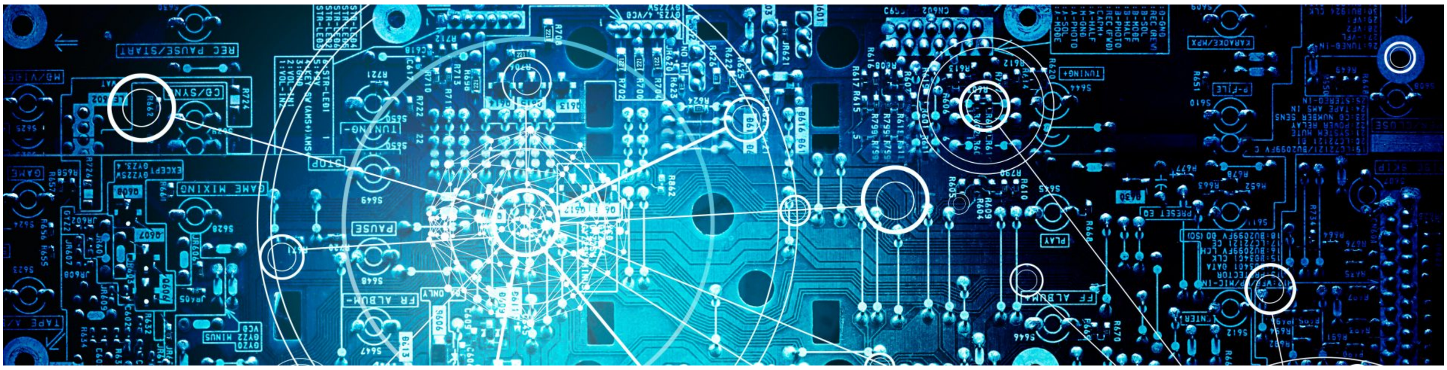
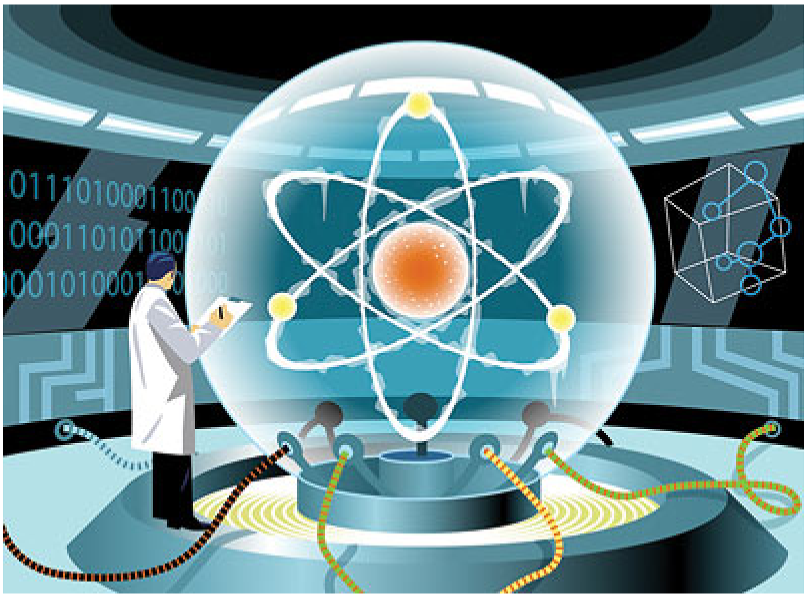
KUDELSKI SECURITY RESEARCH

The Latest News from Research at Kudelski Security



THE QUANTUM COMPUTER FAQ

February 6, 2017 JP Aumasson Crypto 3 comments



This is probably how a quantum computer looks ¯\(°_o)/¯

Several readers of the post Defeating Quantum Algorithms with Hash Functions found it difficult to follow without background information on quantum computers. So here I'd like to summarize basic facts about quantum computers and to debunk some preconceived ideas:

What is NOT a quantum computer?

- A quantum computer is **not a super-fast classical computer**.
- A quantum computer is **not** a computer that computes all solutions to a problem **in parallel**.
- A quantum computer **cannot solve all hard problems** instantaneously, in particular it's unlikely to solve NP-complete problems.

How does a quantum computer work?

- A quantum computer does not operate on bits (values either 0 or 1), but instead on quantum bits, a.k.a. **qubits**, which can simultaneously have the values 0 or 1.
    - Until a qubit is observed, it does not have a definite value, but is 0 with some probability *p*, and 1 with some probability 1–*p*.
    - In fact, the probability *p* is defined in terms of a complex number, possibly negative, called an **amplitude**, which is a property of a quantum state.
- Thanks to the rules of quantum mechanics, we know how to transform groups of qubits using specific operators called **quantum operators**:

these include **quantum gates** and **measurements**.

