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

Introduction

Introduction - Elca Security

Introduction - Durée du travail

10.2023 — 03.2024

Projet de semestre :

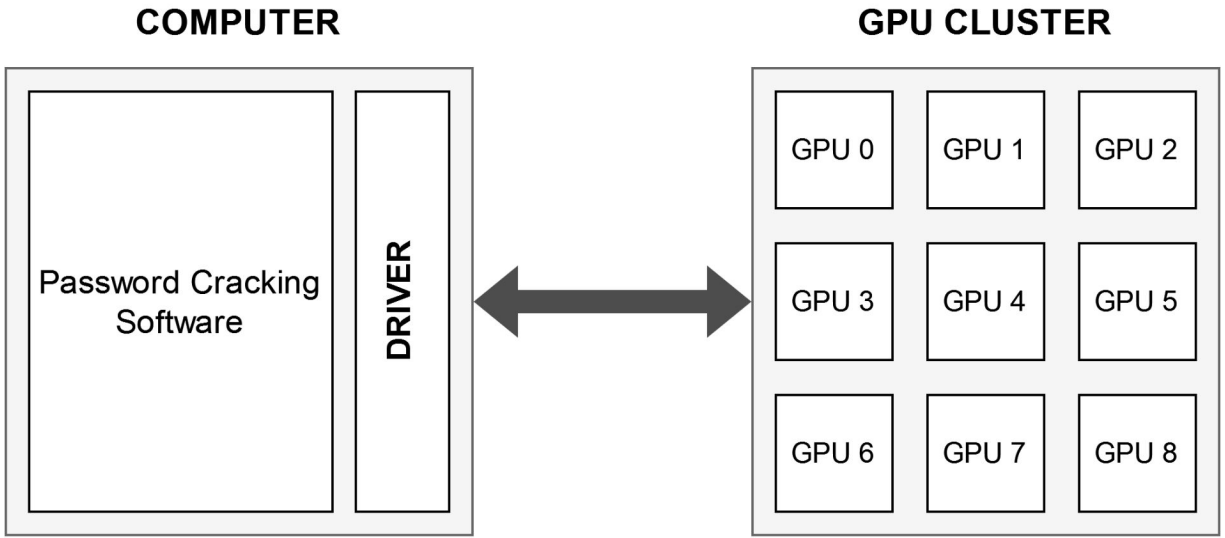
- En parallèle des cours
- 8 h par semaine

