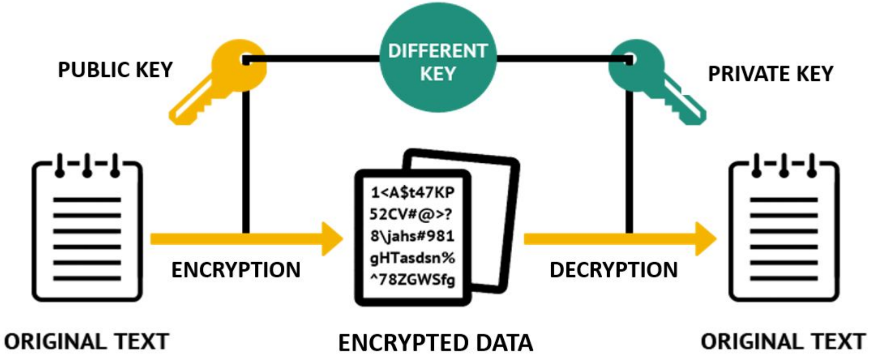
Measurement Device Independent Quantum Key Distribution (MDI-QKD)

MIT 6.2410 | 05/16/2023

Joseph Gross, Jack Rich, Adrian Anaemeje, Kate Arutyunova

Modern Cryptography

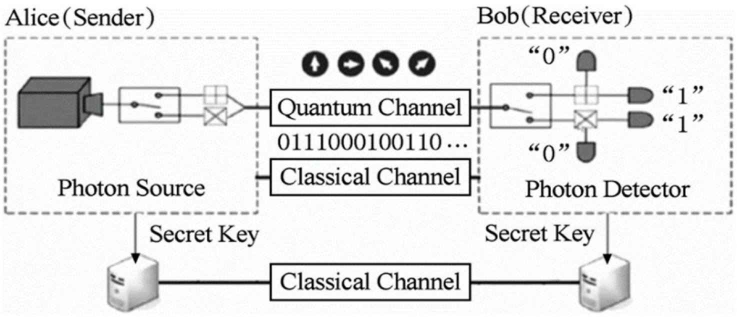
- The value of information privacy is significant for different stakeholders (individuals, businesses, and government)
- Modern cryptographic algorithms are ***NOT*** secure
  - Decryption of all intercepted communications in the last 50 years
  - *Pose a huge security risk for the society!*
- The need to explore alternative encryption methods → **Quantum Cryptography (QKD)**



https://www.simplilearn.com/tutorials/cryptography-tutorial/rsa-algorithm

Quantum Key Distribution

- QKD: Secure communication method for key distribution due to *quantum no-cloning theorem*
  - Immediate detection of third-party intervention
- Widely implemented QKD scheme: BB84 protocol
  - Encodes information using single photons of light in different quantum states
  - Allows two parties to securely create and exchange a secret key for further communication



Appl. Sci. **2020**, *10*, 2906; doi:10.3390/app10082906

- BB84 protocol relies on the assumptions related to detection hardware:
  - Quantum measurement devices are trustworthy and error-free.
- Assumption poses a security risk of of side-channel attacks → **Measurement-Device-Independent (MDI) QKD**

Measurement-Device-Independent (MDI) QKD

Protocol

Alice and Bob: Photon polarization encoding

⇩

Photon transmission to Charlie

⇩

Charlie: Bell State Measurement

⇩

Results announced for Alice and Bob

⇩

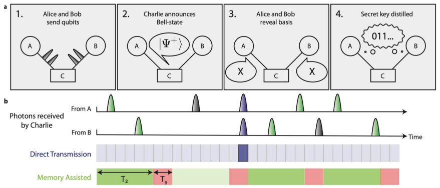
Alice and bob: Bit selection, Post-selection and Bit flip

⇩

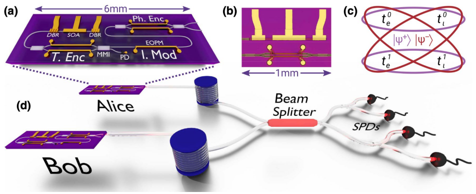
Secret key is generated!

