Projet de semestre

...

FPGA Bruteforce Attack

Kandiah Abivarman

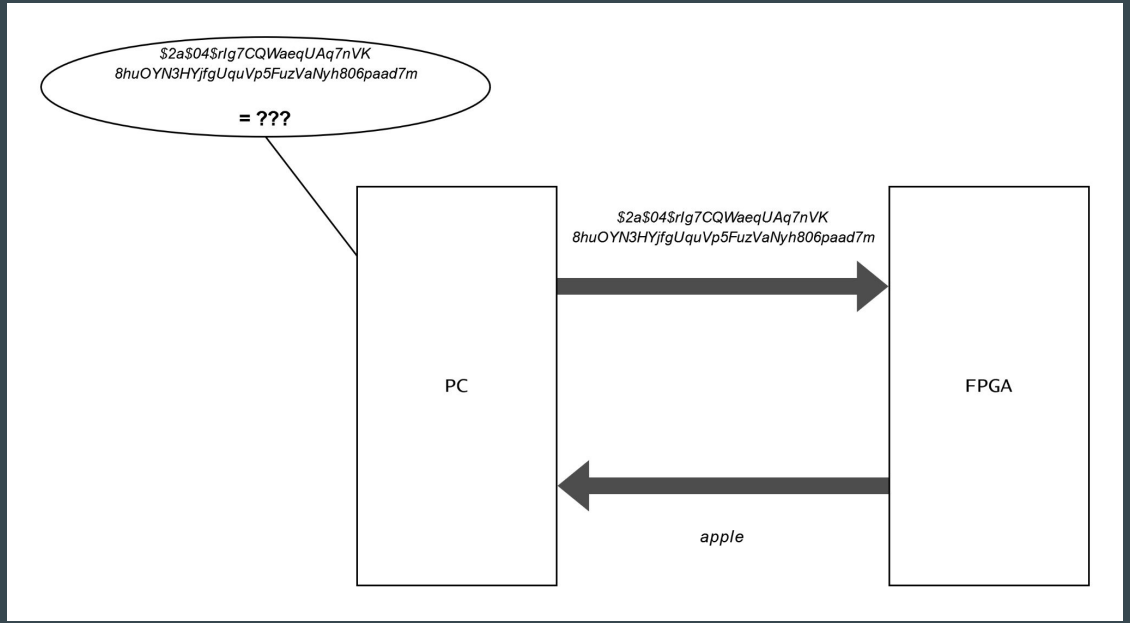
17.02.2024

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

Table des matières :

