Tutorial 1: Setting up the development environment

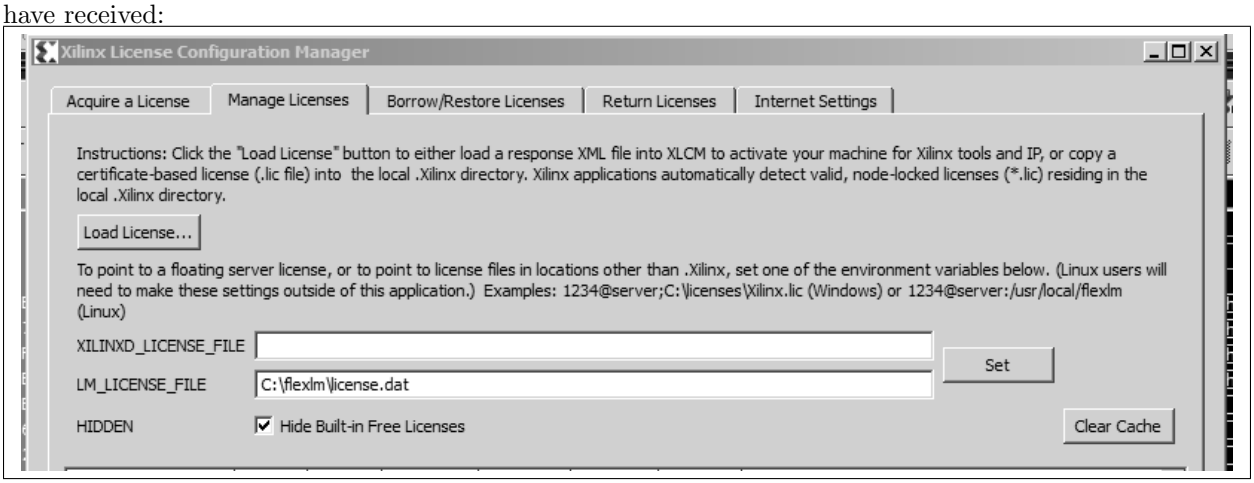
In this tutorial you will learn how to download and install the Xilinx ISE development environment for FPGAs in combination with the ModelSim simulator. Moreover, you will simulate a real design of the NOEKEON[1] block cipher.

Download and install Xilinx ISE 14.7

Xilinx ISE 14.7 can be downloaded from `http://www.xilinx.com/support/download/index.html/content/xilinx/en/downloadNav/design-tools/v2012_414_7.html`. In case the download manager fails in your system, there are direct links in this website[2].
You will have to register first. Then, install it in your platform and send me an e-mail to `a.delapiedra@cs.ru.nl` with the following information:

- Hostname of your computer
- MAC address of the computer
- Operating System of the computer and if the OS is 32 and 64 bits

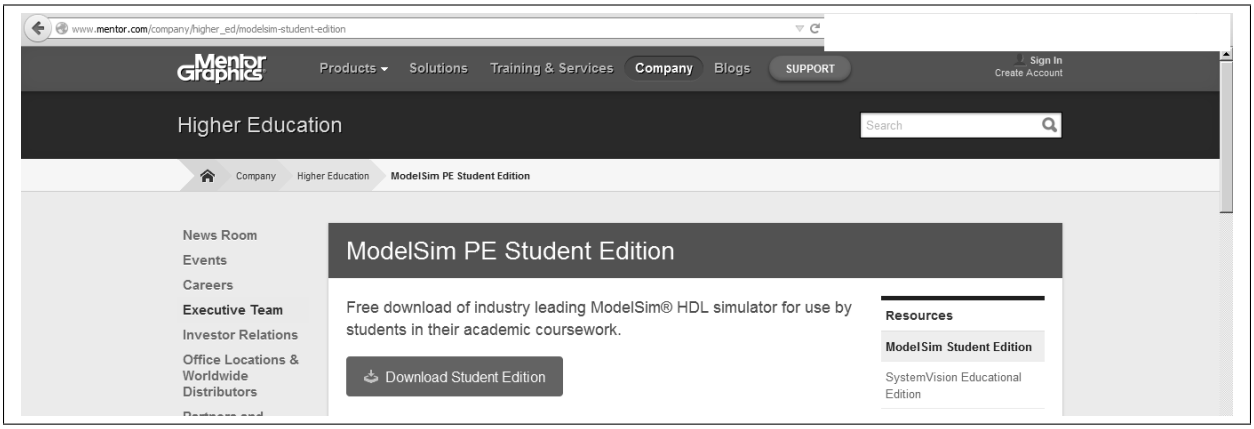
I will generate a license for you so you can use ISE without restrictions. I can generate one license for each member of the group. Otherwise, you can use the trial license but it has limitations and I cannot assure that all will work as expected.
Once you have the license, open the Manage Xilinx Licenses software (from Start: Xilinx Design Tools, ISE Design Suite 14.7, Accessories, Manage Xilinx Licenses). Click Load License and select the license file you have received:



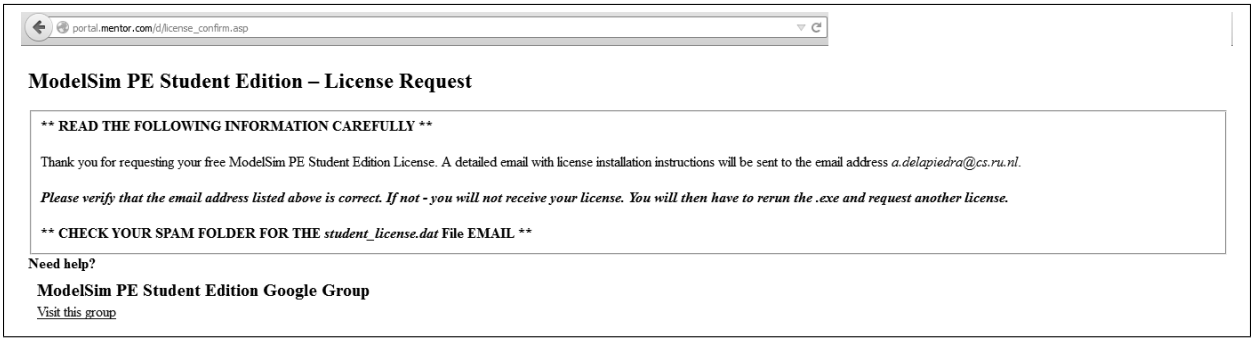
Download and install ModelSim

Go to `http://www.mentor.com/company/higher_ed/modelsim-student-edition`.