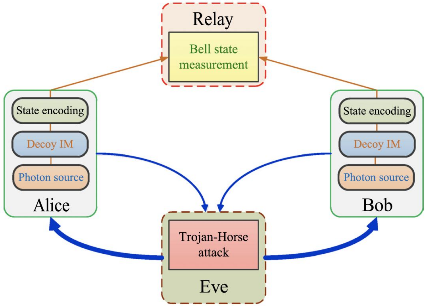
State of the Art

Memory-enhanced MDI-QKD



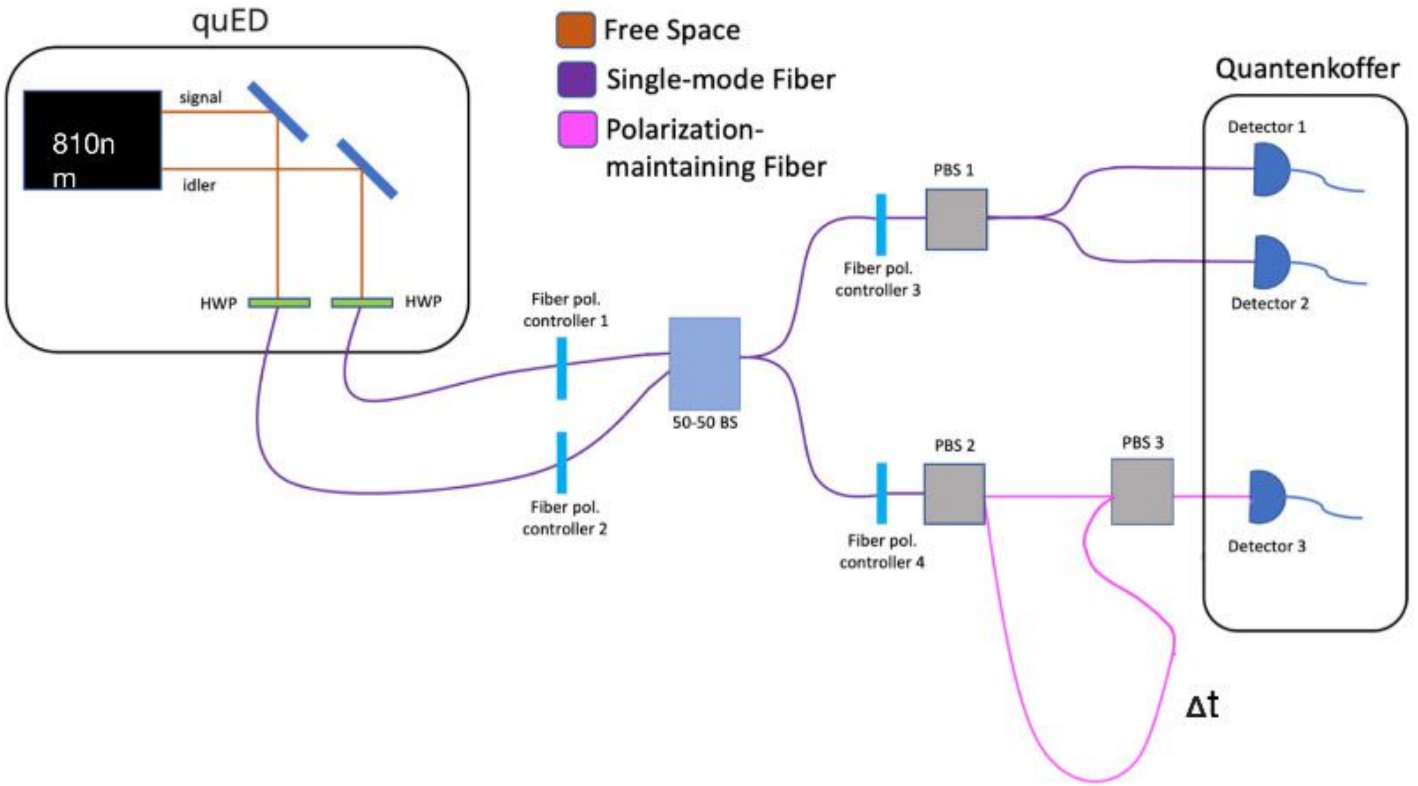
Chip-based MDI-QKD





MDI-QKD with leaky sources

Measurement Setup



Data and Analysis

- Average total counts were roughly 28,800 counts per second → loss (on average) 88%
- Inability to locate HOM dip severely impacted results
- Difficulty correcting for polarization rotation with diagonal and anti-diagonal states

