Telecom Saint-Étienne
FISE 3

Co-Design
– Rapport de TP –

Étude en Filière Ingénieur sous Statut Étudiant
28.01.2026

Bastien DESCOS

Table des Matières

I. Notebook exemple cybersécurité

1. Présentation du dataset

Le dataset que nous allons utiliser est le UNSW-NB15, ce dataset a initialement 2,540,044 entrées réparties en 4 fichiers principaux. Nous allons utiliser 175,341 enregistrements en tant que base de données d'entraînement ainsi que 82,332 en tant que base de données de test.
Il contient différent types d'attaque permettant d'entraîner le modèle pour reconnaître ces attaques:

- Fuzzers
- Analysis
- Backdoors
- DoS
- Exploits
- Generic
- Reconnaissance
- Shellcode
- Worms

En l'occurrence, la version que nous téléchargeons est une version pré-quantifiée ce qui nous permettra un temps de téléchargement beaucoup plus court.

La sortie du réseau est simplement un retour qui indique si l'entrée est suspicieuse ou si elle est seine grâce à une probabilité allant de 0 (l'entrée est sûre) à 1 (l'entrée est suspecte).

2. Entrainement MLP

2.a) Modèle

Le réseau est un MLP avec 593 entrées, 3 couches cachées de 64 neurones, et une couche de sortie de 1 neurone. On retrouve donc 1 sortie qui indique la probabilité que l'entrée soit une attaque ou non.
Un modèle MLP (Multi-Layer Perceptron) est un réseau de neurones artificiels composé de plusieurs couches de neurones entièrement connectées. Chaque neurone dans une couche est connecté à tous les neurones de la couche suivante.
Cela nous fait un total de $593\times64 + 64\times64 + 64\times64 + 64\times1 = 38{,}081$ poids.
Le modèle est entraîné avec une fonction de perte binaire cross-entropy et l'optimiseur Adam. L'entraînement est effectué sur 10 époques avec un batch size de 256.

2.b) Quantification

Nous utilisons une quantification pour nos poids ainsi que nos ReLu de 2 bits.

Il existe plusieurs types de quantification, nous utilisons ici une quantification binaire. Pour la quantification binaire, les poids prennent seulement 2 valeurs possibles: 0 et 1.

Pour la quantification, il exite plusieurs méthodes: QAT (quantization-aware training) et PTQ (post-training quantization). La première méthode consiste à quantifier durant l'entraînement,

la seconde consiste à quantifier après l'entraînement. La quantification utilisée dans notre projet est une quantification QAT.

2.c) FINN

Le framework FINN est un framework open-source développé par Xilinx pour la conception et le déploiement de réseaux de neurones quantifiés sur des FPGA. Il sert d'interface entre le ONNX et Vitis. Il nous permet donc de ne pas avoir à créer le HLS à la main et donc nous simplifie grandement la tâche.
FINN utilise dans notre cas une quantifiaction binaire pour les poids et les activations, ce qui permet de réduire considérablement la taille du modèle et d'améliorer la vitesse d'inférence sur le FPGA.
Le modèle quantifié est ensuite converti en une représentation compatible avec le matériel FPGA à l'aide de FINN, qui génère du code HDL (Hardware Description Language) pour l'implémentation sur le FPGA.
FINN offre également des outils pour l'optimisation du modèle, la génération de bitstreams pour le FPGA.

Pour l'importation dans FINN, on ajoute 7 zéros afin de passer d'un nb premier 593, à un nb facilement découpable (600): W˙new = np.pad (W˙orig, [(0,0), (0,7)]).

Pour que FINN fonctionne, il necessite une quantification binaire codée entre {-1, +1}, c'est pourquoi nous avons dû adapter notre modèle Brevitas pour qu'il corresponde à cette contrainte. Pour ce faire nous avons utilisé un wrapper Brevitas qui convertit les poids et les activations de {0, 1} à {-1, +1}.

