

# Classical crypto, quantum queries

Emily Stark

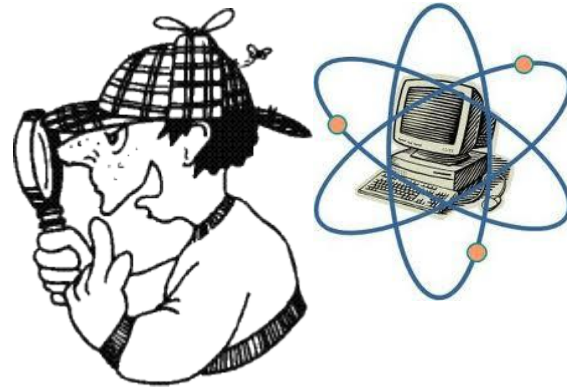
6.845

# Post-quantum crypto

Crypto construction



Quantum adversary

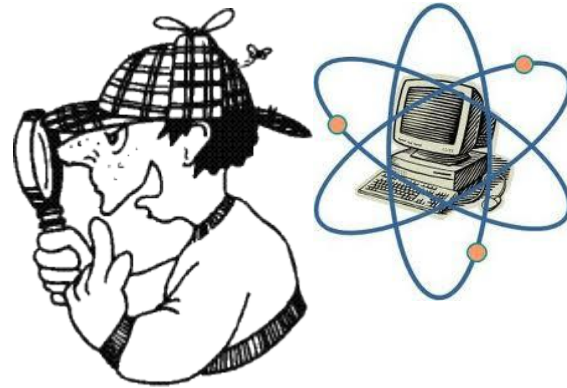


# Post-quantum crypto

Crypto construction



Quantum adversary



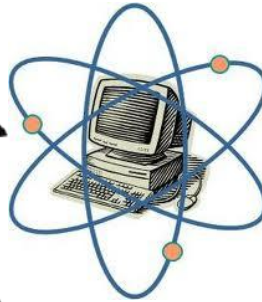
Quantum query power breaks proofs

# Quantum PRF

PRF

Random fn

$|x, y\rangle$   $\begin{array}{c} \uparrow \\ \downarrow \end{array}$   $|x, y + f(x)\rangle$