05.2024 — 08.2024

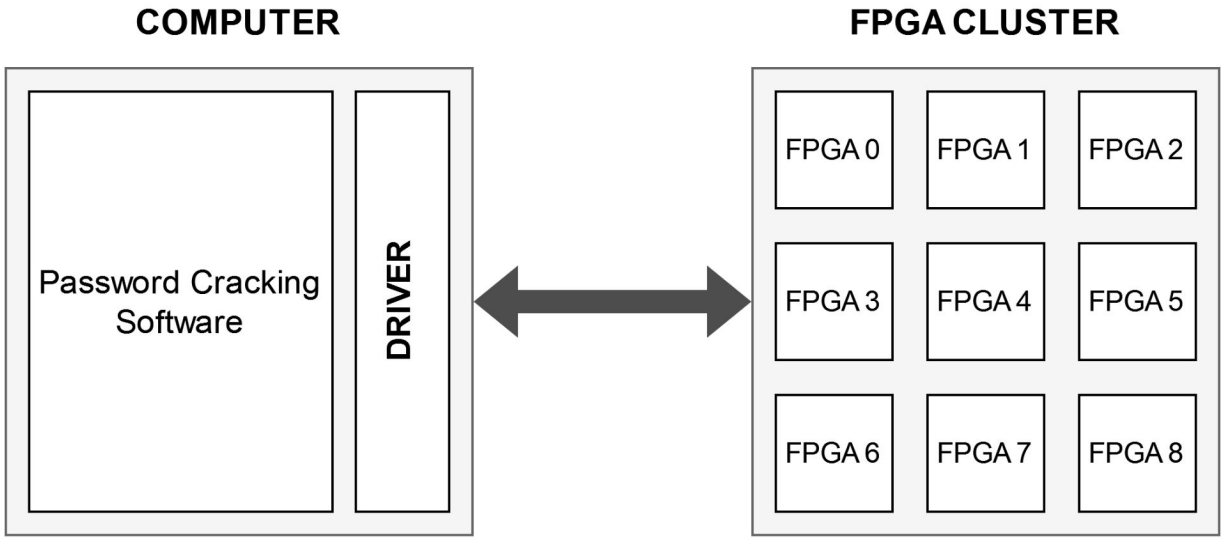
Projet de Bachelor

- Temps plein
- 450 h de travail

Introduction - Solution GPU



Introduction - Solution FPGA



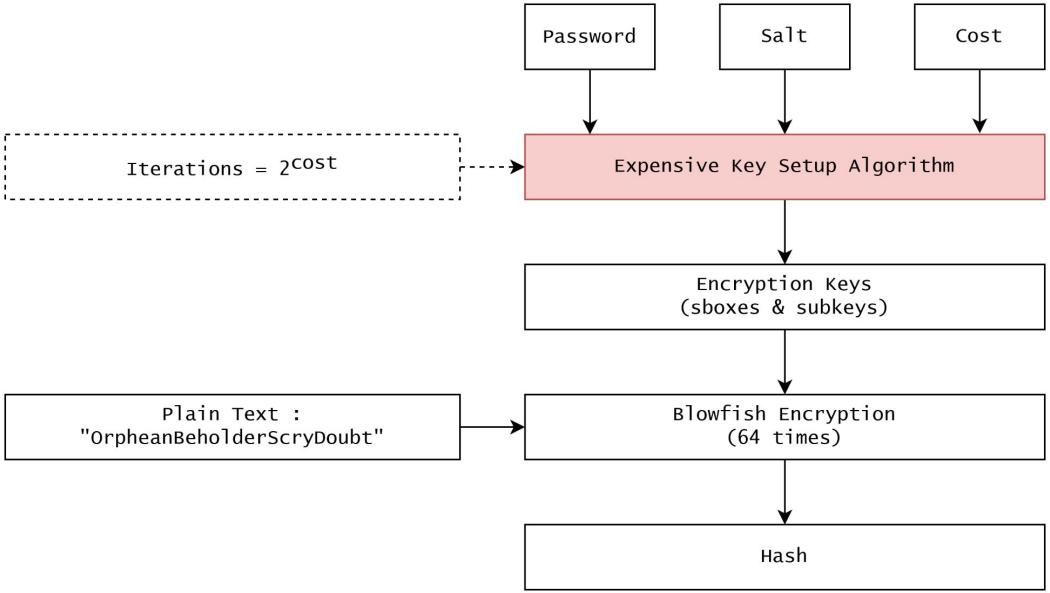
Introduction - FPGA vs CPU vs GPU

Mesures et Comparaisons :

