Post-Quantum Cryptography

Etienne Marcatel

Bull/Atos, Trustway

Univ. Grenoble Alpes, Institut Fourier

October 17th, 2019

financed by
IDEX Université Grenoble Alpes

This work is supported by the French National Research Agency in the framework of the "Investissements d'avenir" program (ANR-15-IDEX-02)

Angular stone of cybersecurity : Cryptography

- Symmetric Cryptography :
  - AES
- Cryptographic Hash Function :
  - SHA-2
  - SHA-3
- Asymmetric Cryptography :
  - RSA
  - ECC

Not in opposition but in ***synergy***.

Context : Quantum Computer

- 1980 : Paul Benioff and Richard Feynman have the idea
- 1984 : Quantum Cryptography : Key Exchange Protocol BB84
- 1994 : Shor's algorithm
- 1996 : Grover's algorithm

Cryptosystem	Impact of Quantum Computer
AES	Key x 2
SHA-2, SHA-3	Digest x 3
RSA	Broken
DH, ECDH	Broken
DSA, ECDSA	Broken

Context : Quantum Computer

- 2001 : First use of Shor's algorithm to factor 15 (dedicated QC of 7 qbits)
- 2009 : First *universal* Quantum Computer (2 qbits)
- 2017 : IBM put a 20 qbits Quantum Computer on the cloud
- 2019 : Google (may have) achieve *Quantum Supremacy* (using 53 qbits) [1]

Solution : ***Post-Quantum Cryptography***

[1] Financial times , Sept 2019

Asymmetric Cryptography which is ***supposed*** to be resistant to Quantum Computer.

- Error Correcting Codes : McEliece in 1978
- Lattices
- Multivariate Equations
- Other :
  - Supersingular elliptic curves Isogenies
  - Hash-based signature
  - Etc.

Known for the organization of crypto competitions :

- AES
- SHA-3

New process to standardized PQ Crypto. (PKE/KEM and Signature)

PQC Standardization : Timeline

- dec 2016 : Call for submission
- dec 2017 : Round 1 : 64 propositions
  - 45 PKE/KEM
  - 19 Signatures
- jan 2019 : Round 2 : 26 propositions
  - 17 PKE/KEM
  - 9 Signatures
- aug 2019 : Second NIST' PQC conference
- 2020 : Round 3
- 2021-ish : Select algorithms
- 2023-ish : Draft standards

Plus the transition time, 5 years? ***Are we too late?***

Theories	PKE/KEM		Signatures	
	R1	R2	R1	R2
Lattices	21	9	5	3
Codes	17	7	2	-
Multivariates	2	-	7	4
Isogenies	1	1	-	-
Symmetric/Hash	-	-	3	2
Others	4	-	2	-
Total	45	**17**	19	**9**

We need time for :

- Proof checking (rip OCB2)
- Constant-time
- Side-Channel Attack
- Platform : Microcontroller, FPGA , ...
- Problem hardness

But do we have enough time ?

Any questions ?