

# Build Results

## I. FPGA Results:

Device: Stratix IV EP4SGX530NF45C3

Fmax: 160.98MHz

	Combinational ALUTs	Registers
aes-gcm	11566	3504
• gctr_block	3789	2987
- aes_core	3489	2469
- aes_decipher_block	991	137
- aes_encipher_block	609	137
- aes_key_mem	1526	2191
- aes_sbox	160	
• ghash_block	7391	
- gfmul	7263	

# II. ASIC Results

## 1. Synthesis Results:

```
Normal exit.
tcl/CheckError_and_GetResult.sh
*****
    Checking Synthesis is cleared
*****

Instance Count
-----
Leaf Instance Count          43408
Physical Instance count      0
Sequential Instance Count    3504
Combinational Instance Count 39904
Hierarchical Instance Count   1

Area
----
Cell Area                    1211087.002
Physical Cell Area           0.000
Total Cell Area (Cell+Physical) 1211087.002
Net Area                     636855.917
Total Area (Cell+Physical+Net) 1847942.919

-----
Instance      Cells  Leakage  Dynamic  Total
              Cells Power(nW) Power(nW) Power(nW)
-----
aes_gcm_TOP    43408  1973.930 869497630.113 869499604.043
```

```
*****
              final Fmax found: 94 MHz
              (2021年  6月  8日 火曜日 11:49:54 JST)
*****
```

	ROHM
Sequential Instance	3504
Combinational Instance	39904
Cells	43408
Cell Area	1211087.002 um2
Net Area	636855.917 um2
Total Power	869.499 mW
Fmax	94 MHz

## PnR Results:

Depth	Name	#Inst	Area (um^2)
0	aes_gcm_TOP	52434	1396007.424
1	U1_GHASH_GFMUL	31977	787391.5392

```
Gate area 9.6768 um^2
Level 0 Module aes_gcm_TOP      Gates=   144263 Cells=   52434 Area= 1396007.4 um^2
Level 1 Module U1_GHASH_GFMUL   Gates=81369   Cells=31977   Area=  787391.5 um^2
```

```
*****
          final Fmax found: 99 MHz
        (2021年  6月  9日 水曜日 14:40:35 JST)
*****
```