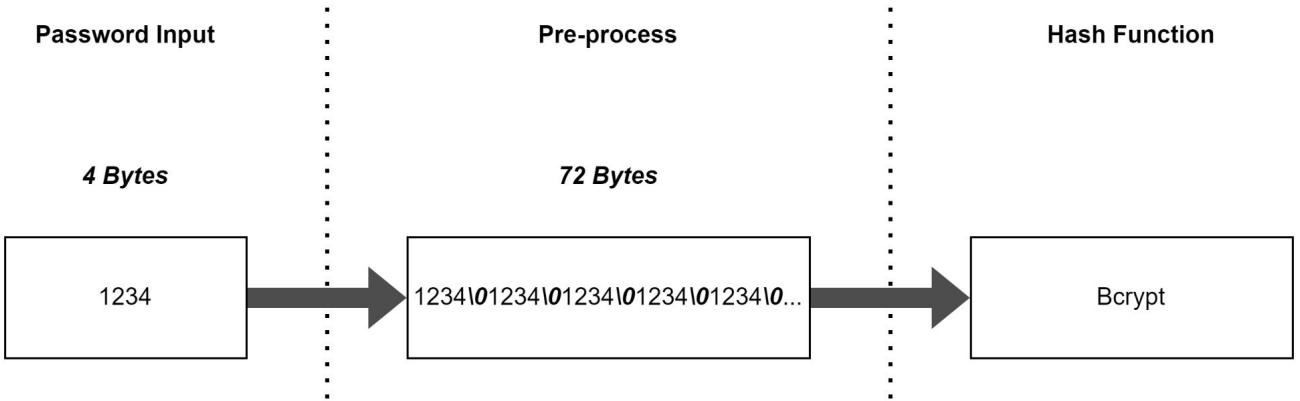
- Consommation
- Hashrate
- Coût

Bcrypt - Algorithme de hash

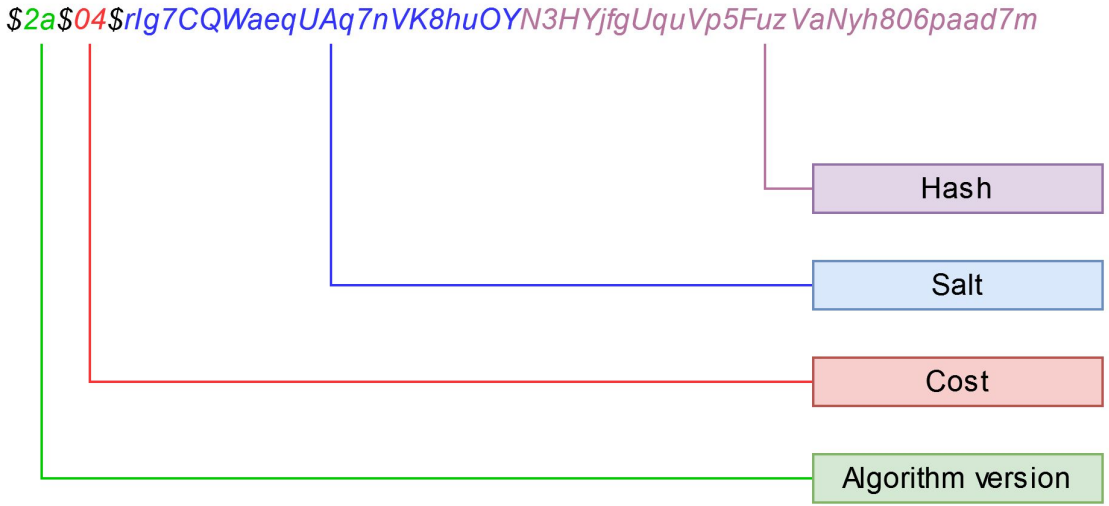
Bcrypt - Algorithme



Bcrypt - Password Hashing

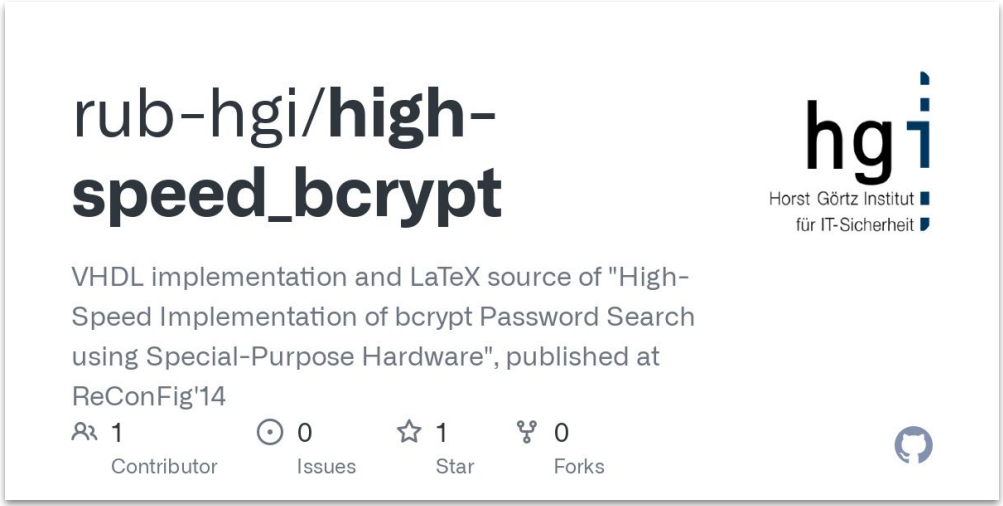


Bcrypt - Format du hash



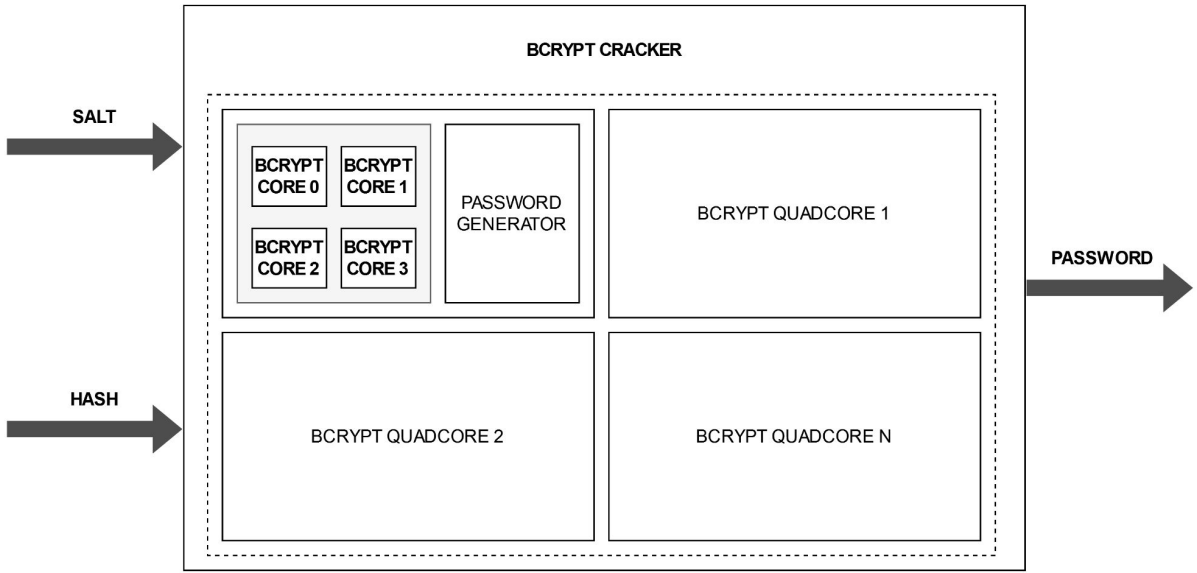
Réalisations - Travail de semestre

Implémentation existante



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

Implémentation existante - Schéma



