Differential Phase Shift Quantum Key Distribution

Hiroki Takesue, Toshimori Honjo,
Kiyoshi Tamaki, and Yasuhiro Tokura

NTT Basic Research Laboratories, NTT Corporation

htakesue@will.brl.ntt.co.jp

Acknowledgements

Collaborators

K. Inoue (Osaka University)

Y. Yamamoto, E. Waks, E. Diamanti, Q. Zhang, K. Wen
M. M. Fejer, C. Langrock, R. V. Roussev
(Stanford University)

S. W. Nam, R. H. Hadfield (NIST)

S. Inoue, N. Namekata, G. Fujii (Nihon University)

Funds

National Institute of Information and Communication (NICT)
CREST, Japan Science and Technology Agency

QKD used for Geneva election

Election fix? Switzerland Tests Quantum Cryptography

Swiss officials will scramble vote data at one gigabit per second to determine whether this experiment lead to more reliable elections

By Larry Greenemeier

TEXT SIZE: − +

During Switzerland's upcoming national elections, officials will use quantum cryptography to secure the network linking its ballot data entry center to the government repository where

Quantum cryptography, which relies on the laws of physics to ensure that encoded messages can be deciphered only by those authorized to do so, has for years promised to deliver encryption far stronger than the public key infrastructures (PKI) more commonly used today. Trouble is, there are few, if any, documented uses of this quantum technology outside of lab settings.

But this is about to change: On Sunday during Switzerland's national elections officials in Geneva will use quantum cryptography to secure the network linking their ballot data entry center to the government repository where votes are stored. Quantum cryptography relies on a highly secure exchange of the keys used to encrypt and decrypt data between a sender and a receiver, and Swiss election officials' confidence that this technology is ready for prime time will provide a strong tailwind for a technology still in its adolescence.

Scientific American Oct 19, 2007.

Outline

1. What is quantum key distribution (QKD) ?

2. Differential phase shift quantum key distribution (DPS-QKD) protocol

3. QKD experiments with various single photon detectors:
- Up-conversion detector
- Superconducting single photon detector: SSPD
- Sine-wave-gated InGaAs/InP Avalanche photodiode

4. Summary

Background

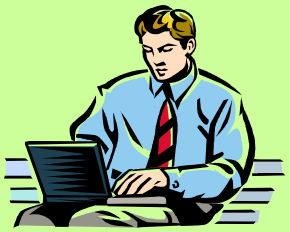
Security system for users who require high-level security.

Sender (Alice)

Receiver (Bob)

