## Intern Requirement

| | |
|---|---|
| No. of students required | 1 |
| Preferred Discipline | • Computer Science/Computer Engineering |
| Prerequisites/ Skills Required | • Experience in C programming<br>• Sound mathematical grounding<br>• Knowledge of Assembly, GPU programming would be beneficial |

## Project Details

| | |
|---|---|
| Title | Evaluating the Security of Elliptic Curve Cryptography |
| Overview/Background | Elliptic Curve Cryptography (ECC) is a public key cryptography sytem based on elliptic curves over finite fields. Recently, ECC has been gaining in popularity in protecting sensitive information of corporate companies, government and individuals. The security of ECC is therefore crucial, especially in view of new computational advances. |
| Objectives/Scope/ Deliverables | The intern will be required to conduct a survey on the security of ECC. From the survey, the intern will implement algorithms on different computational platforms to evaluate the impact of these algorithms on the security of ECC. He will then assess the impact of each platform on ECC. |
| Project Duration | 2-4 months |