Summer school on real-world crypto and privacy – Hardware tutorial

June 6, 2016, Šibenik, Croatia

Ricardo Chaves, Nele Mentens, Ingrid Verbauwhede

(thanks to João Resende for his help in preparing this document)

PRE-TUTORIAL TASKS

1. Download the Vivado WebPack 2016.1 installation files

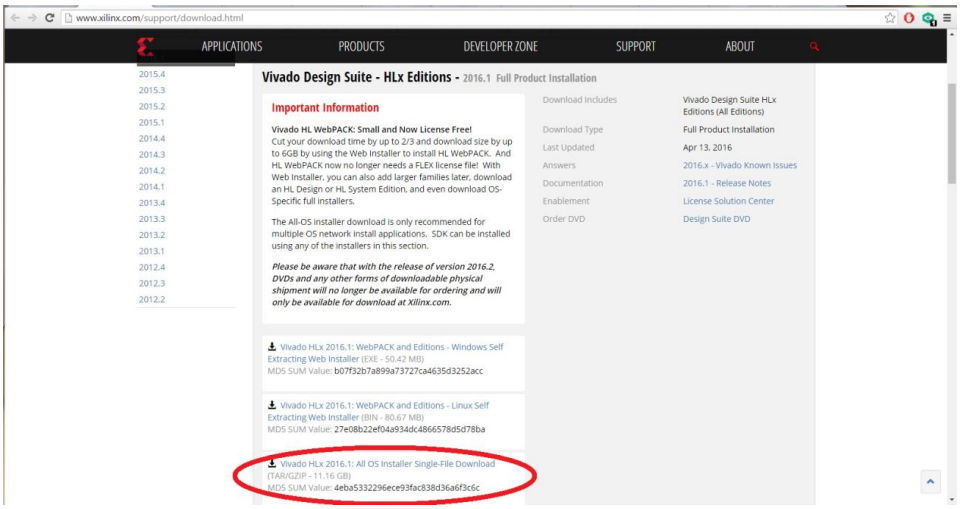
There are 3 ways to access the installation files:

- Option 1: Download the single-file installer (11 GB) from the Xilinx webpage (this requires a registered Xilinx account; you will be prompted to create one as you proceed)
- Option 2: Download the web installer (50-80 MB) from the Xilinx webpage (this also requires a registered Xilinx account)
    - during installation, 10 GB of free disk space is required
    - the download size is 2 GB
- Option 3: Download the single-file installer (11 GB) from our temporary Dropbox link (this way, you can avoid the registration, but you will only be able to obtain a 30-day evaluation license)

Option 1: Download the single-file installer (11 GB) from the Xilinx webpage

1.1 Access the following webpage: http://www.xilinx.com/support/download.html

1.2 In the section of Vivado Design Suite - Full Product Installation, select "All OS Installer Single-File Download".



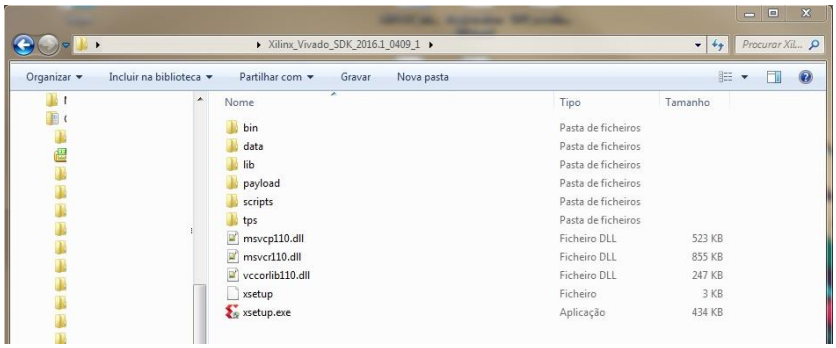
1.3 Once you select the file, you will be sent into a "Sign In" webpage where you have to input your Xilinx account information to log in. Once you do that (or in the case you were already logged in) the download will start. The complete download process may take a while.

ADVICE: It is recommended that the download file is placed in a directory without spaces or non-standard characters in the directory path (e.g. C:\Xilinx\). If you do not download the file into such a directory, please move it there.

1.4 After the download is completed, you will have a "tar.gz" compressed file: "Xilinx_Vivado_SDK_2016.1_0409_1.tar.gz"

Decompress the file using either "Zip" or "7-Zip" (or any other de/compressing program). Some programs recognize "tar.gz" as a single compression, while others consider it as a double compression ".tar" and ".gz". If after your first decompression, you obtain a ".tar" file instead of a directory, decompress the resulting file again.