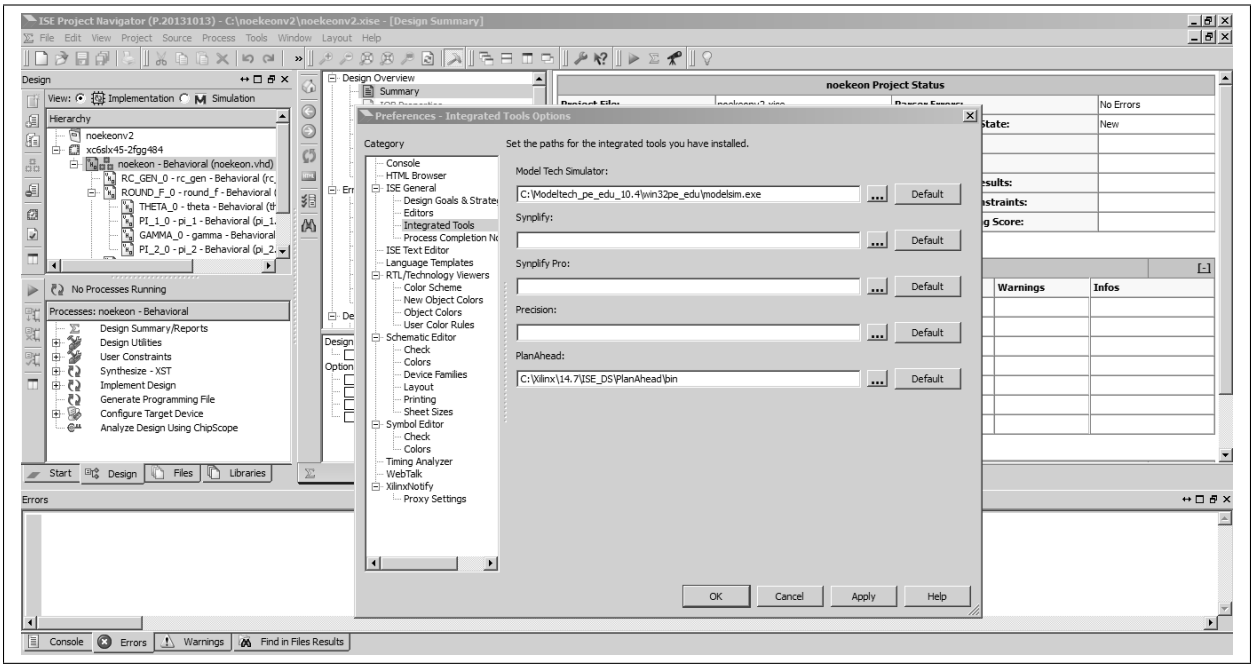
[1] `http://gro.noekeon.org/`
[2] `http://www.xilinx.com/support/answers/57840.html`



After the installation you can generate a student license that will be sent to your e-mail together with instructions for activating ModelSim. Follow them for configuring the simulator with the generated license.

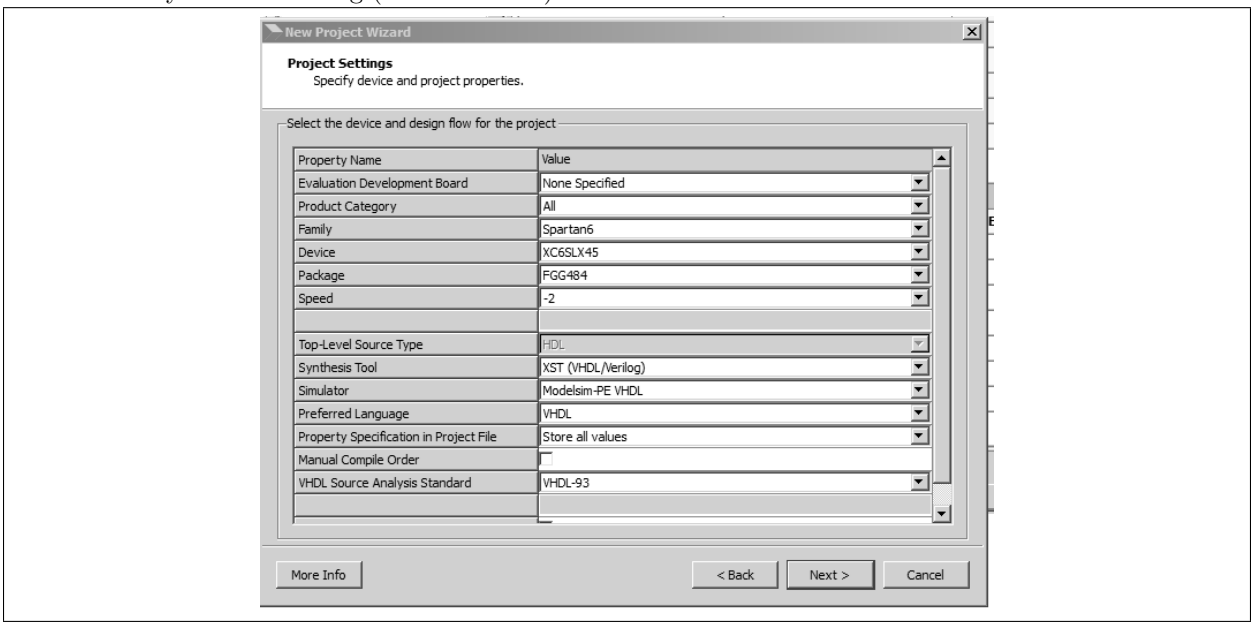


In order to configure Xilinx ISE 14.7 with the simulator, go to Edit, Preferences, ISE General, Integrated Tool and point to the path of the ModelSim executable in your computer in the Model Tech Simulator field:



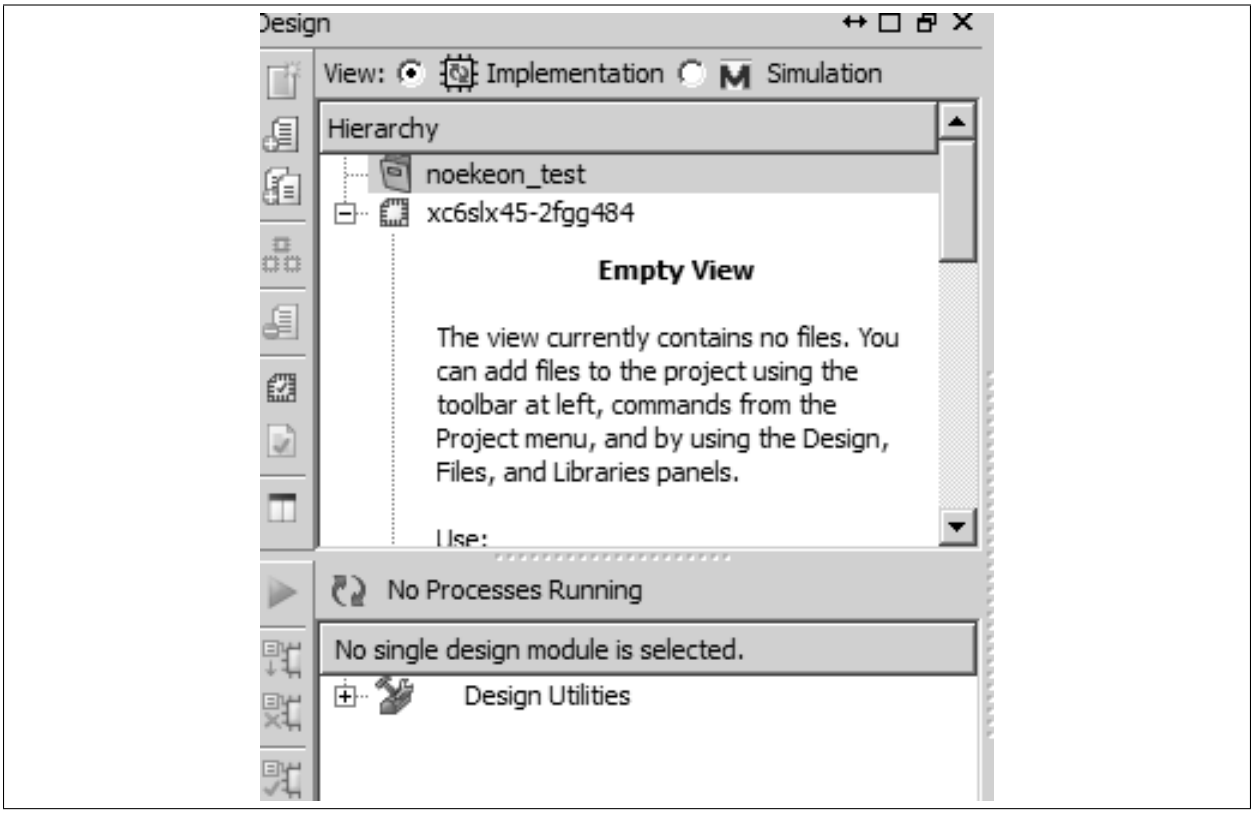
Configure Model Sim

Download the implementation of the NOEKEON block cipher from this URL[3] (or clone it with git from this repository[4]) and extract the source code in your computer. Then, open Xilinx ISE 14.7 and create a new project: File, New Project. Select a name and location and press Next. In the next window select the type of FPGA you will be using e.g. Spartan 6, the hardware description language (VHDL) and the version of the simulator you will be using (ModelSim-PE).

