Post-quantum e-state – why and when?

Jan Willemson

The State. Why e?

- Why do we need a state in the first place?

The State. Why e?

- Why do we need a state in the first place?
  - To provide its citizens services like education, healthcare, safety, etc.
- The services must be available to those who need them when they need them.
- Making services e helps to increase their availability significantly.

Service requirements

- Services come with a number of requirements:
  - The services should be available only to those entitled to them.
  - The services should be fair and accountable in their fairness.
  - Information gathered for/by the services should be handled in a privacy-respecting manner.
  - . . . [include your favourite requirements here]

Service requirements

- Services come with a number of requirements:
  - The services should be available only to those entitled to them.
  - The services should be fair and accountable in their fairness.
  - Information gathered for/by the services should be handled in a privacy-respecting manner.
  - . . . [include your favourite requirements here]
- Such requirements are often summarized under the common term of *security*.

The role of cryptography

- Cryptography is one way of handling security requirements.
  - Confidentiality via encryption and key exchange.
  - Authenticity and integrity via signatures.
  - Accountability via zero-knowledge proofs.

What does it take to break crypto with a quantum computer? (2019)

COMPUTING

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

By Emerging Technology from the arXiv May 30, 2019

What does it take to break crypto with a quantum computer? (2023)

Home > Information Security and Cryptology – ICISC 2023 > Conference paper

Experiments and Resource Analysis of Shor's Factorization Using a Quantum Simulator

Conference paper | First Online: 08 March 2024

pp 119–139 | Cite this conference paper

- Under ideal conditions, breaking RSA-2048 would take about 100 days.
- Under more realistic conditions, it could take years or even decades.

How much would it cost?

SHORT-PAPER OPEN ACCESS

A Performance Model for Estimating the Cost of Scaling to Practical Quantum Advantage

Authors: Daan Camps, Katherine Klymko, Brian Austin, Nicholas J. Wright Authors Info & Claims

SC-W '23: Proceedings of the SC '23 Workshops of The International Conference on High Performance Computing, Network, Storage, and Analysis • November 2023 • Pages 1269–1273 • https://doi.org/10.1145/3624062.3625533

- Achieving quantum advantage would cost about $1,000,000.
- Breaking RSA-2048 is far more complex than achieving just bare minimum quantum advantage.

Risk analysis

- In order to understand whether your application is endangered by a quantum computer, you have to first understand your application.
  - For how long does your application need to withstand attacks?
  - How much can the attacker gain from attacking you?
  - What are the attacker resources available to the attacker (time, money), and how much can he spend them on attacking you?

Risk analysis: authentication

- Authentication happens typically for *one session* and *limited time*.
- Breaking your authentication key allows the attacker to impersonate you potentially for many sessions, but all these sessions separately are likely rather low-utility for the attacker.
- Also, authentication keys can be revoked quite easily without long-term problems.
- In many scenarios, using pre-quantum authentication may be quite OK even after large quantum computers emerge.

Risk analysis: signatures

- Signatures may need to retain the non-repudiation property over a longer period of time (potentially for years).
- Revoking a signature key is something that is a known problem for also pre-quantum cryptography.
- *Time-stamping* was introduced to solve the problem of extending signature validity over the point of revocation. If done correctly, this also helps to protect pre-quantum signatures over the point of introducing sufficiently powerful quantum computers.
- After that point, you need to decide:
  - if the combined value of all your signatures is less than the cost of breaking your key, you can continue using pre-quantum signatures.
  - Otherwise, use a post-quantum signatures.

Risk analysis: encryption

- If the confidentiality horizon of your information is shorter than the time that it takes to break the encryption key, you can use pre-quantum cryptography.
- If the value of the encrypted information is less than the cost of breaking the key, you can use pre-quantum cryptography.
- Otherwise, you must use post-quantum cryptography.

Risk analysis: challenges

- It is not always easy to estimate how much your information/signature is worth for the attacker. Thus, sometimes it may be justified to convert to the post-quantum cryptography ‘just in case’.
- The time and cost estimates of quantum computing are currently very approximate. Again, in order to be on the safe side, introducing post-quantum cryptography may be justified ‘just in case’.

Ecosystems

Transition will be easier to handle in *closed* ecosystems, i.e. in settings where all the key infrastructure components are developed locally.

- CDOC is a *closed* ecosystem.
- PKI is an *open* ecosystem.
- In the IVXV Internet voting system, the authentication/signature components are part of an *open* ecosystem, whereas the vote encryption scheme forms a *closed* ecosystem.

Thank you!

- Questions?

cybernetica
Cybernetica
cybernetica_ee
Cybernetica