100Mb s^{-1} Quantum Key Distribution

Wei Li†, **Likang Zhang**†, Hao Tan, Yichen Lu, Sheng-Kai Liao, Jia Huang, Hao Li, Zhen Wang, Hao-Kun Mao, Bingze Yan, Qiong Li, Yang Liu, Qiang Zhang, Cheng-Zhi Peng, Lixing You, Feihu Xu & Jian-Wei Pan

University of Science and Technology of China

W. Li et al., Nat. Photon. **17**, 416–421 (2023).

Outline

- High-rate QKD: background and challenges
- Our 100 Mb/s BB84 system
  - High-speed laser source
  - Low-error modulator
  - High-speed and high-efficiency SNSPD
  - High-throughput postprocessing
- Summary & Outlook

Why we need high key rate?

Key rate is listed as one of the **major challenges** for practical QKD systems.

1 Gb s^{-1}

key rate scale

npj | Quantum Information

REVIEW ARTICLE OPEN

Practical challenges in q

Eleni Diamanti[1], Hoi-Kwong Lo[2], Bing Qi[3,4] and Zhi

MAJOR CHALLENGES IN PERF

In the quest for high perform both hardware and softwar pursued.

Hardware development

Key rate. Encryption keys gen symmetric cipher scheme, such

Quantum Science and Technology

PERSPECTIVE

Quantum networks: where should we be heading?

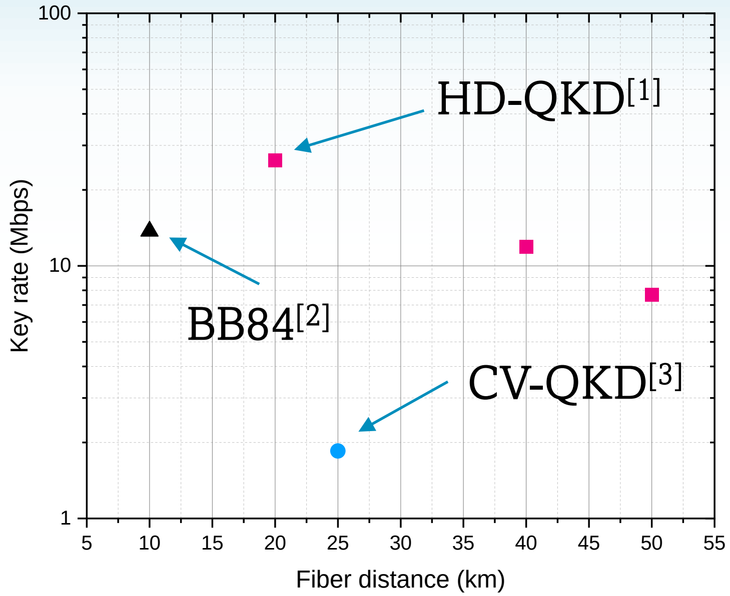
Masahide Sasaki

practical applications. For dealing with realistic data size for one data centre, which is something like Peta byte at least, corresponding to the size of human genomes of million persons, the key generation rate should be a 1 Gb s^{-1} scale. Thus, to realise a killer application of QKD in data storage, the key generation rate needs to be much improved.

Current status of key rates

- Higher key rate: a practicality challenge
- High-rate QKD are mostly based on **BB84**, **high-dimensional** and **continuous-variable** protocol

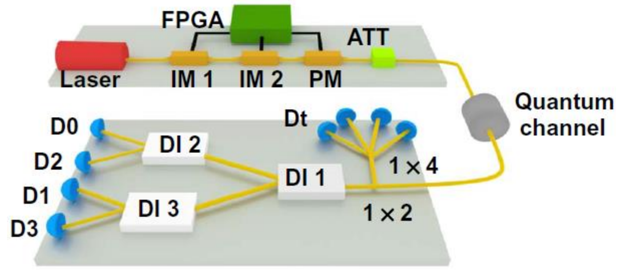
Secret key rate comparison



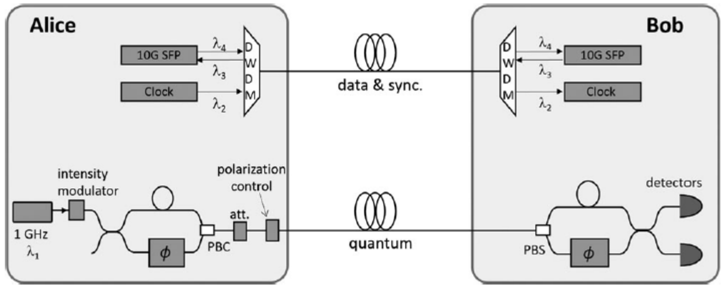
Highest **real-time** secret key rate

13.7 Mbps @ 2 dB

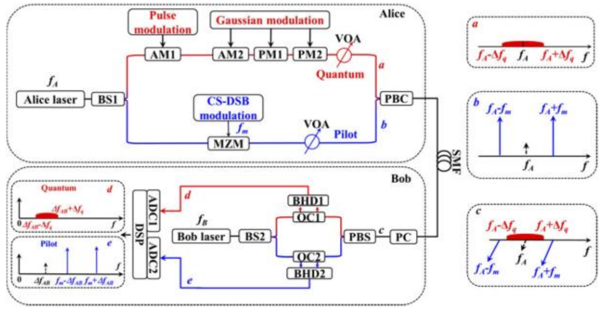
High-dimensional protocol



BB84 protocol



Continuous-Variable protocol



[1]N. T. Islam et al., Sci. Adv. 3, e1701491 (2017).

[2]Z. Yuan et al., J. Light. Technol. 36, 3427 (2018).

[3]Heng Wang et al., Opt. Express 28, 32882-32893 (2020)

Technical challenges

High-speed Laser

High pulse rate and phase-randomized light pulses

High-speed Low-error Modulation

High-speed modulation signal tends to increase QBER due to limited bandwidth and crosstalk