Implémentation existante - Problèmes

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

Réalisations - Travail de bachelor

Solutions

Solution Low-cost :

- FPGA Peu coûteux
- Interface UART
- Génération de mots de passe dans FPGA

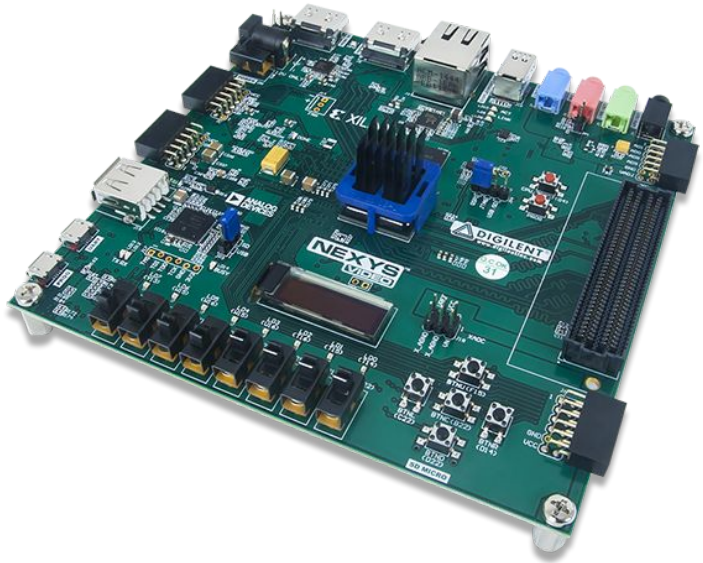
Solution High-cost :

- FPGA coûteux
- Interface PCIe
- Génération de mots de passe sur PC

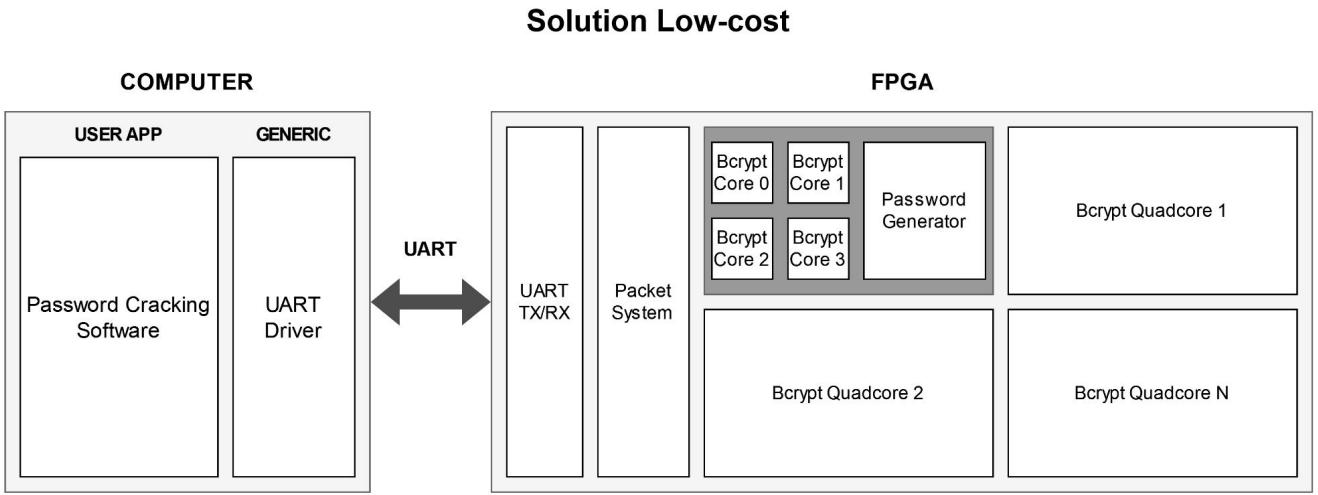
Solution Low-cost

Nexys Video :

