양자 키 분배 실험의 발전 과정과 최근 동향

2003 KAIST-KIAS Workshop on
Quantum Information Science
(2003.8.21-2003.8.22)

한국전자통신연구원
반도체 · 원천기술연구소
기초기술연구본부

홍 종 철

Quantum Cryptographic Steps - Quantum

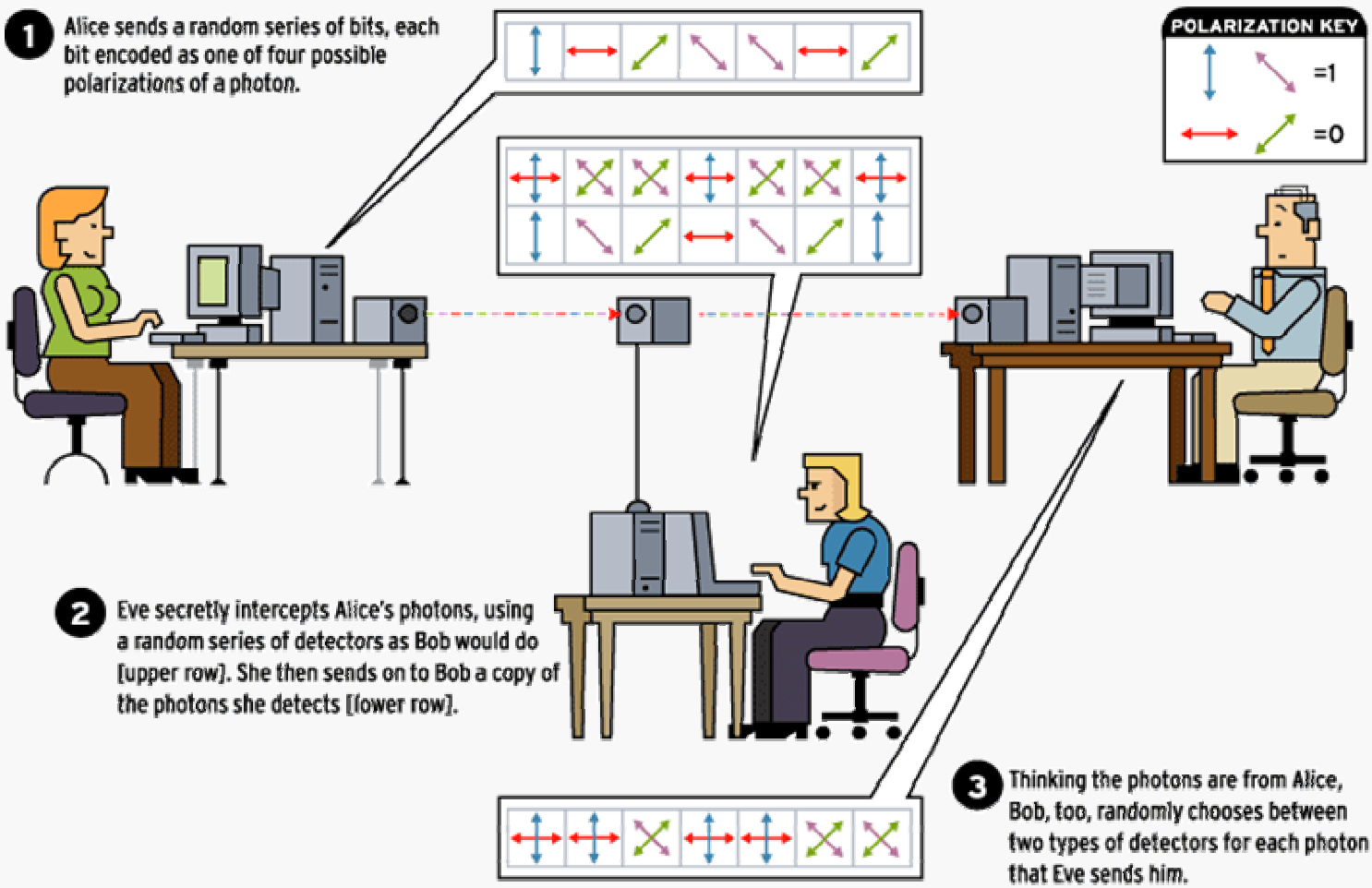
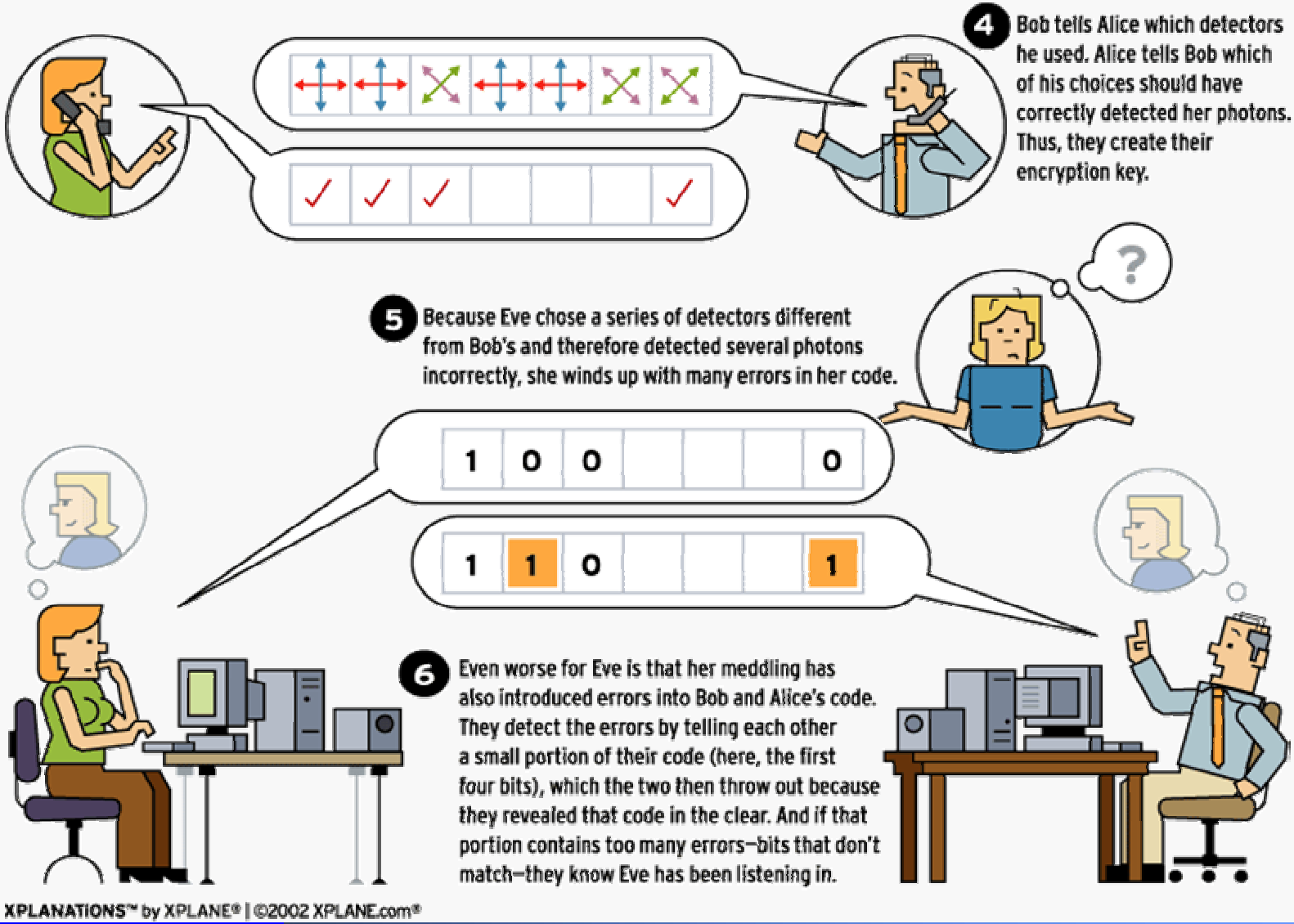


