Projet de bachelor

Bruteforce Password Attack on FPGAs

Kandiah Abivarman

03.09.2024

h e p i a
Haute école du paysage, d'ingénierie
et d'architecture de Genève

Table des matières :

Introduction

Introduction - Elca Security

Introduction - Durée du travail

10.2023 — 03.2024

Projet de semestre :

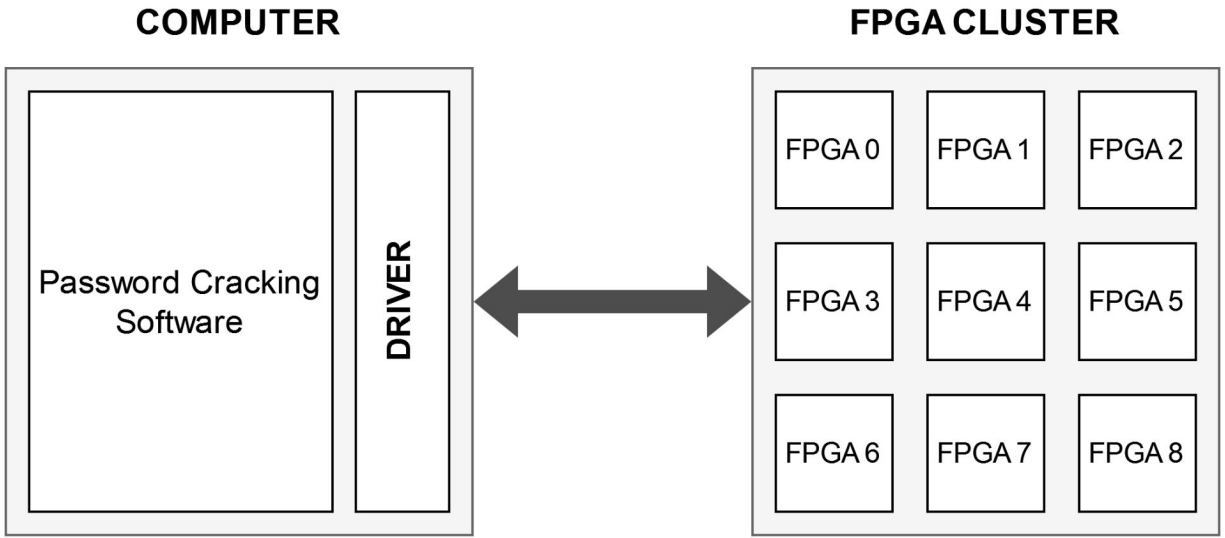
- En parallèle des cours
- 8 h par semaine

