Master SESI
Proposition de stage - M2 - 2021-2022

Etude et caractérisation du projet Pynq pour la distribution quantique de clé sur FPGA

Description générale du projet :

La cryptographie traditionnelle est basée sur la difficulté à résoudre certains calculs mathématiques. Avec l'évolution de la technologie (en particulier de l'ordinateur quantique) on ne peut pas considérer ce type de technologie comme sécurisée à long terme. La cryptographie quantique peut offrir une sécurité absolue basée sur les lois de la physique, et garantir que celle-ci sera la même, indépendamment du temps écoulé. Cet objectif est atteint en utilisant la méthode du masque jetable. La clé nécessaire pour le chiffrement est envoyée de l'émetteur (Alice) vers le récepteur (Bob) à travers un canal quantique (optique) dit « non sécurisé » : on considère que l'on est en présence d'un espion (Eve) disposant d'une puissance illimitée.
Le message pourra ensuite être chiffré puis déchiffré avec cette clé, en utilisant un canal classique authentifié (internet). La partie quantique est limitée à l'échange de clé, donc on parle de distribution quantique de clé ou quantum key distribution (QKD).

Il y a différentes façons d'échanger des clés entre Alice et Bob. Le premier protocole proposé, BB84, utilise des photons uniques (particules de la lumière) pour la transmission de l'information. Plusieurs variantes de ce protocole sont aujourd'hui déjà commercialisées, mais elles présentent différents défis technologiques, en particulier en terme de coût des détecteurs de photons uniques. Dans le groupe d'Information Quantique du LIP6, nous travaillons depuis plusieurs années sur un système alternatif : on transmet l'information dans la phase et l'amplitude du champ électromagnétique quantifié, ce qui est beaucoup plus simple et moins coûteux. En effet, les lasers et les photodiodes utilisées sont normalement conçus pour les systèmes de télécommunications optiques classiques cohérentes. On utilise la dénomination variable continues (continuous variables, CV-QKD) pour appeler ce type de protocoles et les différencier des protocoles à photons uniques (discrete variables, DV-QKD).

Présentation de la partie électronique & informatique :

La plateforme qui porte notre projet repose sur une carte de développement Xilinx de la gamme UltraScale+ RFSoC : la ZCU111. Nous avons développé un ensemble d'IPs et de codes en C et en python qui répondent à nos exigences. Pour cela, nous exploitons un certains nombre d'éléments disponibles, en particulier des DACs et des ADCs, des connecteur SFP (réseau) à 100 Gbps et 32Go de RAM DDR4. Le plus gros enjeu pour ce projet consiste à mettre en place une expérience de CV-QKD fonctionnelle, sachant que ce FPGA atteint ses limites pour les performances désirées.

L'objectif principal de PYNQ (**Py**thon pour la productivité Zy**nq)**, est de rendre plus facile pour les concepteurs de systèmes embarqués, l'exploitation des avantages des produits Xilinx dans leurs applications. En particulier, Xilinx fabrique des systèmes Zynq, une gamme de système sur puce programmable (SoC) qui intègre un processeur multicœur ARM (Processor System : PS) et un FPGA (Programmable Logic : PL) en un seul circuit intégré. Les FPGA et les microprocesseurs sont des technologies complémentaires dans les systèmes embarqués. Chacun répond à des exigences distinctes que l'autre ne peut pas exécuter aussi bien.

Les circuits logiques programmables sont présentés sous forme de bibliothèques matérielles appelées « overlays » . Bien que le design d'un overlay nécessite toujours des ingénieurs avec une expertise dans la conception de circuits logiques programmables, leur utilisation est analogue aux bibliothèques logicielles. En particulier, l'utilisation du langage Python permet d'exploiter un haut niveau de productivité.

Contexte :

Le contexte de ce stage s'inscrit dans un projet global. En particulier, le ou la stagiaire fera partie de l'équipe QI qui travaille sur ce sujet en étroite collaboration avec l'équipe SYEL, il ou elle participera aux différentes réflexions et interrogations, apportera son expérience et aidera à faire avancer le projet dans la globalité. Il n'est pas rare de communiquer avec des collègues d'autres équipes, en particulier DELYS et ALSOC pour des problématiques plus système, Kernel…

Un certains nombre de taches sont en cours, avec différentes interrogations qui empêchent de comprendre en profondeur et d'exploiter correctement le matériel dont nous disposons. Cette offre de stage propose différentes approches, en particulier :

- travailler sur la notion d'overlay, au sens de Xilinx et de Pynq.
- travailler sur la reconfiguration dynamique, et l'implémenter sur la plateforme Pynq.

Pour ces 2 parties, il sera demandé de comprendre et de documenter (au moins pour le LIP6, sur Internet si possible) ces différentes aspects, afin de pouvoir les utiliser correctement dans notre projet. Ces notions ne sont pas encore parfaitement comprises et nécessitent d'être maîtrisées convenablement pour être exploitées ensuite.

De plus, il sera possible de travailler sur plusieurs aspects, par ordre de priorité :

- parallélisation ou synchronisation des BUS HPx de la PS afin d'atteindre le débit maximal atteignable par le processeur ARM (ZCU111)
- utilisation des SD-FECs (Soft-Decision FEC Integrated Block) intégrés à la carte (ZCU111)
- développement de différents modules Kernel Linux afin de réserver et/ou d'allouer proprement un espace mémoire depuis la PS, pour utiliser les différents périphériques (DDR4, ADC, ADC, SFP…)
- optimisation de la partie logicielle (codes C)
- mise en place du réseau à 100Gbps (ZCU111)

Enfin, le ou la stagiaire pourra se former et documenter son travail sur le logiciel Vitis en mettant en avant ses différences avec l'ancien couple Vivado/SDK (au moins pour le LIP6, sur Internet si possible).

Bien sur, le stage est flexible est pourra être adapté à un(e) étudiant(e) motivé(e).

Connaissance requises :

Co-design sur plateforme Xilinx (Microblaze et/ou Zynq) & interface AXI4
Kernel : allocation mémoire, périphériques, communication...
Compréhension de l'anglais technique (GitHub, datasheet, forum Xilinx/Pynq, readthedocs …)
Connaissance en python appréciées (ou connaissance de Matlab)
Une curiosité scientifique et des connaissances générales en physique (et en quantique) seront un plus

Moyens à disposition :

Le stage, rémunéré, se déroulera au LIP6. Un PC avec un OS GNU/Linux sera à disposition. De plus, une carte PYNQ-Z2 et ZCU111 seront disponibles (entre autre).

Au vu du contexte sanitaire actuel, il faut s'attendre à ce qu'une partie du stage soit réalisée à distance.

S'agissant d'un projet open source largement porté par la communauté, l'étudiant aura à sa disposition un ensemble de documents et d'exemples sur le sujet. Il pourra si il le désire publier son travail et ses observations sur un repository (GitHub…) ou le forum de Pynq.

Encadrants :

FRULEUX Damien, GRANADO Bertrand, DIAMANTI Eleni
mail : damien.fruleux@lip6.fr