Implementing Post-Quantum Cryptography in Industry

MAY 11, 2023
Samuel Sabogal Pardo
Vice President
cyte.co
Context of the problem

Current asymmetric crypto will be broken - RSA, ElGamal, ECC. Also, Diffie-Hellman key exchange

![Diagram of asymmetric key exchange]

Current symmetric crypto will **not** be broken. Grover Quantum Algorithm used to attack, downgrades AES-256 to AES-128, which is still secure

![Diagram of symmetric key exchange]
Why quantum computing can do this?

Superposition

$|0\rangle$  
85% chance of being 0

$|1\rangle$  
15% chance of being 1

Entanglement

(Image credit: MARK GARLICK/SCIENCE PHOTO LIBRARY via Getty Images)

Allows new kinds of algorithms due to these properties

Disadvantage example: you can’t copy paste.
Breaking RSA – Optimistic advancement of QC

Using a new a strategy published in Dec 2022, which claims to be a realistic alternative to Shor’s Algorithm (some sceptics to this):

<table>
<thead>
<tr>
<th>RSA number</th>
<th>Qubits</th>
<th>Kn-depth</th>
<th>2DSL-depth</th>
<th>LNN-depth</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-128</td>
<td>37</td>
<td>113</td>
<td>121</td>
<td>150</td>
</tr>
<tr>
<td>RSA-256</td>
<td>64</td>
<td>194</td>
<td>204</td>
<td>258</td>
</tr>
<tr>
<td>RSA-512</td>
<td>114</td>
<td>344</td>
<td>357</td>
<td>458</td>
</tr>
<tr>
<td>RSA-1024</td>
<td>205</td>
<td>617</td>
<td>633</td>
<td>822</td>
</tr>
<tr>
<td>RSA-2048</td>
<td>372</td>
<td>1118</td>
<td>1139</td>
<td>1490</td>
</tr>
</tbody>
</table>

“We find that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048. Such a scale of quantum resources is most likely to be achieved on NISQ devices in the near future.”[1]

(Bao, 2022, p. 5)

“IBM Quantum systems scale up towards the stated goal of 4,000+ qubits by 2025 and beyond”[2]

Today: 433 Qubits
Last year: 128 Qubits
Senior director of data and security research at Fujitsu Dr Tetsuya Izu said: “Our research demonstrates that quantum computing doesn’t pose an immediate threat to existing cryptographic methods”[3] 2023

- They didn’t mention alternative algorithms
- They simulated 39 qubits in a super computer
- Many anecdotes of people predicting the future wrong. E.g. one week before chatGPT
- Not immediate, but, how long?
After how long is it safe to leak some information?

- Credit card expiration time: avg time: 3 to 5 years. Can be 10 years+
- Clinical history: a life span?
- Industrial secrets: generations?
- Military records: 40 years for top secret
- Source code: depends on the company. Some will open source it, other companies keep it undisclosed “eternally”

“harvest now, decrypt later” is a serious attack
Protecting information for many years is needed

Post-Quantum Crypto to be a standard, NOT YET ONE

Public-key Encryption
CRYSTALS-KYBER

Digital Signature
CRYSTALS-DILITHIUM
FALCON
SPHINCS+

Any of these can be run in traditional computers. DON’T NEED QUANTUM COMPUTERS
Hybrid, viable option today in custom software

Current PKI infrastructure can be used

You can’t make a browser use this. Useful for sending sensitive files (today in use).
Sensitive data transmitted from browser to server

Security in depth:

The second layer was added in the past, because of:

• Heartbleed: 64 kb are exposed taking advantage of the TLS heartbeat
• POODLE: Padding Oracle On Downgraded Legacy Encryption (to attack SSL 3.0)
• BEAST: CVE-2011-3389, allows “MITM”
• SWEET32: CVE-2016-2183, When a high number of data is encrypted, information can be leaked.
  • ...

A postquantum public key (CRYSTALS-KYBER) can be added, to transfer a session AES-256 key.
What to do in DevOps

Alternatives to keep proprietary source code safe

• Keep everything in an internal network
  - Unlikely in post-pandemic, even in radical companies

• If your binaries are “public but obfuscated binaries”, you can push obfuscated code and push the mapping encrypted with AES
  - If that is the case, code can be reversed, so beware your code is not secret

• Push AES-256 encrypted source code and decrypt it in the CI server to then run tests etc.
  - Need to put manually the AES in the server and locally.
  - No browser features like navigation of code
  - You could not use github, that violates their terms.
Breaking Asymmetric Crypto – cybersecurity perspective

• In cybersecurity we are not optimistic or pessimistic, we are paranoid!
• In fact, “Paranoia is our Profession”
• We should not take our chances and hope that quantum computing doesn’t advance
• Implement CRYSTALS-KYBER as soon NIST round 4 finishes. (don’t wait, like some still use SSL)
• If operating very sensitive information, might need one of the alternative approaches.
  • In git third party solutions, can be uncomfortable
  • In your own apps, it is easy to implement and works well

Remember: Better to err on the side of caution.
Contacts

Samuel Sabogal Pardo
Vice-President

Juan Sebastián Ramos
Sales Director

Angelica Forero
Chief Sales Officer

Email: info@cyte.co
References


Images from https://pixabay.com/