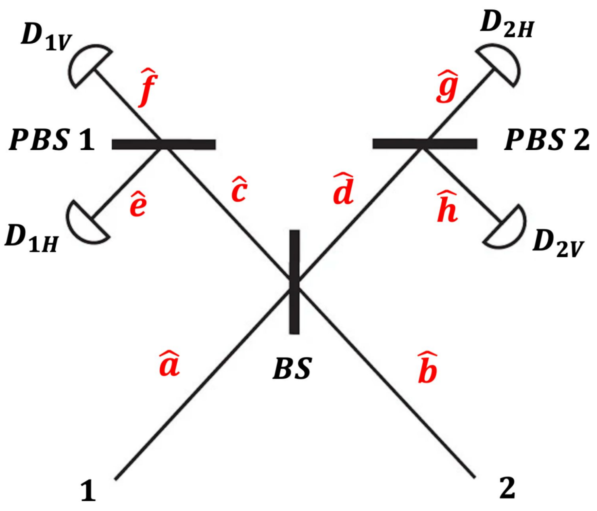
		d1V (c/s)	d1H (c/s)	d2V (c/s)	d2H (c/s)	Total (c/s)	Loss
Alice	Bob						
H	H	3,200	13,300	1,700	9,700	27,900	88.47%
	V	9,400	8,100	7,300	5,500	30,300	87.48%
	D	5,800	11,000	4,100	7,900	28,800	88.10%
	A	6,400	10,600	4,600	7,400	29,000	88.02%
V	H	7,600	8,800	5,900	5,700	28,000	88.43%
	V	13,800	3,600	10,100	1,600	29,100	87.98%
	D	10,400	6,600	7,400	4,000	28,400	88.26%
	A	10,900	6,100	8,700	3,600	29,300	87.89%
D	H	5700	10700	4100	7200	27,700	88.55%
	V	12,000	5,200	9,300	3,000	29,500	87.81%
	D	8,400	8,200	6,300	5,400	28,300	88.31%
	A	9,000	7,800	7,100	5,000	28,900	88.06%
A	H	5,500	11,000	3,900	7,500	27,900	88.47%
	V	11,700	5,600	9,300	3,400	30,000	87.60%
	D	8,100	8,600	6,300	5,600	28,600	88.18%
	A	8,800	8,200	7,000	5,200	29,200	87.93%
Avg						28,806	88.10%

Photon count per detector

		d1V	d1H	d2V	d2H
Alice	Bob				
H	H	0.23	0.95	0.12	0.70
	V	0.62	0.53	0.48	0.36
	D	0.40	0.76	0.28	0.55
	A	0.44	0.73	0.32	0.51
V	H	0.54	0.63	0.42	0.41
	V	0.95	0.25	0.69	0.11
	D	0.73	0.46	0.52	0.28
	A	0.74	0.42	0.59	0.25
D	H	0.41	0.77	0.30	0.52
	V	0.81	0.35	0.63	0.20
	D	0.59	0.58	0.45	0.38
	A	0.62	0.54	0.49	0.35
A	H	0.39	0.79	0.28	0.54
	V	0.78	0.37	0.62	0.23
	D	0.57	0.60	0.44	0.39
	A	0.60	0.56	0.48	0.36

Experimental data normalized and scaled to sum to 2

Simulation



$$\hat{a} = \overbrace{\left[e_f \cdot e_{\text{hwp\_a}} \cdot e_{\text{qwp\_a}}\right]}^{a_e} \left[a_h \left|H\right\rangle + a_v \left|V\right\rangle\right]$$

$$\hat{b} = \overbrace{\left[e_f \cdot e_{\text{hwp\_b}} \cdot e_{\text{qwp\_b}}\right]}^{b_e} \left[b_h \left|H\right\rangle + b_v \left|V\right\rangle\right]$$

