200834411

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：96104248

※ 申請日期：96.2.6　　※IPC 分類：H04B7/535 (2006.01)

一、發明名稱：（中文/英文）

有限場除法器架構之實現方法

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

國立交通大學

代表人：（中文/英文）吳重雨

住居所或營業所地址：（中文/英文）

新竹市大學路 1001 號

國　籍：（中文/英文）　中華民國 TW

三、發明人：（共 2 人）

姓　名：（中文/英文）

1、吳昭逸

2、張錫嘉

國　籍：（中文/英文）

（均同）中華民國 TW

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

本發明是關於一種有限場除法器架構之實現方法。藉由將所有的除法器標準基礎輸入轉換到合成域，在這個網域下用子域的乘法器，平方器，加法器，查表來完成電路，而之後再將其從合成域轉換回標準基礎的有限體下。使用者可以在一個時脈週其下完成除法運算，並且達到低複雜度的須求。在許多有限場的運算上，支援這樣的除法電路是相當有幫助的，例如解RS/BCH碼或是ECC/Security 處理器的應用。

六、英文發明摘要：

七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明:

無

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

九、發明說明：

【發明所屬之技術領域】

本發明是關於一種除法器，特別是一種有限場除法器架構之實現方法。

【先前技術】

現今很多數位電子產品如數位電視衛星廣播、隨身碟和硬碟等產品，都一定會使用到相關有限場的運算。一些常見的有限場運算包含 BCH/RS 碼、AES 碼、Ellipse Curve 密碼以及錯誤控制碼/密碼處理器等。這些碼被廣泛利用在許多應用上，例如高速傳輸的 DVB-S2 和 DVB-S1、儲存裝置的快閃記憶體和硬碟以及 ECC/Security 嵌入式處理器相關之系統廠商與 IC、IP(矽智產)設計產業。

然而在解 RS 碼/BCH 碼或 AES 密碼等相關有限場運算裡，過去會認為有限場除法器是很難實現的硬體，所以傳統上在解有限場相關的系統會將其演算法更改成不須要算除法或逆序(Inverse)的演算法，但是如果避開除法的話，運算週期的數量將會比能夠支援除法的演算法大很多，例如 BCH/RS 解碼器的關鍵多項式及錯誤值解碼電路。另外由於以處理器為基礎的設計是未來的趨勢，若是有限場相關應用的處理器能夠客製一道除法運算的指令集，將會大大的提升設計的優勢。

過去的文獻以及發明很少在有限場的領域裡做位元平行的除法運算，而有許多的論文在平行的有限場算術做逆序。而逆序的方法有許多種：

(1) 利用費馬定理用 m 個週期做出逆序。但多週期為其缺點，而若想得到除法的機能性，須將後端再加一個乘法，那麼總共將會是 m+1 個週期。

(2) 暴力法查表(查出逆序)的方式，然後再串上一個乘法器。但缺點為面積

太大。大約我們的位元數(m)小於等於 8 時，查表法大約等於一個同位元數的雙變數乘法器。但是當 m 大於 9 時，查表法的硬體複雜度會相當的高，例如當 m=10 時，其閘道計算約為 4.2k。若時應用於 GF(2^{16})與 GF(2^{14})的 DVB-S2 BCH 解碼器系統，那麼使用查表法更是合成不出來的。

(3) 利用合成域做出逆序 (Rijndael inversion)，此法可以把逆序轉換到子域而達到低複雜度的結果，但其功能並不如除法器這麼的吸引人。

為了克服逆序技術的缺失，本發明提出了一種使用合成域來設計並只須要一個時脈週期的低複雜度除法器實現方法。

【發明內容】

本發明是關於一種有限場除法器架構之實現方法。藉由將所有含有較高位元的除法器標準基礎輸入轉換到複數個位元較小的合成域網域，然後透過不同的搭配來用資料路徑較小的運算單元、包括查表、平方器、雙變數乘法器、常數乘方器等完成一個關鍵路徑並取代資料路徑數比較長的除法運算，最後再將所得到的結果轉換到標準基礎網域。如此一來可以大幅降低運算與製成的複雜度，並同時可以讓這個過程都在單一時脈下達成。該方式可以將當位元數很長的除法算法的面積降得很低，並且所使用的關鍵路徑與利用合成域所做出來的逆序是一樣的。