Objectif

Objectif - Schéma

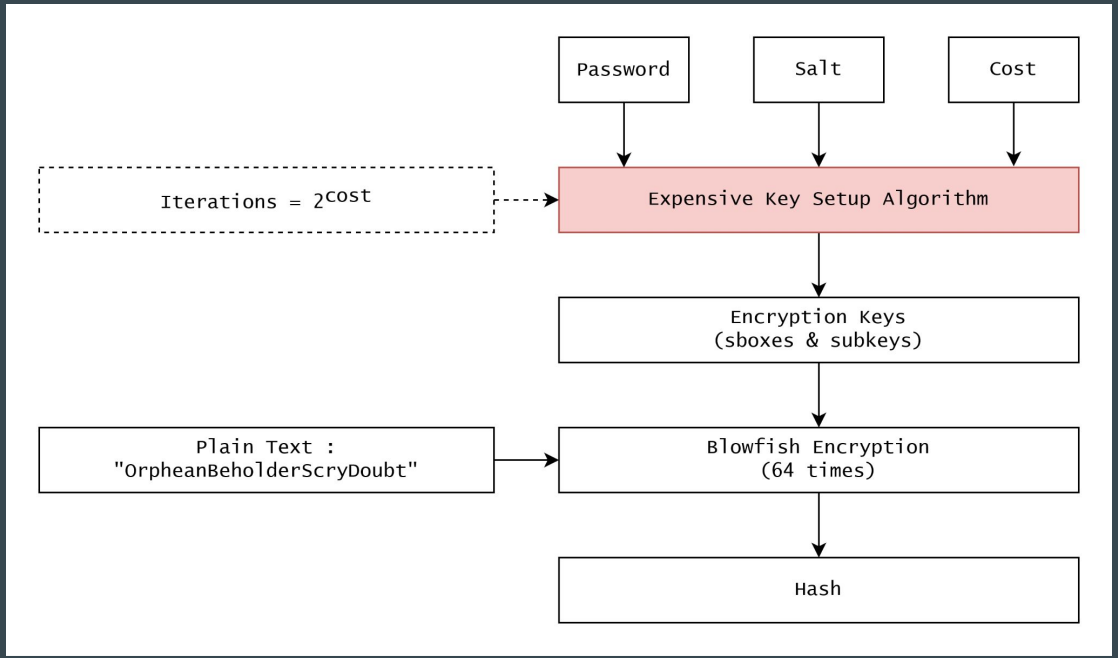


Objectif - FPGA vs CPU vs GPU

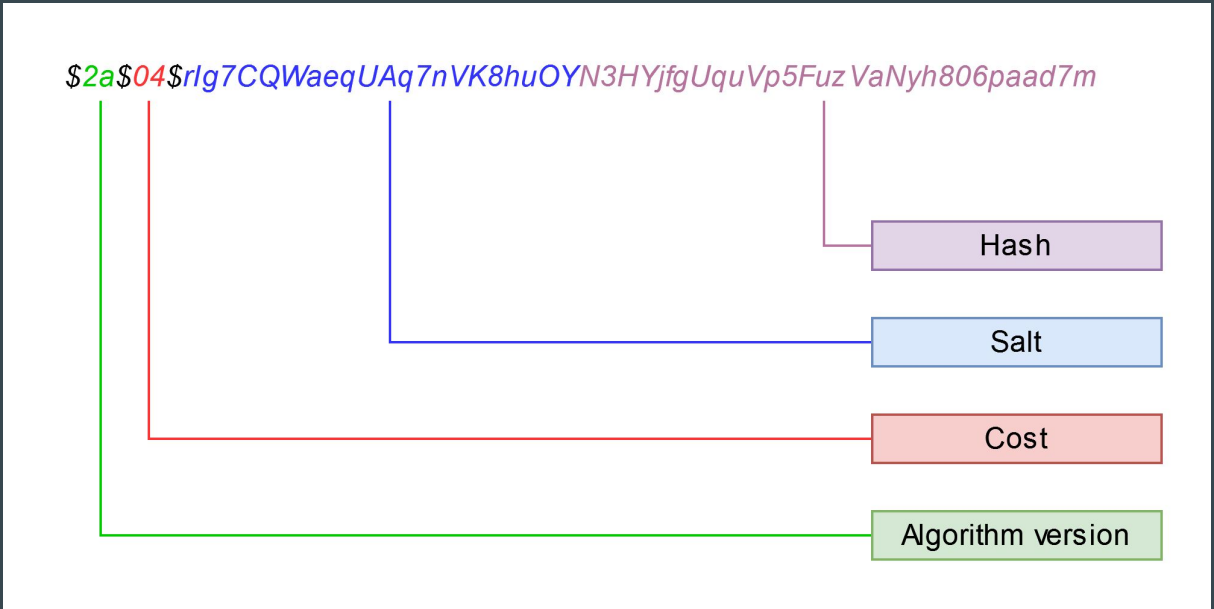
- Cout
- Consommation
- Hashrate

Bcrypt - Algorithme de hash

Bcrypt

