I325560

公告本

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：P5131467

※ 申請日期：25.8.25　　※IPC 分類：G06F7/53、7/38、7/38 (2006.01)

一、發明名稱：（中文/英文）

具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

龍華科技大學

代表人：（中文/英文）嚴文方

住居所或營業所地址：（中文/英文）

桃園縣龜山鄉萬壽路一段 300 號

國　籍：（中文/英文）中華民國

三、發明人：（共 2 人）

姓　名：（中文/英文）

1. 李秋瑩

2. 邱綺文

國　籍：（中文/英文）

中華民國（二位發明人國籍相同）

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：

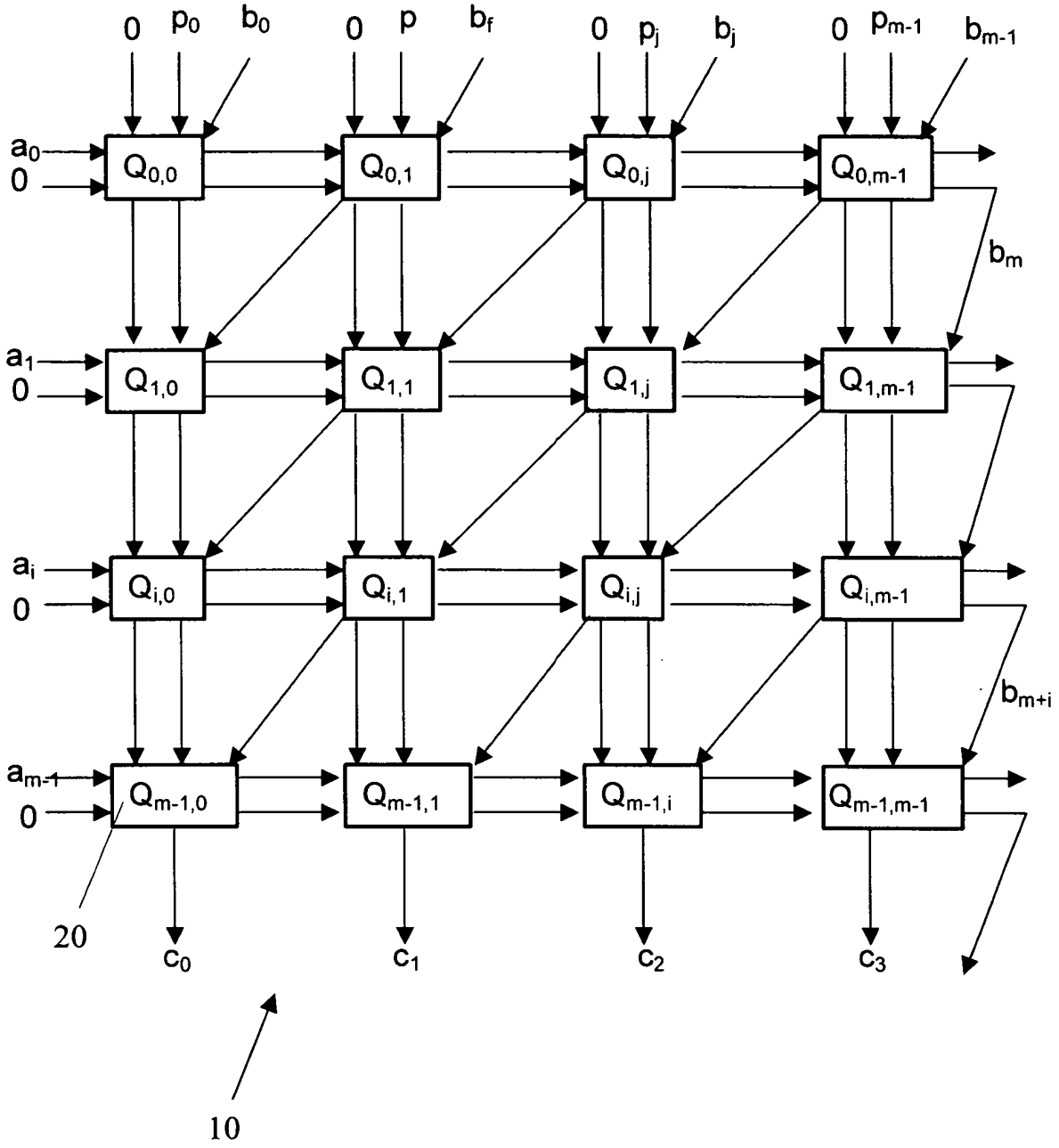
☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

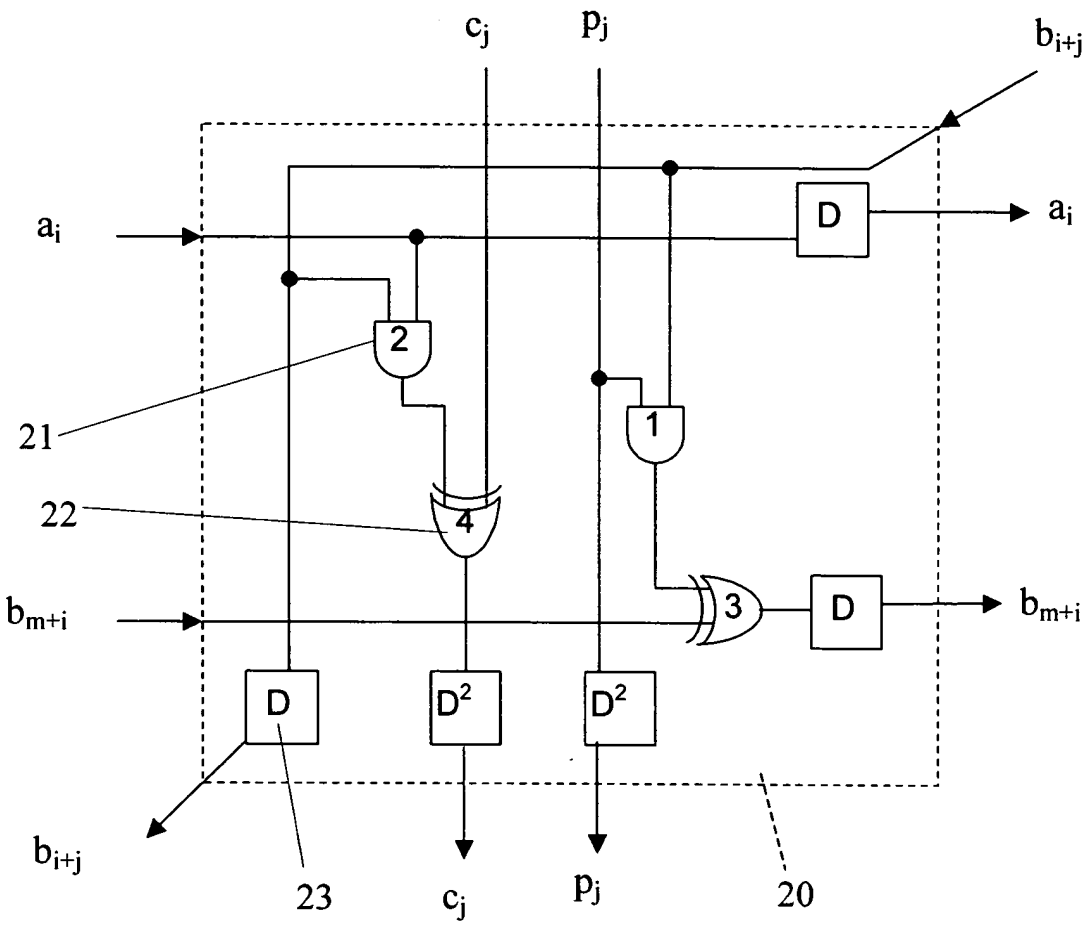
國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

