From Quantum Physics to Post-Quantum Digital Security

JP Aumasson

Sorry, this product is no longer available!

See larger image

100 pcs lot Lava pendants Energy quantum scalar pendant energy card and Resist radiation JHE0151

Price: **US $263.72 - 341.67** / Lot (US $2.64 - 3.42 / Piece) Reference Currency

100 Pieces / Lot

Wholesale Price (Lot):	1 +	3 +	15 +	16 +	32 +
	US $341.67	US $334.70	US $317.96	US $314.75	US $313.17

Quantity: 1 Lot

Shipping Cost: **US $0.95** to Switzerland Via China Post Air Mail

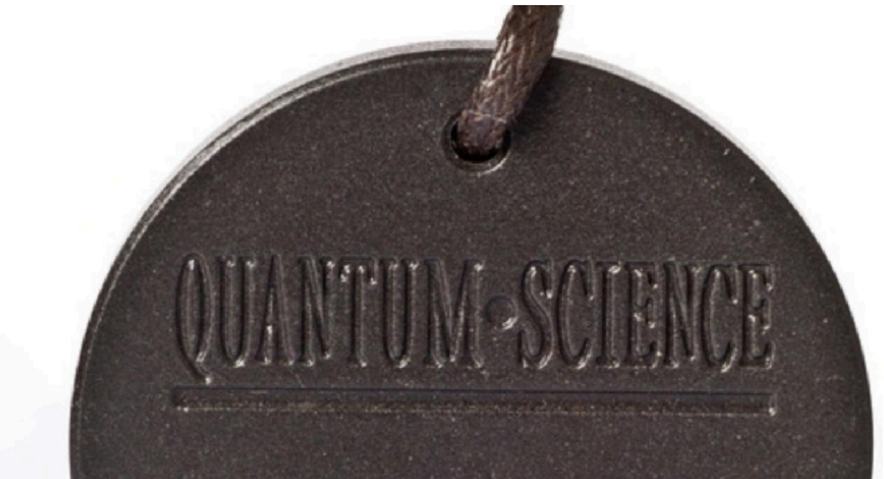
Estimated delivery time: Dec 26 and Jan 5, ships out within 7 business days ?

Total Cost: US $342.62

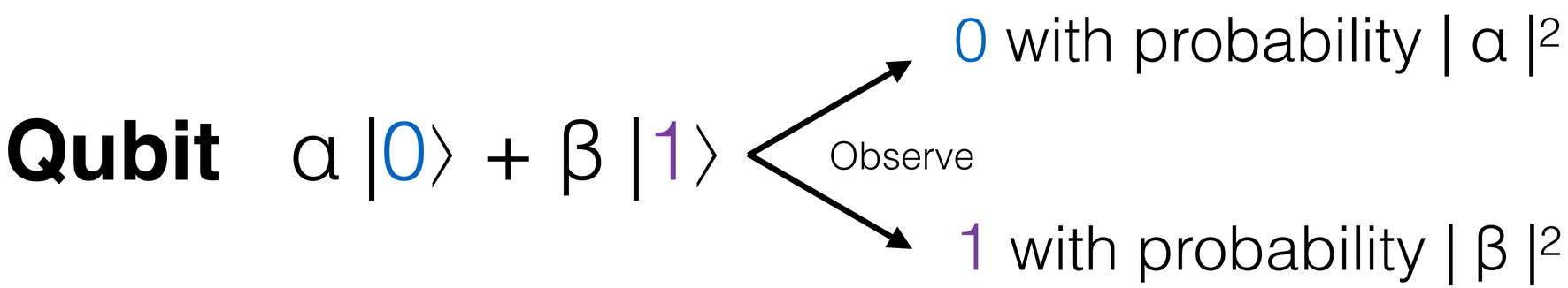
Item sold out Add to Favorite Items (0)

Health Benefits:

1. Reduces inflammation.
2. Promotes unclamping of cells.
3. Enhances immune and endocrine systems.
4. Helps to protect DNA from damage.
5. Improves stamina, endurance and strength.
6. Alleviates soreness, aches and pains, and improves flexibility.
7. Helps to retard the ageing process.
8. Helps to fight cancer cells.
9. Has the ability to destroy viruses and bacteria.
10. Enhances cellular nutrition and detoxification.
11. Enhances cellular permeability.
12. Increases energy.
13. Strengthens the body's biofield preventing electro-magnetic waves from affecting one's health.
14. Increases focus and concentration.
15. Improves blood Circulation.
16. Energizes block cells and reduces "stickiness".



Quantum computer



Stay 0 or 1 forever

Generalizes to more than 2 states: qutrits, qubytes, etc.

