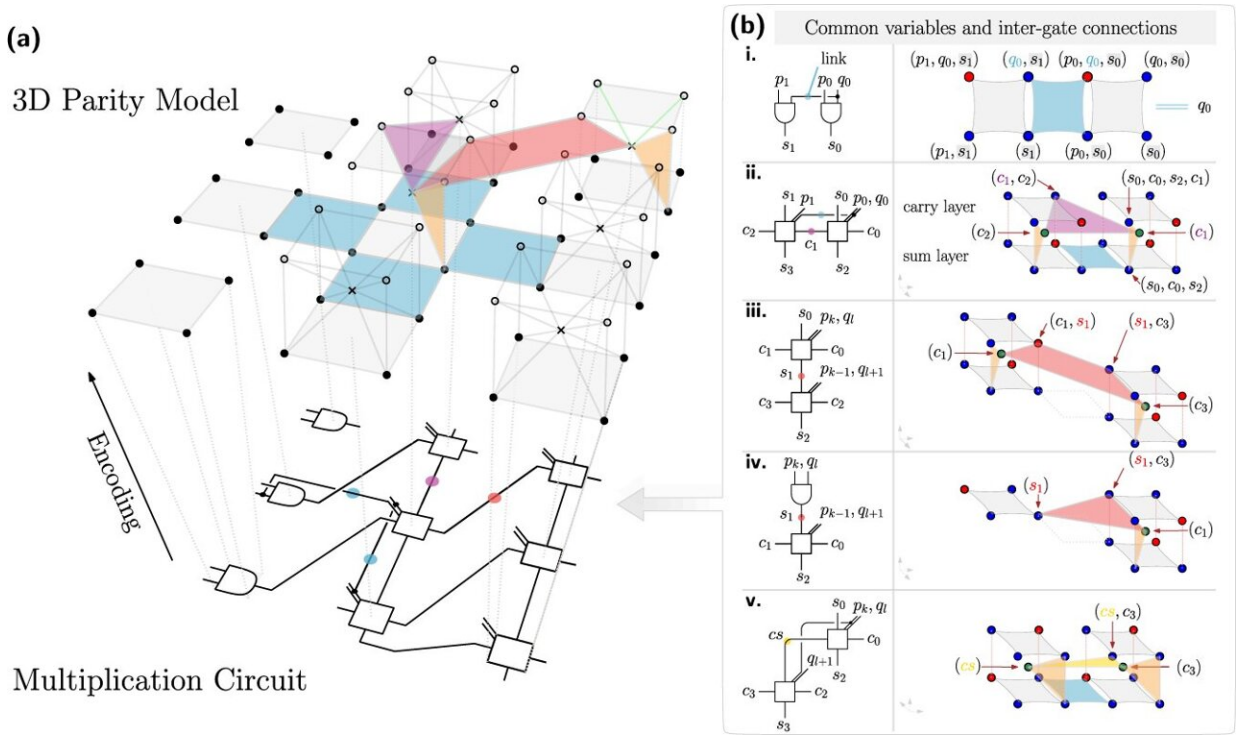
A blueprint for a quantum computer in reverse gear

May 4 2023



Blueprint for parity factorization—Three-dimensional layout. a The multiplication circuit is mapped onto an array of physical qubits arranged on three layers of a 3D lattice. Dots and crosses represent qubits on different layers while faces represent constraints. Beside boundaries, the whole architecture can be constructed from repeating unit cell consisting of nine qubits connected to neighboring cells via additional constraints (blue, red, violet, yellow, orange). For illustrative purposes, only a selected number of qubits and constraints are displayed. b Building instructions. Each connection between logical gates translates into 3-body or 4-body parity constraints (blue, red, violet, yellow). The device is programmable in the sense that a given bi-prime n can be encoded by

imposing additional 2-body constraints (a green). Thus the ground state $|n=pq\rangle$ reveals the factors p and q. Credit: *Communications Physics* (2023). DOI: 10.1038/s42005-023-01191-3

Large numbers can only be factorized with a great deal of computational effort. Physicists at the University of Innsbruck, Austria, led by Wolfgang Lechner are now providing a blueprint for a new type of quantum computer to solve the factorization problem, which is a cornerstone of modern cryptography. The research was recently published in *Communications Physics*.

Today's computers are based on microprocessors that execute so-called gates. A gate can, for example, be an AND operation, i.e., an operation that adds two bits. These gates, and thus computers, are irreversible. That is, algorithms cannot simply run backwards. "If you take the multiplication 2x2=4, you cannot simply run this operation in reverse, because 4 could be 2x2, but likewise 1x4 or 4x1," explains Wolfgang Lechner, professor of theoretical physics at the University of Innsbruck. If this were possible, however, it would be feasible to factorize large numbers, i.e., divide them into their factors.

Martin Lanthaler, Ben Niehoff and Wolfgang Lechner from the Institut für Theoretische Physik at the University of Innsbruck and the quantum spin-off ParityQC have now developed exactly this inversion of algorithms with the help of quantum computers. The starting point is a classical logic circuit, which multiplies two numbers. If two integers are entered as the input value, the circuit returns their product. Such a circuit is built from irreversible operations. "However, the logic of the circuit can be encoded within ground states of a quantum system," explains Martin Lanthaler from Wolfgang Lechner's team. "Thus, both multiplication and factorization can be understood as ground-state

problems and solved using quantum optimization methods."

Superposition of all possible results

"The core of our work is the encoding of the basic building blocks of the multiplier circuit, specifically AND gates, half and full adders with the parity architecture as the ground state problem on an ensemble of interacting spins," says Martin Lanthaler.

The coding allows the entire circuit to be built from repeating subsystems that can be arranged on a two-dimensional grid. By stringing several of these subsystems together, larger problem instances can be realized. Instead of the classical brute force method, where all possible factors are tested, quantum methods can speed up the search process: To find the ground state, and thus solve an optimization problem, it is not necessary to search the whole energy landscape, but deeper valleys can be reached by "tunneling."

The current research work provides a blueprint for a new type of quantum computer to solve the factorization problem, a cornerstone of modern cryptography. This blueprint is based on the parity architecture developed at the University of Innsbruck and can be implemented on all current quantum computing platforms.

More information: Martin Lanthaler et al, Scalable set of reversible parity gates for integer factorization, *Communications Physics* (2023). DOI: 10.1038/s42005-023-01191-3

Provided by University of Innsbruck