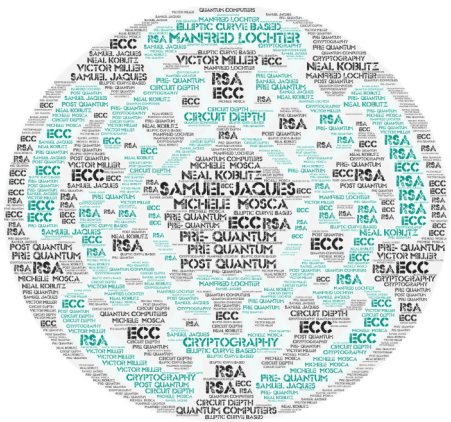
How long can we safely use pre-quantum ECC? [a.k.a. The end of ECC]

Panelists: Samuel Jaques, Manfred Lochter and Michele Mosca.

Moderator: Francisco Rodríguez-Henríquez.



ECC 2020 Third discussion panel

October 29, 2020.

[In praise of] Elliptic-Curve Cryptography (ECC)

- ECC was suggested independently by Neal Koblitz and Victor Miller in 1985 [35 years ago!!]
- After a long, windy and at a times bitter battle against RSA, ECC is now the undisputed most efficient, most effective and most popular pre-quantum public key scheme
- The main applications of ECC are on key exchange and digital signature protocols
- Used and deployed in massive applications such as OpenSSL, SSH, WhatsApp, cryptocoins, ...
- Strong confidence in the *classical* hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP)

The end of ECC

Nevertheless, ECC succumbs to Shor's algorithm implemented on large-scale quantum computers, which begs the question:

How long can we safely use pre-quantum ECC?

[Some] Additional discussion topics

- Can ECC be dead [even] *before* the arrival of large-scale quantum computers?
- *During* the transition period, can possibly ECC co-exist with post-quantum schemes for many years?
- Is there life for ECC *after* the arrival of large-scale quantum computers?
- What would be the cost (in terms of qubits, T-gates, circuit depth) of a quantum artifact that is able to break ECC?
- Which one will be broken first: RSA or ECC?
- If there is no major progress, say in the next 5 years, what is the probability that funding for quantum computing research will decline or even vanish?

How long can we safely use pre-quantum ECC?

Looking forward to an interesting and thought-provoking panel discussion!

Will ECC finally meet *Día de Muertos*?