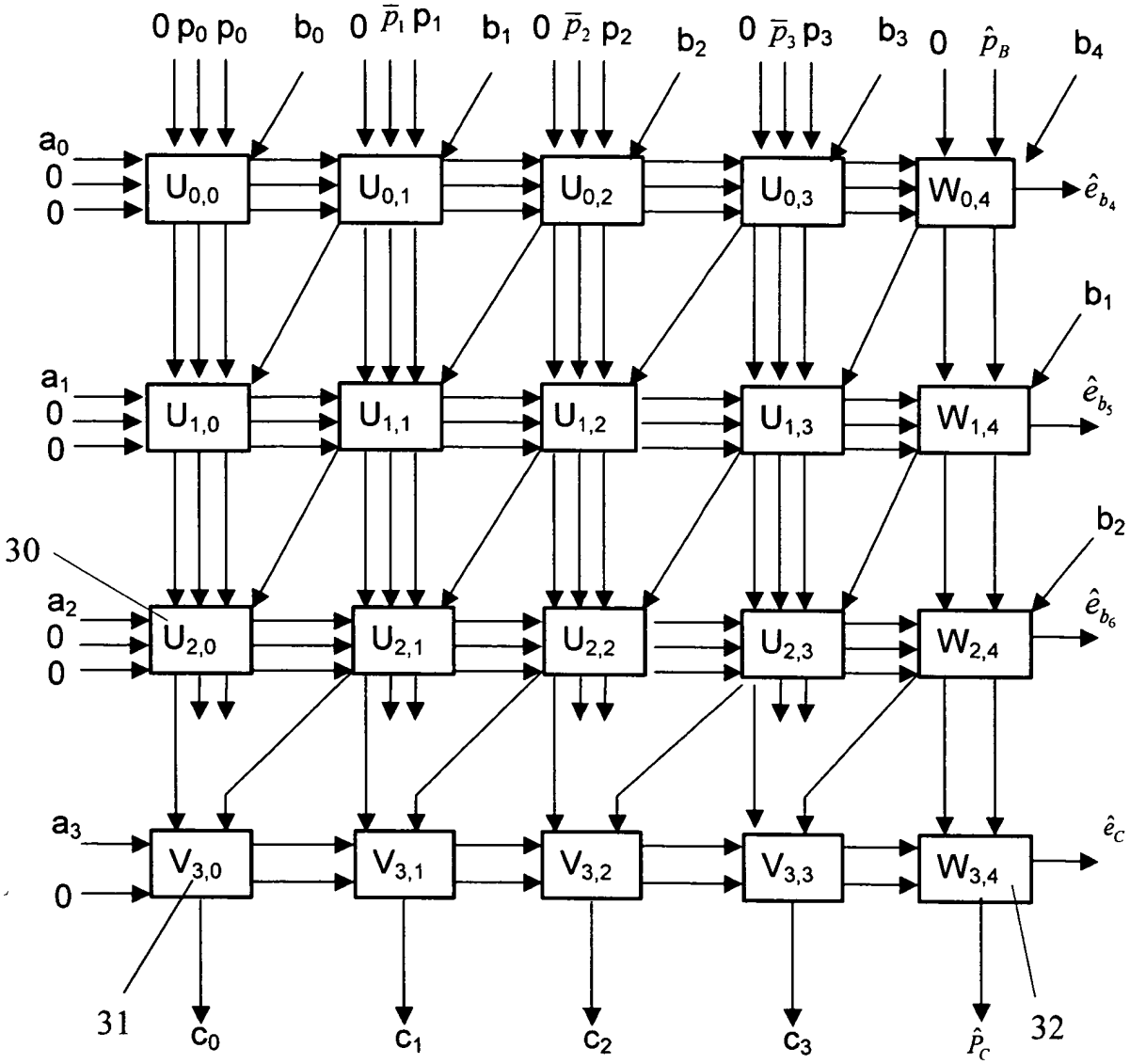
所屬技術領域中具有通常知識者易於獲得時，不須寄存。


0
p0
b0
0
p
bf
0
pj
bj
0
pm-1
bm-1
a0
0
Q0,0
Q0,1
Q0,j
Q0,m-1
bm
a1
0
Q1,0
Q1,1
Q1,j
Q1,m-1
ai
0
Qi,0
Qi,1
Qi,j
Qi,m-1
bm+i
am-1
0
Qm-1,0
Qm-1,1
Qm-1,i
Qm-1,m-1
20
c0
c1
c2
c3
10

