Hughes R. J., et al. 2002. Practical free-space quantum key distibution over 10 km in daylight and at night. New Journal of Physics 4: 43.1-43.14

Kylstra, N. 2001. Introduction to Quantum Optics. (ps file) http://massey.dur.ac.uk/njk/qoptics.html.

Lomonaco, S. J. Jr. 1998. A Quick Glance at Quantum Cryptography. (pdf file). eprint http:xxx.lan.gov/abs/quant-ph/98105.

Lomonaco, S. J. Jr. 1999. A Talk on Quantum Cryptography or How Alice Outwits Eve. Coding Theory and Cryptography: From Geheimscheimschreiber and Enigma to Quantum Theory. n.p.

Rafaat, T., W. Luck and R. De Young. 1999. Temperature control of avalanche photodiodes using thermo-electric coolers. (pdf file). NASA Technical Memorandum 209689.

Rarity, J G, P R Tapster, P M Gorman and P Knight. 2002. Ground to satellite secure key exchange using quantum cryptography. New Journal of Physics 4: 82.1-82.21

Ch. Kurtsiefer, P.Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, and J.G. Rarity: A step towards global key distribution. *Nature* ***419****, 450 (2002).*

Berman, Doolean, Mainieri, Tsifrinovich, "Introduction to Quantum Computers", World Scientific, 1998

Silverman, "A Friendly Introduction to Number Theory", Prentice Hall, 1997

Williams, Clearwater, "Exploration in Quantum Computing", Springer, 1997

Stinson, "Cryptography, Theory and Practice", CRC Press, 1995

M. Atatüre, M. Shaw, G. Di Giuseppe, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, A. J. Miller, and S. W. Nam "Experimental Observation of Quantum Interference using Photon-number Resolving Detectors", Physical Review A, (2002).

Mark C. Booth, M. Atatüre, G. Di Giuseppe, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich "Counter-Propagating Entangled Photons from a Waveguide with Periodic Nonlinearity", *Physical Review A*, **66**, 023815 (2002), [eprint quant-ph/0201150].

G. Di Giuseppe, M. Atatüre, M. Shaw, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich "Entangled-Photon Generation from Parametric Down-Conversion in Media with Inhomogeneous Nonlinearity", *Physical Review A*, **66**, 013801 (2002), [eprint quant-ph/0112140].

M. Atatüre, G. Di Giuseppe, M. Shaw, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich "Multiparameter Entanglement in Quantum Interferometry", Submitted to *Physical Review A*, **66**, 023822 (2002), [eprint quant-ph/0111024].

M. Atatüre, G. Di Giuseppe, M. Shaw, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich "Multiparameter Entanglement in Femtosecond Parametric Down Conversion", *Physical Review A*, **65**, 023808 (2002), [eprint quant-ph/0110154].

Z. Walton, A. V. Sergienko, M. Atatüre, B. E. A. Saleh, M. C. Teich "Performance of Photon-Pair Quantum Key Distribution Systems", *Journal of Modern Optics*, **48**, 2055 (2001).

M. Atatüre, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich "Entanglement in Cascaded-Crystal Parametric Down-Conversion", *Physical Review Letters*, **86**, 4013 (2001).

The Outputs of This Research

The outputs of this research are a prototype free space quantum cryptography system and the publications. Our quantum cryptography system can generate the quantum key bit in the rates of ~5k bits/s where the transmitter and the receiver are 6.5m apart. These keys can be used to encode/decode transaction digital data with today classical cryptography system. The publications are listed below.

We are correcting a paper to publish in International Journal. We will inform to the Thailand Research Fund immediately when our paper is accepted.

List of Publications

"Experimental Quantum Cryptography based on the BB84 Protocol"
1st International Symposium on Optical and Quantum Technology 7-8 December 2001, Faculty of Science, KMITL, Bangkok. Page 80-83

"Photon Counting with Passive Quenched Silicon Avalanche"
1st International Symposium on Optical and Quantum Technology, 7-8 December 2001, Faculty of Science, KMITL, Bangkok. Page 129-133

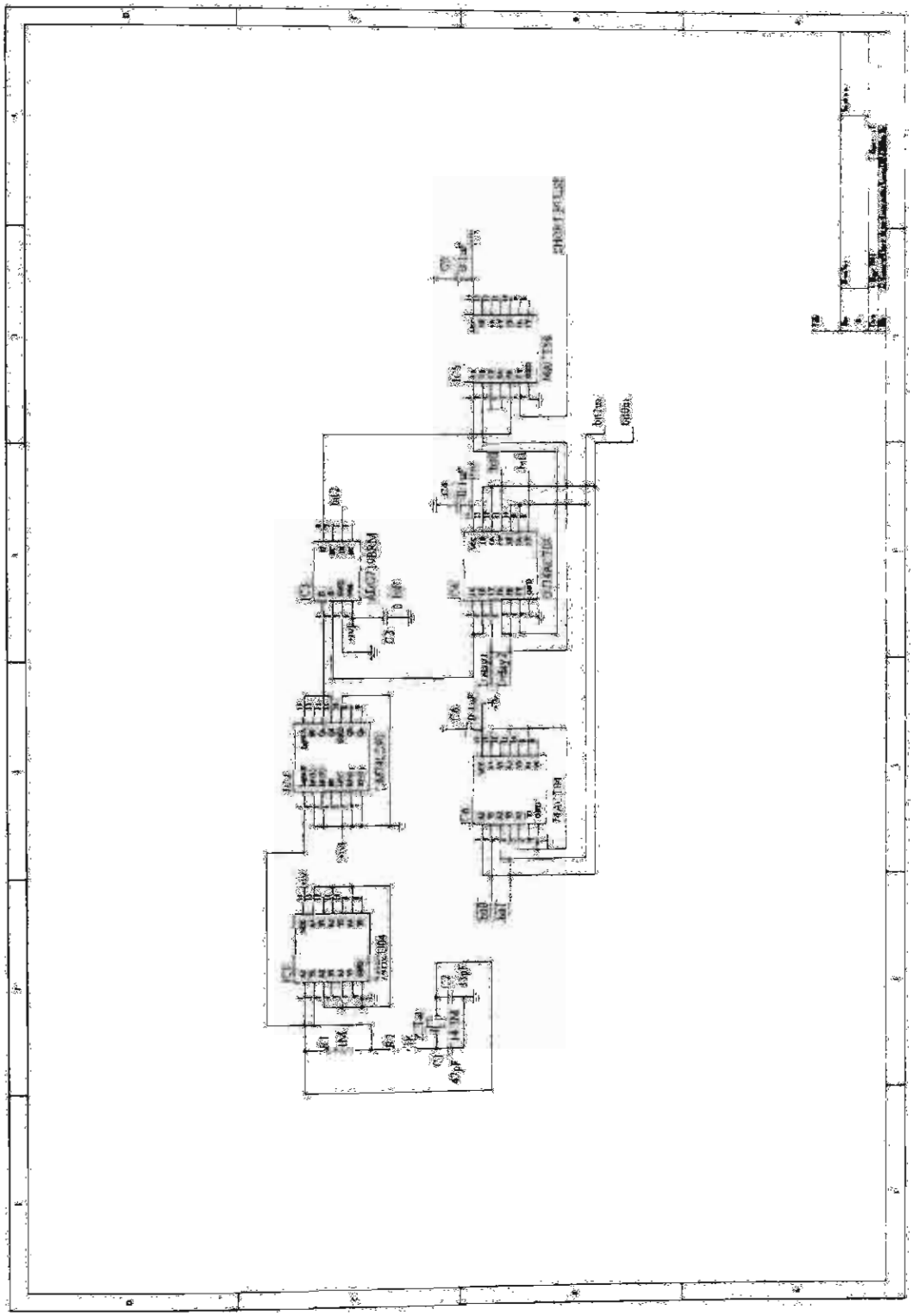
"Experimental Quantum Cryptography Utilized Quantum States of Single Photons"
28th Congress on Science and Technology of Thailand, 24-26 October 2002, Queen Srikit National Convention Center, Bangkok, Page. 220

"Optical Quantum Random Number Generator"
29th Congress on Science and Technology of Thailand, 20-22 October 2003, Golden Jubilee Convention Hall, Khon Khan University, Khon khan.

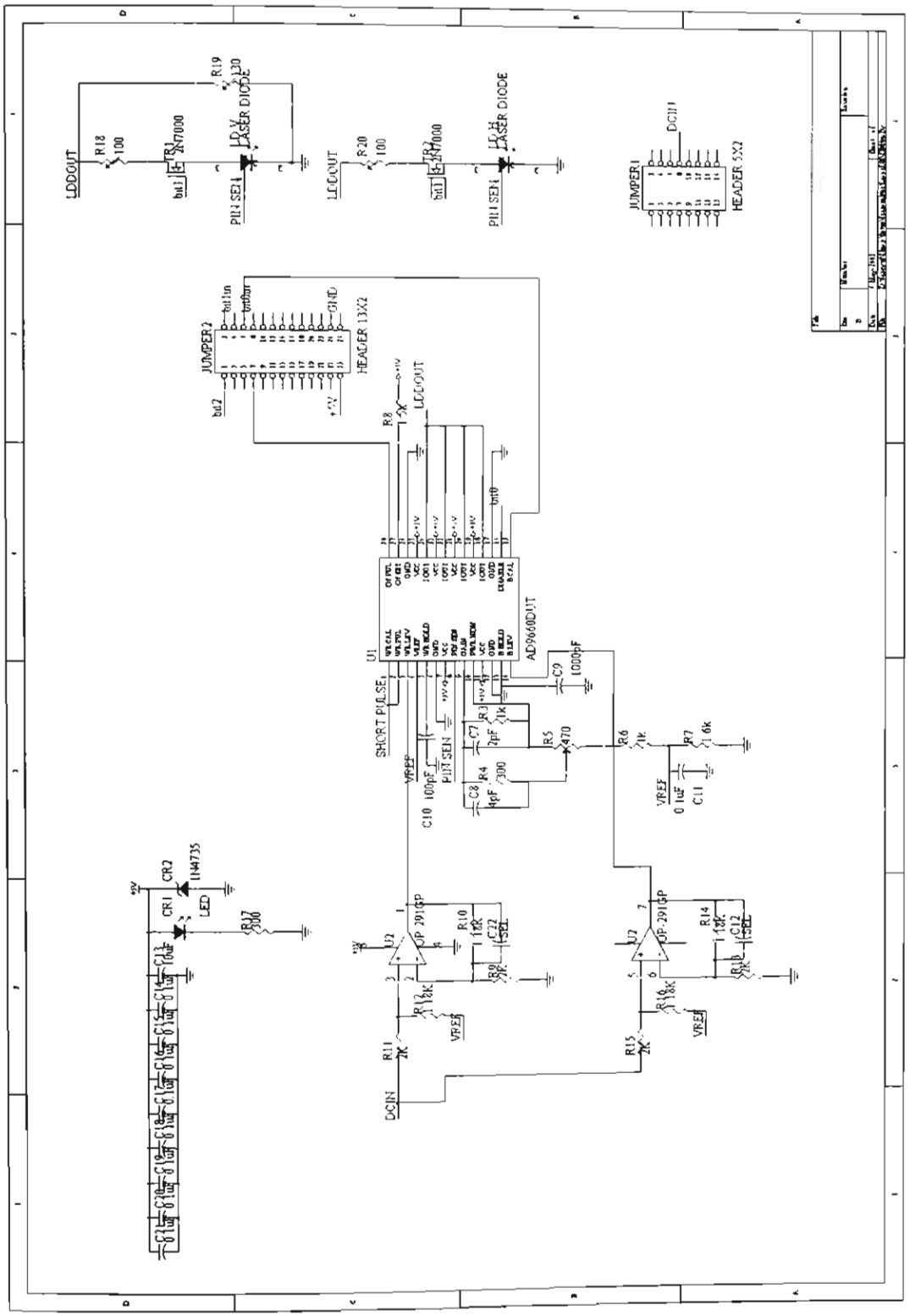
"Experimental Quantum Cryptography Based On The BB84 Protocal"
60th years Anniversary, Kasetsart University. Bangkok, 31st January - 8th February 2003.