05.2024 — 08.2024

Projet de Bachelor

- Temps plein
- 450 h de travail

Introduction - Schéma

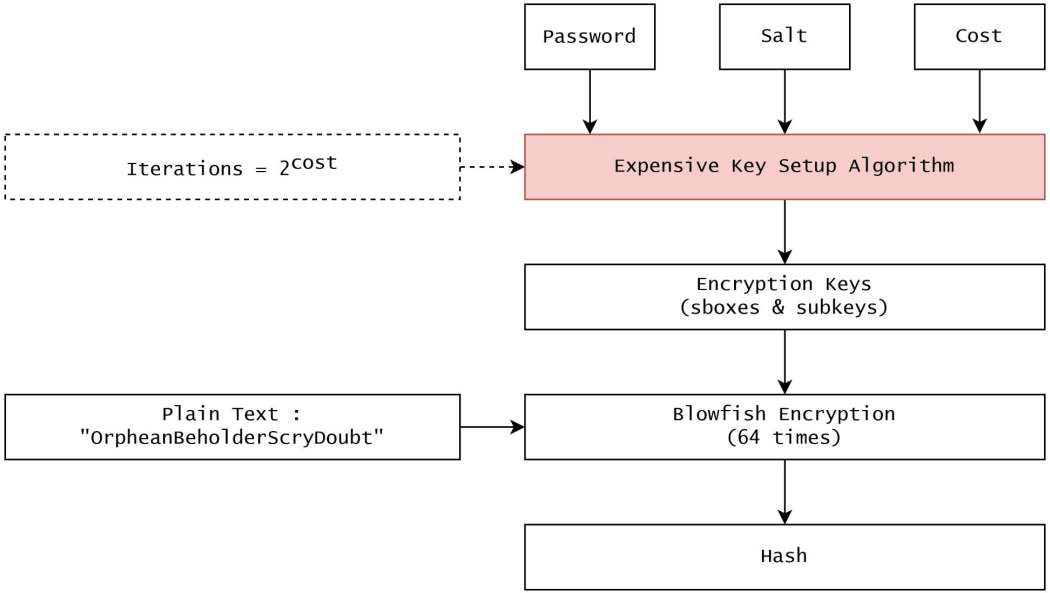


Introduction - FPGA vs CPU vs GPU

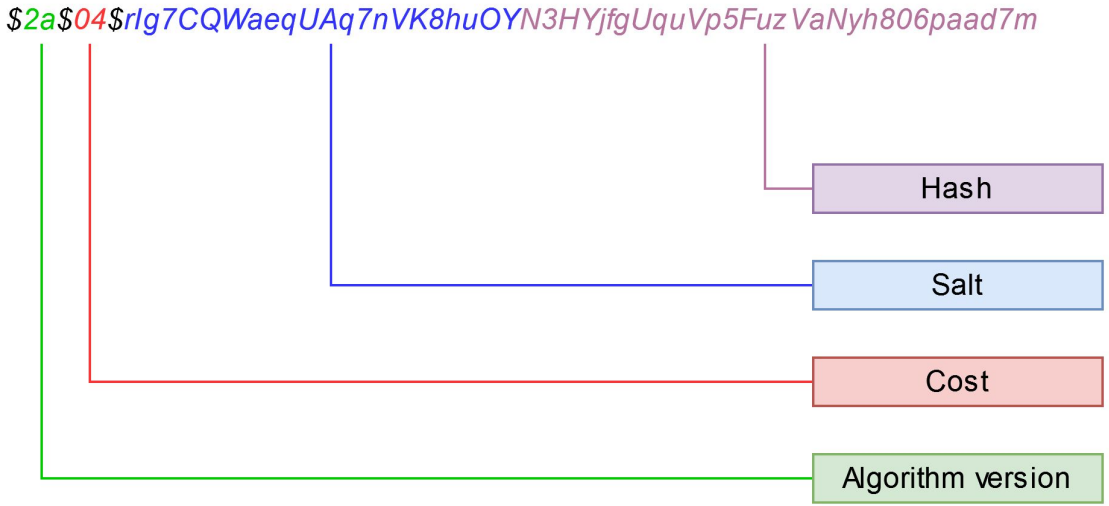
- Consommation
- Hashrate
- Coût

Bcrypt - Algorithme de hash

Bcrypt

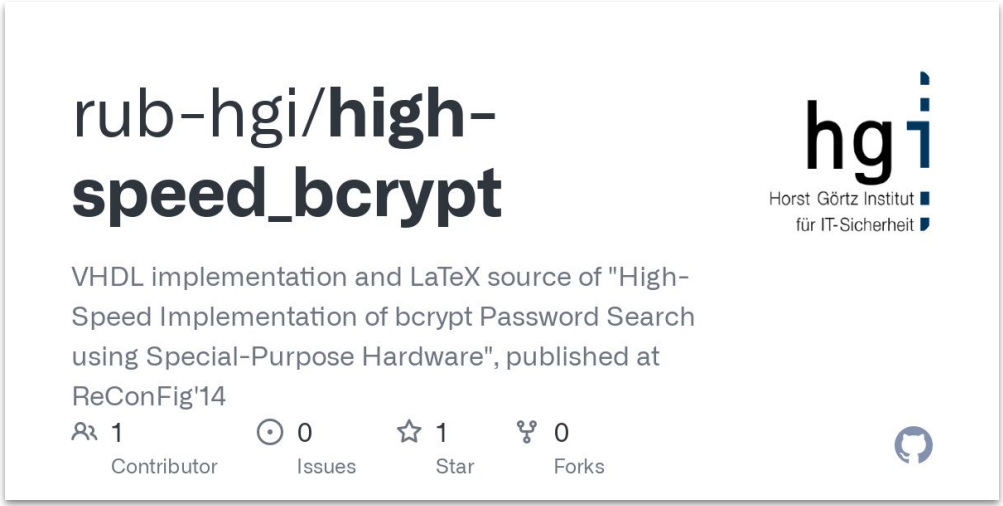

Password
Salt
Cost
Iterations = 2^cost
Expensive Key Setup Algorithm
Encryption Keys
(sboxes & subkeys)
Plain Text :
"OrpheanBeholderScryDoubt"
Blowfish Encryption
(64 times)
Hash