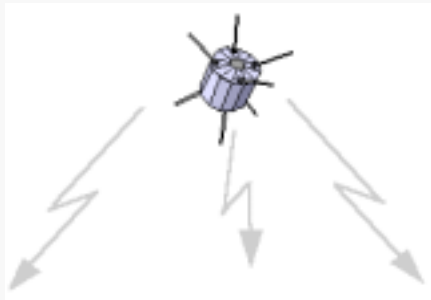
Illustration from **http://www.spectrum.ieee.org/WEBONLY/publicfeature/may02/codef1.html**

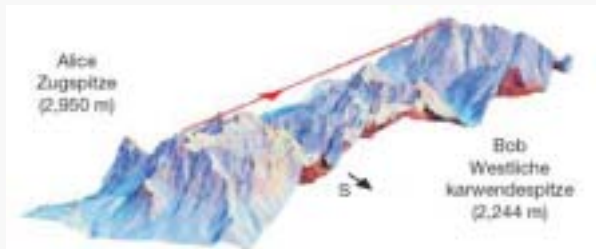
Quantum Cryptographic Steps - Classical

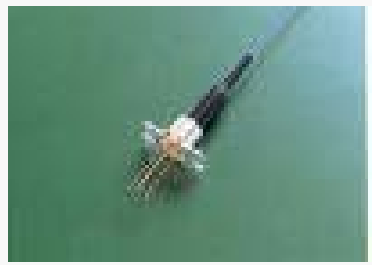


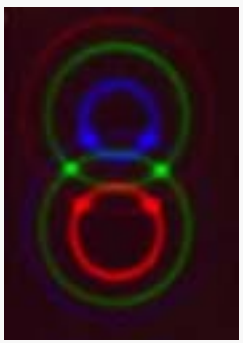
The Quantum Step Components

Coding



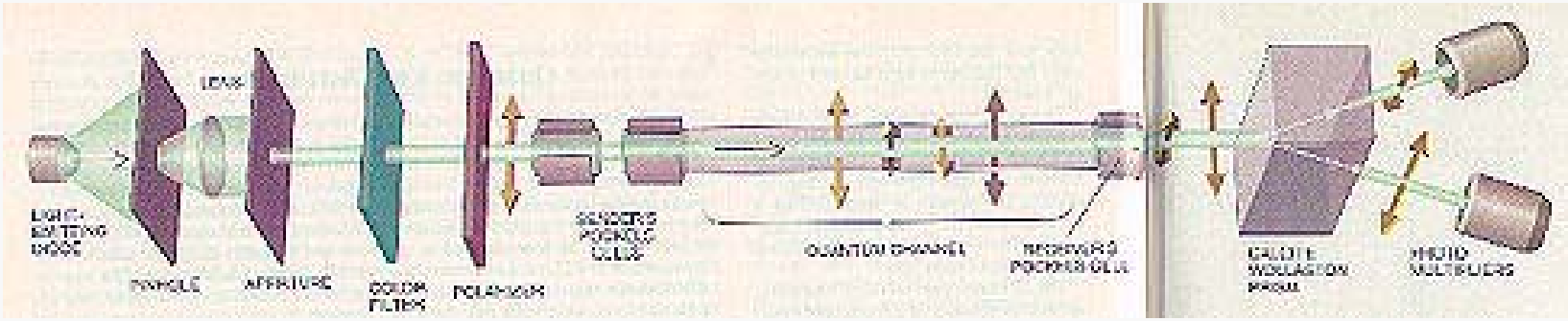






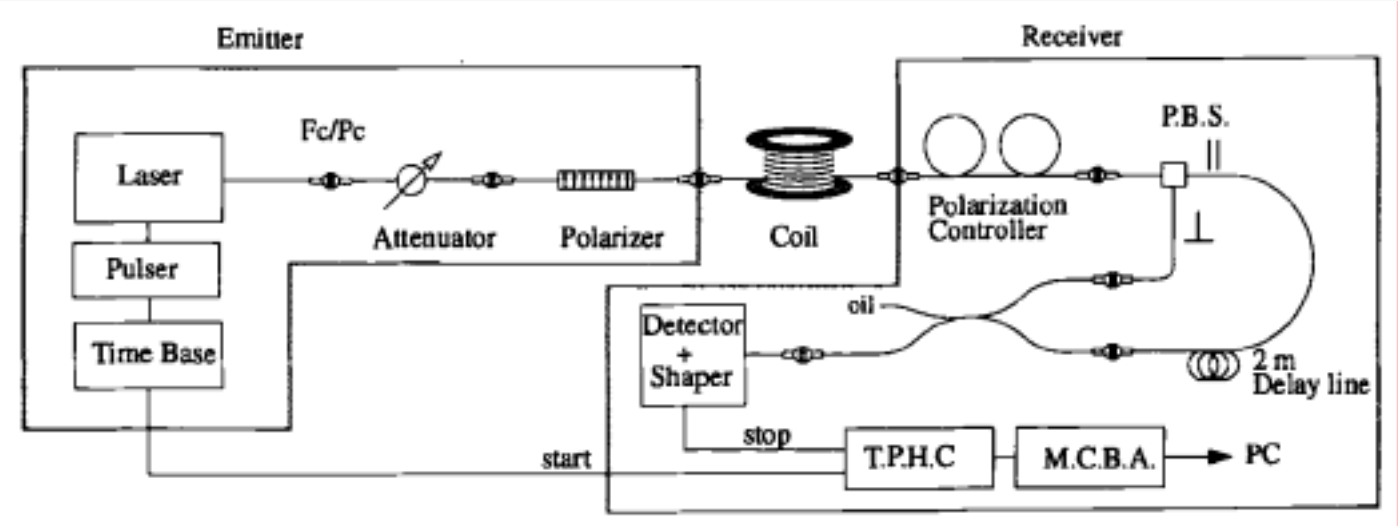
Source — Channel — Detector

The First Experiment



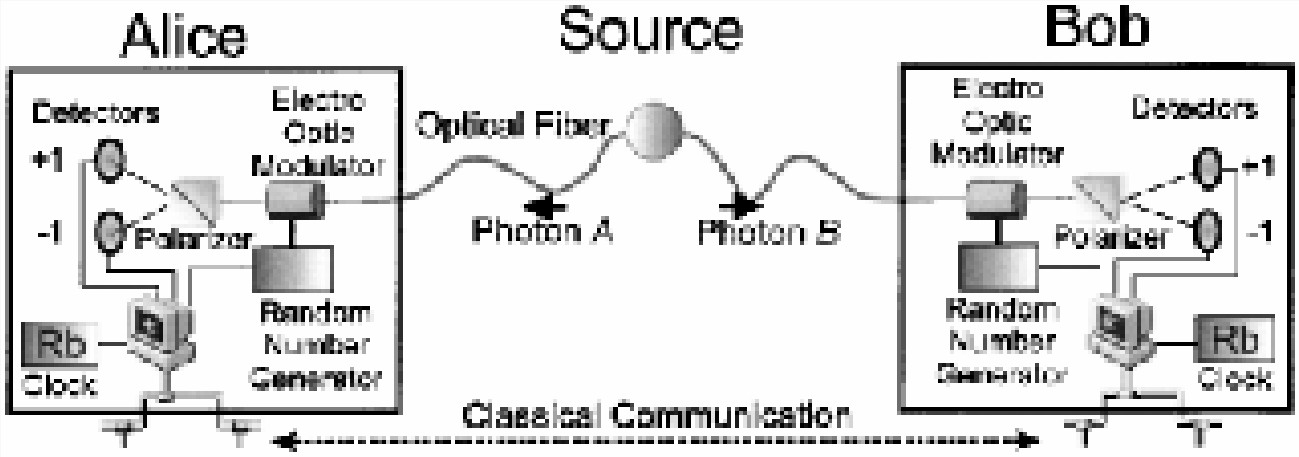
- "Experimental quantum cryptography" , Bennett, et.al. J. Cryptography 5, 3-28 (1992)
  - Green light emitting diode (incoherent source with pinhole)
  - 32 cm free air channel
  - 9% quantum efficiency photomultiplier

