POLYTECH LILLE

Sujets de TP

Circuits Numériques Programmables avancés

A. Boé

Année 2021 / 2022

Introduction

- Évaluation :

  - Rendus intermédiaires après chaque séance (projet git sur archives.plil.fr) avec les sources VHDL, les simulations et autres éléments d'analyse.

  - rapport de projet en format .zip à envoyer à alexandre.boe@univ-lille.fr pour le **lundi 09/05/2020 à 18 h**, délai de rigueur.
    - ✓ Sources VHDL **commentées** (uniquement les fichiers utiles) et configuration des entrées/sorties (.xdc) ;
    - ✓ Rapport de projet (cf. transparent suivant) ;
    - ✓ Autres fichiers pertinents (simulations, schémas, photographie, vidéos, …).

Introduction

- Contenu du compte-rendu :
    - Page de garde avec titre et nom ;
    - Introduction (~ ½ page, < 1 page) ;
    - Principe de fonctionnement (schéma de principe, théorie, justification des choix, …) 1 à 2 pages, < 3 pages, par grand composant développé ;
    - Explication de parties du code (parties intéressantes et/ou ardues), 1 à 2 pages (< 3 pages) ;
    - Procédures de tests et résultats des tests, validation du fonctionnement (1 à 2 pages, < 3 pages) ;
    - Conclusion (~ ½ page, < 1 page).

- Donc compte rendu de 8 pages minimum à 15 pages maximum. Vous serez vigilants sur une mise en page « classique » (police 11, interligne 1,5, marges raisonnables et taille des images / portions de code de taille modérée) ;
- Format .pdf non protégé.

Introduction : unité de calcul FPGA et *hardware trojan*

Le calcul est une fonction primordiale dans les circuits numériques. Les calculs intermédiaires doivent en général rester confidentiels afin de ne pas exposer les algorithmes utilisés. Les circuits étant complexes, il est difficile voire impossible de tester complétement l'intégrité des fonctions réalisées. Il est donc possible d'ajouter un peu de logique non désirée afin de créer une porte dérobée (*backdoor*).

Nous proposons ici de faire une unité de calcul permettant de réaliser diverses opérations mathématiques et d'insérer une porte dérobée pour récupérer les données de calcul.

Introduction : unité de calcul FPGA et *hardware trojan*

Il convient d'évaluer les performances des cicuits générés en termes de :

- Fonctionnalité (simulation ou implémentation et tests) ;

- Fréquence maximale d'utilisation ;
- Surface utilisée (nombre de LUT et ressources spécifiques) ;
- Consommation.

Les différents éléments de performances, affectés par les différentes options de synthèse, seront présentés de façon synthétique.

Étapes

Partie 1 : unité de calcul FPGA

Étape 1 : Addition de deux vecteurs sur N bit, nombres non signés entiers ou à virgule fixe.

- Faire un additionneur permettant d'additionner deux entiers sur N bit ;
- Évaluer les performances en fonction du nombre de bit ;
- Proposer une seconde architecture pipelinée plus efficace ;
- Comparer l'efficacité des deux solutions en fonction du nombre de bit.

Étape 2 : Multiplication de deux vecteurs complexes sur N bit.

- Implémenter un multiplieur complexe naïf et évaluer ses performances ;
- Implémenter le multiplieur optimisé et pipeliné et comparer les performances.

Étapes

Partie 2 : RAM « sécurisée »

Cette étape consiste à réaliser une mémoire possédant une zone « sécurisée » :

- Une partie de la RAM est accessible sans limitation, que ce soit en lecture en écriture ;
- Une deuxième partie de la RAM n'est accessible qu'en lecture, sauf si une entrée particulière est activée (unlock_w_in) ;
- Une troisième partie de la RAM accessible ni en lecture ni en écriture, sauf si une entrée particulière est activée (unlock_rw_in)

Partie 3 : Porte dérobée

Cette étape propose de réaliser une porte dérobée dans la mémoire « sécurisée ».

- Un émetteur en OOK (On Off Keying) basé sur la fréquence d'horloge du FPGA (100 MHz) ;
- Un automate de détection d'une séquence d'activation de la porte dérobée. Une fois la séquence détectée, l'automate accédera aux données protégées en lecture / écriture et transmet les données sur une E/S.

Le test final consiste à vérifier la validité de la fonction réelle à l'aide d'un test fonctionnel sans déclencher la porte dérobée et en la déclenchant.