Bcrypt - Format du hash



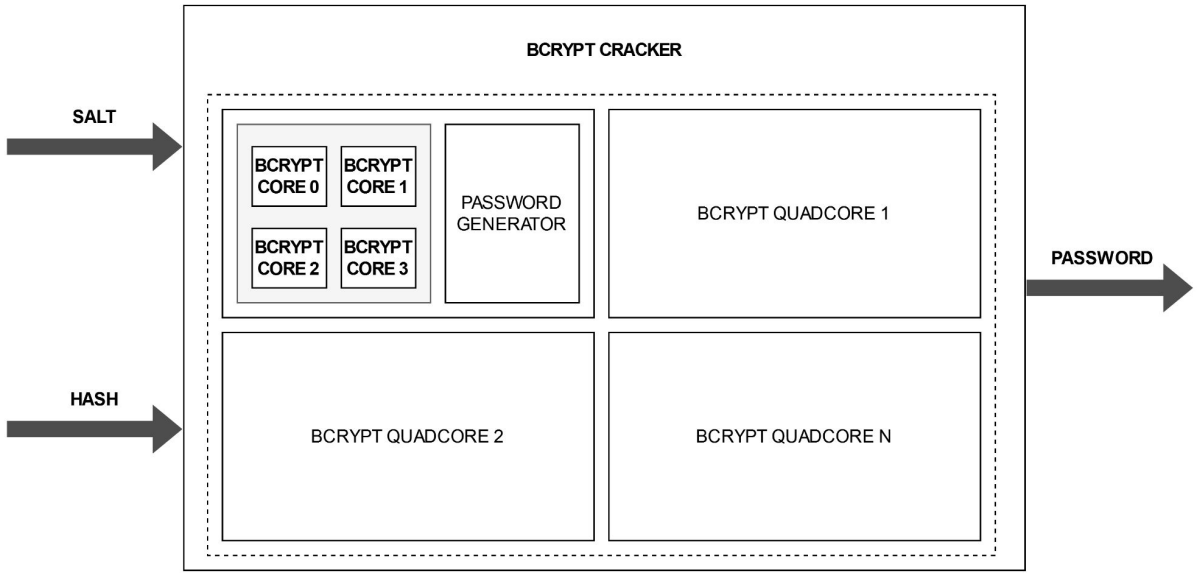
Réalisations - Travail de semestre

Implémentation existante

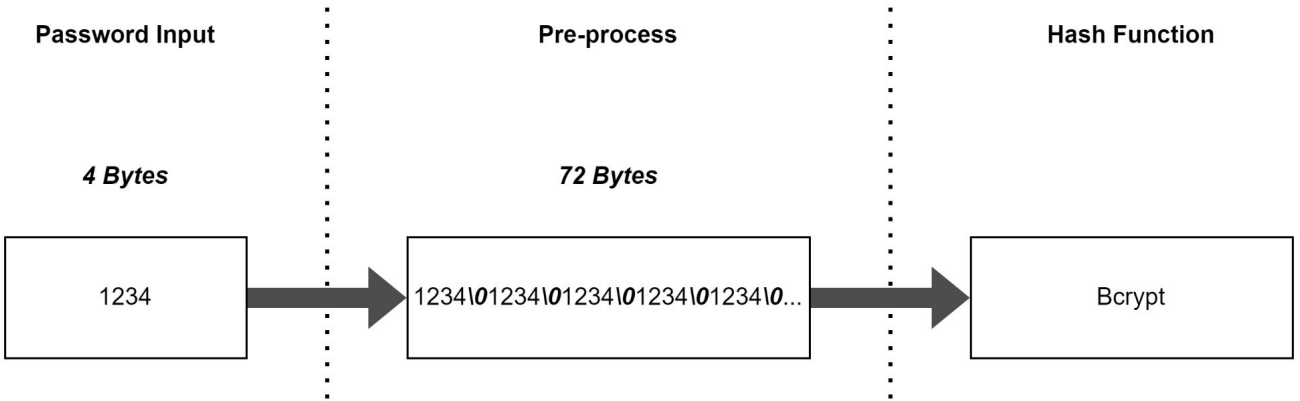


https://github.com/rub-hgi/high-speed_bcrypt

Implémentation existante - Schéma

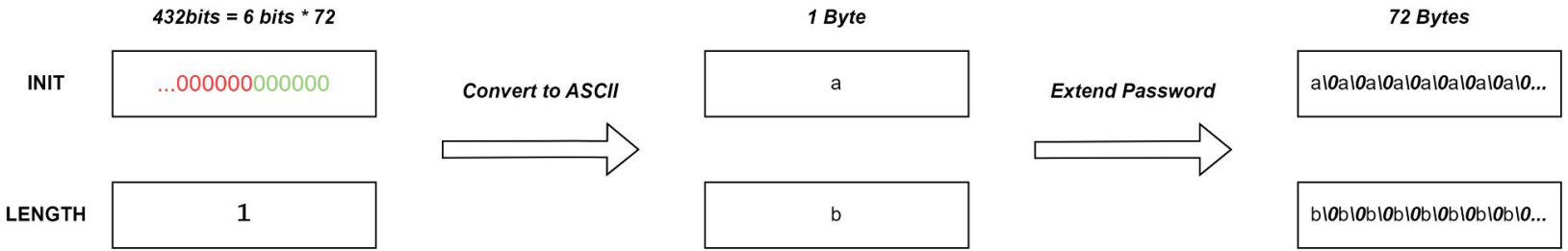


Bcrypt - Password Hashing

