Moving the Goal to Post Quantum

Prof. dr. ir. Roland van Rijswijk-Deij
University of Twente, The Netherlands
WHO HERE HAS NOT HEARD OF QUANTUM COMPUTING?
Quantum Computing Hype Cycle Just Getting Started

Quantum computing could be to the 2020s what cloud computing was to the 2010s

By Dana Blankenhorn, InvestorPlace Contributor  Jul 25, 2018, 1:24 pm EST

Quantum Computing Under Hype Cycle and Market Clock Scrutiny

With new technology come the plaudits and the critics. Quantum computing is no different from any other sector

By James Dargan  August 1, 2019

The hype around quantum computing: it's not too early to get in

by Jurgita Lapienytė  © 15 February 2021
HYPE ➡ PRESSURE ➡ MISTAKES
HYPE ➡ PRESSURE ➡ MISTAKES

NOS Nieuws • Maandag 8 maart 2021, 17:00 • Aangepast maandag 8 maart 2021, 23:18

Onderzoeker Kouwenhoven erkent fout: deeltje voor quantumcomputer niet gevonden
Kouwenhoven departs, Microsoft presents Majoranas

In a strange combination of events, Microsoft announced both the departure of Leo Kouwenhoven this week and the discovery of scalable Majoranas - developed in Denmark.
HYPE ➡ PRESSURE ➡ MISTAKES

Kouwenhoven departs, Microsoft presents Majoranas

In a strange combination of events, Microsoft announced both the departure of Leo Kouwenhoven this week and the discovery of scalable Majoranas – developed in Denmark.

Delftse onderzoekers kwantumcomputers 'verwijtbaar onzorgvuldig'

Het College van Bestuur van de TU Delft oordeelt dat Leo Kouwenhoven en Hao Zhang 'onzorgvuldig' hebben gehandeld en dat er deels ook sprake is van 'verwijtbare onzorgvuldigheid' bij de publicatie van hun werk over Majoranaeeltjes. Deze deeltjes zijn veelbelovend als basis voor een stabiele kwantumcomputer.

Geen schending wetenschappelijke integriteit.
Quantum supremacy using a programmable superconducting processor

Quantum Computing: Is it the end of blockchain?

June 3rd 2018

Is this the end of blockchain?
OK, ONE MORE ‘CAUSE I CAN’T RESIST…

Quantum Computing: Is it the end of blockchain?

June 3rd 2018

SPOILER: YES!
THE HYPE ISN’T HELPFUL

• The tech **news sites** are abuzz with quantum
• It may seem like **quantum computing** is just around the corner
• And that **it’s going to change the world** (it is)
• Some **quick facts**:
  • Practical quantum computers require **1,000s of so-called logical qubits** (which consist of **10,000s of physical qubits**)
  • Google’s **quantum supremacy** machine had 53 physical qubits — how supreme is that?
THE HYPE ISN’T HELPFUL

• The tech news sites are abuzz with quantum computing.
• It may seem like quantum computing is just around the corner.
• And it’s going to change the world (it is).

Some quick facts:
• Practical quantum computers require 1,000s of so-called logical qubits (which consist of 10,000s of physical qubits).
• Google’s quantum supremacy machine had 53 physical qubits — how supreme is that?

Goal of this talk:
Poke through the hype and tell you why you should care about quantum computing and what challenges we face when deploying quantum-resistant cryptography.
WHY, THEN, WORRY ABOUT QUANTUM?

Lov Grover
(image: dotquantum.io)

Peter Shor
(image: dotquantum.io)
WHY, THEN, WORRY ABOUT QUANTUM?