【實施方式】

本發明是關於一種有限場除法器架構之實現方法，藉由將所有的輸入轉換到合成域網域，然後用資料路徑較小的運算單元來完成一個資料路徑

較長的除法運算，再將所得到的結果轉換到標準基礎網域已達成一種除法器。

合成域是一種擴張域，而它的基本域(Ground Field GF)是佈於 $GF(2^n)$ 而不是 GF(2)，下例以一個較佳實施例來說明。假如 α 屬於 $GF((2^2)^2)$，可以將其寫成 $\alpha=a_1x+a_0$，而 a_1, a_0 屬於 $GF(2^2)$，例如 $\alpha=\{10\}x+\{11\}$。假如 α 屬於 $GF((2^3)^3)$，可以將其寫成 $\alpha=a_2x^2+a_1x+a_0$，而 a_2, a_1, a_0 屬於 $GF(2^3)$，例如 $\alpha=\{110\}x^2+\{011\}x+\{100\}$ 以此類推。本發明的概念就是將一般標準基礎下的有限場的加減乘除運算轉換到這個合成域下來做，完成除法運算後再將其轉換回標準基礎。此法可應用於 BCH/RS 解碼器或有相關於有限場的應用上面，例如 BCH/RS 解碼器在解關鍵多項式或解值的 Foeney 演算法上面時常會遇到除法的運算。

以下是一個實施例說明如何導入一個除法運算，舉一個應用於 Reed Solomon 解碼器的 10 位元除法器的實例。本發明將 10 位元的標準基礎網域轉換到兩個 5 位元的合成域網域以降低複雜度，再透過比較小的(m=5)的資料路徑，例如變數乘法器、常數乘法器、加法器、逆序表、平方器等等來完成演算法和電路。本發明的關鍵路徑和利用合成域所做出來的逆序是一樣的，同時也是將查逆序的動作轉到子域下面來進行，例如關鍵路徑可以為：2 子域乘法器+加法器(1 XOR)+子域 LUT。下例中是執行 kx+q 除以 bx+c 的運算，如第 1 圖所示，假設 kx+q 與 bx+c 已經先被轉換到合成域網域，kx+q/bx+c 的演算法可以如下：

$$\frac{kx+q}{bx+c}=(kx+q)[b(b^2w^3+bc+c^2)^{-1}+(b+c)(b^2w^3+bc+c^2)^{-1}]$$
$$=(b^2w^3+bc+c^2)^{-1}(bx+b+c)(kx+q)$$
$$=(b^2w^3+bc+c^2)^{-1}(kbx^2+kbx+kcx+qbx+qb+qc)$$
$$=(b^2w^3+bc+c^2)^{-1}(kb(x+w^3)+kbx+kcx+qbx+qb+qc)$$
$$=(b^2w^3+bc+c^2)^{-1}(kbw^3+kcx+qbx+qb+qc)$$
$$=(b^2w^3+bc+c^2)^{-1}((kc+qb)x+kbw^3+qb+qc)$$

其中在該演算式裡，GF(2^5)的本質多項式(Primitive Polynomial)是x^5+x^2+1，GF(2^{10})的本質多項式(Primitive Polynomial)是$x^{10}+x^3+1$以及GF((2^5)^2)的莫尼克(Monic)本質多項式是x^2+x+w^3，其中w^3代表 01000 而w是GF(2^5)的原根。透過這個演算式可以證實假設在 0.18um 的製程下，一個 10 位元的有限場除法器可以合成到 180MHz，而且只用了約 1K 的閘道數量，約 2 個同樣寬度的變數乘法器並同時具備低複雜度。而且主要的重點是整個過程都是在單一時脈下完成。因此若將其應用在有限場相關領域的應用上將是非常吸引設計者的架構。

惟以上所述者，僅為本發明之較佳實施例而已，並非用來限定本發明實施之範圍。故即凡依本發明申請範圍所述之形狀、構造、特徵及精神所為之均等變化或修飾，均應包括於本發明之申請專利範圍內。

【圖式簡單說明】

第 1 圖為 10 位元除法器示意圖。

【主要元件符號說明】

無

十、申請專利範圍：

1. 一種有限場除法器的架構方法，包含：

將含有較高位元的除法運算標準基礎輸入從基礎網域轉換到複數個位元較小的合成域網域;

