

PRESS RELEASE

PRESSEINFORMATION

17.06.2026 || Seite 1 | 4

Quanten-Zufallszahlengenerator (QRNG) als 19-Zoll-Racksystem und Online-Service-Plattform

Fraunhofer IPMS stellt Q-Dice vor: Quanten-Zufallszahlengenerator liefert Multi-Gbit/s echte Zufälligkeit für sicherheitskritische Anwendungen

Das Fraunhofer-Institut für Photonische Mikrosysteme IPMS präsentiert Q-Dice, einen Quanten-Zufallszahlengenerator (QRNG), der echte Zufälligkeit aus Quanten-Vakuumfluktuationen gewinnt. Das System erzeugt echte Zufallszahlen mit Bitraten von über 4 Gbit/s auf Basis von intrinsisch zufälligen und unbeeinflussbaren Quanteneffekten. Im Vergleich zu bestehenden Verfahren basiert Q-Dice nicht auf potenziell angreifbaren Algorithmen und ermöglicht deutlich höhere Datenraten. Dadurch eignet sich das System insbesondere für sicherheitskritische Anwendungen. Die Qualität der erzeugten Zufallszahlen wurde mit etablierten und international anerkannten Testverfahren wie BSI AIS 20/31 und der Test-Suite NIST SP 800-22 validiert.

Echte Zufälligkeit ist eine zentrale Voraussetzung für moderne kryptografische und sicherheitskritische Systeme, in denen deterministische oder unsichere Zufallszahlengeneratoren Schwachstellen in Verschlüsselung und Authentifizierung verursachen können. Durch die Messung inhärent unvorhersagbarer Quanten-Vakuumfluktuationen erzeugt Q-Dice vom Fraunhofer IPMS Quanten-Entropie für eine Vielzahl von Anwendungen, darunter sichere Kommunikation, Datenverschlüsselung (z.B. mittels QKD oder PQC), Authentifizierung und Zugriffsmanagement sowie großskalige Simulationen.

Das System ist mit einem starken Fokus auf Sicherheitsanforderungen konzipiert. Es erfüllt die strengen Anforderungen des Bundesamts für Informationssicherheit (BSI) gemäß AIS 20/31 und wird mit EAL3 Level (Evaluation Assurance Level) und als PTG 3 (Physical Random Number Generator) eingestuft, was einen wichtigen Beweis für die Sicherheit des Systems darstellt.

»Mit Q-Dice machen wir hochwertige Quanten-Zufälligkeit praktisch nutzbar und zugänglich«, sagt Dr. Alexander Noack, Bereichsleiter Data Communication & Computing am Fraunhofer IPMS. »Unsere Technologie steht sowohl als robustes 19 Zoll Rack System für den Einsatz in eigener Infrastruktur zur Verfügung als auch über unsere Online-Entropy-as-a-Service Plattform. Damit reduzieren wir die Hürden für den Einsatz quantenbasierter Sicherheit deutlich.«

QRNG-Kompetenzen am Fraunhofer IPMS

Um maximale Zuverlässigkeit zu gewährleisten, bündelt das Fraunhofer IPMS alle zentralen Kompetenzen im eigenen Haus und ermöglicht so eine durchgängige

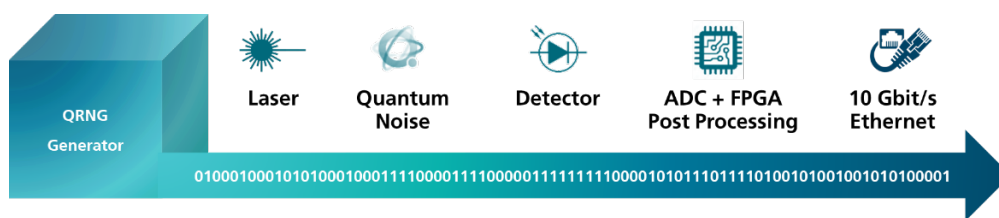
FRAUNHOFER-INSTITUT FÜR PHOTONISCHE MIKROSYSTEME IPMS

Entwicklung von der Photonik bis zur Systemintegration:

- Design von Laser- und optischen Front-End-Systemen zur stabilen Erzeugung und Kontrolle von Quantenrauschen
- Low-noise Analog-Front-End (AFE) zur Detektion von Quanten-Vakuumfluktuationen
- Hochgeschwindigkeits-Datenerfassung (Analog-Digital-Umsetzung – ADC) sowie FPGA-basierte Zufallsextraktion und Nachverarbeitung
- Systemintegration mit Hochdurchsatzschnittstellen, einschließlich 10 Gbit/s Ethernet

PRESSEINFORMATION

17.06.2026 || Seite 2 | 4



Fraunhofer IPMS QRNG Kompetenzen
©Fraunhofer IPMS

Dieser Ende-zu-Ende-Ansatz gewährleistet eine präzise Kontrolle über die Qualität, die Stabilität und die Leistungsfähigkeit der Entropiegewinnung. Dieselbe physikalische Rauschquelle bildet die Grundlage sowohl für den hardwarebasierten als auch für den cloudbasierten Zugang zu Quantenentropie.