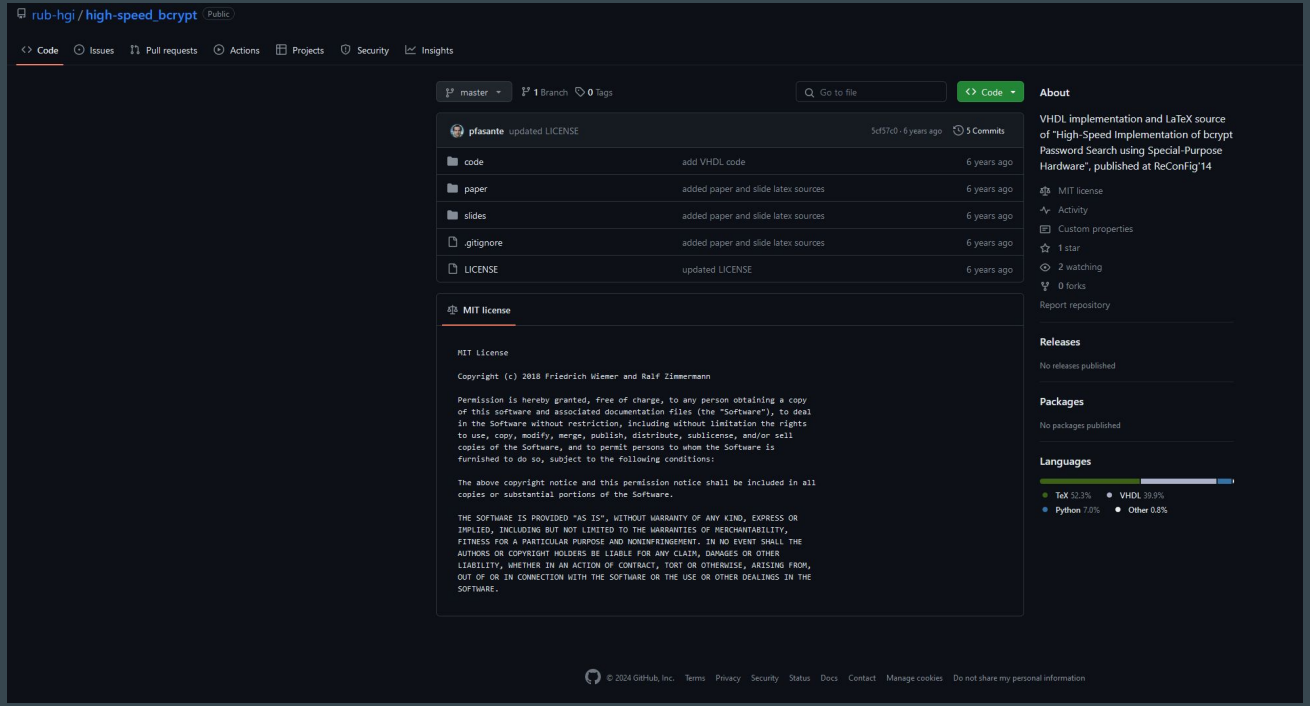

Password
Salt
Cost
Iterations = 2^cost
Expensive Key Setup Algorithm
Encryption Keys
(sboxes & subkeys)
Plain Text :
"OrpheanBeholderScryDoubt"
Blowfish Encryption
(64 times)
Hash