1.5 Once you obtain the directory "Xilinx_Vivado_SDK_2016.1_0409_1" you are ready to install the software.



Option 2: Download the web installer (50-80 MB) from the Xilinx webpage

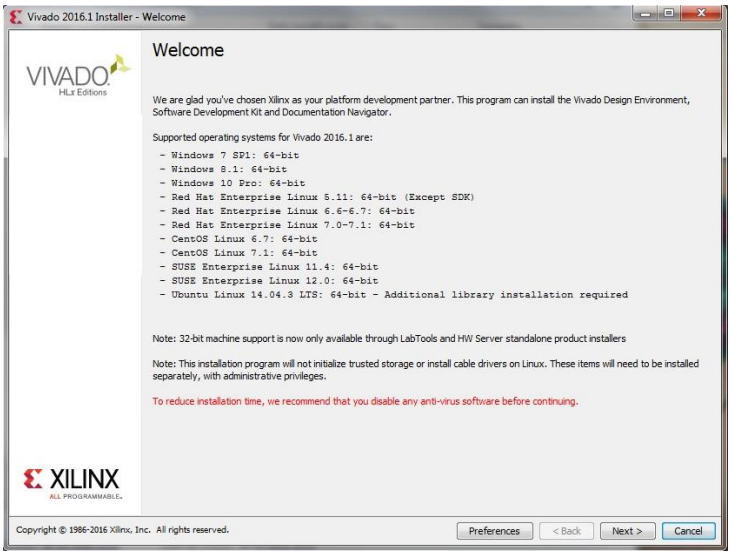
Access the same webpage as in Option 1 and select the appropriate web installer corresponding to your operating system (50 MB for Windows, 80 MB for Linux). After signing in, the web installer can be downloaded. Running the web installer will extract the installation files (2 GB download size, 10 GB free disk space required) and automatically start the installation (see Step 2 in this instruction document).

Option 3: Download the single-file installer (11 GB) from our temporary Dropbox link

Go to https://www.dropbox.com/s/ycjzuc9fdlj71g8/Xilinx_Vivado_SDK_2016.1_0409_1.tar.gz?dl=0 and download the installation files. Follow steps 1.4 and 1.5 above to decompress the files.

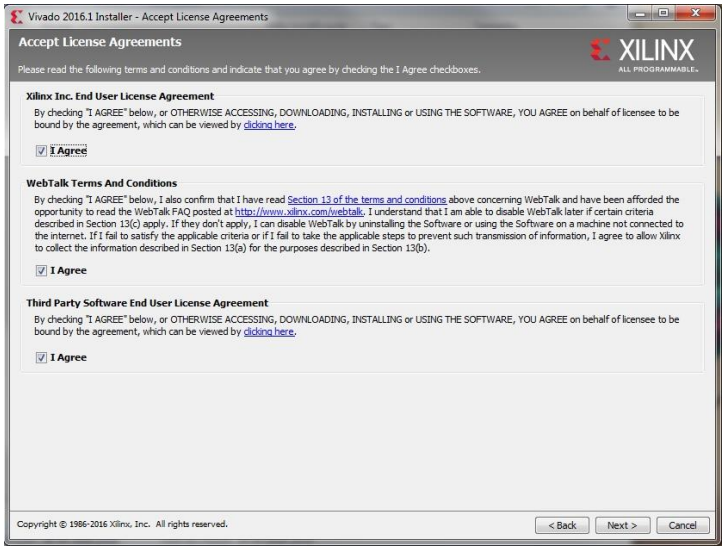
2. Install Vivado Suite 2016.1

2.1 Run "xsteup.exe" to start the installer of the Vivado Suite. The installation will take 20-30min. The first window is the Welcome window. There is nothing to do in this window so press Next.

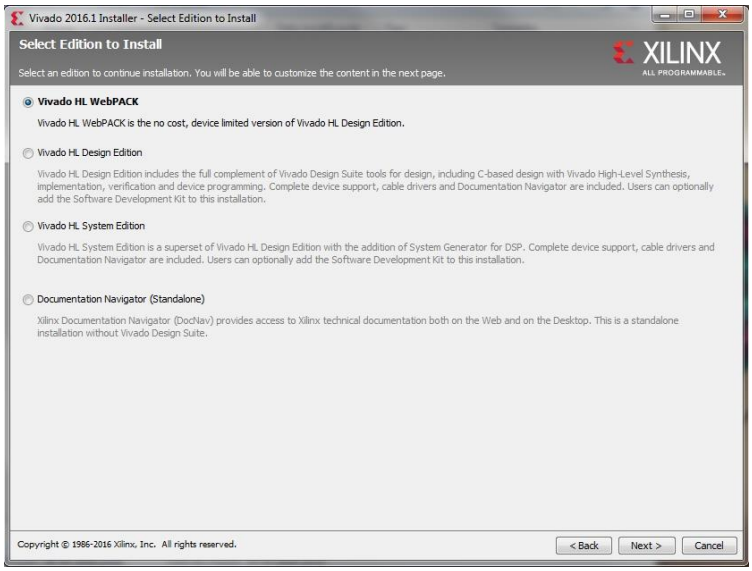


2.2 The next window is the usual License agreement. You need to agree to all 3 license agreements and conditions before you can continue by pressing Next.