Zwei Bereitstellungsmodelle: Hardware oder Cloud-Zugang

Das Fraunhofer IPMS bietet Q-Dice in zwei Konfigurationen an, um unterschiedliche Einsatz- und Betriebsanforderungen zu unterstützen:

1. Q-Dice Hardware 19-Zoll-Rack-System

Eine All-in-One-Hardwarelösung für den Einsatz in Rechenzentren und On-Premises-Umgebungen.

Q-Dice Spezifikationen

- Zufallsbitrate: 4,1 Gbit/s
- All-in-One-Lösung
- 19-Zoll-Rack-System (andere Formfaktoren auf Anfrage verfügbar)
- 10G Ethernet-Schnittstelle (weitere Schnittstellen auf Anfrage)
- Entwickelt für Integrationsumgebungen mit hohem Durchsatz und evaluiert nach BSI AIS 20/31 sowie der NIST SP 800-22 Test-Suite

2. Online QRNG on Demand (Entropie als Service)

PRESSEINFORMATION17.06.2026 || Seite 3 | 4

Eine sichere Online-Schnittstelle ermöglicht direkten Zugriff auf quantengenerierte Zufälligkeit, ohne dass eine spezielle Hardwareinstallation erforderlich ist. Der Service ermöglicht eine schnelle Evaluierung, Prototypenentwicklung sowie die skalierbare Integration von Quantenentropie in Softwaresysteme und cloudbasierte Anwendungen.

Mit dem Übergang der Technologie in die Implementierungsphase setzt das Fraunhofer IPMS auf kollaboratives Wachstum. »Unser Ziel ist es, gemeinsam die Messlatte für Sicherheit und Vertrauen im digitalen Zeitalter weiter anzuheben. Daher laden wir Partner ein, die Technologie zu testen und gemeinsam Anwendungen für die Praxis zu entwickeln«, ergänzt Noack abschließend.

Weitere Informationen zu QRNG-Technologien und Kompetenzen am Fraunhofer IPMS finden Sie unter: [Quantum Random Number Generation \(QRNG\) – Fraunhofer IPMS](#)

Über das Fraunhofer IPMS

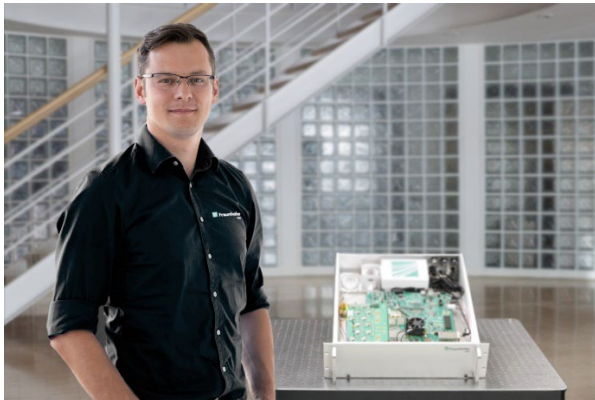
Das Fraunhofer IPMS ist ein international führender Forschungs- und Entwicklungsdienstleister für elektronische und photonische Mikrosysteme. Unsere Technologien finden Anwendungen in Industrie, Mobilität sowie Biotechnologie und Medizintechnik. Zugleich adressieren wir zentrale Zukunftsfelder wie Quantentechnologien und neuromorphes Computing. Mit unserer Forschung im Bereich grüner Mikroelektronik leisten wir Beiträge zu einer ressourcenschonenden und nachhaltigen Welt.

Der Geschäftsbereich Data Communication und Computing (DCC) entwickelt als Experte für sichere Datenkommunikationslösungen innovative Technologien in den Zukunftsfeldern IP-Cores, Li-Fi (lichtbasierte Datenübertragung) und Quantum Technologies. Diese Entwicklungen ebnen den Weg für neuartige und sichere Kommunikationslösungen in Schlüsselindustrien wie Mobilität, Telekommunikation, Industrieautomation oder der Energieversorgung.

Bildmaterial

PRESSEINFORMATION

17.06.2026 || Seite 4 | 4



Dr. Alexander Noack neben QRNG R19" Demonstrator
©Fraunhofer IPMS