In IC design, a great deal of research focus on the accelerator of cryptographic algorithm. In the related field, ECC (Elliptic Curve Cryptography) is relatively popular, due to its smaller key size with better security. ECC can operate under both binary field and prime field, and each field leads to different hardware design, leading to the diversity of ECC-related research.

In the proposed design, we utilized the lookup table to optimize the whole design. With the lookup table, we can reduce the number of point addition by storing coordinate value of P, 2P, 3P in the lookup table. Compared with traditional double and add algorithm, we can double twice and add once per iteration, and the key shifter will shift two bits per iteration. For the two bits read from key shifter with the value 01, 10, and 11, we utilize the point P, 2P, and 3P, which are stored in lookup table, to execute the point addition. For the two bits read from key shifter with the value 00, we can just execute point double without point addition. As a result, the design can reduce the total execution time, in the expense of the slight increase on overall area.

在IC設計的研究領域裡，有相當多的研究在進行密碼學演算法相關的加速器，其中，橢圓曲線加密由於需要的key size較小，耗能也比其他非對稱式密碼學來得小，而被用在IOT（Internet of Thing）上面。由於橢圓曲線能在質數體以及二元體兩種field下進行運算，相對應的硬體設計也有所不同，因而造成有許多相關的研究蓬勃發展。

而在這次的設計中，我們使用了lookup table來進行運算速度的優化，藉由事先存取P~3P的座標，來讓key shifter能一次shift兩個bit，並且一次讀取兩個bit，讀出來的結果如果是00，則會對點座標直接進行double；如果是01、10、11的話，會讓點座標分別和P、2P、3P的座標做point addition後，再進行point double，進而讓point addition的數量能減少，達成降低減少運算時間的目標。這樣的設計，為的就是在整體面積小幅增加的情況下，讓整體的運算時間下降，達成合理而有效的面積及時間的trade off。