High-count-rate High-efficiency Detector

SPAD : High speed *but* limited efficiency

SNSPD : High efficiency *but* limited count rate

Solutions

High-speed DFB laser diode

with high-amplitude narrow-pulse driving signals

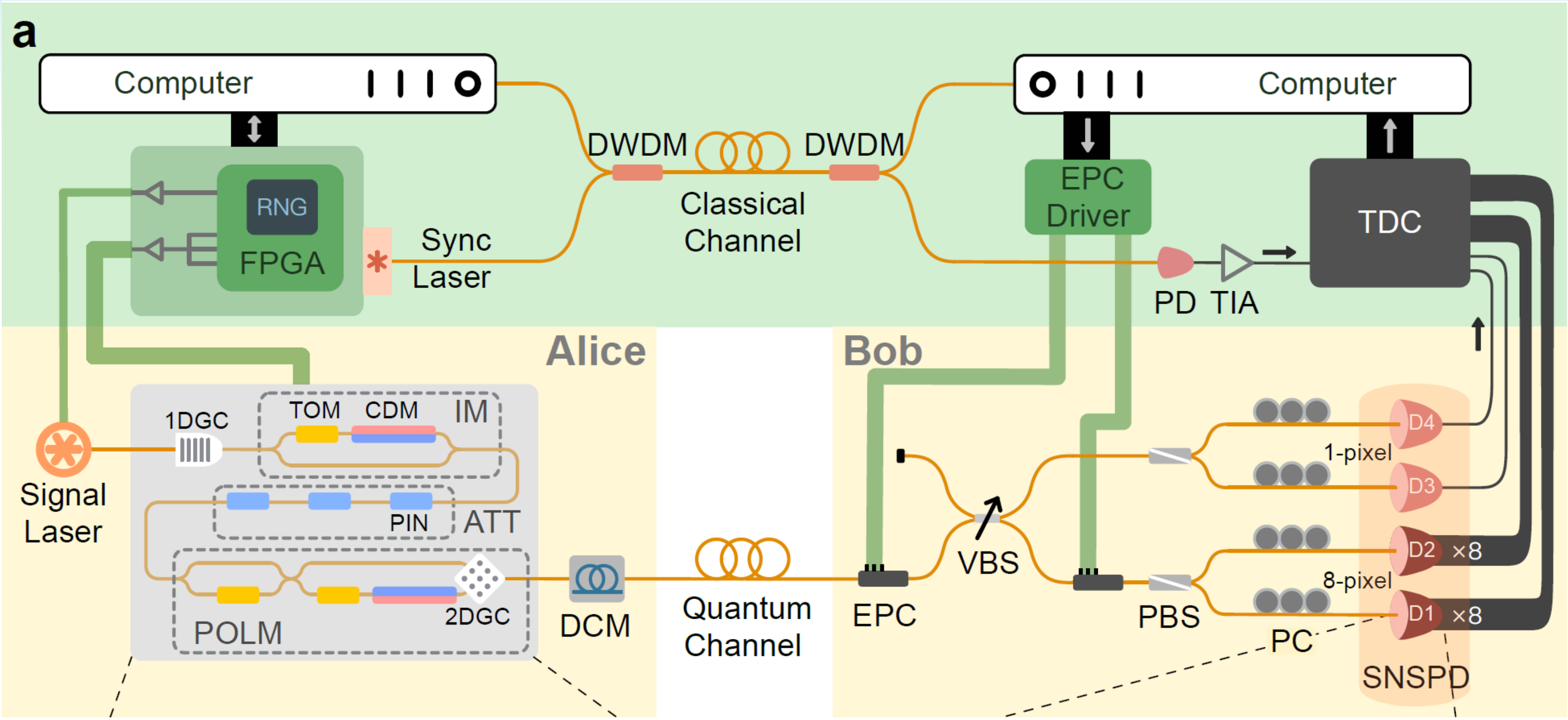
Silicon photonic transmitter

featuring high-bandwidth and stable modulation with DC-coupled high-speed driving signals

Multi-pixel SNSPD

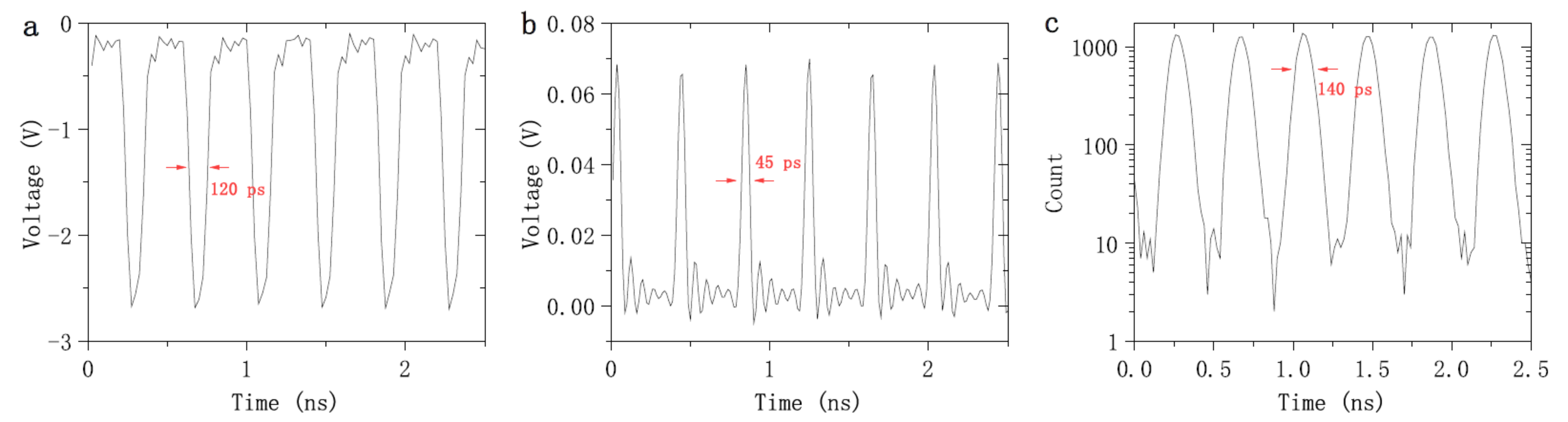
with high speed *and* high efficiency

System setup



- 1-decoy 4-state efficient BB84 protocol
- 2.5-GHz random polarization modulation with 0.4% QBER on a silicon photonic transmitter
- 8-pixel SNSPD detect 552M photons with 62% efficiency
- 344 Mbps postprocessing throughput
- Time synchronization and polarization compensation

Light pulse generation



Electrical driving signal

Light pulse waveform (measured by high-speed photodiodes)

Light pulse histogram (measured by SNSPD)

Driving waveform:

- DC bias
- Swing amplitude
- Pulse width

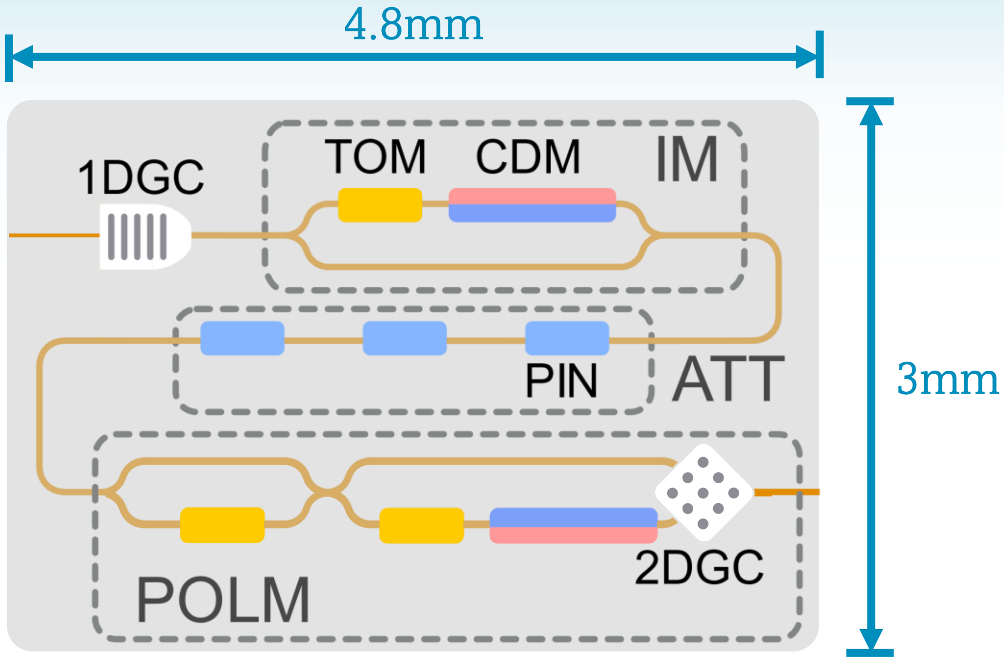
> First relaxation oscillation

< Second relaxation oscillation[1]

Narrow and low-jitter pulses

[1]E. H. Bottcher et al., Journal of Applied Physics 63, 2469 (1988)

Silicon photonic transmitter

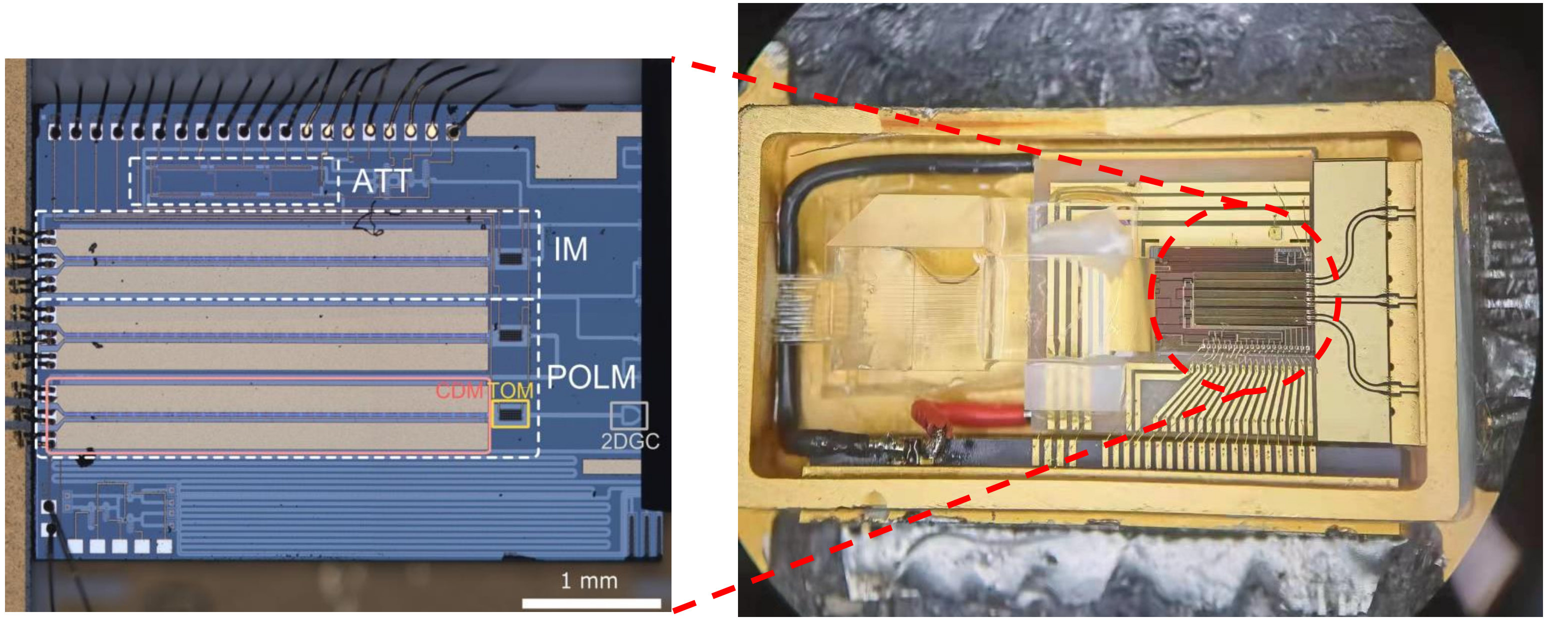


Components:

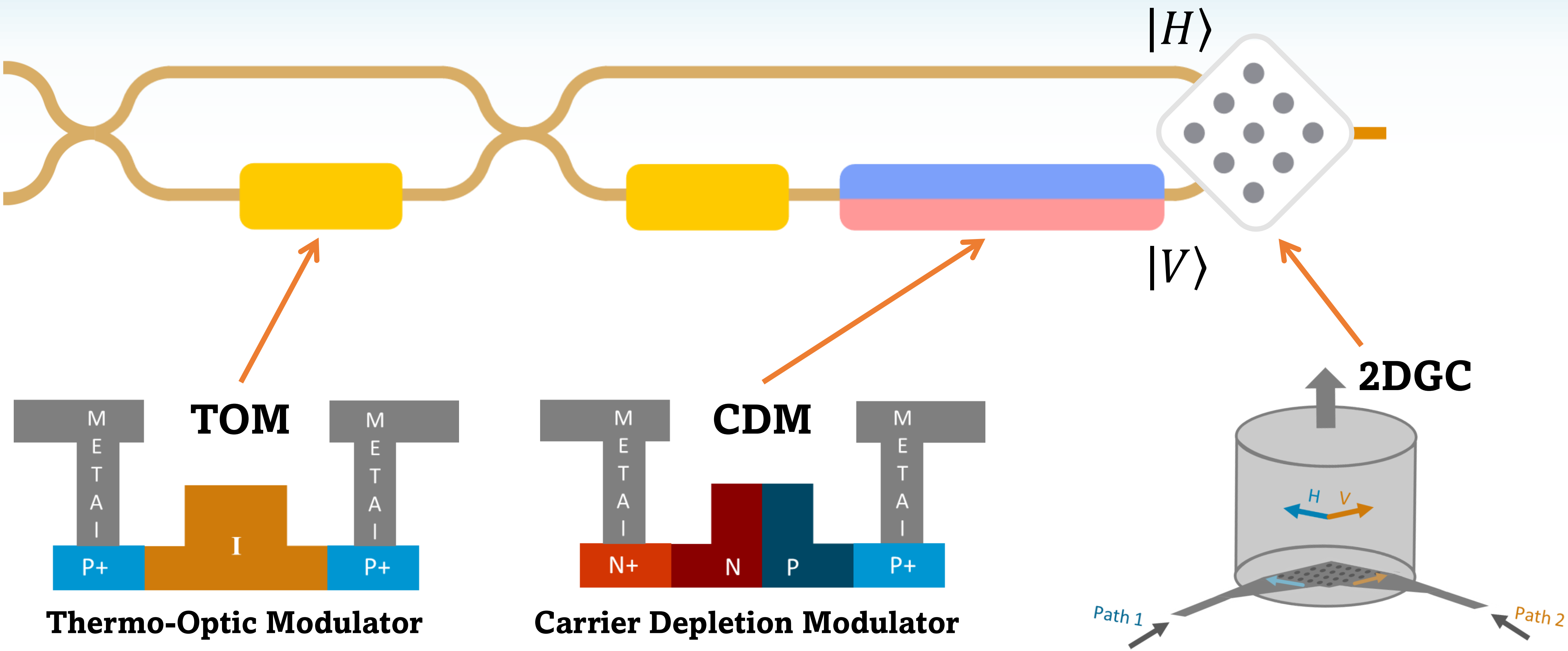
- One intensity modulator
- One polarization modulator
- Three cascaded adjustable attenuators