APPENDIX A

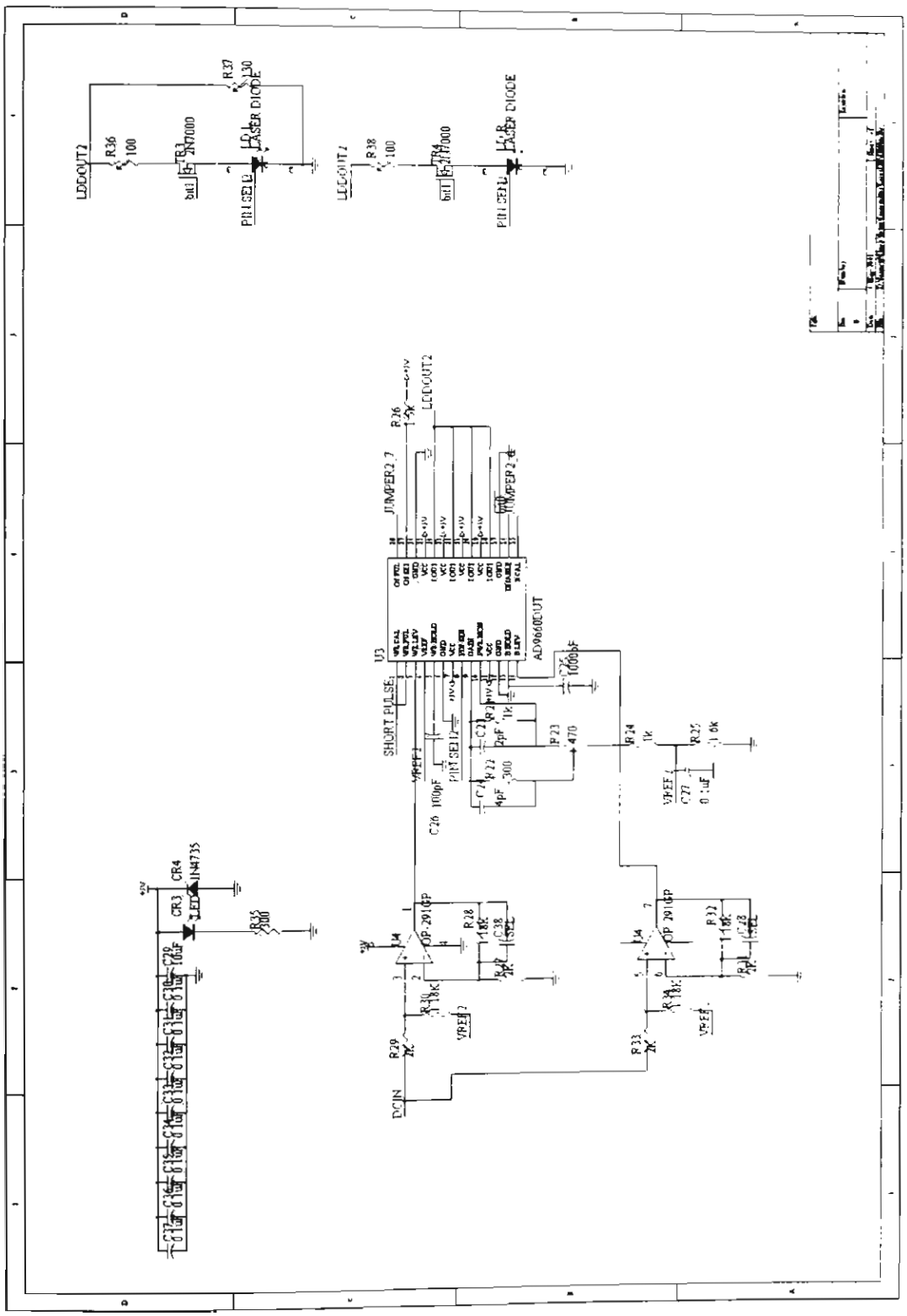
The schematic diagram of the Transmitter circuit (1)



The schematic diagram of the Transmitter circuit (2)

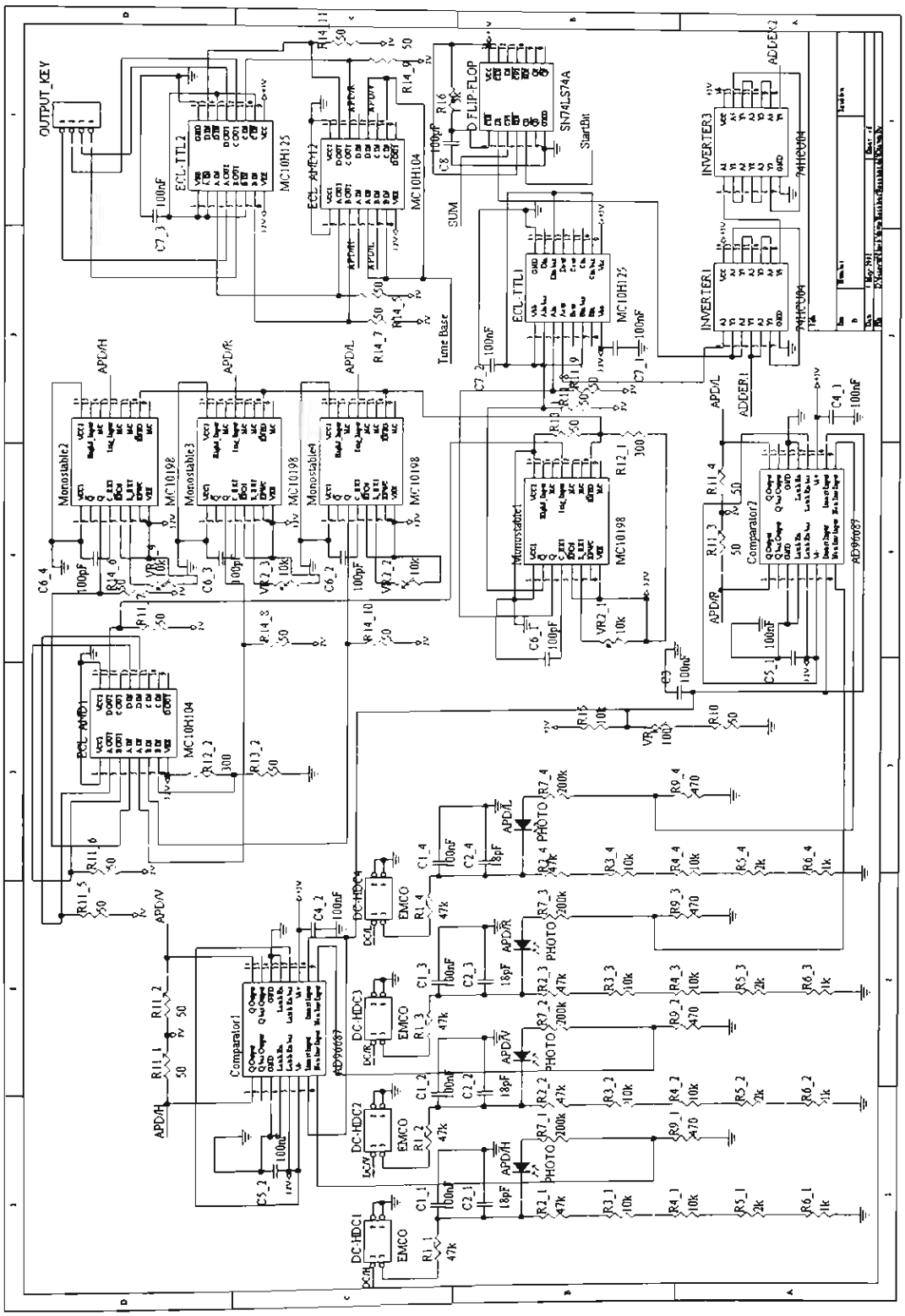


The schematic diagram of the transmitter circuit (3)



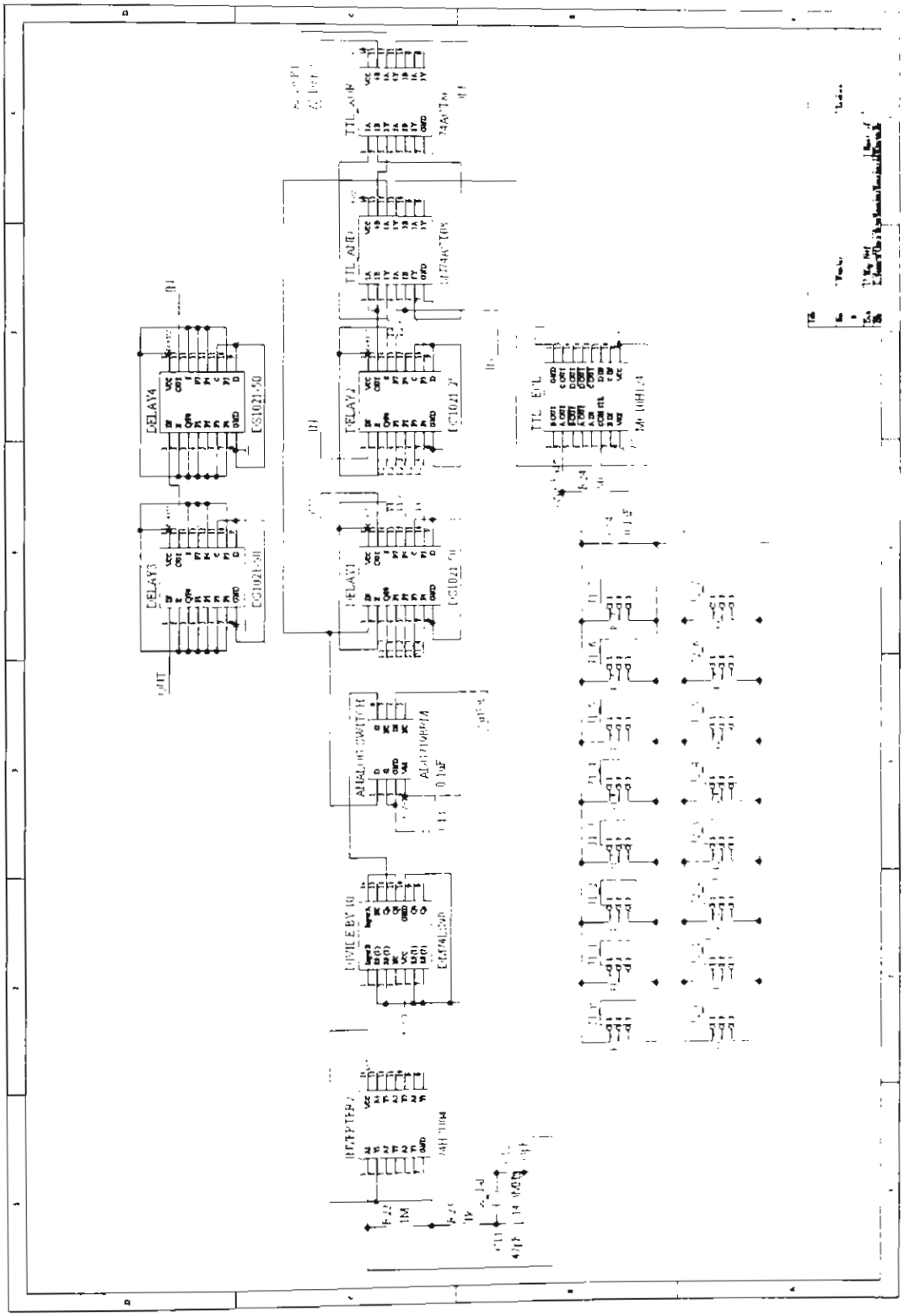
APPENDIX B

The schematic diagram of the receiver circuit



APPENDIX C

The schematic of the synchronization circuit



Appendix D

Photon Counting and temperature dependence of The APD

The APD can be triggered not only by photons, but also by carriers generated due to thermal, tunneling and trapping processes inside the semiconductor. These processes cause a self-triggering rate of the detector which is called *dark counting rate.* Thus counting all the pulses can lead to overestimating the light intensity at the detector.

