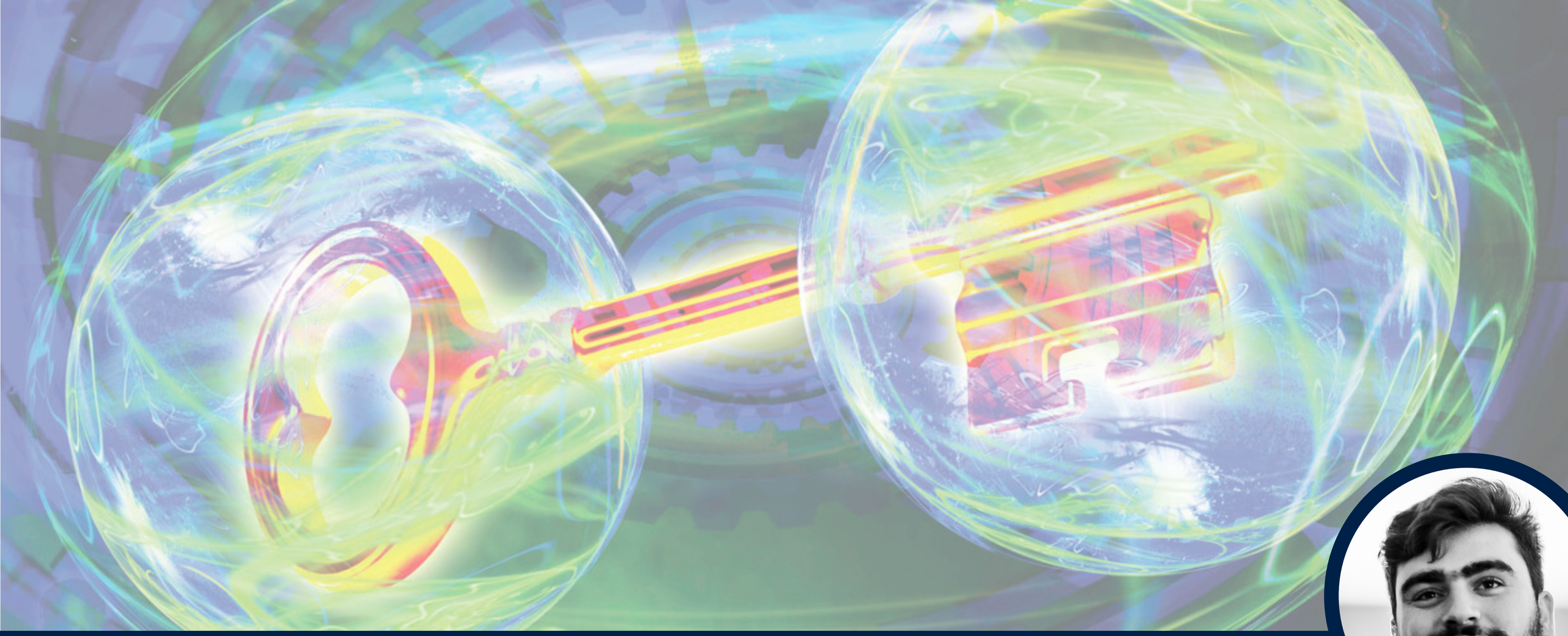


Matthew Gray: Oxford DPhil Student in TCS

Quantum Cryptography

Outline

- Quantum breaking Cryptography
- Cryptography secure against Quantum
- Using Quantum to do Cryptography

Pre-Quantum Cryptography

- RSA
- Diffie-Hellman Key Exchange
- AES

Pre-Quantum Cryptography

- We do not know if these schemes are secure.
- All schemes* are based on assumptions.

Pre-Quantum Cryptography

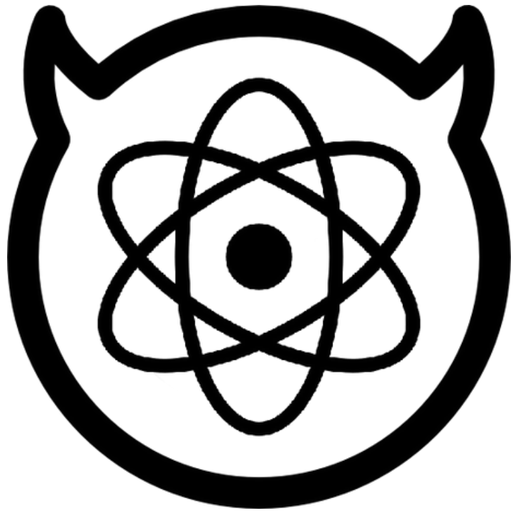
- RSA:
  - Factorization
- DH KE:
  - Discrete Logarithm
- AES:
  - Block Ciphers