在該合成域網域透過複數個資料路徑較小的運算單元來完成一個關鍵路徑並取代資料路徑較長的除法運算；以及

將所得結果轉換到標準基礎網域來完成一個除法器。

2. 如申請專利範圍第 1 項所述之有限場除法器的架構方法，其中該運算單元包括查逆序表、平方器、雙變數乘法器、常數乘方器等運算器。

3. 如申請專利範圍第 2 項所述之有限場除法器的架構方法，其中該查逆序的動作是轉到子域下面來進行。

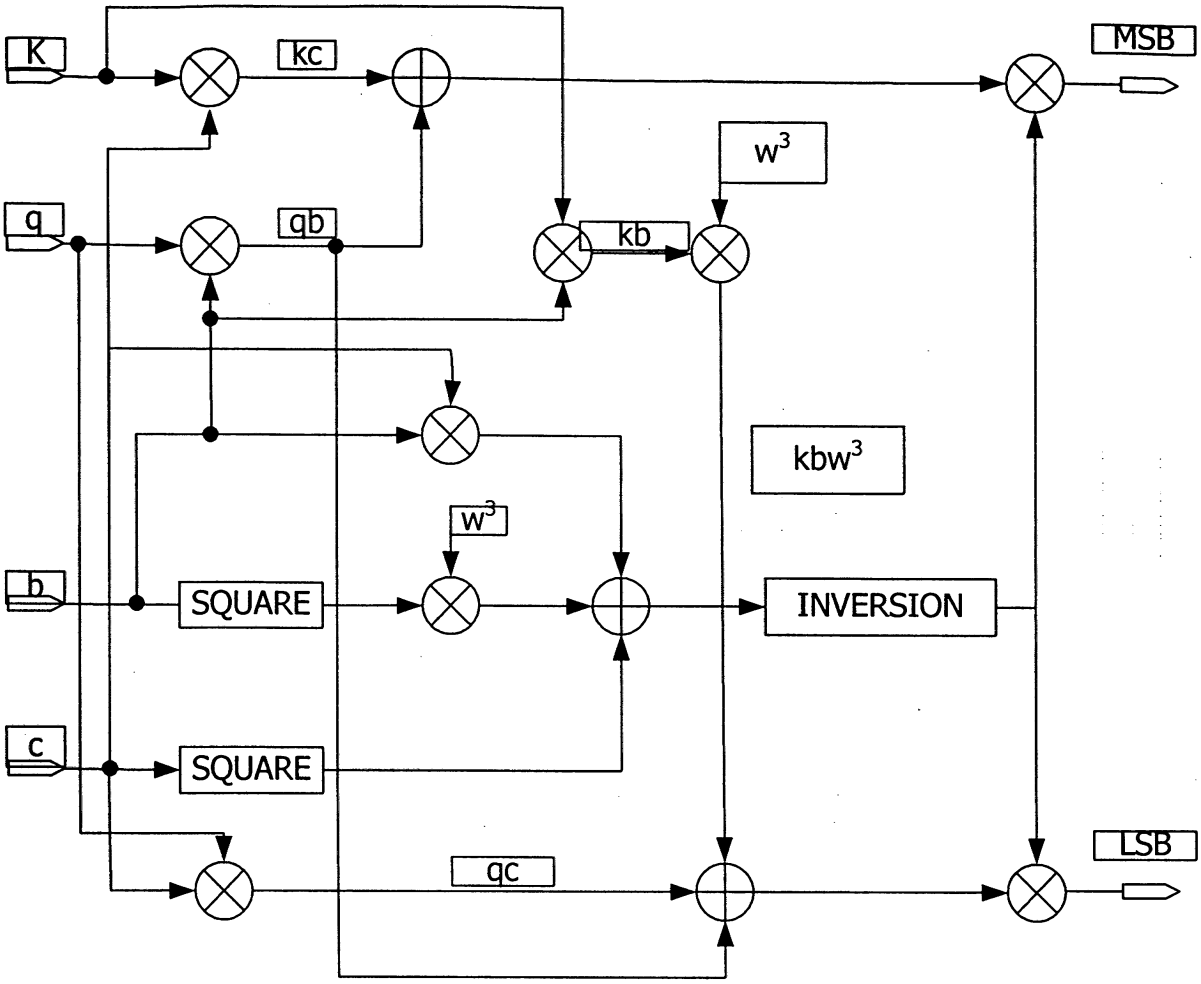
4. 如申請專利範圍第 1 項所述之有限場除法器的架構方法，其中該除法器過程在單一時脈下達成。

5. 如申請專利範圍第 1 項所述之有限場除法器的架構方法，其中該關鍵路徑與利用合成域所做出來的逆序關鍵路徑一樣。

6. 如申請專利範圍第 1 項所述之有限場除法器的架構方法，其中該合成域屬於一種擴張域。

7. 如申請專利範圍第 1 項所述之有限場除法器的架構方法，其中該合成域的基本域是佈於 2^n。

8. 如申請專利範圍第 1 項所述之有限場除法器的架構方法，其中該除法器可應用在解 RS/BCH 碼或是 ECC/Security 處理器。



第1圖