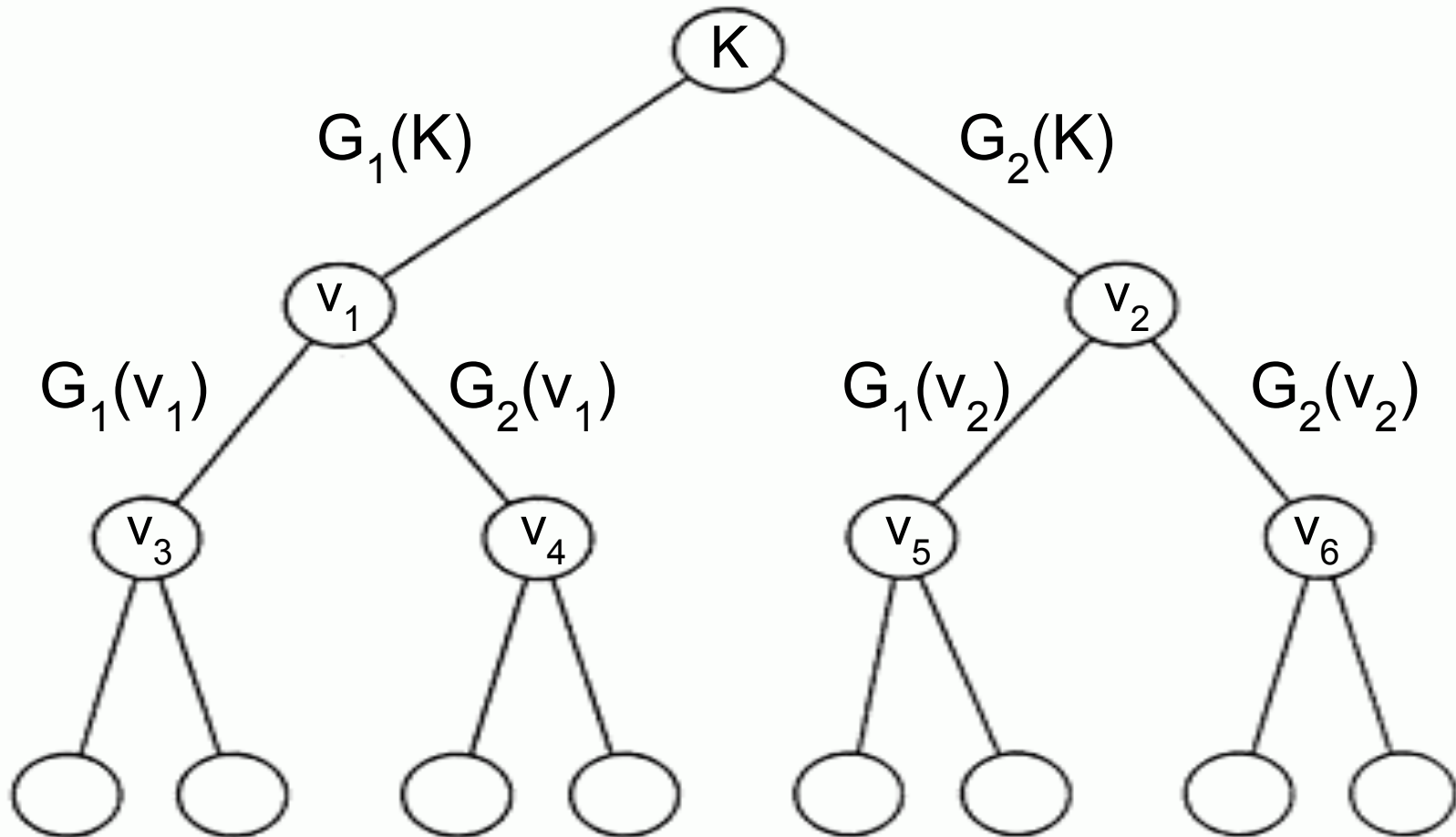


# Are all secure PRFs quantum secure?

No.

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

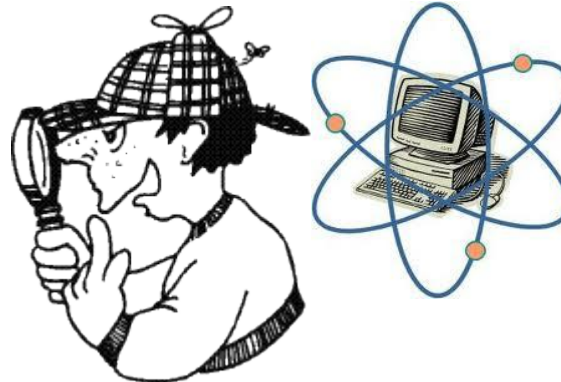
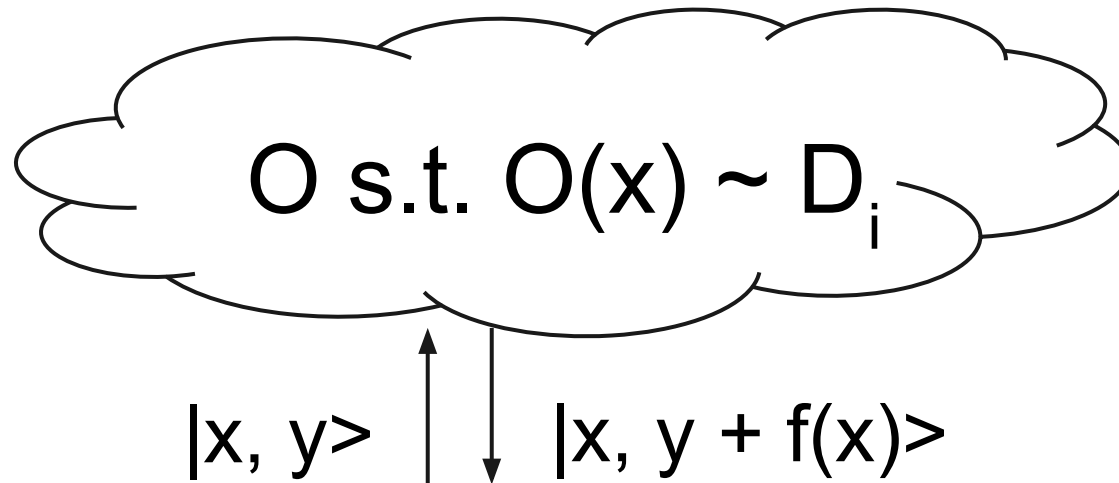
# PRF construction



