

## Projekt

## Ultraschnelle Quantenschlüssel-Verteilung durch Parallelisierung der Detektionskanäle (QuPAD)

Koordinator:	Dr. Andreas Bültter PicoQuant GmbH Rudower Chaussee 29 12489 Berlin Tel.: 030 1208820-0 Fax: 030 1208820-90 E-Mail: buelter@picoquant.com
Projektvolumen:	2,2 Mio. € (Förderquote 81,5%)
Projektlaufzeit:	01.11.2018 – 28.02.2021
Projektpartner:	➔ PicoQuant GmbH, Berlin ➔ WWU Münster, Physikalisches Institut, CeNTech II ➔ Entropy GmbH, München

## Die technische Grundlage für die Erschließung quantenphysikalischer Anwendungen

Die Erforschung neuer Quantentechnologien erfährt derzeit weltweit einen beträchtlichen Aufschwung. Dieser wird vor allem von den Erwartungen an die Leistungsfähigkeit des Quantencomputers gestützt. Doch auch andere Quantentechnologien versprechen erhebliche Fortschritte in den Bereichen Messtechnik, Sensorik, Medizintechnik oder Biotechnologie.

Die vielversprechendsten Anwendungen der Quantentechnologien sind jedoch kurzfristig nicht praktisch umzusetzen. Es fehlt hierfür die erforderliche Gerätetechnik, die in großen Teilen erst entwickelt werden muss. Die genutzten Quantenphänomene reagieren sehr empfindlich auf äußere Einflüsse und sind daher sehr kurzlebig. Ihre Bereitstellung und Kontrolle ist mit einem beträchtlichen apparativen Aufwand verbunden. Selbst dort, wo man bereits grundlegende Funktionen nachweisen konnte, ist die technische Beherrschung der Quantensysteme noch viel zu kostspielig und zu wenig robust für eine praktische Nutzung. Es gilt daher, in enger Zusammenarbeit zwischen den Herstellern der technischen Ausrüstungen und den Forschern in den Labors neue Geräte für den Einsatz in den Quantentechnologien zu entwickeln. Stabile und kostengünstige Systeme sollen die Aussichten auf eine erfolgreiche wirtschaftliche Nutzung der Quanteneffekte erheblich verbessern. Eine wesentliche Zielstellung der geförderten Projekte liegt darin, einheimische Unternehmen dabei zu unterstützen, sich als weltweit führende Ausrüster für Forschung und Entwicklung zu etablieren.



Bild 1: Die apparative Beherrschung von Quantenphänomenen für neue Anwendungen ist derzeit noch sehr kostenintensiv und benötigt hochqualifiziertes Personal. (Quelle: iStock.com/ Maartje van Caspel)

## Abhörsichere Quanten-Verschlüsselungsverfahren für die Kommunikation

Vor etwa 100 Jahren hat die Entwicklung der Quantenmechanik die Grundlagen für eine Reihe von revolutionären Techniken, wie z. B. die Halbleitertechnik, den Laser oder die Atomuhr gelegt. Heute erleben wir eine zweite Welle der Nutzbarmachung der Quantentechnologien, deren Kernstück die gezielte Manipulation, Übertragung und das Auslesen des Quantenzustandes einzelner oder gekoppelter Quantensysteme ist. Ein Beispiel für eine bereits relativ weit fortgeschrittene Anwendung ist die Quantenkommunikation und insbesondere die Quantenschlüssel-Verteilung (Quantum Key Distribution – QKD). Heutige Verschlüsselungsverfahren könnten durch Quantencomputer angreifbar werden. Zugleich bieten die Quantentechnologien die Lösung für dieses Problem: der Einsatz quantenkryptografischer Verfahren in der Kommunikation. Entsprechende Verfahren und Protokolle sind bekannt, leiden aber unter Reichweiten- und insbesondere Geschwindigkeitsproblemen in der Erzeugung von Verschlüsselungen, was ihren alltäglichen Einsatz heute noch unpraktikabel macht.

## Hohe Verschlüsselungsraten durch Parallelisierung der Detektionskanäle

In diesem Projekt sollen Komponenten entwickelt werden, mit denen sich Schlüssel in einem geeigneten QKD-Protokoll um Größenordnungen schneller als bisher erzeugen lassen. Dazu sollen Photonen, die in den meisten QKD-Protokollen die Quanten-Information tragen, mit höchster zeitlicher Präzision erfasst werden. Im Rahmen des Verbundvorhabens soll als erste Schlüsselkomponente ein Photonen-Detektor auf der Basis von supraleitenden Nanodrähten entstehen. Dieser soll eine so hohe Empfindlichkeit auf Photonen, dass sogar einzelne von ihnen detektiert werden können. Außerdem soll er Licht-Wellenlängen im Nah-Infrarot detektieren können, was ihn kompatibel zu bestehender Telekommunikations-Technik machen soll. Die zweite

Schlüsselkomponente stellt eine neuartige, schnelle Messelektronik für den Detektor dar, welche die Ankunftszeiten der detektierten, einzelnen Photonen auf den Billionsten Teil einer Sekunde genau bestimmen kann. Der zentrale Innovationsansatz besteht dabei darin, nicht nur den einzelnen Detektor in Bezug auf Detektionseffizienz, Geschwindigkeit und Zeitauflösung zu optimieren, sondern gleichzeitig den Detektor und die damit verbundene Messelektronik zu parallelisieren und für hohen Datendurchsatz auszuliegen. Dafür wird er viele höchst sensitive Detektionskanäle aufweisen, die voneinander unabhängig sind und parallel arbeiten. Mit diesen können in einem geeigneten QKD-Protokoll um Größenordnungen höhere Verschlüsselungsraten erzielt werden. Mit höheren Raten wäre der Aufbau eines High-Speed-Netzwerks möglich, in dem Nachrichten bzw. Daten ohne merkbare Zeitverzögerung sicher ausgetauscht werden können. Die avisierten Schlüsselkomponenten wären darüber hinaus für eine Vielzahl von Anwendungen einsetzbar, wie z. B. bildgebende Verfahren in der Optik und Biologie, Detektion von Fertigungsfehlern in der Prozesstechnik, „Deep Space Communication“, LIDAR, oder der Entwicklung des Quantencomputers.

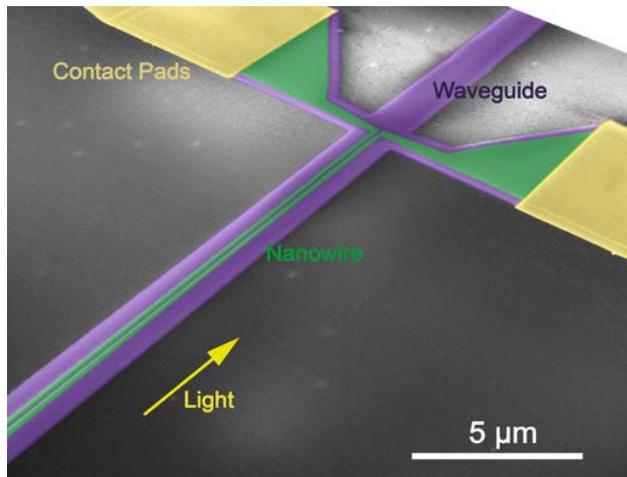


Bild 2: Supraleitender Nanodraht-Detektor (grün) auf einem nanophotonischen Wellenleiter (violett). Die elektrische Kontaktierung erfolgt über metallische Kontaktpads (gelb). (Quelle: WWU Münster)