  - Quantum gates can be seen as **linear algebra transforms** (think, matrix multiplications) that obey certain rules.
  - Measurements correspond to the observation of a qubit's value. Once measured, the qubit stays either 0 or 1, and is no longer in **superposition**.
- A combination of quantum operators is called a **quantum algorithm**, or more accurately a **quantum circuit**.
- You can see the application of a quantum algorithm as the **evolution of a set of amplitudes**, or complex-valued probabilities.

In what sense are quantum computers faster?

- Quantum algorithms can perform certain tasks fundamentally faster than classical algorithms can. When this happens, we talk of a **quantum speed-up**.
- When the speed-up is so large that practically impossible tasks (because they are too slow) become possible, we talk of an **exponential speed-up**.
- The poster child of exponential speed-ups is **Shor's algorithm**: simply put, it can factor numbers in time commensurate with their size (for example, 2048 bits) rather than with their value (for example 2^{2048}, for a 2048-bit number).

What kind of crypto would be broken?

- Shor’s quantum algorithm’s performance isn’t just a mathematical curiosity: it could be used to break the RSA encryption algorithm, and in fact to **break all public-key cryptography** deployed today (thereby breaking TLS, IPSec, and SSH, for example).
- Yes, **elliptic-curve crypto** would be totally broken too (except maybe for some constructions called isogeny-based).
- Alas, a quantum computer that would break our crypto **does not exist today**.
- In fact, some experiments did run Shor’s algorithm to factor the number **15=3×5**. You may read claims that larger numbers such as 56,153 were factored on a quantum computer, but these weren’t using Shor’s algorithm, and were sort of cheating.

What kind of crypto would NOT be broken?

- Today, the **AES** encryption algorithm gets you 128-bit security. With quantum computers, you’d only get 64-bit security, because of **Grover’s search algorithm**.
- This isn’t specifically targeting AES, a quantum computer would halve the security of **any symmetric** cipher, hash function, or message authentication code (things like Salsa20, BLAKE2, HMAC, respectively).

- So if you want AES with 128-bit security in a world of quantum computers, just use a 256-bit key.

What is post-quantum cryptography?

- **Post-quantum** (a.k.a. quantum-safe, or quantum-resistant) cryptographic schemes are algorithms purposefully designed to resist quantum computers.
- Post-quantum crypto schemes aim to **eventually replace** RSA, elliptic-curve cryptography, and Diffie-Hellman schemes used today.
- The **NSA recommends** to "transition to quantum resistant algorithms in the future", and to help this NIST is running a **competition** for new post-quantum algorithms.
- Today, we know of **four promising approaches** to build post-quantum schemes:
    - Hash-based schemes, which use **hash functions** (things like SHA-3, BLAKE2).
    - Code-based schemes, which use **error-correcting codes**.
    - Multivariate schemes, which use **systems of equations** in many variables.
    - Lattice-based schemes, which use problems such as **learning with errors** (LWE).

When can I buy a quantum computer?

- Some people will tell you that such a quantum computer will come in 5 years, some people say never. In fact, **nobody knows**.

Why is a quantum computer hard to build?

- A quantum computer is hard to build chiefly because it's very hard to maintain qubits in a **stable state and free of errors**.
- We know a trick to **deal with errors** in qubits, but it requires adding more qubits to the system, and therefore makes it more complex.
- Today, several groups are attempting to build a quantum computers. One of the recent achievements is a stable system of **9 qubits**.
- To break crypto algorithms such as RSA, we estimate today that we'd need of the order of a **million qubits**.

What about D-Wave?

- The **D-Wave** company claims to have built a quantum computer, but it's really not a full-blow quantum computer. Although it works with qubits, it cannot run any of the cryptographically useful quantum algorithms.
- In particular, the D-Wave machine **can't run Shor**'s algorithm, and therefore can't break crypto algorithms.
- In fact, there is still **no evidence** that D-Wave's machine is more efficient than a classical computer.

Can I still try a quantum computer?

- There are **simulators** of quantum computers, but these use a classical computer to run the simulation, and are limited to a small number of qubits.
- You can even run quantum circuits on a real 5-qubit system, thanks to IBM's quantum computing **platform**.

« Forging RSA-PSS signatures with mbedTLS

Wire Cryptography Audit (with X41 D-Sec) »

3 COMMENTS

Pingback: The Quantum Computer FAQ

Pingback: ควอนตัมคอมพิวเตอร์ FAQ | Panya's Blog: Programmer Thoughts

Pingback: Our submission to NIST's post-quantum project: Gravity-SPHINCS

LEAVE A REPLY

Enter your comment here...