# RSA Encryption Using Quantum Computer


An intriguing challenge for AI: creating a visual representation of this topic. I experimented with various prompts for a while until I was satisfied with the results. In the end, I even modified the original version.

Here is a refined English prompt suitable for generating a symbolic image representing “China Breaks RSA Encryption Using Quantum Computer”: An artistic, metaphorical illustration depicting China as a red dragon. In the background, a glowing quantum computer with floating qubits and intricate digital circuits. The scene merges cyberpunk and futuristic aesthetics, set against a dark, high-tech backdrop, symbolising the breakthrough in encryption. The image evokes the notion of cutting-edge quantum technology overpowering conventional cryptographic security.

In later iterations, I decided to omit the dragon.

Earth.com: „China Breaks RSA Encryption Using Quantum Computer | What It Means for Cybersecurity“.

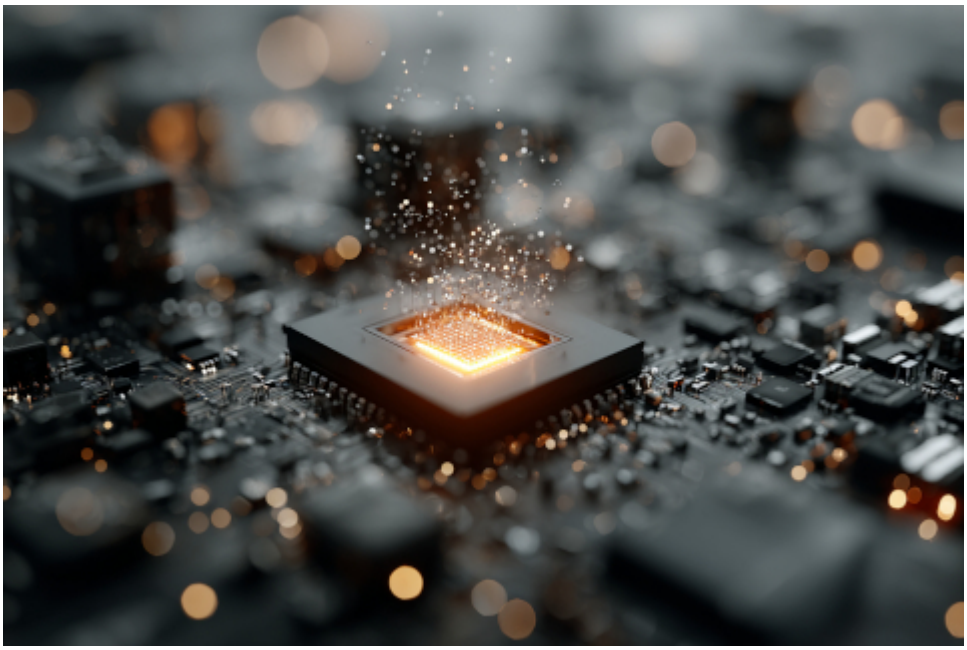
This is fascinating. The *conclusio* of a similar article by UniSense Advisory, translated from German, reads as follows:

“Currently, there are no quantum computers capable of breaking RSA-2048 or ECC encryption. Nevertheless, this recent

development in quantum computing in China serves as a proof of concept, demonstrating that quantum machines are becoming increasingly sophisticated. The gap between theory and practical application is steadily narrowing.

Cybersecurity leaders refer to this foreseeable turning point as ‘Q-Day’ – the moment when today’s asymmetric cryptography can no longer be considered secure. The timeline for Q-Day has shifted from a distant theoretical concern to an imminent, real-world risk that requires proactive preparation today.”

In other words, precisely the opposite of what the sensational headline suggests.



But I still wasn’t satisfied. Back in 2024, Barış Ege (Keysight Technologies) had already written: “Security Highlight: China’s Quantum Leap, and Why RSA Isn’t at Risk (Yet).” Naturally, I had the AI translate the article for me, as the original English was rather complex. I then instructed: “Rephrase the text in less technical, more accessible language, but without shortening it.”

Certainly! Here’s the text rephrased in plain, easy-to-understand English – all content remains intact, only the technical jargon and complicated explanations have been

simplified:

In recent days, headlines have sparked considerable excitement, suggesting that Chinese scientists might now be capable of breaking even highly secure RSA encryption with quantum computers. Unsurprisingly, this raised concerns about the safety of our online data. But when you take a closer look at the facts, it quickly becomes clear: we are not there yet. Here's what's really behind the headlines.