Complex, negative "probabilities" (amplitudes), **real randomness**

Quantum computing = reversible evolution of a qubits groups

Quantum parallelism

Quantum computers operate on values in “superposition"

But they **do not try every answer in parallel** and pick the best one

Quantum speedup

When quantum computers can solve a computing problem faster than any classical computers

"**Exponential** quantum speedup”:

Very few computing problems admit a quantum speedup
A quantum computer is not a faster computer!

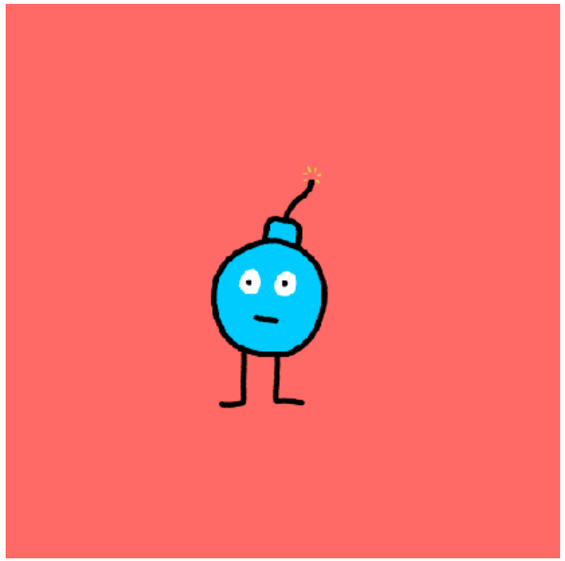
Quantum computing vs. crypto

"Shor's algorithm" solves the following problems efficiently:

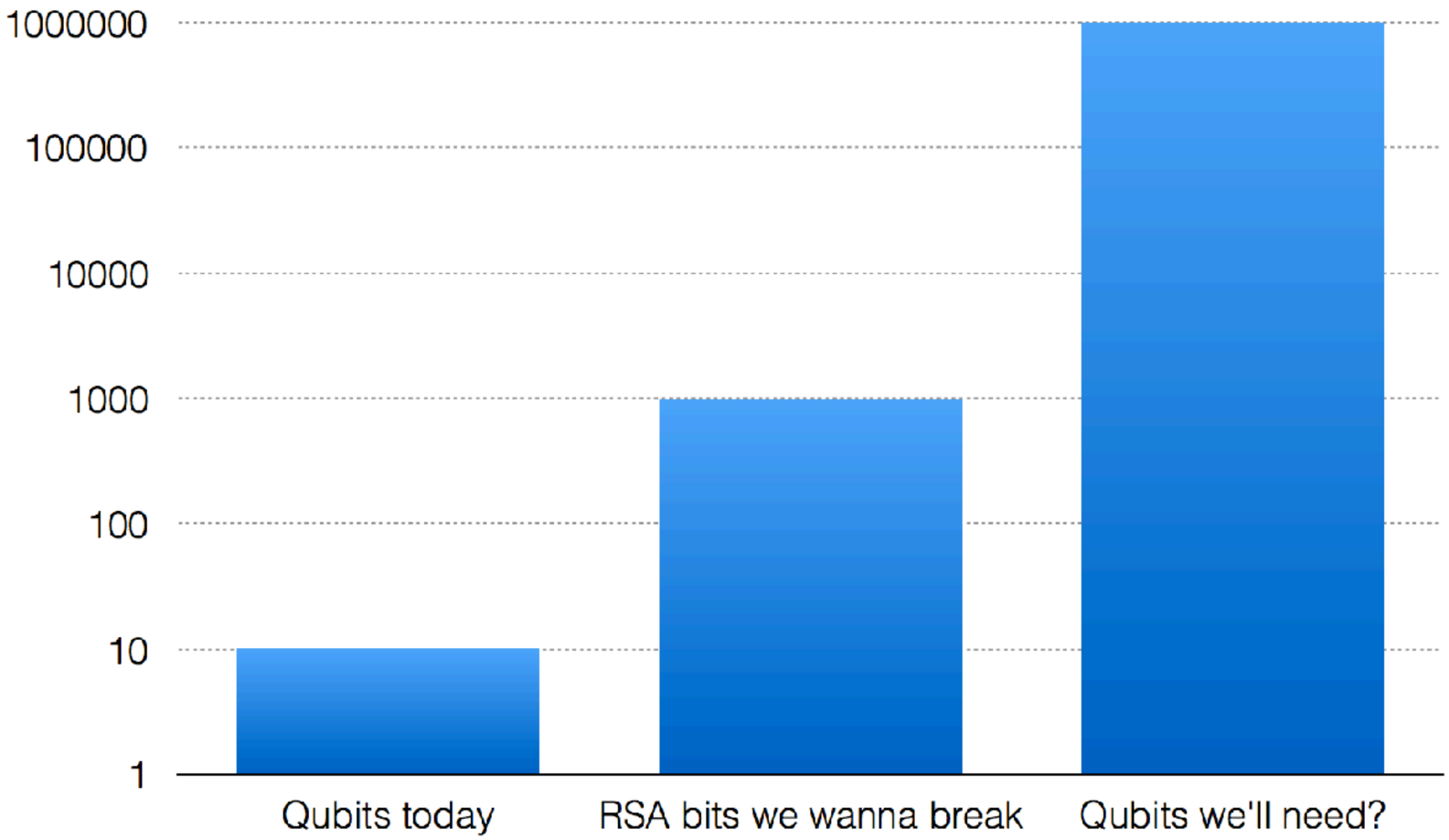
- Finds **p** given **n** = **pq**
- Finds **d** given **y** = $\mathbf{x^d}$ mod **p**