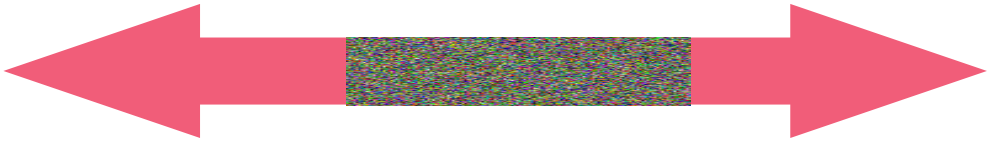
Private line →

High cost, possible eavesdropping



Public line + Public cryptosystem

→ *Possible eavesdropping ?*

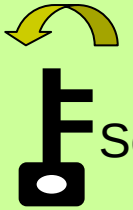


Public line + QKD

→ *Secure !*

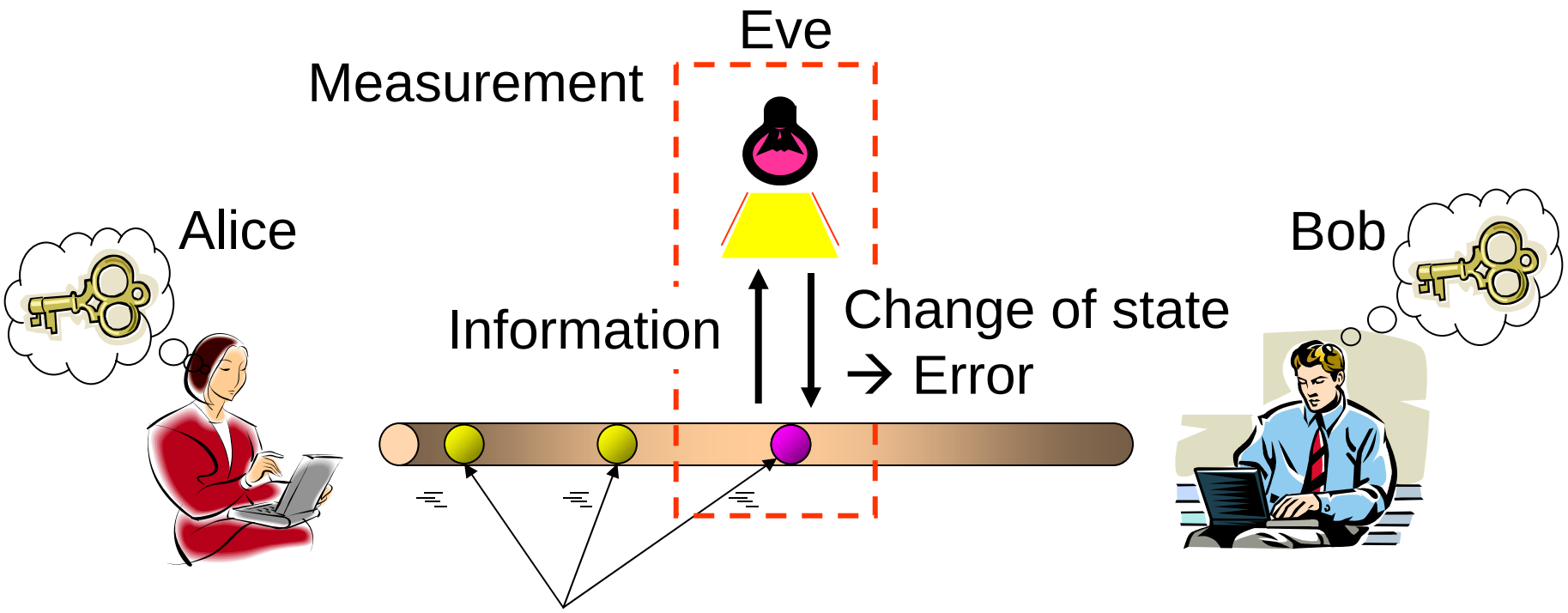
QKD channel

Secret keys



Secret keys

Quantum key distribution (QKD)



Eavesdropping is revealed from increase of errors.

Outline

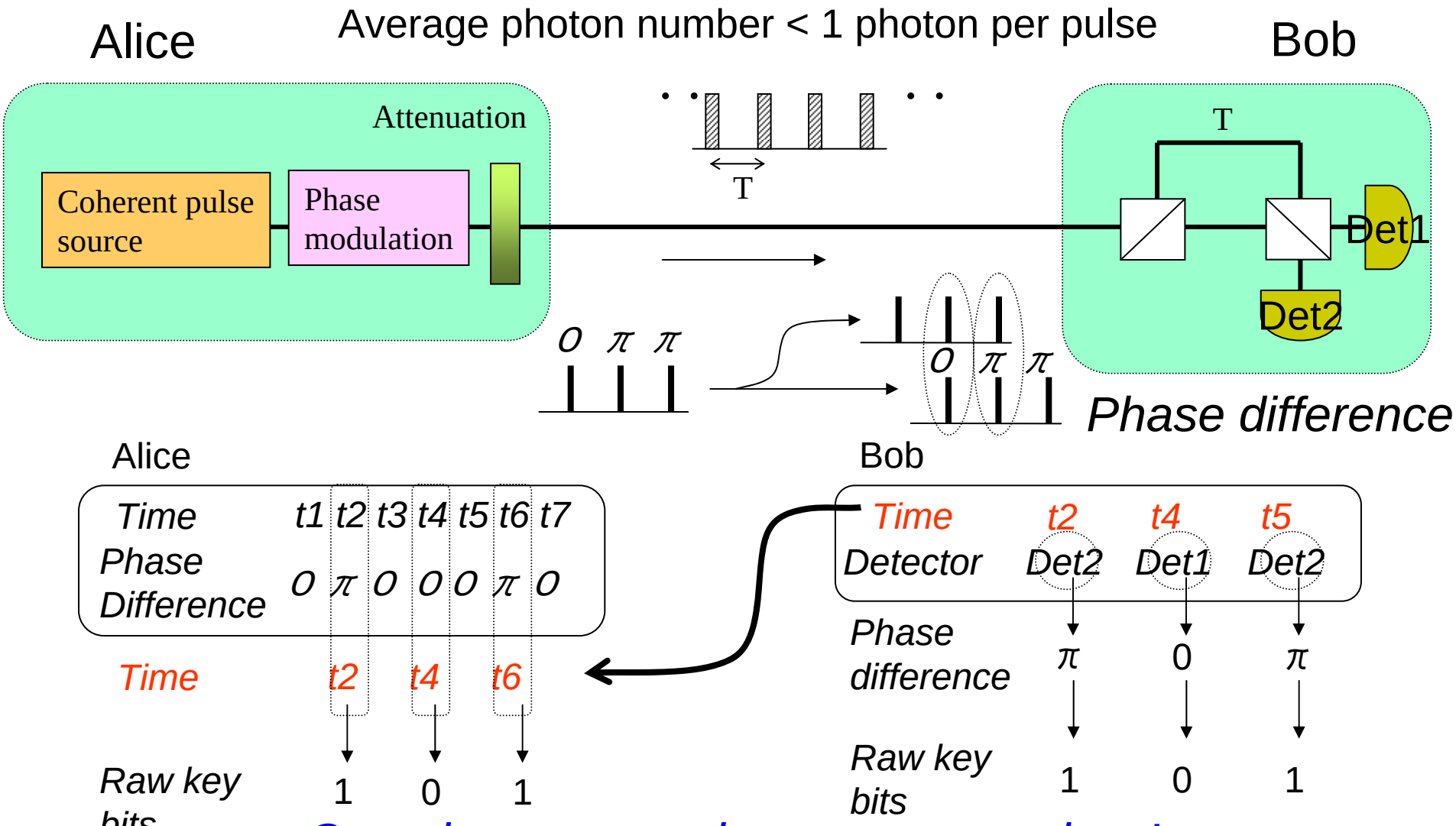
1. What is quantum key distribution (QKD) ?

2. Differential phase shift quantum key distribution (DPS-QKD) protocol

3. QKD experiments with various single photon detectors:
- Up-conversion detector
- Superconducting single photon detector: SSPD
- Sine-wave-gated InGaAs/InP Avalanche photodiode

4. Summary

Differential phase shift QKD (DPS-QKD)



Inoue, Waks Yamamoto., PRL, 89, 037902 (2002).

Merits of DPS-QKD

1. Easy implementation (simple configuration)

2. Easy to increase key rate by increasing clock frequency

3. Secure against a specific attack called “photon number splitting attack” that limited the key distribution distance of previous QKD systems.

