

## 補償光学を用いた量子認証のシステム実験

## Quantum Secure Authentication system experiment using Adaptive Optics

日大量科研<sup>1</sup>, 国立天文台<sup>2</sup>, 総研大<sup>3</sup>, ABC<sup>4</sup>°大矢正人<sup>1</sup>, 行方直人<sup>1</sup>, 西川淳<sup>2,3,4</sup>, 井上修一郎<sup>1</sup>Nihon Univ.<sup>1</sup>, NAOJ<sup>2</sup>, SOKENDAI<sup>3</sup>, ABC<sup>4</sup>°Masahito Oya<sup>1</sup>, Naoto Namekata<sup>1</sup>, Jun Nishikawa<sup>2,3,4</sup>, Shuichiro Inoue<sup>1</sup>

E-mail: masahito.ooya@phys.cst.nihon-u.ac.jp

2014年、S.A.Goordenらによって、鍵に物理的複製不可能 (PUF) 鍵を使用し、鍵との接触媒体に空間位相変調器 (SLM) による光の多次元量子状態を利用した量子認証 (QSA) が提案された [1]。SLMを用いて光の量子状態の次元を $1100 \pm 200$ まで高めることによって、平均光子数を $230 \pm 40$ /光パルスと非常に高くした状態においても認証を達成している。

本研究では、繰り返し速度の向上のため、空間位相変調器 (SLM) (<60Hz) の代わりに変調速度の速い可変形鏡 (DM) (<1kHz) を使用している。量子認証システムでは、2台のDMと鍵、検出器による認証光学系を用い、データベース化と認証の2つの制御を行う。DM1での量子状態の多次元化によって、入射光は最終焦点面で検出するとスペckルパターンとなる。この時、鍵の後方に設置したDM2と焦点面検出器を用いたAOによって波面の復元を施すと、点像分布関数 (PSF) 状のパターンに近づくので、1つの鍵に合わせてDM1と2の制御パターン対をデータベースとして保存しておく。次に認証では、被認証者が鍵を認証光学系へ設置すると、データベースから2台のDMの制御パターン対を読み出す。そして、正規と非正規の鍵は、最終焦点面での単一光子検出器による光子の検出確率の差によって識別される。これまでに、我々は、1個の正規の鍵に対して制御パターン対を1組のみとした実証実験結果について報告した [3]。今回、認証の制御の自動化を図り、光源には十分に減衰したパルスレーザー ( $\lambda=655\text{nm}$ , パルス幅50ps, 5光子/パルス) を用いた。パルスレーザーの発振のタイミングでDMの制御パターン対をランダムに常に入れ替え、焦点面の単一光子検出器で光子検出を行う。システム自動化によって、DMのパターンの入れ替えが可能となり、3組のDMの制御パターン対をデータベースとして用いた量子認証システム実験を行った。Fig.1は、正規、非正規の鍵を使用した場合の最終焦点面における光子計数分布を示したものである。正規、非正規における光子計数分布は明瞭に分離されており、誤り確率は0.068%で正規鍵の認証に成功した。

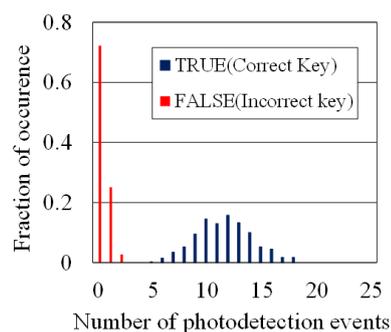


Fig. 1 Histogram of photon detection events with true and false key

謝辞 本研究は日本大学理工学部プロジェクト研究助成を受けて実施されたものである。

[1]S. A. Goorden *et.al.*, *Optica*, 1, 6, 421 (2014)

[2]M. Oya *et.al.*, *Optical review*, 22, 5, 736 (2015)

[3]第63回応用物理学会秋季学術講演会, 13p-B2-12 (2016)