Polarization Coding QKD via Optical Fiber



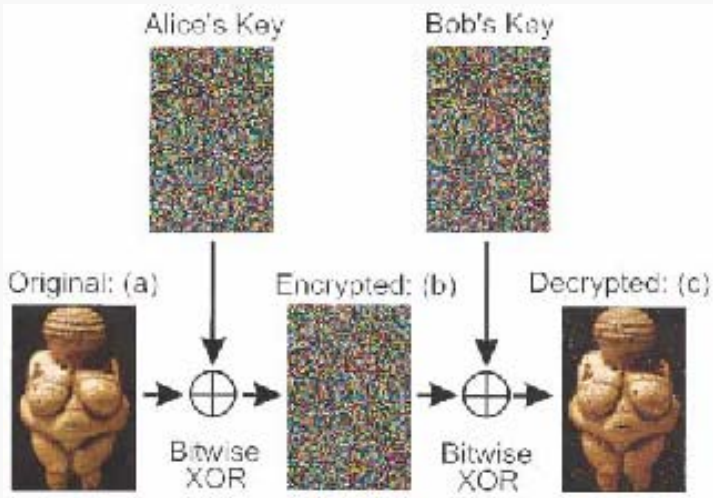
- "Quantum cryptography with polarization photons in optical fibres" , Brequet, et.al. J. Mod. Opt. 41, 2405-2412 (1994)
  - 800nm wavelength, {300m, 1100m} optical fiber channel
  - Si APD(RCA SPCM-100), quantum detection efficiency : 40%
  - Quantum bit rate : order of KHz, error rate : {0.35%,0.54%}

Ekert Protocol via Optical Fiber - I



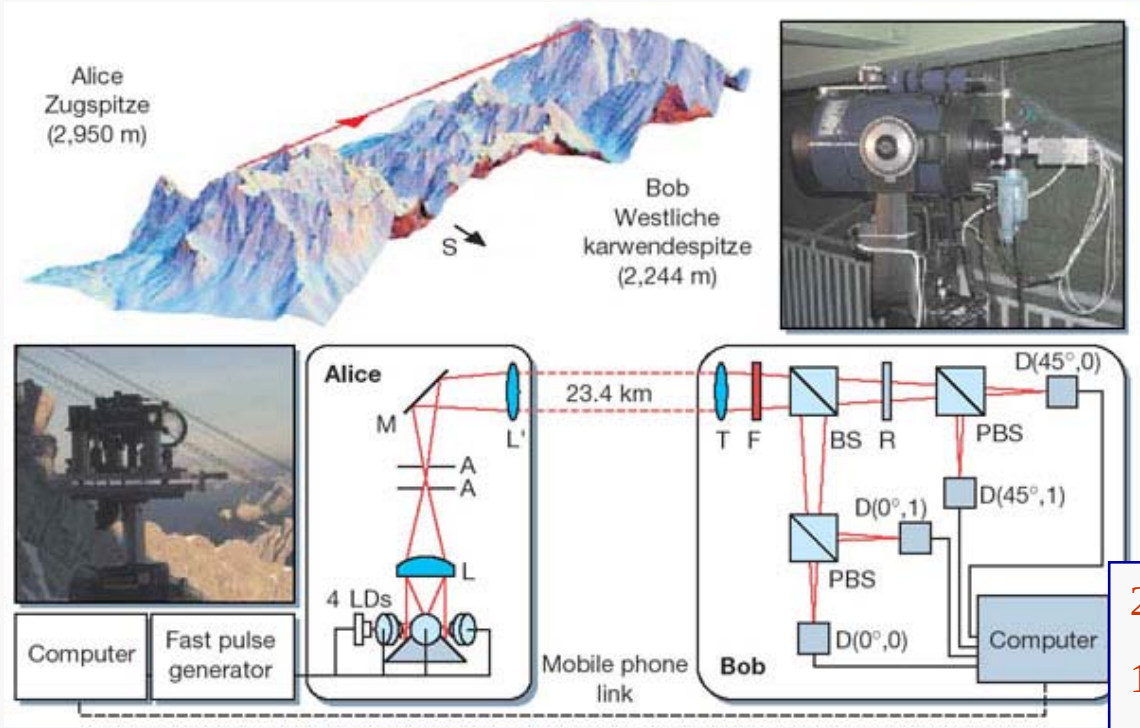
- "Qautnum cryptography with entangled photons" , Jennewein, et.al. Phys. Rev. Lett. 84, 4729-4732 (2000)
  - Type II parametric down conversion using β-barium borate (BBO)
  - Argon-ion laser (351nm) , 350mW
  - 702nm wavelength, 500m long optical fiber channel
  - Si APD

Ekert Protocol via Optical Fiber - II



- Total coincidence rate ~ 1700 s^{-1}
- Singles rate ~ 35000 s^{-1}
- Quantum detection efficiency : 5%
- pair production rate : 7 x 10^5 s^{-1}
- Coincidence window : 4ns
- Establish 2162 bits raw keys
- Bit rate : 420 bit/s
- Quantum bit error rate : 3.4 %