Pre-Quantum Cryptography

✗ Factorization

✗ Discrete Logarithm

✓ Block Ciphers

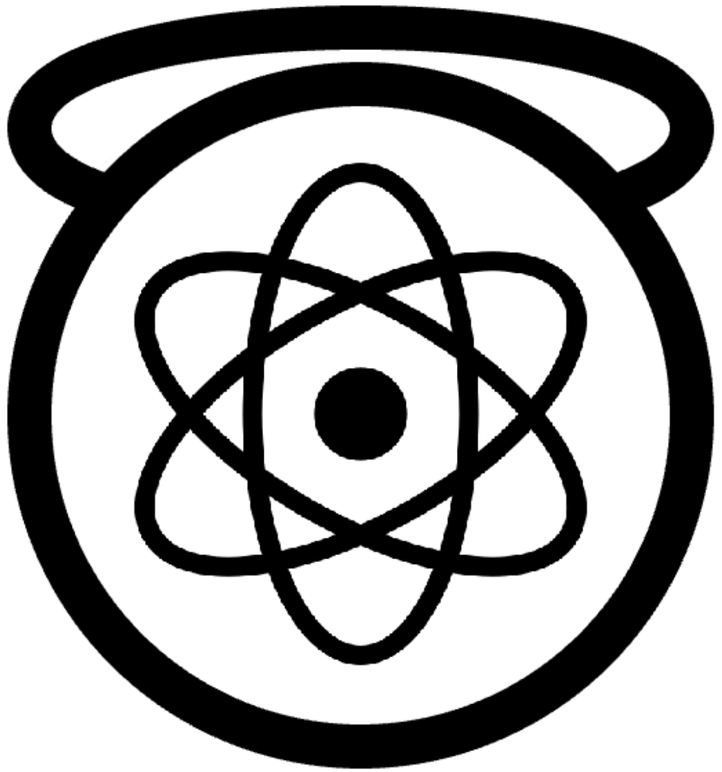


Post-Quantum Cryptography???

- Pretty confident in these.

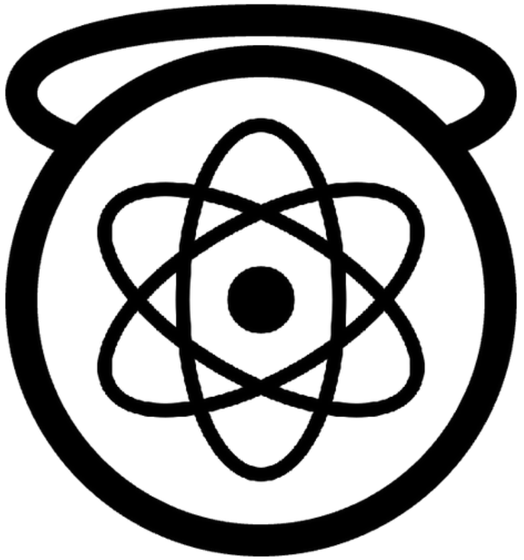
- However, paranoia pays.

Quantum Cryptography?