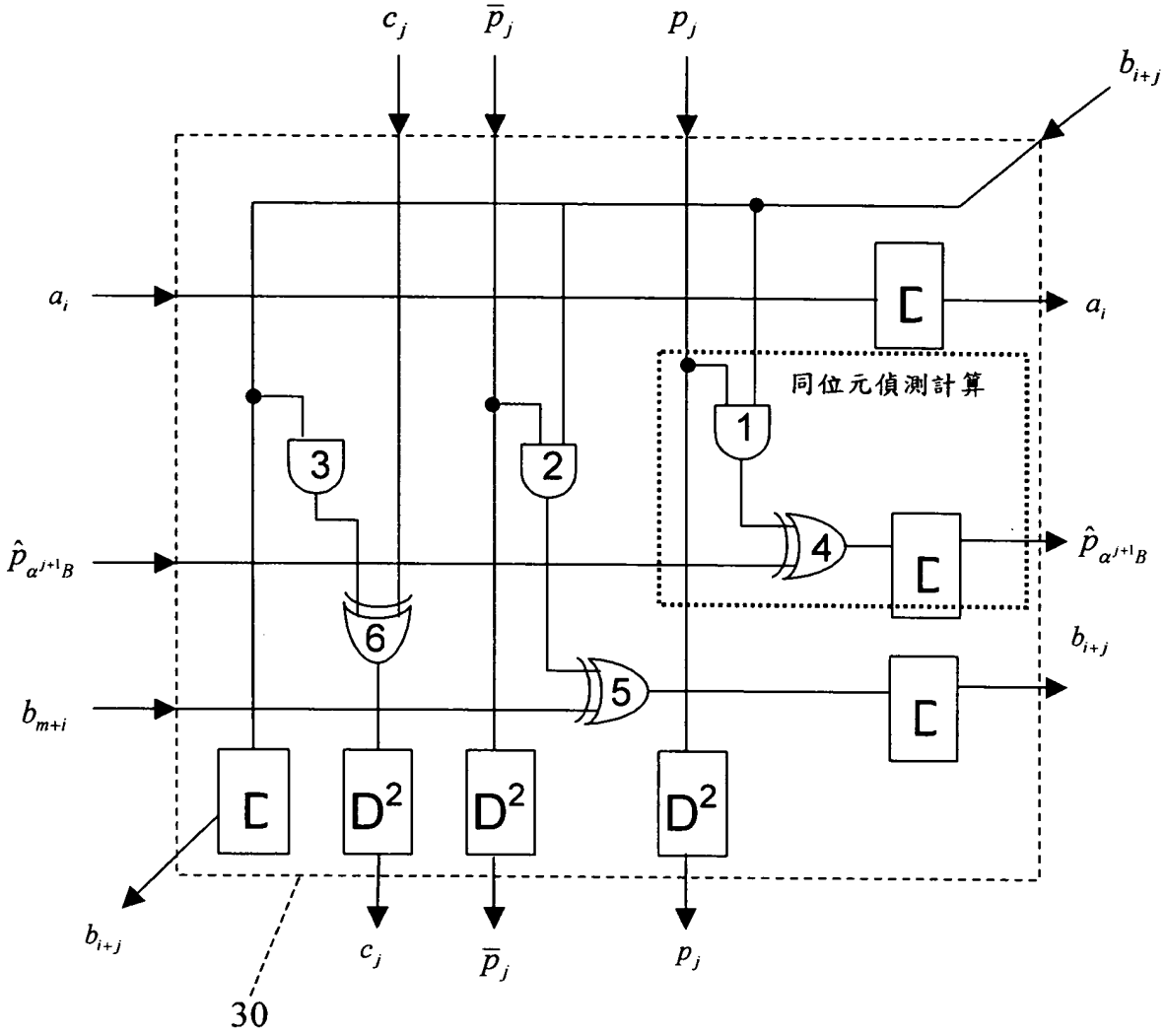
第一圖



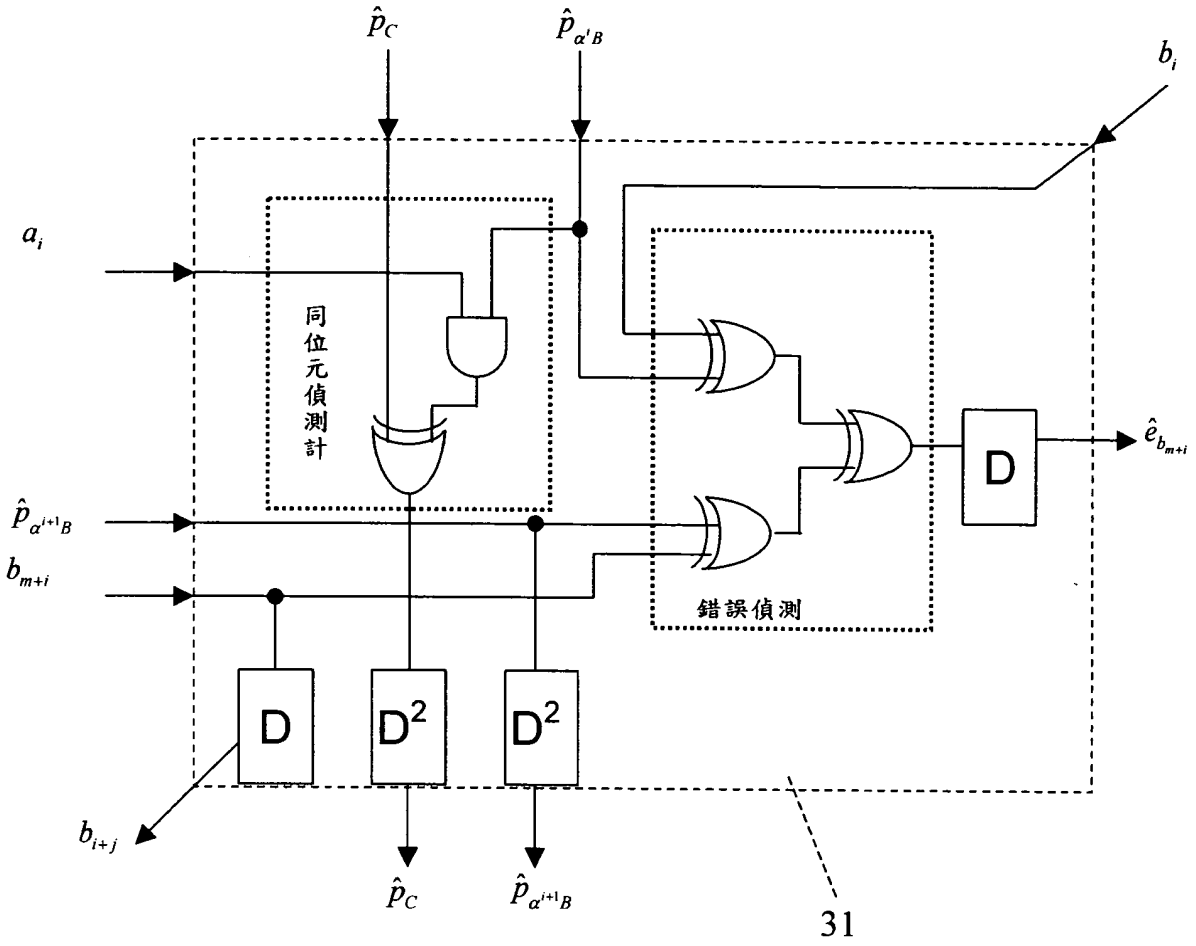
第二圖


0 p0 p0
b0
0 $\overline{p}_1$ p1
b1
0 $\overline{p}_2$ p2
b2
0 $\overline{p}_3$ p3
b3
0
$\hat{p}_B$
b4
a0
0
0
U0,0
U0,1
U0,2
U0,3
W0,4
$\hat{e}_{b_4}$
b1
a1
0
0
U1,0
U1,1
U1,2
U1,3
W1,4
$\hat{e}_{b_5}$
30
b2
a2
0
0
U2,0
U2,1
U2,2
U2,3
W2,4
$\hat{e}_{b_6}$
a3
0
V3,0
V3,1
V3,2
V3,3
W3,4
$\hat{e}_C$
31
c0
c1
c2
c3
$\hat{P}_C$
32

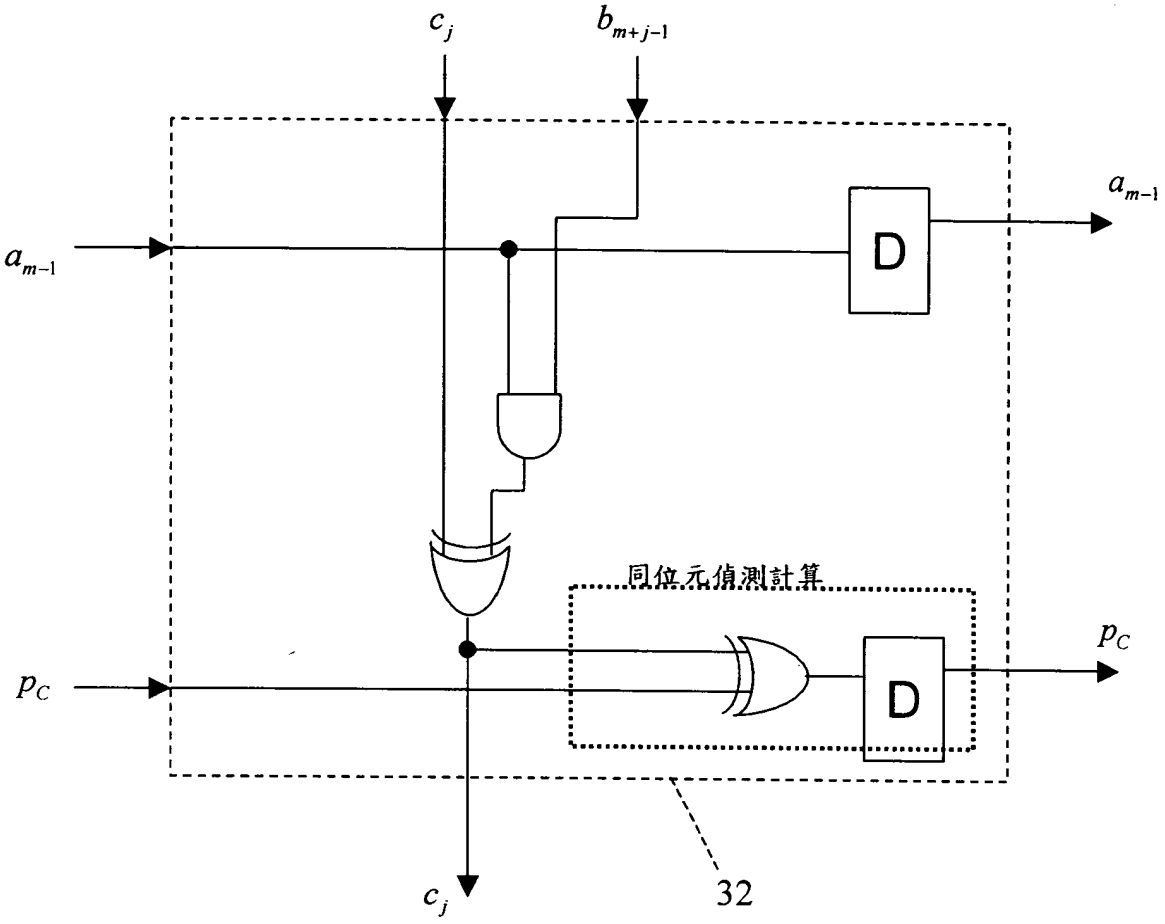
第三圖


c_j
$\overline{p}_j$
p_j
b_{i+j}
a_i
a_i
同位元偵測計算
1
2
3
4
5
6
$\hat{p}_{\alpha^{j+1}B}$
$\hat{p}_{\alpha^{j+1}B}$
b_{i+j}
b_{m+i}
D^2
D^2
D^2
b_{i+j}
c_j
$\overline{p}_j$
p_j
30

第四圖


$\hat{p}_C$
$\hat{p}_{\alpha^i B}$
b_i
a_i
同位元偵測計
$\hat{p}_{\alpha^{i+1}B}$
b_{m+i}
錯誤偵測
D
$\hat{e}_{b_{m+i}}$
D
D^2
D^2
b_{i+j}
$\hat{p}_C$
$\hat{p}_{\alpha^{i+1}B}$
31

第五圖



第六圖

九、發明說明：

【發明所屬之技術領域】

本發明係提供一種具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，尤指一種應用於有限場GF(2^m)，具即時性錯誤偵測能力之乘法器之創新技術。

【先前技術】

按，目前我國揭露於中華民國專利公報中的『乘法器』相關發明專利技術，較相關者概可列舉如下：

1、公告編號第382088號『有限場GF(2^m)的細胞陣列次方和電路』發明專利案。

2、公告編號第440789號『乘法器』發明專利案。

3、公告編號第255957號『t位元半平行處理式格羅瓦場乘法器之設計方法』發明專利案。

4、公告編號第360845號『陣列式乘法器架構及其方法』發明專利案。

5、公告編號第405086號『快速正規乘法器架構』發明專利案。

在有限場GF(2^m)中，有效的代數運算(含加法、乘法、除法、及指數等運算)已廣泛地被應用於錯誤更正碼和密碼技術，舉凡二進位BCH碼(Binary BCH Code)之解碼、RS碼(Reed-Solomon Code)之編碼與解碼及在安全通信(Secure Communication)上數位信息的加密(Encryption)與解密(Decryption)等。

儘管如此，有現場GF(2^m)的乘法及乘法反元素的運算

仍然相當複雜；針對有現場 GF(2^m)中的乘法運算陸續有學者提出快速演算法及快速電路，例如 Itoh-Tsujii、Sunar-Koc、Hasan 等，這些乘法器架構均基於特殊的多項式，它包括全一多項式（All-One Polynomial, AOP）、等距多項式（Equally-Spaced Polynomial, ESP）和三項多項式(Trinomial)。

另外，有學者 Guo 和 Wang 發展二段式乘法器，這是使用一般乘法單元和降次方的處理單元所構成的；儘管上面所述低複雜度乘法器是很適合於密碼技術，但其電路結構並非心臟收縮陣列式電路，因此，假若 m 很大，即會產生很長的傳播延遲。

有關低複雜度乘法器可以參考下列文獻：

[1] D. E. R. Denning, Cryptography and Data Security, Reading, MA: Addison-Wesley, 1983.

[2] M. Y. Rhee, Cryptography and Secure Communications, McGraw-Hill, Singapore, 1994.

[3] T. Itoh and S. Tsujii, "Structure of Parallel Multipliers for a Class of Finite Fields *GF(2^m)*," Information and Computation, Vol. 83, pp. 21-40, 1989.

[4] C. K. Koc and B. Sunar, "Low Complexity Bit-Parallel Canonical and Normal Basis Multipliers for a Class of Finite Fields," IEEE Trans. Computers, Vol. 47, No. 3, PP. 353~356, Mar. 1998.

[5] B. Sunar and C.K. Koc, "Mastrovito Multiplier for All Trinomials," IEEE Trans. Computers, Vol. 48, No. 5, PP. 522-527, May 1999.

[6] J. H. Guo and C.L. Wang, "Low-Complexity Power-Sum Circuit for *GF(2^m)* and Its Applications", IEEE Trans. Circuits and Systems-II, Vol. 47, No. 10, PP. 1091-1097, Oct. 2000.

[7] M. A. Hasan, M. Wang, V. K. Bhargava, "Modular construction of low complexity parallel multipliers for a class of finite fields GF(2^m)," IEEE Trans. Computers, Vol.41, No.8, pp.962-971, August 1992.