Free Space QKD



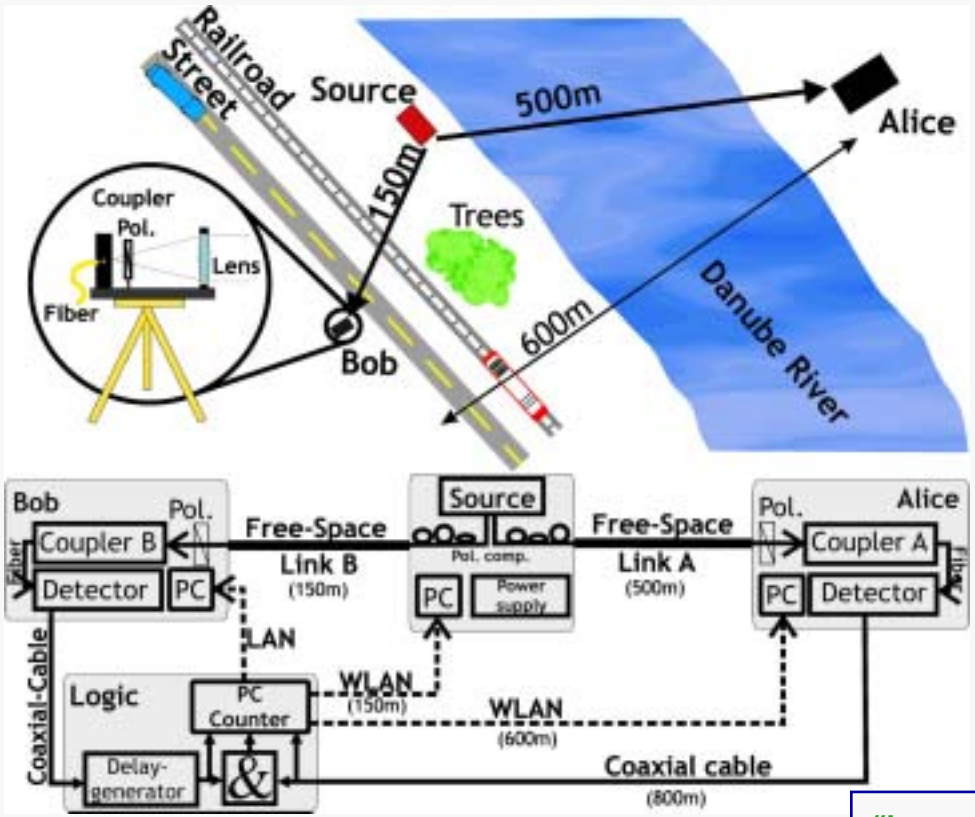
23.4 km free space channel

18-20 dB optical loss

1.5-2 Kbit/s

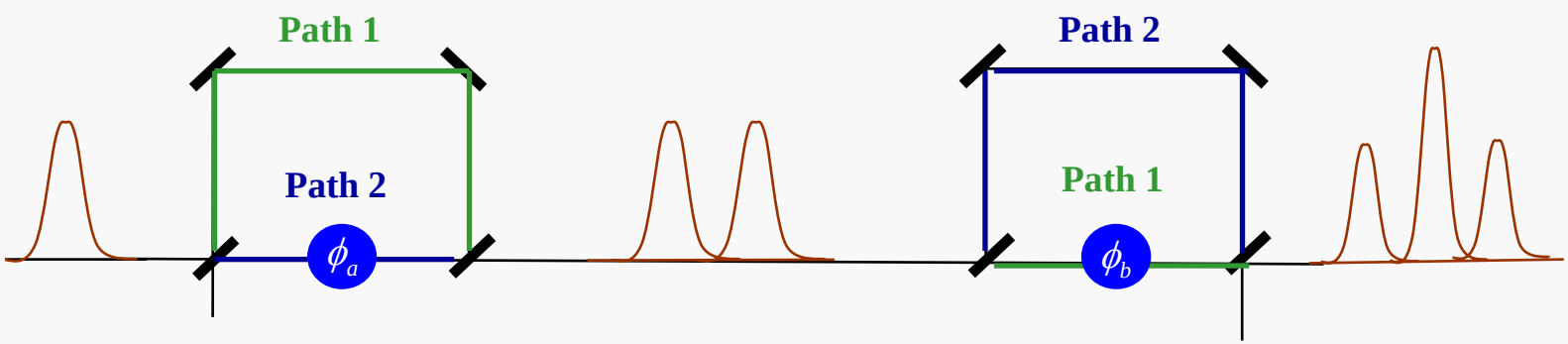
"A step towards global key distribution", Kurtsiefer, et.al. nature 419, 450 (2002)

Free Space Entanglement Distribution



"Long-distance free-space distribution of quantum entanglement" , Zeilinger, et.al. science 301, 621-623 (2003)

New Coding Scheme – Phase Coding



$$e^{i\phi_a}e^{i\phi_b}\left|S,0\right\rangle + ie^{i\phi_a}e^{i\phi_b}\left|S,1\right\rangle + \left|L,0\right\rangle - i\left|L,1\right\rangle$$
$$-\left(e^{i\phi_a}+e^{i\phi_b}\right)\left|C,0\right\rangle + i\left(e^{i\phi_a}-e^{i\phi_b}\right)\left|C,1\right\rangle$$

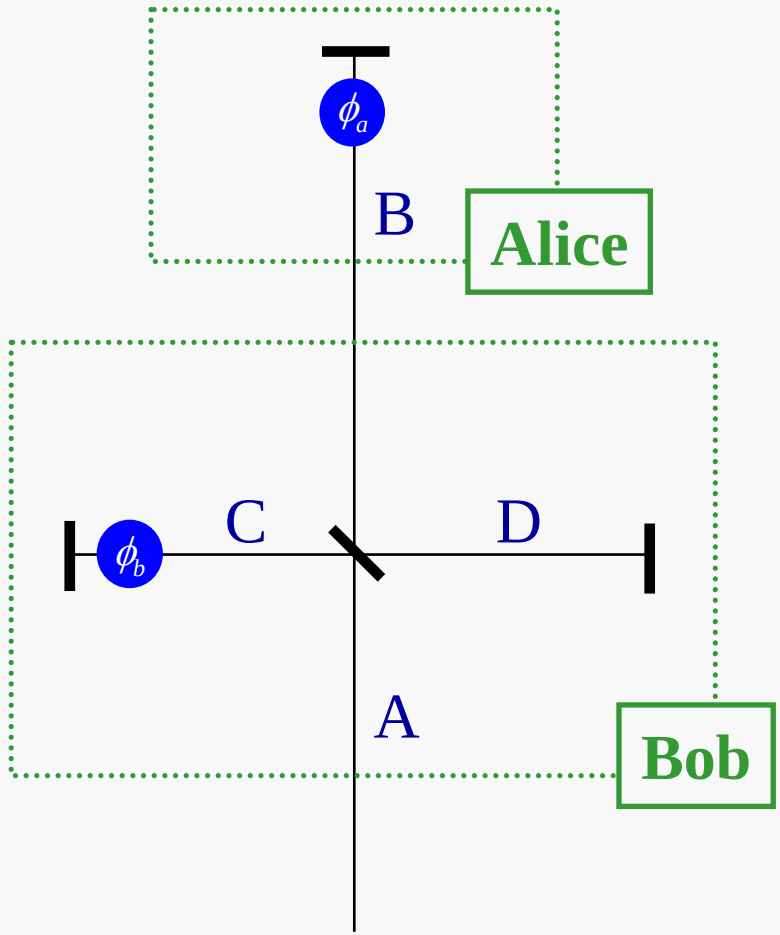
Double Mach-Zehnder Interferometry

QKD with Phase Coding via Optical Fiber

- 0.3 dB/km fiber attenuation
- Typical travel time : 225 μm
- 5ns separation between the different path
- 100kHz laser pulse rate
- Bit error rate (BER) ~ 9.3 %
- 10 Hz key generation rate

- "Quantum key distribution over a 48km optical fibre network" , R.J. Hughes, et.al. J. Mod. Opt. 47, 533-547 (2000)
  - 1300nm wavelength
  - InGaAs APD (efficiency : 10-40%, Dark count : 10-100kHz)
  - $\Delta T \gg T_{coh}$ (the difference between travel time is much higher than the coherence time)

