十一、研究計畫中英文摘要：請就本計畫要點作一概述，並依本計畫性質自訂關鍵詞。

（一）計畫中文摘要。（五百字以內）

近年隨著 ID-based 密碼系統的興起，擴大了雙線性配對的應用層面。使得植基於雙線性配對的密碼系統設計，在近代密碼學上佔有一席之地，而利用雙線性配對建構的密碼學相關應用有：加密系統、認證式金鑰協定、數位簽章等等。時至今日，這些相關應用更在近代密碼學研究上扮演一個重要的角色。這些密碼系統的主要特性為其所需之金鑰長度很短，但是卻可以達到相對上的安全需求。不過 Pairing 的計算仍較其他常見的公鑰系統的相關運算複雜與費時，因此 Pairing 計算效能之提升就成為這類密碼系統成敗的關鍵。

而在 Pairing-based 密碼系統中，Pairing 計算佔據最大的計算量，因此對於相關密碼系統來說，如何加速雙線性配對函數的計算就成了一個非常重要的課題。然而第一個能有效率計算 Pairing 的演算法，是由 Miller 在 1986 年所提出，而直到近幾年才再有學者利用不同之概念，提出能增進 Pairing 運算效能的方法。2006 年，學者 Black 等人以共軛直線的概念提出了三種版本的演算法以改善 Miller 演算法[12]，隨後我們也對 Black 等人的前兩個版本提出改進方案[52]。而學者 Wu 等人則利用我們的概念[80]，改進了[12]中第三個版本之計算效率，而在執行先前計畫時，我們也使用更新之技術修正了[52]的缺點。

因此在本計畫的第一年，我們將評估先前計畫的成果應用於 Black 等人第三種版本之可行性，並據以改善在特徵值為 3 基本體之 Pairing 計算效率。最後整合出一套可適用於所有版本之有效率的 Pairing 計算模式，並在完成效能分析與正確性證明後撰寫成論文發表。

而計畫的第二年，我們將應用計畫第一年所得之成果，針對在網路環境中計算能力受限之行動裝置，進行 Pairing 計算負載之評估。在完成相關評估後設計出合於需求之不對稱型態之 Pairing 計算模式。

關鍵詞：橢圓曲線密碼系統、雙線性配對密碼系統、Pairing 計算、Miller 演算法、密碼學。