VOL. 59 JULY 2025

NTU Q

HIGHLIGHTING NEWS

THE MOST TRUSTWORTHY RANDOM-NUMBER GENERATOR

Researchers at the U.S. National Institute of Standards and Technology (NIST) have developed the most verifiable and tamper-proof quantum random-number generator (QRNG) to date. Building on their 2018 photon entanglement protocol, they now integrate blockchain-based timestamping to log every step in the generation process, enabling full public traceability. Their system emits pairs of entangled photons whose polarization measurements—performed at spatially separated stations—yield inherently unpredictable bit strings, as dictated by quantum mechanics. The measurement settings are chosen randomly and independently to prevent any causal interference, ensuring the randomness is both fundamental and demonstrable. Compared to the original version, the upgraded setup is 30× faster, producing 512 random bits in 20 seconds. This work demonstrates how quantum and cryptographic technologies can jointly create trustworthy public randomness, with implications for cryptography, clinical trials, lotteries, and digital governance.

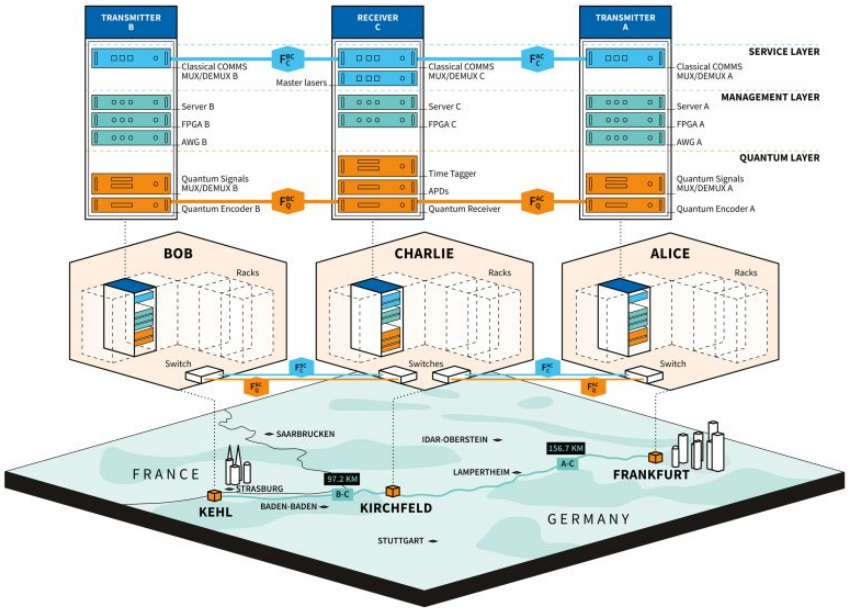
READMORE

Long-distance coherent quantum communications

Toshiba Europe has achieved a major milestone by successfully deploying coherent twin-field quantum key distribution (TF-QKD) over a **254 km commercial telecom fiber** in Germany, using **standard semiconductor components** and operating at **room temperature**. The system, for the first time outside the lab, sustained stable quantum-phase coherence and securely distributed cryptographic keys at **∼110 bits/s**, demonstrating a quantum-safe communication over national-scale telecom infrastructure via Deutsche Telekom's network.

This achievement addresses a long-standing barrier: previous systems required cryogenic cooling and specialized equipment to preserve coherence of phase-encoded quantum signals. The new setup uses **off-the-shelf avalanche photodiodes**, eliminating the need for complex and costly low-temperature apparatus. The results confirm that coherent quantum communications, including twin-field QKD, can now be scaled up and integrated into **existing colocation data centers**, marking a critical step toward a **global quantum internet**.

The work underscores the security advantage of TF-QKD—the provable protection derived from quantum physics—and the practicality of deploying it at scale without laboratory-grade equipment. Co-lead authors included Mirko Pittaluga and Robert Woodward of Toshiba Europe, with participation from GÉANT, PSNC, and Anglia Ruskin University.



READMORE

READMORE

計畫補助單位：NSTC 國家科學及技術委員會 National Science and Technology Council

IBM Quantum Computer Hub at National Taiwan University

Rm.711, Dept. of Physics /Center for Condensed Building

No. 1, Sec.4 Roosevelt Rd., Da'an Dist. Taipei City 106319, Taiwan

ntuq2018@gmail.com :+886 2-33669928 http://quantum.ntu.edu.tw/