Bcrypt - Format du hash

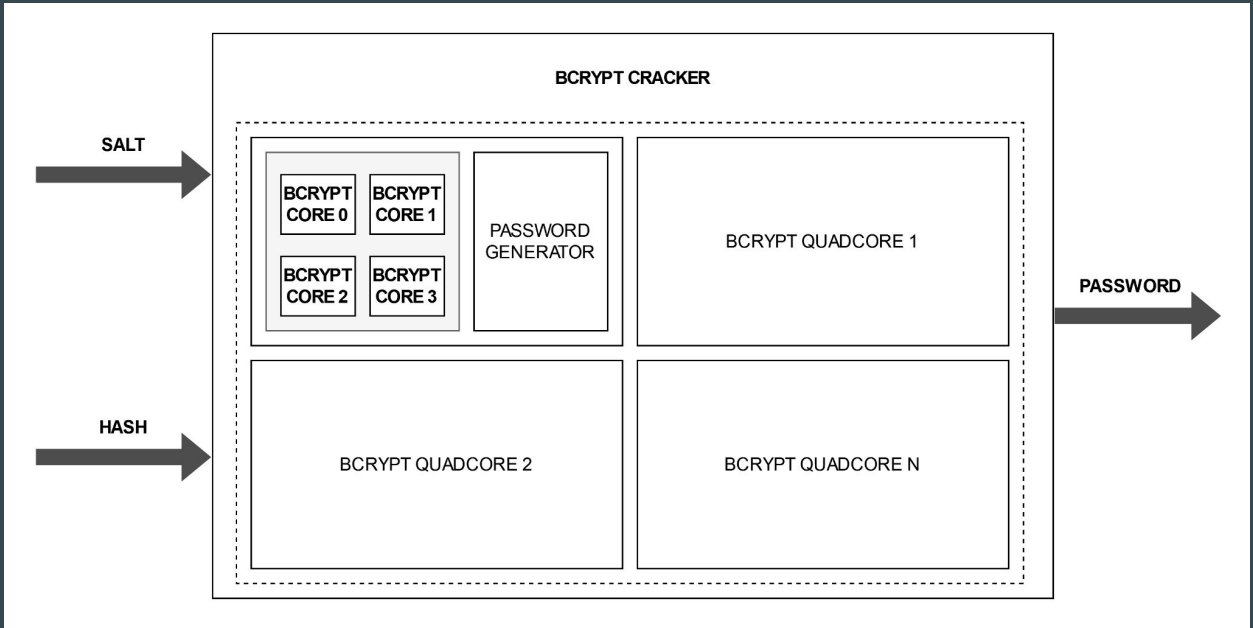


Implémentation existante

Implémentation existante



Implémentation existante - Schéma

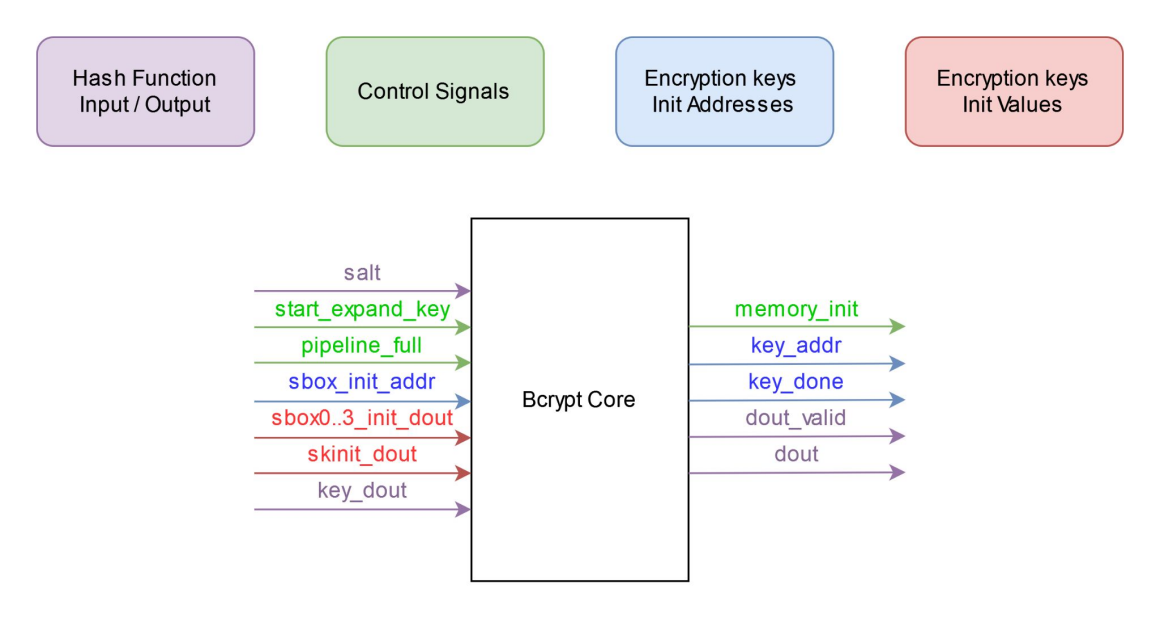


Implémentation existante - Problèmes

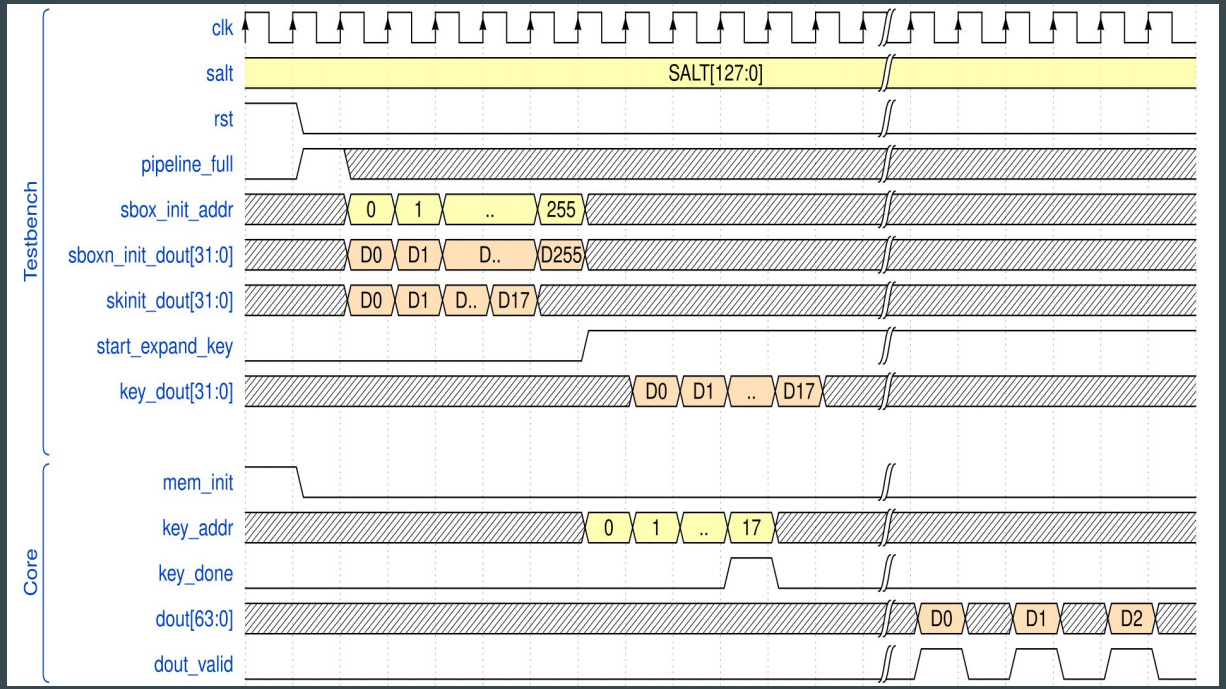
- Documentations
- Versions - Incohérences
- Testbenches incomplets
- Petites erreurs