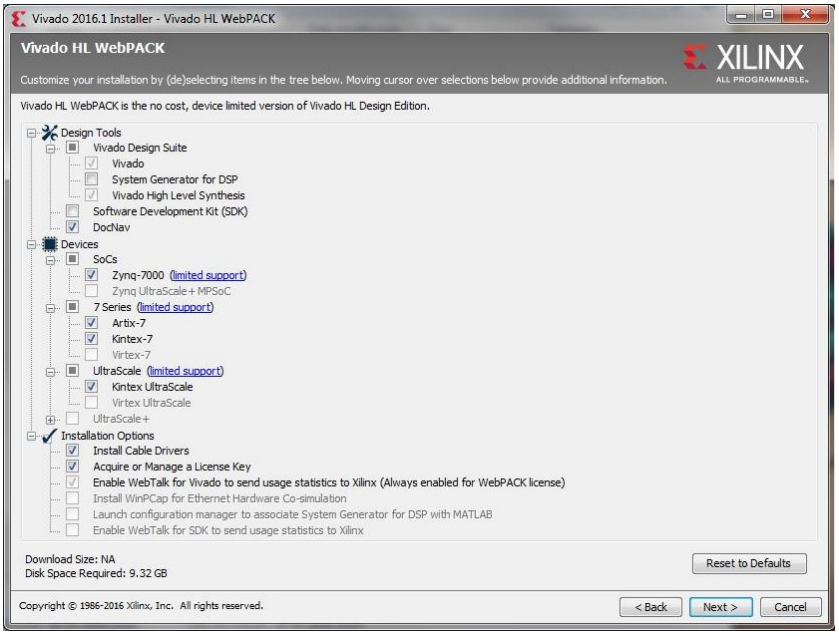
DISCLAIMER: The authors of this instruction manual advise all readers to read, within their available time, any license agreement of any software before installation and use.



2.3. The next window is the software edition selection. Select Vivado HL WebPACK as it is the only one that does not require a paid license, although it provides limited functionality. You can also deselect the Standalone Documentation Navigator if you want. This is an instruction manual of Vivado Suite and Xilinx devices, which is not required for this exercise. Once you are done with your selection press Next.



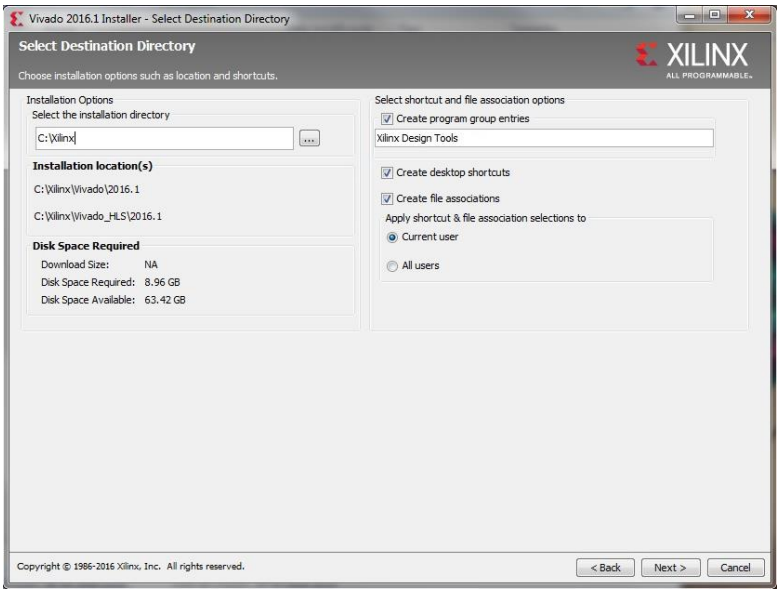
2.4 The new window is the software customization. Since you already selected the Vivado HL WebPACK edition, the standard options will be selected. For this exercise, make sure that "Devices > 7-Series > Kintex-7" is selected and do not change any other option. Press Next to continue.



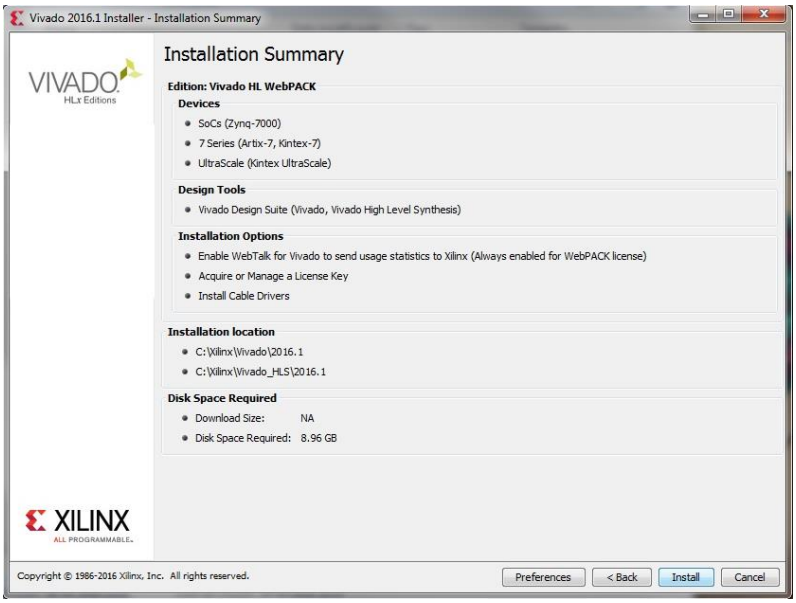
2.5 The new window is the Destination Directory Selection. Make sure the installation directory is C:\Xilinx and press Next.