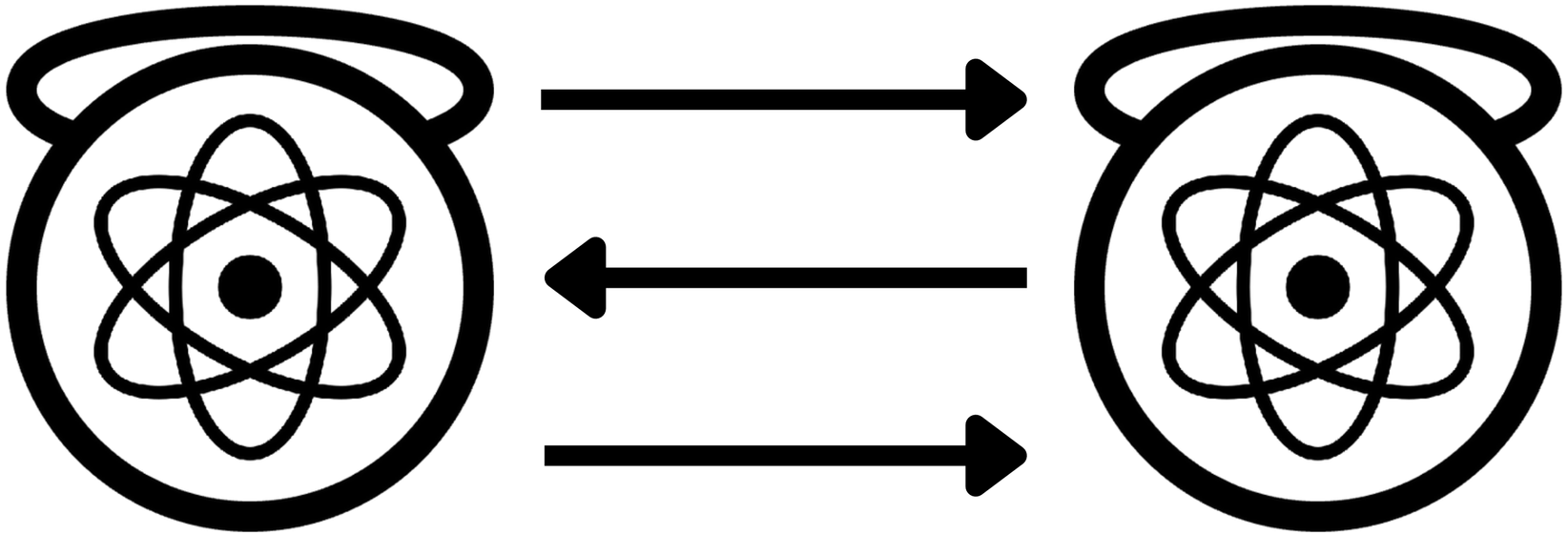
Quantum Cryptography

- New unconditional crypto!
- New functionalities!
- “Post-classical” crypto?