As a result, all public-key crypto is **broken**

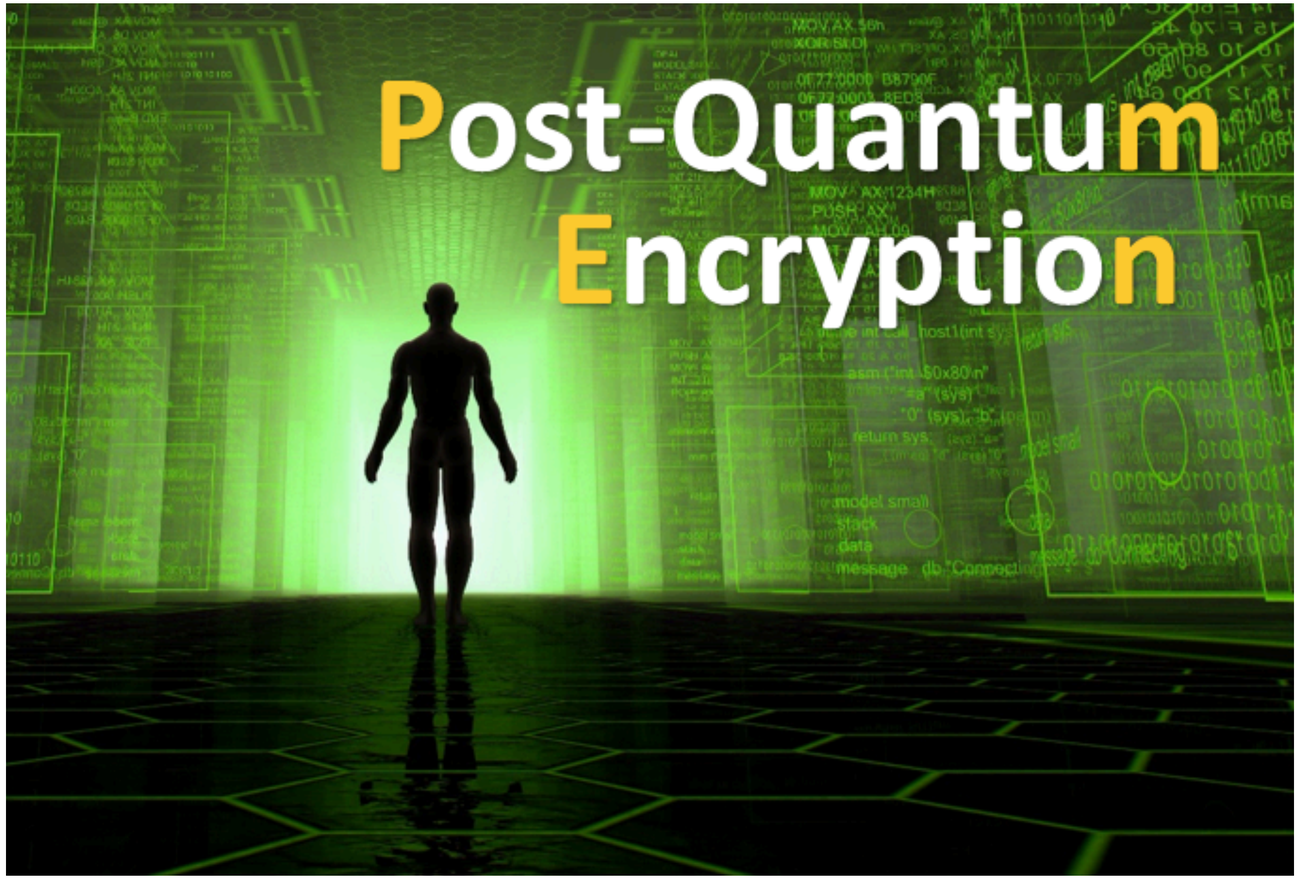
- HTTPS connections, SSH, VPNs
- Bitcoin and most cryptocurrencies