Great theory, but no relevant impact on cryptography

Lov Grover  
(image: dotquantum.io)

Peter Shor  
(image: dotquantum.io)
SHOR’S ALGORITHM

• Reduces effort of factoring integers and solving discrete logarithms to **polynomial time**

• This is a **big deal** - a sufficiently powerful quantum computer **could break all current public key crypto**

• E.g. break RSA 2048 **in hours**
SHOR’S ALGORITHM: IMPACT

• Asymmetric crypto is used for many purposes: key negotiation and authentication for HTTPS, legally binding digital signatures, …, …, …

• A sufficiently powerful quantum computer would cause major problems for all of the Internet
Asymmetric crypto is used for many purposes: key negotiation and authentication for HTTPS, legally binding digital signatures, …, …, …

A sufficiently powerful quantum computer would cause major problems for all of the Internet.

In normal user terms, we go from this:

For all of the Internet
# WHEN WILL SHOR BE A PROBLEM?

<table>
<thead>
<tr>
<th>Public Key System</th>
<th>Key Size</th>
<th>Security</th>
<th>Logical qubits</th>
<th>Physical qubits</th>
<th>Running time</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>1024 bits</td>
<td>80 bits</td>
<td>2,050</td>
<td>$8.05 \times 10^6$</td>
<td>4 hours</td>
</tr>
<tr>
<td></td>
<td>2048 bits</td>
<td>112 bits</td>
<td>4,098</td>
<td>$8.56 \times 10^6$</td>
<td>29 hours</td>
</tr>
<tr>
<td></td>
<td>4096 bits</td>
<td>128 bits</td>
<td>8,194</td>
<td>$1.12 \times 10^7$</td>
<td>~10 days</td>
</tr>
<tr>
<td>ECC</td>
<td>256 bits</td>
<td>128 bits</td>
<td>2,330</td>
<td>$8.56 \times 10^6$</td>
<td>11 hours</td>
</tr>
<tr>
<td></td>
<td>384 bits</td>
<td>192 bits</td>
<td>3,484</td>
<td>$9.05 \times 10^6$</td>
<td>38 hours</td>
</tr>
<tr>
<td></td>
<td>512 bits</td>
<td>256 bits</td>
<td>4,719</td>
<td>$1.13 \times 10^7$</td>
<td>~2 days</td>
</tr>
</tbody>
</table>

IBM unveils its 433 qubit Osprey quantum computer
IBM unveils its 433 qubit Osprey quantum computer

Largest quantum computer ever; about 9,999,567 bits to add before the first public key can be broken.

IBM Unveils Its 433 Qubit Osprey Quantum Computer bit.ly/3UrVGd4
## WHEN WILL SHOR BE A PROBLEM?

<table>
<thead>
<tr>
<th>Public Key System</th>
<th>Key Size</th>
<th>Security</th>
<th>Logical qubits</th>
<th>Physical qubits</th>
<th>Running time</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>1024 bits</td>
<td>80 bits</td>
<td>2,050</td>
<td>$8.05 \times 10^6$</td>
<td>4 hours</td>
</tr>
<tr>
<td></td>
<td>2048 bits</td>
<td>112 bits</td>
<td>4,098</td>
<td>$8.56 \times 10^6$</td>
<td>29 hours</td>
</tr>
<tr>
<td></td>
<td>4096 bits</td>
<td>128 bits</td>
<td>8,194</td>
<td>$1.12 \times 10^7$</td>
<td>~10 days</td>
</tr>
<tr>
<td>ECC</td>
<td>256 bits</td>
<td>128 bits</td>
<td>2,330</td>
<td>$8.56 \times 10^6$</td>
<td>11 hours</td>
</tr>
<tr>
<td></td>
<td>384 bits</td>
<td>192 bits</td>
<td>3,484</td>
<td>$9.05 \times 10^6$</td>
<td>38 hours</td>
</tr>
<tr>
<td></td>
<td>512 bits</td>
<td>256 bits</td>
<td>4,719</td>
<td>$1.13 \times 10^7$</td>
<td>~2 days</td>
</tr>
</tbody>
</table>

WHAT QUANTUM EXPERTS THINK

2023 EXPERTS’ ESTIMATES OF LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

Number of experts who indicated a certain likelihood in each indicated timeframe. Stacked area chart with baseline separating estimates larger or lower than 30%.
[*Shaded grey area corresponds to the 25-year period, not considered in the questionnaire.]

likelihood

< 1%  < 5%  < 30%  ~ 30%  > 70%  > 95%  > 99%

This figure illustrates the central information collected through our survey. The experts were asked to indicate their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specified sense of being able to break RSA-2048 in 24 hours—for various time frames, from a short term of 5 years all the way to 30 years.

