2020/08/26 Naoki Hirayama

SnakeCube 実機再現

RSA 2048bit(Private CRT) 1.74[ms]の再現テストを行えるための測定条件の記録

verilog ファイルのハッシュ値

SHA256(d2020_08_26.tar.xz)=
6fe6aebc55184190df3d01753858c63bef7ea30cce22c4926d65407ac7aa823b
SHA512(d2020_08_26.tar.xz)=
0c52283d097f752e35824ab9e64edc7fa2c30c39cee3d441de91d4a671c949c4cd584d934482e
009d27f89ffb1802b819e1115f027b9f6c74e36cf733f555d67

証拠画像のファイルのハッシュ値

SHA256(scubew1k_SS_2020_08_26.tar.gz)=
1a74e24c940358a135556bc69df52ed06a729c79180f5f8e34ddef82b40c1652
SHA512(scubew1k_SS_2020_08_26.tar.gz)=
adf4336173fbee811ce4655957ae117dff6156ffae373e33f904eee08cfcee2bd107fc6dae576aec
ea5ae344180f139516d9a6dcf714788adfdd15f4c6d679cf

測定日 2020 年 8 月 26 日
SnakeCube 構成 : 暗号プロセッサとモンゴメリ乗算器 2 個
SnakeCube バージョン : 0.36
SnakeCube クロックの設定 : Arty 236MHz
FPGA ボード : Digilent Arty
FPGA デバイス : Xilinx XC7A35TICSG324-1L
Vivado : 2020.1

結果

(1)Flow_AreaOptimized_high / Performance_NetDelay_high WNS=0.035
(2)Flow_AreaOptimized_high / Performance_ExploerWithRemap WNS=0.001
(3)Flow_AreaOptimized_medium / Performance_ ExploerWithRemap WNS=0.004