Optoelectronic packaging:

- Airtight sealing
- 8 IO fiber optic arrays
- 3 RF + 26 DC connectors
- Packaging TEC



Polarization modulation



Thermo-optic effect

Bandwidth ~kHz, V_π ~1V

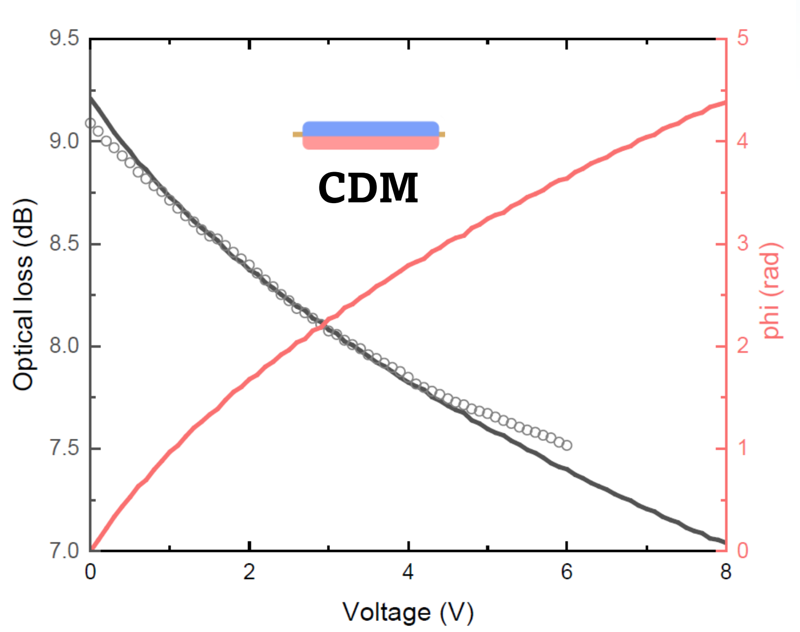
Plasma dispersion effect

Bandwidth ~GHz, V_π ~5V

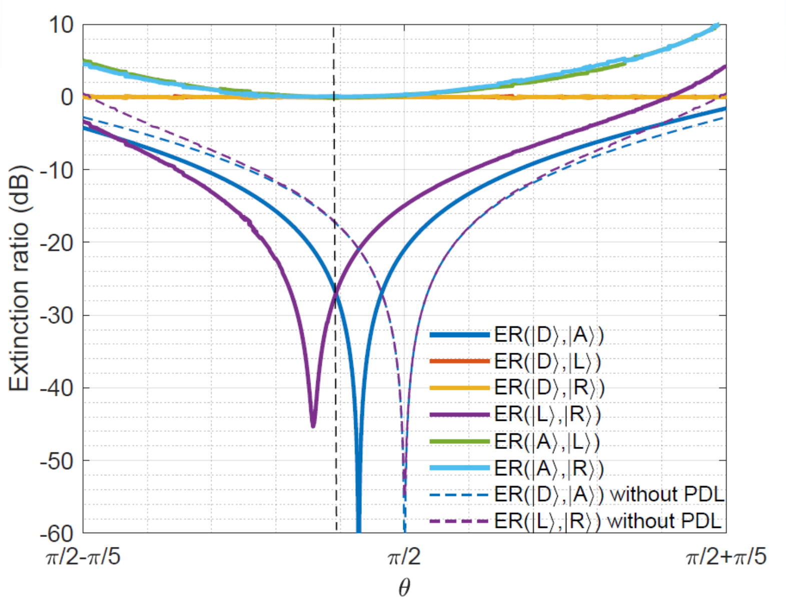
2-Dimensional Grating Coupler

Path to polarization converter

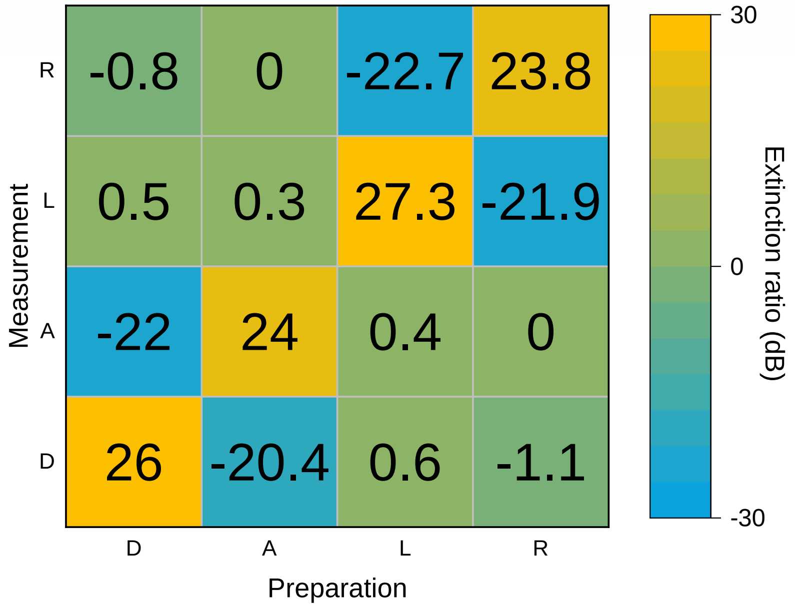
Polarization extinction ratio



Refractive index and absorption rate affected by carrier concentration

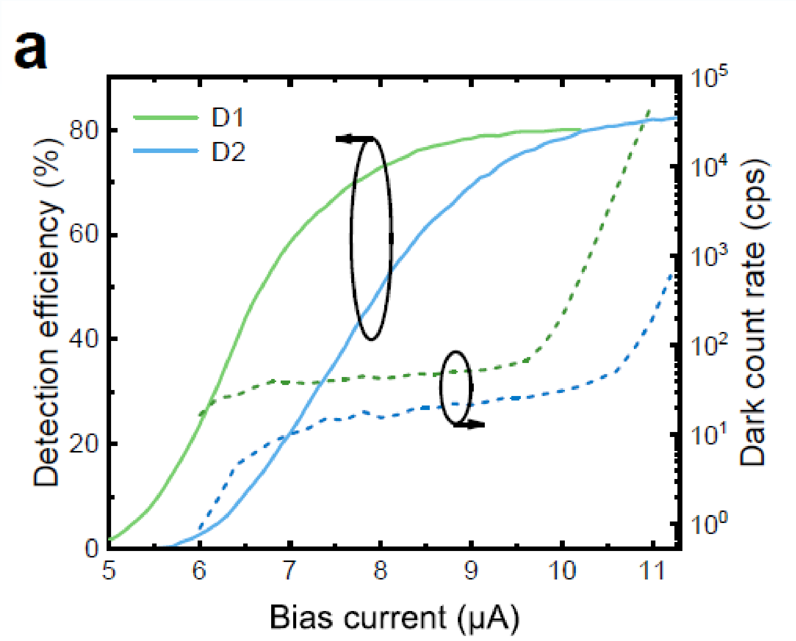


Polarization extinction ratio simulation with phase-dependent loss (2 dB)