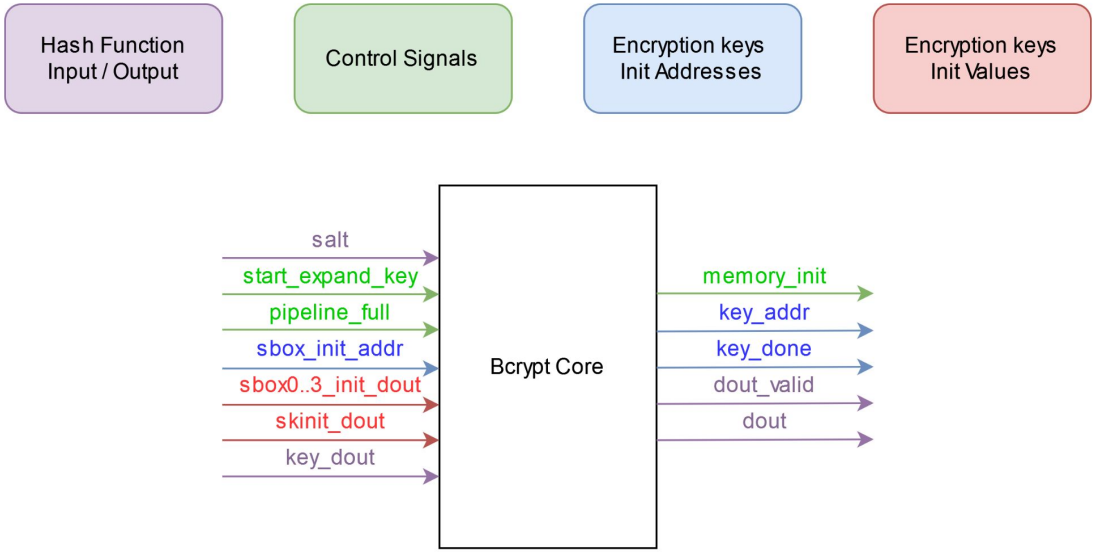


Password Generator

Conversion Table				
0x00	0x01	0x02	0x1b	0x35
NULL '\0'	'a'	'b'	'A'	'0'



Bcrypt Core Interface

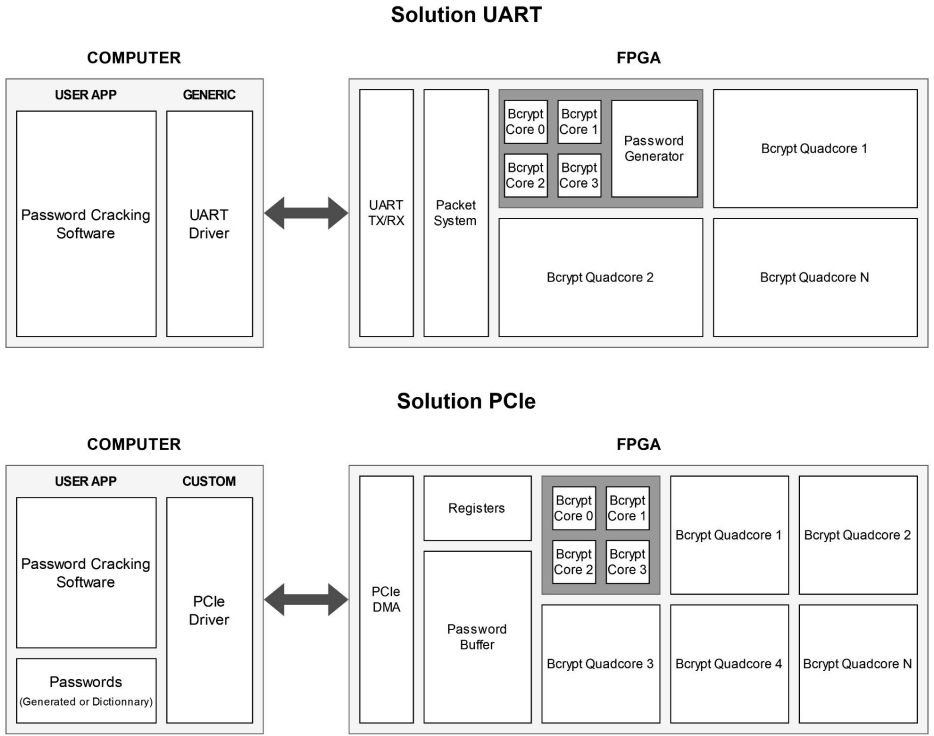


Implémentation existante - Problèmes

- Documentations
- Versions - Incohérences
- Testbenches incomplets
- Petites erreurs

