NCL-DES: An asynchronous DES encryption chip on NCL logic

A. Romero

Abstract:

In order to check and verify the Theseus NCL (Null Convention Logic) design flow, we have designed the core of a DES encryption chip at Infineon Technologies.

We will present our experiences on the use of the NCL design flow for the development of this test chip. The strong points and limitations of this flow will be discussed, as will as the main problems found while designing the NCL-DES chip. We will also present an introduction on the architectural solutions used on the implementation of the DES algorithm.

Theseus’ design flow for NCL logic uses standard EDA tools to simulate and to synthesise VHDL code into delay-insensitive circuits but is limited to a special sub-set of VHDL and requires the use of special signal types that are defined on different packages and library modules provided by Theseus. A two-step process, using Synopsys and special scripts, generates a netlist of the circuit based on a special library of threshold gates.

The NCL-DES chip transfers plain text and one of eight selectable keys to the DES core, performs a single-DES encryption on the plain text and writes it back to a storage block. The encrypted texts can serve as a plain text for another DES round.

The test chip consists of a fully-asynchronous NCL DES block, a clocked (non-NCL) storage block for the plain text and the keys, and an interface that links both parts. All the design has been VHDL-coded, using library modules and packages provided by Theseus Logic. It was then synthesised by the Theseus two-step process using a 0.13 micron technology cell library created by Infineon. While most of the circuit description was on behavioural VHDL, the core was done on structural VHDL, to better exploit the advantages of the asynchronous implementation.