# Big theorem

Oracle indistinguishability  
equivalent to  
indistinguishability

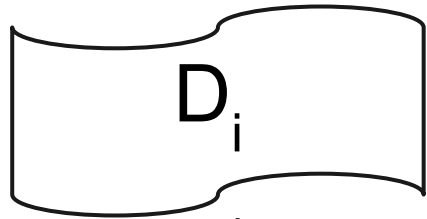
# Oracle indistinguishability



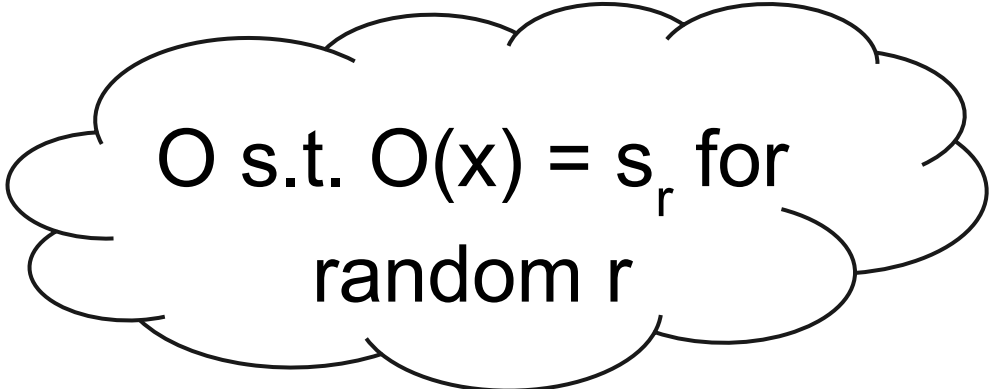


# Grossly simplified proof

Small range distribution



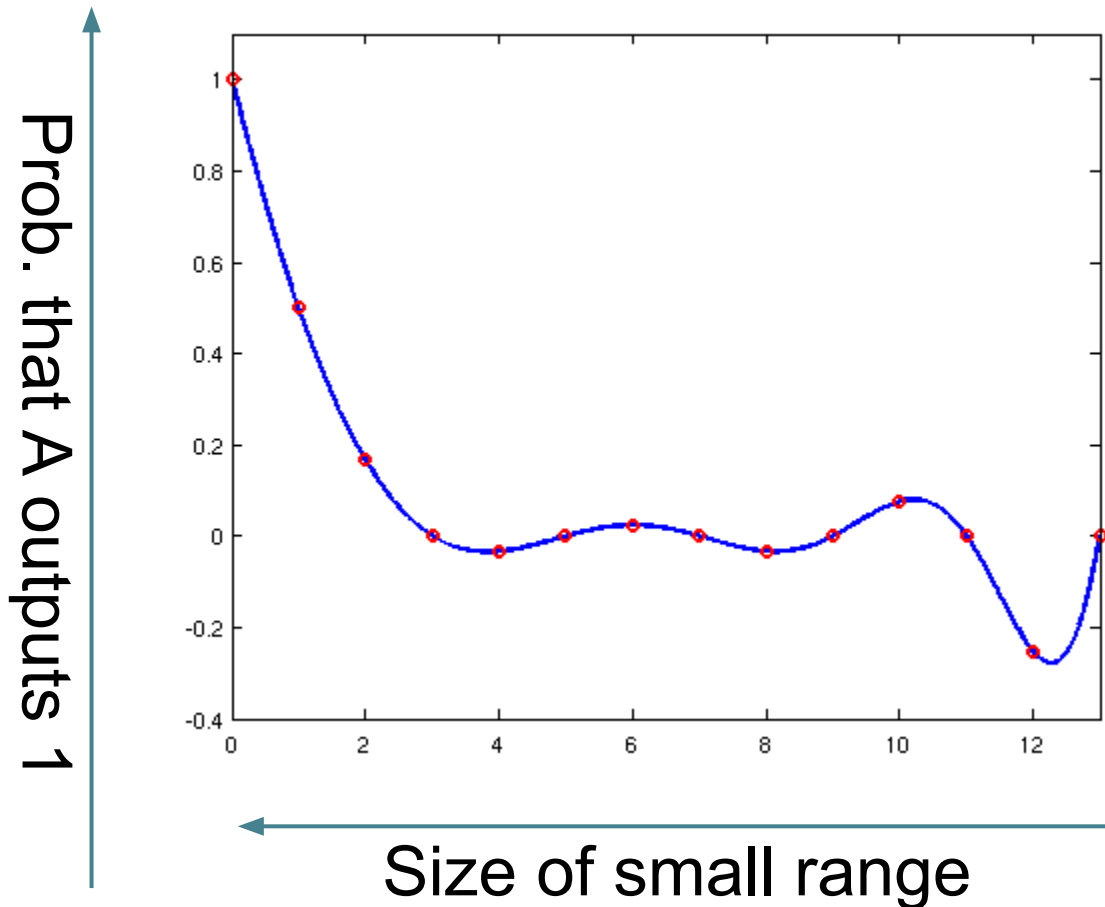
