# Classical crypto, quantum queries

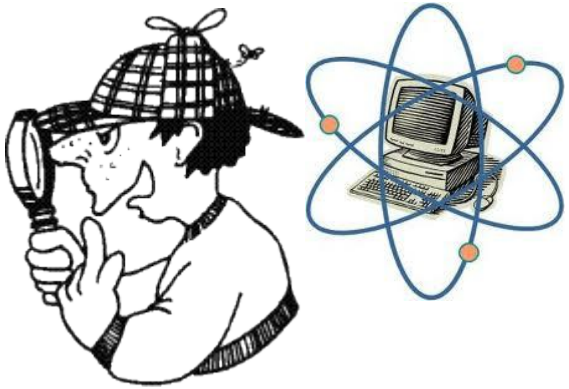
Emily Stark

6.845

# Post-quantum crypto

Crypto construction

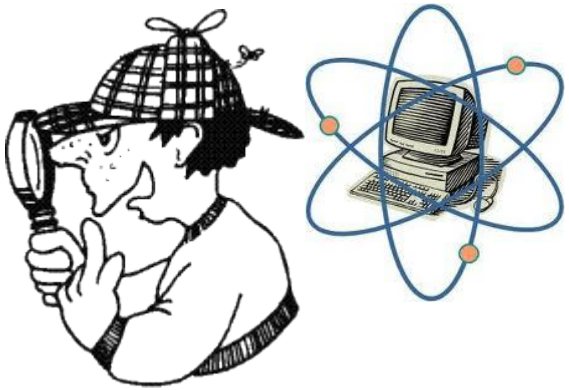
Quantum adversary