Fonctionnement & Test

Bcrypt Core Interface

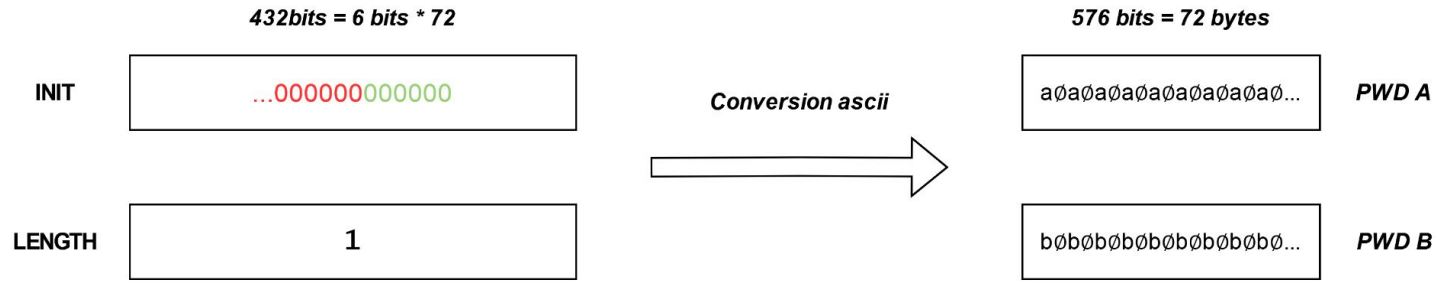


Bcrypt Core Timing

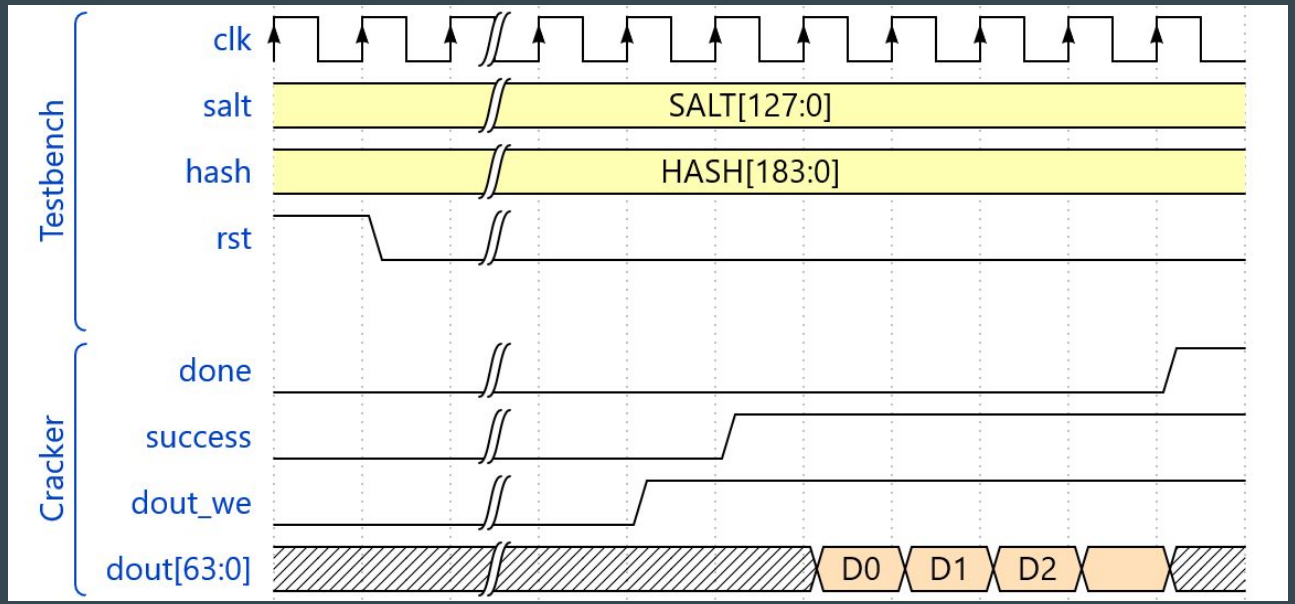


Password Generator

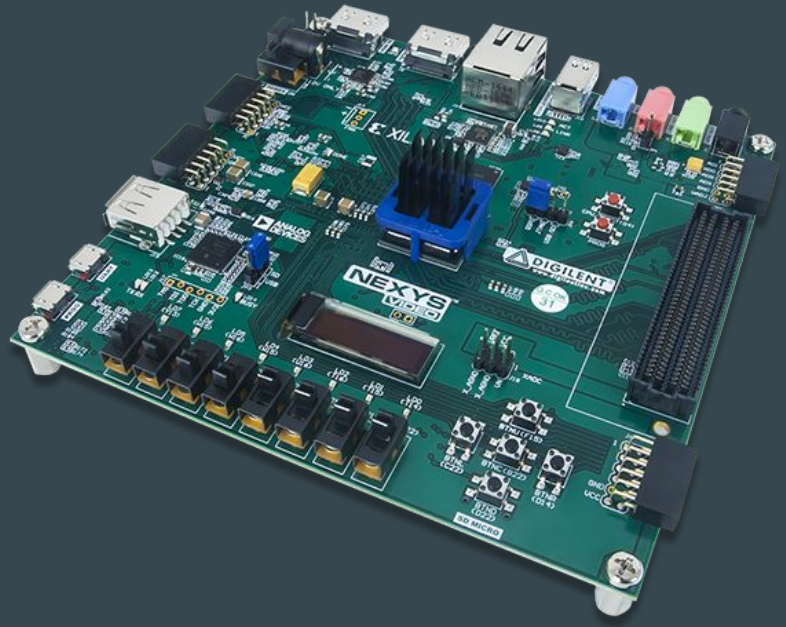
Conversion Table				
0x00	0x01	0x02	0x1b	0x35
NULL ø	'a'	'b'	'A'	'0'