- FPGA : *Artix 7 - XC7A200T*
  - LUT : *134’600*
  - BRAM : *365*
  - *Prix : 300.-*
- Prix : *550.-*

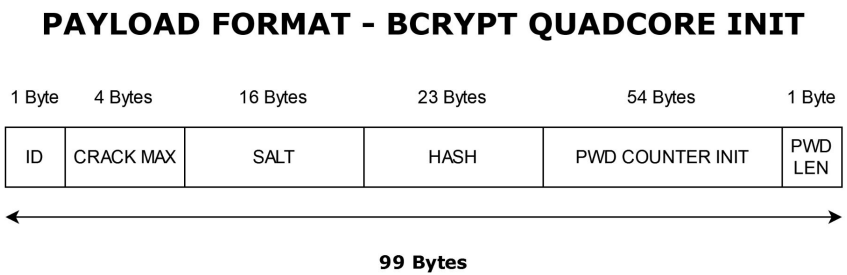


Solution Low cost - Schéma



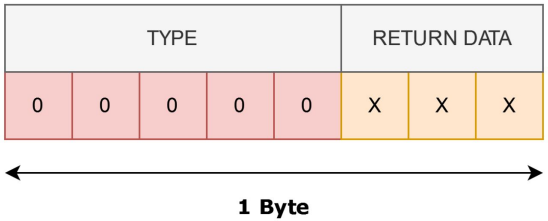
Solution Low cost - Initialisation des Quadcores

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



Solution Low cost - Réponse du système

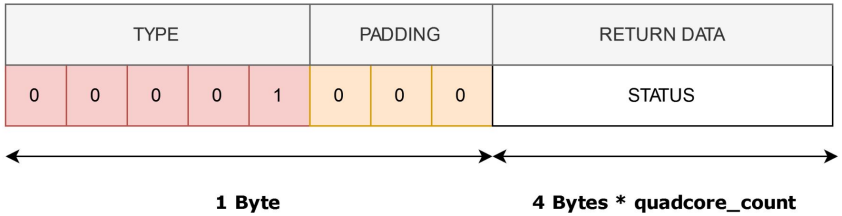
PAYLOAD FORMAT - RETURN



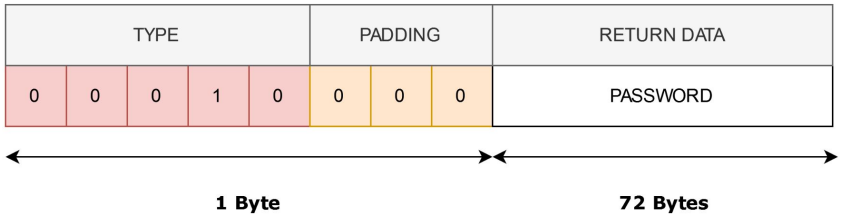
Return Code	Return
000	OK
001	Packet size greater than expected
010	Packet size smaller than expected
011	Quadcore ID not valid
100	CRC Error

