

Lab Frontend Backend Asic

Bruno Pons

Analysis:

Unroll Factor	Période d'horloge (ps)	Surface de portes logiques	Consommation (mW)	Crypto débit: crypto/s (en millions) *
1	2780	1724	1,148	11,2
2	4050	4555	1,439	15,4
4	7800	11089	2,012	16
8	15000	26183	4,568	16,7
16	29500	56876	9,681	17

Tableau 1: Période d'horloge, surface, consommation d'énergie et performance en fonction du facteur de déroulement.

* Pour effectuer les calculs de performance, nous considérons qu'un cryptogramme prend 32 tours, lorsqu'il est parallélisé par le facteur de déroulement (tours par cycle), le nombre de cycles pour un cryptogramme est exprimé comme suit : $\text{cycles} = 32 \text{ tours} / \text{unroll_fctr}$, par exemple, avec un facteur de déroulement égal à 2, il faut 16 cycles pour un cryptogramme.

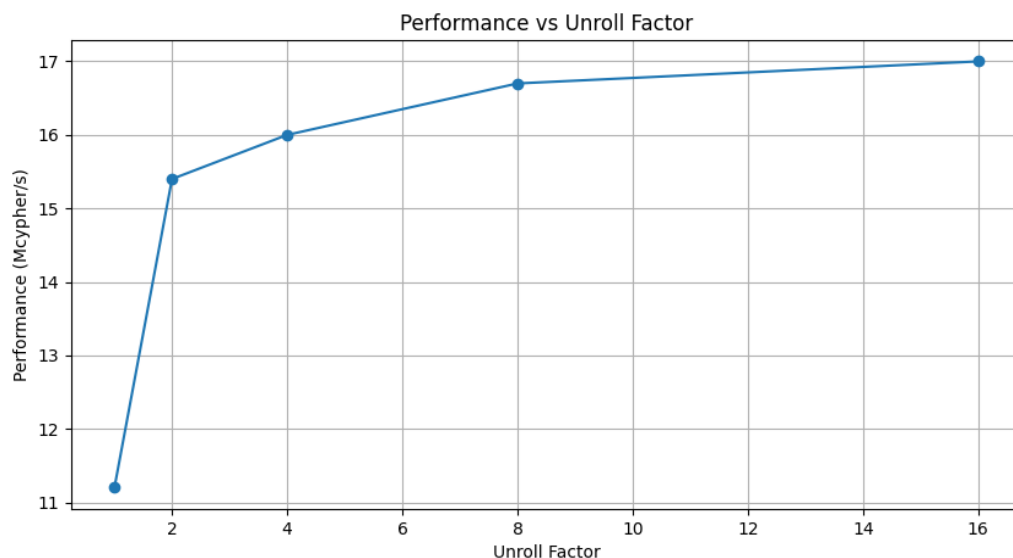


Figure 1: Performance en fonction du facteur de déroulage

Nous pouvons déduire de la figure 1 que ce n'est pas linéaire, nous avons une forte augmentation des performances pour un faible facteur de déroulage, pour un facteur de

déroulage plus important l'amélioration tend à être monotone. Si l'on tient compte des mesures de la surface et de la consommation d'énergie qui augmentent approximativement de façon linéaire en fonction du facteur de déroulage, mais que les performances ne s'améliorent pas considérablement, le facteur de déroulage optimal serait alors de 2.

Bonus 1:

Unroll Factor	Période d'horloge (ps)	Surface de portes logiques	Consommation (mW)	Crypto débit: crypto/s (en milliers) *
1	601380	1219	5,191	51,9
2	603438	1821	7,010	103,6
4	607106	3002	13,24	205,9
8	614453	5430	32,37	406,9
16	629199	10306	91,56	794,7

Tableau 2: Période d'horloge, surface, consommation d'énergie et performance en fonction du facteur de déroulement.

Nous pouvons voir dans le tableau 2 que si nous ne mettons pas de contraintes de temps, le synthétiseur utilise une période d'horloge élevée (puisqu'il trouve le mou de manière paresseuse). Par conséquent, les performances diminuent considérablement, bien que nous obtenions une surface plus petite et une consommation d'énergie nettement plus faible (2 ordres de moins).

Bonus 2:

Unroll Factor	Période d'horloge (ps)	Surface de portes logiques	Consommation (mW)
1	601235	1219	4,912
2	602682	1819	6,317
4	605467	3005	11,05
8	611258	5430	26,36

Tableau 3: Période d'horloge, surface, consommation d'énergie et performance en fonction du facteur de déroulement.

Nous pouvons voir dans le tableau 3 que les résultats ne varient pas beaucoup par rapport à ceux obtenus précédemment dans la synthèse non spatiale, nous pouvons donc dire que la synthèse non spatiale donne des résultats acceptables.