WARNING: Do not select any other installation directory rather than C:\Xilinx, unless you are already well experienced with Xilinx software installations.

ADVICE: We highly recommend the creation of desktop shortcuts for easy access, but is not mandatory. "Create desktop shortcuts" is the only option you should choose whether or not to select.



2.6 The last window of the pre-installation is the Summary. Skip it by pressing Next and start the actual installation.



2.7 Close to the end of the installation process, you might see the message window below. As it states, you need to unplug from your computer any Xilinx devices and respective cables that you might have already connected before installing the drivers. Click OK to proceed.

2.8 After the installation is completed, the License Manager will open. For now, select "Start Now! 30 Day Trial (No Bitstream)" and then apply/activate. Close the window after that. This concludes the installation of the Vivado Design Suite.

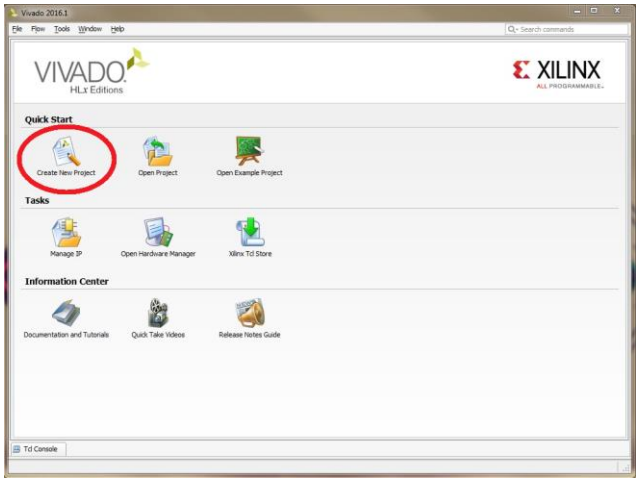
ADVICE: The 30 day trial option allows you to experiment with Vivado without the need to request a license or to create a Xilinx account (if you downloaded the installation files through our Dropbox link). Nevertheless, this option does not allow the actual programming of a physical Xilinx FPGA. For this exercise, such programming is not required, but if you wish to do so in the future you will have to acquire a free WebPACK license through Xilinx.

3. Create the Noekon project in Vivado

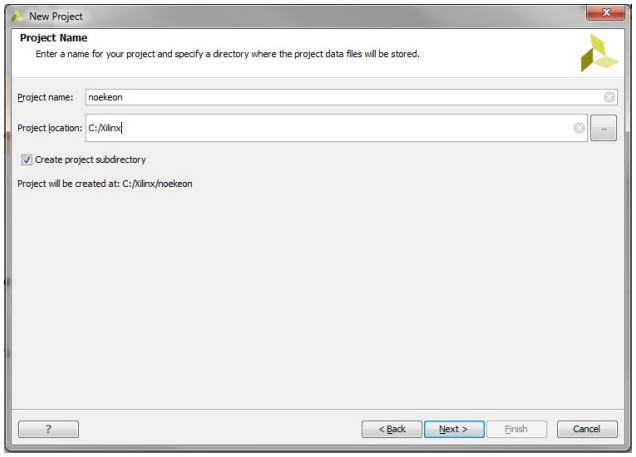
In this tutorial, we will use the Noekeon cipher as an example to explore different hardware architectures. This step explains how to create a new project in Vivado, using the basic Noekeon architecture that consists of a number of VHDL files provided through the following link: https://www.dropbox.com/s/s0s24fvf1ks4kjc/Noekeon-VHDL.zip?dl=0. More information on Noekeon can be found at http://gro.noekeon.org; especially “The reference code” on the website, containing the reference C code and some test vectors, is interesting.

3.1 Start Vivado either by clicking the Vivado 2016.1 icon on your desktop, or selecting the program from the start menu.
ADVICE: Do not confuse "Vivado 2016.1" with "Vivado HLS 2016.1". The later is a different program that we will not be using.

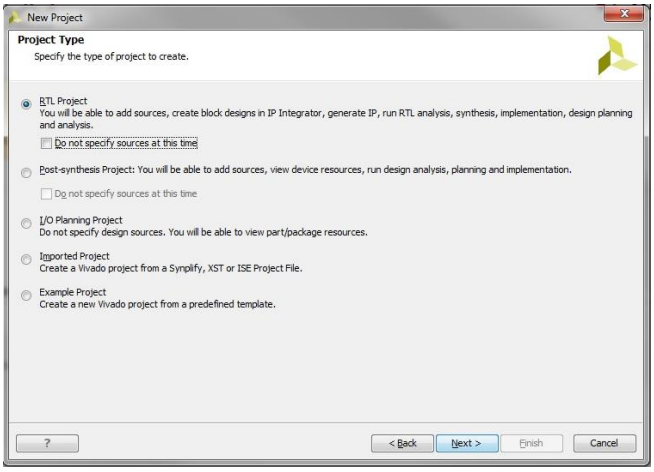
3.2 The entry menu of Vivado will open. Select "Create New Project".