Outline

1. What is quantum key distribution (QKD) ?

2. Differential phase shift quantum key distribution (DPS-QKD) protocol

3. QKD experiments with various single photon detectors:

- Up-conversion detector
- Superconducting single photon detector: SSPD
- Sine-wave-gated InGaAs/InP Avalanche photodiode

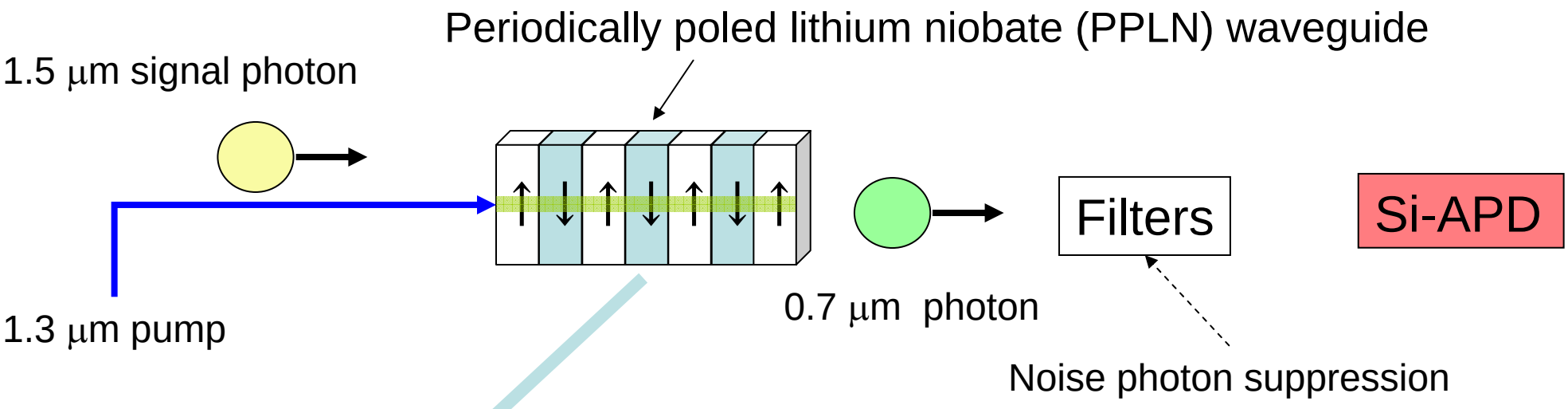
4. Summary

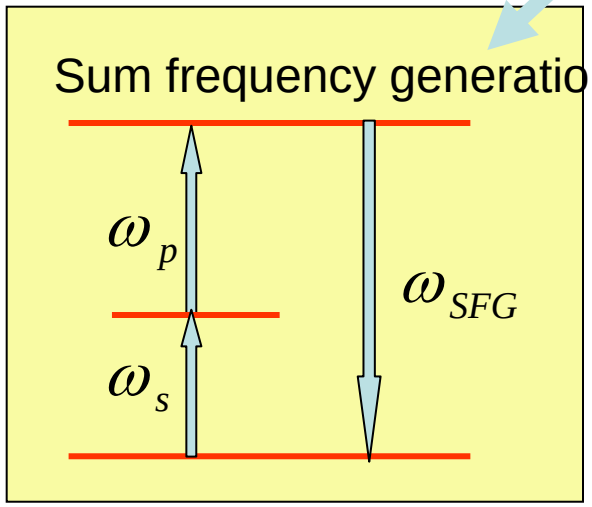
Comparison between InGaAs APD and Si APD

	InGaAs	Si
Wavelength [nm]	1300-1600	300-900
Quantum efficiency	～10 %	～70 %
Dark count rate[Hz]	10000 (typ)	50 (typ)
Afterpulse probability	Large → Gated mode operation (up to 10 MHz)	Small → continuous counting

Can we detect a 1.5-μm photon with a Si-APD?

Frequency up-conversion detector





•The wavelength of a 1.5 μm photon is converted to 0.7 μm, and the converted photon is detected by Si-APD.

Fast, highly efficient single photon counting in the 1.5 μm band.