We’re not there yet



(logarithmic scale)


Post-Quantum
Encryption

Post-quantum cryptography

A.k.a. “quantum-safe”, “quantum-resilient”

Algorithms not broken by a quantum computer…

- Must not rely on factoring or discrete logarithm problems
- Must be well-understood with respect to quantum

Has nothing to do with “quantum cryptography” :-)

Why care?

Post-quantum crypto is an **insurance**

CSO reasoning:

- “I think QC has a probability *p* work in year 2YYY”
- "I have information worth $$$ to protect until 2YYY+N"
- “I’d like to eliminate this risk”

Why care?

Post-quantum crypto is an **insurance**

CSO reasoning:

- “I think QC has a probability *p* work in year 2YYY”
- "I have information worth $$$ to protect until 2YYY+N"
- “I’d like to eliminate this risk”
- “And I have reduced all higher risks” (realistic?)

Why care?

NSA recommendations for National Security Systems

"we anticipate a need to shift to quantum-resistant cryptography in the near future."

(In CNSS advisory 02-15)

Post-quantum signatures: the simplest example

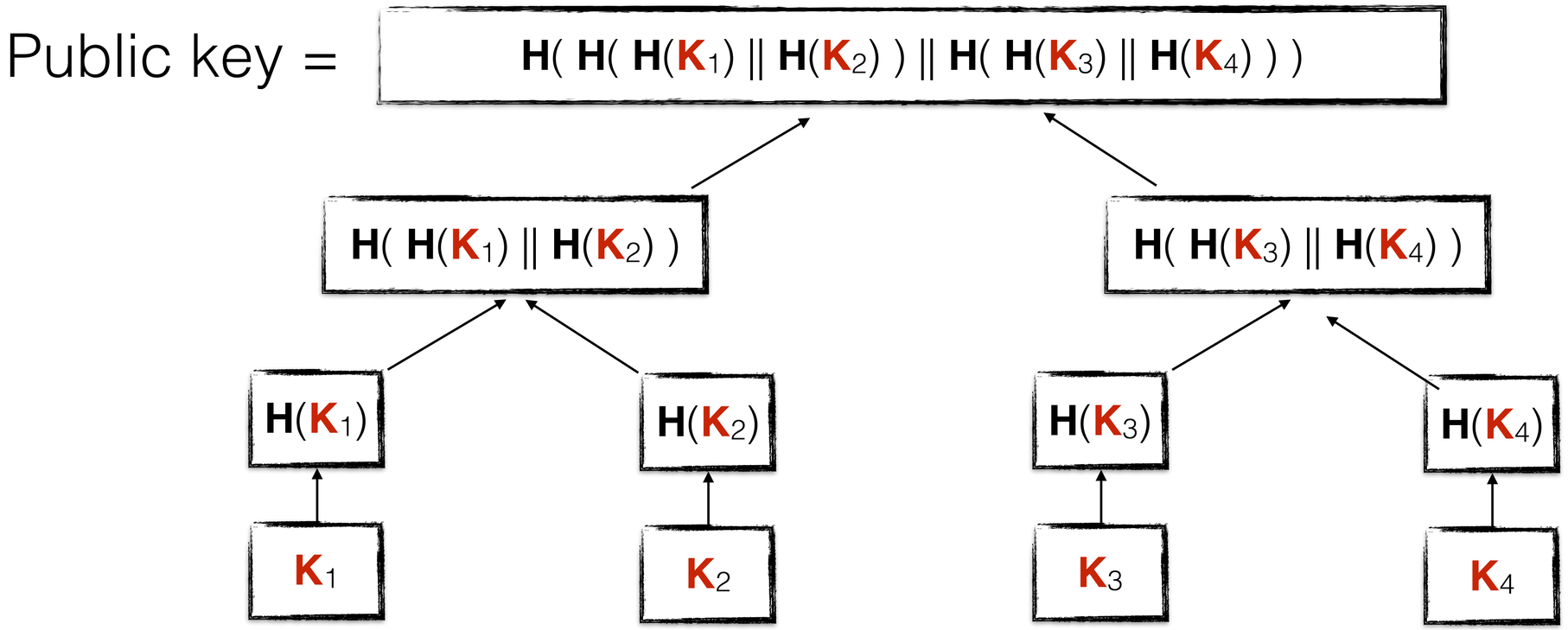
A.k.a. “one-time signatures” (1979)