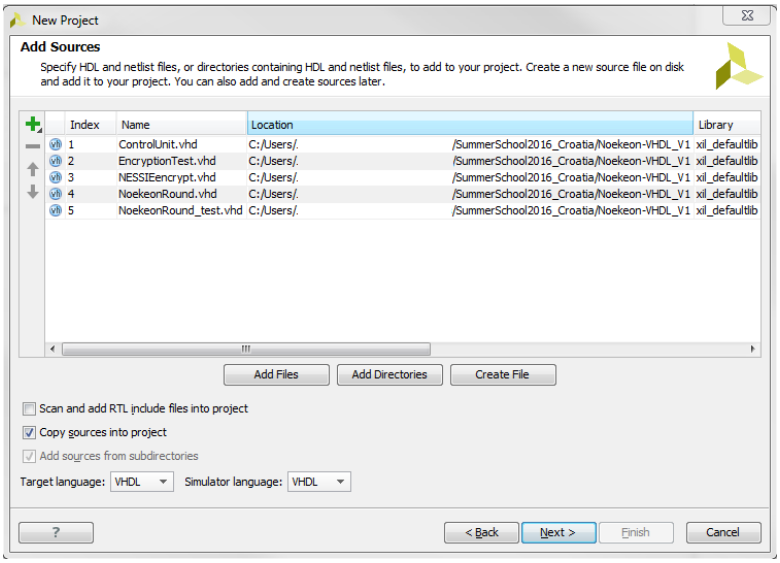
3.3 The "New Project Wizard" will open. Press Next. The following window is the Project Name. In this example, we will name the project "noekeon", but you can change it to any other name. Do not change the storage directory. Select the option to "Create project subdirectory". Press Next.



3.4 In the Project Type window, select RTL project. Press Next.



3.5 In the Add Sources window select Add Files. Proceed to search and select all ".vhd" files that were provided to you for this exercise (note that there are more files in the downloaded folder than in the screenshot below; select all files in the folder anyway). Select "Copy sources into project". Select VHDL, both in "Target" and "Simulator language". Press Next.

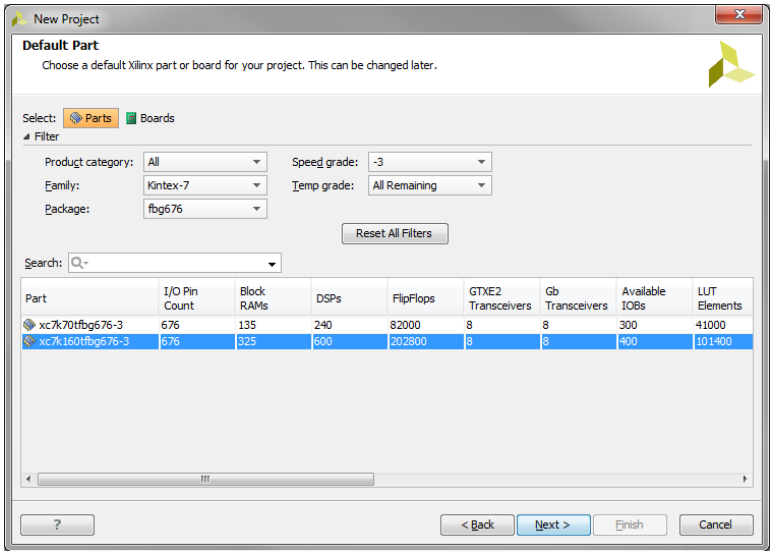


3.6 Skip the "Add Existing IP" window by selecting Next. Skip the "Add Constraints" window by selecting Next.

3.7 In the "Default Part" window, select "Parts" and input the following filters:

- "Family" → "Kintex-7"
- "Package" → "fbg676"
- "Speed grade" → "-3"

Only 2 products should be left available. Select the "xc7k160tfbg676-3" part and press Next.