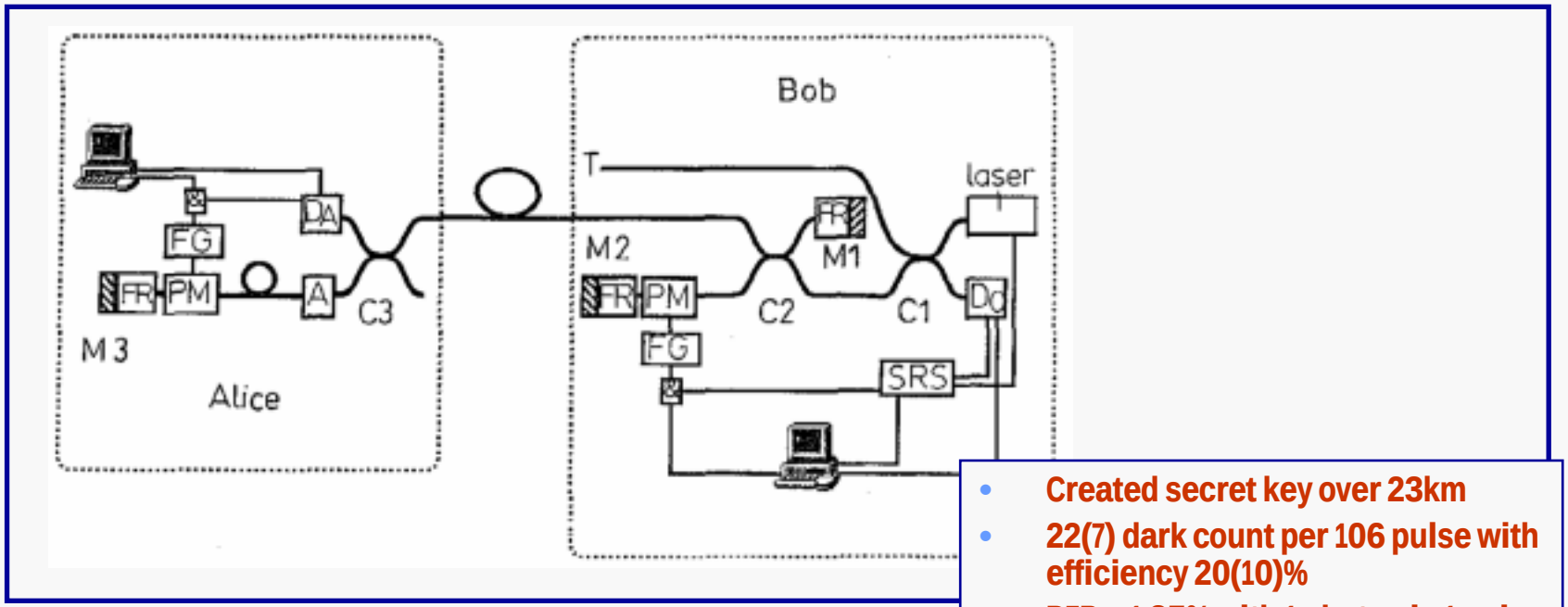
Phase Coding Using Michelson Interferometry



- Interfering paths
  - A → C → C → D → D → B → B → A
  - A → B → B → D → D → C → C → A

Plug & Play System

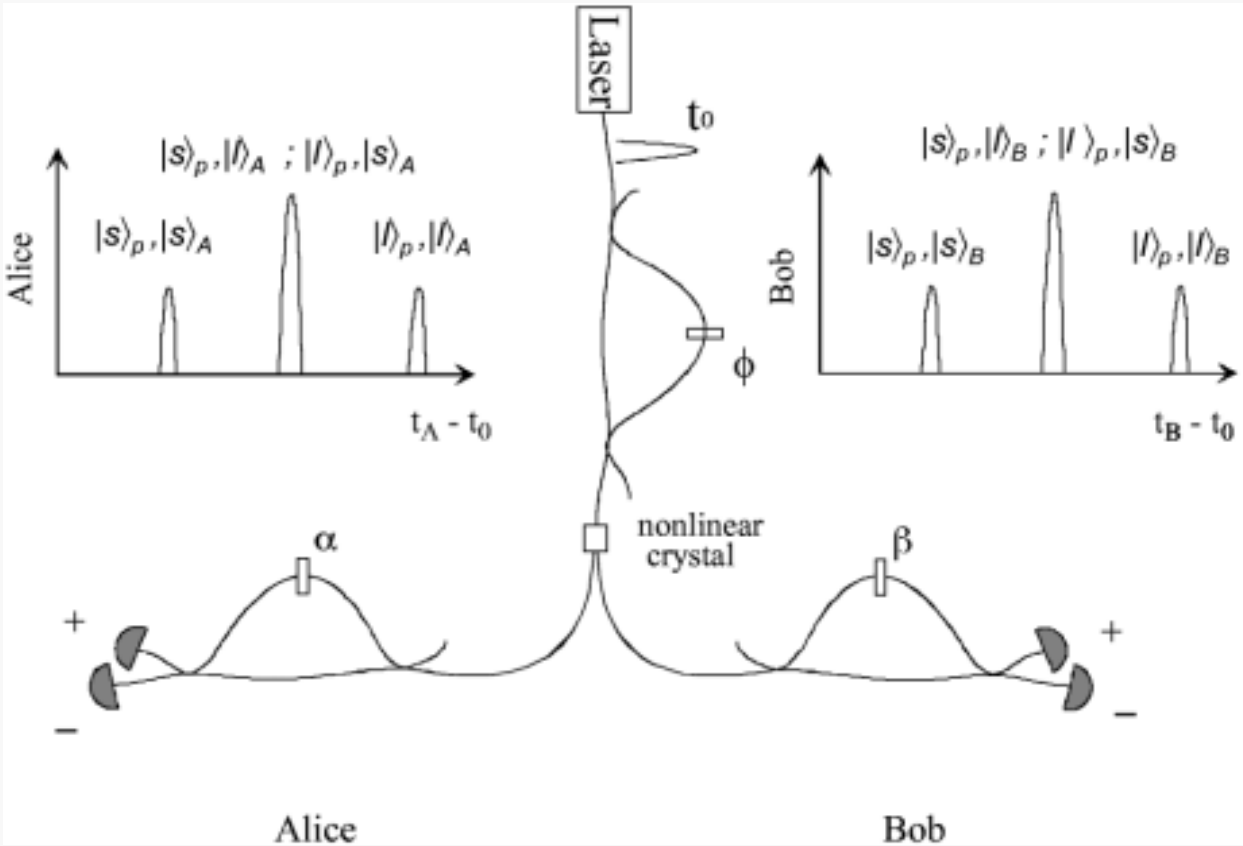
Demonstration of PNP System



- Created secret key over 23km
- 22(7) dark count per 106 pulse with efficiency 20(10)%
- BER = 1.35% with 1 photon in 1 pulse

- "Interferometry with Faraday mirrors for quantum cryptography" , H. Zbinden, et.al. Electron. Lett. 33, 586-588 (1997)
  - LN_2 Cooled Ge APD
  - Faraday mirror : compensate the birefringence of fiber
  - Bob : PZT phase modulator (Modulation freq. ~ 10kHz)
  - Alice : 4GHz $LiNbO_3$ waveguide phase modulator

QKD Using Energy-Time Entanglement - I



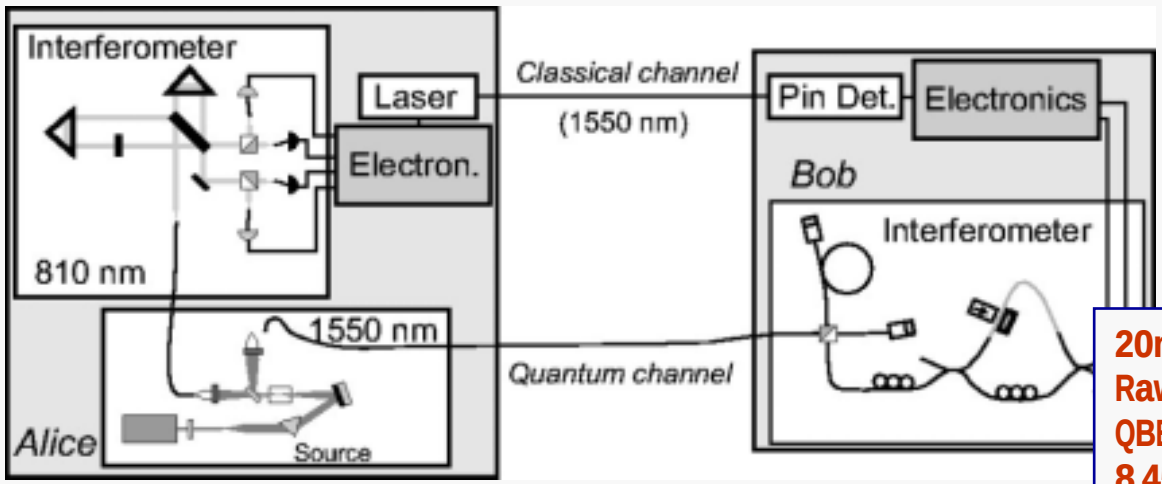
"Quantum cryptography using entangled photons in energy-time Bell state" ,
W. Tittel, et.al. Phys. Rev. Lett. 84, 4737-4740 (1999)

