"Security mainly involves being able to differentiate between a legitimate party and an adversary. Most of the time security provided by any system is due to a secret key shared by the legitimate parties. Hence it is very important to have a very secure way of communicating the key between legitimate parties. In my thesis I along with my guides have built a secure way to establish a key between two parties.

 At present there exists a lot of state-of-the-art key establishment protocols. They mostly rely on advantages which already exists or a more unconventional ones. Some examples or recent approaches are public key infrastructure, physical layer security or privacy amplification. We have used a resource which has not been used much : time. A lot of times the parties involved in a secure key exchange spend a lot of time in close proximity. They are in the same environment and which is mostly secure. We have used the long and mostly uninterrupted interval of time as an advantage to establish a key without use of a third party. "