Апарат еліптичних кривих є потужним математичним апаратом, що використовується у сучасній криптології для побудови асиметричних криптосистем: систем цифрового підпису, протоколів обміну ключами, навіть систем шифрування. Особлива увага у останні роки приділяється так званим кривим Едвардса, у зв`язку з їх певними властивостями, зручними для побудови криптосистем.

У будь-якому випадку для побудови криптосистеми на еліптичних кривих необхідно спочатку обрати базову точку – утворюючий елемент деякої циклічної підгрупи групи точок кривої. Ця дипломна робота присвячена, в першу чергу, оптимізації алгоритмів вибору базової точки.

У дипломній роботі наведено огляд основних властивостей еліптичних кривих взагалі (розділ 1), основних властивостей кривих Едвардса (розділ 2), отримано алгоритм добування кореня довільного степеню у групі точок кривої Едвардса (розділ 3), сформульовано та доведено критерії подільності точок кривої на 2, 4 та інші натуральні числа.

З використанням отриманих результатів запропоновано нові алгоритми генерації базової точки кривої Едвардса та проведено детальний порівняльний аналіз нових та класичних алгоритмів