C. Langrock et al., Opt. Lett., 30, 1725 (2005).

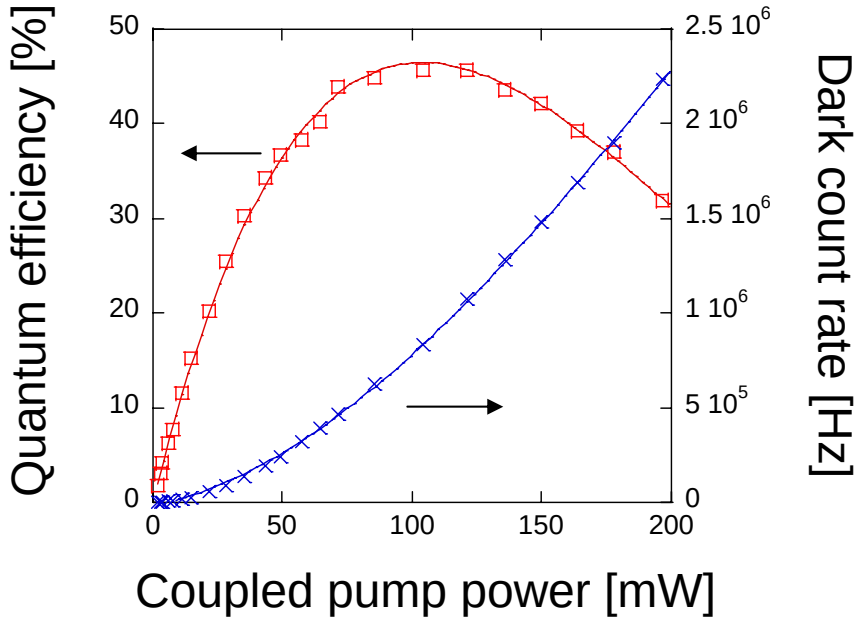
Characteristics

Peak quantum efficiency: 46 %

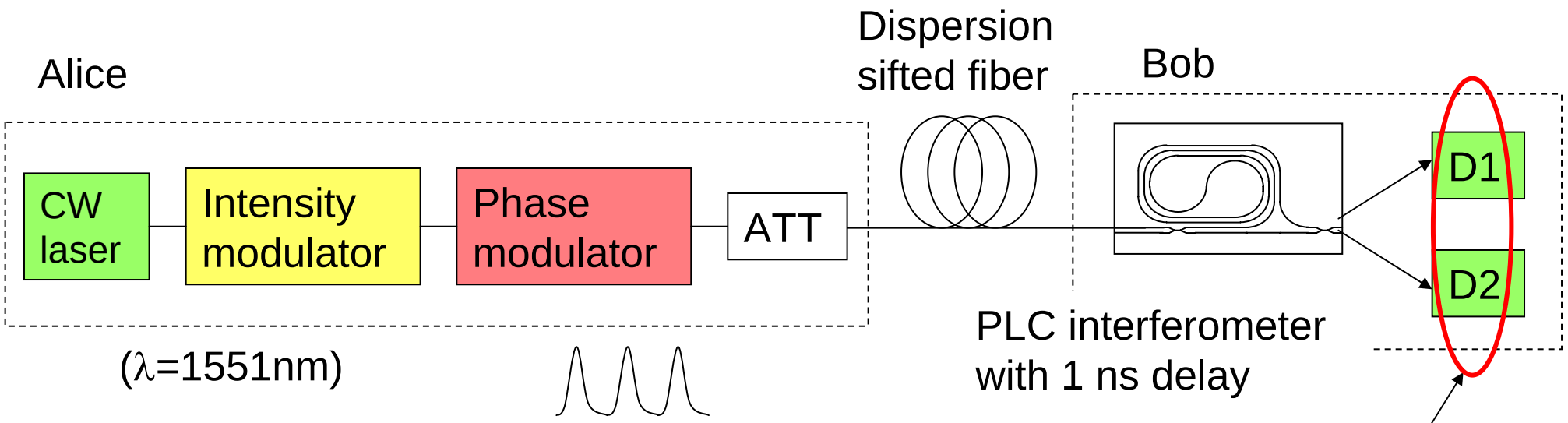
Continuous mode photon counting.

Timing jitter : 30 ps FWHM, but with long tail.
→ Applicable to 1 GHz clock QKD system (but not to10 GHz clock)

Noise photons due to spurious nonlinear effects.
→ SNR improved
when quantum efficiency is low.



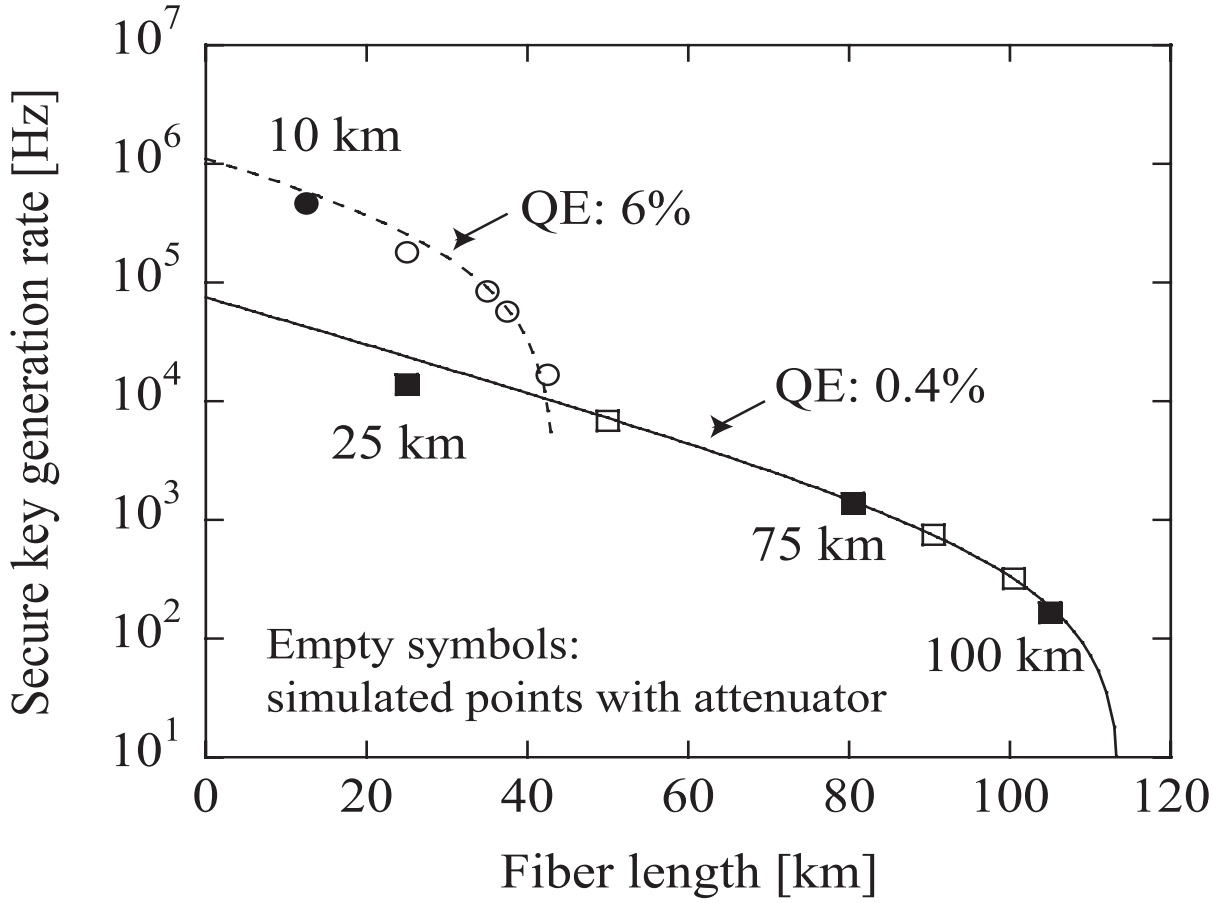
Experimental setup (1-GHz clock)