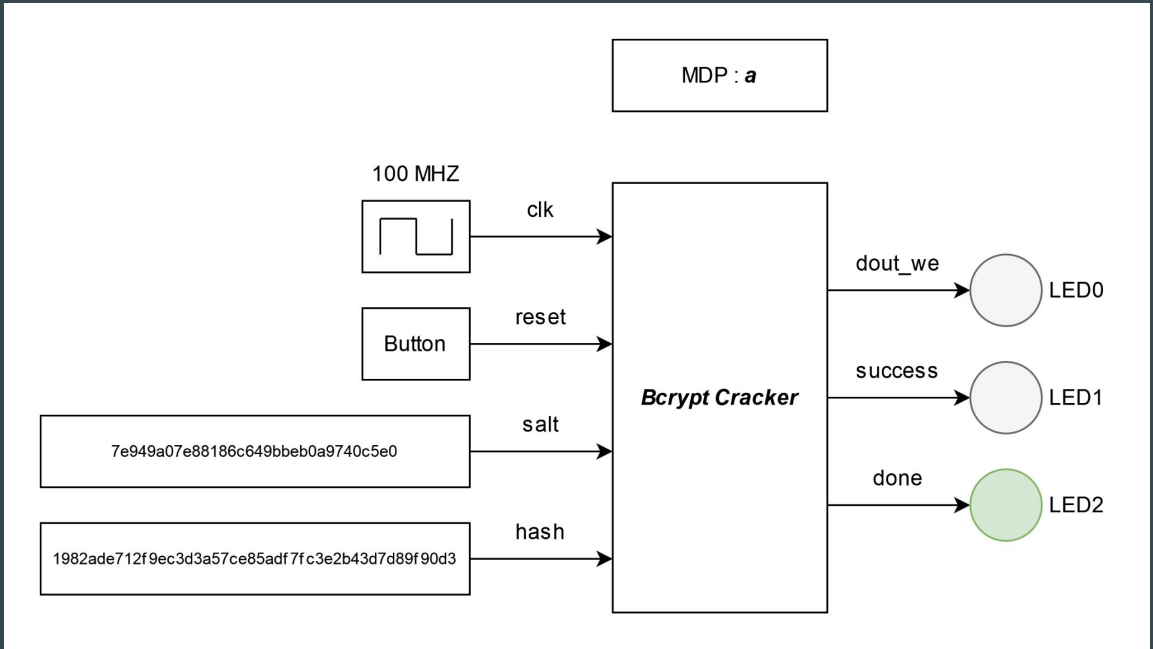
Bcrypt Cracker Timing



Bcrypt Cracker Test Board - Nexys Video

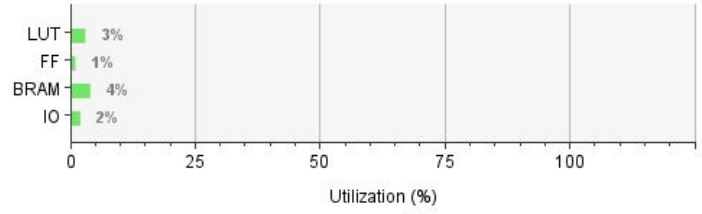


Bcrypt Cracker Test - Schéma



Bcrypt Cracker - Bilan

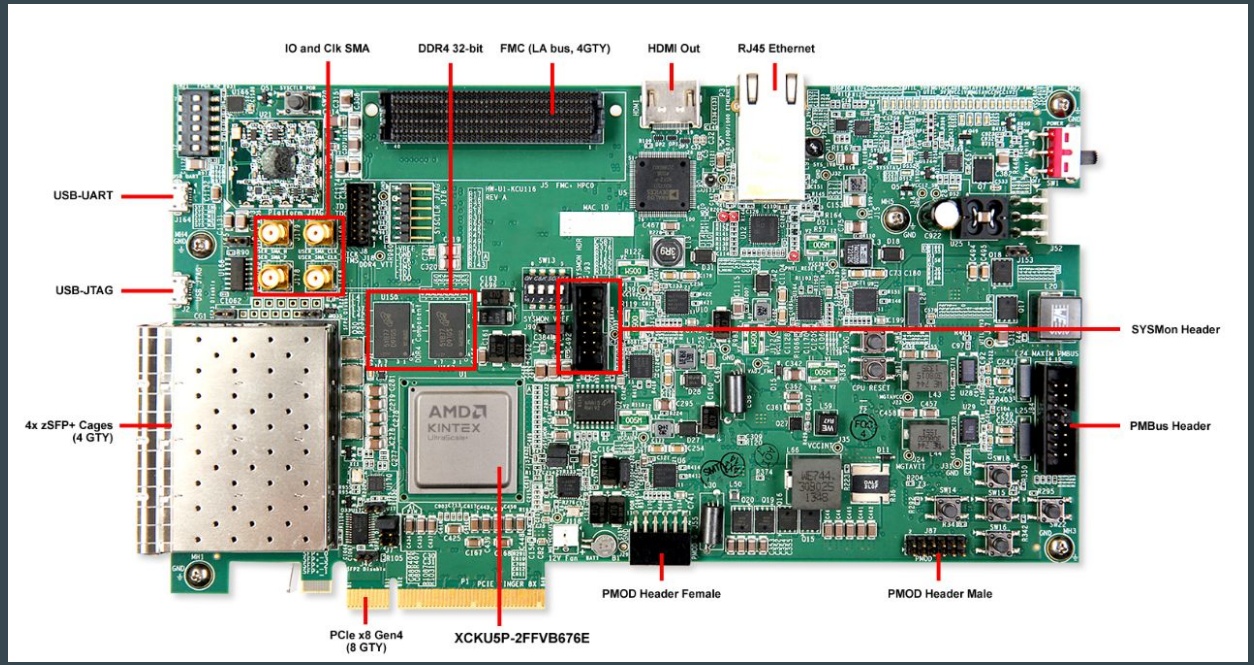
Resource	Utilization	Available	Utilization %
LUT	3640	134600	2.70
FF	2878	269200	1.07
BRAM	13	365	3.56
IO	6	285	2.11



