S3-2

単一光子検出技術高度化とその応用展開
Si-APD による高効率単一光子検出器とその量子認証技術への応用
Advanced Single-Photon detector and Its Applications
High-Efficiency Single-Photon Detector Based on a Si-APD and Quantum Secure Authentication Experiment Using It

○行方直人[1], 大矢正人[2], 多田彬子[3], 高畑理希[3], 渡辺正孝[4], 松田健一[5], 前田穂[6], 西川淳[7,8], 井上修一郎[1]
*Naoto Namekata[1], Masahito Oya[2], Akiko Tada[3], Riki Takahata[3], Tadataka Watanabe[4], Kenichi Matsuda[5], Minoru Maeda[6], Jun Nishikawa[7,8], and Shuichiro Inoue[1]

Abstract: Single-photon detectors (SPD) in a wavelength range from visible to near infrared are essential for imaging and sensing that require the detection of weak optical signals, and especially quantum information and communications technology (QICT). In this research, a single photon detector based on a semiconductor device, i.e. a silicon avalanche photodiode (Si-APD) has been highly developed in order to satisfy requirements for the applications. The developed SPD was applied to quantum secure authentication (QSA). Then, we achieved the full implementation of a physical-key-based QSA protocol.

１．はじめに

光のエネルギー最小単位である単一光子でさえ検出可能な“単一光子検出器”（SPD）は，極微弱光検出を必要とする（レーザー）光センシングやイメージング，そして量子情報通信技術（QICT）に不可欠なものである．現状，SPD の候補として半導体素子：なだれフォトダイオード(APD)[1]や超伝導ナノ細線(SNSPD)[2]が挙げられる．前者は，実用的でありながら，可視光域で～70%程度の単一光子検出効率(PDE)を有している．一方，後者は極低温動作（液体ヘリウム温度以下）が必要であるものの，可視光から近赤外領域において 90%程度の超高効率を有し，かつ雑音計数（暗計数）が極めて低い．しかし，APD ベースの SPD によっても SNSPD 級の性能を実現できる可能性はある．

本研究では，先ず，シリコン（Si-）APD を用いた超高効率単一光子検出の実現を目指した．Si-APD の動作手法や雑音低減手法の改良等により，最終的に，SNSPD に匹敵する 80～85%（波長 650 ～ 780 nm）の PDE を達成した [3].

開発した高効率 SPD は既に量子安全認証(QSA) [4]へ応用展開された．物理鍵を用いた QSA プロトコルの完全実装は今回が初となり，しかも最も高い安全性基準をほぼ満たすことが明らかとなった．

２．ゲート動作 Si-APD による高効率単一光子検出

本研究では，波長 650 nm において 92±1%と非常に高い量子効率(QE)をもつ市販の一般用用途向け Si-APD を利用した．QE と PDE は一般的に同値にはならず，PDE は QE と ADP の積によって与えられる．ここで，ADP は電子なだれ降伏確率であり，単一光子吸収によって励起された電子 1 個が検出可能な電流出力へ返還される確率を指す[5]．これまでは，APD ベースの SPD は不完全な ADP によって高 PDE が実現されてこなかった．今回，矩形電圧パルスによるゲート動作を採用し、電圧パルスを独自開発の回路によって高振幅化することで ADP を増強し，高 PDE 実現を試みた．

試験 Si-APD は改良されたゲート動作型受動クエンチング回路(GPQC)によって駆動された．本回路では，ゲート用電圧パルス入力ポートに本来並列接続される 50 Ω終端抵抗が取り除かれており，ゲート用電圧パルス入力部は高入力インピーダンスとなっている．したがって，Si-APD のカソードへはゲート用電圧パルスの開放端電圧が印加され，ゲート用電圧パルス発生回路を変更せずとも 2 倍の振幅を持つ電圧パルス印加が可能となった．本改良型 GPQC によって，最終的に，幅 4 ns，振幅 40V のゲート電圧印加が可能となった．図 1 に直流オフセット(DCF)逆電圧に対する波長 650 nm における PDE の測定結果を示す．印加可能な最大の DCF

１：日本大学量子科学研究所、Institute of Quantum Science, Nihon University, ２：日本大学理工学研究所、 Research Institute of Science and Technology, Nihon University, ３：日本大学大学院理工学研究科、Graduate school of Science and Technology, Nihon University, ４：日本大学理工学部物理学科、Department of Physics, College of Science and Technology, Nihon University, ５：日本大学理工学部電気学科、Department of Electrical engineering, College of Science and Technology, Nihon University, ６：物質材料研究機構、National Institute for Materials Science, ７：国立天文台、National Astronomical Observatory of Japan, ８：アストロバイオロジーセンター、Astrobiology Center.