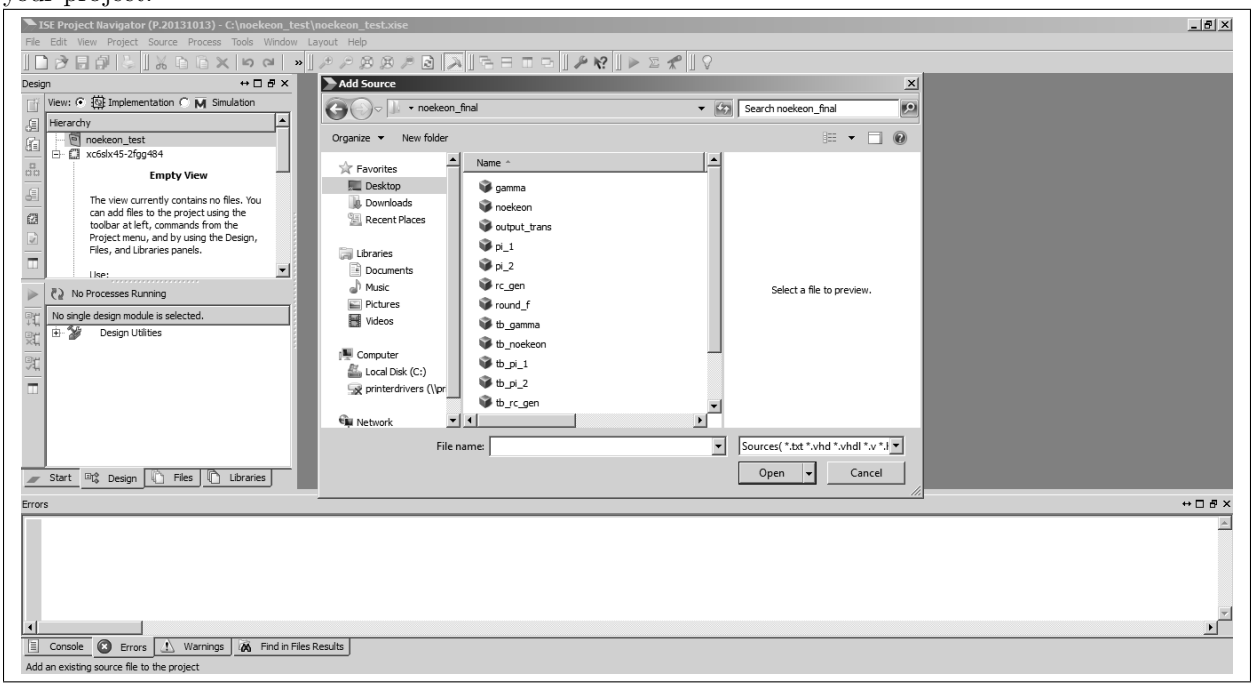


Then, press Finish. Now, we are going to import the source code you have downloaded that corresponds to the implementation of the NOEKEON block cipher. Click on your project and select Add source

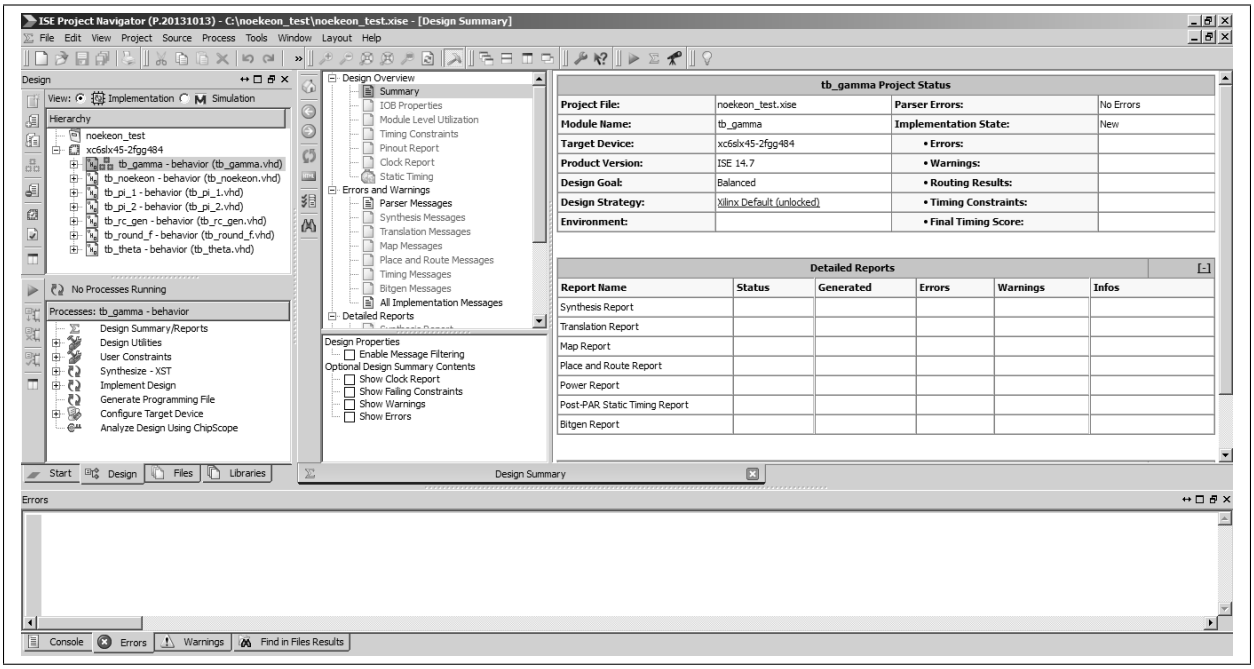
[3] `https://github.com/adelapie/noekeon/archive/master.zip`
[4] `https://github.com/adelapie/noekeon.git`



Then, select every file you found in the ZIP file (but ignore the license file and the README) and add it to your project:

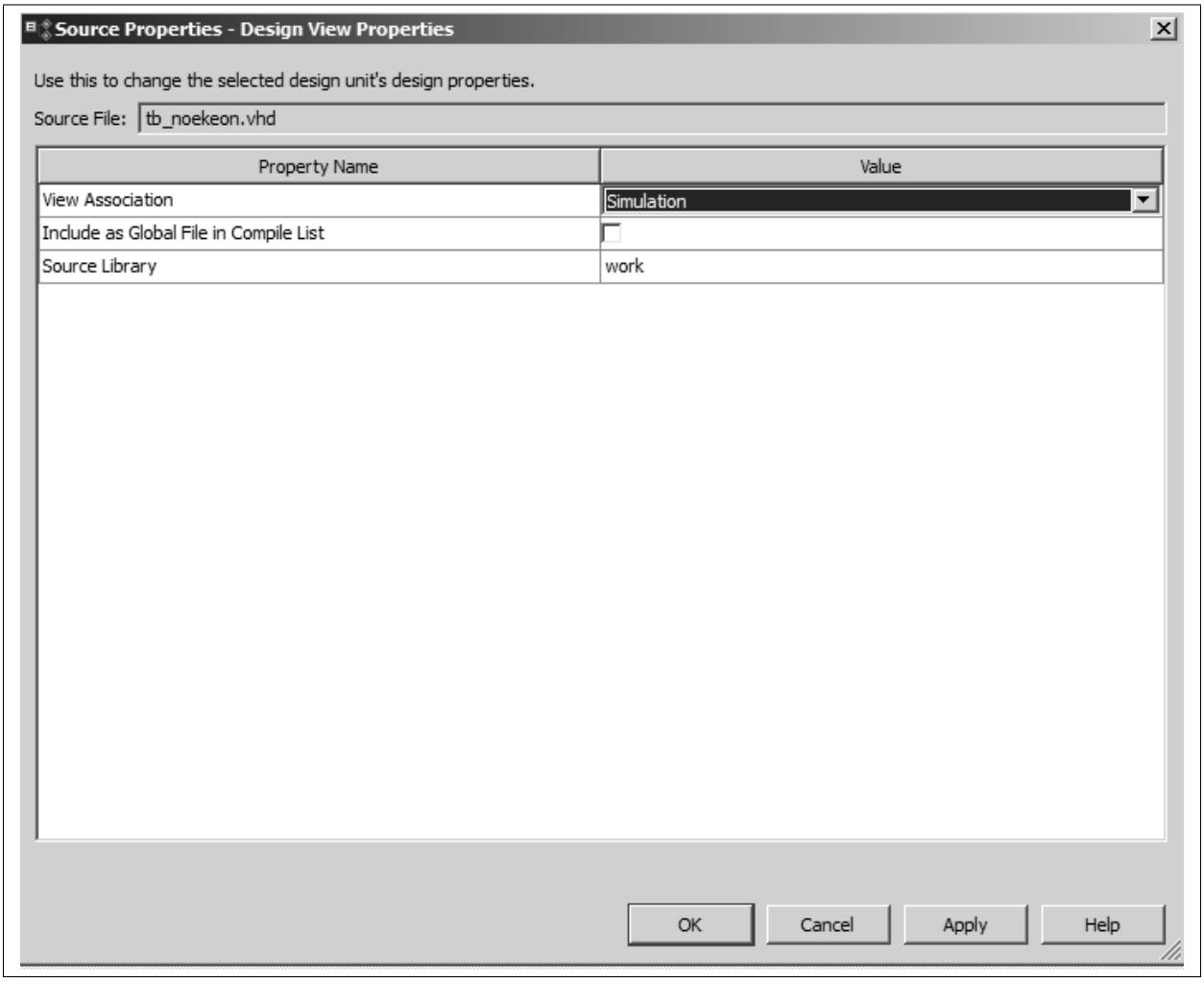


After importing the source code, you should see the list of files of your project as:

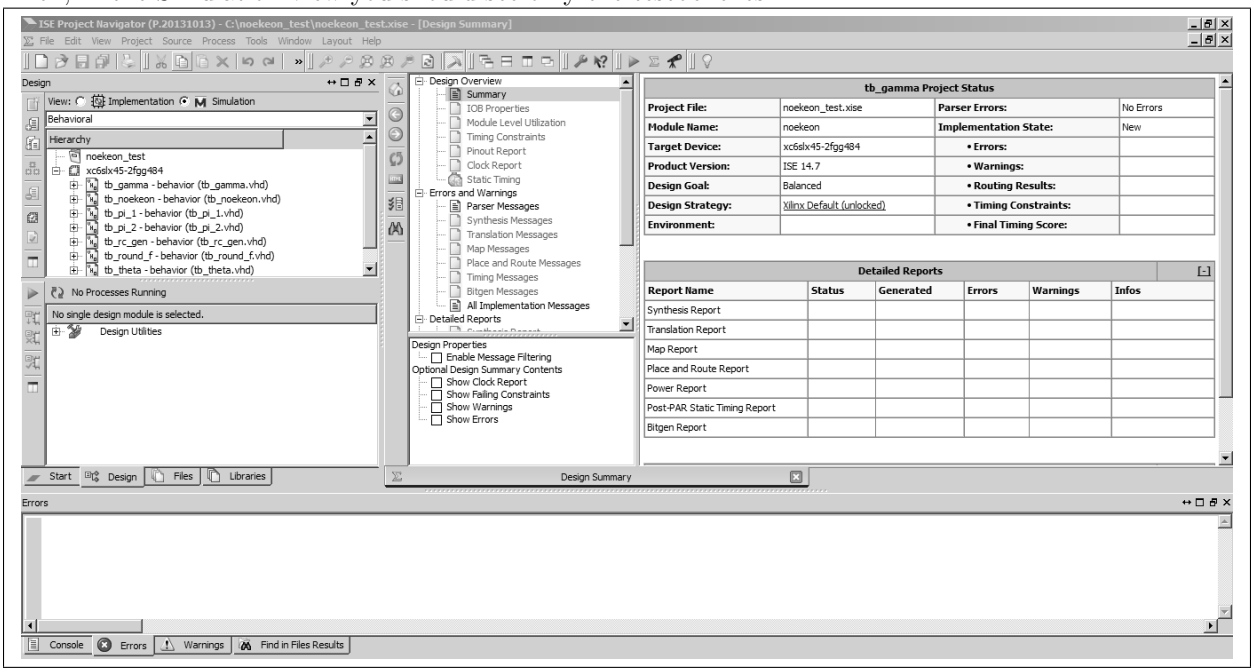


However, the testbenches[5] of each module appear in the Implementation view whereas they should be moved to the Simulation one. In that respect, you should right click each tb_ file, select Source properties and change the association to Simulation e.g.