Top: stacked bar chart with explicit indication of the number of experts estimating a certain likelihood. Bottom: stacked area chart conveying the same information, but allowing one to better appreciate the shift in likelihood estimates moving from short-term to long-term timeframes.

Please note the inclusion of a dummy 25y timeframe.

WHAT QUANTUM EXPERTS THINK

2023 EXPERTS’ ESTIMATES OF LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

Number of experts who indicated a certain likelihood in each indicated timeframe.

TL;DR:
Most quantum computing experts now think a cryptographically relevant quantum computer is an inevitability!

TIME OF USE

- Whether we are safe depends on how long cryptographic data is used

- Rule of thumb:
  - **Short-term use**: no need to worry and no need for immediate action
  - **Long(er)-term use**: need to start thinking about transitioning now
TIME OF USE EXAMPLES

• Short-term use:
  (Two-factor) authentication, short-lived digital signatures (e.g. website certificates), online authentication protocols such as OpenID connect, SAML, ... (essentially **anything where the result of the cryptographic operation loses relevance quickly**)

• Long-term use:
  Encrypted long-term archives, legally binding digital signatures, ephemeral key exchange, ... (essentially **anything where the result of the cryptographic operation should be safe for decades**)
Cryptographers are working on new public key algorithms that are "quantum safe."

That is: they remain secure, even after a sufficiently powerful quantum computer comes to be.

Development states of algorithms range from ripe to green.

**Post-Quantum Cryptography**

cryptographers are working on *new public key algorithms* that are “quantum safe.”

That is: they *remain secure*, even after a sufficiently powerful *quantum computer* comes to be.

Development states of algorithms range from *ripe* to *green*.

**Post- /pəʊst/** a prefix, meaning “behind,” “after,” “later,” “subsequent to,” “posterior to,” occurring originally in loanwords from Latin (postscript), but now used freely in the formation of compound words (*post-Elizabethan*; postfix; postgraduate; postorbital).
RADICALLY DIFFERENT

• For some algorithms, every key can only be used once
• Some require much more CPU power or memory
• Some algorithms have much larger keys (100s of KBs) or signatures (1,000s of bytes)
• Has consequences for applications!
NIST COMPETITION

- Competition to select secure quantum safe algorithms for different applications (encryption, key exchange, signatures)
- End goal: standardise secure and suitable algorithms
- Current status: first algorithms selected for standardisation
WHEN, NOT IF

• It is now a matter of when, not if post quantum algorithms will be adopted

• Once NIST standards exist, the US and other governments will start requiring their use in tenders

• This will likely take years, and impact many Internet industries
ROCKY ROAD

- There is a *rocky road ahead*
- PQC has really only been *tested* in mainstream *Web* applications
- Yet the *Internet* is much *more than* just the *Web*
- The $1B question: how do we transition the entire Internet to PQC?
- This is the main research question for our *SHARQS* project
ROCKY ROAD

- There is a rocky road ahead.
- PQC has really only been tested in mainstream Web applications.
- Yet the Internet is much more than just the Web.
- The $1B question: how do we transition the entire Internet to PQC?
- This is the main research question for our SHARQS project.