Unconditional Crypto

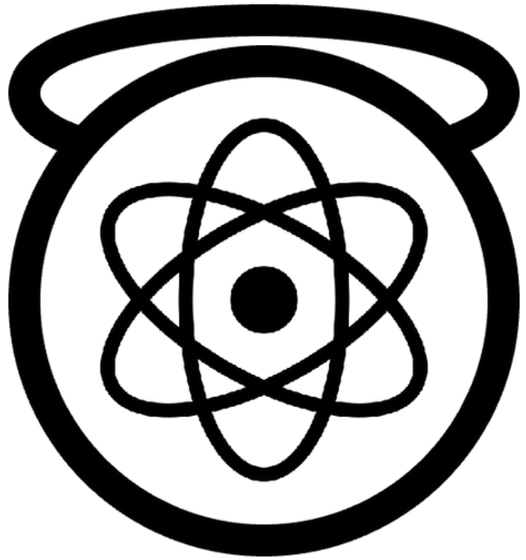
- **Ironclad Key Agreement**



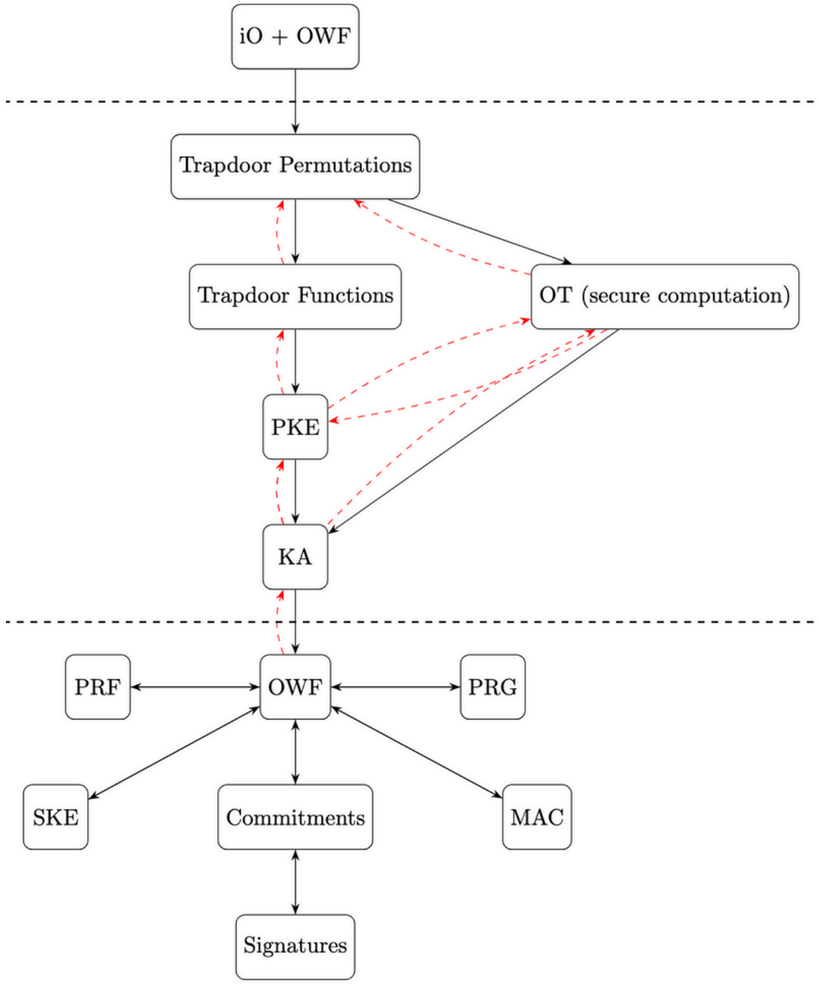
Shared Key

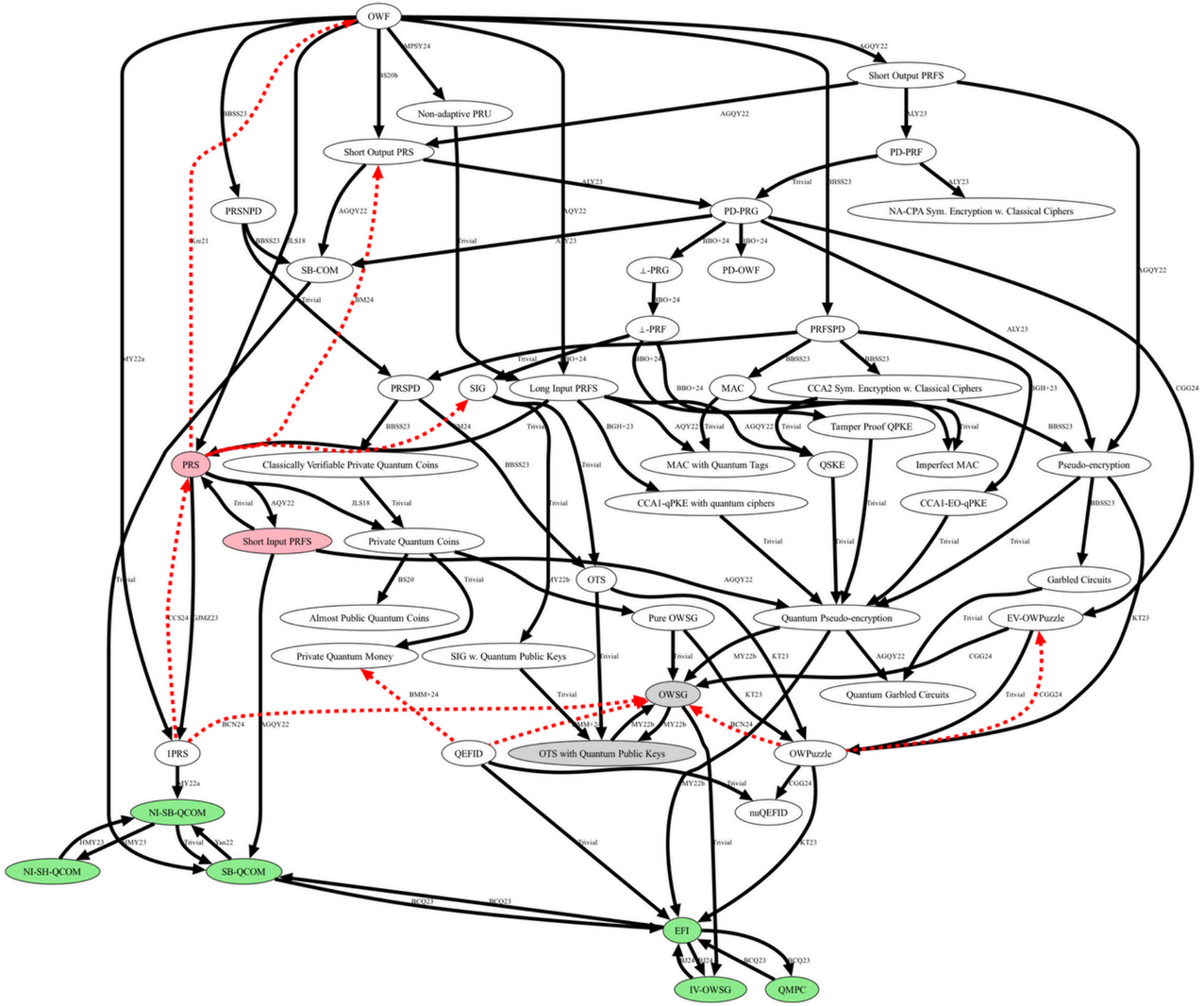
Quantum Functionalities

- “Copy Protection”
- “Certified Deletion”
- “Quantum Money”