3.8 You will now see the project creation summary. Press Finish to conclude the process.

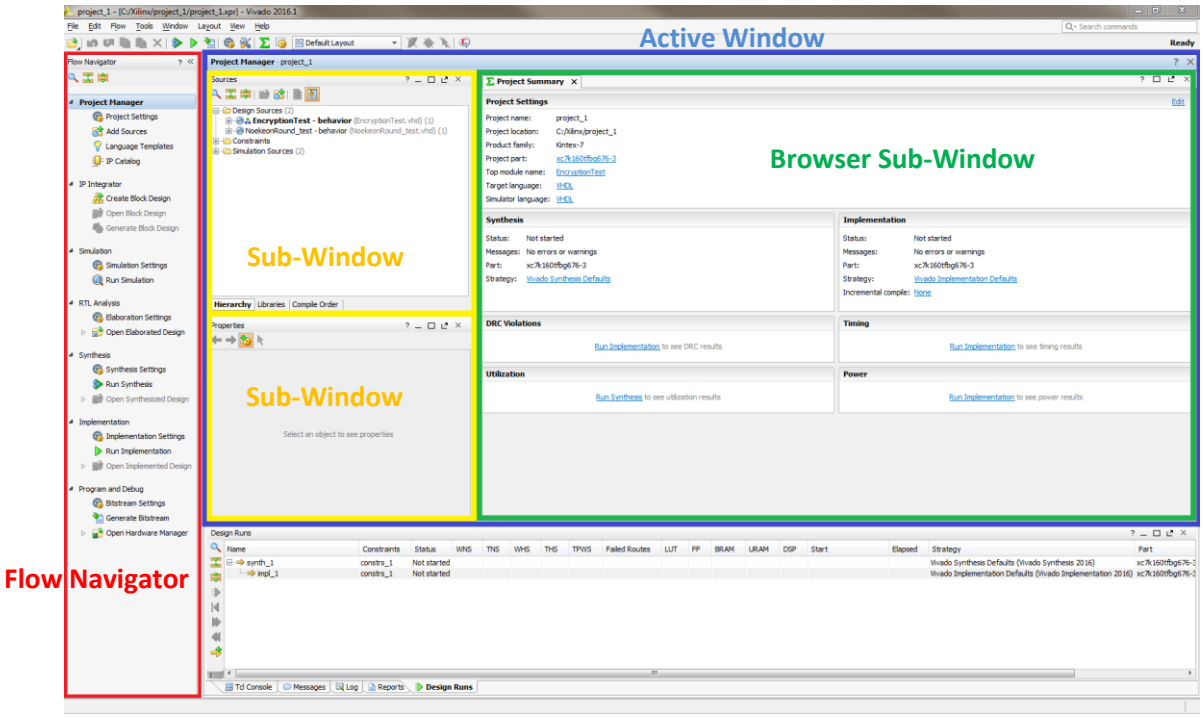
4. Implement the Noekeon architecture in Vivado

After you created the project, you are faced with the Vivado interface.

At the very left you should have the "Flow Navigator" window. In this window you can find the most common operations required for the development of an FPGA design. This window does not disappear when you proceed through the different stages of development.

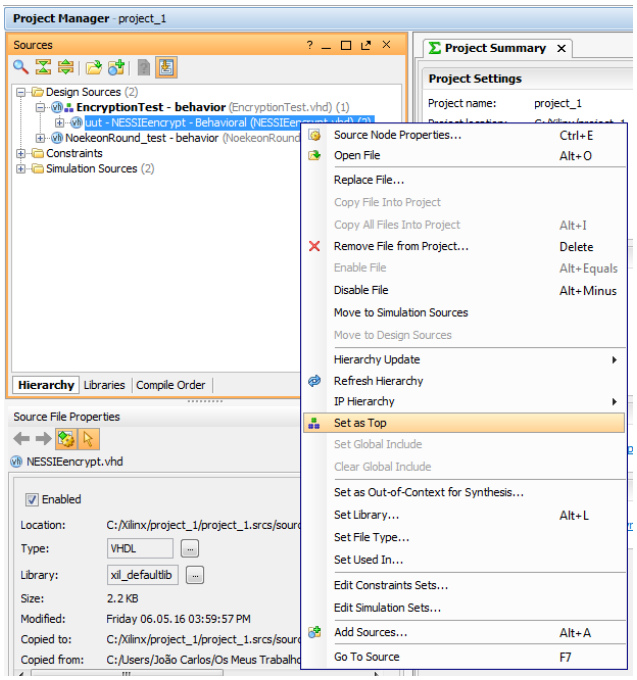
The "Active Window" is occupying the rest of the Vivado Interface, which can change depending on the stage of development. Each active window has a different layout of sub-windows and one "Browser Sub-Window" with tabs.

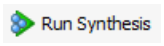
As soon as you start your project, the "Active Window" should be the "Project Manager". The "Sources" sub-window should be on the top-left. The open tab on the "Browser Sub-Window" should be "Project Summary".



4.1 First go to the "Sources" sub-window with the "Hierarchy" tab open. Expand "Design Sources" and "EncryptionTest - behavior". Within "EncryptionTest" you should find "uut - NESSIEencrypt - Behavioral". Right-click it and select "Set as top". "EncryptionTest" is the testbench we will use in Step 6 for simulation. "NESSIEencrypt" is the file that contains the description of the top architecture. When you expand "NESSIEencrypt", you can see the the hierarchical components that are contained in the top architecture.

ADVICE: the previous steps are to be done only on the "Design Sources" folder, NOT on the "Simulation Sources" folder.

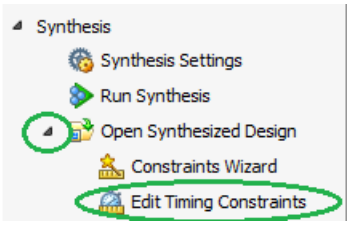


4.2 As you can see, the "Project Summary" does not have much to report because Vivado has not yet analyzed the source files. To start, select  in the "Flow Navigator" (a little waiting bar should appear at the top-rightmost corner of the Vivado window). Depending on your computer, the Synthesis process can take between 1-10min.