FINN sort beaucoup de fichiers de sortie, certains peuvent être très imposant comme le bitfile, c'est pourquoi il y a des paramètres afin de gérer les fichiers de sortie:

- **ESTIMATE_REPORTS**: fourni les rapports des ressources attendues et des performances par couche et pour l'ensemble du réseau sans synthèse Vivado complète;
- **STITCHED_IP**: crée un design IP stream-in stream-out qui peut être intégré dans d'autres designs Vivado IPI ou RTL;
- **RTLSIM_PERFORMANCE**: utiliser PyVerilator pour effectuer un test de performance/latence du design STITCHED˙IP;
- **OOC_SYNTH**: exécuter une synthèse hors contexte (juste l'accélérateur lui-même, sans aucun système l'entourant) sur le design STITCHED˙IP pour obtenir les ressources FPGA post-synthèse et la fréquence d'horloge réalisable;
- **BITFILE**: intégrer l'accélérateur dans un shell pour produire un bitfile autonome;
- **PYNQ_DRIVER**: générer un pilote Python PYNQ qui peut être utilisé pour lancer l'accélérateur;
- **DEPLOYMENT_PACKAGE**: créer un dossier contenant les sorties BITFILE et PYNQ_DRIVER, prêt à être copié vers la plateforme FPGA cible.
- **OUTPUT_DIR**: indique le dossier dans lequel l'ensemble des sorties du programmes seront écrites.
- **STEPS**: indique la liste des étapes prédefinie ou personnalisée que FINN va faire pour le build de l'accélérateur.

Pour le déploiement sur la carte nous aurons besoin du BITFILE ainsi que du PYNQ_DRIVER. L'ESTIMATE_REPORTS peut être utile en amont pour savoir les ressources et les performances de notre accélérateur.

3. Comparaison des performances

Nous allons faire varier la quantification des poids et des activations de 2 bits à 16 bits et comparer les performances du modèle sur le dataset UNSW-NB15.
Nous allons mesurer la précision (accuracy) ainsi que le temps d'inférence sur CPU.
Voici les résultats obtenus:

Modèle	MLP	MLP	MLP	MLP	MLP
Nb quantification	2	4	8	16	32
Accuracy (%)	73.5	79.2	81.3	82.1	82.3
Avg Loss	0.6012	0.5123	0.4789	0.4567	0.4501
Temps CPU (s)	12.34	13.45	14.56	15.67	16.78
Temps Inférence (s)	0.001234	0.001345	0.001456	0.001567	0.001678
Temps inférence (ms)	1.234	1.345	1.456	1.567	1.678
Nb Inférences/s	810	743	686	638	596

Comme nous pouvons le voir, la quantification a un impact significatif sur les performances du modèle. En effet, plus la quantification est faible, plus la précision diminue. Cependant, le temps d'inférence diminue également, ce qui peut être bénéfique pour les applications en temps réel. Nous remarquons aussi que la diminution de la précision n'est pas linéaire par rapport à la taille de la quantification. En effet, dès que la quantification est de 4 bits, nous observons une accuracy qui est très semblable.
Il est donc important de trouver un compromis entre la taille de la quantification et les performances du modèle en fonction des besoins de l'application.

4. Estimations implémentations FINN

Les max FPS visés sont de 1 000 000 (1 MOps). La période est de 10ns soit une fréquence de 100 000 000 Hz, soit 100MHz.
En baissant TARGET˙FPS, nous pouvons réduire la configuration matérielle nécessaire.
Coté ressource, le programme estime les utilisations suivantes:

- LUT: 9354
- BRAM_18K: 45

Les performances estimées sont de 1 562 500,0 FPS.

L'architecture comporte les élements suivants:

- "PE": 16 + 1 + 1 +1 = 19
- "SIMD": 40 + 64 + 64 + 1 = 169

B. Partie Stitched IP et PYNQ bitfile and Driver

Estimation par FINN:

- LUT: 17640 + 1096 + 1042 + 268 = 20046

- BRAM_18K = 0
- FF: 2037 + 801 + 803 + 68 = 3909
- DSP = 32 + 32 + 1 = 65

Les performances estimées par FINN sont de 448430.49327354255 FPS.

Les FIFOS permettent de passer les informations d'une couche à une autre ainsi que de synchroniser l'ensemble. Ici elles sont de 32 à 2 entre la couche d'entrée et le couche 1 puis de 2 à 2 entre les autres couches. Cela veut donc dire que les couches ont besoin d'un certain nombre d'entrées pour pouvoir fonctionner (ici 2).