Pulse width: 70 ps
Average photon number per pulse: 0.2

Low-jitter up-conversion detectors
Quantum efficiency: 6%. 0.4%

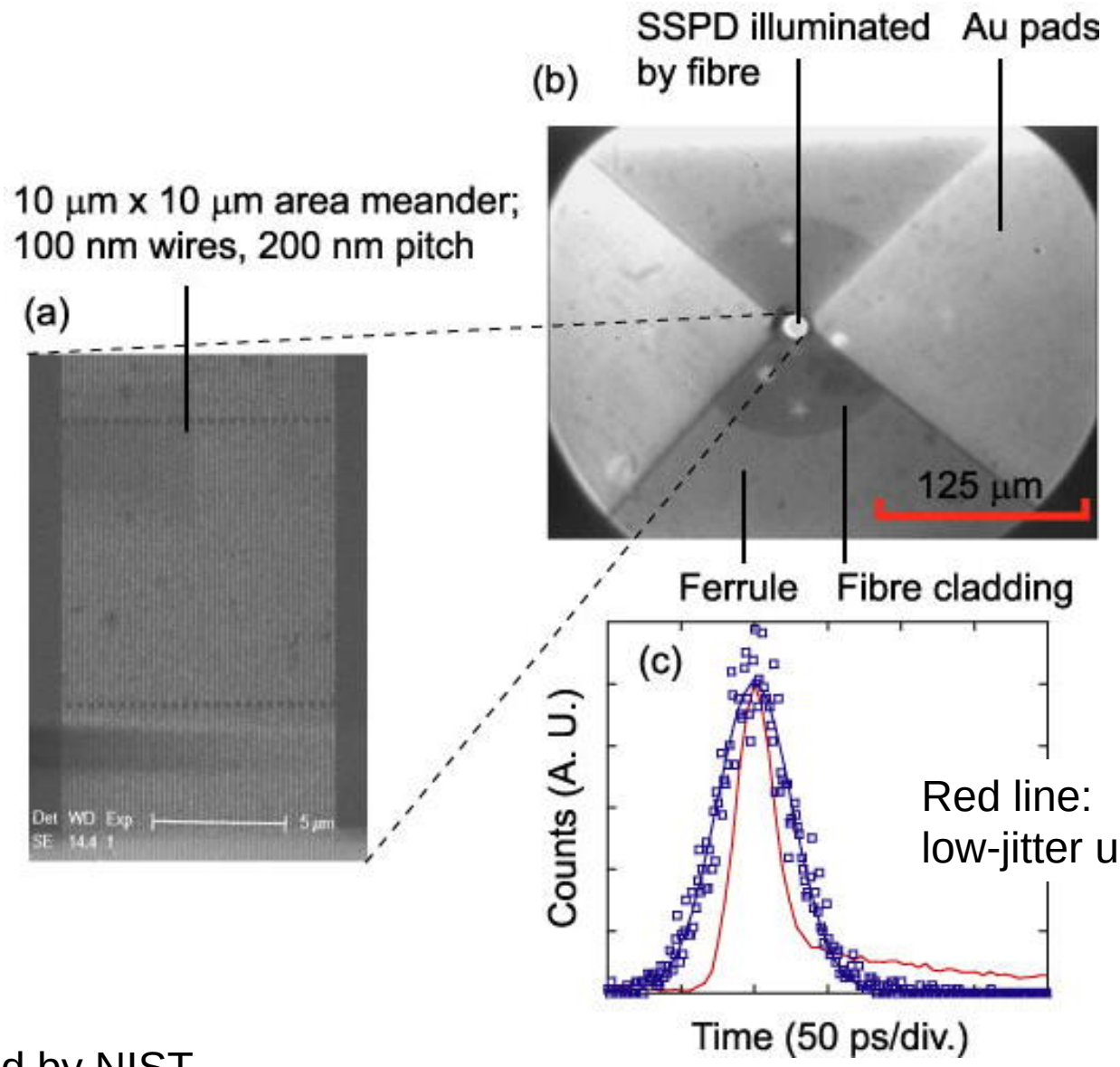
1-GHz clock QKD experiment result



166 bit/s secure key at 100 km.
2 Mbit/s sifted key at 10 km.