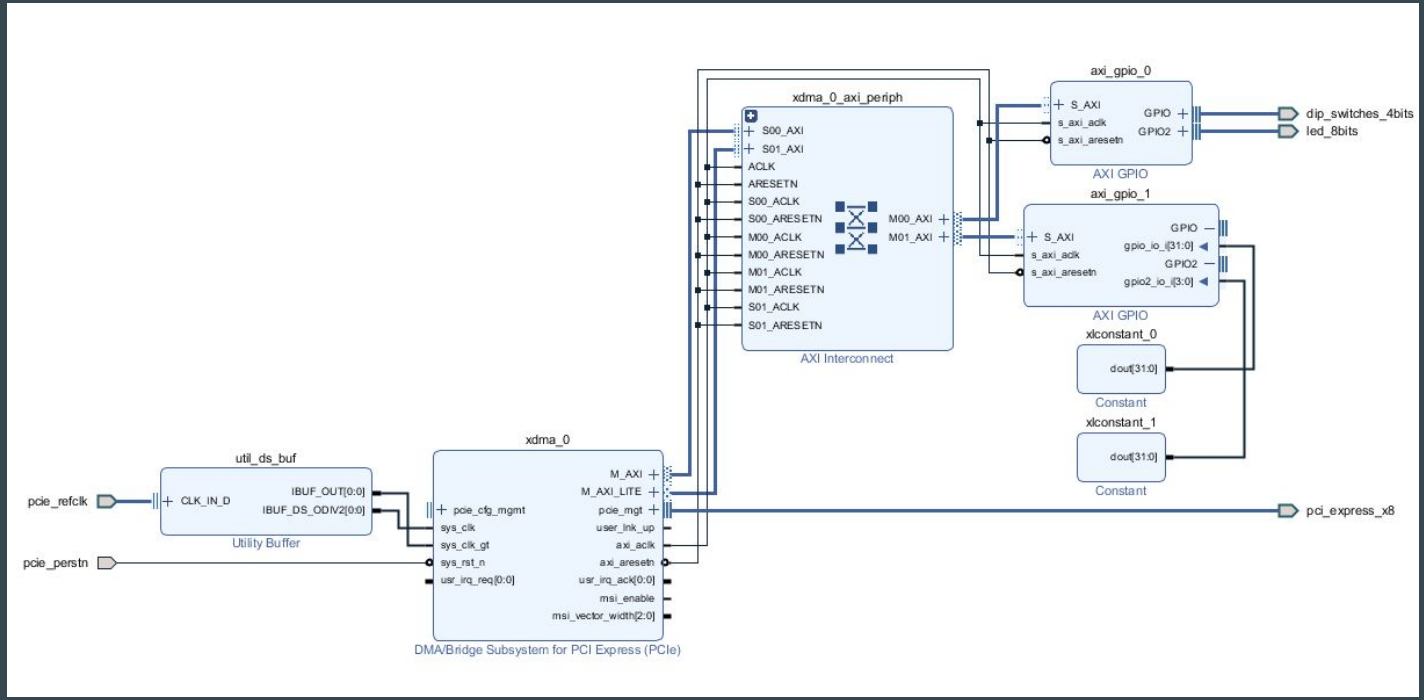
Cost = 4
Quadcores = 1
Hashrate = 1205.57 [Hash/s]