5. Synthèse Vivado

Nous pouvons maintenant regarder les ressources utilisées après synthèse Vivado. Pour les lire, nous nous sommes rendus dans le rapport post synthèse Vivado qui est parmi les rapports dans le final output du programme 3. Nous obtenons les résultats suivants:

- LUT: 12711
- BRAM_18K: 2
- FF: 15854
- BRAM_36K: 22
- DSP: 129
- SRL: 381

Pour ouvrir Vivado, nous devons definir l'environnement avec la commande suivante en étant à la racine:

```
source /etc/Xilinx/Vivado/2020.2/settings64.sh
```

Puis nous ouvrons Vivado en étant dans le dossier /tmp et dans le sous dossier créé par le programme 3 avec la commande:

```
vivado finn_zynq_link.xpr
```

Les valeurs indiqués dans le rapport post-synthèse sont également retrouvable au sein de Vivado dans les ressources implémentées:

Resource	Utilization	Available	Utilization %
LUT	12711	53200	23.89
LUTRAM	1013	17400	5.82
FF	15854	106400	14.90
BRAM	23	140	16.43
DSP	129	220	58.64
BUFG	1	32	3.13

Figure 1. Tableau de l'utilisation des ressources

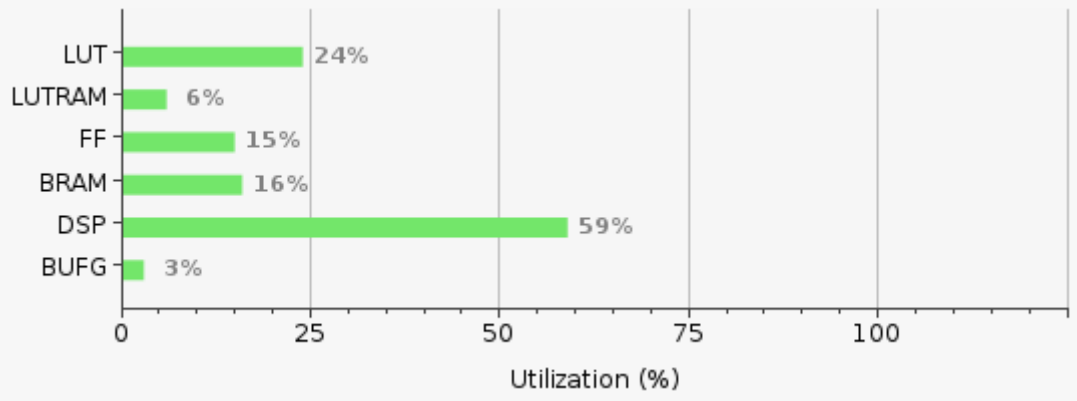

Figure 2. Graphique de l'utilisation des ressources

Comme nous pouvons le voir, l'utilisation des ressources est très faible par rapport aux ressources disponibles sur la carte FPGA. On voit que les ressources utilisées sont largement inférieures aux ressources estimées par FINN. Cela peut être dû à plusieurs facteurs, notamment les optimisations effectuées par le synthétiseur Vivado qui peuvent réduire l'utilisation des ressources par rapport aux estimations initiales de FINN.

La répartition des ressources utilisées est la suivante:

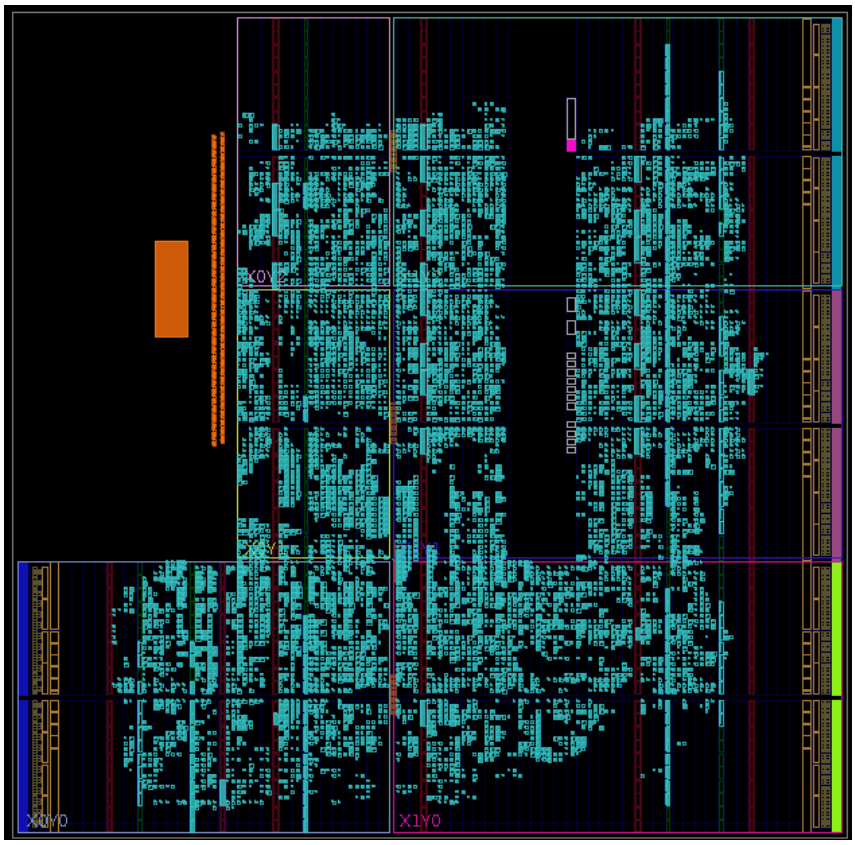

Figure 3. Image de la répartition des ressources utilisées

Nous pouvons croire que la majorité des ressources sont utilisées mais en réalité, nous voyons bien dans la table ainsi que dans le graphique que l'utilisation des ressources est très faible par rapport aux ressources disponibles sur la carte FPGA. La présence de bleu de partout dans l'image explique juste un grand étalement des ressources utilisées sur la carte.

6. Carte

Ici je dois mettre ce que le prof envoi en sceenshot et aussi faire un équivalent entre FPGA et CPU/GPU.

II. Modification MLP pour MNIST

1. MNIST dans FINN

Le dataset MNIST est un ensemble de données utilisé pour la reconnaissance de chiffres manuscrits. Il contient 60,000 images d'entraînement et 10,000 images de test, chaque image étant une image en niveaux de gris de 28×28 pixels représentant un chiffre de 0 à 9.
Afin de nous servir de MNIST, nous allons utiliser à nouveau le framework FINN.

2. Impact de la quantification

Ici je dois mettre les résultats d'impact de la quantification sur MNIST / CIFFAR10. Afin de réaliser la quantification, nous allons utiliser Brevitas qui est une bibliothèque de quantification pour PyTorch. Pour ce faire, nous avons utilisé des couches de Brevitas pour remplacer les couches standards de PyTorch. Cela s'effectue comme suit:

```
import brevitas.nn as qnn
qnn.QuantConv2d(3, 6, kernel_size=5, bias=True, padding = 2, weight_bit_width=16)
```

Nous voyons dans cette ligne la définition d'une couche de convolution quantifiée avec des poids sur 16 bits (weight_bit_width=16). Le reste ne change pas par rapport à une couche de convolution standard de PyTorch.

Pour réaliser l'impact de la quantification, nous avons entraîné plusieurs modèles avec des poids et des activations de différentes tailles (2, 4, 8, 16 bits) et nous avons comparé les performances de ces modèles sur le dataset CIFFAR10. Nous avons également comparé ces modèles avec un modèle non quantifié (poids et activations en 32 bits flottants).
Pour les modèles utilisés nous avons utilisé un modèle simple de CNN avec 2 couches de convolution suivies de 2 couches fully connected type LeNet-5.
Nous avons également utilisé un modèle de MLP avec 3 couches soit 1 couche d'entrée (100 neurones), une couche cachée (50 neurones), et une couche de sortie (10 neurones).
Les métriques pour la mesure seront la précision (accuracy) ainsi que le temps d'inférence.

Modèle	CNN	CNN	CNN	CNN	CNN	CNN
Nb quantification	1	2	4	8	16	32
Accuracy (%)	10	56.2	61.2	63.6	64.9	64.4
Avg Loss	NaN	1.257583	1.112131	1.048991	1.024594	1.026724
Temps CPU (s)	4.574	3.6179	4.1767	5.34	4.0933	6.4669
Temps Inférence (s)	0.0004574	0.00036179	0.00041767	0.000534	0.00040933	0.00064669
Temps inférence (ms)	0.4574	0.36179	0.41767	0.534	0.40933	0.64669
Nb Inférences/s	2186	2765	2394	1872	2443	1545

3. Performances estimées

Ici je dois mettre les résultats d'estimations FINN, avec les ressources utilisées, la fréquence max, etc. Ainsi que la synthèse Vivado avec les ressources utilisées, la fréquence max, etc.

III. Bibliographie

Liens vers les références utilisées pour la réalisation du rapport:

https://www.kaggle.com/code/mrwellsdavid/unsw-nb15-dataset-mlp-classifier/notebook
https://xilinx.github.io/brevitas/v0.12.1/tutorials/tvmcon2021.html
https://github.com/Xilinx/brevitas?tab=readme-ov-file
https://arxiv.org/pdf/2103.13630