The APD is a strong function of the device temperature. On the other hand, the APD dark current, as well as the dark current noise, is also dependent on the APD temperature. The EG&G APD C30902S-DTC is supplied with a built-in TEC cooler to control the detector temperature. The temperature status of the APD is sensed by the thermistor, R_T, which is located as close as possible to the APD in order to ensure a minimal temperature gradient between the two devices. For this particular thermistor, the relation between its resistance (Ω) and the temperature (K) given by

$$T = \left\{ \frac{\ln\left(\frac{R_T}{5.1X10^3\,\Omega} \right)}{3200} + \frac{1}{298} \right\}^{-1}$$

The bridge is supplied by the zener diode, with a zener voltage V_Z. The temperature monitor voltage reading, V_{TM}, is given in term of the zener voltage as (Fig. 18.)

$$V_{TM} = \frac{R_S}{R_S + R_T} V_Z$$

Where R_S is bridge balance resistance.

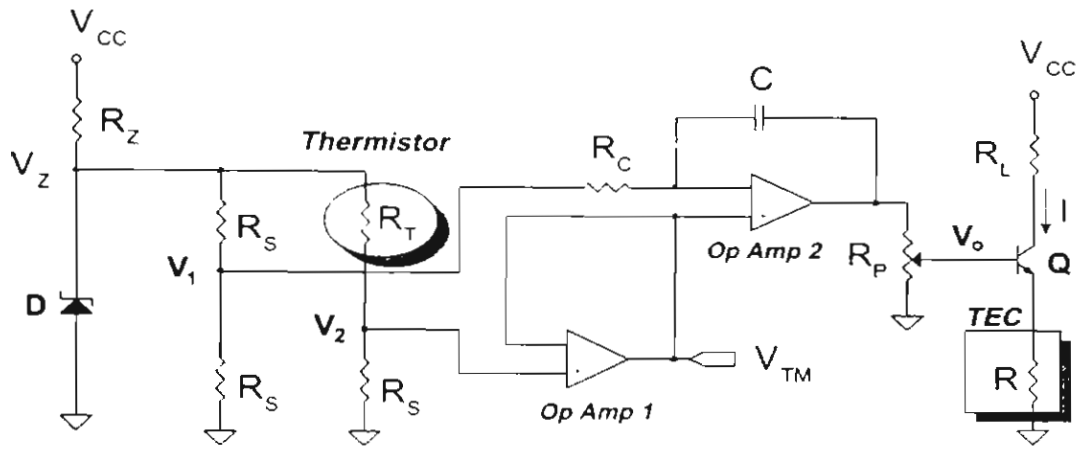


Fig.21. The temperature controller circuits for the APD

Source: Rafaat *et al.* (1999)

Appendix E

Principle Equipment

1. GaAlAs Laser Diodes; λ = 830 nm P = 40mW: HL8325G Hitachi
2. Avalanche photodiode: Model C30902S-DTC PerkinElmer
3. IC AD9660 laser driver: Analog Devices
4. DC power supply: Model GPC-3020D GW
5. Digital Multimeter: Model 973A Hewlett Packard
6. Digital oscilloscope: Model TDS 220 and TDS 784D Tektronix
7. IR viewing scope Edmund
8. Laser diode driver: Model 501 Newport
9. High-Speed Si Detector: DET210 Thorlabs
10. DC to HDC converter: Model G05 and CA05P EMCO
11. MCS-51 Microcontroller 24 MHz.
12. Universal time interval counter: Model SR620 Stanford Research
13. Non-polarizing cube beamsplitter: Model 03BSL062 Melles Griot
14. Polarizing cube beamsplitter: Model 03PBS062 Melles Griot
15. Half-wave plate: Model 02WRQ027 Melles Griot
16. Quarter-wave plate: Model 02WRQ007 Melles Griot
17. Computer Pentium III 866 MHz
18. Electronic software (Protel version 99)
19. Interference filter
20. lens

ส่วนที่ ๔ สล้างงานวิจัย (ผลงานวิจัยเด่นของอาจารย์ นักวิจัย และนิสิต มหาวิทยาลัยเกษตรศาสตร์)

- เพิ่มรสชาติให้กับชีวิต : พริก
- พุทธรักษาพันธุ์ใหม่จากการฉายรังสี
- ไม้ป่ายืนต้นของไทย 20 ชนิด ที่ควรขยายพันธุ์เพื่อใช้ในงานภูมิสถาปัตยกรรม
- ข้าวโพดสีม่วงสำหรับอุตสาหกรรมอาหารและยา
- อ้อยเคี้ยว "หยวนเจียง"
- **การเพิ่มผลผลิตและคุณภาพอ้อย โดยการปรับเปลี่ยนระยะแถว ปลูกและอัตราปุ๋ยที่เหมาะสม :**
  - อ้อยปลูกข้ามแล้ง
  - อ้อยปลูกต้นฝน
- โครงการอุทยานแมลงเฉลิมพระเกียรติ
- **การใช้ประโยชน์กวาวเครือในสัตว์เศรษฐกิจ**
  - การขยายพันธุ์กวาวเครือโดยการแบ่งหัวตอต้น
  - การวัดปริมาณสารออกฤทธิ์คล้ายฮอร์โมนเอสโตรเจนจากหัวกวาวเครือขาว 3 แหล่ง เมื่ออายุ 6, 9 และ 12 เดือนหลัง
    การปลูกเพื่อประโยชน์ในสัตว์เศรษฐกิจ
  - ผลของกวาวเครือขาวต่อสมรรถภาพการผลิตและคุณภาพซาก
    ของสุกรในระยะรุ่น-ขุน
  - ผลของกวาวเครือขาวในอาหารไก่ไข่ระยะให้ไข่สูงสุดถึงสิ้นสุด
    การไข่
  - ระดับที่เหมาะสมของการใช้กวาวเครือขาวในสูตรอาหารกระต่ายระยะรุ่น-ขุน
- การทำฟาร์มกวางรูซาเพื่อขยายพันธุ์และผลิตเขากวางอ่อน
- การใช้โปรแกรมจัดการสุขภาพและผลผลิตระดับฝูงเพื่อเพิ่มประสิทธิภาพการผลิตในฟาร์มโคนมขนาดเล็ก
- พรรณปลาชนิดใหม่ที่พบโดยคณาจารย์มหาวิทยาลัยเกษตรศาสตร์
- ความหลากหลายทางพันธุกรรมของปลาดุก (สกุล Clarias)
- การจำแนกชนิดไดอะตอมที่พบบนปะการังเทียมบริเวณอ่าวขามเกาะเสม็ด จ.ระยอง ด้วยกล้องจุลทรรศน์อิเล็กตรอนแบบส่องกราด
- งานวิจัยศักยภาพสิ่งแวดล้อมทางน้ำเพื่อการพัฒนาการประมงในเขื่อนป่าสักชลสิทธิ์อย่างยั่งยืน
- การผลิตอาหารสัตว์น้ำจากมันสำปะหลัง วัสดุพื้นบ้าน และสมุนไพร
  กวาวเครือ
- การเพิ่มมูลค่าปลานิลด้วยกรดไขมันโอเมก้า 3 โดยการใช้น้ำมันปลาทูน่าในอาหาร
- การสำรวจการเปลี่ยนแปลงการใช้ประโยชน์ที่ดินชายฝั่งทะเลโดยใช้เทคนิคการสำรวจระยะไกล
- พิพิธภัณฑ์ธรรมชาติป่าชายเลน : ห้องเรียนธรรมชาติชายฝั่ง
- ผลิตภัณฑ์ทางการเกษตรเพื่อทดแทนไม้
- การผลิตเส้นใยสับปะรดเพื่ออุตสาหกรรมสิ่งทอโดยวิธีการแช่ฟอก
- การใช้ 1% H_2SO_4 ในขบวนการฟอกขาวเปลือกในปอสาด้วย H_2O_2
- ผลของรำข้าวและโปรตีนสกัดจากถั่วเหลืองต่อคุณสมบัติของอาหาร
- ค้กยภาพในการต้านสารอนุมูลอิสระของผัก
  สุขภาพ และการป้องกันมัน
  ผลิตภัณฑ์อาหารจากพืชกรา
- การผลิตไวน์และน้ำผลไม้พร้อมดื่มจากหว้า
  ชุมชน
- ยีสต์สายพันธุ์ใหม่ *Pichia kasetsartensis* *siamensis* sp. nov., *Candida sithepens* *Citeromyces siamensis* sp. nov. ค้นพบ
  ของมหาวิทยาลัยเกษตรศาสตร์
- ห้องปฏิบัติการวิเคราะห์สารพิษจากเชื้อรา
  มุ่งสู่ระบบคุณภาพ ISO/IEC 17025
- มหัศจรรย์สมุนไพรไทย
- การเพิ่มประสิทธิภาพการสังเคราะห์สารทุติย
  การผลิตพืชเศรษฐกิจภาคตะวันตก โดยใช้
- การออกแบบโมเลกุลตัวยับยั้งเอนไซม์การ
  โดยวิธีเคมีคอมพิวเตอร์
- การทดลองวิทยาการเข้ารหัสลับควอนตัมโ
- การจัดกลุ่มเอกสารข้อความภาษาไทยแบบ
  แบบจำลองการค้นคืนสารสนเทศไทย
- การพัฒนาและออกแบบเครื่องขายนนทรีเฉล
- อรรถาภิธานศัพท์เกษตรไทย
- โครงการระบบประชุมทางไกลแอดเซลกริด
- **การประยุกต์ข้อมูลระบบภูมิสารสนเทศกับแ**
  ทรัพยากร
  - การศึกษาสัมพันธภาพของลุ่มน้ำเจ้
    จำลอง MIKE 11
  - Thailand Tributaries Relativity Assessme
    Geoinformatic System and SWAT Mode
    : Study on Amphoe Omkoi, Chiang Mai P
- SMART II - สวนสลับสัญญาณเครื่องขายเอทีเอ็มความเร็
- การแข่งขันหุ่นยนต์เตะฟุตบอล (ROBOCUP
- การแปรรูปวัสดุเหลือใช้ทางการเกษตรเป็น
  และปุ๋ยเพื่อลดต้นทุนการผลิต
- การศึกษาและวิจัยอุปกรณ์ที่ใช้ในการพรวน
- เครื่องอัดฟางหมักสำหรับการเพาะเห็ดในถุ
- เครื่องนวดเมล็ดข้าวน้ำนม
- เครื่องเพาะถั่วงอกอนามัยอัตโนมัติ
- บ้านเพื่อการอยู่อาศัยแบบยั่งยืน
- ผลกระทบการทางกายภาพอันเนื่องจากการ
  กรณีศึกษา มหาวิทยาลัยเกษตรศาสตร์ วิท
- การศึกษาหารูปแบบเมืองในจังหวัดเพชรบุรี
  คณิตศาสตร์
- **งานวิจัยภาษาศาสตร์**
  - พจนานุกรมลาว - ไทย - อังกฤษ อ
  - การพัฒนาโปรแกรมคอมพิวเตอร์ช่ว
    จากเพลงสำหรับนิสิตวิชาภาษาอังก
    มหาวิทยาลัยเกษตรศาสตร์
  - ลหสัมพันธ์ระหว่างกลองเสียงกับภา
    อานวรรณคดีร้อยกรองของไทย
- หลักสูตรการสอนคนตรีสากลโดยใช้วิธีการ