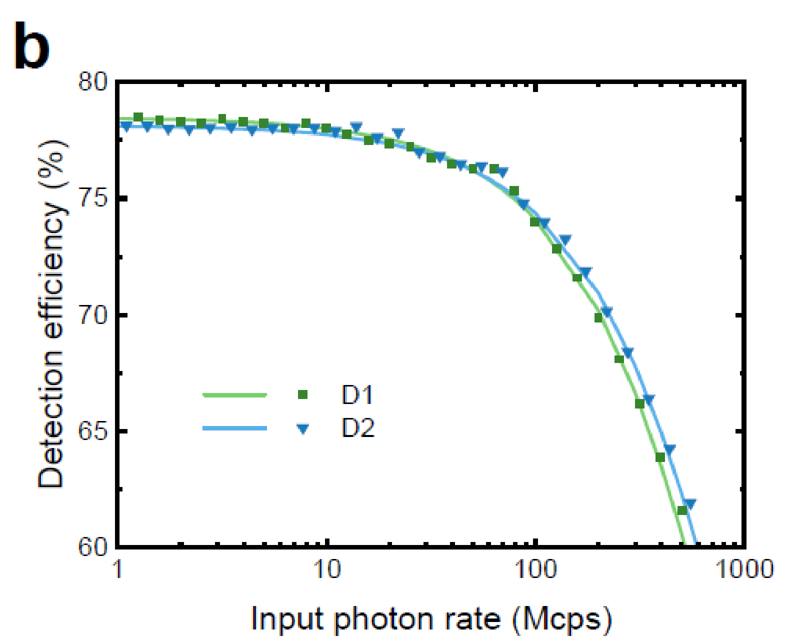


- 23.7 dB average extinction ratio
- 0.4% average bit error rate

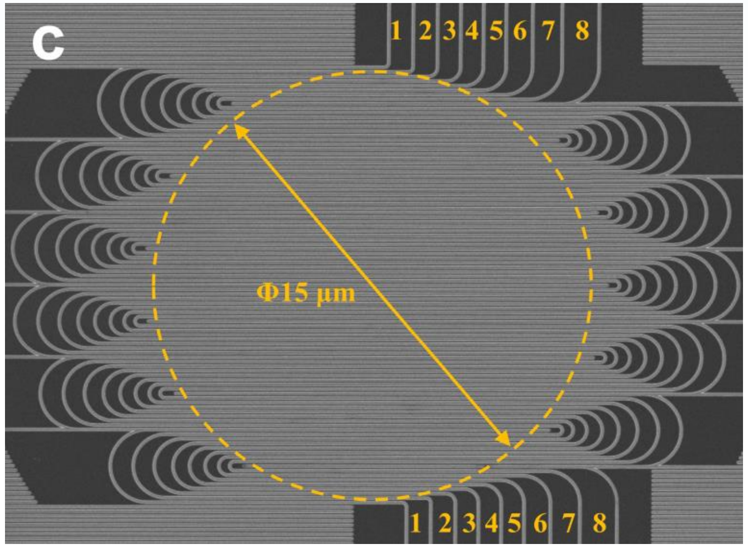
8-pixel SNSPD



- Overall efficiency ~ 80%
- Total dark count ~ 100Hz

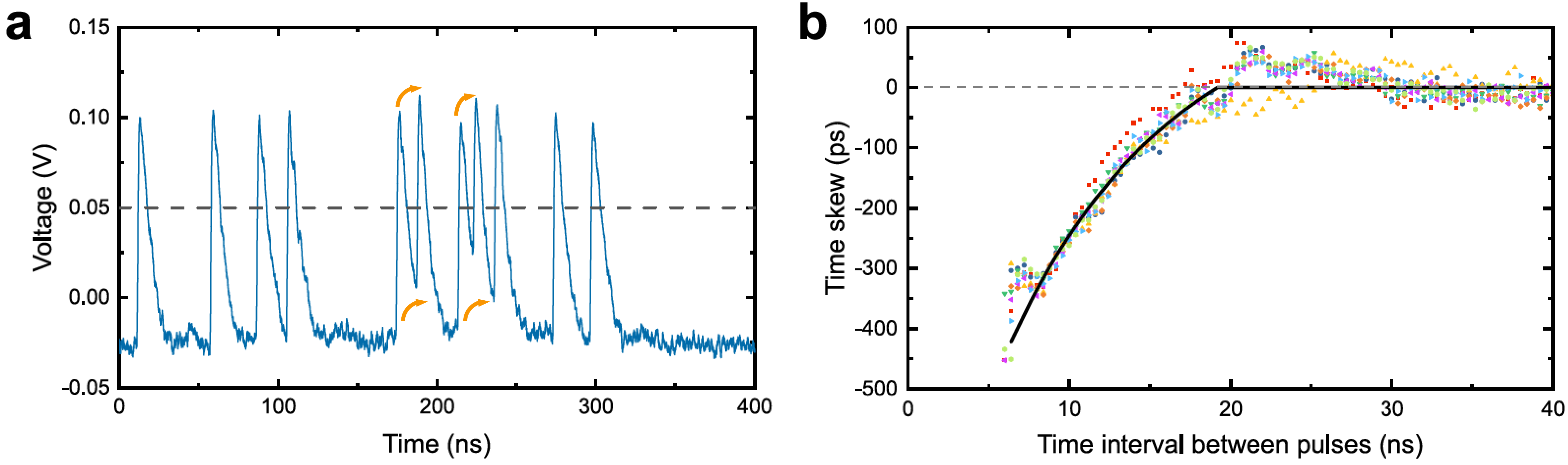


- Recovery time **< 1 ns**
- Maximum count rate **~ 340 Mcps**



Scanning electron microscope image of 8-pixel SNSPD

Time skew and compensation

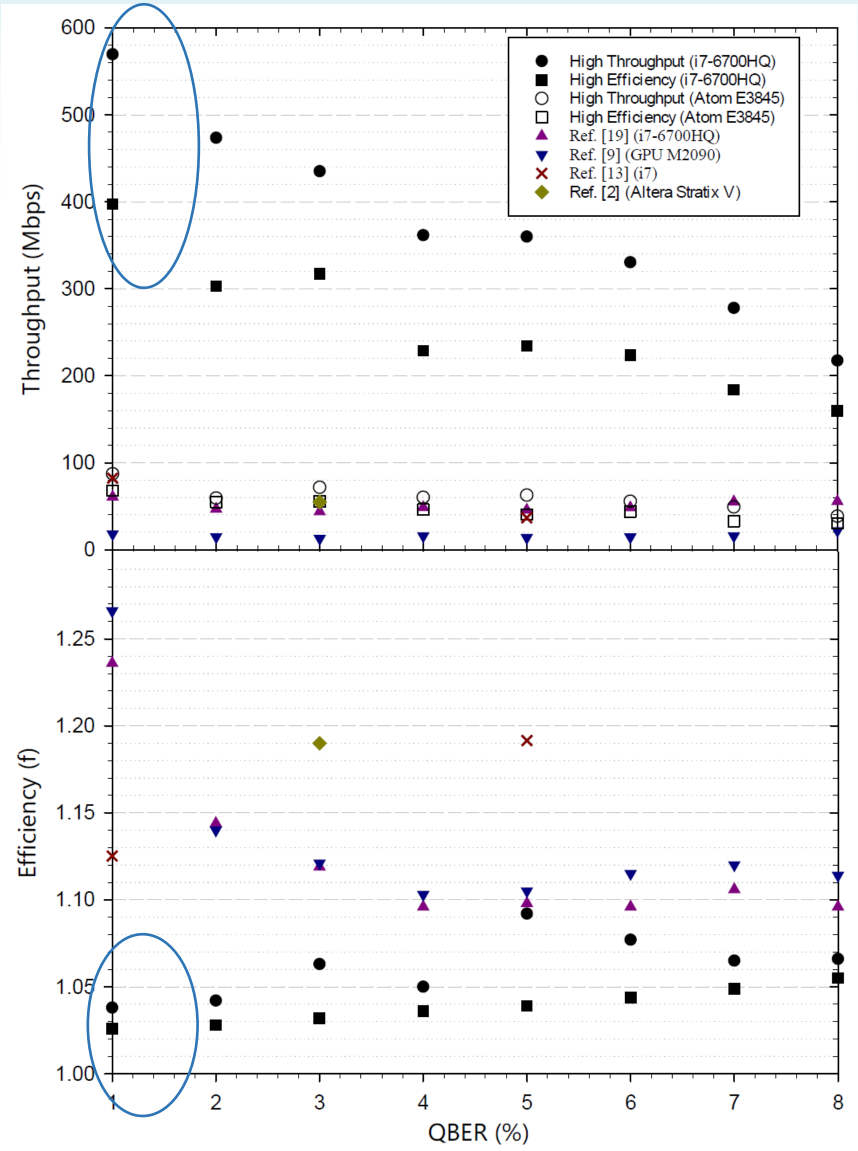


Threshold discrimination
+
Pulse pile up

→ **Detection time skew**

- Shorter intervals → Larger time skew
- 0km *without* compensation : QBER = 7.01%
- 0km *with* compensation : QBER = 0.83%