Interface PC - FPGA

Interface PCIe - Kyntex Ultrascale +



Interface PCIe - Block Design



Interface PCIe - lspci

lspci

```
sudo lspci -vv -d 10ee:9038
01:00.0 Serial controller: Xilinx Corporation Device 9038 (prog-if 01 [16450])
    Subsystem: Xilinx Corporation Device 0007
    Control: I/O- Mem+ BusMaster- SpecCycle- MemWINV- VGASnoop- ParErr- Stepping- SERR+ FastB2B- DisINTx-
    Status: Cap+ 66MHz- UDF- FastB2B- ParErr- DEVSEL=fast >TAbort- <TAbort- <MAbort- >SERR- <PERR- INTx-
    Interrupt: pin A routed to IRQ 16
    Region 0: Memory at ef000000 (32-bit, non-prefetchable) [size=1M]
    Region 1: Memory at ef100000 (32-bit, non-prefetchable) [size=64K]
    Capabilities: [40] Power Management version 3
        Flags: PMEClk- DSI- D1- D2- AuxCurrent=0mA PME(D0-,D1-,D2-,D3hot-,D3cold-)
        Status: D0 NoSoftRst+ PME-Enable- DSel=0 DScale=0 PME-
    Capabilities: [48] MSI: Enable- Count=1/1 Maskable- 64bit+
        Address: 0000000000000000  Data: 0000
    Capabilities: [70] Express (v2) Endpoint, MSI 00
        DevCap: MaxPayload 1024 bytes, PhantFunc 0, Latency L0s <64ns, L1 <1us
            ExtTag+ AttnBtn- AttnInd- PwrInd- RBE+ FLReset- SlotPowerLimit 75.000W
        DevCtl: CorrErr+ NonFatalErr+ FatalErr+ UnsupReq+
            RlxdOrd+ ExtTag+ PhantFunc- AuxPwr- NoSnoop+
            MaxPayload 256 bytes, MaxReadReq 512 bytes
        DevSta: CorrErr+ NonFatalErr- FatalErr- UnsupReq+ AuxPwr- TransPend-
        LnkCap: Port #0, Speed 8GT/s, Width x8, ASPM not supported
            ClockPM- Surprise- LLActRep- BwNot- ASPMOptComp+
        LnkCtl: ASPM Disabled; RCB 64 bytes, Disabled- CommClk+
            ExtSynch- ClockPM- AutWidDis- BWInt- AutBWInt-
        LnkSta: Speed 8GT/s (ok), Width x8 (ok)
            TrErr- Train- SlotClk+ DLActive- BWMgmt- ABWMgmt-
        DevCap2: Completion Timeout: Range BC, TimeoutDis+ NROPrPrP- LTR-
             10BitTagComp- 10BitTagReq- OBFF Not Supported, ExtFmt- EETLPPrefix-
             EmergencyPowerReduction Not Supported, EmergencyPowerReductionInit-
             FRS- TPHComp- ExtTPHComp-
             AtomicOpsCap: 32bit- 64bit- 128bitCAS-
        DevCtl2: Completion Timeout: 50us to 50ms, TimeoutDis- LTR- OBFF Disabled,
             AtomicOpsCtl: ReqEn-
        LnkCap2: Supported Link Speeds: 2.5-8GT/s, Crosslink- Retimer- 2Retimers- DRS-
        LnkCtl2: Target Link Speed: 8GT/s, EnterCompliance- SpeedDis-
             Transmit Margin: Normal Operating Range, EnterModifiedCompliance- ComplianceSOS-
             Compliance De-emphasis: -6dB
        LnkSta2: Current De-emphasis Level: -6dB, EqualizationComplete+ EqualizationPhase1+
             EqualizationPhase2+ EqualizationPhase3+ LinkEqualizationRequest-
             Retimer- 2Retimers- CrosslinkRes: unsupported
    Capabilities: [100 v1] Advanced Error Reporting
        UESta:  DLP- SDES- TLP- FCP- CmpltTO- CmpltAbrt- UnxCmplt- RxOF- MalfTLP- ECRC- UnsupReq- ACSViol-
        UEMsk:  DLP- SDES- TLP- FCP- CmpltTO- CmpltAbrt- UnxCmplt- RxOF- MalfTLP- ECRC- UnsupReq- ACSViol-
        UESvrt: DLP+ SDES+ TLP- FCP+ CmpltTO- CmpltAbrt- UnxCmplt- RxOF+ MalfTLP+ ECRC- UnsupReq- ACSViol-
        CESta:  RxErr+ BadTLP- BadDLLP- Rollover- Timeout- AdvNonFatalErr-
        CEMsk:  RxErr- BadTLP- BadDLLP- Rollover- Timeout- AdvNonFatalErr+
        AERCap: First Error Pointer: 00, ECRCGenCap- ECRCGenEn- ECRCChkCap- ECRCChkEn-
            MultHdrRecCap- MultHdrRecEn- TLPPfxPres- HdrLogCap-
        HeaderLog: 00000000 00000000 00000000 00000000
    Capabilities: [1c0 v1] Secondary PCI Express
        LnkCtl3: LnkEquIntrruptEn- PerformEqu-
        LaneErrStat: LaneErr at lane: 3
```

Conclusion :

- Faire fonctionner sur la carte Nexys Video
- Tester le PCIe avec un driver linux
- Réfléchir à des améliorations au système
- Faire le rapport