PRESSEINFORMATION

Photonischer Quantenchip für schnelle und zuverlässige Zufallszahlengenerierung

Das BMBF fördert das Projekt CBQD – Chip-basiertes Quantenzufalls-Device – zur Forschung an quantensicherer Hochgeschwindigkeitskommunikation. Im Projekt CBQD wird ein kompakter Chip entwickeln, der in hoher Geschwindigkeit Zufallszahlen auf Basis von quanten-photonischen Effekten generiert und den Anforderungen der Common Criteria für die Sicherheit von IT-Produkten entspricht. Der Chip soll Grundlage für zahlreiche Anwendungen der IT-Sicherheit werden. Das Fraunhofer IPMS übernimmt im Projekt die Koordination und die QNRG-Chipintegration.

In der IT-Sicherheit sind Zufallszahlen von enormer Bedeutung, da sie für kryptografische Verfahren wie die Schlüsselerzeugung genutzt werden und so die Sicherheit von Daten in Bezug auf Vertraulichkeit, Integrität und Authentizität gewährleisten. Quantum-Zufallszahlengeneratoren (QRNGs) nutzen quantenmechanische Phänomene wie den Zerfall von Atomen oder das Photonen-Phasenrauschen von Laserquellen, um unvorhersehbare und zufällige Daten zu erzeugen und versprechen höchstmögliche Sicherheit, da die Ausgabewerte auf den quantenmechanischen Prinzipien der Unbestimmtheit und Superposition beruhen. Sie bieten sichere Zufallszahlengenerierung für zukünftige Kommunikationssysteme und können in verschiedenen Bereichen wie Behörden, Banken, kritischer Infrastruktur und im Internet der Dinge eingesetzt werden.

»Im Projekt soll ein kompakter QRNG-Chip mit einer Rauschbitrate von 5 Gbit/s entwickelt werden. Die Rauschbitrate ist ein entscheidender Faktor für die Geschwindigkeit in der Zufallszahlenerzeugung», erklärt Christoph Posenau, Projektleiter am Fraunhofer IPMS. »Ziel ist es, hohe Geschwindigkeit mit einer kompakten Bauform zu kombinieren und gleichzeitig den Anforderungen der Common Criteria AIS 20/31 PTG.3 zu entsprechen, einem Standard für Sicherheitsanforderungen an IT-Produkte des Bundesamts für Sicherheit in der Informationstechnik (BSI).«

Das Projekt zur Umsetzung des QRNG-Chips nutzt moderne Silizium-Germanium-Technologien zur Entwicklung elektrophotonischer integrierter Schaltungen (EPIC), um eine vollintegrierte Lösung mit Laserquelle, Wellenleiterstrukturen, Photodioden und analoger/digitaler Signalverarbeitung zu entwickeln. Die QRNG-Lösung wird im Projekt in zwei Anwendungen der Quantum Key Distribution (QKD) getestet. Das interdisziplinäre Projektteam bringt umfassende Expertise von Quantentheorie über Sicherheitsbeweise, Security-by-Design-Erfahrung für RNGs, Siliziumphotonik bis hin zu QKD-Systemen und deren Integration in Anwendungen mit.

Redaktion
Franka Balvin | Fraunhofer-Institut für Photonische Mikrosysteme IPMS | Telefon +49 351 8823-1144 |
Maria-Reiche-Straße 2 | 01109 Dresden | www.ipms.fraunhofer.de | franka.balvin@ipms.fraunhofer.de

Bei der Entwicklung des Chips wird das Fraunhofer IPMS mit vier Partnern und einem assoziierten Partner zusammenarbeiten:

- Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF
- Leibniz Universität Hannover (LUH)
- Leibniz-Institut für innovative Mikroelektronik (IHP)
- Technische Universität Darmstadt (TUDa)
- Adva Network Security GmbH (assoziierter Partner)

Über das Fraunhofer IPMS

Das **Fraunhofer-Institut für Photonische Mikrosysteme IPMS** erforscht mikroelektronische und mikromechanische Sensoren, Aktoren sowie aktive und passive Wellenleiterelemente. Auch drahtlose Mikrosysteme, Hochgeschwindigkeits-FPGA- und Mixed-Signal-ASIC-Design gehören zum Portfolio. Die elektronische Ansteuerung und Auswertung von Qubits und aktiven photonischen Einzelelementen bis hin zu Rechenbeschleunigern über dedizierte integrierte Elektronik (CMOS, BJT, BiCMOS) liegen dabei im Fokus. Zudem werden neue Materialien, Prozesse und Integrationskonzepte für Kryoelektronik sowie supraleitende Metallisierungen erforscht.

Bildmaterial

Im BMBF-geförderten Projekt CBQD – Chip-basiertes Quantenzufalls-Device wird ein kompakter Chip entwickeln, der in hoher Geschwindigkeit Zufallszahlen auf Basis von quanten-photonischen Effekten generiert und den Anforderungen der Common Criteria für die Sicherheit von IT-Produkten entspricht.