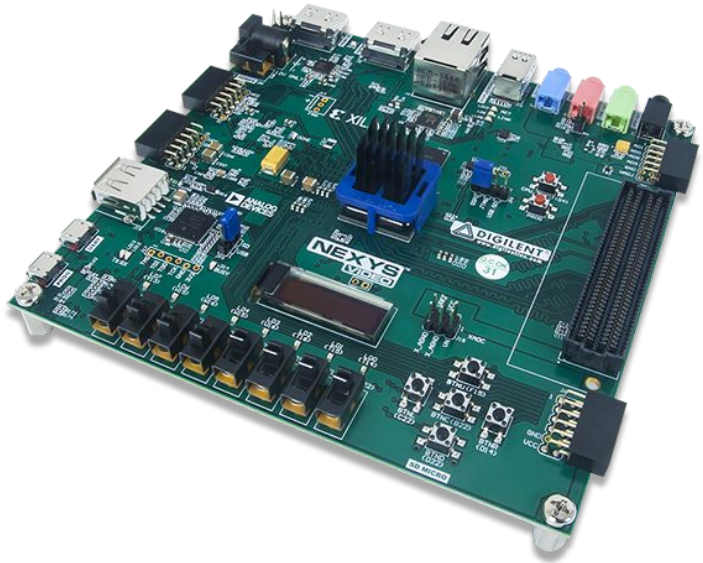
Réalisations - Travail de bachelor

Solutions - Schéma



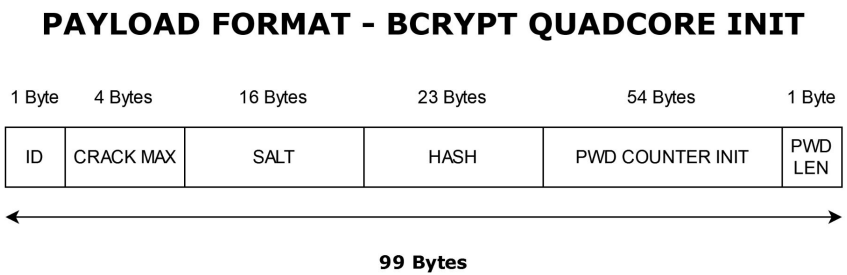
Solution UART

CARTE FPGA - Nexys Video
Artix 7



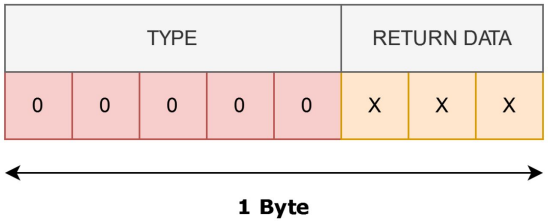
Solution UART - Initialisation des Quadcores

- Le nombre d’essais
- Le HASH et le SALT
- Initialisation du générateur de mots de passe



Solution UART - Réponse du système

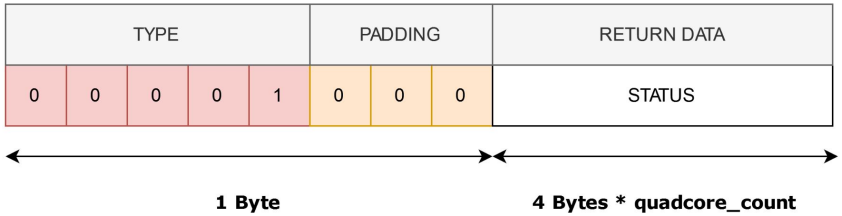
PAYLOAD FORMAT - RETURN



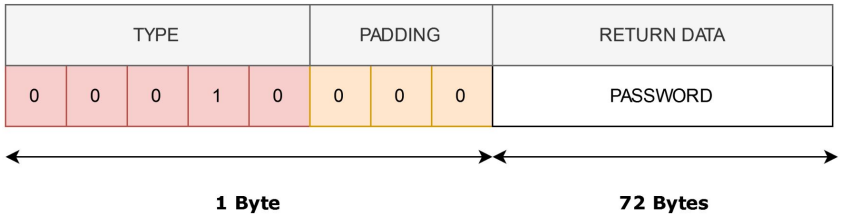
Return Code	Return
000	OK
001	Packet size greater than expected
010	Packet size smaller than expected
011	Quadcore ID not valid
100	CRC Error