在超大型積體電路技術（VLSI）中，陣列式處理器具有簡單和規則的電路系統，包括三個類型電路架構：心臟收縮（Systolic）、細胞（Cellular）和管道（Pipeline）；陣列式處理器的優點是可定義成一個基本細胞（Basic cell）或者一些細胞。對於有限場 GF(2^m)的現存心臟收縮陣列乘法器大多數基於兩種演算法：最低位元處理優先(Least significant bit first)陣列及最高位元處理優先(Most significant bit first)陣列來計算有限場的兩個元素之乘積。這些乘法器適合在錯誤更正碼方面的應用，但是，這些心臟收縮陣列乘法器就密碼應用而言，則具有很複雜的電路和較長的計算延遲。例如 Wei 的乘法器的等待時間需要 3×m 脈波延遲；Guo-Wang 的乘法器之等待時間則需要

2.5×m 脈波延遲。

對於有限場 GF(2^m)，元素的表示式主要包含有多項式基底（Polynomial basis）（或稱為標準基底(Standard basis))、雙重基底（Dual basis）和正規基底（Normal basis)。在雙重基底中，根據線性回饋，串聯式 Berlekamp 乘法器能夠很有效地被實現。Wang 發展了另外一類型的雙重基底乘法器，其係使用自身雙重的正規基底（Self-dual normal basis)。前不久，Wu-Hasan-Blake 使用雙重基底來設計低複雜度位元並列輸出型乘法器。Fenn 則提出了雙重和標準基底之間的轉換關係，他也提出位元並列輸出和串列型的雙重基底乘法器。

相關的心臟收縮乘法器可以參考下列文獻：

[1] S. W. Wei, "A Systolic Power-Sum Circuit for GF(2^m)," IEEE Trans. Computers, Vol. 43, No. 2, PP. 226~229, Feb. 1994.

[2] C. S. Yeh, S. Reed, and T. K. Truong, "Systolic Multipliers for Finite Fields *GF(2^m)*," IEEE Trans. Computers, Vol. C-33, PP. 357-360, Apr. 1984.

[3] C. Y. Lee, E. H. Lu, and J. Y. Lee, "Bit-Parallel Systolic Multipliers for *GF(2^m)* Fields Defined by All-One and Equally-Spaced Polynomials," IEEE Trans. Computers, No. 5, PP. 385-393, May 2001.

[4] C.Y. Lee, E.H. Lu, and L.F. Sun, "Low-Complexity

Bit-Parallel Systolic Architectures for Computing AB^2+C in a Class of Finite Field $GF(2^m)$ ", IEEE Trans. CS-II, No. 5, PP. 519-523, May 2001.

[5] C.Y. Lee and C.W. Chiou, "Design of low-complexity bit-parallel systolic Hankel multipliers to implement multiplication in normal and dual bases of GF(2^m)," IEICE Tran. Fund., vol. E88-A, no.11, pp. 3169-3179, Nov. 2005.

[6] C.Y. Lee, J.S. Horng and I.C. Jou, "Low-complexity bit-parallel systolic Montgomery multipliers for special classes of GF(2^m)," IEEE Trans. Computers, vol. 54, no. 9, pp. 1061-1070, Sep. 2005.

在超大型積體電路技術（VLSI）設計中，分佈於有限域 GF(2^m)之心臟收縮陣列式結構基本上適合於快速計算，並且依靠規則性電路去執行算術運算，他們的共通性質提供結構特性，例如一致性、輸入/輸出平衡和簡單且有規則的設計。從超大型積體電路技術（VLSI）技術觀點，半導體製造商努力保證他們的產品是可靠的，然而在系統任何時間中幾乎不可能沒有錯誤；一個在估計可靠性基本的問題是在已知時間的週期、環境及規定的方法中任一個系統功能，因此，如何在運用於 GF(2^m)位元並列輸出型

心臟收縮陣列式的乘法器上加上即時錯誤偵測技術能力，將是非常重要的。

為達到輸出無錯誤，許多錯誤偵測結構如對稱的密碼系統和不對稱的密碼系統已經有許多的報告發表出來。Fenn等提議一種即時偵測方法，係使用奇偶同位元預測結構於位元串列輸出型 $GF(2^m)$乘法器。藉由使用相同的奇偶同位元偵測結構，Reyhani-Masoleh 和 Hasan 提供錯誤偵測方法在 $GF(2^m)$位元並列輸出型和位元串列輸出型多項式基底乘法器，其主要的問題在使用奇偶同位元偵測會花費長時間來產生同位元；因此，這種方法不被允許提供位元並列輸出型心臟收縮陣列式乘法器即時偵測能力，為了解決這個問題，Chiou 使用位移重計算(RESO)方法提供全一的多項式基底乘法器即時錯誤偵測能力。

令人遺憾，不可簡約的全一多項式非常稀有。假如 m 小於和等於 100，只有 13 個數值存在。

相關具有即時錯誤偵測能力之乘法器可以參考下列文獻：

[1] S. Fenn, M. Gossel, M. Benaissa, and D. Taylor, "On-line error detection for bit-serial multipliers in $GF(2^m)$," Journal of Electronic Testing: Theory and Applications, Vol.13, pp.29-40, 1998.

[2] A. Reyhani-Masoleh and M.A. Hasan, "Error detection in polynomial basis multipliers over binary extension fields," Proc. of Cryptographic Hardware and Embedded Systems-CHES 2002, LNCS 2523, pp.515-528, 2003.

[3] C.W. Chiou, "Concurrent error detection in array multipliers for GF(2^m) fields," IEE Electronics Letters, Vol.38, No.14, pp.688-689, July 2002.

緣是於此，本發明係在於提出了一種具有即時性錯誤偵測能力的 GF(2^m)乘法器。

【發明內容】

在超大型積體電路（VLSI）設計，分佈於有限場領域的 GF(2^m)心臟收縮陣列式結構基本上適合於快速計算，並且依靠規則性電路去執行算術運算，其共通性質是提供結構特性，例如一致性、輸入/輸出平衡和簡單和有規則的設計。從 VLSI 技術觀點，半導體製造商努力保證他們的產品是可靠的，但在系統中任何時間裡幾乎不可能沒有錯誤產生；所以在已知時間的週期、環境及規定的方法中任一個系統功能中，可靠性基本問題的估計是非常重要的，因此，如何對分佈於 GF(2^m)位元並列輸出型心臟收縮陣列式雙重基底乘法器提供即時錯誤偵測技術能力，將是本案的目的。

為達上述之目的，本發明提出一種具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，其電路特性係包含有：

一檢測裝置，用以控制資料編碼、解碼及密碼技術之錯誤檢測，該乘法器的電路特性係對有限場 GF(2^m)中之一第一元素 A 與一第二元素 B 進行乘積運算，以得到第三元素 C，其中元素 A 是以多項式基底 $(1,\alpha,\alpha^2,\Lambda,\alpha^{m-1})$之表示式，元素 B 及 C 是以雙重基底之表示式，該有限場 GF(2^m)為不可分解之多項式所產生的，及α為該不可分解的多項式之根；該第一元素 A 被表示為一 m 位元 $A=a_0+a_1\alpha+a_2\alpha^2+\Lambda+a_{m-1}\alpha^{m-1}$，該第二元素 B 被表示為一 m 位元 $B=b_0\beta_0+b_1\beta_1+b_2\beta_2+\Lambda+b_{m-1}\beta_{m-1}$，該第三元素 C 被表示為一 m 位元 $C=c_0\beta_0+c_1\beta_1+c_2\beta_2+\Lambda+c_{m-1}\beta_{m-1}$，其中所有元素的係數是等於 0 或 1，該乘法器包括有兩單元：

一雙重基底乘法單元，其電路包括由(m+1)×m 個細胞組成，以形成(m+1)×m 陣列，且每一細胞包含有三個以上輸入信號線、三個以上輸出信號線；每一細胞包含一個以上 AND 閘、一個以上 XOR 閘和三個以上單位元暫存器(Latch)；及

一雙重基底轉換單元，其電路包括樹狀式 2-input XOR 閘所構成。

其中，該乘法器的雙重基底乘法單元包含：

U 細胞，係在第 i 列執行下列函數：計算 b_{m+i}，$\alpha^i B$和 $\hat{P}_{\alpha^{i+1}B}=b_{i+1}p_0+\sum_{j=1}^{m-1}b_{i+j+1}\overline{p}_j$，其中 $0\le i\le m-2$；

W 細胞，其中在 b_{m+i}和 $\hat{P}_{\alpha^{i+1}B}$兩者在 U 細胞是最後計算時，係使用 4 個信號，b_i，b_{m+i}，$\hat{P}_{\alpha^{i+1}B}$和 $\hat{P}_{\alpha^iB}$，去完成 b_{m+i}計算的

錯誤檢測，其中 $\hat{P}_{\alpha^i B}$ 在 U-細胞的第(i-1)列被計算，特別是假若 i = 0，則 $\hat{P}_B = P_B$ 時；且 W 細胞使用 $\hat{P}_{\alpha^i B}$ 和 a_i，其中在 $0 \le i \le m-2$，則是為了計算已預測的奇偶同位檢測 $\hat{P}_C$；

V 細胞，在最後列，$V_{m-1,j}$ 細胞在 $0 \le j \le m-1$ 執行 $\alpha^{m-1}B$ 和 P_C 兩者計算；此 $V_{m-1,m}$ 細胞需負 $a_{m-1}\hat{P}_{\alpha^{m-1}B}$ 計算責任和整體乘法器錯誤檢測。

