Laboratoire #5 : Intégration système du SHA256

INF3500 - Conception et réalisation de systèmes numériques
Hiver 2019

Objectifs

Ce laboratoire a trois objectifs :

— vous familiarisez avec les outils utilisés lors des laboratoires du cours INF3500 ;
— approfondir votre connaissance de l'intégration système ; et
— vous introduite le concept de co-design logiciel/materiel.

Préparation au laboratoire

Avant d'arriver au laboratoire, suivre les étapes suivantes :

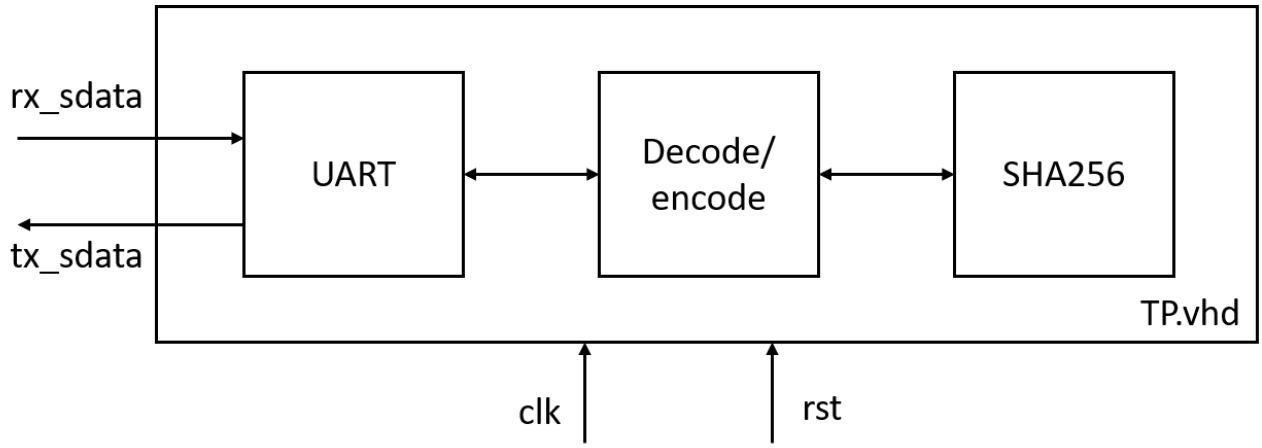
1. Revoir la matière des cours des semaines 7, 8, 9 et 10 ; et,
2. Lire le guide d'utilisation de Vivado.
3. Lire la FAQ du laboratoire

Familiarisation avec les outils

Suivre les instructions du guide pratique d'utilisation de Vivado. Ce tutoriel est indispensable pour faire la simulation, la synthèse, l'implémentation et la programmation du FPGA.

Partie A : Intégration système logiciel-matériel SHA256

Au cours de cette session, vous avez developpe des modules indépendants afin d'implementer l'algorithme SHA256. Maintenant, vous allez l'intégrer dans un environnement de la "vie réel". Un script python qui vos êtes fournit, enverra de requêtes de calcul du SHA256 par UART. Les requêtes devraient être decoders par une machine à états avant de passer les données au module SHA256. Le résultat du SHA sera encodé par une autre machine à états avant d'être envoyé par UART. La figure suivante décrit l'architecture proposée.



Le message de requête de calcul est encodé sur 4 trames UART. Le format de la message présenté ci-dessous est du LSB (”Least Significant Bit”) vers le MSB (”Most Significant Bit”).

bit 0	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7
1	1	0	0	0	0	1	0
1	0	1	0	0	0	1	0
D[8]	D[9]	D[10]	D[11]	D[12]	D[13]	D[14]	D[15]
D[0]	D[1]	D[2]	D[3]	D[4]	D[5]	D[6]	D[7]

Le message de réponse utilise le même encodage, mais les champs des données sont remplis avec le résultat du calcul du hash.

Livrable : Remettre le code de vos machines à états, les diagrammes des transitions d'états et une preuve que la simulation fonctionne.

Partie B : Synthèse et Implémentation

Synthétisez et implémentez votre système de calcul SHA256 sur la carte Nexys4 DDR. Pour tester votre circuit, vous devez communiquer en utilisant l'interface utilisateur fournie. Vous devez fournir une preuve que votre circuit fonctionne (montrer aux charges de labo au par vidéo).preuve que votre circuit fonctionne (montrer au charge de labo au par video).

Fichiers fournis

Voici les fichiers de base pour l'implementation du laboratoire 5. Dans le répertoire *sw* vous allez trouver le script python pour communiquer avec la carte, dans *hw* vous allez trouver les fichiers vhd (avec un banc d'essai) ainsi que le fichier xdc.

Rapport

Important : le rapport pour ce laboratoire n'est pas demandé.

Barème

Critère	points
Partie A	10
Partie B	10
Total	20