เคยวแบบกรอบพองจากเครองเอกซทรูเดอร
- การเปลี่ยนแปลงลักษณะโครงสร้างขององค์ประกอบภายในเส้น
บะหมี่ที่มีผลจากกระบวนการนึ่ง
- ขนมจีนแห้งและน้ำยาผงกึ่งสำเร็จรูปเพื่อการส่งออก
- การวิจัยพัฒนา และถ่ายทอดเทคโนโลยี การผลิตและ
แปรรูปวุ้นสวรรค์สู่ชุมชนครบวงจร และการพัฒนา SMEs
- การพัฒนาผลิตภัณฑ์มะม่วงเพื่อเพิ่มมูลค่าและการส่งออก การยก
ระดับ
อุตสาหกรรมแปรรูปมะม่วงดองในท้องถิ่นให้ได้มาตรฐาน
- การศึกษาหาพันธุ์พริกที่เหมาะสมต่อการแปรรูปเป็นผลิตภัณฑ์
อาหาร:ซอสพริก
- การพัฒนากระบวนการผลิตก๋วยเตี๋ยว และเส้นหมี่เพื่อลด
ปัญหาสิ่งแวดล้อม

โคไดและออร์ฟในระดับประถมศึกษา
- การสื่อสารเพื่อพัฒนาเกษตร "ทฤษฎีใหม่"
เจ้าอยู่หัว
ภูมิพลอดุลยเดช์
- การพัฒนารูปแบบกระบวนการจัดการเรียนก
แนว
การสร้างองค์ความรู้ในระดับชั้นประถมศึกษ
มก.
- กระบวนการพัฒนาหลักสูตรท้องถิ่นที่เอื้อต
นม :
กรณีศึกษาจังหวัดราชบุรี
- โครงการถ่ายทอดความรู้หลักสูตร "การผลิ
ชุมชน"
ให้กับเกษตรกรผู้ปลูกมะขามหวาน ต.วังชม
- รูปแบบการพัฒนาวนเกษตรในพื้นที่ลมน้ำเ
และสร้างมูลค่าเพิ่มอย่างยั่งยืน
- การจัดเก็บค่าชลประทานในภาคการเกษตร
ใหญ่
จังหวัดระยอง

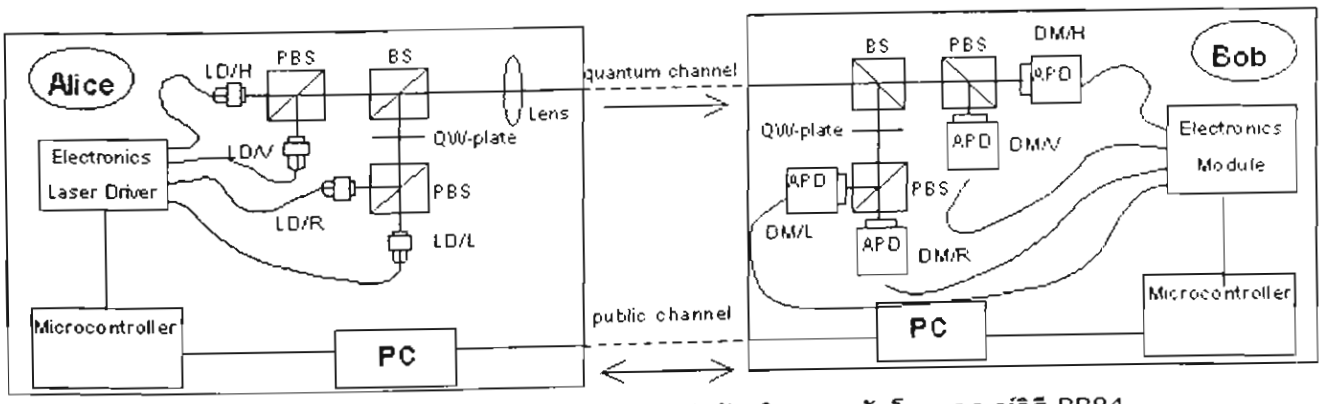
หน้าแรก

นิทรรศการงานวิจัย
๖๐ ปี มหาวิทยาลัยเกษตรศาสตร์
พัฒนาคน พัฒนาชาติ ศาสตร์แห่งแผ่นดิน

การทดลองวิทยาการเข้ารหัสลับเชิงควอนตัมโดยเกณฑ์วิธี BB84
Experimental Quantum Cryptography Based on the BB84 Protocol

สุรศักดิ์ เชียงกา สรายุธ เดชะปัญญา และ พิทักษ์ พานทอง
ภาควิชาฟิสิกส์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

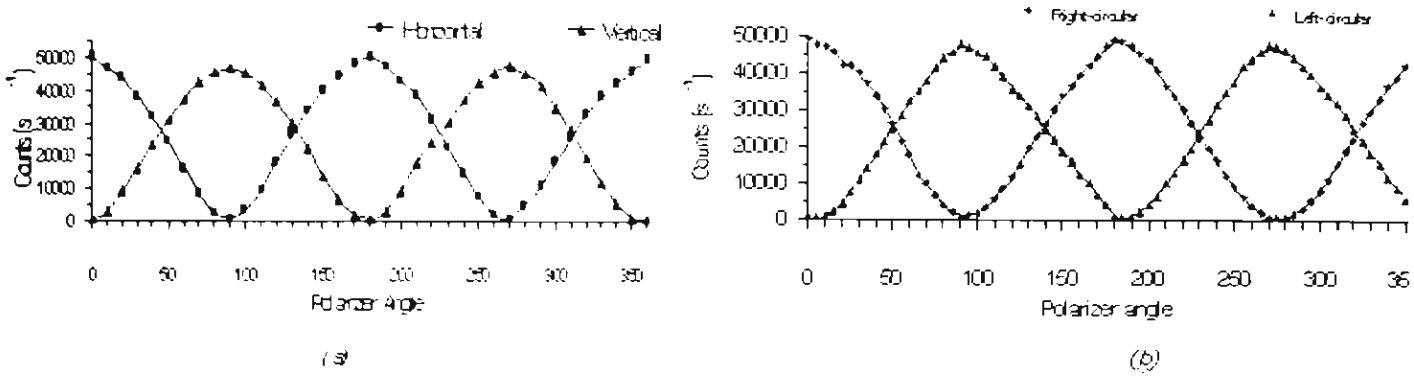
วิทยาการเข้ารหัสลับ (*cryptography*) เป็นการศึกษาเกี่ยวกับเทคนิคและการประยุกต์ต่างๆ ในการส่งข้อมูลผ่านช่องสื่อสารทั่วไปเพื่อทำให้ผู้ดักฟังไม่สามารถเข้าใจข้อมูลนั้นได้ วิธีการที่นิยมใช้คือการเข้ารหัสข้อมูลด้วยรหัสลับ (key) ดังนั้นความปลอดภัยของข้อมูลจึงขึ้นอยู่กับความปลอดภัยของรหัสลับ รหัสลับของระบบวิทยาการเข้ารหัสลับที่ใช้กันอยู่ในปัจจุบันสร้างขึ้นมาจากความซับซ้อนของปัญหาทางคณิต-ศาสตร์และไม่สามารถพิสูจน์ถึงความปลอดภัยของรหัสลับที่สร้างขึ้น โดยการทำลายรหัสลับจะขึ้นอยู่กับความเร็วของคอมพิวเตอร์ที่ใช้ในการหาผลเฉลยจึงมีความเสี่ยงสูงเนื่องจากแนวโน้มการพัฒนาความเร็วของคอมพิวเตอร์ในปัจจุบันเป็นไปอย่างรวดเร็วมาก ซึ่งตรงกันข้ามกับวิทยาการเข้ารหัสลับเชิงควอนตัมที่ความปลอดภัยของระบบรับประกันไว้ด้วยกฎต่างๆทางควอนตัมฟิสิกส์และวิธีการเข้ารหัสแบบเวอร์แนม (*Virnam cipher*) ซึ่งเป็นวิธีการเดียวที่ได้รับการพิสูจน์ว่ามีความปลอดภัยและระบบสามารถตรวจจับผู้ดักฟังข้อมูลได้อย่างแน่นอน



รูปที่ 1 แผนผังชุดทดลองวิทยาการเข้ารหัสลับเชิงควอนตัมโดยเกณฑ์วิธี BB84

ภาคส่ง(*Alice*)กำเนิดโฟตอนเดี่ยวด้วยเลเซอร์ไดโอด (*LD*) ที่กำหนดสถานะโพลาไรส์ของโฟตอนเดี่ยว ตามเกณฑ์วิธีBB84 ด้วยกระจกแยกลำโฟตอนชนิดโพลาไรส์ (*PBS*) , แผ่นหน่วงครึ่งคลื่น (*QW-plate*) และรวมลำโฟตอนด้วยกระจกแยกลำโฟตอน (*BS*) ส่งผ่านอากาศไปยังภาครับ(Bob)ที่ประกอบด้วยทัศนอุปกรณ์เช่นเดียวกับภาคส่งเพื่อวิเคราะห์สถานะโพลาไรส์ของโฟตอนเดี่ยวและตรวจจับด้วยอะวัลลันช์โฟโตไดโอด (*APD*) และจะเข้ารหัสเป็นเลขบิตฐานสอง (*key*) โดยตรวจสอบผู้ดักฟังข้อมูล (*eavesdropper*) ด้วยคอมพิวเตอร์ *(PC)* ผ่านระบบอินเตอร์เน็ต

ในงานวิจัยนี้เป็นการทดลองของระบบต้นแบบที่สร้างขึ้นตามเกณฑ์วิธี BB84 ซึ่งประกอบด้วยภาคส่งและ
ภาครับ (รูปที่1) โดยภาคส่งประกอบด้วยเลเซอร์ไดโอดจำนวน 4 ตัว ที่กำหนดให้ทำงานแบบพัลส์ ความถี่ 1 MHz
โดยมีจำนวนโฟตอนเฉลี่ยประมาณ 0.05 โฟตอนต่อพัลส์ สถานะโพลาไรส์ของโฟตอนเดี่ยวสร้างได้จากชุด
ทัศนอุปกรณ์ชนิดพาสซีฟ ภาครับประกอบด้วยอะวัลลันช์โฟโตไดโอดจำนวน 4 ตัวและชุดทัศนอุปกรณ์ชนิด
พาสซีฟเช่นเดียวกับภาคส่งเพื่อใช้ในการวิเคราะห์สถานะโพลาไรส์ของโฟตอน