其中，該乘法器在上述 U、V 和 W 細胞之一發生不良時會發生單一陷入錯誤，並藉由該乘法器偵測出該錯誤。

其中，可檢測的錯誤包括：在 P_j 上的錯誤，細胞 $U_{i,j}$ 的輸出信號 P_j，使用來自輸入信號 P_j 的一通過線。

其中，可檢測的錯誤更包括：在 a_i 上的錯誤，細胞 $U_{i,j}$ 的輸出信號 a_i，亦是來自輸入信號 a_i 的通過線。

其中，可檢測的錯誤更包括：在 b_{i+j} 上的錯誤，細胞 $U_{i,j}$ 的輸出信號 b_{i+j}，也使用來自輸入信號 b_{i+j} 的一通過線。

其中，可檢測的錯誤更包括：在 $\overline{P}_j$ 上錯誤，細胞 $U_{i,j}$ 的輸出信號 $\overline{P}_j$，也使用來自輸入信號 $\overline{P}_j$ 的一通過線，因此其上錯誤容易檢測出。

其中，可檢測的錯誤更包括：在 c_j 上的錯誤，假如一個錯誤在不良的細胞 $U_{i,j}$ 的輸入信號 c_j 上出現，該錯誤將影響輸出信號 c_j 的最後結果，因此，計算在 V-細胞 C 的奇偶同位檢測位元，使用方程式 $P_C = \sum_{j=0}^{m-1} c_j$ 能被計算，在 W-細胞 C 的已預測奇偶同位檢測位元，使用方程式 $\hat{P}_C = \sum_{j=0}^{m-1} a_i \hat{P}_{\alpha^i B}$ 被執

行，最後在 $V_{m-1,m}$-細胞，比較實際的奇偶同位檢測 P_C 和已預測奇偶同位檢測 $\hat{P}_C$，這個錯誤則檢測出。

其中，可檢測的錯誤更包括：在 b_{m+i} 或 $\hat{P}_{\alpha^{i+1}B}$ 上的錯誤，假如一個錯誤在不良的細胞 $U_{i,j}$. 的輸入信號 b_{m+i} 上出現，這個錯誤將影響輸出信號 b_{m+i}；因此，使用方程式 $\hat{e}_{b_{m+i}} = \hat{P}_{\alpha^i B} + \hat{P}_{\alpha^{i+1}B} + b_{m+i} + b_i$，$\hat{e}_{b_{m+i}}$ 在此 $W_{i,m}$-細胞能變成邏輯 1，那就是說此錯誤能被檢測出，且在細胞 $U_{i,j}$ 上 $\hat{P}_{\alpha^{i+1}B}$ 錯誤也能使用方程式 $\hat{e}_{b_{m+i}} = \hat{P}_{\alpha^i B} + \hat{P}_{\alpha^{i+1}B} + b_{m+i} + b_i$ 檢測出。

其中，可檢測的錯誤更包括：在 $\hat{P}_C$ 或 P_C 上錯誤，假如一個錯誤在細胞 $W_{i,m}$. 的輸入信號 $\hat{P}_C$ 上出現，則在細胞 $V_{m-1,m}$，$\hat{e}_C$ 藉由應用方程式 $\hat{e}_C = \hat{P}_C + P_C$ 將變成邏輯 1，而能被檢測出此錯誤；且在 $V_{m-1,j}$-細胞，P_C 的輸出信號不良時，使用方程式 $\hat{e}_C = \hat{P}_C + P_C$，亦能發現在 $V_{m-1,m}$ 的錯誤。

有關本發明所採用之技術、手段及其功效，茲舉一較佳實施例並配合圖式詳細說明於后，相信本發明上述之目的、構造及特徵，當可由之得一深入而具體的瞭解。

【實施方式】

【有限場 $GF(2^m)$ 簡介】

假設有限場 $GF(2^m)$ 是由不可分解的多項式 $F(x) = x^m + f_{m-1}x^{m-1} + \Lambda + f_1 x + f_0$ 所產生的，其中所有係數 f_i 均為 0 或 1，$1 \le i \le m-1, f_0 = 1$。假設 α 是 $F(x)$ 的一個根，$GF(2^m)$ 的元素能夠被表示如下：

$$A = a_0 + a_1\alpha + \Lambda + a_{m-1}\alpha^{m-1}。$$

其中所有係數均為 0 或 1 且基底 $\{1, \alpha, \Lambda, \alpha^{m-1}\}$ 稱之為標準基底或多項式基底(Standard basis，Polynomial basis)。此外，標準基底對應之雙重基底(Dual basis)的形式 $\{\beta_0, \beta_1, \Lambda, \beta_{m-1}\}$

有下列特性：

$$Tr(\gamma\alpha^i\beta_j)=\begin{cases}1 & if \quad i=j\\ 0 & if \quad i\neq j\end{cases} \qquad (1)$$

其中 $Tr(\bullet)$ 是軌跡函數（Trace function），且 $\gamma\in GF(2^m)$，$\gamma\neq 0$。對於 $A\in GF(2^m)$，$A=\sum_{i=0}^{m-1}a_i\alpha^i=\sum_{i=0}^{m-1}a_i^*\beta_i$，其中 a_i 和 a_i^* 分別為元素 A 的多項式基底與雙重基底之對應函數。從 $a_i^*\in GF(2)$，我們得到

$$Tr(\gamma\alpha^i\beta_j)=Tr\left(\gamma\alpha^i\sum_{j=0}^{m-1}a_j^*\beta_j\right)=\sum_{j=0}^{m-1}a_j^*Tr\left(\gamma\alpha^i\beta_j\right)=a_j^* \qquad (2)$$

從 $F(\alpha)=0$，我們可獲得下列關係式

$$\alpha^m=\sum_{i=0}^{m-1}f_i\alpha^i=\sum_{i=0}^{m-1}f_i^{(0)}\alpha^i$$

$$\alpha^{m+1}=\sum_{i=0}^{m-1}f_i^{(0)}\alpha^{i+1}=f_{m-1}^{(0)}f_0^{(0)}+\sum_{i=1}^{m-1}\left(f_{i-1}^{(0)}+f_{m-1}^{(0)}f_i^{(0)}\right)\alpha^i=\sum_{i=0}^{m-1}f_i^{(1)}\alpha^i \qquad (3)$$

$$\alpha^{2m-2}=\sum_{i=0}^{m-1}f_i^{(m-2)}\alpha^i$$

其中所有係數都等於 1 或 0。假設元素 $B=b_0\beta_0+b_1\beta_1+\Lambda+b_{m-1}\beta_{m-1}$ 是以雙重基底表示式，應用軌跡函數於方程式(3)之兩邊可得

$$Tr(\gamma\alpha^iB)=b_i,\quad i=0,1,\Lambda\ ,m-1 \qquad (4a)$$

及

$$Tr(\gamma\alpha^i B)=\sum f_j^{(i-m)}b_j,\quad i=m,m+1,\Lambda\ ,2m-2 \qquad (4b)$$

假設 $\tilde{b}=Tr(\gamma\alpha^i B)$，$i=0,1,\Lambda\ ,2m-2$。假如元素 C 是兩元素 A 及 B 之積，則有下列關係式

$$\begin{bmatrix}\tilde{b}_0 & \tilde{b}_1 & \Lambda & \tilde{b}_{m-1}\\ \tilde{b}_1 & \tilde{b}_2 & \Lambda & \tilde{b}_m\\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \mathrm{M}\\ \tilde{b}_{m-1} & \tilde{b}_m & \Lambda & \tilde{b}_{2m-2}\end{bmatrix}\begin{bmatrix}a_0\\ a_1\\ \mathrm{M}\\ a_{m-1}\end{bmatrix}=\begin{bmatrix}c_0\\ c_1\\ \mathrm{M}\\ c_{m-1}\end{bmatrix} \qquad (5)$$

其中 $\tilde{b}=Tr(\gamma\alpha^i B)$（$i=0,1,\Lambda\ ,2m-2$），$c_i=Tr(\gamma\alpha^i C)$（$i=0,1,\Lambda\ ,m-1$），且 $A=\sum_{i=0}^{m-1}a_i\alpha^i$。

從上述方程式，m×m 矩陣被叫為 Hankel 矩陣-向量。為了探究分佈於 GF(2^m)位元並列輸出型雙重基底乘法器，乘積 C 使用方程式（3）-（4）能被寫成

$$C=a_0B+a_1\alpha B+\Lambda+a_{m-1}\alpha^{m-1}B=\sum_{i=0}^{m-1}a_iC_i \qquad (6)$$

其中

$$C_i=\alpha^i B=c_{i,0}\beta_0+c_{i,1}\beta+\Lambda+c_{i,m-1}\beta_{m-1},\quad c_{i,j}=f(\gamma\alpha^{i+j}B)=b_{i+j}$$

如上所述，下列演算法可實現雙重基底乘法。

雙重基底乘法的演算法：

Input: $A=[a_0,a_1,\ldots,a_{m-1}]$, $B=[b_0,b_1,\ldots,b_{m-1}]$ and $P=[p_0,p_1,\ldots,p_{m-1},1]$

Output: $C=[c_0,\ c_1,\ \ldots,\ c_{m-1}]=AB$

```
For i=0 to m-1
{
    c_i=0
}
For i=0 to m-1
{
    b_{m+i}=0
    For j=0 to m-1
    {
        c_j=c_j+a_i b_{i+j}
        b_{m+i}=b_{i+j} p_j+b_{m+i}
    }
}
```