Solution UART - Retour du système

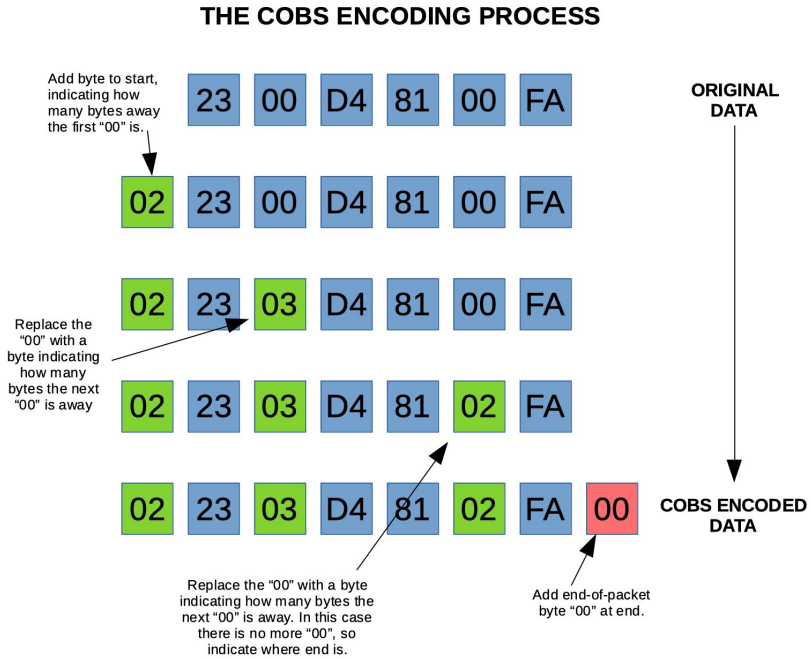
PAYLOAD FORMAT - STATUS REPORT



PAYLOAD FORMAT - PASSWORD FOUND



Solution UART - Encodage COBS

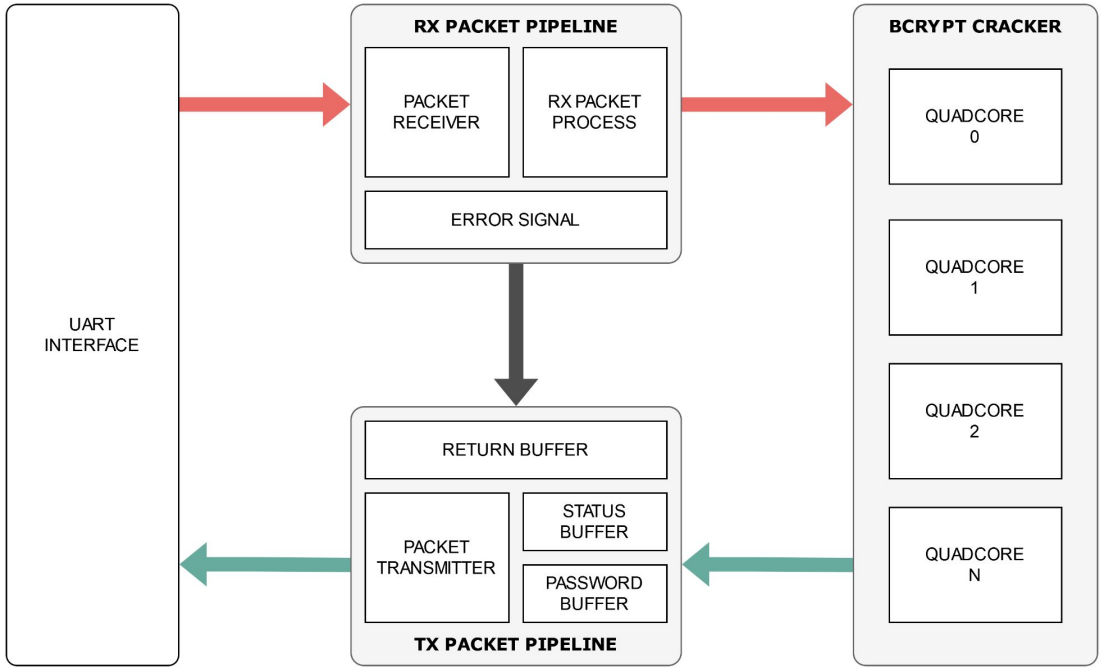


PACKET FORMAT

1 Byte	1 Byte	Variable	1 Byte	1 Byte
COBS HEAD	PAYLOAD LENGTH	PAYLOAD	CRC	COBS END