รูปที่ 2 แสดงการวิเคราะห์สถานะโพลาไรซ์ของภาคส่งด้วย APD (a) สถานะ| H>และ | v>(b) สถานะ | R>และ | L>

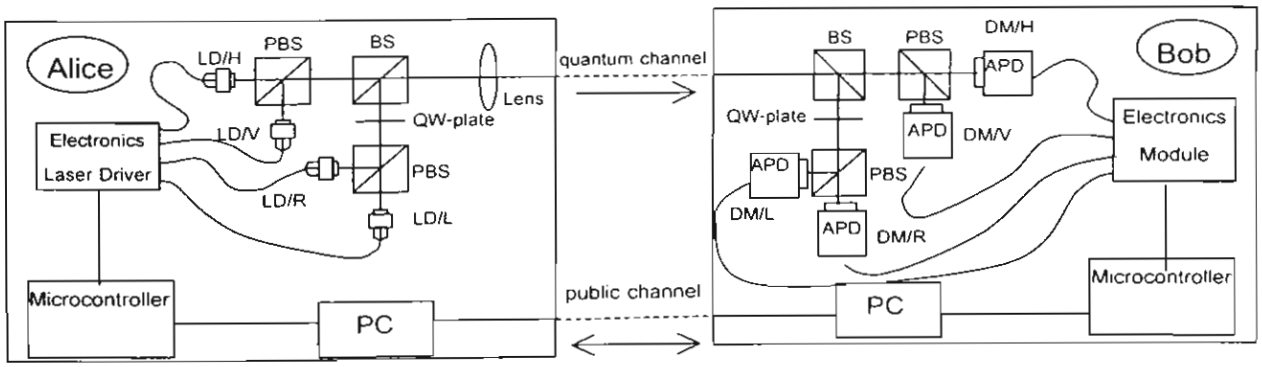
จากผลการทดลอง(รูปที่2) สามารถวัดค่าสภาพมองเห็นได้ (*visibility*) ของสถานะโพลาไรซ์ของโฟตอนเดียวแต่ละสถานะ
ได้ดังนี้ V_H=0.99, V_V=0.99, V_R=0.97, และ V_L=0.97 ซึ่งชี้ให้เห็นว่าสามารถที่จะสร้างรหัสลับด้วยระบบต้นแบบนี้ได้

การทดลองวิทยาการเข้ารหัสลับเชิงควอนตัมโดยเกณฑ์วิธี BB84

EXPERIMENTAL QUANTUM CRYPTOGRAPHY BASED ON THE BB84 PROTOCOL

สุรศักดิ์ เชียงกา, สรายุธ เดชะปัญญา, พิทักษ์ พานทอง
ภาควิชาฟิสิกส์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

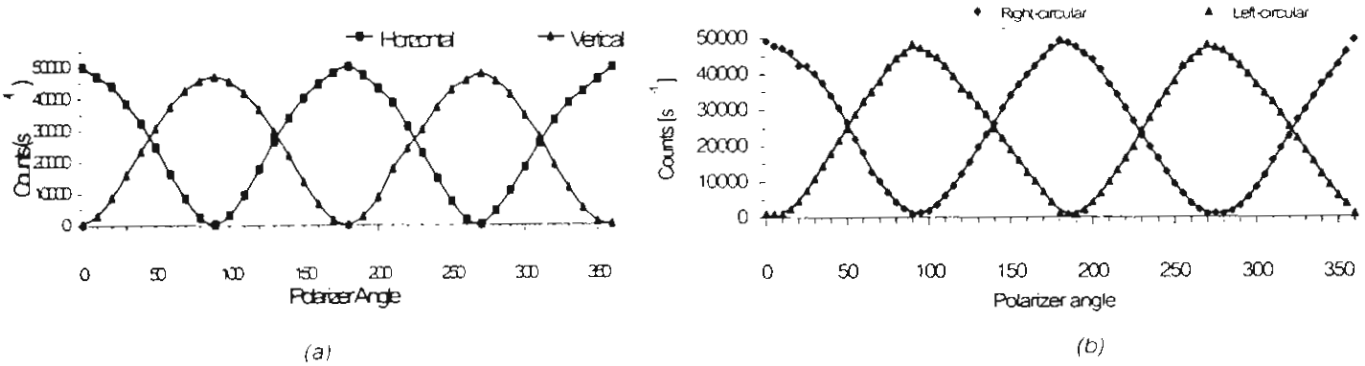
วิทยาการเข้ารหัสลับ (*cryptography*) เป็นการศึกษาเกี่ยวกับเทคนิคและการประยุกต์ต่างๆ ในการส่งข้อมูลผ่านช่องสื่อสารทั่วไปเพื่อทำให้ผู้ดักฟังไม่สามารถเข้าใจข้อมูลนั้นได้ วิธีการที่นิยมใช้คือการเข้ารหัสข้อมูลด้วยรหัสลับ (*key*) ดังนั้นความปลอดภัยของข้อมูลจึงขึ้นอยู่กับความปลอดภัยของรหัสลับ รหัสลับของระบบวิทยาการเข้ารหัสลับที่ใช้กันอยู่ในปัจจุบันสร้างขึ้นมาจากความซับซ้อนของปัญหาทางคณิตศาสตร์และไม่สามารถพิสูจน์ถึงความปลอดภัยของรหัสลับที่สร้างขึ้น โดยการทำลายรหัสลับจะขึ้นอยู่กับความเร็วของคอมพิวเตอร์ที่ใช้ในการหาผลเฉลยจึงมีความเสี่ยงสูงเนื่องจากแนวโน้มการพัฒนาความเร็วของคอมพิวเตอร์ในปัจจุบันเป็นไปอย่างรวดเร็วมาก ซึ่งตรงกันข้ามกับวิทยาการเข้ารหัสลับเชิงควอนตัมที่ความปลอดภัยของระบบรับประกันไว้ด้วยกฎต่างๆทางควอนตัมฟิสิกส์และวิธีการเข้ารหัสแบบเวอร์แนม (*Virnam cipher*) ซึ่งเป็นวิธีการเดียวที่ได้รับการพิสูจน์ว่ามีความปลอดภัยและระบบสามารถตรวจจับผู้ดักฟังข้อมูลได้อย่างแน่นอน



รูปที่ 1 แผนผังชุดทดลองวิทยาการเข้ารหัสลับเชิงควอนตัมโดยเกณฑ์วิธี BB84

ภาคส่ง(Alice)กำเนิดโฟตอนเดี่ยวด้วยเลเซอร์ไดโอด(LD)ที่กำหนดสถานะโพลาไรส์ของโฟตอนเดี่ยวตามเกณฑ์วิธีBB84 ด้วยกระจกแยกลำโฟตอนชนิดโพลาไรส์(PBS), แผ่นหน่วงครึ่งคลื่น(QW-plate)และรวมลำโฟตอนด้วยกระจกแยกลำโฟตอน(BS)ส่งผ่านอากาศไปยังภาครับ(Bob)ที่ประกอบด้วยทัศนอุปกรณ์เช่นเดียวกับภาคส่งเพื่อวิเคราะห์สถานะโพลาไรส์ของโฟตอนเดี่ยวและตรวจจับด้วยอะวัลลันช์โฟโตไดโอด(APD)และจะเข้ารหัสเป็นเลขบิตฐานสอง(key) โดยตรวจสอบผู้ดักฟังข้อมูล(eavesdropper)ด้วยคอมพิวเตอร์(PC)ผ่านระบบอินเตอร์เน็ต

ในงานวิจัยนี้เป็นการทดลองของระบบต้นแบบที่สร้างขึ้นตามเกณฑ์วิธี BB84 ซึ่งประกอบด้วยภาคส่งและภาครับ (รูปที่1) โดยภาคส่งประกอบด้วยเลเซอร์ไดโอดจำนวน 4 ตัว ที่กำหนดให้ทำงานแบบพัลส์ ความถี่ 1 MHz โดยมีจำนวนโฟตอนเฉลี่ยประมาณ 0.05 โฟตอนต่อพัลส์ สถานะโพลาไรส์ของโฟตอนเดี่ยวสร้างได้จากชุดทัศนอุปกรณ์ชนิดพาสซีพ ภาครับประกอบด้วยอะวัลลันช์โฟโตไดโอดจำนวน 4 ตัวและชุดทัศนอุปกรณ์ชนิดพาสซีพเช่นเดียวกับภาคส่งเพื่อใช้ในการวิเคราะห์สถานะโพลาไรส์ของโฟตอน



รูปที่ 2 แสดงการวิเคราะห์สถานะโพลาไรซ์ของภาคส่งด้วย APD (a) สถานะ $|H\rangle$ และ $|V\rangle$ (b) สถานะ $|R\rangle$ และ $|L\rangle$

จากผลการทดลอง(รูปที่2) สามารถวัดค่าสภาพมองเห็นได้ (*visibility*) ของสถานะโพลาไรซ์ของโฟตอนเดี่ยวแต่ละสถานะได้ดังนี้ V_H=0.99, V_V=0.99, V_R=0.97, และ V_L=0.97 ซึ่งชี้ให้เห็นว่าสามารถที่จะสร้างรหัสลับด้วยระบบต้นแบบนี้ได้

กิตติกรรมประกาศ: สรายุธ เดชะปัญญา ได้รับทุนอุดหนุนและส่งเสริมวิทยานิพนธ์ระดับปริญญาโท-เอก จากบัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์, สุรศักดิ์ เชียงกา ได้รับทุนอุดหนุน จากสำนักงานกองทุนสนับสนุนการวิจัย สัญญาเลขที่ PDF43/22/2543

เอกสารอ้างอิง: [1] Gilles Brassard, Charles H. Bennett and Arthur K. Ekert. *Quantum cryptography.* Scientific American, pages 26-33, October 1992.

Experimental Quantum Cryptography based on the BB84 Protocol

S. Deachapunya[1], S. Chiangga[1], H. Weinfurter[2,3]
[1]Department of Physics, Kasetsart University, Bangkok 10900
[2] Sektion Physik, Ludwig-Maximilians-Universität München,
Schellingstr. 4/III, D-80799 München, Germany
[3] Max-Planck-Institut für Quantenoptik, D-85748 Garching, Germany

Abstract

Quantum cryptography is a new technique that provides verifiable secure key exchange between the sender and receiver. The security of the quantum cryptographic system is protected by the laws of quantum physics, which ensure that any eavesdropping can always be detected. This is in strong contrast with classical key exchange, where the security depends on (unprovable) assumptions. Recent experimental implementation of quantum cryptography achieved about 50 km point-to-point key exchange over optical fibers and about 1 km over a free space connection in daylight. Here we report the development of experimental free space quantum cryptographic systems based on the BB84 protocol. Our system does not use any active manipulation elements, resulting in compactness, reliability and easy handling.

Keywords: quantum cryptography, quantum information

1. INTRODUCTION

Cryptography is the study of techniques and applications of secure communication. The fundamental objective of cryptography is to transmit information over an insecure channel in such a way that an opponent cannot understand it. This goal can be achieved if the sender and receiver both possess some secret information, referred to as a key. The safety of the information transmission thus depends entirely on the safety of the key [1]. With conventional communications, it is taken for granted that digital communication can always be passively monitored or copied. Numerical cryptoanalysis is possible for many systems. Their security therefore depends crucially on the computational power a potential eavesdropper might have.