Solution Low cost - Retour du système

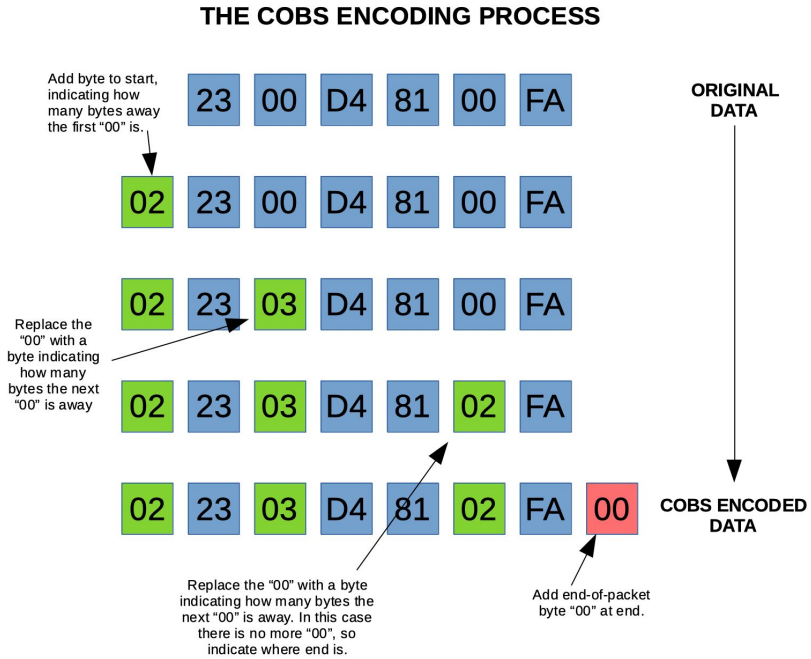
PAYLOAD FORMAT - STATUS REPORT



PAYLOAD FORMAT - PASSWORD FOUND



Solution Low cost - Encodage COBS

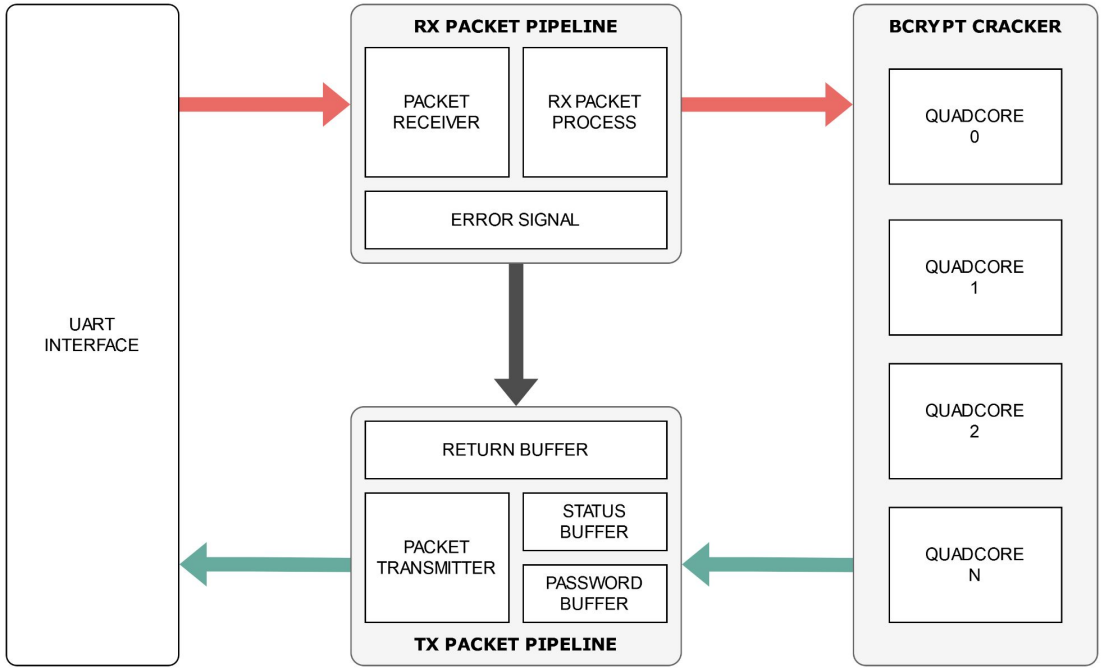


PACKET FORMAT

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/

