中華大學電機工程研究所碩士, 1996

適用於有限場 GF(2m)之算術運算單元電路架構研究
A VLSI Architecture of Arithmetic Unit for Finite Field GF(2m)

陳棟洲

中文摘要

有限場(finite fields）的理論在通訊及電腦領域中，扮演著一個很重要的角色。而在這些有限場中，有限場 GF(2m)更是經常被廣泛地應用。目前有關於有限場 GF(2m)運算電路架構的研究，大部分皆偏向於追求快速的運算架構。然而，這些快速運算的架構往往在硬體電路上是複雜且龐大的，而不容易被實現。對於某些通訊系統（例如，無線個人通訊服務(PCS) 系統）而言，傳送資料的速率(bit rate)並不是如此的快，但是系統的硬體部分卻必須要非常地轉便。因此，研究一個具備低電路複雜度(lowcircuit complexity) 的有限場 GF(2m)運算架構是有其價值性。另一方面，目前已有數個運算於有限場 GF(2m)的電路架構已被提出。然而，這些架構中的大部分都只是被設計來完成有限場 GF(2m)的單一基本運算（乘法運算(multiplication)、乘法反元素運算(multiplicative inverse)、除法運算(division)及指數運算(exponentiation)。本論文提出一個整合所有有限場 GF(2m)基本運算於單一架構的概念。這個架構是多功能且具備低電路複雜度的特性。一個運算於有限場 GF(2m)的運算單元(Arithmetic Unit, AU) 架構在本論文中提出。這個運算單元是架構在細胞陣列次方和 AB2+C 電路(cellular-array power-sum AB2+C circuit)之上，且採用了管線式(pipeline)的架構。這個運算單元能夠執行有限場
GF(2m)中所有的算術運算。以這個運算單元爲基礎，我們預期未來能設計出一個適用於有限場 GF(2m)的特殊數位處理器(special purpose DSP chip)。利用此數位處理器(DSP chip)，使用者將可很容易地對各種錯誤更正碼(error-correcting codes)製作出低電路複雜度的解碼器(decoder) 。

關鍵字：電機工程; 有限場; 乘法運算; 除法運算
Key words：ELECTRICAL-ENGINEERING; GF(2m); FINITE FIELDS; MULTIPLICATION