根據上述演算法，參閱第一圖所示，顯示位元並列輸出型心臟收縮陣列式雙重基底乘法器（１０），其包含 m^2 相同的功能單元細胞（２０）。而每個功能單元細胞（２０）則如第二圖中所示，係包括二個 2 輸入 AND 閘（２１），二個 2 輸入 XOR 閘（２２）及七個 1 位元栓閘（２３）所組成；該電路需要 3×m 時脈週期的傳輸延遲，且每個細胞是需要由一個 2 輸入 AND 閘（２１）、一個 2 輸入 XOR 閘（２２）及一位元栓閘(Latch)（２３）的最大計算延遲。此外，該雙重基底乘法器由 Fenn 等提議，其適於實現超大型積體電路（VLSI）技術。然而，此乘法器卻不能偵測任何錯誤。因此，為了解決這個問題，我們可以使用奇偶同位元偵測結構，使得乘法器具有即時錯誤偵測能力。

【單一功能單元細胞錯誤(Single-cell Fault)模型】

在陣列電路中，使用的錯誤模型為單一功能單元細胞錯誤**(Single-cell Fault)**模型，亦即同時間允許單一個功能單元細胞失效。單一個功能單元細胞失效的更細部行為又可以從功能單元細胞的輸出埠的 stuck-at fault 上觀察。在邏輯電路中，造成邏輯電路的功能失效，如信號線路的

斷路或短路、

1. stuck-at-1(s-a-1)錯誤型態:如邏輯電路的輸出信號值均固定為邏輯 1 值。

2. stuck-at-1(s-a-0)錯誤型態: 如邏輯電路的輸出信號值均固定為邏輯 0 值。

根據上述陷入錯誤模型，以 2-input XOR 閘為例，C=A⊕B，若輸入信號 A 發生 s-a-1 錯誤時，XOR 閘的輸出值為 $C=\overline{B}$；若輸入信號 A 發生 s-a-1 錯誤時，XOR 閘的輸出值為 C=B。

本發明係使 GF(2^m)位元並列輸出型心臟收縮陣列式雙重基底乘法器具有即時錯誤偵測能力。

假設單一功能單元細胞錯誤(Single-cell Fault)模式。從先前的有限場說明在方程式（6）裡，此雙重基底乘法包含兩種運算：狀況 1 由 $0\le i\le m-2$ 計算 b_{m+i} 的錯誤偵測和狀況 2 在原有的乘法上的錯誤偵測。因此，以下將分別討論分析兩種狀況之錯誤偵測結構，並利用本發明新的即時錯誤偵測技術結構來解決。其討論如下：

狀況 1：

在 $0\le i\le m-2$ 中計算 b_{m+i} 的錯誤偵測 讓我們考慮 b_{m+i} 計算。從方程式 (6), b_{m+i}可由下式計算得到

$b_{m+i}=b_i p_0+b_{1+i}p_1+\Lambda+b_{m-1+i}p_{m-1}$ 在以下假設中單一功能單元細胞錯誤(Single-cell Fault)模式可再分解成細胞輸出訊號發生單一陷入錯誤(single stuck-at fault)，對於此錯誤模型而言，一個錯誤在邏輯閘(如 XOR 及 AND 等)導致在其輸入或輸出其中之一 s-a-0 錯誤或者 s-a-1 錯誤。 從上述方程式中

計算 b_{m+i}，在第一圖的細胞 $Q_{i,j}$ 使用一個 2 輸入 AND 閘（21）及一個 2 輸入 XOR 閘（22）去完成 b_{m+i} 計算，如第二圖中所顯示。在細胞 $Q_{i,j}$ 錯誤行為能被分類如下的 5 種情況。

(a): 假如輸入信號 p_i 在 AND-1 閘有一陷入錯誤，則在第 i 列細胞，計算 b_{m+i} 如

$$b_{m+i}=\begin{cases}\sum_{k=0}^{j-1}b_{k+i}p_k+\sum_{k=j+1}^{m-1}b_{k+i}p_k & for\ \ s-a-0\\ \sum_{k=0}^{j-1}b_{k+i}p_k+b_{i+j}+\sum_{k=j+1}^{m-1}b_{k+i}p_k & for\ \ s-a-1\end{cases}$$

(b): 假如輸入信號 b_{i+j} 在 AND-1 閘有一陷入錯誤，則在第 i 列細胞，計算 b_{m+i} 如

$$b_{m+i}=\begin{cases}\sum_{k=0}^{j-1}b_{k+i}p_k+\sum_{k=j+1}^{m-1}b_{k+i}p_k & for\ \ s-a-0\\ \sum_{k=0}^{j-1}b_{k+i}p_k+p_i+\sum_{k=j+1}^{m-1}b_{k+i}p_k & for\ \ s-a-1\end{cases}$$

(c): 假如輸入信號 b_{m+i} 在 XOR-3 閘有一陷入錯誤，則在第 i 列細胞，計算 b_{m+i} 如

$$b_{m+i}=\begin{cases}\sum_{k=j+1}^{m-1}b_{k+i}p_i & for\ \ s-a-0\\ \overline{b}_{j+1}\overline{p}_j+\sum_{k=j+1}^{m-1}b_{k+i}p_k & for\ \ s-a-1\end{cases}$$

(d): 假如 AND-1 閘的輸出信號有一陷入錯誤，則在第 i 列細胞，計算 b_{m+i} 如

$$b_{m+i}=\begin{cases}\sum_{k=0}^{j-1}b_{k+i}p_k+\sum_{k=j+1}^{m-1}b_{k+i}p_k & for\ \ s-a-0\\ \sum_{k=0}^{j-1}b_{k+i}p_k+1+\sum_{k=j+1}^{m-1}b_{k+i}p_k & for\ \ s-a-1\end{cases}$$

(e): 假如 XOR-3 閘的輸出信號有一陷入錯誤，則在第 i 列細胞，計算 b_{m+i} 如

$$b_{m+i}=\begin{cases}\sum_{k=j+1}^{m-1}b_{k+i}p_i & for\ \ s-a-0\\ 1+\sum_{k=j+1}^{m-1}b_{k+i}p_k & for\ \ s-a-1\end{cases}$$

令 P_B 是 B 元素的奇偶同位校驗位元且被定義成

$$P_B=b_0+b_1+\Lambda+b_{m-1}$$

其中"+"符號指表示模數 2 加法（modulo-2 addition）(即互斥或計算)。

從方程式(6)能獲得那 $\alpha B=b_1\beta_0+b_2\beta_1+\Lambda+b_m\beta_{m-1}$。因此，$\alpha B$ 預測奇偶同位檢測位元被計算如下：

$$\hat{P}_{\alpha B}=b_1+b_2+\Lambda+b_m \qquad (7)$$

從方程式 (4), b_m 可計算如下

$$b_m=f(\gamma\alpha^m B)=f(\gamma\sum_{i=0}^{m-1}p_i\alpha^i B)$$

$$=\sum_{i=0}^{m-1}p_i f(\gamma\alpha^i B)=\sum_{i=0}^{m-1}p_i b_i \qquad (8)$$

將方程式 (8)代入方程式 (7), 此 αB 預測的奇偶同位檢測位元可被執行如下

$$\hat{P}_{\alpha B}=b_0p_0+\sum_{i=1}^{m-1}b_i(1+p_i)=b_0p_0+\sum_{i=1}^{m-1}b_i\bar{p}_i$$

因此，假設奇偶同位檢測位元 P_B 被預先計算好，因為

$\hat{P}_{\alpha B}=\sum_{i=0}^{m-1}b_{1+i}$ ， 且 $\hat{P}_B=P_B$

則我們有

$$\hat{P}_{\alpha B}+\hat{P}_B=b_m+b_0$$

因此，讓我們定義參數 $\hat{e}_{b_m}$ 如下列函數； 這樣的參數能被用於 b_m 計算的檢測。

$$\hat{e}_{b_m}=\hat{P}_{\alpha B}+\hat{P}_B+b_m+b_0 \qquad (9)$$

此參數 $\hat{e}_{b_m}=1$ 指示錯誤 b_m 計算的存在。類似地，b_{m+i} 的錯誤偵測能被執行且使用下列函數

$$\hat{e}_{b_{m+i}}=\hat{P}_{\alpha^i B}+\hat{P}_{\alpha^{i+1}B}+b_{m+i}+b_i \tag{10}$$

其中

$$\hat{P}_{\alpha^i B}=b_{i-1}p_0+\sum_{j=1}^{m-1}b_{i+j-1}\overline{p}_j \tag{11}$$

狀況 2：

在整個乘法計算上的錯誤偵測 根據 $G=\sum_{i=0}^{m-1}g_i\beta_i$，已知 $G=aB$，其中 $g_i=ab_i$，它可以直接地被獲得，當 $a=0$，G 的輸出是邏輯 0 和當 $a=1$輸出是邏輯 B。令 $B=\sum_{i=0}^{m-1}b_i\beta_i$ 且 $P_B=\sum_{i=0}^{m-1}b_i$ 被分別地表示成雙重基底和 B 的奇偶同位檢測位元。則輸出 G 的奇偶同位檢測，根據 $P_G=\sum_{i=0}^{m-1}g_i$ 對應 a 和 B 的輸入信號是已知，其中 $g_i=ab_i$，$0\le i\le m-1$，是 G 的係數。因此 輸出 G 的此預測的奇偶同位檢測位元能被表示如下：

$$\hat{P}_G=a\hat{P}_B \tag{12}$$

首先，從方程式（6）計算 $\alpha^j B$，由 $\alpha^j B=b_j\beta_0+b_{j+1}\beta_1+\Lambda+b_{i+m-1}\beta_{m-1}$ 被執行。如同 $P_{\alpha^i B}=b_{i-1}p_0+\sum_{j=1}^{m-1}b_{i+j-1}\overline{p}_j$ 它是容易計算 $\alpha^j B$ 的奇偶同位