**What exactly happened?**

A Chinese scientific journal recently published a study in which researchers from Shanghai University report that they successfully used a special quantum machine from D-Wave to break down a 22-bit binary number – essentially, a very small number – into its factors. This process, known as factoring, is the fundamental mathematical challenge behind cracking certain types of encryption.

The study demonstrated that this type of quantum machine, known as a quantum annealer, can turn encryption problems into computational tasks that are easier to solve. However, this success only applies to very small numbers.

For context: the encryption keys used in modern RSA encryption typically have at least 2048 bits. So the tiny 22-bit number from the study is nowhere near the scale needed to threaten real-world encryption. In other words, while this success marks a small scientific step forward, it poses no immediate threat to the encryption technology we rely on today.

RSA encryption remains secure because breaking it requires factoring extremely large numbers into their prime factors – something that overwhelms conventional computers. In theory, quantum computers could one day solve this task much faster – but for now, that remains purely theoretical.

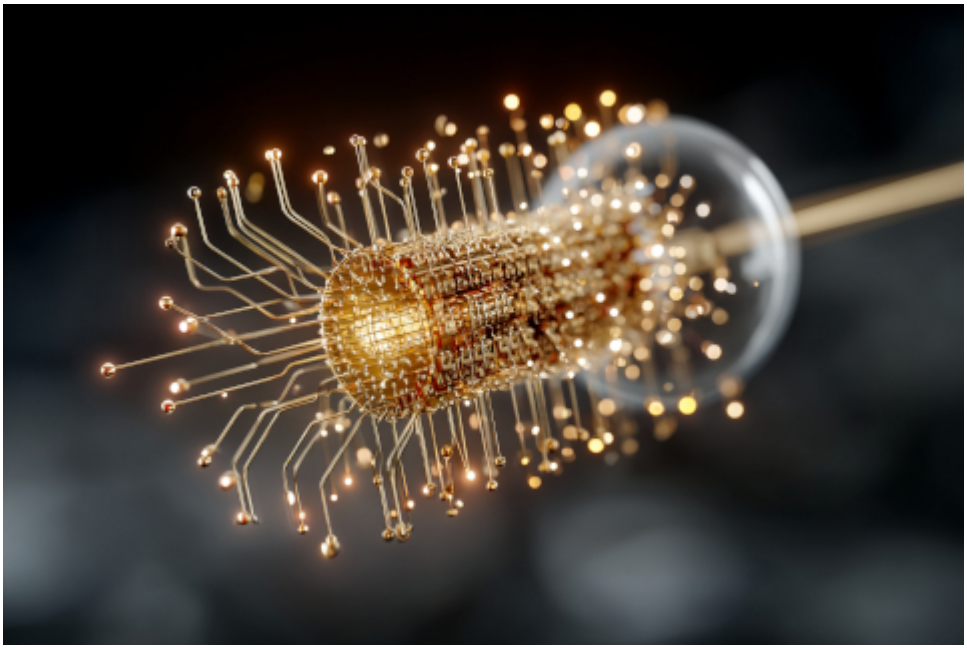
**Quantum Annealing versus True Quantum Computers – A**

## Distinction Worth Noting

In their experiment, the researchers did not use a fully functional, universal quantum computer, but rather a specialised machine designed to solve optimisation problems – the so-called "Quantum Annealer" developed by D-Wave. These devices are capable of handling certain types of calculations but currently lack the power required to deal with the large numbers used in modern encryption.

Moreover, the researchers did not rely solely on quantum technology; instead, they applied a hybrid approach combining both classical and quantum computing resources. It remains uncertain whether their method could ever be applied effectively on a large scale – achieving this would require significantly more powerful quantum devices or universal quantum computers capable of running the well-known Shor's algorithm. In theory, such an algorithm could break large RSA keys – but in practice, that remains a distant possibility.

Even though quantum annealing may one day offer a faster route to cracking RSA keys than classical computers, it is doubtful that such machines will become widely available before fully functional universal quantum computers capable of running Shor's algorithm.



## How Real Is the Threat to Modern Encryption?

As fascinating as quantum computing may be, the actual threat it poses to today's encryption is often exaggerated. Numerous challenges still need to be overcome:

Limited computational power so far: The D-Wave machine has so far only managed to factor a tiny 22-bit number. By contrast, RSA keys typically contain at least 2048 bits, with some even doubling that length. Quantum machines are nowhere near handling such large numbers.

Classical computers still outperform quantum machines: Even the most advanced quantum devices to date cannot compete with classical computers when it comes to factoring large numbers. For comparison: using conventional methods, researchers have already factored a 250-digit decimal number – equivalent to an 829-bit number. Quantum technology still lags far behind this benchmark.

