**Chengdu University of Technology Oxford Brookes College**

**Project Module (CHC 6096)**

**Weekly Report Sheet**

|  |  |
| --- | --- |
| STUDENT NAME: | Tony |
| STUDENT NUMBER: | 201918020429 |
| SUPERVISOR NAME: | Jakir Hossain |
| DATE: | 2022.3.24 |
| Briefly list all the main tasks you accomplished in the week.   1. Read a lot of papers on improving ECC underlying operations: such as improving ECC point multiplication, such as fast point multiplication, NAF point multiplication, w-NAF point multiplication and so on. 2. Through many research , calculation and understanding of the improved ECC encryption algorithm proposed by Leca et al and other improved ECC encryption algorithms, it was found that they did not design the elliptic curve 3P+Q, so the calculation expression of 3P+Q was derived according to the derivation of their underlying algorithm. Then the expression of 3P+Q is improved to the expression of only one derivative operation, and finally my own improved ECC encryption algorithm is proposed. | |
| Briefly state all the challenges you encountered in the week.   1. The derivation process of 3P+Q is very complicated, and the middle calculation is wrong for many times, especially because there are too many variables, several times because the Angle label is wrong, which leads to an error in the middle of the derivation. 2. The extrapolation process of Leca et al. 's improved ECC encryption algorithm is not complete, only the key steps, so it is difficult to deduce only according to their improved algorithm, and only according to their results to design the improved algorithm. | |
| Briefly Plan out the agenda for next week.  1. Implement my own improved algorithm in JAVA  2. ECC encryption algorithm based on binary point multiplication and ECC encryption algorithm based on NAF point multiplication are implemented in JAVA | |
| SUPERVISOR SIGNATURE: |  |