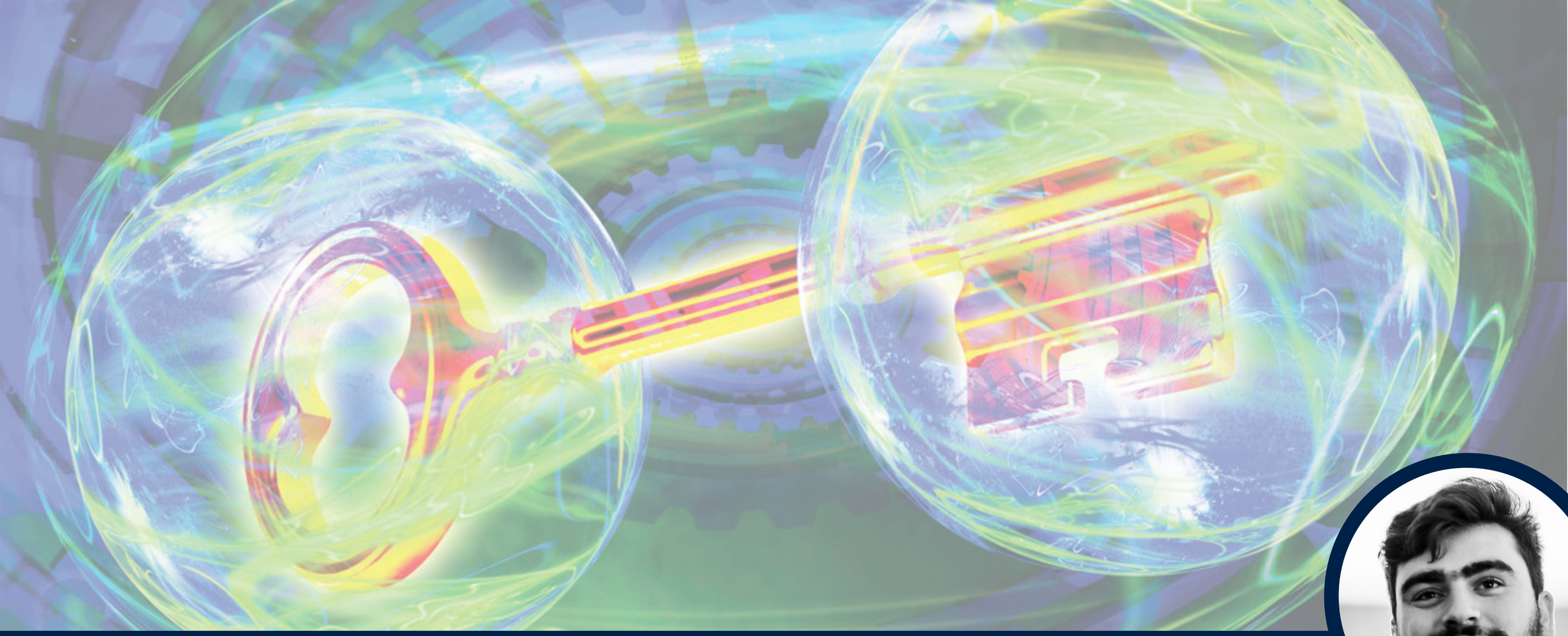
“Post Classical” Cryptography





Takeaways

- Quantum will not break the internet.
- If using post-quantum, use both.
- Exciting new world of quantum cryptography.
- Possible savior of cryptography.



Matthew Gray: Oxford DPhil Student in TCS

Your Questions?