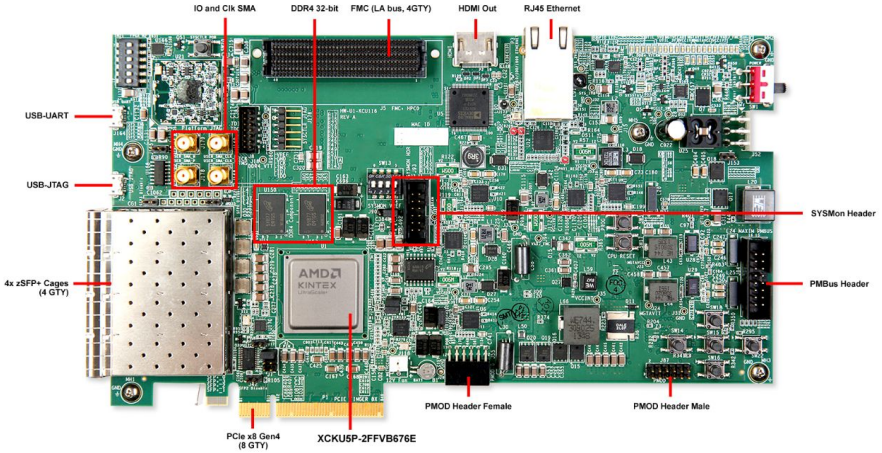
Solution Low cost - Schéma FPGA



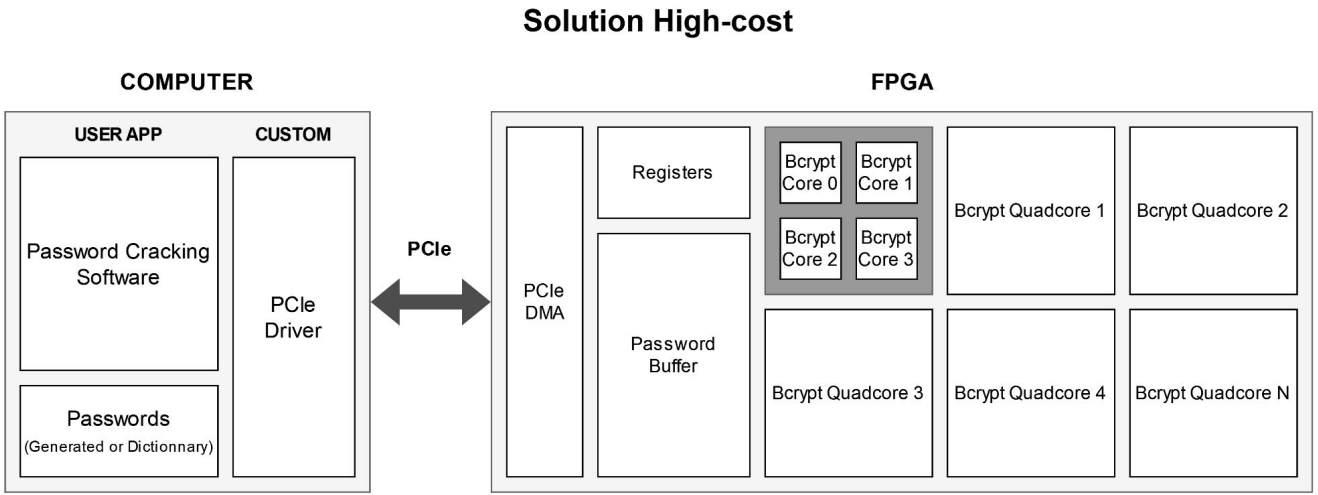
Solution High-cost

KCU 116 :

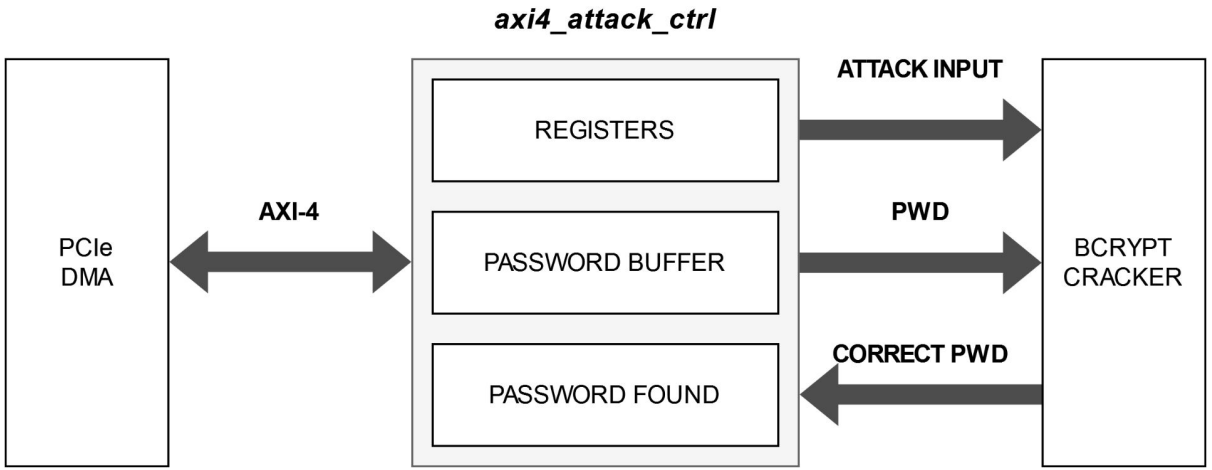
- FPGA : *Kintex UltraScale+ XCKU5P*
  - LUT : *474,600*
  - BRAM : *480*
  - *Prix : 2800.-*
- Prix : *3900.-*



