Implémentation de l'algorithme de hachage MD5

Objectif

Réaliser votre première conception d'un système réel.

Description

MD5 est un algorithme classique de hachage utilisé dans de nombreuses applications. Le but est de réaliser une implémentation FPGA pour accélérer le calcul de cet algorithme. Votre application doit pouvoir calculer le hash de n'importe quel fichier.

Si vous avez une implémentation software du MD5, vous pouvez taper :

```
#./md5 mon_fichier
```

Vous obtenez comme résultat un hash de 128b bits.
exemple : 595F44fec1e92a71d3e9e77456ba80d1

Votre objectif est de créer un device (et son driver) de telle manière que l'on puisse l'exécuter sur linux.

```
#cat mon_fichier > /dev/votre_device_MD5
```

suivi de

```
#cat /dev/votre_device_MD5
```

et de récupérer le hash :

```
595F44fec1e92a71d3e9e77456ba80d1
```

Pour vous simplifier la réalisation de ce laboratoire, nous vous fournissons une IP de l'algorithme MD5 permettant de l'implémenter dans la partie FPGA du SoC. L'IP fournie permet de calculer le hash pour un bloc de 512 bits.

Références

Différentes implémentations logicielles peuvent être trouvées sur internet, comme par exemple sur le site https://rosettacode.org/wiki/MD5 qui dispose d'un vaste catalogue d'implémentation.

Sur l'algorithme en lui-même, il y a également beaucoup de documentation. Wikipedia est un point de départ très utile https://en.wikipedia.org/wiki/MD5; si vous voulez tout savoir sur l'algorithme, le standard est disponible sur https://tools.ietf.org/html/rfc1321.

N'hésitez pas à discuter de vos idées d'architectures et de développement avec nous avant de les implémenter ! Votre temps est limité et nous pouvons éviter des erreurs classiques.

Documents à rendre

Vous devez rendre un rapport à l'issu de ce laboratoire contenant les explications concernant votre architecture et vos analyses de performance.

Vous devez également rendre le code source de votre driver et du design FPGA.

Les fichiers sont à rendre sur Moodle.

Déroulement et validation

Le laboratoire est réalisé individuellement et se déroule sur 2 séances de 4 périodes.

La validation finale de votre projet sera réalisée à distance.