Cascade information reconciliation



Plot of throughput and efficiency vs. QBER [1].

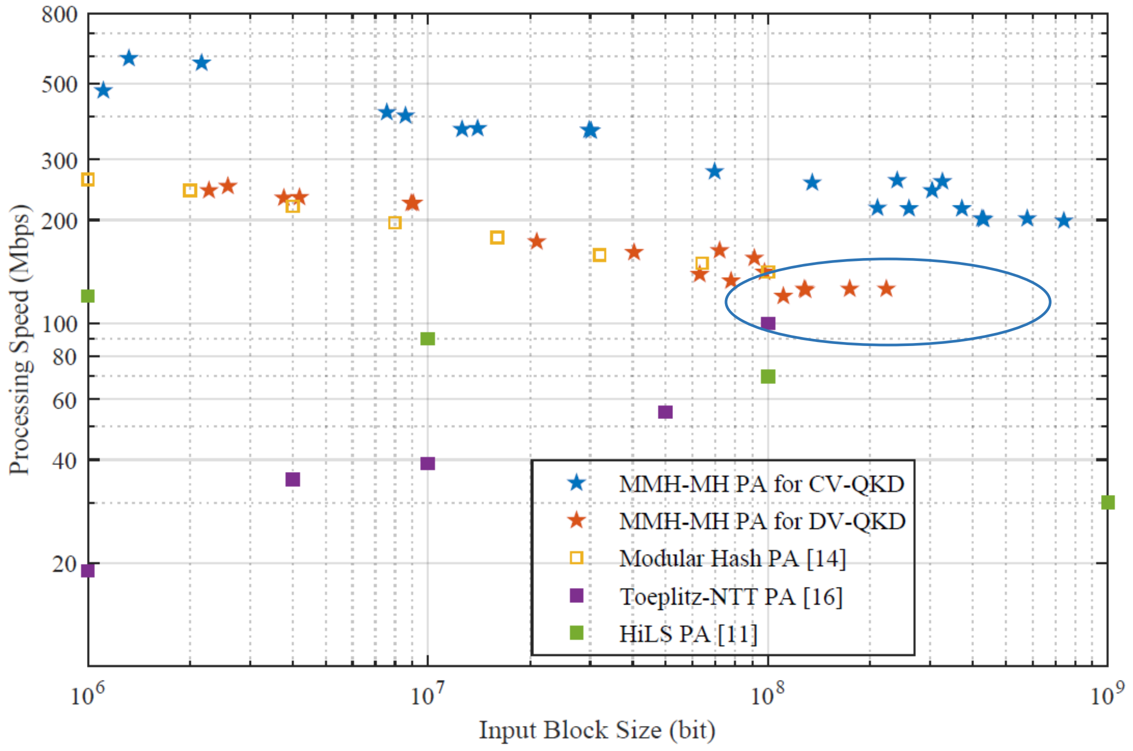
- High throughput, high reconciliation efficiency Cascade error correction based on CPU platform
- When QBER is 1%, the throughput is 570Mbps and the reconciliation efficiency is 1.04

Why Cascade?

- Good QBER fluctuation adaptability
- Better performance when QBER is low
- Less computational resource

[1] H.-K. Mao et al., Opt. Quantum Electron. 54, 163 (2022).

MMH-MH privacy amplification



The throughput comparison between MMH-MH (multilinear-modular-hashing and modular arithmetic hashing) privacy amplification scheme and existing schemes [1].

