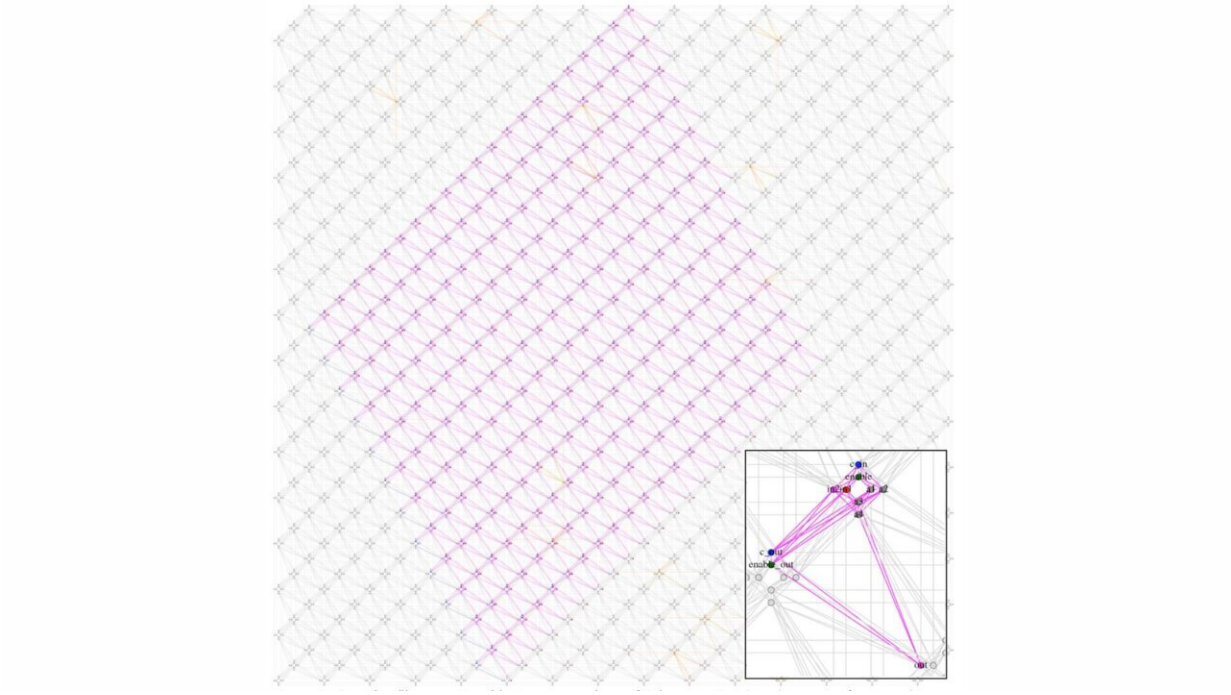
Quantum annealers and the future of prime factorization

February 21 2024, by Tejasri Gururaj



Grey dots/lines: 5760-qubit Pegasus topology of Advantage 4.X QAs (courtesy of D-Wave). Violet dots/lines: Subgraph used by the most space-efficient modular encoding for a 21x12-bit multiplier mentioned in the study. Orange dots/lines: Faulty qubits & couplings in the HW of the Advantage 4.1 machine used in the study. Credit: Jingwen Ding et al

Researchers at the University of Trento, Italy, have developed a novel approach for prime factorization via quantum annealing, leveraging a

compact modular encoding paradigm and enabling the factorization of large numbers using D-Wave quantum devices.

Prime factorization is the procedure of breaking down a number into its prime components. Every integer greater than one can be uniquely expressed as a product of prime numbers.

In cryptography, prime factorization holds particular importance due to its relevance to the security of encryption algorithms, such as the widely used RSA cryptosystem.

The process of prime factorization becomes challenging because of the nature of prime numbers, and it gets even more complicated as the numbers being factored become bigger, leading to a vast number of possibilities to consider.

The impracticality of efficiently factoring large numbers ensures the integrity of encrypted communication. The robustness of these cryptographic systems relies on the computational complexity of prime factorization, making it a crucial component in safeguarding sensitive information in the digital age.