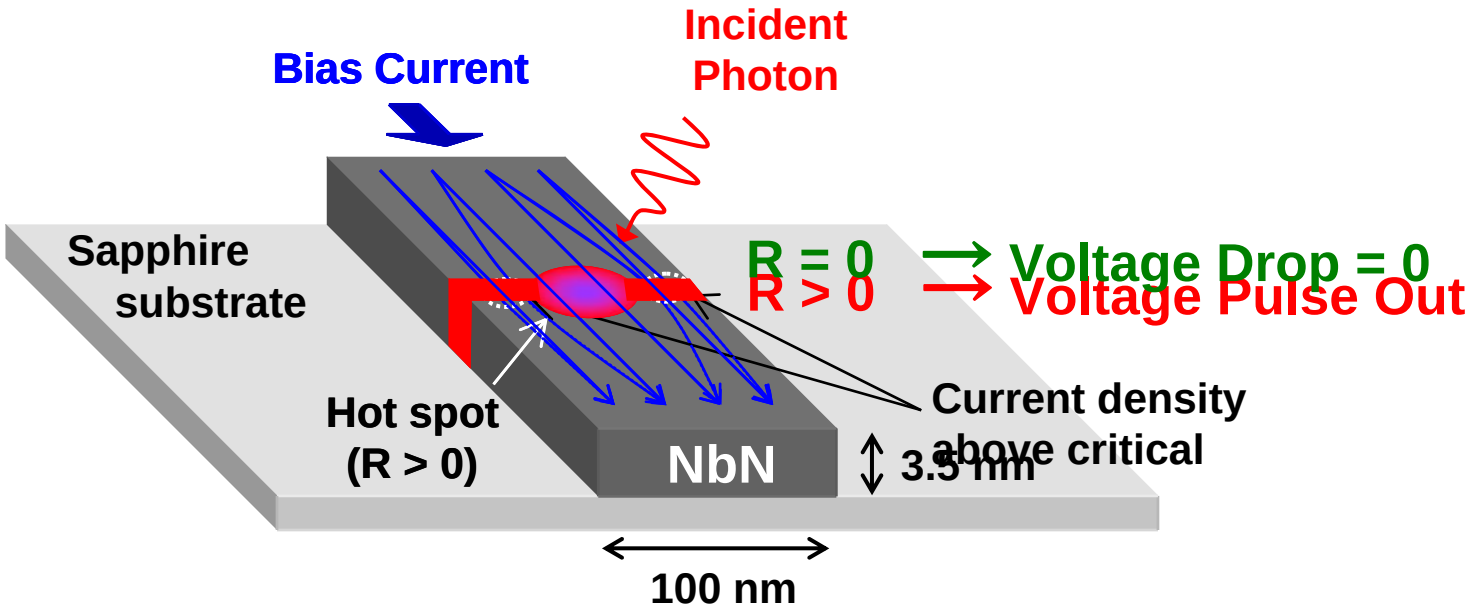
E. Diamanti et al, Opt. Express 14, 13073 (2006).

Superconducting single photon detector (SSPD)



Pictures provided by NIST

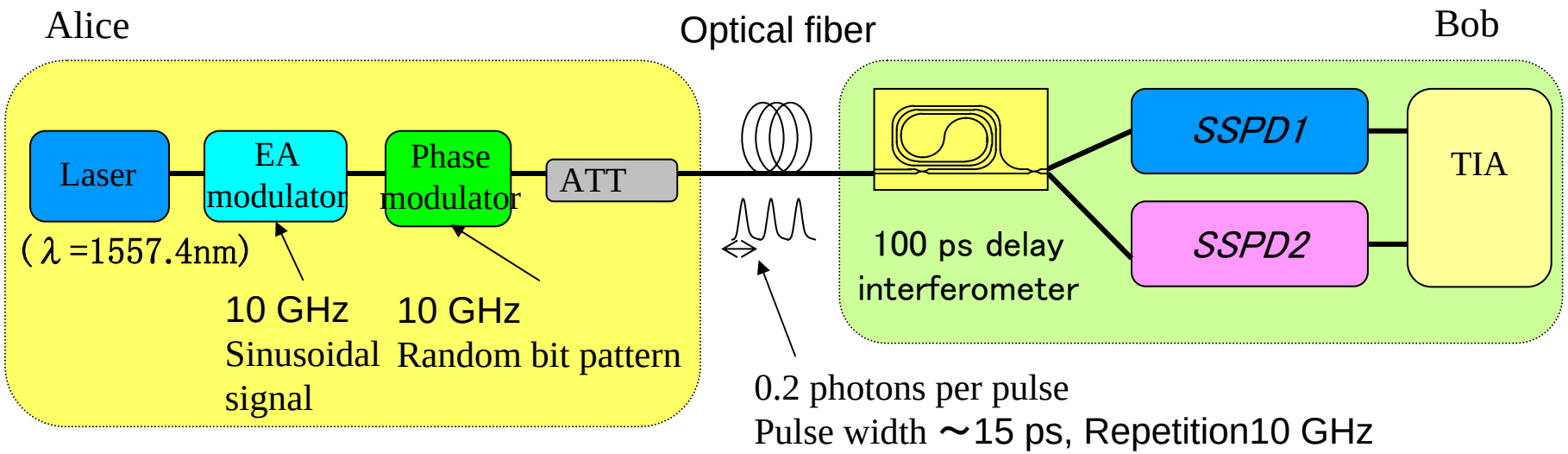
Principle of SSPD

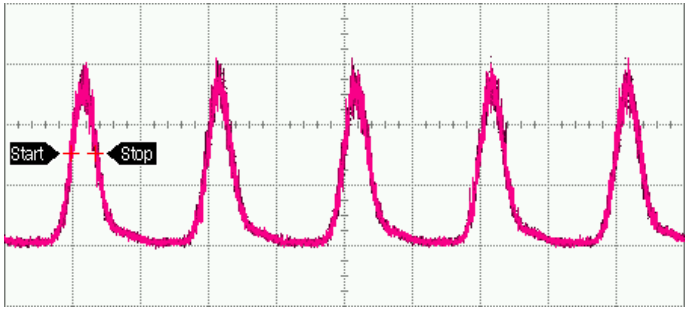


Cryogenic emvironment (3 K)	⇨	Low dark count (about 10 Hz)
Fast response of NbN	⇨	Low jitter (65 ps FWHM, well fitted with Gaussian)
Quantum efficiency	⇨	Currently about 1 %