By contrast, the security of quantum cryptographic keys is based on fundamental and immutable laws of quantum physics, one of which is the Heisenberg uncertainty principle. Any eavesdropping attempts to intercept the communication channel can always be detected. The original quantum cryptography scheme was proposed in 1984 by Bennett and Brassard [2] abbreviated as BB84. The first prototype constructed in 1989 was based on a coding scheme involving polarized photons, in which the linear and circular polarization states formed the required pair of bases. Due to the Heisenberg uncertainty principle, measuring, say, the linear polarization of a single photon projects its state into an eigenstate of linear polarization and perfectly destroys any prior value one might have had for circular polarization. Therefore, if the wrong choice of measurement basis is made by the eavesdropper, he will raise the key error rate above a threshold value which alerts the legitimate users of the presence of an eavesdropper.

In this paper, we give a short introduction into the theory of quantum cryptography. Then we describe the experimental aspects involved in the actual realization of our quantum cryptographic system based on polarization encoding of attenuated coherent light pulses.

2. THEORY

The general quantum cryptographic system comprises of a transmitter and a receiver. The transmitter consists of the sources of photons and an optical system. In realistic systems, the sender (Alice) generates an approximation to the desired sequence of single photons by attenuating short pulses of light from laser diodes. The optical system randomly assigns polarization states to the photons. Each photon's polarization state is then encoded by the sender according to a random, binary number "1" or "0".

The receiver (Bob) comprises of an optical system similarly to the transmitter and of the single photon detectors. The receiver randomly projects the incoming photon onto either one of two distinct perpendicular optical paths, where each optical path is oriented to detect a specific polarization state and the bit number "1" or "0" encoded by the receiver. The quantum key generation requires several steps as follow: [3], [4].

1. Alice sends a sequence of photons, each randomly encoded with one of the four polarization states, and each occupying a well-defined time slot.

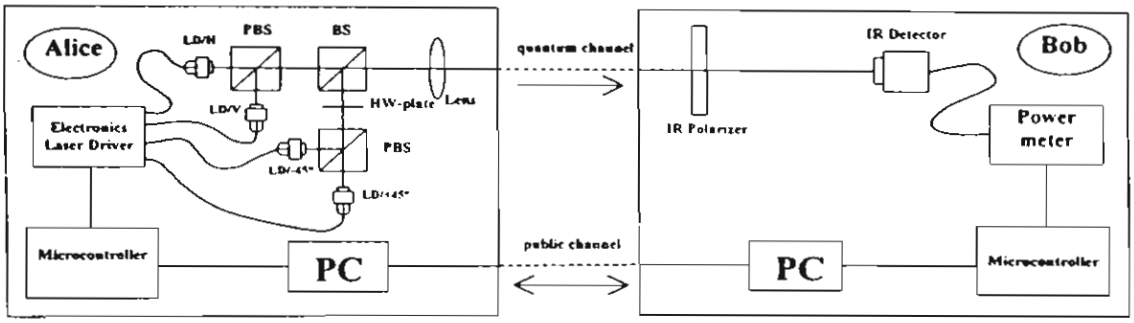


Figure 1. The simplified diagram of our practical quantum cryptography transmitter.

2. Bob's clock is well synchronized with Alice's clock and in each of the time slots he randomly chooses to measure one of the two polarization types; i.e. circular or linear. He records the result of that measurement.

3.After the transmission, Alice and Bob communicate publicly e.g. telephone, newspaper etc.:Bob tells Alice when he detected a photon and which type of polarization measurement he used in this particular time slot, but keeps the result secret.

Alice tells Bob for which detection they had chosen the same basis. They then agree to discard all the events in which they used a different measurement basis.

4. Alice and Bob now choose a random subset of the remaining bit string, which they use to test for the presence of an eavesdropper.

This test again is carried out over the public channel, but now Alice and Bob perform a statistical comparison of their selected bits. If no errors are found Alice and Bob can be sure that the remaining bits which have not been revealed publicly are secure and therefore constitute a useful shared secret key.

3. EXPERIMENTAL SETUP

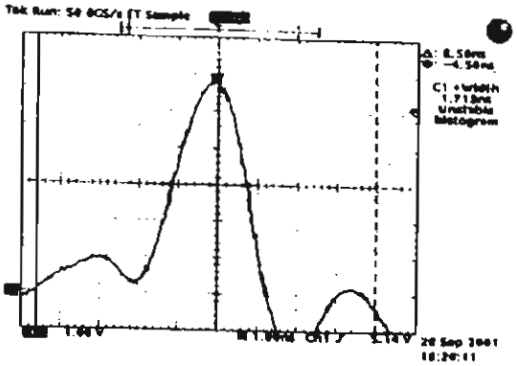
A simplified diagram of our quantum key distribution transmitter module is shown in Figure 1. The attenuated pulse is generated by applying a 1.7 ns electrical pulse with a 2.86

MHz repetition rate to one of four low power laser diodes (Hitachi, 830nm 40mW) which is selected randomly with the pseudo-random number generated from a personal computer. The Coherence states $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle$ are generated by each laser operation well above the threshold. In our case the amplitude $|\alpha|^2 = 0.1$ was chosen, to give a photon number distribution per pulse according to $P_n = e^{-|\alpha|^2}|\alpha|^{2n}/n!$. A passive optical system sets the photon's polarization to $|H\rangle$, $|V\rangle$, $|+45\rangle$, or $|-45\rangle$ depending on whether the binary number is a "0" or a "1". It is comprised of a half wave plate ($\lambda/2$), two polarizing beam splitters (PBS), a beam splitter (BS) and lens. A pair of laser diodes in the upper paths is oriented so that the light beams overlapped at PBS have horizontal polarization, $|H\rangle$ (after transmission) and vertical polarization, $|V\rangle$ (after reflection). A pair of laser diodes on the lower path is also oriented similarly to the first pair, but a half wave plate rotates the plane of polarization by 45°. Therefore, they allow us to set the necessary $|+45\rangle$ and $|-45\rangle$ polarization states. The polarizer and the optical power meter (Newport, 1830-C) in series is used to test the performance of the transmitter.

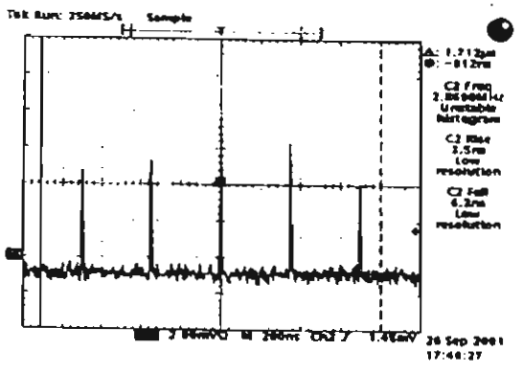
4. RESULTS

Figure 2(a) shows the 1.7 ns, 2.86 MHz input signal to the four laser diodes monitored with an oscilloscope (Tektronix, TDS784D). The optical pulse signal generated by a laser diode, measured with the Si-PIN photodiode (Thorlab, DET210), is shown in Figure 2(b). The observed width of 7 ns is currently limited from below by the bandwidth of the detection system, but surely is not longer than the driving pulse.

Figure 3 presents the variation of the observed intensity depending on the angle of the analyzing IR-polarizer for the four input polarizations. We observe visibilities of V_H=0.97, V_V=0.93, $V_{+45°}$=0.97, and $V_{-45°}$=0.97, which clearly demonstrates the usability of our simple transmitter for low-noise, free-space quantum cryptography.



(a)



(b)

Figure 2. (a) The 1.7 ns, 2.86 MHz input signal, (b) The optical output signal, measured with the Si-PIN photodiode

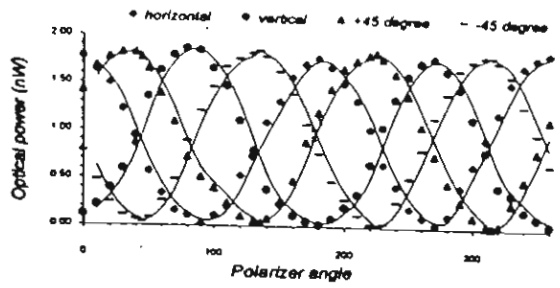


Figure 3. The polarization analysis of the transmitter

5. CONCLUSION

In this work, we present first tests of the quantum cryptographic transmitter module for a free space application of the BB84 protocol. The data measured with the optical power meter shown in Figure 3 indicate that it is feasible to send the random polarization state of photons to the receiver by our fast and compact transmitter. By contrast to other experimental set-ups which commonly use some active manipulation devices to set the photon's polarization, our system utilizes merely laser diodes and a few passive optical components. Most of the hardware is constructed in our laboratory, resulting in cost effective and easy to reconfigure systems.

6. ACKNOWLEDGEMENTS

S. Chiangga acknowledged financial support by Kasetsart University Research and Development Institute under contract □.□. 12.43 and by the Thailand Research Fund under grant PDF 22/2543. And S. Deachapunya appropriately acknowledged financial support by UDC scholarship.

REGERRENCES

[1] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. pp. 175-179, December 10-12, 1984. *Proceedings of the International Conference on Computers, Systems & Signal Processing*, Bangalore, India.

[2] Charles H. Bennett and Gilles Brassard. An update on quantum cryptography. In G. R. Blakley and D. C. Chaum, editors, *CRYPT084*, pp. 475-480. Springer, 1985. Lecture Notes in Computer Scitnce No. 196.

[3] Gilles Brassard, Charles H. Bennett and Arthur K. Eckert. Quantum cryptography. *Scientific American*, pp. 26-33, October 1992.

[4] Richard J. Hughes et al., Secure communications using quantum cryptography, *SPIE Proceedings* **3076**, 2 (1997).

Photon Counting with Passive Quenched Silicon Avalanche

S. Deachapunya[1], D. Jarukanont[1], P. Panthong, S. Chiangga[2]
Department of Physics, Kasetsart University, Bangkok 10900

Abstract

We investigate the performance of silicon avalanche photodiode (APD) with passive quenching circuit for photon counting in the near-infrared range. The characterizations of an APD cooled at –20 °C are described in terms of dark counts, operating temperature and bias-voltage.

Keywords: optoelectronics, optical detector.

1. INTRODUCTION

It is well known that photon counting is the technique of applications in which faint and fast responsibilities of light detection are required. In recent years, significant demonstrations have been widely used in quantum teleportation [1], quantum cryptography [2], optical communication and in sensor applications [3]. For the first telecommunication window, there are commercially available single photon detectors. They are based on silicon (Si) avalanche photodiodes, which have high quantum efficiencies (≥ 50%) and low noise rates.

Several groups have reported the Ge APDs operating in the Gieger mode, i.e., at a voltage higher than the breakdown level, can detect a single photon at 1.3 μm if they are first cooled to 77 K to reduce noise.

However, the single photon efficiency is very low (~10-30%) and intrinsic noise rate (dark counts rate) ≥1000 times higher than Si APD at 0.85 μm [4].

After a brief introduction to the principle of operation of a Geiger mode APD with passive quenching, we then report the performance of a C30902S-DTC Si APD manufactured by EG&G which includes a built-in thermoelectric cooler (TEC) and a thermistor. The experimental results of temperature controller and dark counts as a function of the temperature and bias voltage are discussed.