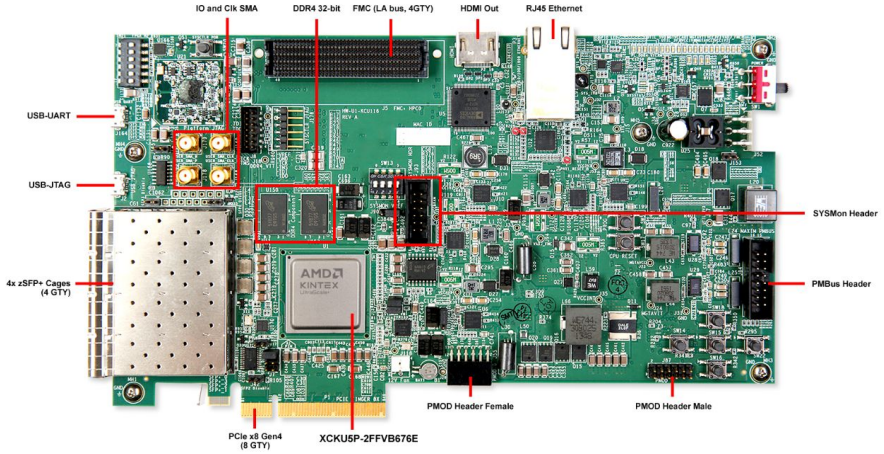
https://blog.mbedded.ninja/programming/serialization-formats/consistent-overhead-byte-stuffing-cobs/

Solution UART - Schéma

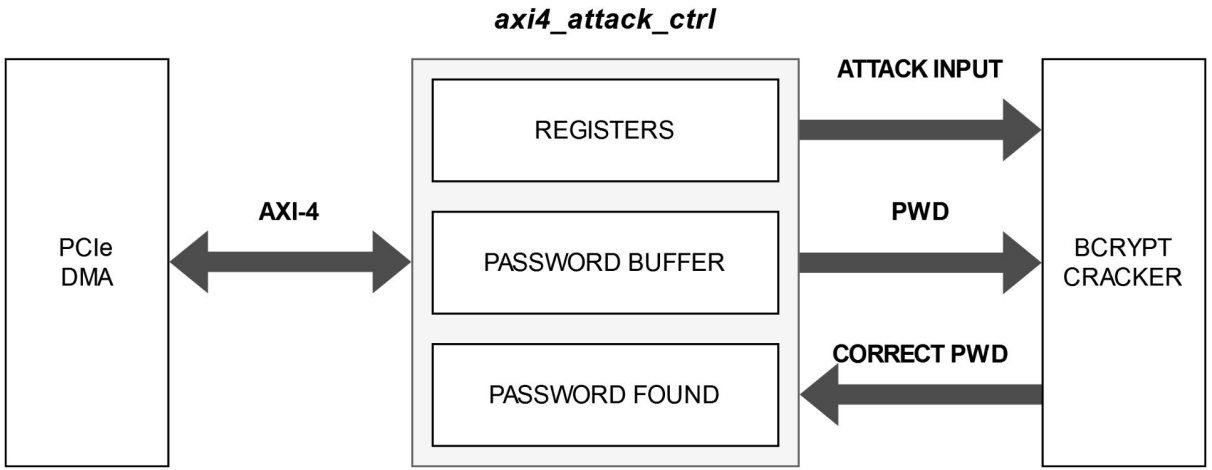


Solution PCIe

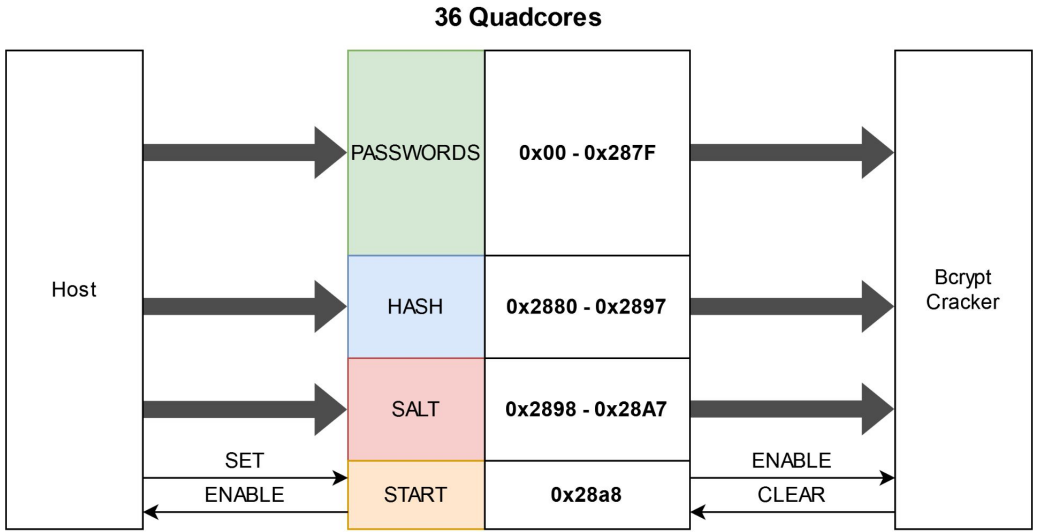
CARTE FPGA - KCU 116
Kintex Ultrascale +