QKD Using Energy-Time Entanglement - II

	++	+-	-+	--
$s_p s_a, s_p s_b$	278±6	197 ±5	187 ±5	147 ±4
$l_p l_a, l_p l_b$	304 ±7	201 ±5	200 ±5	148 ±5
$s_p s_a, l_p l_b$	11 ±0.8	10.4 ±0.8	9.2 ±0.7	9.4 ±0.7
$l_p l_a, s_p s_b$	11.2 ±0.4	8.6 ±0.4	9.1 ±0.4	8.5 ±0.4
QBER (%)	3.7 ±0.2	4.6 ±0.2	4.5 ±0.2	5.7 ±0.3

	++	+-	-+	--
Visibility (%)	92.5±1.8	92.6 ±1.4	89.3 ±1.9	94.5 ±1.6
Max.	518 ±13	416 ±8	359 ±9	279 ±7
Min.	20 ±5	16 ±3	20 ±4	8 ±2
QBER (%)	3.7 ±0.9	3.7 ±0.7	5.3 ±1	2.8 ±0.8

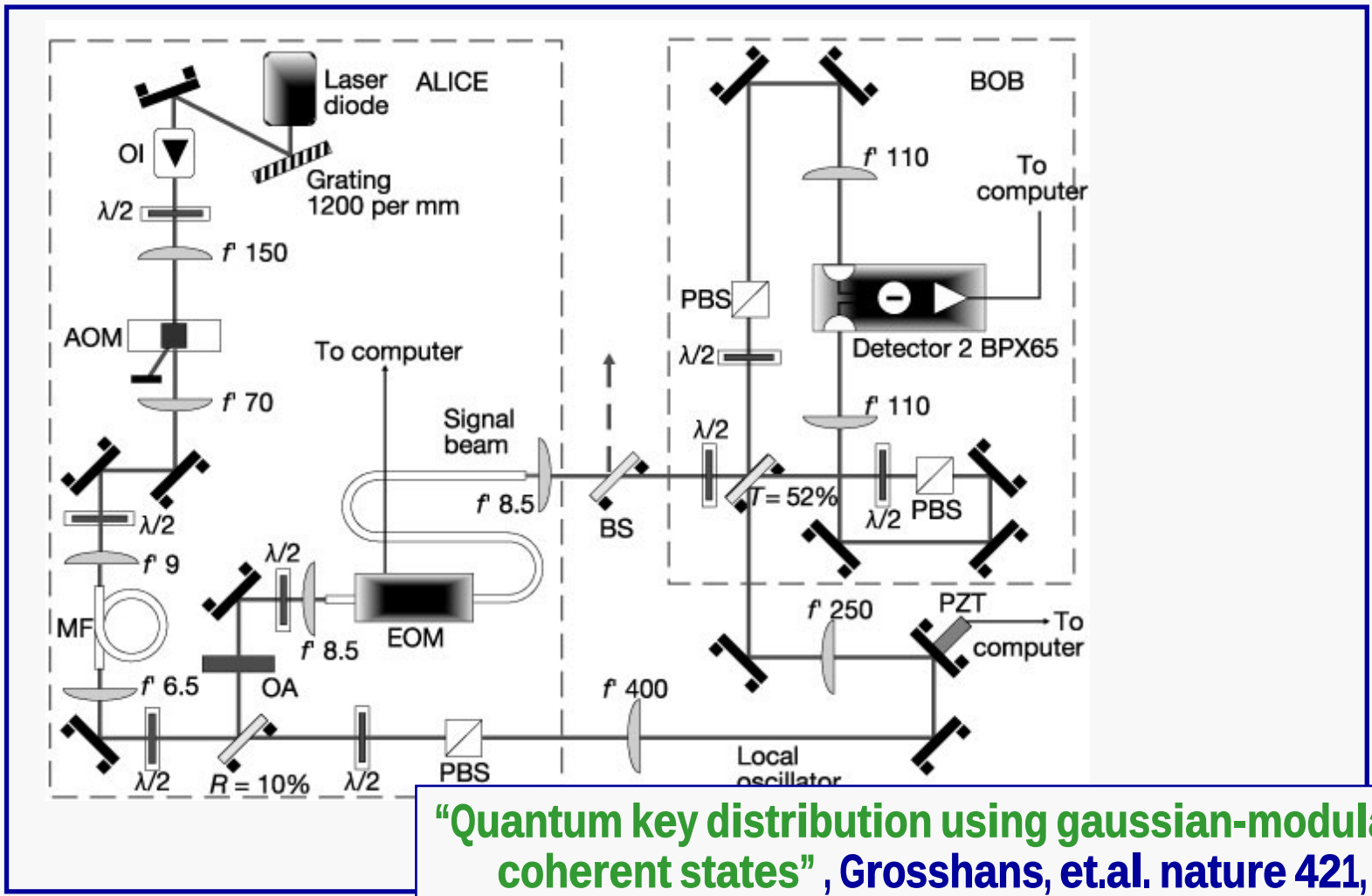
Phase Coding Experiments with Entangled Photons



20m distance
Raw key distribution rate : 450Hz
QBER : 4.7%±0.3%
8.45km distance
Raw key distribution rate : 134Hz
QBER : 6.6%±0.6%

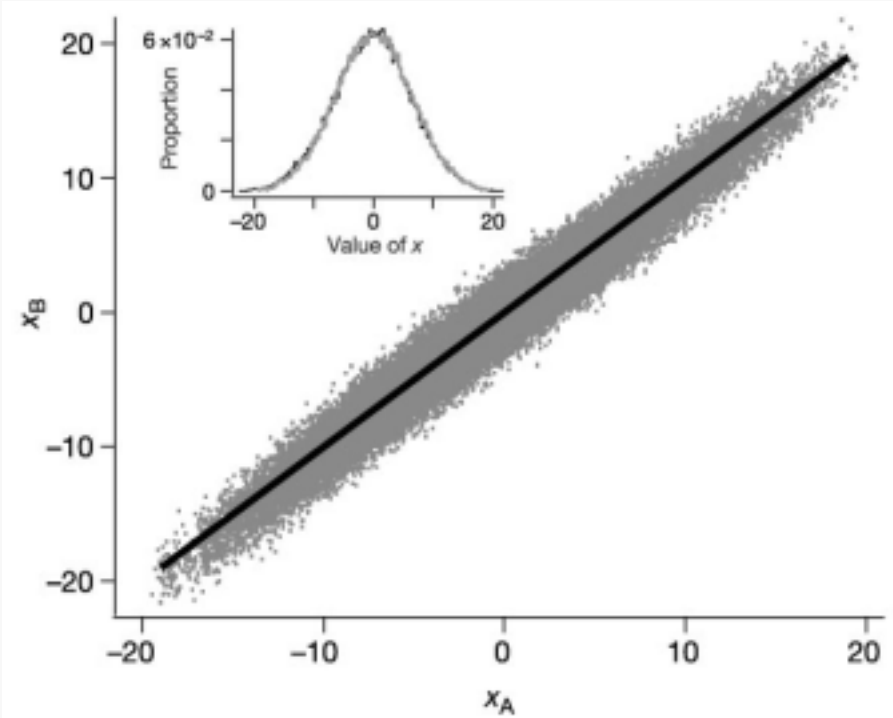
"Long-distance entanglement-based quantum key distribution" , G. Ribordy, et.al. Phys. Rev. A 63, 012309 (2001)

