Algorand in QuantumLand

Zhenfei Zhang

August 25, 2020

1. Alice in Wonderland (2010)

Algorand

ENU

nature

Article | P

Quan
progr
proce

Frank Arut

Nature 57

749k Acc

5G REVOLUTION

No, Google and Its Quantum Computer Aren't Killing Bitcoin Anytime Soon

A computing breakthrough won't break down cryptocurrency right away.

BY ERIC MACK, COLUMNIST, INC.COM @ERICCMACK

Algorand

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Schemes at risk:

- Protocols: HTTPS, TLS, X.509, ...
- PKIs: RSA, DH, ECDH, ECDSA, Ed25519, ...
- Blockchain cryptography: BLS, VRF, SNARKs, ...

- NSA announces plan to migrant to post-quantum cryptography[2]
- NIST first round submission: 87 candidate algorithms
- NIST second round evaluation: 26 survivors
- NIST third round result: 7 finalists

Public Key Encryption	Digital Signature
NTRU, Kyber, Saber, McEliece	Falcon, Dilithium, Rainbow

2. Post-quantum cryptography are the cryptography that are secure against quantum computers

What are at risk

Digital signatures

- Ed25519 (Algorand)
- BLS signature (Eth2.0, Dfinity, etc)

Cryptographic Sortition

- ECVRF (Algorand)
- BLS-VRF (Dfinity, Harmony, etc)

Active Attack

- Require access to quantum computer
- **Cannot** travel back in time and forge authenticity

Passive Attack

- Require access to quantum computer
- **Can** travel back in time and create a fork

Digital signatures: Solution I

	Pre-quantum		Post-quantum			
	Ed25519	BLS	Falcon	Dilithium	Rainbow	Sphincs+
PK	32 B	96 B	900 B	1.2 KB	150 KB	48 B
Signature	64 B	48 B	700 B	2 KB	64 B	31 KB
Hardness Assumption	ECC	pairing	lattice	lattice	multivariate quadratic	hash

- None of post-quantum solutions scales well for Algorand's use case (1000+ TPS)

Digital signatures: Solution II

- Aggregatable signatures
  - State-of-the-art: one-time, post-quantum **aggregatable** signature
  - Research direction: making this signature scheme practical

Verifiable random functions

	Pre-quantum		Post-quantum		
	ECVRF	BLS-VRF	OT-LB-VRF	VRF (w. Falcon)	VRF (w. Rainbow)
PK	32 bytes	96 bytes	3.3 KB	900 B	150 KB
Proof	80 bytes	48 bytes	4.8 KB	8.8 KB	8.1 KB
Prove	0.15 ms	0.7 ms	1.4 ms	WIP	WIP
Verify	0.2 ms	2.0 ms	1.4 ms	WIP	WIP
Hardness Assumption	ECC	pairing	lattice	lattice	lattice + MQ

- Research direction:
  - complete the construction
  - benchmarking and evaluation

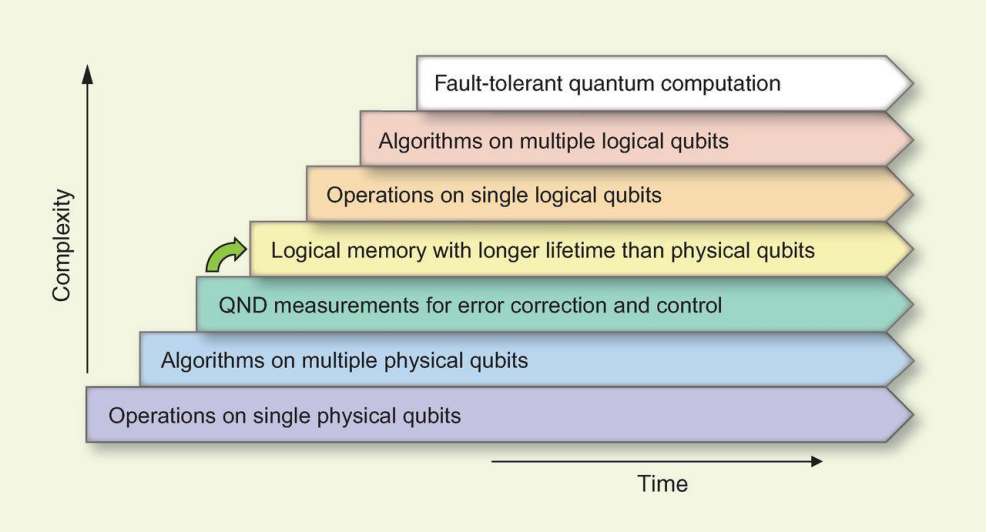
Q & A

- If you are interested in deploying any of the schemes over Algorand, please reach out :-)

When will quantum computers arrive?

If you really want to ask...

Optimistic view[3]



Pessimistic view[4]

3. Superconducting Circuits for Quantum Information: An Outlook. M. H. Devoret and R. J. Schoelkopf
4. Avengers: Endgame (2019)