# 周报：2011-03-24

07300720419 蒋菁

**本周已完成工作：**

 首先，我认真研读了SASEBO实验板附带的说明文档，主要关注的是实验板系统的构成、初始化配置模式和板上接口、开关、指示灯的用途。SASEBO-GII和核心是两块Xilinx FPGA（Spartan-3A & Virtex-5），其中Virtex完成数据的加密运算的工作，而Spartan负责控制数据流在板上的路径以及协调各部件的工作。两块FPGA各配有一块Flash ROM，作用是存储配置信息的镜像文件（\*.mcs），在对FPGA编程时需先将镜像文件下载到ROM中，再由ROM对FPGA编程。



图1 实验板模块框图

 接下来是对实验板进行最简单的配置，使其完成基本的加密运算。安装完成必要的应用程序（Xilinx ISE Webpack）及数据线驱动（FDTI D2XX Driver）后，将USB数据线和并行数据线连接到板上，电源设置为USB供电（SW1）和内部提供FPGA核心电压（SW2）。打开iMPACT，通过边界扫描确定待机芯片（Initialize Chain），选择SASEBO实验板附带的实验用数据包中的位流文件（\*.bit）和配置文件（\*.mcs），选择正确的ROM型号（45DB16D），即写入数据并编程。出现提示成功信息（Programming Succeeded）后，运行附带的加密程序（SASEBO\_Checker\_AES），按下Start按钮后程序自动输入设定数量（1000）的随机数据，并接收经过密钥加密的密文。



图2 配置成功提示



图3 加密程序

**遇到的问题：**

 首先发现了说明文档中存在的小错误，例如连接Virtex-5的并行数据端口应是CN4，而文档中写的是CN3。其实板上的标记已指出CN7和CN4的功能是config，CN3的功能是SPI-ROM，因此能容易地纠正此错误。

 主要的困难是无法正确配置FPGA，这几乎耽误了本周工作的一大半时间。根据文档QuickStartGuide的提示，应分别向Spartan和Virtex的ROM下载sasebo\_gii\_ctrl.mcs和sasebo\_aes\_comp\_lx50.mcs（文档中为sasebo\_aes\_comp\_lx30.mcs，已纠正），而数据包的根目录下就包含了这两个文件，所以我反复尝试将这两个文件下载到ROM中。结果Spartan的ROM能接受而Virtex的ROM却不能，实际上是Virtex不能接受ROM的Programming，提示为“DONE did not go high”，意思是表示config\_done的LED指示灯没有亮，反复尝试多次仍无果。期间我甚至怀疑指导文档又出了差错，于是尝试更改JUMP和DIP的设置，都导致设备无法识别（too many unknown device）。张跃军指出配置FPGA不仅需要mcs文件，还需要bit文件，但是他只能找到位于sasebo\_gii\_aes\_comp和sasebo\_gii\_des文件夹中已有的bit文件，因此能对Virtex正确编程而无法对Spartan编程。我发现，在sasebo\_gii\_ctrl、sasebo\_gii\_aes\_comp、sasebo\_gii\_des等包含需下载到板上数据的文件夹中，都有后缀为ise的文件，能由Xilinx ISE打开为工程，其中手动添加同目录下的\*.v文件后进行综合（Implement Top Module），生成的文件中找到\*.bit文件，下载到板上编程成功。



图4 “DONE did not go high”

 文档中指出可通过指示灯的状态判断配置是否成功，其中LED1亮表示电源正常，LED2、LED11亮表示FPGA被正确编程。我发现，最初上电时（还未做任何编程工作），LED11已经亮起，对Spartan编程后LED11如预想点亮；Virtex未成功编程时LED2不亮，成功编程后点亮。由于安全因素，在更换编程对象芯片时，我将USB（电源）和并行数据线与PC端断开，更换插口后发现，LED11仍保持点亮，而即使LED2原来已点亮，重新上电后不能恢复原状。FPGA是在线储存信息的芯片，掉电后信息全部丢失；而Flash ROM是掉电后仍能储存信息的芯片，因此往往FPGA芯片组设定系统上电时FPGA自动从ROM中载入配置数据，从外部看来好像FPGA也能断电保存信息一样。事实上，按下Spartan和Virtex对应的config\_reset键，LED11仍点亮而LED2熄灭，作用和断电相同。



**LED2**

**LED11**

**LED1**

图5 Virtex未配置成功情形



**LED11**

**LED2**

**LED1**

图6 Virtex配置成功情形

 为了直接判断FPGA是否能够正常工作，运行SASEBO\_Checker\_AES.exe，点击Start，发现上电后（或按下config\_reset后）若未做任何动作或仅对Spartan编程，则程序不能运行；仅对Virtex编程，程序能够正常运行。这种现象似乎是Spartan能保存配置信息而Virtex不能，但是原因不明。

 最后，为了更加全面地了解实验板的各种功能，获得板上的指示灯、开关、接口等的意义及用途是十分必要的，但是目前仍未获得足够的书面材料支持。

下周工作任务：

 数据包提供的密钥程序仅提供自动生成的明文和密钥，且密文无法保存，因此需要编写一个能从指定位置（键盘或文件）输入数据，自由设定密钥，且能保存输出的密文的程序，使用C语言编写。另外，使用示波器观察实验板的电源波形，使用MATLAB分析波形并进行统计分析，试图破解密钥。