Continuous Variable QKD - I



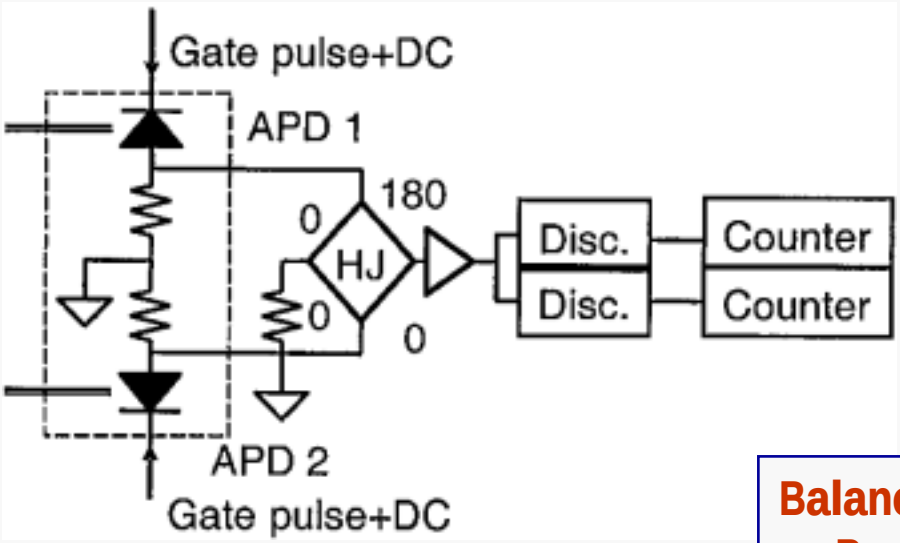
"Quantum key distribution using gaussian-modulated coherent states" , Grosshans, et.al. nature 421, 238-241 (2003)

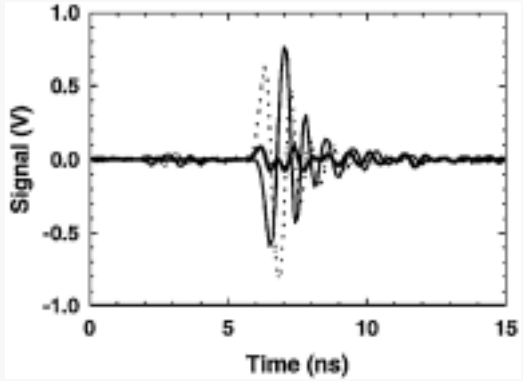
Continuous Variable QKD - II



1690 bps at 1dB channel loss

QKD over 100km - I

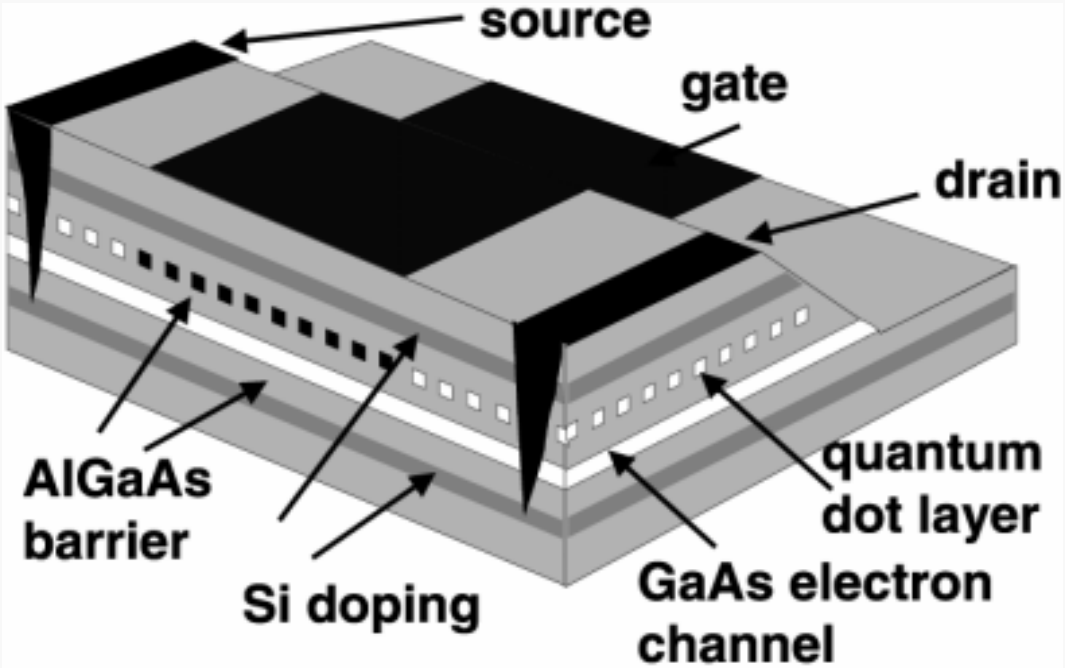


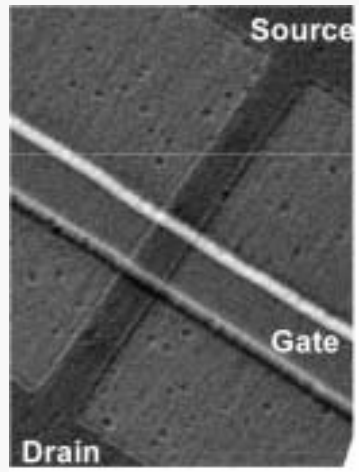


Balanced Gated Mode APD & PNP System
→ Reduce the transient spikes
→ Reduce the quantum threshold

"Single photon interference experiment over 100km for quantum cryptography system using a balanced gated-mode photon detector" , H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, quant-ph/0306066 (2003)

QKD over 100km - II





Reported by Shields, et.al. (Toshiba Research Europe) at CLEO 2003 (Baltimore, US)

Improving single photon detector other than APD : "Detection of single photons using a field effect transistor with a layer of quantum dots", Kardynal, et.al. Meas. Sci. Technol. 13, 1721-1726 (2002)

Error Sources in QKD Experiments

- **Source error**
  - Multi-photon pulse
- **Detector error**
  - Dark count
  - Gate spikes
  - After pulse
- **Channel error**
  - Dispersion
  - Back scattering
  - Polarization rotation & dispersion
  - Attenuation

Conclusion & ETRI Experiment Plan

- Current State
  - Several Hz key rate via 100km length optical fiber channel
  - Several kHz key rate via 23.4km length free space line of sight link
  - Proposing satellite key distribution
- ETRI Experiment Plan
  - Achieve a few kHz raw key distribution via a few 10 km optical fiber channel within 3 years
  - Develop new QKD protocol
  - Improve photon detector

Literatures - I

- Polarization coding experiments
  - “Experimental quantum cryptography” , Bennett, Bessette, et.al. (1992), J. Cryptology, 5, 3-28
  - “Experimental Demonstration of quantum cryptography using polarized photons in optical fiber over more than 1km” , Muller, Breguet, and Gisin (1993), Europhys. Lett. 23, 383-388
  - “Quantum cryptography with polarized photons in optical fibers” , Brequet, Muller, and Gisin (1994), J. Mod. Opt. 41, 2405-2412
  - “Quantum cryptography with entangled photons” , Jennewein, Simon, Weihs, Weinfurterm and Zeilinger (2000), Phys.Rev.Lett. 84, 4729-4732
  - “Entangled state quantum cryptography : eavesdropping on the Ekert protocol” , Naik, Peterson, White, Berglund, and Kwiat (2000), Phys.Rev.Lett. 84, 4733-4736
- Double Mach-zehnder implementation (phase coding) - I
  - “Single photon interference in 10km long optical fiber interferometer” , P.D. Townsend, J.G. Rarity, and P.R. Tapster, Electron. Lett. 29, 634–639 (1993a)