1. Generate a key pair
   - Pick random strings $\mathbf{K}_0$ and $\mathbf{K}_1$ (the private key)
   - The public key is the two values $\mathbf{H}(\mathbf{K}_0)$, $\mathbf{H}(\mathbf{K}_1)$
2. To sign the bit 0, show $\mathbf{K}_0$, to sign 1 show $\mathbf{K}_1$

Hash-based signatures

Like one-time signatures, but with many keys…

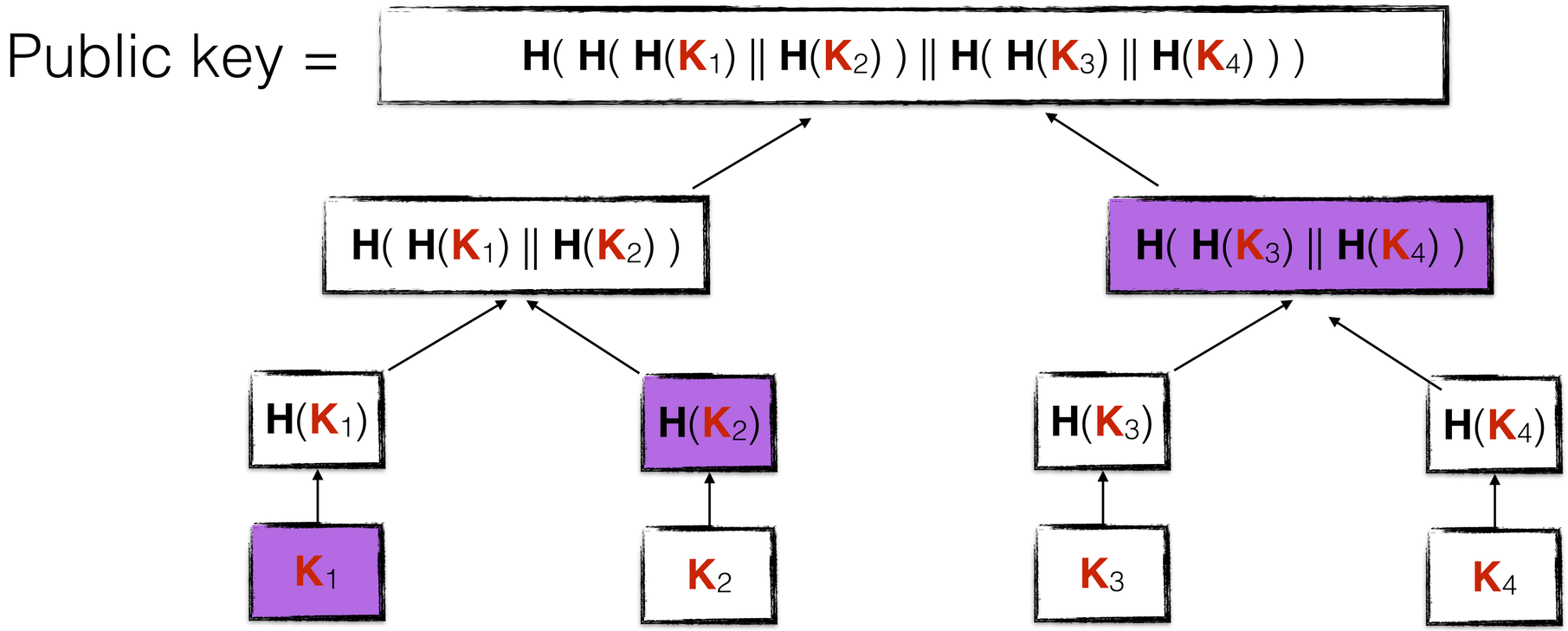
… represented in a compact way, using a **binary tree**



Many-time signatures

When a new one-time key $\mathbf{K}_i$, is used…

… give its **authentication path** to the tree's root



Takeaways

- A quantum computer works directly on subatomic particles, to create **quantum bits** (qubits) that follow quantum mechanics law
- A quantum computer is **not a faster** computer!
- Useful **quantum computers unlikely** before 50 (?) years from now
- You can already buy an insurance! **Post-quantum cryptography**
- **Bitcoin/blockchain can wait**: signatures can be replaced later, unlike encrypted messages

Thank you!

jp.aumasson@kudelskisecurity.com
https://kudelskisecurity.com

https://aumasson.jp
https://twitter.com/veorq