**Topic: Data Security**

**Introduction – Problem of Data Security**

* Equifax breach
  + Scope and significance of attack
  + Data was not encrypted
* Development of quantum computers
  + Could break almost every method of encryption currently used
  + Most widely used types of encryption today: RSA and Diffie Hellman key exchange
    - Based on idea that no one could develop algorithms for efficiently computing their solutions
    - Peter Shor developed algorithm in 1994 for quantum computers to efficiently break both of these methods – if/when sufficiently powerful quantum computers are developed, they could break every encryption scheme
* Opinion – data security is one of the foremost problems facing twenty-first century society, in which so much of our data is held online, possibly at a single point of failure (Equifax had social security numbers, addresses, etc.)

**Recent Developments in Data Security**

* Lattice-based cryptography schemes
  + Finding nearest point in lattice with hundreds of spatial dimensions (point associated with private key) given arbitrary location in space (public key)
  + Began in 1980s – too slow to work
  + 1995 – Brown researchers devised new lattice scheme – “cyclic” lattices – that has not been broken since
  + 2005 – Oded Regev (NYU) proved that “learning with errors” schemes are secure against quantum computers as long as they are sufficiently difficult
    - Regev and others then developed similar schemes based on “ideal” lattices that fulfill this condition – called Ring-LWE
* Problem is considered NP hard to find approximate solutions
  + 2009 – Craig Gentry introduced first fully homomorphic encryption scheme, based on a lattice problem

**Usefulness/Value to Society (need to research)**

* Security Innovation now owns NTRU – successor to RSA for protecting financial transactions
  + Approved by Accredited Standards Committed as new encryption standard for data protection
* Little widespread use at this point because of an enormous investment in RSA based security and slow progress towards working quantum computer
* Quick transition if quantum computing made serious progress
* Investment for the future of data security, so breaches like the one at Equifax are not repeated