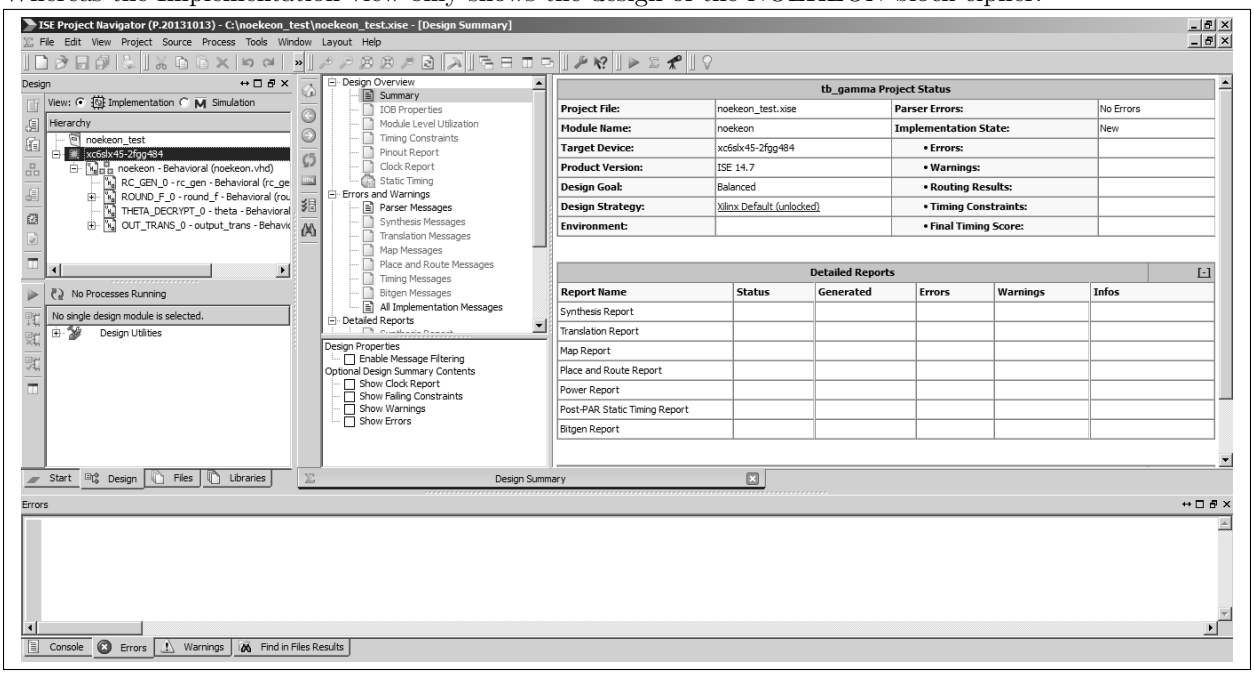
[5]These test files verify the correct functionality of each submodule of NOEKEON.



Then, in the Simulation view you should see only the testbenches:

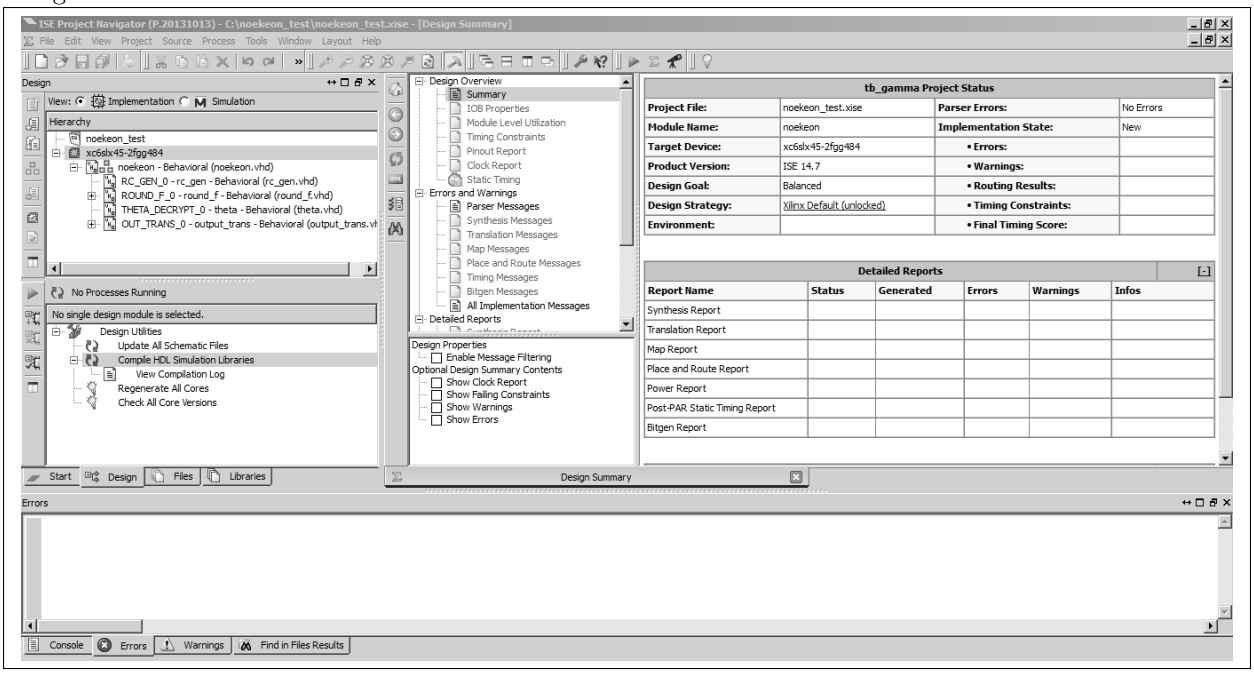


Whereas the Implementation view only shows the design of the NOEKEON block cipher:

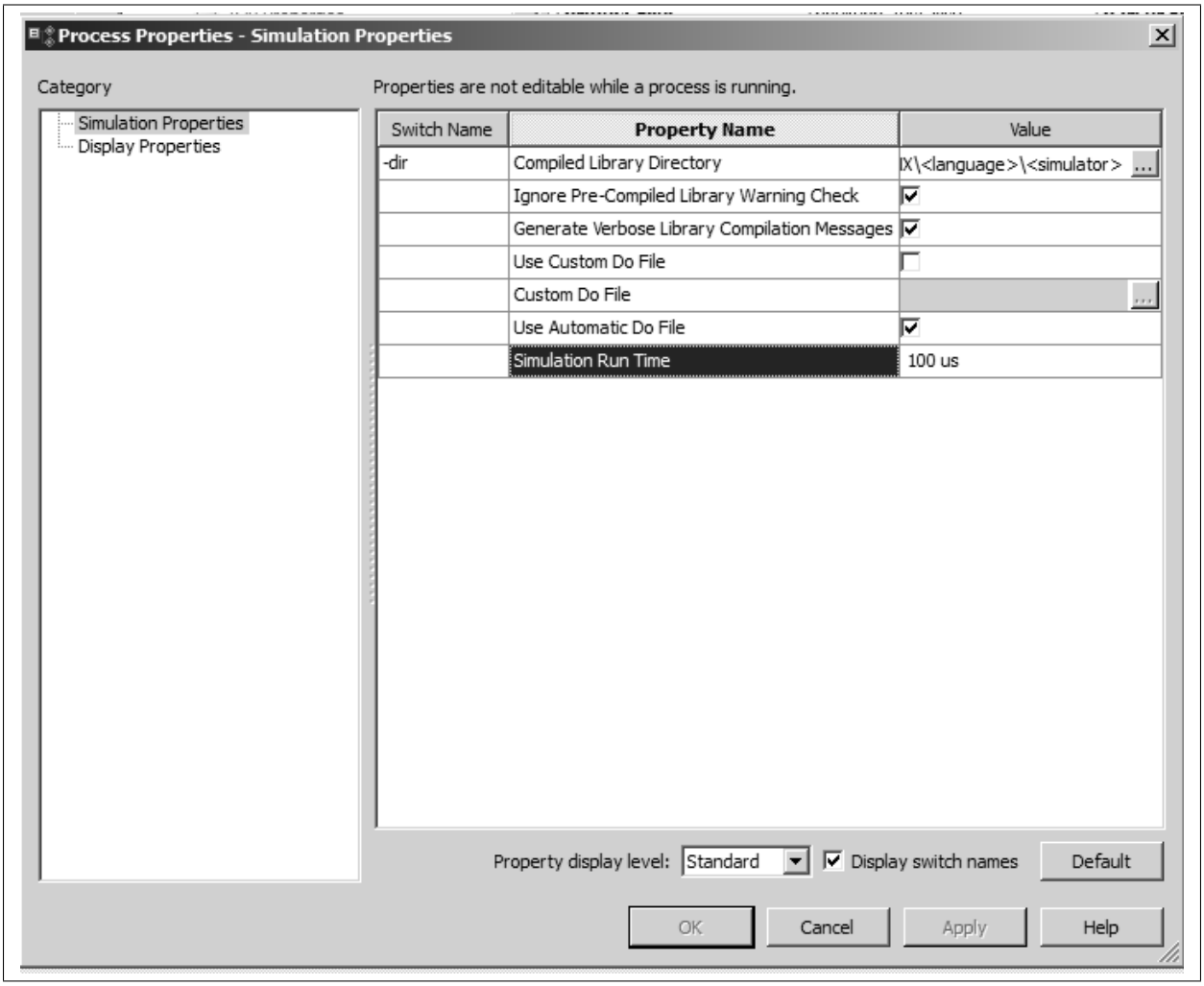


Xilinx ISE has two modes of operation that follow the typical cycle of digital design e.g. design and simulation before synthesis. For that reason, there two views that allow the user to change between Implementation and Simulation and work with an independent set of files in each one.

Before simulating the design we should compile the Xilinx libraries into ModelSim. In order to do that, click into the name of the FPGA of your project, and double-click Compile HDL Simulation Libraries under the Design Utilities menu:

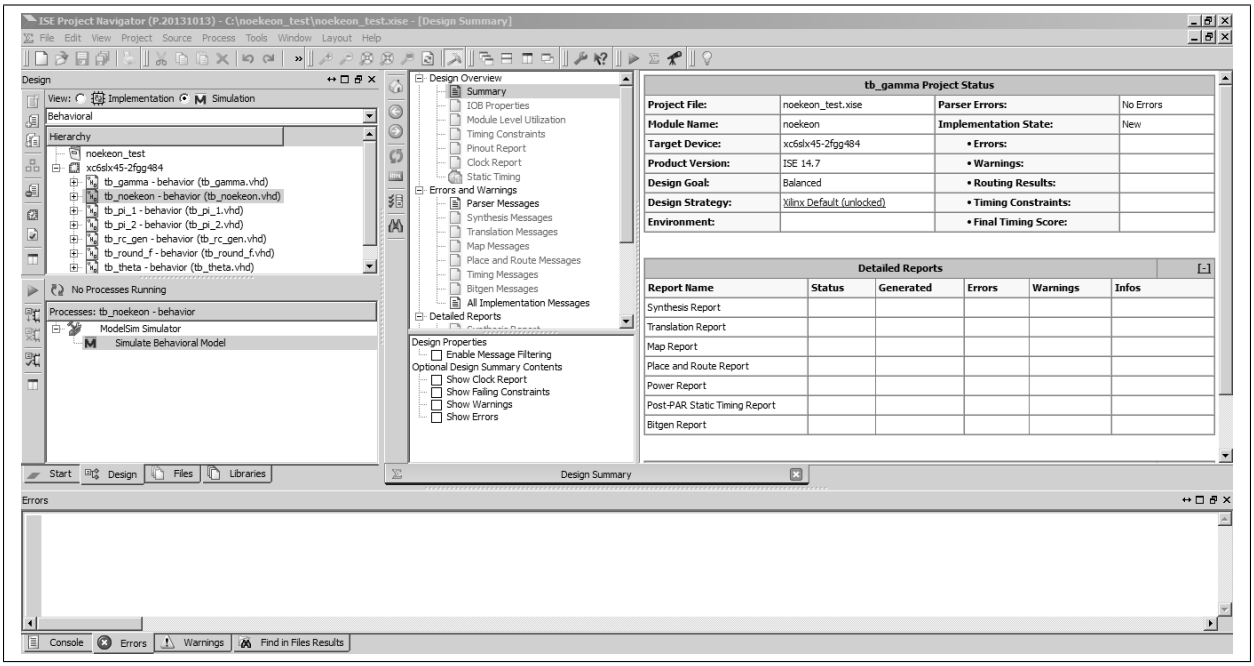


This will take some time. Afterwards, go the Simulation view, select one of the testbenches, then ModelSim simulator, then right-click into Simulate Behavioral Model, Process properties and set the following values: Ignore Pre-Compiled Library Warning Check and increase the Simulation Run Time to 100 us:

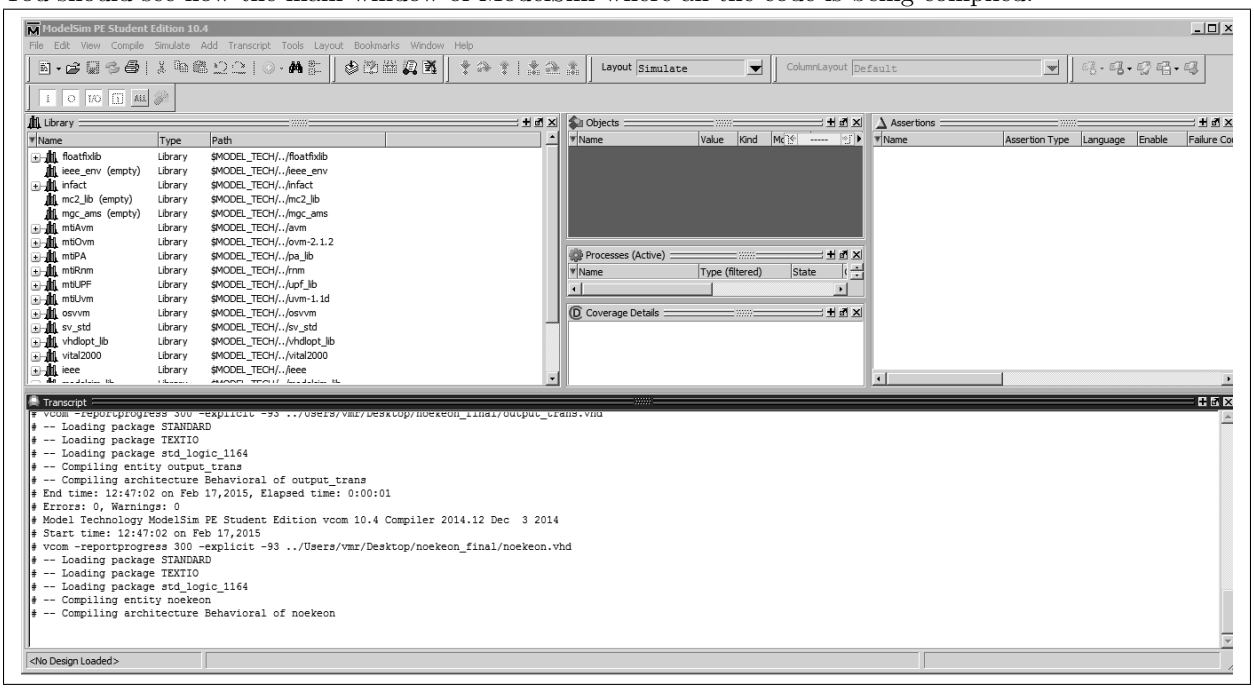


Simulating the NOEKEON block cipher

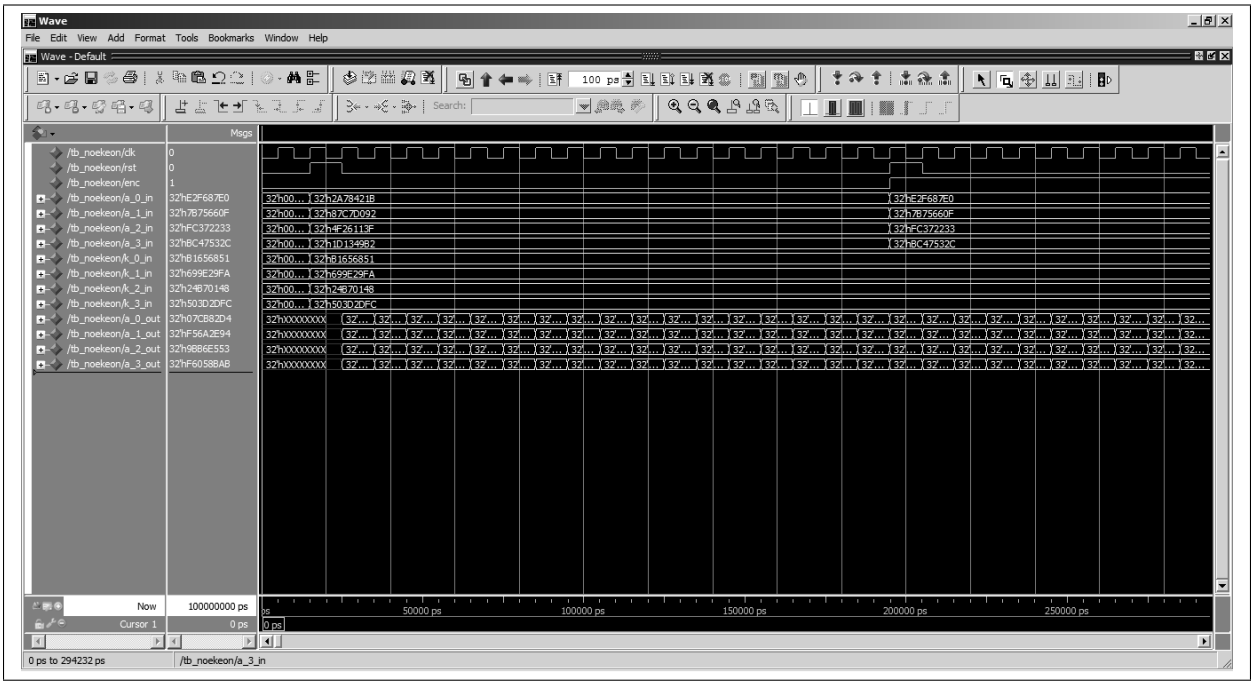
Once we have configured the ModelSim simulator on Xilinx ISE, we can simulate the NOEKEON block cipher. You can start with the basic functions of the round (gamma, theta, pi1, pi2) or with the encryption and decryption operations of the cipher. Go to the Simulation view, click into the tb_noekeon testbench and double-click on ModelSim Simulator, Simulate Behavioral Model:



You should see now the main window of ModelSim where all the code is being compiled:



And then the wave window with every signal of the block cipher:



Continue with the second tutorial for learning how to create your own combinational circuits and testbenches.