摘要

混沌系統具有不規則，非周期性，無法預測和對於初始條件相當敏感的特質。而這些特質符合與密碼學上混亂和擴散的特性。因此，近年來混沌系統在密碼學上的應用被廣泛的討論與研究。然而，當混沌系統數位化的過程中，原先所保有的混沌特質產生了變化，這種現象又稱為動態特性的降低。一個明顯的例子就是數位化的混沌系統容易產生出一個短周期的輸出軌道。而一個短周期的軌道在統計學的角度上則是容易被分析且不適合應用於密碼系統。在這一篇論文中，我們將研究動態退化的現象並且提出數個方法來提升數位化混沌系統的隨機品質。主要的研究內容如下。首先，我們提出了強化型邏輯映射混沌系統。此系統擁有比傳統邏輯映射混沌系統更大範圍的可用參數，而且這個可用參數範圍內不會存在短周期的參數。基於強化型邏輯映射混沌系統，我們更提出了強化型多維度混沌系統，使其具有更多的可用參數來應用於安全傳輸系統。第二，我們提出了變化型邏輯映射混沌系統。此系統明顯的增加了單位時間的輸出量與隨機品質。此外我們串接數個變化型邏輯映射混沌系統來建立多變化型邏輯映射混沌系統，使其 可容易擴張，並可以快速的產生具有高複雜度與長週期特性的混沌數列。最後，在本論文的第三部分則是針對偽隨機變數產生器應用提出了數位化變更型邏輯映射混沌系統。在這個系統中我們使用了參數選擇與擾動技術，我們有效的減少了系統的計算量並提高了輸出的複雜度。在現行的偽隨機亂數數列測試平台測試結果顯示，相比於先前所提出的混沌偽隨機亂數產生器，我們的系統使用了較低的硬體成本產生了較高隨機品質的偽隨機數列。