Quantum Authentication and Quantum Communication

P.W.H. Pinkse
MESA+ Institute for Nanotechnology, University of Twente, 7500AE Enschede, The Netherlands

The possible construction of large universal quantum computers forms a threat to most modern cryptography since algorithms exist that can break these cryptography algorithms on a sufficiently advanced quantum computer. Quantum communication at the same time offers a way out. However, quantum communication is vulnerable to man-in-the-middle attacks as long as authentication is not intrinsically solved.

A physical unclonable function (PUF) is a unique key which cannot be physically copied with existing technology. Multiple-scattering samples such as white paint or ceramic form good optical PUFs. We have demonstrated authentication by quantum-secure optical readout of a PUF [1] and more recently, we have devised a quantum communication scheme based on PUFs [2]. In order to investigate the limits of state-of-the-art nanofabrication techniques, we started making multiple-scattering media by direct laser writing. A new class of PUFs we realize in the form of complex integrated photonic circuits. These integrated photonic circuits can be read out at a distance, potentially solving the authentication problem in secure communication channels.

References

1. S. A. Goorden, *et al.*, Optica **1**, 421 (2014).
2. R. Uppu *et al.*, Quantum Sci. Tech. **4**, 04501 (2019).

Kwantumauthenticatie en kwantumcommunicatie

P.W.H. Pinkse
MESA+ Institute for Nanotechnology, University of Twente, 7500AE Enschede, The Netherlands

De mogelijke constructie van grote universele kwantumcomputers vormt een bedreiging voor de meeste moderne cryptografie, aangezien er algoritmen bestaan die deze cryptografie-algoritmen op een voldoende geavanceerde kwantumcomputer kunnen breken. Kwantumcommunicatie biedt tegelijkertijd een uitweg. Kwantumcommunicatie is echter kwetsbaar voor man-in-the-middle-aanvallen zolang de authenticatie niet intrinsiek is opgelost.

Een *physical unclonable function* (PUF) is een unieke fysieke sleutel die niet kan worden gekopieerd met de bestaande technologie. Meervoudige verstrooiende materialen zoals witte verf of wit keramiek vormen goede optische PUF's. We hebben authenticatie gedemonstreerd door kwantumveilige optische uitlezing van een PUF [1] en recenter hebben we een kwantumcommunicatieschema bedacht op basis van PUF's [2]. Om de grenzen van de modernste nanofabricagetechnieken te onderzoeken, zijn we begonnen met het maken van media met meervoudige verstrooiing door direct laserschrijven. Een nieuwe klasse PUF's realiseren we in de vorm van complexe geïntegreerde fotonische circuits. Deze geïntegreerde fotonische circuits kunnen op afstand worden uitgelezen, waardoor mogelijk het authenticatieprobleem in beveiligde communicatiekanalen wordt opgelost.

Referenties

1. S. A. Goorden, *et al.*, Optica **1**, 421 (2014).
2. R. Uppu *et al.*, Quantum Sci. Tech. **4**, 04501 (2019).