- Detector Efficiency (e_d)
- PBS 1 Efficiency (e_{pbs1})
- PBS 2 Efficiency (e_{pbs2})
- 50/50 BS Efficiency (e_{bs50})
- Fiber $\leftrightarrow$ Free Space (e_{fff})
- HWP A Efficiency (e_{hwp_a})
- QWP A Efficiency (e_{qwp_a})
- HWP B Efficiency (e_{hwp_b})
- QWP B Efficiency (e_{qwp_b})

$$n_{d1h} = e_d * \hat{e}^\dagger \hat{e} = e_d * \frac{(e_{bs50} * e_{pbs1})^2 (a_e a_h - b_e b_h)^2}{2}$$

$$n_{d1v} = e_d * \hat{f}^\dagger \hat{f} = e_d * \frac{(e_{bs50} * e_{pbs1})^2 (a_e a_v - b_e b_v)^2}{2}$$

$$n_{d2h} = e_d * \hat{g}^\dagger \hat{g} = e_d * \frac{(e_{bs50} * e_{pbs2})^2 (a_e a_h + b_e b_h)^2}{2}$$

$$n_{d2v} = e_d * \hat{h}^\dagger \hat{h} = e_d * \frac{(e_{bs50} * e_{pbs2})^2 (b_e a_v + b_e b_v)^2}{2}$$

Expected Photon Counts

6.2410 Optics Lab

Alice	Bob	d1v	d1h	d2v	d2h
States.H	States.H	0.0000	0.0000	0.0000	0.0189
	States.V	0.0044	0.0051	0.0046	0.0047
	States.D	0.0023	0.0004	0.0022	0.0130
	States.A	0.0024	0.0004	0.0022	0.0129
States.V	States.H	0.0043	0.0044	0.0044	0.0044
	States.V	0.0000	0.0000	0.0181	0.0000
	States.D	0.0004	0.0024	0.0140	0.0021
	States.A	0.0129	0.0023	0.0004	0.0020
States.D	States.H	0.0022	0.0004	0.0022	0.0136
	States.V	0.0003	0.0021	0.0136	0.0023
	States.D	0.0000	0.0000	0.0089	0.0092
	States.A	0.0088	0.0000	0.0000	0.0084
States.A	States.H	0.0023	0.0004	0.0024	0.0130
	States.V	0.0139	0.0021	0.0004	0.0024
	States.D	0.0093	0.0000	0.0000	0.0086
	States.A	0.0000	0.0000	0.0088	0.0094

0.0005 bits/second

No Loss

Alice	Bob	d1v	d1h	d2v	d2h
States.H	States.H	0.0000	0.0000	0.0000	2.0000
	States.V	0.4963	0.4988	0.5013	0.5036
	States.D	0.2495	0.0425	0.2529	1.4551
	States.A	0.2503	0.0430	0.2510	1.4557
States.V	States.H	0.4983	0.4991	0.5005	0.5020
	States.V	0.0000	0.0000	2.0000	0.0000
	States.D	0.0419	0.2495	1.4587	0.2500
	States.A	1.4583	0.2500	0.0430	0.2487
States.D	States.H	0.2500	0.0435	0.2497	1.4569
	States.V	0.0430	0.2493	1.4571	0.2506
	States.D	0.0000	0.0000	0.9993	1.0007
	States.A	0.9993	0.0000	0.0000	1.0007
States.A	States.H	0.2526	0.0440	0.2489	1.4545
	States.V	1.4582	0.2496	0.0426	0.2496
	States.D	0.9991	0.0000	0.0000	1.0009
	States.A	0.0000	0.0000	1.0017	0.9983

1 x 10^5 bits/second

State of the Art

Alice	Bob	d1v	d1h	d2v	d2h
States.H	States.H	0.0000	0.0000	0.0000	1.9602
	States.V	0.4884	0.4913	0.4904	0.4897
	States.D	0.2433	0.0422	0.2473	1.4260
	States.A	0.2428	0.0428	0.2497	1.4248
States.V	States.H	0.4908	0.4904	0.4866	0.4912
	States.V	0.0000	0.0000	1.9593	0.0000
	States.D	0.0432	0.2434	1.4291	0.2438
	States.A	1.4270	0.2453	0.0425	0.2454
States.D	States.H	0.2446	0.0424	0.2422	1.4312
	States.V	0.0419	0.2472	1.4240	0.2460
	States.D	0.0000	0.0000	0.9796	0.9817
	States.A	0.9802	0.0000	0.0000	0.9808
States.A	States.H	0.2425	0.0411	0.2436	1.4335
	States.V	1.4300	0.2439	0.0427	0.2430
	States.D	0.9768	0.0000	0.0000	0.9824
	States.A	0.0000	0.0000	0.9776	0.9838