My esteemed academic colleagues working on post-quantum crypto think that now we have algorithms we are (almost) done…

I think they are wrong 😁
AN NREN EXAMPLE: FEDERATED IDENTITY
AN NREN EXAMPLE: FEDERATED IDENTITY

IDP

Browser

SP

Access request
AN NREN EXAMPLE: FEDERATED IDENTITY

1. **Browser**
   - Access request
   - Redirect to IDP

2. **IDP**

3. **SP**
AN NREN EXAMPLE: FEDERATED IDENTITY

- IDP
- Browser
- SP

- Login request
- Access request
- Redirect to IDP
AN NREN EXAMPLE: FEDERATED IDENTITY

- **IDP**
- **Browser**
- **SP**

- Access request
- Redirect to IDP
- Login request
- Attribute assertion
AN NREN EXAMPLE: FEDERATED IDENTITY

1. **IDP**
2. **Browser**
3. **SP**

**Flow of Communication:**
- **Login request** from **Browser** to **IDP**
- **Redirect to IDP** from **SP** to **Browser**
- **Access request** from **SP** to **Browser**
- **Attribute assertion** from **IDP** to **SP**
- **Attribute assertion** from **IDP** to **Browser**
AN NREN EXAMPLE: FEDERATED IDENTITY

IDP

Browser

SP

- Login request
- Access request
- Redirect to IDP
- Attribute assertion
- Login successful
AN NREN EXAMPLE: FEDERATED IDENTITY

Diagram showing the flow of communication between IDP, Browser, SP, and TLS.
AN NREN EXAMPLE: FEDERATED IDENTITY

Browser

IDP

SP

Access request

Redirect to IDP

Login request

Attribute assertion

Attribute assertion

Login successful

Sign assertion

TLS

TLS

TLS
AN NREN EXAMPLE: FEDERATED IDENTITY

IDP

Browser

SP

TLS

Login request

Attribute assertion

TLS

Sign assertion

TLS

Access request

Redirect to IDP

TLS

Verify signature on assertion

Attribute assertion

Login successful
WELL ACTUALLY…
WELL ACTUALLY...

IDP

IDP

IDP

SP

Sign assertion

SP

SP
WELL ACTUALLY...

Diagram:

- **IDP**
  - Connects to multiple **SPs**
  - Signs assertion

- **SP**
  - Receives signed assertions
  - Verifies signature on assertion
WELL ACTUALLY…

IDP

IDP

IDP

SP

IDP

SP

Sign assertion

Verify signature on assertion

Sign assertion

Verify signature on assertion

Sign assertion
WELL ACTUALLY…

- IDP
- SP
- IDP
- SP
- IDP
- SP

Sign assertion
Verify signature on assertion
Sign assertion
Verify signature on assertion
Some more missing details:

- Hub-n-spoke —> more TLS connections
- Where-Are-You-From (WAYF), even more TLS connections
- Signing (and verifying) federation metadata

All in all (in hub-n-spoke + WAYF):
- 6 TLS connections
- 2 signatures, 2 verifications
GOAL OF THIS ONE EXAMPLE
GOAL OF THIS ONE EXAMPLE

- There is potentially even more complexity just in the web identity federation case
GOAL OF THIS ONE EXAMPLE

• There is potentially even **more complexity just in the web identity federation case**

• This is just one example, we have **other federations**
GOAL OF THIS ONE EXAMPLE

• There is potentially even more complexity just in the web identity federation case

• This is just one example, we have other federations

• These are just examples for “mainstream computing”; what about HPC? IoT? ICS?
The main potential issue is to develop a distributed identity management system for federated identity. The complexity is high, but there are solutions available. There are even more complex scenarios, such as the web identity federation case. This is just one example; we have other federations as well. These are just examples for "mainstream computing"; what about HPC, IoT, ICS?

I have left out even more detail 😜

I hope I convinced you were are only just starting the transition to post-quantum cryptography.
WHAT TO DO?...

• Powerful *quantum computers* are years, if not decades away

• Treat any vendor *claim* that you need to act *NOW*, or hype-panic with suspicion

• Do *take* the *PQC transition* seriously, it is the *biggest change* to the Internet in decades
COMMUNITY

• We have our work cut out for us the coming years
• The NREN community can take up a pioneering role
• Close ties with academia mean we can work together
• Our research needs your help and your input (and data)!

Photo by Hannah Busing on Unsplash
THANK YOU! QUESTIONS?