If someone can efficiently factorize the product of two large prime numbers, they could potentially break the security of cryptographic systems. Understanding and advancing techniques for prime factorization contribute to ensuring the robustness of cryptographic protocols and safeguarding sensitive information in digital communication.

In a new study published in *Scientific Reports*, researchers led by Prof. Roberto Sebastiani from the University of Trento, Italy, aimed to tackle this process using quantum annealers. The team also consisted of Jingwen Ding and Giuseppe Spallitta, Ph.D. students at the University of

Trento.

"As a computer scientist who has spent a whole career developing classical procedures for solving computationally hard logical and optimization problems, I was very intrigued to deal with a technology like quantum annealing based on a computing paradigm far from anything I had encountered before," Prof. Sebastiani told Tech Xplore.

Quantum annealers

Quantum computers are uniquely suited for prime factorization problems due to their ability to perform parallel computations and exploit quantum phenomena. Specifically, quantum annealers, like those from D-Wave, are designed to tackle optimization problems by searching for optimal solutions among a vast number of possibilities simultaneously.

In the context of prime factorization, where finding the prime factors involves exploring numerous combinations quickly, the inherent parallelism of quantum computing offers a potential advantage.

Quantum annealers leverage quantum phenomena like quantum superposition and quantum tunneling to explore multiple solutions concurrently, making them well-suited for prime factorization problems. This parallel exploration of possibilities can significantly enhance the efficiency of searching for prime factors compared to classical algorithms.

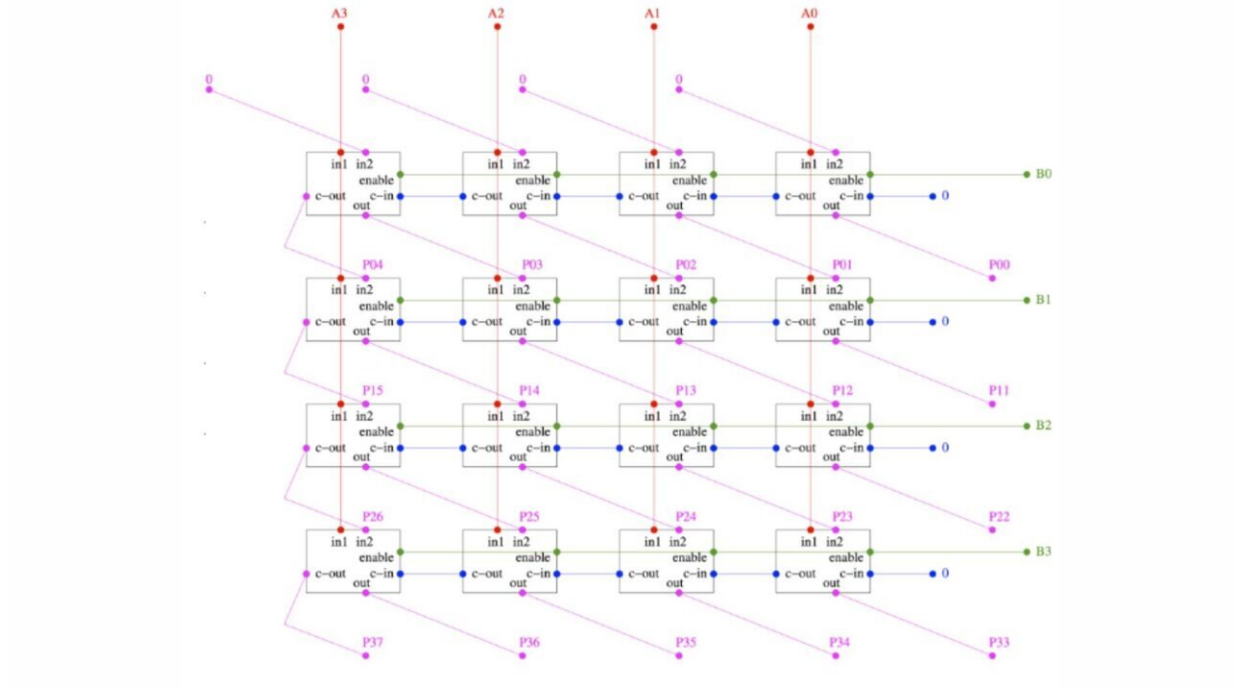
Compact encoding

The research has a two-fold nature. In the first aspect of their work, the researchers achieved a breakthrough by developing a compact modular

encoding of a 21×12-bit binary multiplier circuit directly into a single 8-qubit module within the Pegasus topology of D-Wave's quantum annealers.

