Complexity Assumptions for Cryptographic Schemes

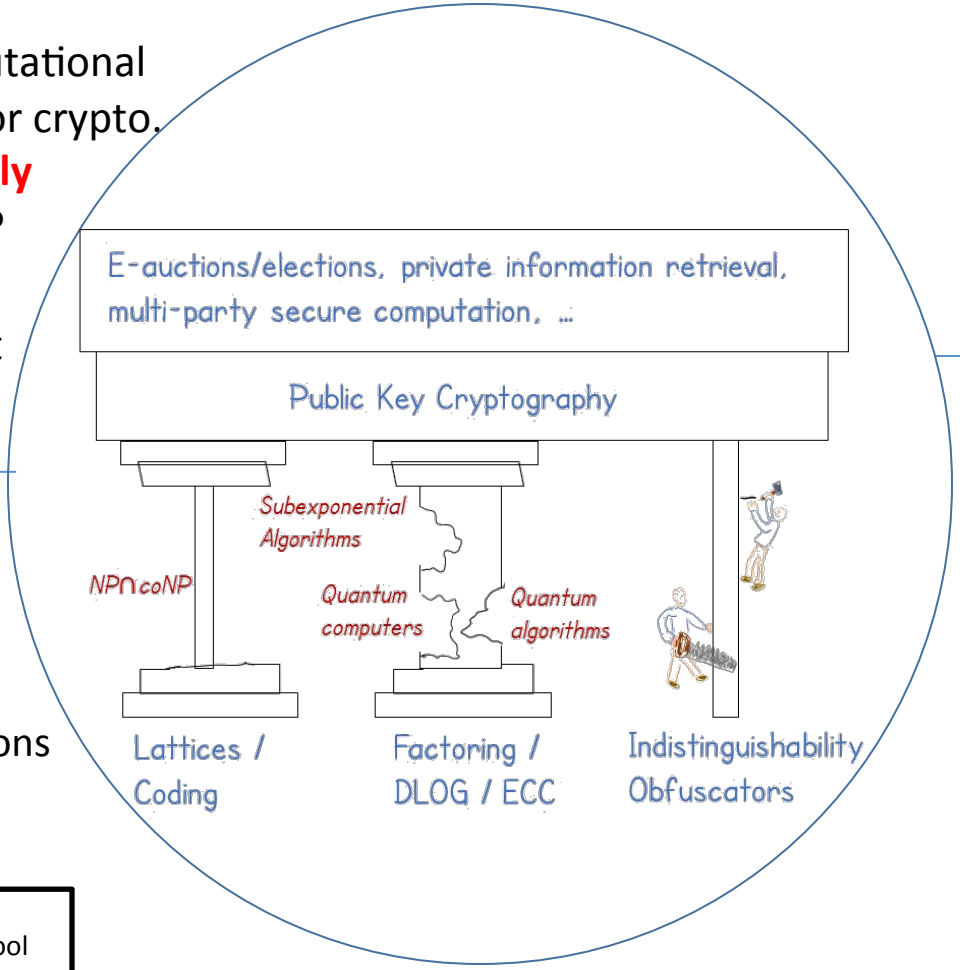
Challenge:

Understand the computational assumptions needed for crypto. Can we use **qualitatively different** assumptions?

What kind of **evidence** can we give for current assumptions?

Solution:

No solutions yet!!
(Project just started)
Talk to me about questions and directions!



Scientific Impact:

- Provide stronger foundations for cryptography.

Broader Impact:

- **Quantum computing** a current **threat** to all widely deployed public key crypto.
- Currently only one family (i.e. lattice based crypto) of PKC with well founded conjecture of quantum resistance – **single point of failure**.
- Alternatives with **sound theoretical basis** are sorely needed.

Award #1618026.

PI: Boaz Barak, Harvard Paulson School
http://www.boazbarak.org
boaz@seas.harvard.edu