$s_1, s_2, \dots, s_m$



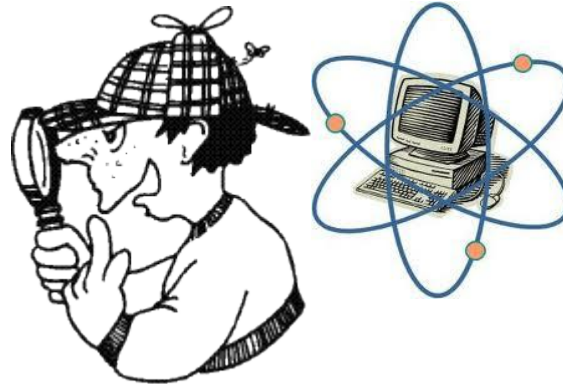
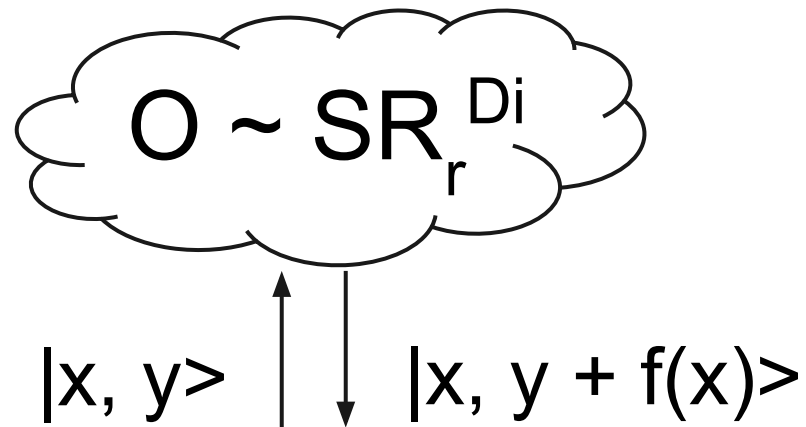
A cloud-shaped diagram containing the constraint text.

O s.t.  $O(x) = s_r$  for  
random  $r$

# 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)