»Ghost« ermöglicht sichere Kommunikation

Klassische Photonenkorrelationen und unpolarisiertes Licht im Fokus

Wissenschaftler am Institut für Angewandte Physik konzipierten und realisierten einen neuartigen Ansatz für eine sichere Nachrichtenkommunikation zwischen zwei Parteien. Ihre Erkenntnisse veröffentlichten sie im Fachmagazin »Physical Review Applied«.

Sichere Kommunikation ist derzeit ein wichtiges und herausforderndes Thema für den globalen digitalen Datenaustausch und gewährleistet die Interaktion vonInternet-of-Things-Geräten sowie die private Nachrichtenübermittlung zwischen zwei Parteien. Parallel zu den Bemühungen bei der Entwicklung von Quantencomputern sind sichere quantenkryptografische Systeme von aktuellem Interesse und diese Entwicklungen stehen auch im Mittelpunkt des EU-Flagship »QUANTUM« und an der TU Darmstadt im Zentrum des SFB »CROSSING« und des Profilbereichs Cybersecurity (CYSEC).

In einem kürzlich veröffentlichten Fachartikel hat die Gruppe Halbleiteroptik des Instituts für Angewandte Physik der TU Darmstadt einen anderen Ansatz verfolgt. Wie Professor Dr. Wolfgang Elsäßer erläutert, basiert ihre Idee im Wesentlichen auf drei wissenschaftlichen Säulen, der sicheren verschlüsselten Kommunikation, der Quantenoptik im Sinne von Hanbury-Brown und Twiss-Photonenkorrelationen, hier im Sinne von »Ghost«-Metrologietechniken, und der klassischen Optik im Sinne des Stokes'schen Formalismus und der Poincaré-Kugel.

Die Autoren konzipierten und realisierten einen neuartigen Ansatz für ein Nachrichtenkodierungsschema zwischen zwei Parteien, typischerweise »Alice« und »Bob« genannt, indem sie die unendlich große Anzahl von Polarisationszuständen auf der Poincaré-Kugel von unpolarisiertem thermischem Licht zusammen mit ihren Korrelationseigenschaften zur Tarnung und Rekonstruktion einer Nachricht nutzten und so »Ghost«-Polarisationskommunikation (GPC) realisierten – ein Name in Analogie zu anderen »Ghost«-Modalitäten (GM), also Messtechniken, die auf Photonenkorrelationen basieren, seien sie klassischer oder verschränkter Natur.

Markus Rosskopf, der wissenschaftliche Mitarbeiter in dem Projekt, untersuchte zunächst den Intensitätskorrelationskoeffizienten $g^{(2)}(\tau)$ von unpolarisiertem, breitbandigem, verstärktem Spontanemissionslicht (ASE), das von einem Erbium-dotierten Faserverstärker bei einer telekommunikationsüblichen Wellenlänge von 1.550 Nanometer emittiert wird. Er modifizierte dessen instantanen Polarisationszustand unter Verwendung verschiedener Polarisationsoptiken in den Strahlengängen einer Hanbury-Brown & Twiss-ähnlichen »Ghost«-Polarimetrieanordnung und detektierte $g^{(2)}(\tau)$ durch ultraschnelle Zwei-Photonen-Absorption in der Kathode eines Photomultipliers, um so die notwendige Zeitauflösung im Femto-Sekundenzeitbereich ($\approx 10^{-14}$ s) zur Verfügung zu haben. Diese Beobachtungen, die im Rahmen eines Modells verstanden und erklärt werden konnten, waren nun die Basis für die Realisierung eines neuartigen sicheren Nachrichtenkodierungsschemas.

Bob sendet nun die Hälfte seines korrelierten Photonenstrahls zu Alice. Mithilfe der Winkelposition einer Halbwellenplatte kodiert Alice darauf eine Nachricht und überträgt diesen nun mit der Botschaft aufgeprägten momentanen Polarisationszustand wieder zu Bob. Die getarnte Nachricht kann von ihm unter Zuhilfenahme der Winkelposition seiner Viertelwellenplatte eindeutig wiederhergestellt werden, indem er die Korrelationen zwischen dem Photonenstrahl von Alice und seinem Referenzstrahl misst. Durch Verwendung einer vereinbarten Kodierungstabelle kann er so die Bitwerte (»0« oder »1«) der von Alice kodierten Nachricht bestimmen.

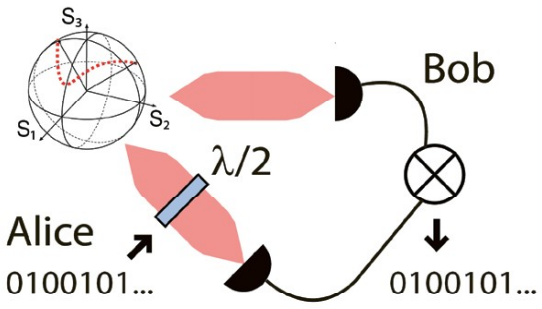
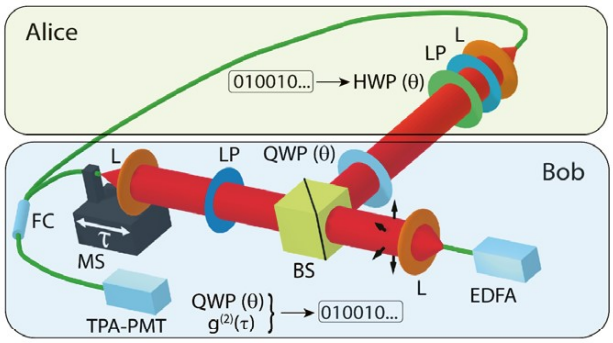


Illustration der Ghost Polarization Communication zwischen Alice und Bob mit der entsprechenden Bitsequenz, die Alice mithilfe der λ/2 Platte aufprägt und die Bob durch die Korrelationsmessung mit seinem Referenzstrahl rekonstruiert



Der experimentelle Aufbau für die »Ghost«-Kommunikations-Demonstration, die Polarisationskorrelationen von unpolarisiertem thermischem Licht aus einem Erbium-dotierten Faserverstärker ausnutzt

GPC ist die erste Proof-of-Principle-Demonstration einer sicheren, versteckten Kommunikation zwischen zwei Parteien, die auf Polarisationskorrelationen von klassischem Licht basiert; sie ergänzt Quanten- und Chaos-Kryptografie und befruchtet so den Austausch und die Diskussion zwischen diesen Bereichen. Durch dieses neuartige, in Analogie zu Ghost-Imaging und Ghost-Spektroskopie realisierte Kommunikationsverfahren werden nicht nur neue Wege für »Ghost«-Modalitäten eröffnet, sondern auch neue Einsichten in die Polarisation gewonnen, und dies mehr als 175 Jahre nach dem »Vater der Polarisation«, Sir Gabriel Stokes.

PROFESSOR DR. WOLFGANG ELSÄSSER

Die Publikation: Markus Rosskopf, Till Mohr, Wolfgang Elsäßer (2020): Ghost Polarization Communication, Phys. Rev. Appl. 13: 034062 (2020); https://doi.org/10.1103/PhysRevApplied.13.034062. bit.ly/3crBGB5