Think of the Pegasus topology as a web connecting qubits, determining how data flows.

"The game changer in this work—which came out as a positive surprise to us—was the successful encoding of a controlled full-adder (CFA) sub-circuit into a single 8-qubit module of the Pegasus Quantum Annealer topology," explained Prof. Sebastiani.



Schema of a modular 4x4 multiplier with 16 CFA modules. Credit: *Scientific Reports* (2024). DOI: 10.1038/s41598-024-53708-7

CFA is a quantum sub-circuit that performs 1-bit addition operations under specific control conditions, which the team encoded into a module of the annealer's topology using Optimization Modulo Theories (OMT), a technology combining logical reasoning and optimization.

Unlike past approaches that overlooked the system's layout, the team utilized OptiMathSAT, their Optimization Modulo Theories tool, to craft an encoding well aware of the topology. This demonstrated the efficiency of their approach and marked a significant advancement in encoding techniques for quantum annealers.

The modularity of their encoding approach is a game-changer. They demonstrated the capability of encoding into the annealer the factorization of up to the number 8,587,833,345 into the product of two prime numbers, 2,097,151 and 4,095. This marks the largest factorization problem ever encoded into a quantum annealer using their novel method.

"We noticed two key facts. We can decompose an n×m-bit multiplier circuit into a matrix of interconnected CFA sub-circuits, and we can align it with the Pegasus lattice of 8-qubit modules," explained Prof. Sebastiani.

This allowed the researchers to create a structure that can scale effortlessly with the growth of qubit numbers in future quantum annealer chips.

Experimental factorization

In the second phase of their research, the team conducted an extensive experimental evaluation on a D-Wave Advantage 4.1 quantum annealer. The goal was to investigate the actual solving of encoded PF problems and assess the capabilities of the quantum annealer in practice.

"Overall, due to faulty qubits and limited QUPU-time resources, 8,219,999 = 32,749×251 was the highest prime product we were able to factorize. To the best of our knowledge, this is the largest number ever factorized employing a quantum device without relying on external search or preprocessing procedures run on classical computers," explained Prof. Sebastiani.

The achievement holds significant implications for quantum computing and its applications. The researchers showcased progress in solving complex computational problems, proving that substantial advancements are possible even with the limitations of current quantum annealer hardware.

One of the challenges in this work is that with each prime factorization problem having at most two solutions (e.g., 35=7×5 or 35=5×7), the quantum annealer needs to search for these global minima in an exponentially vast solution space.

Prof. Sebastiani elaborated, "This is akin to finding a needle in a haystack. Luckily, many annealing techniques and tricks are available to cope with these problems, but it took a lot of practice to get satisfactory results."

Beyond factorization

Prof. Sebastiani emphasized the potential to extend the use of these devices beyond prime factorization, envisioning applications in encoding and checking the satisfiability of various circuits.

"We believe that quantum annealers can be used to encode and check the satisfiability of many other circuits of interest. Thus addressing the propositional satisfiability of Boolean circuits (SAT)—a far more general problem than prime factorization and allows for representing a

variety of real-world problems," shared Prof. Sebastiani.

Looking ahead, the researchers stressed the importance of developing hybrid quantum-classical procedures, where the annealer can be invoked by classical procedures to solve small but computationally very hard combinatorial subproblems.

However, it's crucial to note that despite the remarkable achievements presented in their paper, the researchers are cautious about the limitations. They emphasize that they are still far from solving prime factorization problems significant enough to compromise the security of current cryptographic systems.

More information: Jingwen Ding et al, Effective prime factorization via quantum annealing by modular locally-structured embedding, *Scientific Reports* (2024). DOI: 10.1038/s41598-024-53708-7