|  |
| --- |
| 橢圓曲線一般式 |
| 交換群的特性 |
| ECDSA 內所使用的是特殊規範的橢圓曲線 |
| ECDSA 使用的交換群符號 |
| ECDSA 會使用的交換群特性 |
| P、Q、R 三點的繪製 |
| 如何進行 ECDSA 點的加法 |
| 如何進行 ECDSA 點的乘法 |
| 質數體的特性 |
| 舉個例子 |
|  |
| 測試（1, 4） |
| 所有符合 d = 1，e = 1，p = 13 的橢圓曲線的點 |
| 測試每個元素有一反元素：           |  |  | | --- | --- | | P | -P | | (0, 1) | (0, 12) | | (1, 4) | (1, 9) | | (4, 2) | (4, 11) | | (5, 1) | (5, 12) | | (7, 0) | (7, 0) | | (8, 1) | (8, 12) | | (10, 6) | (10, 7) | | (11, 2) | (11, 11) | |
| 計算 R 點 |
| 如何計算 |
|  |
| 點的乘法 |
| 透過橢圓曲線及私鑰來建立公鑰 |
| 透過橢圓曲線、私鑰、公鑰來進行簽章 |
| 透過橢圓曲線、私鑰、公鑰來進行驗章 |
| 證明驗章通過 |
| 已知 k 求私鑰 |
| RFC6979 提出較佳的 k 選法 |
|  |