Chapter 5

Conclusion

From the simulation results and analysis, there are some conclusions that can be made at the end of this discussion. They are:

− Trivium and Mickey are hardware oriented stream cipher that can be implemented on Altera board DE2_70.
− Trivium can be implemented in parallel operation up to 64 bit, and parallel implementation in general will decrease the speed of the circuit but give some increase in power dissipation.
− The time required to initialize a 1-bit Trivium is 1153 clock cycle, and 19 clock cycles for the 64-bit Trivium.
− The parallel operation of Trivium gives higher throughput without a major price according to the throughput per area or throughput per power dissipation.
− The most recommended parallel operation of Trivium is 64-bit, but for a circuit with limited number of logic elements, a smaller parallel operation may be chosen.
− Mickey needs more logic elements and bigger power dissipation than Trivium, but give smaller throughput than Trivium.
− For over all performance Trivium is thus superior to Mickey.