# Post-quantum crypto

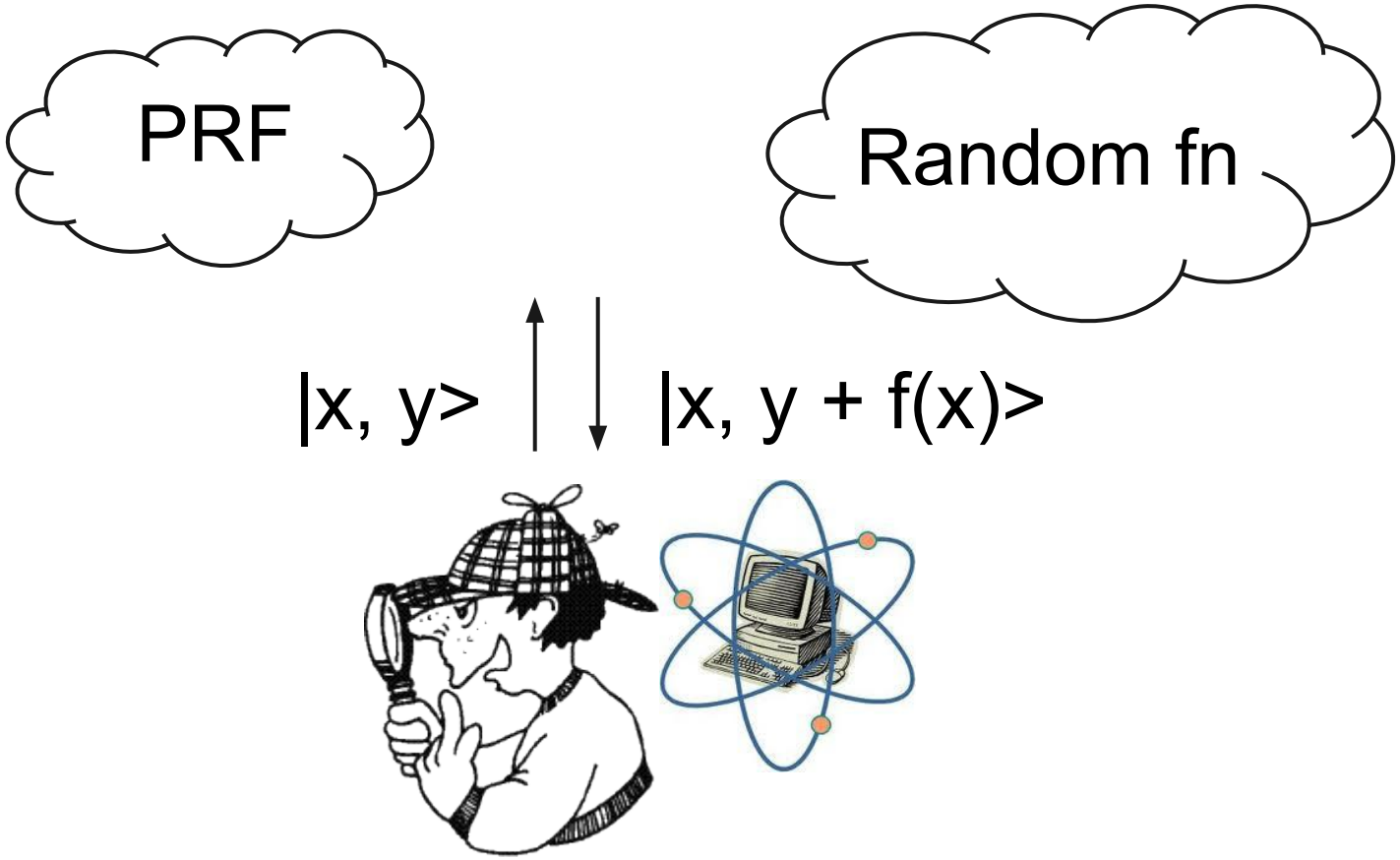
Crypto construction

Quantum adversary



Quantum query power breaks proofs

# Quantum PRF

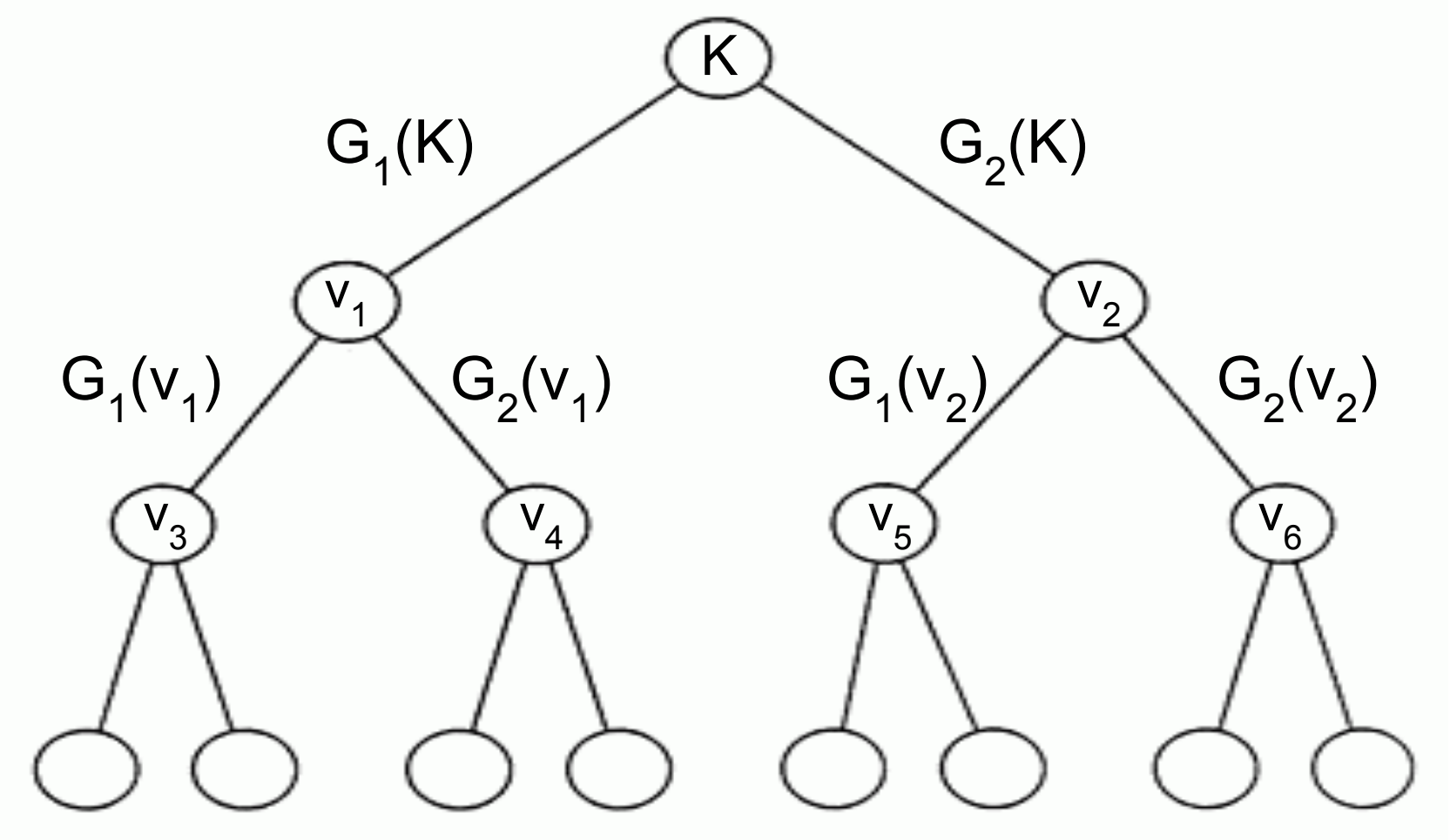


# Are all secure PRFs quantum secure?

No.

