**Travail Pratique #1**

INF3500 : Conception et réalisation de systèmes numériques

Rapport remis par :

Anastasiya Basanets (1933929)

Mariam Sarwat (1928777)

Groupe : B1

|  |  |
| --- | --- |
| Critère | Points |
| Partie A : conception du module  Partie B : banc d’essai et simulation  Partie C : implémentation  Discussion  Rapport : présentation et qualité du français | 8  4  4  2  2 |
| Total | 20 |

École Polytechnique de Montréal

Date de remise (08-02-2019)

**Partie A : Implémentation des fonctions de compression de l’algorithme SHA-256**

Tout d’abord, nous avons dû écrire nos 6 fonctions de compressions en VHDL. Pour ce faire, nous nous sommes inspiré des exemples vus en cours. Par la suite, nous avons simulé nos fonctions selon les étapes fournies dans TP.

*Schéma 1 :* Simulation du banc d’essai

A picture containing text, scoreboard

Description automatically generated

La simulation du banc d’essai se retrouve ceci dessus. En effet, nous avons 3 entrées, soit x, y et z, et 6 sorties qui représentent la sortie de nos fonctions de compressions. Afin de vérifier le bon fonctionnement de nos fonctions, nous avons comparer les entrées avec les valeurs de sorties. Prenons comme exemple les entrées x, y et z qui sont mis à la valeur 0. Nous devons avoir 0 comme sortie pour les 6 variables de sorties, qui est le cas. Nous avons, de plus, vérifier avec les entrées 2 et 5. Comme on obtient les bonnes sorties, on peut conclure que nos fonctions de compression sont bien écrites.

**Partie B : Simulation**

*Schéma 2 :* Simulation du SHA256 Compression

A picture containing grass

Description automatically generated

La simulation du SHA256 compression se retrouve ceci dessus. En effet, comme pour la simulation du banc d’essai fait à la partie 1, nous avons 3 entrées et 6 sorties. Comme ce fichier possède déjà des valeurs de tests, nous avons dû s’assurer que pour les entrées données, nous avons eu les sorties correspondantes. Ce qui a été le cas. On a donc revérifié que nos fonctions de compressions correspondent aux équations données dans l’énoncé.

**Partie C : Implémentation**

Afin de faire l’implémentation des fonctions de compressions nous avons du crée un fichier top qui les relient ensembles dans l’ordre décrit dans l’énoncé du TP1. Il était important de s’assurer que notre valeur d’entrée et de sortie étaient en 16 bits. Alors, pour ce faire, nous avons fait la conversion de 16 bits à 32 bits pour notre entrée et de 32 bits à 16 bits pour la sortie. Lorsque la conversion c’est complet, la valeur d’entrée va passer par tous les fonctions dans notre fichier top et va sortir une valeur de sortie.

**Discussion**

Finalement, nous avons atteint les objectifs de ce laboratoire, soit de faire la description d’un circuit combinatoire. De plus, nous avons réussi à simuler et implémenter correctement notre circuit.