Literatures - II

- Double Mach-zehnder implementation (phase coding) – II
  - “Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel” , P.D. Townsend, J.G. Rarity, and P.R. Tapster, Electron. Lett. 29, 1291–1293 (1993b)
  - “Quantum key distribution over distances as long as 30 km” , C. Marand, and P.D. Townsend, Opt. Lett. 20, 1695–1697 (1995)
  - “Quantum cryptography on optical fiber networks” , P.D. Townsend, Opt. Fiber Technol. 4, 345–370 (1998b)
  - “Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using WDM” , P.D. Townsend, Electron. Lett. 33, 188–190 (1997a)
  - “in Advances in Cryptology—CRYPTO ’96 Proceedings” , R. Hughes, G.G. Luther, G.L. Morgan, and C. Simmons, Lecture Notes in Computer Science 1109, edited by N. Koblitz (Springer, New York), pp. 329–342 (1996)
  - “Quantum key distribution over a 48-km optical fiber network” , R. Hughes, G. Morgan, and C. Peterson, J. Mod. Opt. 47, 533–547 (2000)

Literatures - III

- Energy-time entanglement coding
  - “Bell inequality for position and time” , J.D. Franson , Phys.Rev.Lett. 62, 2205-2208 (1989)
  - “Long-distance entanglement-based quantum key distribution” , G. Ribordy, J. Brendel, J.D. Gautier, N. Gisin, and H. Zbinden, Phys.Rev.A 63, 012309 (2001)
  - “Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication” , J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys.Rev.Lett. 82, 2594-2597 (1999)
  - “Quantum cryptography using entangled photons in energy-time Bell state” , W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. 84, 4737-4740 (2000)
- Plug & Play systems - I
  - “A universal compensator for polarization changes induced by birefringence on a retracing beam” , M. Martinelli, Opt. Commun. 72, 341–344 (1989)
  - “Time reversal for the polarization state in optical systems” , M. Martinelli, J. Mod. Opt. 39, 451–455 (1992)

Literatures - IV

- Plug & Play systems - II
  - "'Plug and play' systems for quantum cryptography" , A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. 70, 793–795 (1997)
  - "Interferometry with Faraday mirrors for quantum cryptography" , H. Zbinden, J.-D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Electron. Lett. 33, 586–588 (1997)
  - "Fast and user-friendly quantum key distribution" , G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, J. Mod. Opt. 47, 517–531 (2000)
  - "An autocompensating fiberoptic quantum cryptography system based on polarization splitting of light" , D. Bethune, and W. Risk, IEEE J. Quantum Electron. 36, 340–347 (2000)
  - "Experiments on long wavelength (1550 nm) 'plug and play' quantum cryptography system " , M.F. Bourennane, Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, Opt. Express 4, 383–387 (1999)
  - "Single photon interference experiment over 100km for quantum cryptography system using a balanced gated-mode photon detector" , H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, quant-ph/0306066 (2003)

Literatures - V

- Plug & play systems – II
  - “Experimental long wavelength quantum cryptography: from single photon transmission to key extraction protocols “ , M.F. Bourennane, D. Ljunggren, A. Karlsson, P. Jonsson, A. Hening, and J. P. Ciscar, J. Mod. Opt. 47, 563–579 (2000)
  - “Single photon interference experiment over 100km for quantum cryptography system using a balanced gated-mode photon detector” , H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, quant-ph/0306066 (2003)
- Frequency coding – I
  - “Long-distance frequency-division interferometer for communication and quantum cryptography” , P.C. Sun, Y. Mazurenko, and Y. Fainman, Opt. Lett. 20, 1062–1063 (1995)
  - “Spectral coding for secure optical communications using refractive index dispersion” , Y. Mazurenko, R. Giust, and J. P. Goedgebuer, Opt. Commun. 133, 87–92 (1997)
  - “Single-photon interference in sidebands of phase-modulated light for quantum cryptography” , J.-M. Merolla, J-M., Y. Mazurenko, J. P. Goedgebuer, and W. T. Rhodes, Phys. Rev. Lett. 82, 1656–1659 (1999)

Literatures - VI

- Frequency coding – II
  - “Quantum cryptography based on photon ‘frequency’ states: example of a possible realization” , S.N. Molotkov, Sov. Phys. JETP 87, 288–293 (1998)
- Free space channel - I
  - “Quantum cryptography in free space” , B. Jacobs, and J. Franson, Opt. Lett. 21, 1854–1856 (1996)
  - “Practical free-space quantum key distribution over 1 km” , W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C. Simmons, Phys. Rev. Lett. 81, 3283–3286 (1998)
  - “Free-space quantum key distribution in daylight” , R. Hughes, W. Buttler, P. Kwiat, S. Lamoreaux, G. Morgan, J. Nordhold, and G. Peterson, J. Mod. Opt. 47, 549–562 (2000)
  - “Daylight quantum key distribution over 1.6 km” , W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, Phys. Rev. Lett. 84, 5652–5655 (2000)

Literatures - VII

- Free space channel - II
  - “Secure free-space key exchange to 1.9 km and beyond” , P.M. Gorman, P.R. Tapster, and J.G. Rarity, J. Mod. Opt. 48, 1887–1901 (2001)
  - “A step towards global key distribution” , C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, J. G. Rarity, nature 419, 450 (2002)
- Continuous variable QKD - I
  - “Cloning and cryptography with quantum continuous variables” , N.J. Cerf, S. Iblisdir, and G. Van Assche, Eur. Phys. J. D 18, 211-218 (2002)
  - “ContinuousVariable Quantum Cryptography: Beating the 3 dB Loss Limit” , Ch. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, Phys. Rev. Lett. 89, 167901 (2002)
  - “Continuous Variable Quantum Cryptography Using Coherent States” , Frédéric Grosshans and Philippe Grangier, Phys. Rev. Lett. 88, 057902 (2002)

Literatures - VIII

- Continuous variable QKD – II
  - “Continuous variable quantum cryptography” , T. C. Ralph, Phys. Rev. A 61, 010303 (1999)
  - “Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations” , M. D. Reid, Phys. Rev. A 62, 062308 (200)
  - “Quantum cryptography with squeezed states” , Mark Hillery, Phys. Rev. A 61, 022309 (2000)
  - “Quantum distribution of Gaussian keys using squeezed states” , N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A 63, 052311 (2001)
  - “Quantum key distribution using gaussian-modulated coherent states” , Frederic Grosshans, Gilles Van Assche, Jerome Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier, nature 421, 238-241 (2003)
  - “Quantum Key Distribution with Bright Entangled Beams” , Ch. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. 88, 167902 (2002)
  - “Quantum key distribution with continuous variables” , K. Bencheikh,, T.H. Symull, A. Jankovic, and J. A. Levenson, J. Mod. Opt. 48, 1903-1920 (2001)

Literatures - IX

- Continuous variable QKD – III
  - “Reconciliation of a Quantum-Distributed Gaussian Key” , Gilles Van Assche, Jean Cardinal and Nicolas J. Cerf, cs.CR/0107030 (2002)
  - “Reverse reconciliation protocols for quantum cryptography with continuous variables” , Frederic Grosshans and Philippe Grangier, quant-ph/0204127 (2002)
  - “Secure quantum key distribution using squeezed states” , Daniel Gottesman and John Preskill, Phys. Rev. A 63, 022309 (2001)
  - “Security of continuous-variable quantum cryptography” , T. C. Ralph, Phys. Rev. A 62, 062306 (2000)