2. THEORY

2.1 Principle of operation

The APD is a solid state quantum, optical detector intended for low light level application in the visible and near infrared region. It operates in a reverse bias in either its normal linear mode when the bias voltage, V_R, less than the breakdown voltage, V_{BR}. In this mode the gain is up to 250 or greater, or as a photon counter in Geiger mode when V_R held above the breakdown voltage. Under this condition, a single photoelectron can trigger an avalanche pulse of about 10^8 carriers. In this mode, no amplifiers are necessary and single-photon detection probabilities up to 50% are possible. After the avalanche is triggered, the current keeps flowing until the avalanche is quenched by lowering the bias voltage down to V_{BR} or below. The bias voltage is then restored in order to detect another photon. The APD current can either be turned off passively by limiting the current flowing with a suitable resistor, or actively by lowering the bias voltage after the onset of the avalanche.

2.2 Passive quenching circuit

Passive quenching is simple to implement, requires a minimum of power,

---

[1] S. Deachapunya and P. Panthong are the graduated physics students at department of physics, Kasetsart University, Bangkok, 10900.
[2] D. Jarukanont is a senior DPST physics student at department of physics, Kasetsart University, Bangkok, 10900.

space and is robust. In this mode, the APD is reverse biased beyond breakdown through a high impedance resistor R_L in Figure1. To be in the conducting state at V_{BR} two conditions must be met [5]:

1. The avalanche must have been triggered by either a photoelectron or a bulk-generated electron entering the avalanche region of the diode. (holes are inefficient at starting avalanches in silicon) The probability of an avalanche being initiated is discussed above.

2. To continue to be in the conducting state a sufficiently large current, called the latching current, I_{LATCH}, must be passing through the device so that there is always an electron or hole in the avalanche region. Typically in the C30902S-DTC, I_{LATCH} =50 μA. For currents $(V_R-V_{BR})/R_L$, much greater than I_{LATCH}, the diode remains conducting. If the current $(V_R-V_{BR})/R_L$, is much less than I_{LATCH}, the diode switches almost immediately to the non-conducting state. If $(V_R-V_{BR})/R_L$, is approximately equal to I_{LATCH}, then the diode will switch at an arbitrary time from the conducting to the non-conducting state depending on when the number of electrons and holes in the avalanche region statistically fluctuates to zero.

When R_L is large, the photodiode is normally nonconducting, and the operating point is at $V_R-I_{ds}R_L$ in the non-conducting state where I_{ds} is the dark surface current. Following an avalanche breakdown, the device recharges to the voltage $V_R-I_{ds}R_L$ with the time constant CR_L where C is the total device capacitance including stray capacitance. Using C = 1.6 pF and R_L = 400kΩ. a recharge time constant of 0.64 microseconds is calculated.

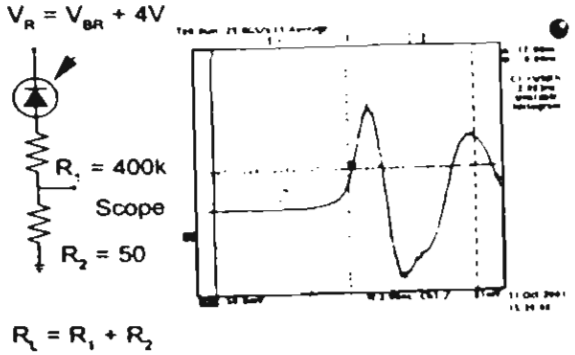


Figure 1 Passively quenched APD in the photon-counting mode and real-time trace pulse shape

2.3 Photon counting

The APD can be triggered not only by photons, but also by carriers generated due to thermal, tunneling and trapping processes inside the semiconductor. These processes cause a self-triggering rate of the detector which is called dark counting rate, R. Thus counting all the pulses can lead to overestimating the light intensity at the detector.

In photon counting measurements, the signal is produced by the photoelectron counted by the detector while the noise is contributed to the statistical fluctuation. The minimum detectable optical power P_m can be expressed:

$$P_m = \frac{h\nu}{\eta}\left(\frac{R}{T}\right)^{1/2} = \frac{NEP}{(2T)^{1/2}} \qquad (1)$$

Where NEP is the detector noise-equivalent power, T is the measurement time, η is the photon detection efficiency of the detector, and hν is the photon energy.

When APDs is operated with a passive quenching circuit, and the count rate is low (< 250 kHz), the dead-time correction count rate, n_s, can be estimated from [3]

$$n_s = \frac{n_c}{1 - n_c\tau} \qquad (2)$$

Where n_c is the observed count rate, and τ is the dead time.

2.4 APD temperature dependence

An APD is a device similar to a rectifier diode, except its output current contains a term which is dependent on the incident light intensity on its surface in the operating wavelength range. The APD output current is given by

$$I_{APD} = -I_d + I_s\left(e^{\frac{qV}{kT}} - 1\right) \qquad (3)$$

where I_{APD} is the APD output current, I_d is the detected photo-current, I_s is the saturation dark current, q is the electron charge, V is the

device bias voltage (negative for reverse bias), k is Boltzmann's constant, and T is the temperature. The second term of equation (3) represents the APD dark current and the first term, I_d, represents the photo-current, given by

$$I_d = \Re P \qquad (4)$$

where $\Re$ is the APD responsivity, and P is the incident optical power. The APD responsivity, $\Re$ (A/W), is obtain from

$$\Re = \eta G \cdot \frac{q}{hc} \cdot \lambda \qquad (5)$$

where η is the wavelength dependent quantum efficiency, G is the APD internal gain, h is Planck's constant, c is the speed of light, and λ is the wavelength of the incident light. At a constant bias voltage, the APD operating temperature affects its output current. The APD gain, and therefore its responsivity, is a strong function of the device temperature. On the other hand, the APD dark current, as well as the dark current noise, is also dependent on the APD temperature.

2.5 APD temperature controller

The EG&G APD C30902S-DTC is supplied with a built-in TEC cooler to control the detector temperature. The temperature status of the APD is sensed by the thermistor, R_T, which is located as close as possible to the APD in order to ensure a minimal temperature gradient between the two devices. For this particular thermistor, the relation between its resistance (Ω) and the temperature (K) given by

$$T = \left\{ \frac{ln\left(\frac{R_T}{5.1X10^3\,\Omega}\right)}{3200} + \frac{1}{298} \right\}^{-1} \qquad (6)$$

The bridge is supplied by the zener diode, D, with a zener voltage V_Z.

The temperature monitor voltage reading, V_{TM}, is given in term of the zener voltage as

$$V_{TM} = \frac{R_S}{R_S + R_T} V_Z \qquad (7)$$

Where R_S is bridge balance resistance.

3. EXPERIMENTAL SETUP AND RESULTS

The simple setup of our APD module for photon counting is illustrated in Fig 2. The avalanche photodiode was placed in the closed black box to ensure that there is no any light reaching the APD. The output signal from the APD without amplification (Figure 1) has an amplitude ~100 mV and duration <5ns FWHM. The dead time in the detector $\sim 1\mu s$ is in reasonable agreement with calculation. This signal is discriminated by an comparator (Analog Device, AD96687). Dark counting rate and after pulse can be effectively reduced by this pulse shape discriminator (PSD). The pulse stretcher circuit (PS) is used so that the maximum APD output fit the minimum digital counter limit. The output detected signal from the PS is then applied to the digital counter (Leybold, 54745). In our experiments we incorporate a non paralyzable electronic dead time that ignores those counts that arrive within a short time (250-1000 ns) after every pulse. We find that most afterpulses occur within a few microseconds of an initial pulse, so the electronic dead time serves to eliminate some of the afterpulses from the count rates that we measure. Since the APD responsivity is a strong function of its voltage bias and temperature. The low ripple (0.025%) high voltage bias controller was designed follow Ref. 6 which can be adjusted manually to apply a constant voltage to APD.

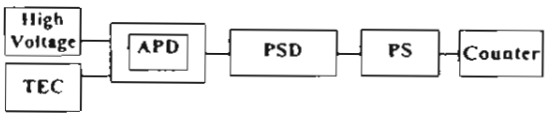


Figure 2. The experimental

The proportional integral temperature controller circuit from Ref. 8 was adopted to cool the detector to a fixed set point from the ambient temperature. With the precision resistors R_S = 34.8 kΩ ± 50 ppm, the APD temperature was set to –20 °C from the initial room temperature of 20 °C.

The temperature measurement is obtained by coverting the temperature monitor voltage to a thermistor resistance according to equation (7), and then this is further converted into temperature according to equation (6). Figure

3. shows the temperature variation of the APD with the thermoelectric cooler controller. The steady-state temperature is -20±0.1 °C with the settling time approximately 3 s.

Figure 4. shows the measured dark counting rate as a function of voltage beyond breakdown and operated at -20 °C to keep the dark count rate low.

We observed that the breakdown voltage of our detector is about 193 Volt and the dark counts rate is exponentially increased approximated by

$y = 0.4513x^2 - 0.4847x - 0.0072$,

where y is the dark counts rate (kHZ) and x is the excess bias (Volt).

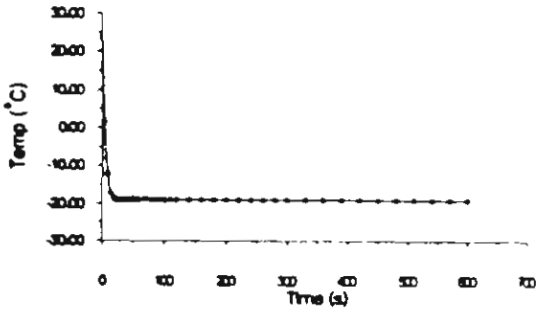


Figure 3. APD temperature variation.

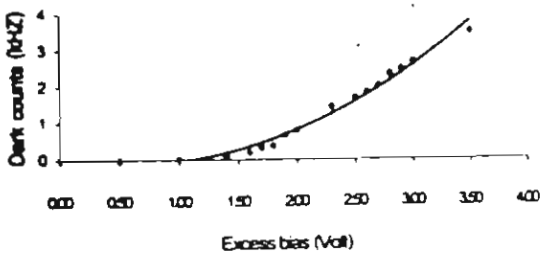


Figure 4. Dark counts versus excess bias (threshold 193V) @ -20 °C.

4. CONCLUSION

In this paper, we have carried out measurements on commercially silicon APD to implement it as single-photon counting in the first telecommunication window. The experimental results show that the simple but robust passive quenching circuit corporated with the high voltage controller, and proportional integral thermoelectric cooler are well suit to reduce the dark count rate and afterpulse at the low count rate. The APD module are potential for applications requiring high efficiency and high counting rate capability as, for instance, quantum cryptography, single molecule detection, fluorescent decays, etc. The active quenching circuit or the gated mode technique is preperable to use in the high counts rate for reducing the dead time and increasing the counting rate.

5. ACKNOWLEDGEMENTS

This work was supported by Kasetsart University Research and Development Institute under contract □.□. 12.43 and by the Thailand Research Fund under grant PDF 22/2543.

REFERENCES

[1] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Hanald Weinfurten, and Anton Zeilinger, Experimental Quantum Teleportation, *Nature* , **Vol.390**, pp. 575-579, 1997.

[2] 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.M. Simmons, *Phys. Rrv. Lett.***81** 3283, 1998.

[3] M. Ghioni, S. Cova, F. Zappa, and C. Samori, Compact Active Quenching Circuit for Fast Photon Counting with Avalanche Photodiodes, *Rev. Sci, Instrum.* **67**(10) 3440-3448, 1996.