G. N. Gol'tsman et al, Appl. Phys. Lett. 79, 705 (2001).

10-GHz clock DPS-QKD with SSPDs

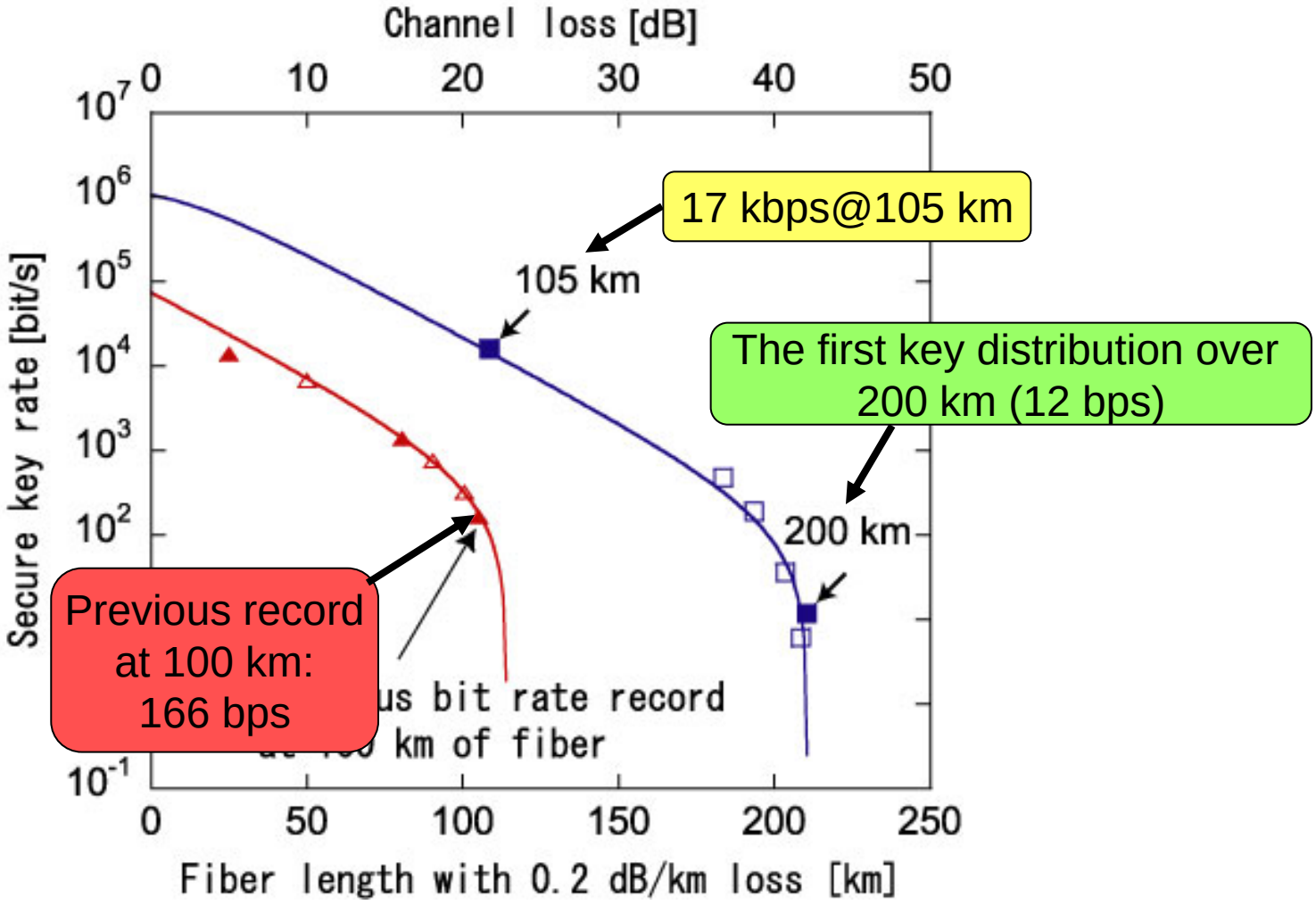




50 ps / div.

Electro-absorption (EA) modulator output waveform
observed with sampling oscilloscope