$$PRF'((k, a), x) = PRF(k, x \bmod a)$$

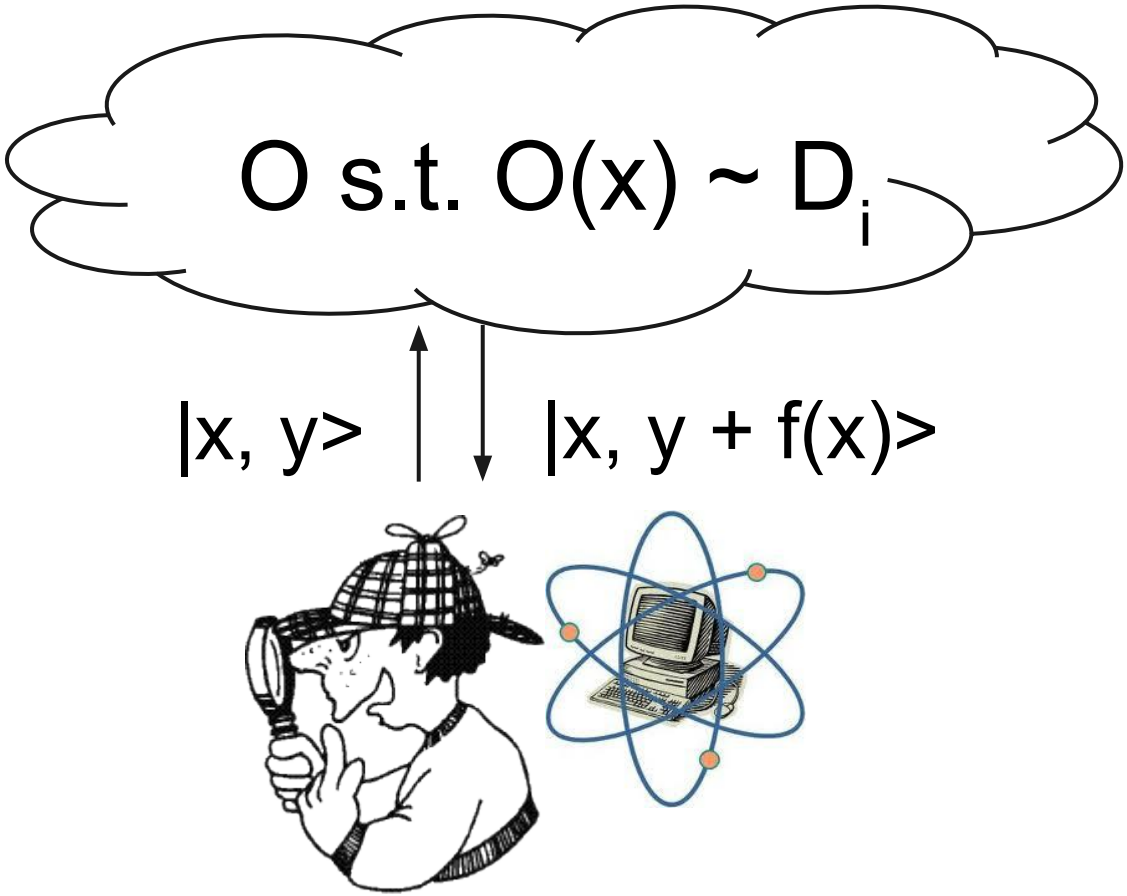
# PRF construction



# Big