Term Project Proposal

- **Team member**
  r09221017 / 張霈萱(leader)
  r10921a22/柯以恆
  b07901113 / 廖甜雅
  b09801029 / 張震奕

- **Project title:**
  - **Study of Post-quantum cryptography : NTRU Cryptosystem**
  - **Main Reference and Conference**
    - NTRU and RSA Cryptosystem for Data Security in IoT Environment
    - Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)

- **Project type**
  - (c) reading and implementation

- **Motivation**
  1994 年，Shor's algorithm 問世，無疑為 RSA 的安全性帶來質疑。2011 年 5 月，量子電腦公司 D-Wave Systems 推出了 (arguably) 第一個商用量子電腦，大量的資金與技術開始投入量子電腦的發展，汰換掉 RSA 幾乎勢在必行。因此，我們希望能瞭解 post-quantum cryptography 及 RSA 在相同安全性下，運算速度及 key size 的差異，藉以刻劃未來密碼學可能的發展趨勢。

- **Brief description and expectation**
  透過研讀這篇 paper，了解 NTRU 演算法的基本架構，並比較 NTRU 及 RSA 的效能差異，探討 NTRU 在量子電腦時代的安全性，與未來可以改良的方向。最後，我們將以實作 NTRU 為目標，比較我們做出來的數據與文章提供的數據差異，並提出可能的原因。