10-GHz clock QKD result



H. Takesue et al., Nature Photonics 1, 343 (2007).

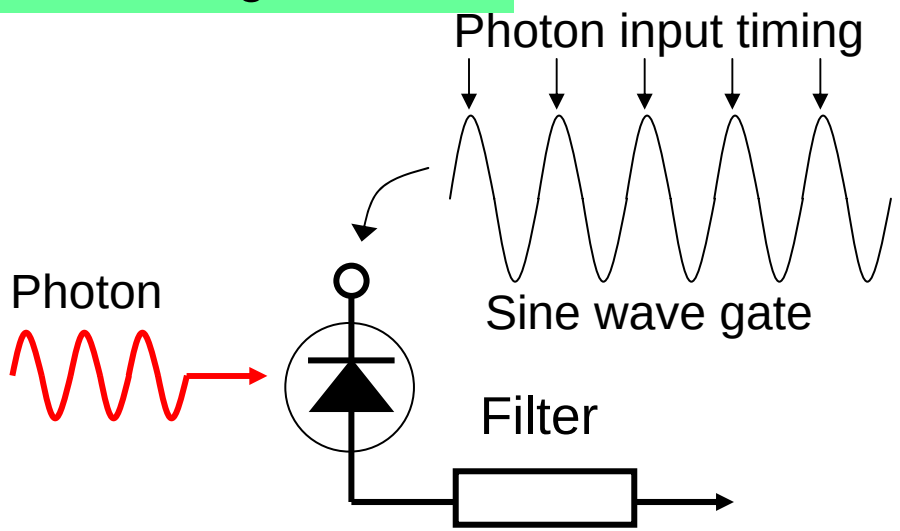
InGaAs/InP APD with sine-wave gating

Up-conversion detector : fragile optical components
SSPD: cryogenic environment

→ Very expensive!

Semiconductor-based detector is desirable for low-cost QKD systems.

Sine-wave gated APD

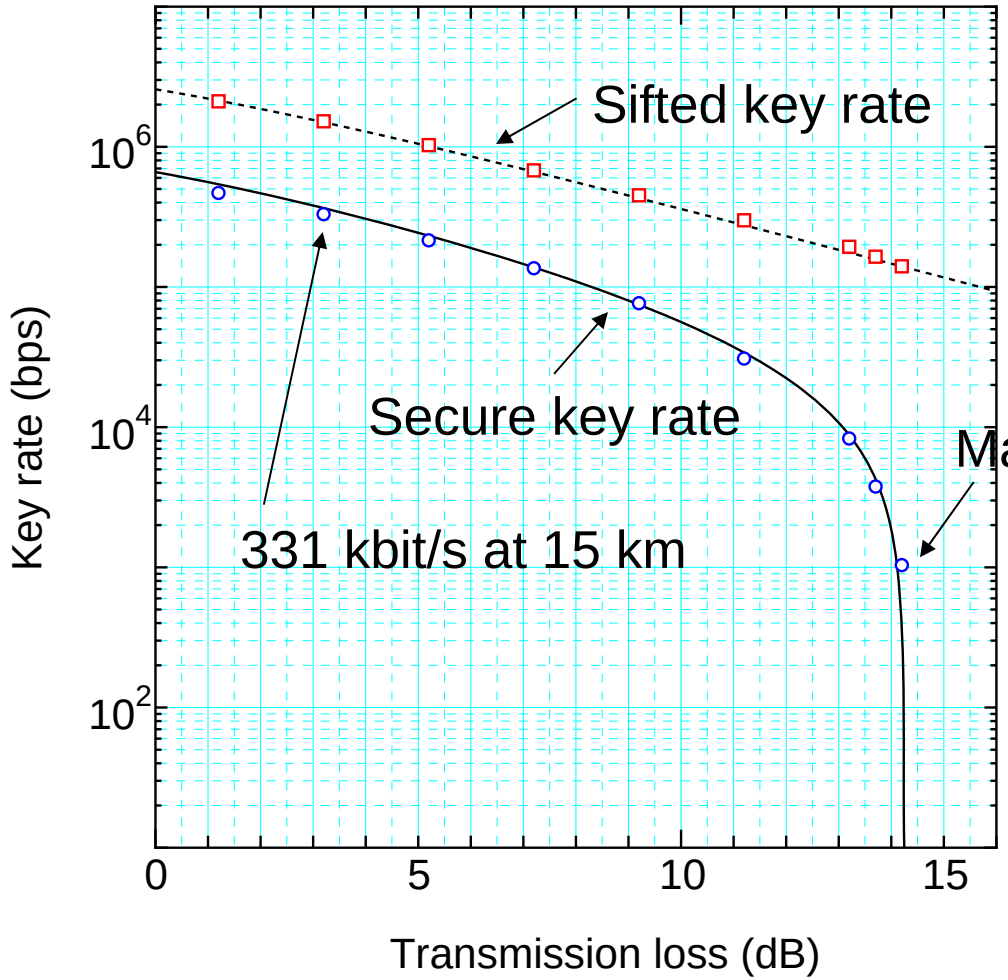


Gate and avalanche are easily distinguished in frequency domain.

Smaller avalanche signal detected.
(resulting in smaller afterpulsing).

500-MHz clock DPS-QKD with sine-wave gated APDs

Deadtime: 200 ns (afterpulsing probability: 2.5%)



N. Namekata et al., Appl. Phys. Lett. 91, 011112 (2007).

Comparison of single photon detectors

	Quantum efficiency	Dark count rate (in Hz)	Maximum clock rate	Cost
Gated mode InGaAs APD	~10 %	~10^4	10 MHz	Low
Up-conversion	< 10 %	350 at QE=0.4%	1 GHz	High
SSPD	~1 %	~10	10 GHz	High
Sine-wave gated InGaAs APD	~10 %	~10^4	1 GHz	Low

Green: fair, red: poor, others: moderate

Summary

DPS-QKD protocol:

Easy implementation, suitable for high-clock rate system, PNS secure

Experiments with various high-speed single photon detectors

Up-conversion, SSPD, Sine-wave gating APD

200 km key distribution (distance record)

2 Mbit/s sifted key at 10 km (bit rate racord)

Future works

Security proof

Development of high-speed electronics

Quantum repeater

Development as a real system

Open issues related to DPS-QKD

1. Unconditional security is not proven yet.
→ Theorists are now preparing the first proof.

2. High-speed electronics designed for QKD.

3. Further increase of key distribution distance.
→ “quantum repeaters” using quantum entanglement.