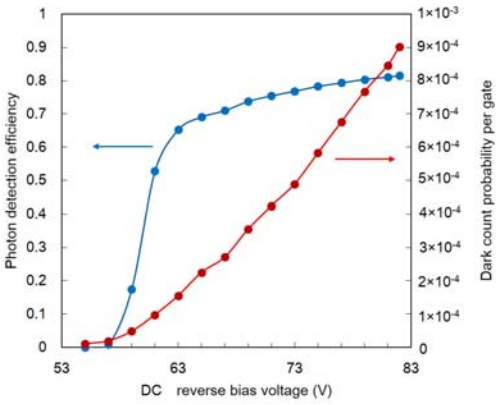

Figure 1. Photon detection efficiency as a function of the DC reverse bias voltage when the gate voltage pulse with an amplitude of 40 V and a duration of 4 ns was used.

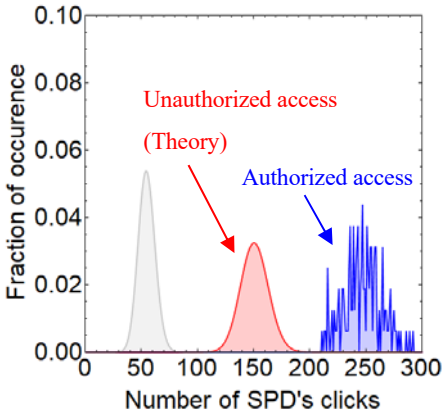

Figure 2. Distributions of the SPD's clicks with authorized and unauthorized (quantum cloning attack) accesses.

逆電圧 82V において, 82%の PDE を得た(ADP = 0.89). また，同図より，未だ PDE は完全に飽和しているとは言えず，より高振幅をもつゲートパルスの採用によって 85%以上の PDE が実現される可能性を示唆している.

3．量子安全認証の完全実装実験

量子安全認証(QSA)は正規通信者の認証を行う方法であり，無条件安全性が実現する可能性のある唯一の方法である[4]．QSAでは，多次元量子状態にある微弱コヒーレントパルス(平均光子数~1個)を物理鍵との接触媒体として用い，また，物理鍵には複製不可能性が保障されたもの(PUF)を用いる．以上2つの特徴によって，鍵の複製および不正アクセス者によるデジタルエミュレーション攻撃を防ぐことができる．QSAの原理検証実験[4]では，プロトコルの検証にとどまり，プロトコルの完全実装が可能かは明らかとされていなかった．また，仮定された安全性基準が低く，本プロトコルの優位性，有用性は再考される必要があった.

本研究では，開発した高効率SPDを用い，さらには可変形鏡(DM)による補償光学手法を用い，QSAプロトコルの完全実装を試みた．また，最も強力な不正アクセスであるUniversal quantum cloning (UQC)攻撃[6]を仮定し，安全性の検証を行った.

図2にQSAの実験結果を示す．同図は，物理鍵1つ(被認証者)の認証のために繰り返し行った試行回数10^4回の内，DMとSPDによる多次元量子状態識別器(認証者)がクリックした回数の分布を示している．正規アクセスの場合におけるクリック回数の分布はUQC攻撃を仮定した不正アクセスの場合のそれとよく離れており，認証を認める閾値を200クリック以上とすると，認証成功確率は99%，不正認証成功確率は5.9×10^{-4}となり，UQC攻撃を避けたQSAが可能であることが明らかとなった.

4．まとめ

本研究では，Si-APD によって SNSPD にせまる高効率単一光子検出を実現し，また，より高性能化が可能であることも明らかとした．本検出技術は量子安全認証へ応用され，UQC 攻撃をも避けられる QSA システムの構築に成功した.

謝辞

本研究は日本大学理工学部，理工学部プロジェクト研究助成 (2015-2016) を受けて実施されたものである.

参考文献

[1] N. Namekata, S. Adachi, and S. Inoue, "Ultra-Low-Noise, Gated Avalanche Photodiode for High-Speed Single-photon Detection at Telecommunication Wavelengths," IEEE Photo. Tech. Lett. **22**, 529 (2010).

[2] F. Marsili, *et.al*, "Detecting single infrared photons with 93% system efficiency," Nat. Photon. **7**, 210 (2013).

[3] A. Tada, N. Namekata, and S. Inoue, "Gated Silicon Avalanche Photodiode With 85% Single-Photon Detection Efficiency," *Single Photon Workshop 2015*, Geneva, Switzerland, (2015).

[4] S.A.Goorden, *et.al*, "Quantum-secure authentication of a physical unclonable key," Optica, **1**, 421, (2014).

[5] S. Suzuki, N. Namekata, K. Tsujino, and S. Inoue, "Highly enhanced avalanche probability using sinusoidally gated silicon avalanche photodiode," Appl. Phys. Lett. **104**, 041105 (2014).

[6] D.Bruss and C.Macchiavello, "Optimal state estimation for *d*-dimensional quantum systems," Phys.Lett. **A253**, 249 (1999).