- Large block size, high speed MMH-MH privacy amplification based on CPU platform
- When the block size is 10^8, the processing speed is 140 Mbps per CPU thread

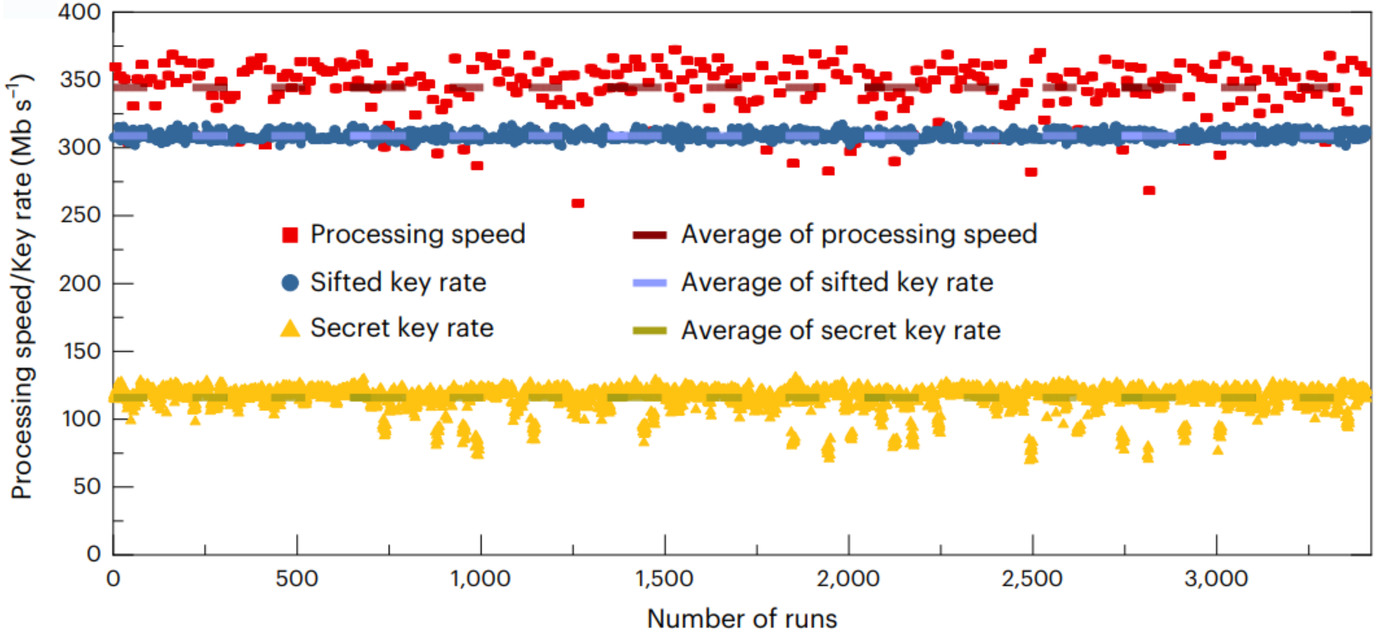
Why MMH-MH?

- Higher processing speed
- Larger block size
- Large integer multiplication

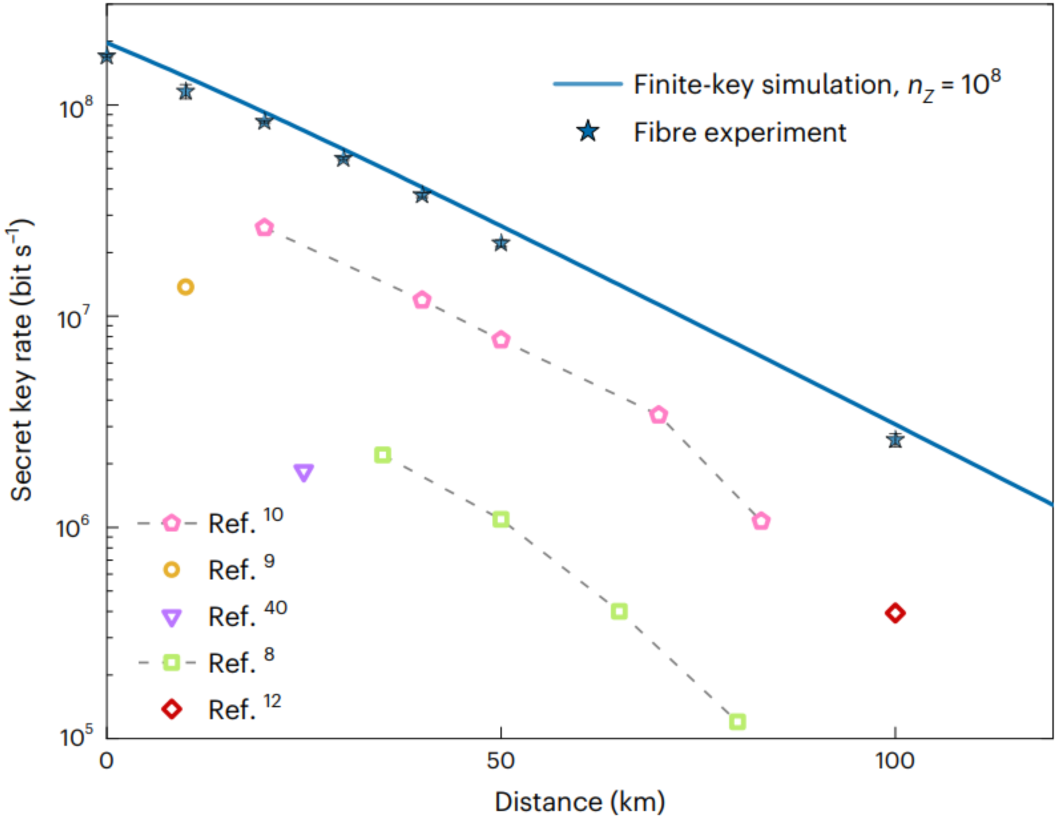
[1] B. Yan et al., Quantum Inf. Process. 21, 130 (2022).