檢測位元。因此，此乘積 $C=a_0B+a_1\alpha B+\Lambda+a_{m-1}\alpha^{m-1}B$ 的預測奇偶同位檢測位元能被計算如下：

$$\hat{P}_C=\sum_{i=0}^{m-1}a_j\hat{P}_{\alpha^j B} \qquad (13)$$

原先的乘積 C 的奇偶同位檢測位元是由方程式（6）直接獲得，即，

$$P_C=\sum_{i=0}^{m-1}c_i, \text{其中} \quad c_i=\sum_{i=0}^{m-1}a_j b_{i+j}$$

最後，乘積 C 的錯誤檢測能被比較與實際奇偶同位檢測 P_C 和預測奇偶同位檢測 $\hat{P}_C$，那就是，

$$\hat{e}_C=\hat{P}_C+P_C \qquad (14)$$

此參數 $\hat{e}_C=1$ 表明存在單一陷入錯誤。

如上所述，兩方程式(10)和(14)被用來偵測乘法器輸出。假若 b_{m+i} 計算是無錯誤，則 $\hat{e}_{b_{m+i}}=0$，且 $\hat{e}_{b_{m+i}}=1$ 旗標存在單一陷入錯誤。特別地，當此單一陷入錯誤發生在 b_{m+i} 計算，這錯誤是不引入進 b_{m+i} 計算的輸出，其中 $i\neq j$。基於方程式 (10)，我們能偵測所有單一陷入錯誤發生於 b_{m+i} 計算。當陷入錯誤發生於 c_i 計算，此錯誤是不引入 c_i 計算的輸出，其中 $i\neq j$。因此，為偵測在整個乘法器全部陷入錯誤，陷入錯誤的旗標 $\hat{e}_C=1$ 出現。因方程式 (10)和(14)是分佈於 GF(2)，其 $\hat{e}_{b_{m+1}}$ 和 $\hat{e}_C$ 的值將偵測不僅單一陷入錯誤，並且偵測任何奇數的陷入錯誤。由於相似的討論，很清楚的偶數的陷入錯誤發生在細胞第 i 列將不被 $\hat{e}_{b_{m+i}}$ 檢測出。與此類似，$\hat{e}_C$ 值不能檢測任何偶數的陷入錯誤發生在細胞第 i 行。

因此，為達上述之目的，本發明提出一種有限場 GF(2^m) 之低複雜度的心臟收縮陣列式雙重基底乘法器，其電路特性係包含有：

一檢測裝置，用以控制資料編碼、解碼及密碼技術之錯誤檢測，該乘法器係對有限場 GF(2^m)中兩種類型的奇偶位元檢測預測功能由(m+1)×m 個細胞組成，其包括 m×(m-1)個 U 細胞，(m+1)個 V 細胞和(m-1)個 W 細胞。

U 細胞在第 i 列執行下列函數：計算 b_{m+i}，$\alpha^i B$和 $\hat{P}_{\alpha^{i+1}B} = b_{i+1}p_0 + \sum_{j=1}^{m-1} b_{i+j+1}\overline{p}_j$，其中 $0 \le i \le m-2$。當 b_{m+i}和 $\hat{P}_{\alpha^{i+1}B}$兩者在 U 細胞是最後計算，W 細胞使用 4 個信號，b_i、b_{m+i}、$\hat{P}_{\alpha^{i+1}B}$和 $\hat{P}_{\alpha^i B}$，去完成 b_{m+i}計算的錯誤偵測。其中 $\hat{P}_{\alpha^i B}$在 U-細胞的第(i-1)列被計算。特別是，假若 i = 0，則 $\hat{P}_B = P_B$。除此之外，W 細胞使用 $\hat{P}_{\alpha^i B}$和 a_i，在 $0 \le i \le m-2$，為了計算已預測的奇偶同位檢測 $\hat{P}_C$計算。在最後列，$V_{m-1,j}$細胞在 $0 \le j \le m-1$執行 $\alpha^{m-1}B$和 P_C兩者計算。最後，此 $V_{m-1,m}$細胞需要 $a_{m-1}\hat{P}_{\alpha^{m-1}B}$計算和整體乘法器錯誤檢測。根據上述結構，此電路需要 3m+1 時鐘週期的延遲。每一細胞需要一個 2 輸入 AND 閘，一個 2 輸入 XOR 閘和一位元栓閘的最大計算延遲。

在本發明的乘法器中，單一陷入錯誤模式被假設。令陣列的第 i 列和第 j 行在圖三被指示為 $X_{i,j}$-細胞，其中"X"表示 U，V 和 W 等 3 種細胞類型之一。假設 $X_{i,j}$細胞是不完美的。不良的行為能被分類為以下的 7 種情況可被檢測。

(1)在 p_j 線路上的錯誤

細胞 $U_{i,j}$ 的輸出信號 p_j，使用來自輸入信號 p_j 的一通過線，因此在圖三中陣列比較原始輸入信號 p_j 和原始輸出信號 p_j 容易檢測出在它上一個錯誤。因此，在信號 p_j 線路上的錯誤能被忽視。

(2)在 a_i 線路上的錯誤

細胞 $U_{i,j}$ 的輸出信號 a_i，亦是來自輸入信號 a_i 的通過線，因此其上錯誤容易檢測出。因此，在信號 a_i 線路上的錯誤能被忽視。

(3)在 b_{i+j} 上的錯誤

細胞 $U_{i,j}$ 的輸出信號 b_{i+j}，也使用來自輸入信號 b_{i+j} 的一通過線，因此其上錯誤容易檢測出。因此，在信號 b_{i+j} 上的錯誤能被忽視。

(4) 在 $\overline{P}_j$ 上錯誤

細胞 $U_{i,j}$ 的輸出信號 $\overline{P}_j$，也使用來自輸入信號 $\overline{P}_j$ 的一通過線，因此其上錯誤容易檢測出。因此，在信號 $\overline{P}_j$ 上的錯誤能被忽視。

(5)在 c_j 上的錯誤

假如一個錯誤在不良的細胞 $U_{i,j}$ 的輸入信號 c_j 上出現。這個錯誤將影響輸出信號 c_j。那就是，此錯誤影響在輸出信號 c_j 最後結果。因此，計算在 V-細胞 C 的奇偶同位檢測位元，使用方程式 $P_C = \sum_{j=0}^{m-1} c_j$ 能被計算。

在 W-細胞 C 的已預測奇偶同位檢測位元，使用方程式

$\hat{P}_C = \sum_{j=0}^{m-1} a_i \hat{P}_{\alpha^i B}$被執行。最後在 $V_{m-1,m}$-細胞，比較實際的奇偶同位檢測 P_C和已預測奇偶同位檢測 $\hat{P}_C$，這個錯誤則檢測出。

(6)在 b_{m+i}或 $\hat{P}_{\alpha^{i+1}B}$上的錯誤

假如一個錯誤在不良的細胞 $U_{i,j}$.的輸入信號 b_{m+i}上出現。這個錯誤將影響輸出信號 b_{m+i}。因此，使用方程式（10），$\hat{e}_{b_{m+i}}$在此 $W_{i,m}$-細胞能變成邏輯 1，那就是說此錯誤能被檢測出。與此類似地，在細胞 $U_{i,j}$ 上 $\hat{P}_{\alpha^{i+1}B}$錯誤也能使用方程式（10）被檢測出。

(7)在 $\hat{P}_C$或 P_C上錯誤

假如一個錯誤在細胞 $W_{i,m}$.的輸入信號 $\hat{P}_C$上出現，則在細胞 $V_{m-1,m}$ ．$\hat{e}_C$藉由應用方程式（14）將變成邏輯 1。那就是說，此錯誤能被檢測出。與此類似地，在 $V_{m-1,j}$-細胞，P_C的輸出信號是不良的。使用方程式(14),在 $V_{m-1,m}$錯誤能被發現。

如上所述，被提議的即時錯誤檢測結構使用兩個奇偶同位檢測預測，$\hat{P}_C$和 $\hat{P}_{\alpha^i B}$，在整個乘法器裡執行檢測錯誤。此被提議的乘法器優點被描述如下：

(1)全部單一原有的錯誤（single stuck-at fault）藉由使用方程式（10）及（14）能被檢測。

(2)被提議有即時錯誤檢測的乘法器與在無即時錯誤檢測雙重基底乘法器比較，僅需要一個額外的時鐘週期。

為讓本發明之上述目的、特徵、和優點能夠明顯易懂，

下文特舉一較佳實施例，並配合所附圖式，作詳細說明如下，以期能使熟悉本發明相關技術之人士，得依本說明書之陳述據以實施。

習用的在不具即時錯誤檢測位元並列輸出心臟收縮陣列式雙重基底乘法器表示如第一圖，而本發明具即時錯誤檢測位元並列輸出心臟收縮陣列式雙重基底乘法器被顯示在第三圖,其乘法器由(m+1)×m 個細胞組成，其包括 m×(m-1)個 U 細胞（３０），(m+1)個 V 細胞（３１）和(m-1)個 W 細胞（３２）。U，V 和 W 細胞（３０）、（３１）、（３２）的詳細的電路被分別描述在第四圖、第五圖及第六圖。

