

H/W 実装評価概要 (MULTI-S01)

MULTI-S01 暗号のCで作成されたプログラムに対して、FPGA への H/W 実装を VerilogHDL により回路記述し、シミュレーションを行った。

復号化時使用する A⁻¹ 鍵は、ソフトウェア生成とした。

実装結果として、Cプログラムでの実行結果と同じ暗号と復号データを得られる事を確認し、以下の評価結果を得た。

FPGA はアルテラ社の「EP20K1000E」を使用した。

動作クロック	: 18.8 MHz
実行速度	: 1.203 G B P S (6 4 b i t / クロック)
回路規模	: 19811 ATOMs of 42240 (46%)