Result: postprocessing speed and secret key rate

Key rate and processing capability at 10-km fiber channel



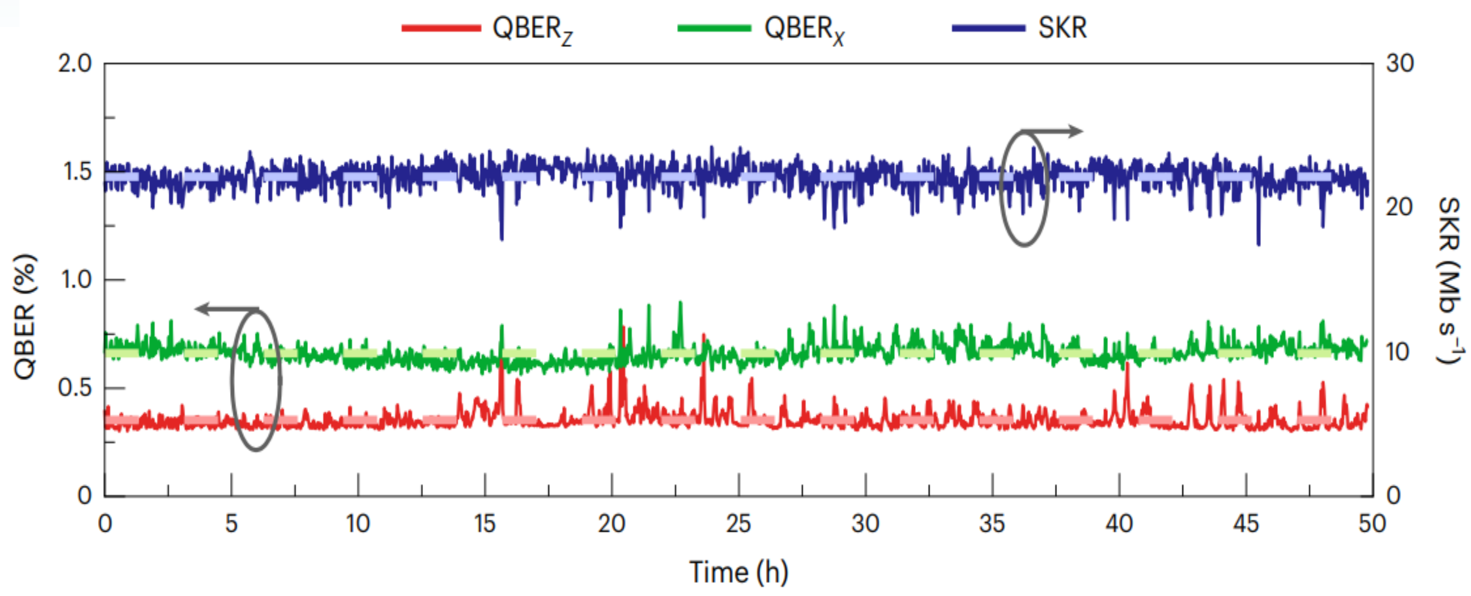
Key rate result and comparison



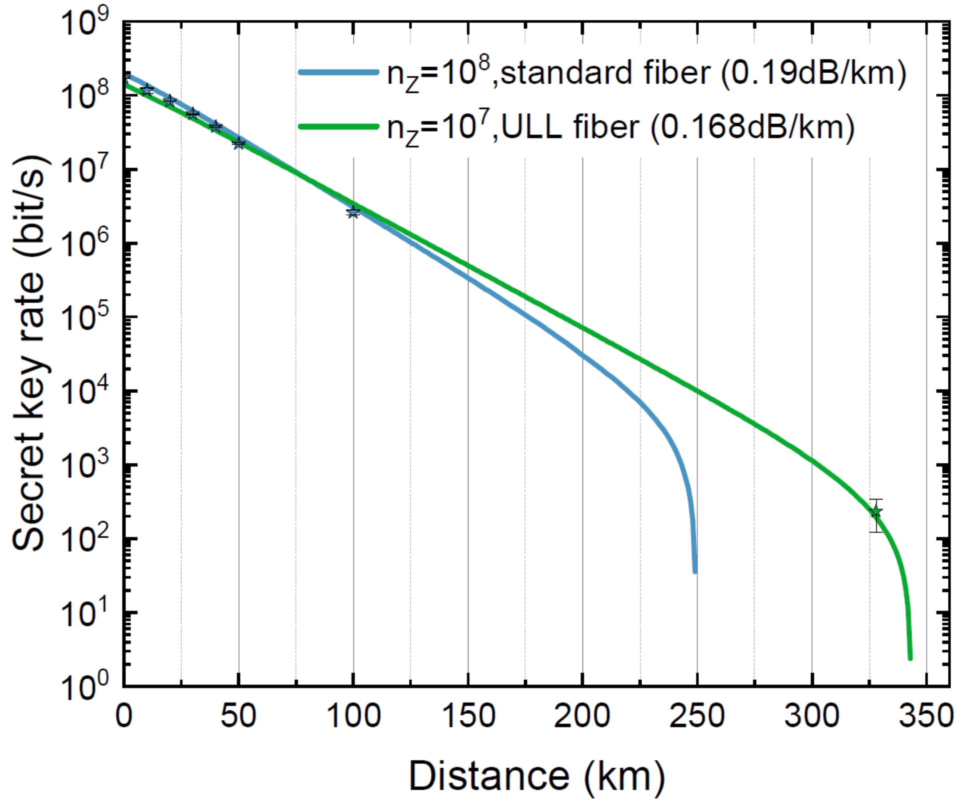
- High-speed postprocessing algorithm based on CPU platforms
- An enhanced Cascade-reconciliation algorithm and a hybrid hash-based privacy-amplification algorithm
- An average throughput of **344.3Mb/s**

115.8 Mbps@10 km

Result: system robustness



- Time synchronization based on Sync laser and WDM
- Polarization compensation based on calibration pulses
- Stable over 50 km standard fibres for 50 hours



The longest distance (328 km) of fibre channel in polarization-encoding QKD systems

Review & Outlook

Table 1 | A list of high-rate QKD experiments

Reference	Protocol	CR (GHz)	QBER (%)	DE (%)	Detector	Loss (dB)	SKR (Mbs^{-1})	PP
Lucamarini et al.[8]	Decoy BB84	1	4.26	20	InGaAs	7.0	2.20	No
Yuan et al.[9]	Decoy BB84	1	3.0	31	InGaAs	2.0[a]	13.72	Yes
Grünenfelder et al.[12]	Decoy BB84	5	1.9	80	SNSPD	20.2	0.39	No
Islam et al.[10]	High dimension	2.5	4.0	70	SNSPD	4.0[a]	26.2	No
Wang et al.[40]	Gaussian CV	0.1	N/A	56	BHD	5.0	1.85	No
This work	Decoy BB84	2.5	0.61	78	SNSPD	2.2	115.8	Yes

CR, clock rate; DE, detector efficiency; PP, post-processing; CV, continuous variable; BHD, balance homodyne detector. [a]Emulated attenuation, fibre channels otherwise.

One order increase of the real-time secret key rate capacity[1]

communications physics

ARTICLE

Check for updates

https://doi.org/10.1038/s42005-022-00941-z OPEN

Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area

Heng Wang[1], Yang Li[1], Yaodi Pi[1], Yan Pan[1], Yun Shao[1], Li Ma[1], Yichen Zhang[2], Jie Yang[1], Tao Zhang[1], Wei Huang[1] & Bingjie Xu[1]

Roads to higher key rate (1 Gbps and beyond)

- Faster light sources, modulation, detectors, postprocessing
- Wavelength division multiplexing
- CV-QKD and HD-QKD protocols

[1] W. Li et al., Nat. Photon. **17**, 416–421 (2023).