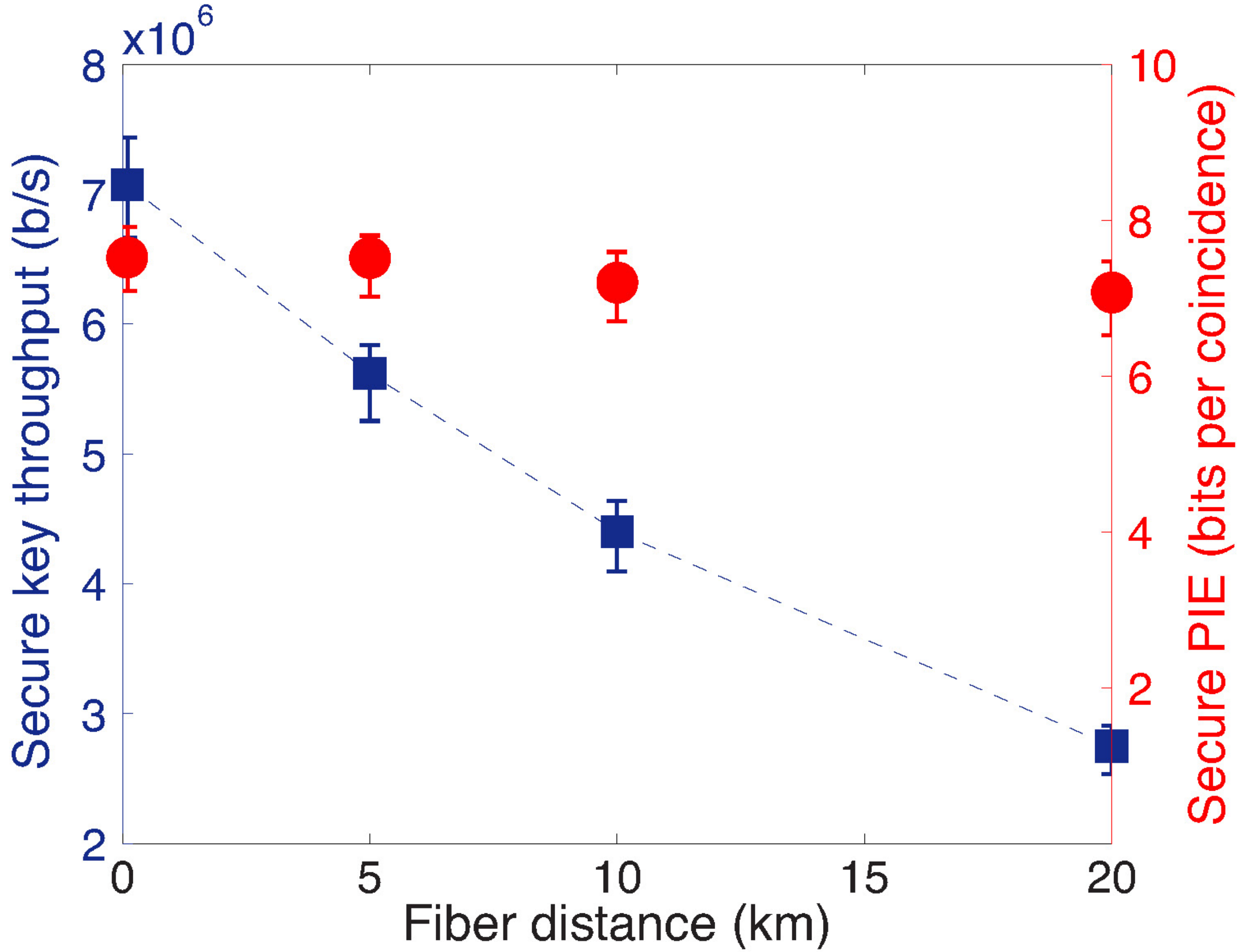
Franson visibility measurements bound Eve's Holevo information

HDQKD Improvement
500x throughput

Comparison with BBM92 [Treiber *et al.*, New J. Phys. **11,** 045013 (2009)]

	BBM92	Franson HDQKD
Secure bits/coincidence	0.35	7.5
Secure key rate	14.5 kbps	7.1 Mbps

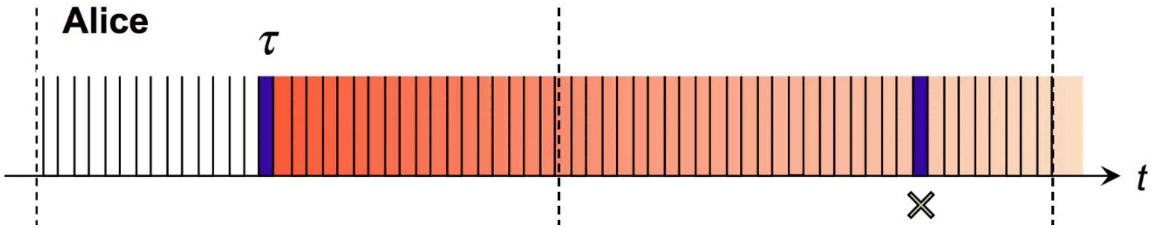
Franson HDQKD results versus distance



Secure PIE stays unaffected: 7.1 bits per coincidence

Secure key rate drops due to fiber loss

Summary



- Entanglement-based QKD with high dimensional encoding
  - multiple bits per coincidence
  - efficient error correction and privacy amplification
  - high flux single-spatial-mode PPKTP waveguide source
  - efficient WSi superconducting nanowire single photon detectors
  - security checks tightly bound Eve's Holevo information
- HDQKD security protocols
  - dispersive optics (oppositely chirped fiber Bragg gratings)
  - single Franson interferometer that does not degrade with loss
- High secure key capacity and throughput
  - dispersive optics: > 3 bpc, > 270 kbps
  - Franson: > 7 bpc, > 7 Mbps

Team members and funding

- Personnel
  - Tian Zhong, Catherine Lee, Zheshen Zhang, Hongchao Zhou, Jake Mower, Greg Steinbrecher, Ligong Wang, Xiaolong Hu, Greg Wornell, Jeff Shapiro, Dirk Englund, *MIT*
  - Rob Horansky, Varun Verma, Adriana Lita, Alessandro Restelli, Josh Bienfang, Richard Mirin, Thomas Gerrits, Sae Woo Nam, *NIST*
  - Francesco Marsili, Matt Shaw, *JPL*
- Funding
  - DARPA Information in a Photon, Columbia Optics and Quantum Electronics IGERT, NASA