theorem

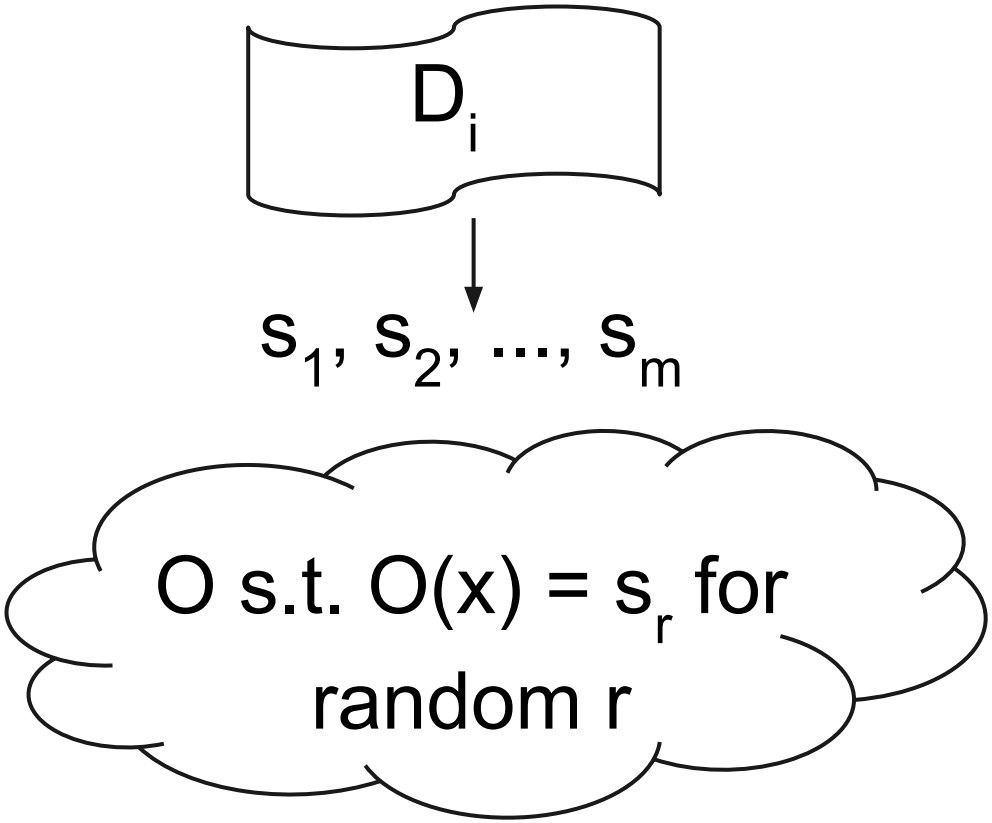
Oracle indistinguishability equivalent to indistinguishability

