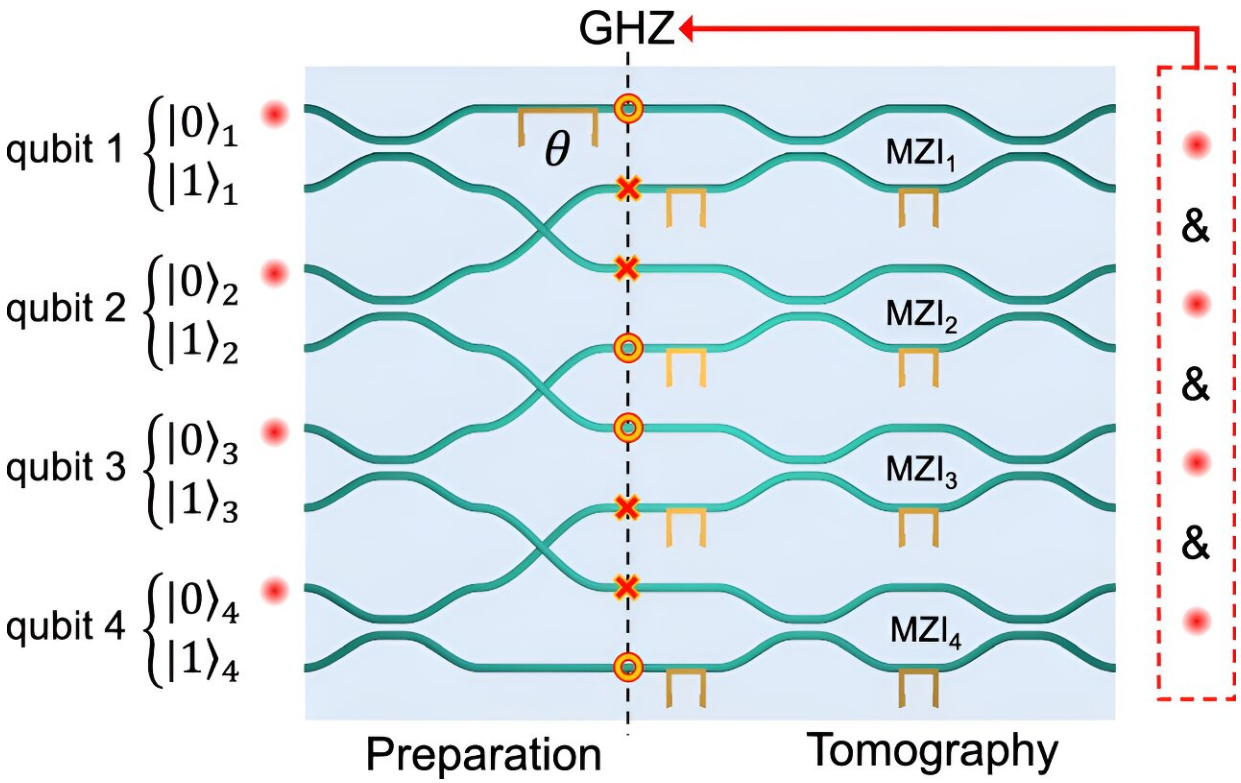
Chip that entangles four photons opens up possibility of inviolable quantum encryption

August 12 2024, by José Tadeu Arantes



Integrated path-encoded 4-GHZ generator. Credit: *npj Quantum Information* (2024). DOI: 10.1038/s41534-024-00830-z

Unlike classical encryption, which relies on mathematical algorithms, quantum encryption assures security based on physical principles. Detection of espionage or interference is guaranteed by unavoidable

alteration of the quantum states involved.

Comparisons between the two systems yield impressive results. Classical supercomputers would currently take thousands of years to break strong encryption, but it will be possible to decipher the same codes in seconds with sufficiently powerful quantum computers.

"This highlights the urgent need to develop and implement quantum security protocols that are immune to such capabilities," said Paulo Henrique Dias Ferreira, a researcher in the Department of Physics at the Federal University of São Carlos (UFSCar) in São Paulo state, Brazil.

During a postdoctoral internship at the Polytechnic University of Milan in Italy, Ferreira worked with the group led by Professor Roberto Osellame and contributed significantly to the creation and characterization of entangled four-photon GHZ (Greenberg-Horne-Zeilinger) states on a photonic chip. The research is published in the journal *npj Quantum Information*.

"The study combined quantum dot technology with glass photonic circuits, representing a milestone in device enhancement and integration, and opening up new possibilities for secure and efficient quantum communication," Ferreira said.

In the field of quantum information theory, a GHZ state is a type of entangled state that involves at least three subsystems (particle states, qubits or qudits). It was first studied in the late 1980s by Daniel Greenberger, Michael Horne and Anton Zeilinger. In this study, the circuits were written on a glass chip by femtosecond laser machining, creating three-dimensional (3D) waveguides that permitted precise photon manipulation.

"We chose production using a glass matrix because it was easily

prototyped. In addition, fabrication in a single stage produces 3D waveguides, unlike conventional lithography or electron beam writing. Circuit reconfigurability, obtained by means of thermal shifters, permits fine-tuning of the photons' optical phases, which is essential for the desired overlap," Ferreira said.

He used an analogy to explain how the device performs its cryptographic function. "Imagine you have four coins. In the normal state, each coin can be independently in heads or tails position when tossed randomly, but in the entangled GHZ state, all four photons are connected in a special way: when observed, all the coins are heads or tails, and a mixed combination never occurs.

"This state can be described mathematically as a quantum overlap in which each photon is entangled with the other three, with no classical analog. The connection is so strong that when you verify one photon, you instantly know the state of the other three, whatever the distance between them. In the coin analogy, once you've discovered that one coin is heads [and not tails], all the others must be heads," he said.

The phenomenon can be used to implement quantum secret sharing systems, in which a regulator securely shares a key with several participants. Any attempt at unauthorized access alters the quantum correlations, permitting immediate detection.

"For example, if an intruder tries to measure the state of one of the particles in order to obtain information about the key, the measurement will unavoidably make the quantum state of that particle collapse and alter the original quantum correlation between all the particles involved. When the legitimate participants in the protocol compare part of their data, they can detect discrepancies caused by this interference," he explained.

According to Ferreira, the use of GHZ states in commercial transactions will not only strengthen the security of communications but also offer a robust mechanism for detecting intruders, which is essential to protect sensitive data in an increasingly digital and interconnected world.

"Quantum systems that use GHZ states and other entanglement protocols offer a solution that can't be broken even by the most advanced quantum computers, because any attempt to interfere in a quantum channel alters the state of the particles involved, permitting immediate detection of any intruder," he said.

The article demonstrates the feasibility of generating high-fidelity entangled GHZ states in a photonic chip, paving the way for large-scale production of quantum devices.

"With continuous advances, we can expect these systems to be integrated into communications and computing infrastructures, leading to a new era of security and efficiency," he said.

More information: Mathias Pont et al, High-fidelity four-photon GHZ states on chip, *npj Quantum Information* (2024). DOI: 10.1038/s41534-024-00830-z

Provided by FAPESP