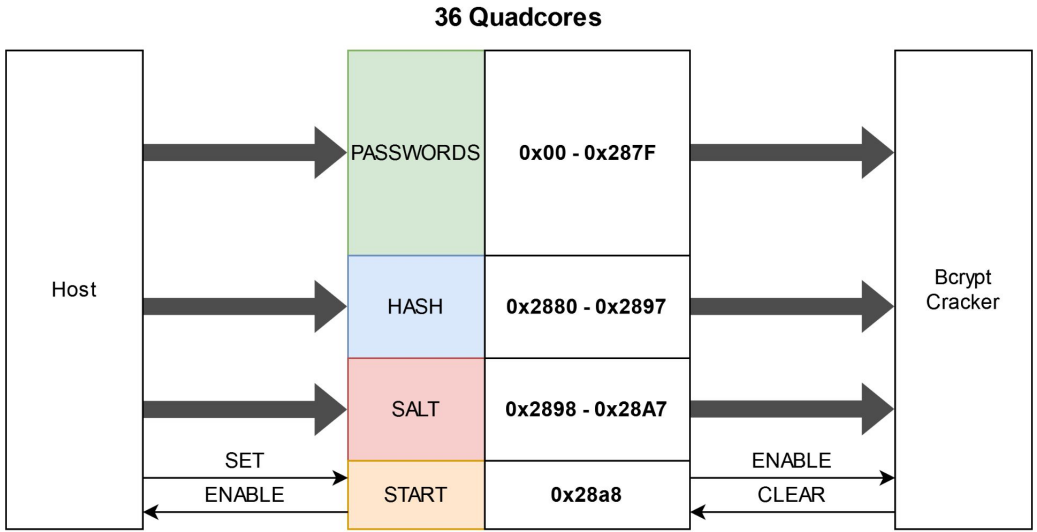
Solution High cost - Schéma



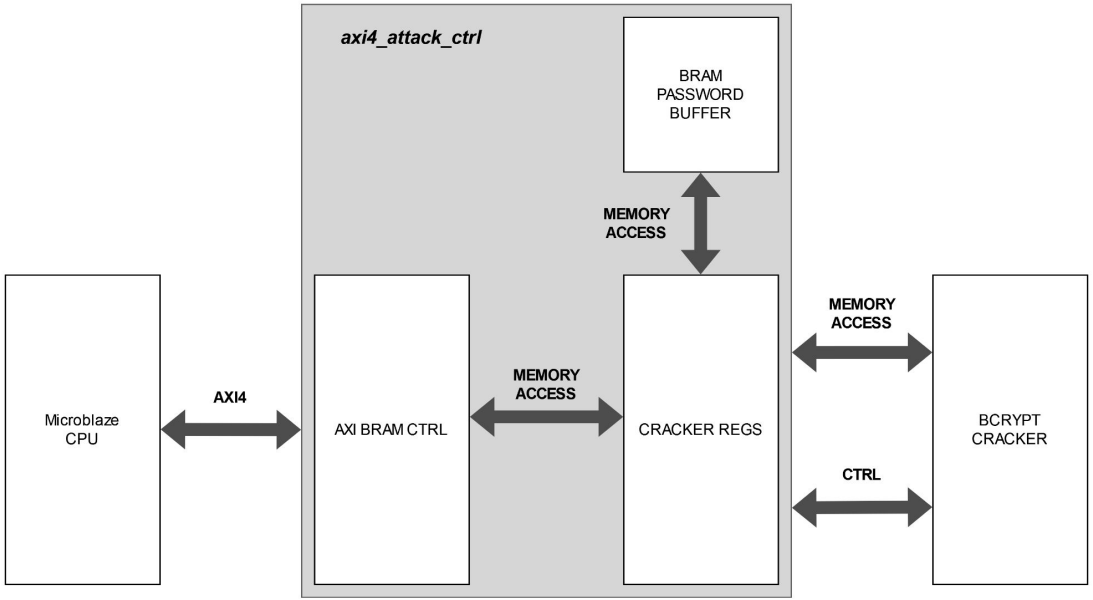
Solution High cost - Schéma FPGA



Solution High cost - Accès Mémoire



Solution High cost - 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	Prix	Puissance (W)	Hashrate (cost : 5)	Efficacité Énergétique	
FPGA (Artix 7, 22 Quadcores, 100 MHz)	~300 CHF	**4.38**	13’554 Hash/s	3’094 Hash/J	11.140 MHash/Wh
FPGA (Kintex Ultrascale+, 36 Quadcores, 250 MHz)	~2800 CHF	11.7	**55’450 Hash/s**	**4’739 Hash/J**	**17.06 MHash/Wh**
CPU (AMD Ryzen 7 4800U, 16 threads)	~100-200 CHF	~25	**8’200 Hash/s**	328 Hash/J	1.18 MHash/Wh
GPU (NVIDIA GTX 1660 Super)	~300 CHF	**125**	19’201 Hash/s	**154 Hash/J**	**0.552 MHash/Wh**

Conclusion :

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

Démo