9 bits/second

School of Engineering

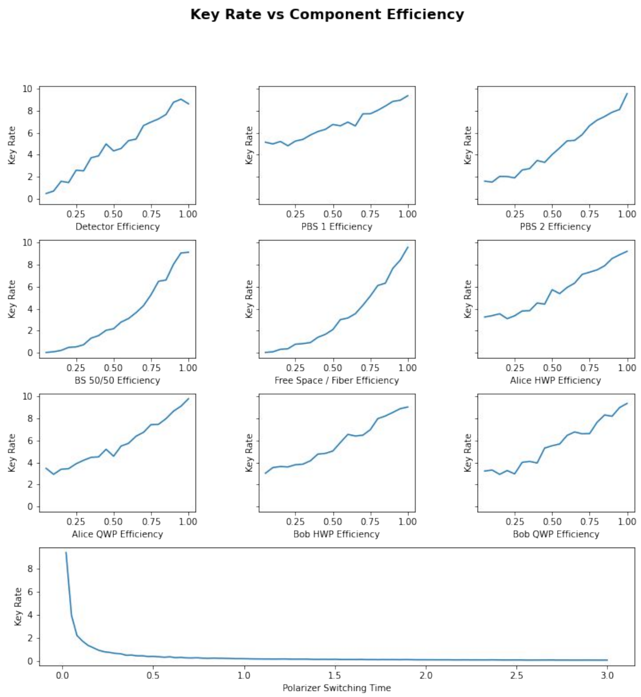
Simulation Results / Data Analysis

- Polarizer switching time has biggest impact on secret key rate
- Detector efficiency, BS 50/50, and Free Space to Fiber conversion are next most important components

No Loss SKR: 1 x 10^5 bits/second

MIT Optics Lab SKR: ~0.0005 bits/second

State of the Art SKR: ~9 bits/second



MIT | School of Engineering

Remaining Challenges

Two primary sources of errors that can cause a reduction in the SKR:

- Imperfect visibility of the Hong-Ou-Mandel (HOM) effect
  - Affects the detectors that fire on any given combination of polarization states
  - Leads to incorrect detection events
- Disturbance of polarization maintenance in fiber
  - Adds noise to our data due to unexpected polarization states

Conclusions & Broader Implications

- Implemented the MDI-QKD protocol, developed a simulation, demonstrated its security
- Shown that our system simulation is able to generate secure keys in reasonable amount of time

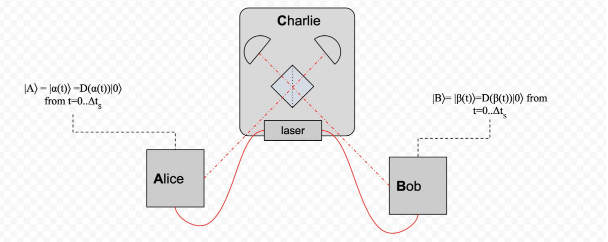
Potential impact of MDI-QKD:

(1) additional security measures to enhance the security of traditional QKD against potential attacks that exploit device imperfections and vulnerabilities,

(2) potential to extend the distance of secure communication over optical fiber networks.

Possible future direction:

- Charlie in MDI-QKD implemented via secure distributed Machine Learning (ML) computation model



Alice and Bob ensure the security of the channel by testing Bell inequality, as in measurement device independent QKD (HK Lo, etc). Let's say, specifically, that for this, they encode qubits of duration Δt_s . They intersperse multi-symbol waveforms $\alpha(t)$ and $\beta(t)$ encoded on N symbols (samples), i.e. at symbol duration $\Delta t_s/N$.

Thus, Alice and Bob can delegate to Charlie the computation of an inner produce C=**A**.**B** where C\elem[C1,C2] for detector 1 or detector 2. Here, we're postselecting on Charlie getting a click on either of the detector, just as we would for qubits under the MDI-QKD scheme.

Courtesy of Professor Dirk Englund

References

Lo, Hoi-Kwong, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution." Physical review letters 108.13 (2012): 130503.

Wang, W., Tamaki, K. & Curty, M. Measurement-device-independent quantum key distribution with leaky sources. Sci Rep 11, 1678 (2021).

Bhaskar, Mihir K., et al. "Experimental demonstration of memory-enhanced quantum communication." Nature 580.7801 (2020): 60-64.

L. Cao, W. Luo, et al. "Chip-Based Measurement-Device-Independent Quantum Key Distribution Using Integrated Silicon Photonic Systems." Phys. Rev. Applied 14, 011001 (2020).

C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. Physical Review Letters, 59(18):2044–2046, November 1987.