* Slide 1: Introduction
  + Mobile payment is the method of using your phone to pay for your purchases
    - The two main services for this are Android and Apple pay.
  + Support for these continues to grow each day, and we are able to use it more and more in our daily lives
    - You can use for everything like gas to groceries to restaurants. Basically, if a store supports it, you can use it.
  + However, despite the support from merchants, there’s been a very slow adoption rate for mobile payments in places such as the United Kingdom.
  + This is due to security concerns and theft. People are afraid that hackers and thieves can steal the credit card numbers off their phones and use their money.
* Slide 2:
  + Apple and Android Pay both use NFC, and NFC has a major security flaw. It cannot protect against or detect eavesdropping.
    - Eavesdropping is where hackers intercept and read the data sent by consumers. It’s just like when people eavesdrop on other people’s conversations.
  + The main defense that NFC can use is establishing a secure channel that is encrypted using methods like 3DES or AES
    - Also, Android and Apple pay use a tokenization process when paying. The apps do not pass your actual credit card number when paying. The token card is encrypted and sent to the card reader along with a cryptogram (similar to a public key). These are one time use, so even if a hacker eavesdrops and gets the data, they won’t get your real card.
  + These are all good methods of security but they do not solve the problem of eaves dropping.
* Slide 3:
  + The Solution is Quantum technology: Developed by Dr. Iris Choi and an Oxford University collaboration along with Nokia and Bay Photonics
    - It can detect eavesdropping and other hacking and shut down the system if any of these occur.
    - It works by sending millions of single particles of light for use as encryption keys.
* Slide 4:
  + The system uses movable mirrors and ultrafast LEDs for the data transmission.
    - There are 6 pairs of the LEDs, and each pair has a different polarization and position than every other pair.
      * There is a circularly polarized pair which serves as the main key while the other pairs are used to verify the security of the data transmission as well as correct any errors.
  + This is a picture of the prototype that they had built. It was built using ordinary materials without the need for custom parts.
* Slide 5:
  + To protect against eavesdropping, the system uses an innovative steering system.
    - The lights have to go to an exact position, and any deviation from their path will alter the code being sent and make the system detect an error.
    - An example of this is when a hacker tries to intercept the quantum signal. Even just trying to read the signal will change it just enough that now the code will be wrong.
  + Humans have a natural motion to their hand when trying to keep things still, so to prevent false readings, the researchers were able to counter act this motion. They found the exact measurement of this slight motion and used this to calibrate and optimize the design of the steering system.
  + Also, to prevent the hackers from just guessing or quickly finding out the code, the system uses an extremely long quantum key. So even if the hackers found a way to start decrypting the code, it would take a very long time.
* Slide 6:
  + The prototype is hand held and quite clunky as seen from the previous slide. It works, but it’s a long way from being part of the phones that we use on a daily basis.
  + Dr. Choi believes that the system can be shrunk down into a component that can be put into phones. This process could be aided Nokia since they make phones.
  + Also, by being put into phones, it could be used to create secure connections for NFC and Wi-Fi networks.
  + Most importantly, it could lead to greater public trust in mobile payment security and higher adoption rates for these services.