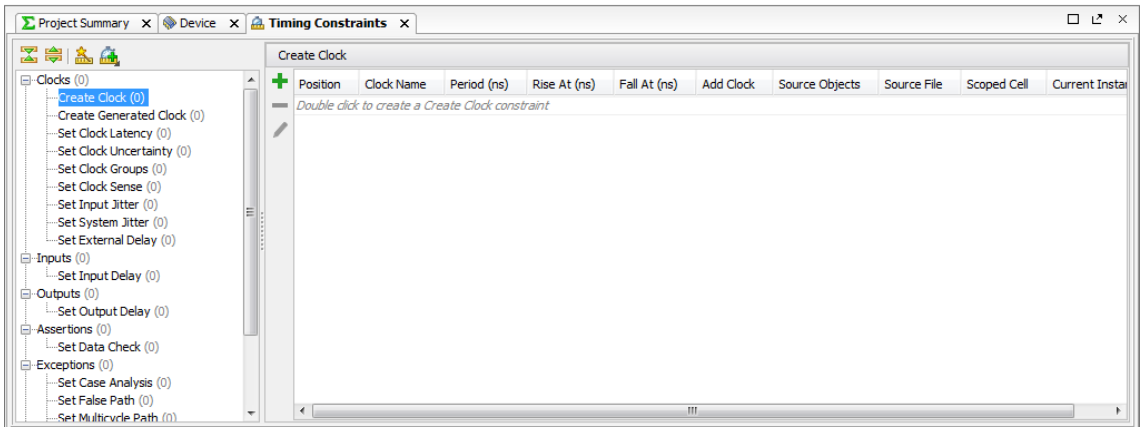
WARNING: the authors strongly advise not to cancel the synthesis process once it as started, regardless of the existence of the "Cancel" button. If you started it, let it finish.

4.3 Once the Synthesis is completed, you will see the respective dialog box. Press "Cancel" as we are not yet ready to proceed with the other given options.

4.4 In order for Vivado to perform a timing analysis on the design, we need to specify where the system clock is and how it behaves. In the "Flow Navigator", press the extensible arrow left to "Open Synthesized Design". After that, select "Edit Timing Constraints".



4.5 A new "Active Window" will open named "Synthesized Design". The tab "Timing Constrains" should also be open in the "Browser Sub-Window". Double-click on "Create Clock".

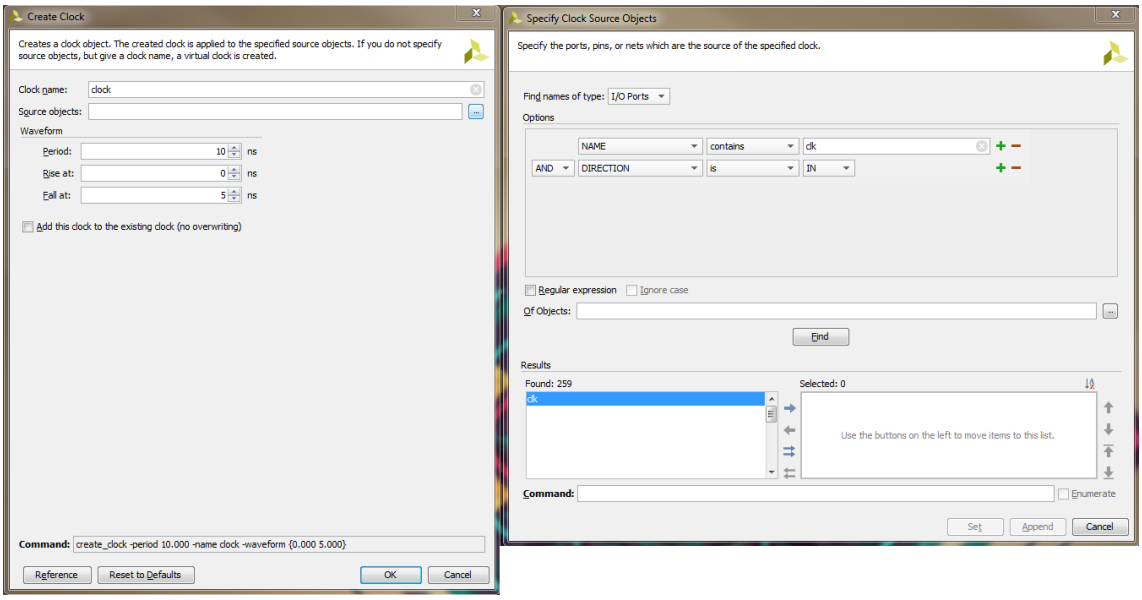


4.6 The "Create Clock" window will open. Give a name to your clock (e.g. "clock"). Select a Waveform Period of 10 ns, Rise at 0 ns and Fall at 5 ns (i.e. a duty cycle of 50%). Press the three dot button on the right side of "Source objects".

