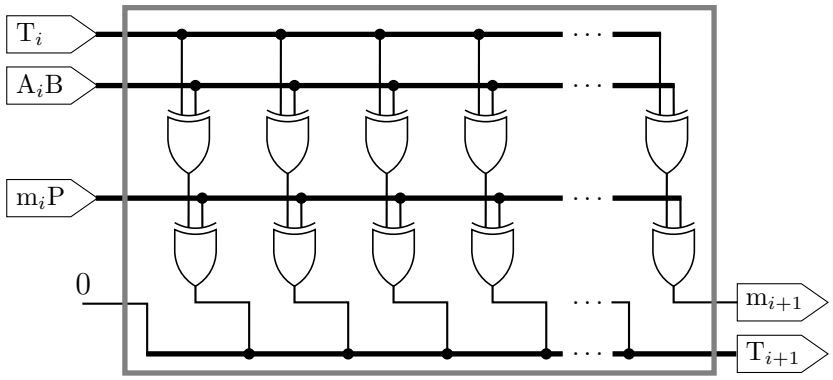
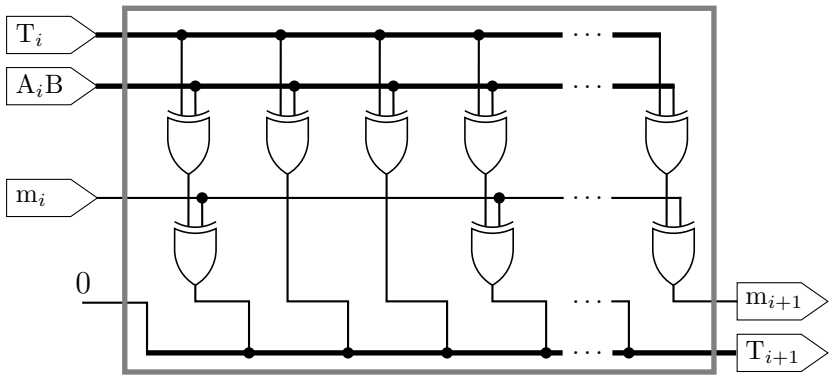
Hoofdstuk 1

Modular Arithmetic Logic Unit (MALU)

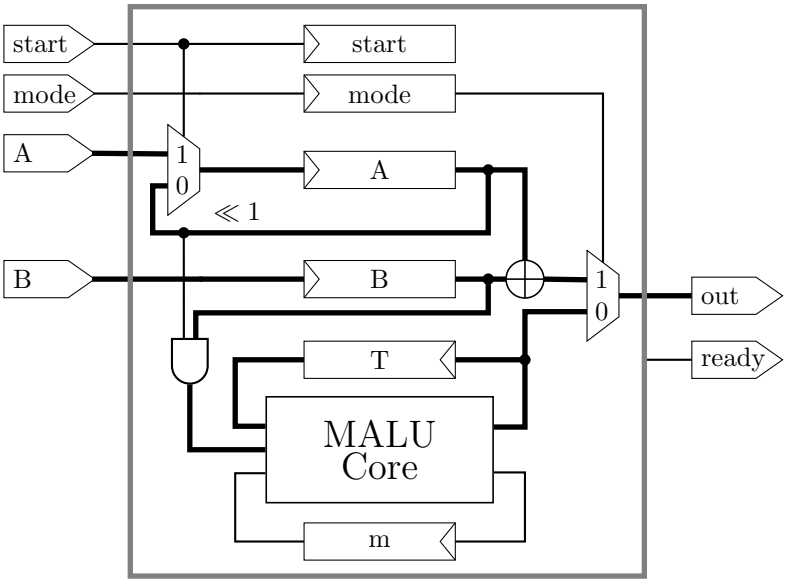
1.1 MALU over GF(2^m)



Figuur 1.1: Basis implementatie van een MALU-blok met $d = 1$



Figuur 1.2: Geoptimaliseerde implementatie van een MALU-blok met $d = 1$



Figuur 1.3: GF_{2^m} Wrapper

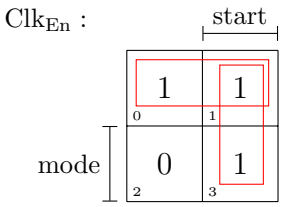
Hoofdstuk 2

Optimalisaties

2.0.1 Clock gating voor het A register

Daar voor het A register gekozen moet worden uit drie inputs, zijnde A, A_{in} of $A_{\ll 1}$, is voor dit register een andere implementatie vereist dan voor de overige registers. Daar moet immers slechts uit X of X_{in} gekozen worden, wat, zoals eerder aangetoond, toelaat een multiplexer uit te sparen door toepassing van clock gating. In tegenstelling tot de andere registers kan men hier niet anders dan een MUX gebruiken. Ook aan het circuit voor de clock gating moeten enkele toevoegingen gebeuren.

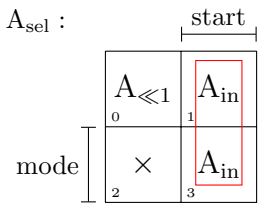
Ten eerste wordt gekeken wat juist de nodige aanpassingen aan het clock gating enable signaal zijn. Indien er vermenigvuldigd wordt ($mode = 0$), moet elke clock cycle $A_{\ll 1}$ in A opgeslagen worden. Het kloksignaal dient dus doorgelaten te worden indien een berekening begint ($start = 1$) of indien een vermenigvuldiging aan de gang is. Dit leidt tot onderstaande Karnaugh map:



M.a.w. het nodige klok enable signaal voor de flip flops is:

$$\text{Clk}_{\text{En}} = \text{start} + \overline{\text{mode}}$$

Ten tweede wordt gezocht welk signaal gebruikt moet worden om de MUX te schakelen. Bij het starten van een berekening moet uiteraard A_{in} geselecteerd worden. Bij de uitvoering van een vermenigvuldiging ($mode = 0$) dient $A_{\ll 1}$ geselecteerd te worden. Wanneer een berekening aan de gang is, maakt het voor een optelling ($mode = 1$) niet uit welke ingang gekozen wordt, aangezien de klok ingang van de flip flop dan uitgeschakeld is. Dit geeft aanleiding tot de volgende Karnaugh map:



Waarbij het ×-symbool staat voor een zogenaamde "don't care". Indien men $A_{\ll 1}$ aansluit op de 0-ingang van de multiplexer en A_{in} op de 1-ingang, kan *start* dus gebruikt worden als schakelsignaal:

$$A_{sel} = \text{start}$$