Not all types of encryption are at risk: Quantum computers primarily threaten so-called asymmetric encryption methods, such as RSA and ECC. Other widely used techniques, such as symmetric AES encryption, are not currently at risk. Even if needed, AES can simply adopt longer keys to maintain security.

## Technical Challenges in Quantum Computing

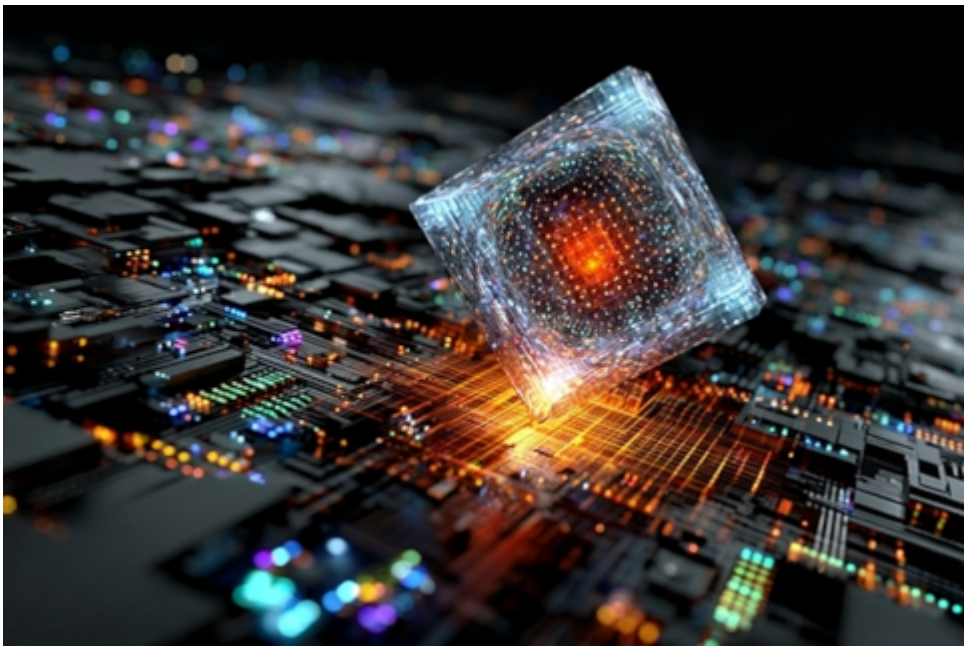
Quantum computers continue to face major technical obstacles. Their basic building blocks, known as qubits, are extremely sensitive to external interference. Keeping them stable and functioning reliably requires highly complex engineering.

Experts estimate that to achieve one reliably functioning "logical qubit," between 100 and 1000 physical qubits are needed. To break a 2048-bit RSA key securely, it is believed that at least 4000 of these logical qubits would be required – an enormous technical challenge that has yet to be achieved.

Microsoft researchers have also estimated that breaking a standard 256-bit key, such as those commonly used in modern encryption systems, would require around 2500 logical qubits – a level of performance that remains far beyond what is technically feasible today.

Despite these limitations, smaller quantum computers are already proving useful for specific tasks, such as complex planning, optimisation problems, or machine learning. However, these applications have nothing to do with cracking RSA keys or other forms of secure encryption.

This is why experts urge caution: the capabilities of quantum computers are often overhyped. If anyone truly possessed the ability to break encryption methods such as RSA on a large scale, it is highly unlikely they would advertise it publicly – let alone publish it in an academic journal.



## The Future: Making Encryption Resilient to Quantum Attacks

Even though the immediate threat may still lie in the future, the IT industry is already preparing for potential quantum attacks. For this purpose, new so-called “quantum-resistant” encryption methods are being developed. These are known as Post-Quantum Cryptography (PQC).

The US standardisation body NIST has already formally approved several of these new algorithms, including Dilithium and Kyber. These are now gradually being implemented across different areas of technology. They are designed to remain secure even if quantum computers become significantly more powerful in the future.

The technology for these new methods is fundamentally ready. However, the greatest challenge lies in implementing them correctly. Mistakes made during the introduction of new encryption methods could create far greater security risks than quantum computers themselves currently pose.

For this reason, it is particularly important to rely on verified and certified products when adopting new encryption. Only then can it be ensured that quantum-resistant encryption provides true security – rather than becoming a vulnerability due to careless implementation.

[This article in German]