模數化簡 Modular Reduction

在我們的實作中，共需配置十一個模數化簡模組：每個 BF 模組中包含一個模數化簡模組，而 PWM 模組中包含兩個個模數化簡模組。對於 46-bit 整數 s 的模數化簡，我們遞迴利用關係式$2^{23} \equiv 2^{13} - 1 \; mod \; q$，方式與文獻 [19] 類似。

$$
\begin{aligned}
s[45:0] &\equiv 2^{23}s[45:23] + s[22:0] \equiv 2^{13}s[45:23] - s[45:23] + s[22:0] \\
&\equiv 2^{23}s[45:33] + 2^{13}s[32:23] - s[45:23] + z \\
&\equiv 2^{13}(s[45:33] + s[32:23]) - (s[45:33] + s[45:23]) + z \\
&\equiv 2^{23}s[45:43] + 2^{13}(s[42:33] + s[32:23]) - (s[45:33] + s[45:23]) + z \\
&\equiv 2^{13}(s[45:43] + s[42:33] + s[32:23]) - (s[45:43] + s[45:33] + s[45:23]) + z \\
&\equiv 2^{13}x - y + z \equiv 2^{23}x[11:10] + 2^{13}x[9:0] - y + z \\
&\equiv 2^{13}(x[11:10] + x[9:0]) - (y + x[11:10]) + z \mod q
\end{aligned}
$$

化簡後的結果仍可能大於2^{23}，因此我們可以重複上述遞迴展開一次，但這將增加邏輯延遲與電路深度。然而我們觀察到，該模數化簡的結果往往已落在區間(−q,2q)之內。對此，只需在結果為負時加上 q，或在結果為正時減去 q 即可。最終的結果會從正值與負值中選擇非負的一方。

在實作上，本模組接收一筆 46-bit 的輸入資料 s=a·b，並進行模數為 q=8380417 的模數化簡運算。整體電路流程可區分為四個主要階段，並於**第一階段的輸出端**與**最終輸出端**各設置一級 pipeline，藉以平衡邏輯延遲並提升整體資料處理速率。

在第一階段，輸入資料 s[45:0]依據其位元位置被拆解為三組資料區段，分別對應三項中間變數的計算。首先，上方加法器負責計算 x=s[45:43]+s[42:33]+s[32:23]， 為後續乘上2^{13}的主體部分。中間加法器則計算

y=s[45:43]+s[45:33]+s[45:23]，

下方則直接取出最低位元 s[22:0]s[22:0]s[22:0] 作為變數

z=s[22:0]。

。為了提升資料穩定性與減少邏輯擁塞，在此階段末端插入一級 pipeline 寄存器，作為後續計算的資料緩衝。

第二階段中，先將 x 拆解為高位 x[11:10]與低位 x[9:0]，並進行加總後左移 13 位（即乘上 2^{13}）。此乘積接著與第一階段所得之 z−y−x 相加，形成整體的中間化簡結果：

Result=213(x[11:10]+x[9:0])+(z−y−x)\text{Result} = 2^{13}(x[11:10] + x[9:0]) + (z - y - x)Result=213(x[11:10]+x[9:0])+(z−y−x)

第三階段負責判斷此結果是否已落於模數 qqq 的合法值域中，亦即檢查是否屬於開區間 (−q,2q)(-q, 2q)(−q,2q)。根據結果大小進行補正：若結果小於 0 則加上 qqq；若大於等於 qqq 則減去 qqq；若已位於合法區間內則不做修正。此判斷邏輯由兩級選擇器（MUX）與加減法單元實現。

最後一階段將補正後結果輸出，並於此處設置一級 pipeline，作為整體模組的輸出緩衝。最終輸出資料為 13-bit 的模 qqq 餘數 out[12:0]\text{out}[12:0]out[12:0]，其值域保證落於區間 [0,q)[0, q)[0,q)，可直接供後續加解密或乘法模組使用。