

Intern Requirement

No. of students required	1
Preferred Discipline	<ul style="list-style-type: none">• Mathematics
Prerequisites/ Skills Required	<ul style="list-style-type: none">• Abstract algebra (especially in group theory)• Linear algebra• Elementary number theory• C/C++ programming

Project Details

Title	Pairing-Based Cryptography
Overview/Background	In the realm of Elliptic Curve Cryptography, pairings are currently one of the most active research areas. They first appeared in cryptography during the mid 80's but were destructive as they were applied to transform the ECDLP into a DLP in the multiplicative group of a finite field. However during the first decade of the 21 st century, pairings have ventured in an opposite direction to become the building blocks of cryptosystems with certain functionality.
Objectives/Scope/ Deliverables	<ul style="list-style-type: none">• Research on cryptography using bilinear maps, with the goal focusing on consequences and applications of pairings.• Demonstrate the application of bilinear maps in identity-based signatures and a tripartite DH protocol.• Show the impact of the Tate and Weil pairings on the complexity of the DH problems applied to 2 different groups.• Present a signature scheme for short signatures (via a C/C++ code if possible).
Project Duration	2-4 months