# Oracle indistinguishability

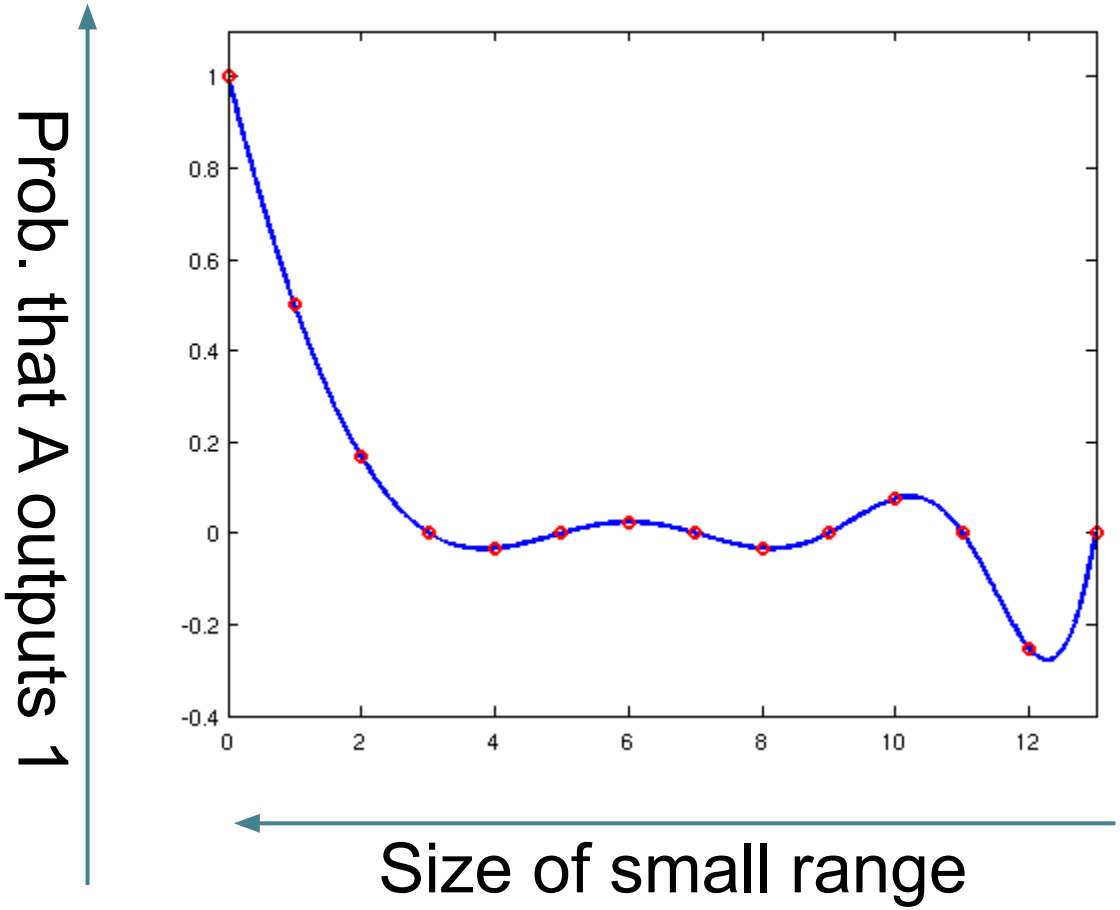


# Grossly simplified proof

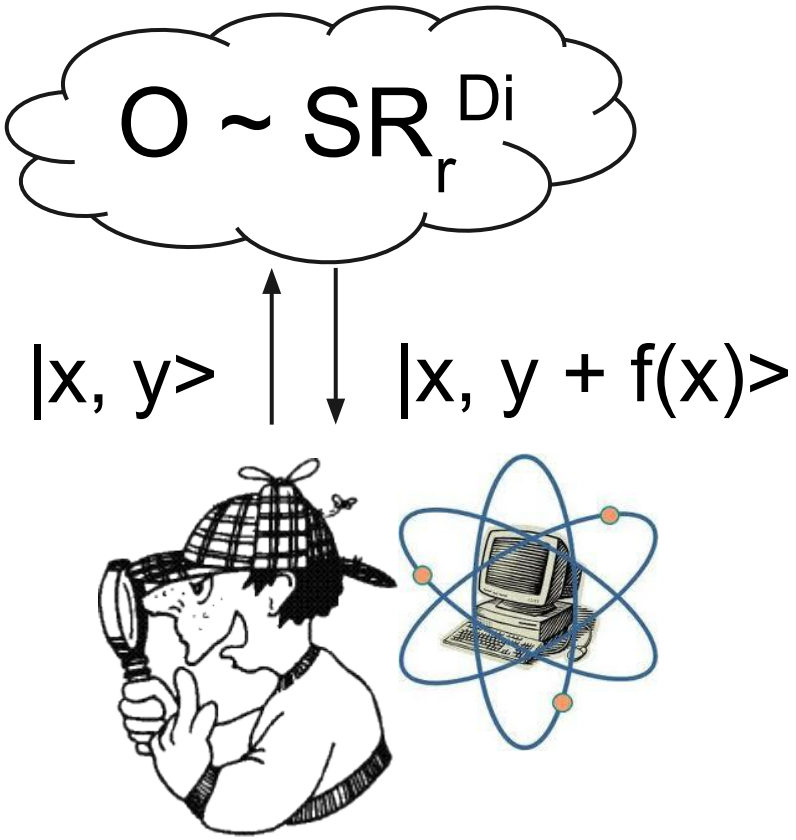
Small range distribution



# Why is SR good enough?



# Simulate with poly samples



# Conclusion

- Random Oracles in a Quantum World (Boneh, Dagdelen, Fischlin, et al. 2011)
- Secure IBE in the Quantum Random Oracle Model (Zhandry 2012)
- How to Construct Quantum Random Functions (Zhandry 2012)
- Quantum-secure Message Authentication Codes (Boneh, Zhandry 2012)