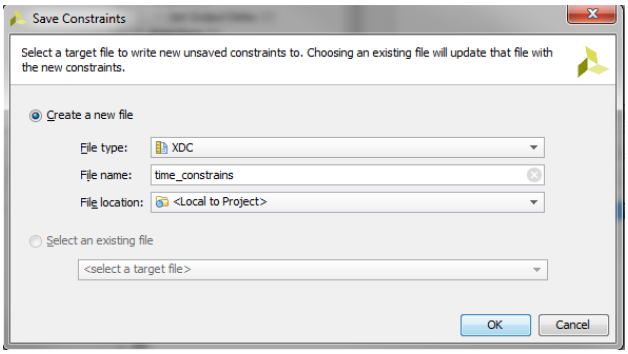
4.7 The "Specify Source Objects" window will open. Select "Find names of type: I/O Ports" and then input the following options:

	NAME	-> contains	-> clk
AND ->	DIRECTION	-> is	-> IN

Press the "Find" button. In the results, a single "clk" signal should appear in the left list (Found). Select it and then press the right arrow next to it, to include it into the right list (Selected). The Command line updates automatically. Press Set and then OK.



4.8 A 10 ns periodic clock is now considered for our design. Click the "Floppy" icon on the top left corner of Vivado to save the constraint file. If an "Out of Date Design" box appears, ignore it and click OK. Give a name to the constraint file we just created (e.g. "time_constraints") and press OK.



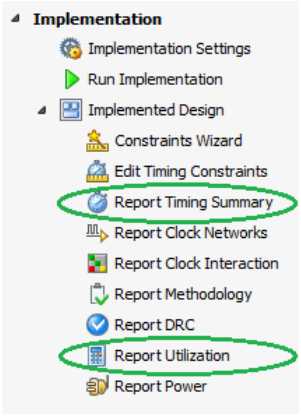
4.9 Now that the clock has been properly created, go to the "Flow Navigator" and select Run Implementation. Vivado will warn you that the Synthesis process has become out-of-date (clock was added). Select "Yes" to run Synthesis and Implementation. Once again, depending on your computer, the Synthesis and Implementation process can take a while to complete. Consult your lab supervisor only if the effect lasts more than 15min.

4.10 Once the Implementation step is completed, you will see the respective dialog box. Press "Cancel" as we do not need any of the given options. We are now ready to analyze the implementation results.

5. Analyze the Noekeon design in Vivado

5.1 In the "Flow Navigator", select "Implementation -> Report Utilization". Press OK in the window that pops up. Notice that a new tab "Utilization" appears at the very bottom of Vivado, in the bottom sub-window. In this tab, you can see the total amount of LUTs, Slices and FF Registers occupied by the implemented design.

5.2 In the "Flow Navigator" select "Implementation -> Report Timing Summary". Press OK in the window that pops up. Notice that a new tab "Timing" appears at the very bottom of Vivado. In this tab, you can see the 10 signals which take the longest to propagate.



When you analyze the "Total Delay" of the signal, you will see it is significantly lower than the clock requirement. So 10 ns (100 Mhz) is not the minimum clock period (maximum frequency) the circuit can handle. In Vivado, in order to discover the minimum clock period you need to iterate the clock period value as follows.

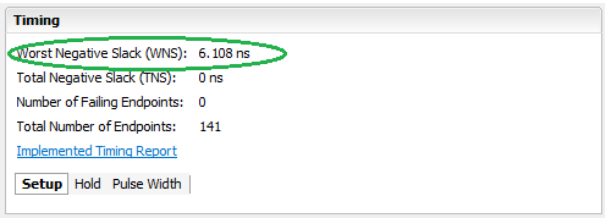
5.2.1 In the "Flow Navigator", go back to "Implementation -> Edit Timing Constrains" and change the clock period to the closest approximation of the largest total delay you found.

5.2.2 Repeat "Implementation -> Run Implementation".

5.2.3 Select "Implementation -> Report Timing Summary" and recheck the total delay values.

5.2.4 Repeat 5.2.1 to 5.2.3.

The purpose of this iteration is to reach the minimum clock period, while keeping the "Worst Negative Slack (WNS)" value positive. You can check the WNS value in the "Project Summary" tab after "Implementation". If the clock period becomes too small, then the WNS value will become negative, which means you have overclocked the design and certain signals will no longer process correctly.



6. Simulate the design

6.1 In order to simulate the functionality of the design (e.g. for debugging), go to the "Flow Navigator" and click on "Run Simulation". Select the option "Run Behavioral Simulation". This will run the testbench "EncryptionTest". After processing, the "Active Window" will change to the simulation environment and the "Browser Sub-Window" will have a tab with the waveform simulation. Using the zoom icons, zoom out until you see the oscillation of the "clk" signal. When you take a careful look at the waveforms, you can see that the testbench implements 3 tests (which can also be found in "NoekeonTestVectors.txt" in the reference code folder on the Noekeon webpage; note that we use the Noekeon cipher in direct-key mode). Each test starts when the "start" input is triggered and ends when the "done" output is high. For each test, different 128-bit values are used for "a_in" and "Key". The corresponding output "a_out" is valid when "done" is high.