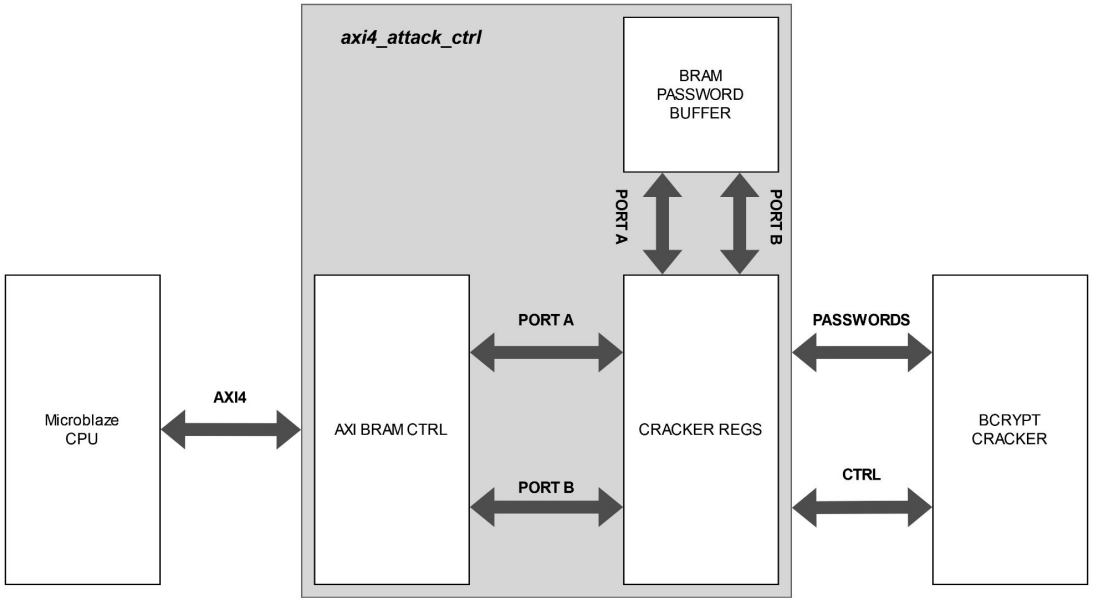
Solution PCIe - Schéma Général



Solution PCIe - Accès Mémoire



Solution PCIe - Schéma de Test



Résultats

Résultats - Hashrate

Carte FPGA	Freq (MHz)	Quadcores Max.	Utilisations (%)	Hashrate (cost : 5)
Nexys Video	100	22	BRAM : 78.36, LUT : 75	13’554 H/s
KCU 116	100	36	BRAM : 97.50, LUT : 68	22’180 H/s
	200	36	BRAM : 97.50, LUT : 68	44’369 H/s
	250	36	BRAM : 97.50, LUT : 68	55’450 H/s
	275	< 30	-	< 50’820 H/s

Résultats - Comparaisons

Architecture	Puissance (W)	Hashrate (cost : 5)	Efficacité Énergétique	
FPGA (Nexys Video, 22 Quadcores, 100 MHz)	**4.38**	13’554 H/s	3’094 H/J	11.140 MHash/Wh
FPGA (KCU116, 36 Quadcores, 250 MHz)	11.7	**55’450 H/s**	**4’739 H/J**	**17.06 MHash/Wh**
CPU (AMD Ryzen 7 4800U, 16 threads)	~25	**8’200 H/s**	328 H/J	1.18 MHash/Wh
GPU (NVIDIA GTX 1660 Super)	**125**	19’201 H/s	**154 H/J**	**552.98 kHash/Wh**

Conclusion :

- Optimisation de l’implémentation Bcrypt
- Finir implémentation solution PCIe
- Mettre en place un driver linux pour PCIe

Démo