綜上所述，雖然本發明已以較佳實施例揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神與範圍，當可作各種之更動與潤飾，因此本發明之保護範圍以申請專利範圍所界定者為準。

【圖式簡單說明】

第一圖係位元並列心臟收縮陣列式雙重基底乘法器之架構圖。

第二圖係位元並列心臟收縮陣列式雙重基底乘法器之細胞圖。

第三圖係本發明具即時錯誤檢測位元並列心臟收縮陣列式雙重基底乘法器。

第四圖係本發明詳細的 $U_{i,j}$ 細胞電路示意圖。

第五圖係本發明詳細的 $W_{i,m}$ 細胞電路示意圖。

第六圖係本發明詳細的 $V_{m,j}$ 細胞電路示意圖。

【主要元件符號說明】

（１０）雙重基底乘法器

（２０）單元細胞

（２１）2 輸入 AND 閘

（２２）2 輸入 XOR 閘

（２３）1 位元栓閘

（３０）U 細胞

（３１）V 細胞

（３２）W 細胞

五、中文發明摘要：

本發明係關於一種具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，該乘法器包含乘法及轉換單元，該乘法單元係由(m+1)×m 的電路架構係由(m+1)×m 個細胞組成，以形成(m+1) ×m 陣列，且每一細胞包含有三個以上輸入信號線、三個以上輸出信號線、一個以上 AND 閘、一個以上 XOR 閘和三個以上單位元暫存器(Latch)；及轉換單元，其電路架構係包括樹狀式 2-input XOR 閘所構成；即時錯誤偵測（On-line Error Detection）演算法得以實現，偵測錯誤範圍包含全部單一功能單元細胞錯誤(Single-cell fault)。

六、英文發明摘要：

十、申請專利範圍：

1．一種具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，其電路特性係包含有：

一檢測裝置，用以控制資料編碼、解碼及密碼技術之錯誤檢測，該乘法器的電路特性係對有限場 $GF(2^m)$ 中之一第一元素 A 與一第二元素 B 進行乘積運算，以得到第三元素 C，其中元素 A 是以多項式基底 $(1,\alpha,\alpha^2,\Lambda,\alpha^{m-1})$ 之表示式，元素 B 及 C 是以雙重基底之表示式，該有限場 $GF(2^m)$ 為不可分解之多項式所產生的，及α為該不可分解的多項式之根；該第一元素 A 被表示為一 m 位元 $A=a_0+a_1\alpha+a_2\alpha^2+\Lambda+a_{m-1}\alpha^{m-1}$，該第二元素 B 被表示為一 m 位元 $B=b_0\beta_0+b_1\beta_1+b_2\beta_2+\Lambda+b_{m-1}\beta_{m-1}$，該第三元素 C 被表示為一 m 位元 $C=c_0\beta_0+c_1\beta_1+c_2\beta_2+\Lambda+c_{m-1}\beta_{m-1}$，其中所有元素的係數是等於 0 或 1，該乘法器包括有兩單元：

一雙重基底乘法單元，其電路包括由 (m+1)×m 個細胞組成，以形成 (m+1) ×m 陣列，且每一細胞包含有三個以上輸入信號線、三個以上輸出信號線；每一細胞包含一個以上 AND 閘、一個以上 XOR 閘和三個以上單位元暫存器 (Latch)；及

一雙重基底轉換單元，其電路包括樹狀式 2-input XOR 閘所構成；其中，

該乘法器的雙重基底乘法單元包含有三種小細胞 (U 細胞、W 細胞與 V 細胞)；其中，

該 U 細胞，係在第 i 列執行下列函數：計算 b_{m+i}，$\alpha^i B$和

$\hat{P}_{\alpha^{i+1}B} = b_{i+1}p_0 + \sum_{j=1}^{m-1} b_{i+j+1}\bar{p}_j$，其中 $0 \le i \le m-2$；

該 W 細胞，其中在 b_{m+i} 和 $\hat{P}_{\alpha^{i+1}B}$ 兩者在 U 細胞是最後計算時，係使用 4 個信號，b_i，b_{m+i}，$\hat{P}_{\alpha^{i+1}B}$ 和 $\hat{P}_{\alpha^{i}B}$，去完成 b_{m+i} 計算的錯誤檢測，其中 $\hat{P}_{\alpha^{i}B}$ 在 U-細胞的第(i-1)列被計算，特別是假若 i = 0，則 $\hat{P}_B = P_B$ 時；且 W 細胞使用 $\hat{P}_{\alpha^{i}B}$ 和 a_i，其中在 $0 \le i \le m-2$，則是為了計算已預測的奇偶同位檢測 $\hat{P}_C$；

該 V 細胞，在最後列，$V_{m-1,j}$ 細胞在 $0 \le j \le m-1$ 執行 $\alpha^{m-1}B$ 和 P_C 兩者計算；此 $V_{m-1,m}$ 細胞需負 $a_{m-1}\hat{P}_{\alpha^{m-1}B}$ 計算責任和整體乘法器錯誤檢測。

2．如申請專利範圍第 1 項所述之具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，其中，該乘法器在上述 U、V 和 W 細胞之一發生不良時會發生單一陷入錯誤，並藉由該乘法器偵測出該錯誤。

3．如申請專利範圍第 2 項所述之具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，其中，可檢測的錯誤包括：在 P_j 上的錯誤，細胞 $U_{i,j}$ 的輸出信號 P_j，使用來自輸入信號 P_j 的一通過線。

4．如申請專利範圍第 2 項所述之具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，其中，可檢測的錯誤更包括：在 a_i 上的錯誤，細胞 $U_{i,j}$ 的輸出信號 a_i，亦是來自輸入信號 a_i 的通過線。

5．如申請專利範圍第 2 項所述之具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，其中，

可檢測的錯誤更包括：在b_{i+j}上的錯誤，細胞 $U_{i,j}$ 的輸出信號b_{i+j}，也使用來自輸入信號b_{i+j}的一通過線。

6．如申請專利範圍第2項所述之具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，其中，可檢測的錯誤更包括：在$\overline{P}_j$上錯誤，細胞 $U_{i,j}$ 的輸出信號$\overline{P}_j$，也使用來自輸入信號$\overline{P}_j$的一通過線，因此其上錯誤容易檢測出。

7．如申請專利範圍第2項所述之具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，其中，可檢測的錯誤更包括：在c_j上的錯誤，假如一個錯誤在不良的細胞 $U_{i,j}$.的輸入信號c_j上出現，該錯誤將影響輸出信號c_j的最後結果，因此，計算在 V-細胞 C 的奇偶同位檢測位元，使用方程式 $P_C=\sum_{j=0}^{m-1}c_j$ 能被計算，在 W-細胞 C 的已預測奇偶同位檢測位元，使用方程式 $\hat{P}_C=\sum_{j=0}^{m-1}a_i\hat{P}_{\alpha^i B}$ 被執行，最後在 $V_{m-1,m}$-細胞，比較實際的奇偶同位檢測P_C和已預測奇偶同位檢測$\hat{P}_C$，這個錯誤則檢測出。

8．如申請專利範圍第2項所述之具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，其中，可檢測的錯誤更包括：在b_{m+i}或$\hat{P}_{\alpha^{i+1}B}$上的錯誤，假如一個錯誤在不良的細胞 $U_{i,j}$.的輸入信號b_{m+i}上出現，這個錯誤將影響輸出信號b_{m+i}；因此，使用方程式 $\hat{e}_{b_{m+i}}=\hat{P}_{\alpha^i B}+\hat{P}_{\alpha^{i+1}B}+b_{m+i}+b_i$，$\hat{e}_{b_{m+i}}$在此 $W_{i,m}$-細胞能變成邏輯 1，那就是說此錯誤能被檢測出，且

在細胞 $U_{i,j}$ 上 $\hat{P}_{\alpha^{i+1}B}$ 錯誤也能使用方程式 $\hat{e}_{b_{m+i}} = \hat{P}_{\alpha^{i}B} + \hat{P}_{\alpha^{i+1}B} + b_{m+i} + b_i$ 檢測出。

9．如申請專利範圍第2項所述之具即時偵錯能力之位元並列輸出型心臟收縮陣列式雙重基底乘法器，其中，可檢測的錯誤更包括：在 $\hat{P}_C$ 或 P_C 上錯誤，假如一個錯誤在細胞 $W_{i,m}$ 的輸入信號 $\hat{P}_C$ 上出現，則在細胞 $V_{m-1,m}$ ，$\hat{e}_C$ 藉由應用方程式 $\hat{e}_C = \hat{P}_C + P_C$ 將變成邏輯1，而能被檢測出此錯誤；且在 $V_{m-1,j}$ 細胞，P_C 的輸出信號不良時，使用方程式 $\hat{e}_C = \hat{P}_C + P_C$，亦能發現在 $V_{m-1,m}$ 的錯誤。

99年1月12日修 正替換頁

十一、圖式：

如次頁

七、指定代表圖：

(一)本案指定代表圖爲：第（ 三 ）圖。

(二)本代表圖之元件符號簡單說明：

（３０）U 細胞

（３１）V 細胞

（３２）W 細胞

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：