[4] P.C.M. Owens, J.G. Rarity, P.R. Tapster, D. Knight, and P.D. Townsend, Photon Counting with Passively Quenched Germanium Avalanche, *Applied Optics* , **Vol.33**(30), pp. 6895-6901, 1994.

[5] P. Webb, R. McIntyre, and J. Conradi, Properties of Avalanche Photodiodes, RCA Review, EG&G Optoelectronics, Canada, 1974.

[6] Data Sheet, "Miniature DC to HVDC Converters", EMCO High Voltage Corporation , 1998.

[7] L. Demers, C30902S-DTC Test sheet, EG&G, Optoelectronics, Canada, 2000.

[8] T. Rafaa *et a*,Temperature Control of Avalanche Photodiodes using Thermo-electric Coolers, NASA Technical Memorandum 209689, 1999.

การทดลองวิทยาการเข้ารหัสลับเชิงควอนตัมโดยใช้สถานะควอนตัมของโฟตอนเดี่ยว

Experimental Quantum Cryptography Utilized Quantum States of Single Photons

สราชุธ เดชะปัญญา, พิทักษ์ พานทอง, สุวิกิตติ์ เชียงกา, นพปฏล สุทธิศิริ และเอกชัย หุ่นนิวัฒน์
S. Dechapunya, P. Panthong, S. Chiangga, N. Suttisiri and E. Hoonnivathana
Department of Physics, Faculty of Science, Kasetsart University, Bangkok 10900, Thailand.

บทคัดย่อ : วิทยาการเข้ารหัสลับเชิงควอนตัมเป็นวิธีการที่พิสูจน์ยืนยันแล้วว่าปลอดภัยที่สุด เนื่องจากใช้กฎควอนตัมฟิสิกส์ทำให้ตรวจสอบเมื่อมีการแทรกแซงระบบได้ทันที ในรายงานการวิจัยนี้กล่าวถึงทฤษฎีการเข้ารหัสลับเชิงควอนตัม การพัฒนาต้นแบบ และการตรวจจับโฟตอนเดี่ยว การทดลองนี้ใช้เกณฑ์วิธี BB84 ที่ใช้สถานะควอนตัมของโฟตอนเดี่ยวในการเข้ารหัสข้อมูล ระบบที่สร้างขึ้นสามารถสร้างรหัสลับที่นำมาใช้กับระบบวิทยาการเข้ารหัสลับทั่วไปได้

Abstract: Quantum cryptography is a technique the most provides verifiable secure key exchange between the sender and receiver. The security of the quantum cryptographic system is protected by the laws of quantum physics, which ensure that any eavesdropping can always be detected. In this paper we shall discuss the theory of quantum cryptography, its potential relevance, development of our prototype and the single photon detection. Our experimental system based on the BB84 protocol is enable to generate the key that can be used with any conventional cryptographic system.

Methodology: A simplified diagram of our quantum cryptographic system is shown in Fig. 1. It comprises of a transmitter (Alice) and a receiver (Bob). The attenuated pulse of the transmitter is generated by applying a 1.7 ns electrical pulse with a 1.43 MHz repetition rate to one of four low power laser diodes which is selected randomly with the pseudo-random number generated from a personal computer. The Coherence states $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle$ are generated by each laser operation well above the threshold. In our case the amplitude $|\alpha|^2 = 0.05$ was chosen, to give a photon number distribution per pulse according to $P_n = e^{-|\alpha|^2}|\alpha|^{2n}/n!$. A passive optical system sets the photon's polarization to $|H\rangle$, $|V\rangle$, $|+45\rangle$, or $|-45\rangle$ depending on whether the binary number is a "0" or a "1". It is comprised of a half wave plate (HW), two polarizing beam splitters (PBS), a beam splitter (BS) and lens. A pair of laser diodes in the upper paths is oriented so that the light beams overlapped at PBS have horizontal polarization, $|H\rangle$ (after transmission) and vertical polarization, $|V\rangle$ (after reflection). A pair of laser diodes on the lower path is also oriented similarly to the first pair, but a half wave plate rotates the plane of polarization by 45°. Therefore, they allow us to set the necessary $|+45\rangle$ and $|-45\rangle$ polarization states. The receiver consists of optical elements quite similar to the transmitter. A couple of avalanche photo-detectors (APD) in the upper path is used to analyze the $|H\rangle$ and $|V\rangle$ coming photons. A couple of APD in the lower path analyzed the $|+45\rangle$ and $|-45\rangle$ arriving photons. The interference filter (IF) $\Delta\lambda = \pm 5nm$ reduces the dark count of the system.

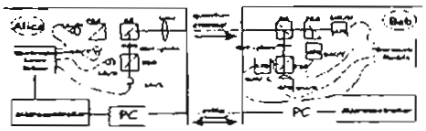


Fig.1 A simplified diagram of the quantum cryptography system.

Results, Discussion and Conclusion: The transmitter comprises of four laser diodes which, controllable to switch on-off one for all by a microcontroller (MCS-51). The pulse signal of our laser diodes measured by the 1GHz 4- channel color oscilloscope have width about 1.8 ns and very stable. We set the Hanbury-Brown and Twiss experiment to analyze the number of photons per laser pulse. The experimental data shown that the dim laser pulse has an average 0.05 photon per pulse. The optical setup of the transmitter comprises of a beam-splitter, two polarizing beam-splitter, a quarter wave plate, to assign the polarization states of photons according to BB84 protocol.

Our receiver contains of four Si-APD to detect the single photons and an optical setup, which consists of a beam-splitter, two polarizing beam-splitter, a quarter wave plate, to analyze the polarization states of photons from the transmitter. We observed the visibilities of the single photon polarization states coming from our transmitter are measured with Si-APD at the receiver are $V_H = 0.99$, $V_V = 0.99$, $V_R = 0.97$ and $V_L = 0.97$.

References: [1] Charles H. Bennett and Gilles Brassard. *Quantum cryptography: Public key distribution and coin tossing*. page 175-179, December 10-12, 1984. Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India.
[2] Charles H. Bennett and Gilles Brassard. *An update on quantum cryptography*. In G. R. Blakley and D. C. Chaum, editors, *CRYPT084*, pages 475-480. Springer, 1985. Lecture Notes in Computer Scitnce No. 196.
[3] Gilles Brassard, Charles H. Bennett and Arthur K. Eckert. *Quantum cryptography*. Scientific American, pages 26-33, October 1992.
[4] Richard J. Hughes et al., *Secure communications using quantum cryptography*, SPIE Proceedings 3076, 2 (1997).

Keywords: quantum cryptography, quantum information, secure communication, photon detection

อุปกรณ์กำเนิดเลขสุ่มโดยวิธีการทัศนศาสตร์ควอนตัม
Optical Quantum Random Number Generator

พิทักษ์ พานทอง[1], วัชระ ทองเสมอ[2], สุรศักดิ์ เชียงกา[1] และ นพปฎล สุทธิศิริ[1]
Pituk Panthong[1], Wadchara Thongsamer[2], Surasak Chiangga[1], Noppadon Suttisiri[1]
[1]Department of Physics, Faculty of Science, Kasetsart University, Bangkok 10903, Thailand
[2]Faculty of Liberal Arts and Science, Kasetsart University, Kamphaeng Saen, 73140, Thailand

บทคัดย่อ: ในงานวิจัยนี้ได้ทำการทดลองเพื่อวิเคราะห์ผลที่ได้จากอุปกรณ์กำเนิดเลขสุ่มโดยวิธีการทัศนศาสตร์ควอนตัม ซึ่งความสุ่มขึ้นอยู่กับผลจากการสุ่มของโฟตอนเดี่ยวที่ผ่านอุปกรณ์แยกลำแสงที่สมมาตร พบว่าค่าสหสัมพันธ์ของพัลส์เลเซอร์เป็น $g^2(0) < 1$ แสดงถึงผลทางควอนตัมของเลเซอร์พัลส์ และจากการวิเคราะห์เชิงสถิติแสดงถึงการสุ่มของอนุกรมของบิต

Abstract: We report the experimental verification of our constructed optical random number generator based on the random outcomes of a single photon incidents on a symmetry beam splitter. The correlation function measurements of the laser pulses yield $g^2(0) < 1$. This is in violation of a classical of light. The statistically analysis of a bits sequence indicate that it is random.

Methodology: The schematic representation of our optical random number generator experiment is shown in Fig1. An infrared laser diode 830 nm pulsed at the repetition rate of 1 MHz, 1.5 ns in width. The laser pulses are filtered by narrow band interference filter ($\Delta\lambda \sim 5$nm), and then impinges onto a 50: 50 beam splitter. Therefore the half of the incidence pulses is directed to avalanche photodiode, APD1, and the rest to APD2. The randomization of the photon statistics by symmetry probability for transmission and reflection beam splitter mainly consequence of inefficient collection of laser pulses, losses in the optical components and inefficient detection of photoelectric detector. A key feature of the laser light is that, the timing between the photons is random. The monobit test and the frequency test with in a block are used to test 10^4 bits yield the P- value > 0.01 and > 0.0, respectively. Therefore we conclude that the bits sequence is random.

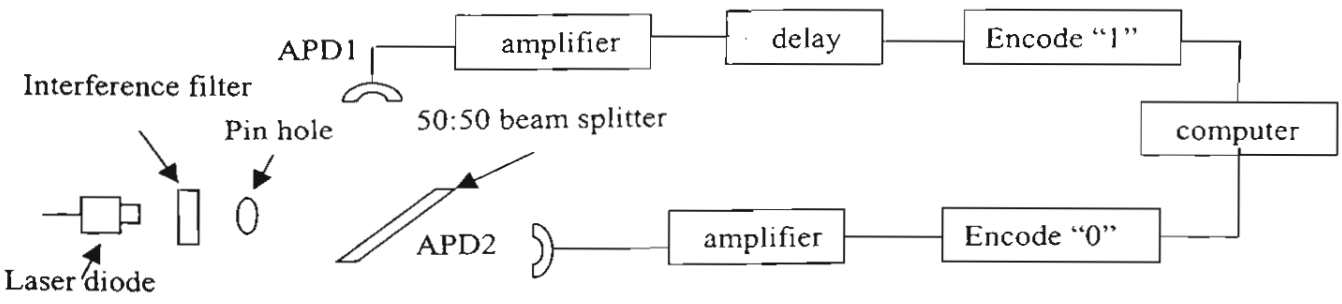


Figure.1. The schematic representation of the optical random number generator experiment.

Results, Discussion and Conclusion: We perform measurements of second order intensity correlation function of the laser pulses , $g^2(\tau)$ .The results are that the APD current with the time delay $\tau = 0$ gives $g^2(0) < 1$, but $g^2(\tau \neq 0) > 1$. This is a clear proof of the quantum nature of our laser pulses.
The monobit test and the frequency test with in a block are used to test 10^4 bits yield the P- value > 0.01 and > 0, respectively. Therefore we conclude that the bits sequence is random.

Acknowledgement: We would like to thank the financial support from the Graduate School, Kasetsart University and the Thailand Research Fund.

References: 1. A. Stefanov et al. " Optical Quantum Random Number Generator " quant-ph/ 99070062 Jul,1999.
2. T. Jennewein et al. " A Fast and Compact Quantum Random Number Generator " Rev. Sci. Intst. 71,1675-1680, 2000.
3. A. Rukhin et al. "A statistical test suite for random and pseudorandom number generators for cryptographic applications", NIST special publication 800-22, 2001

Keywords: Quantum optics, lasers, random number generator