关于获取波形：

以示波器Agilent DSO1024A为例介绍了怎样从AES电路获取功耗波形，并且将波形的相关信息存储至PC。

首先在FTDI VCP/D2XX driver, Microsoft .NET Framework 3.5, and National Instruments NI-VISA 4.6.2.的环境下安装“Setup.msi”

第二步：configuration

把控制电路的二进制编码文件sasebo\_gii\_ctrl.mcs下载到Spartan-3A

把AES电路下载到Virtex-5

三．配置SW7，至工作频率为2MHz （SW7不同的配置对应不同的工作频率）



四．根据要求连接板子，PC和示波器

板子、示波器—>PC: USB

1. 探针：Channel 1: TP2 (GND to TP5)
 Channel 2: 1st pin of J6 (GND to the brace on the corner)．



TP5

GND

J6

TP2

五．然后打开板子和示波器，打开SASEBO的获取波形软件

When the oscilloscope DSO1024A is recognized by the program, USB0:XXXX…” is displayed on the “Oscilloscope” box as shown in Fig. 5. If DSO 1024 A is not recognized, a message “Oscilloscope is not ready!” is displayed.



六．根据用户环境设置参数：X和Y的量程和偏移等。例如：

XOffset: 2.8E-06

XRange: \_500ns

YOffset: -1.03

YRange: \_5mV

然后按“single”检查这些设置是否符合获取波形

七．开始获取波形，最终存储在“\Users\[user]\MyDocuments\SASEBO\_Aquisition\wf\_gii\_yyyy\_MM\_dd\_HHmmss”

关于获取波形的编程指南：

基于MVC的结构（Model, View, Control）

Model: 包括示波器模型和波形模型

View对应用户界面

Control控制功能：在适当的时间开始解密，重复一定次数，获取解密结果



SASEBO\_GII\_AES\_rev1

由SASEBOBaseModule提供基本功能，相当于一块真实的SASEBO板子。

初始化

void ISASEBO.init(SASEBOCore core, Mode mode, Key key)

void ISASEBO.init(SASEBOCore core, Mode mode, Key key, SASEBOParam param)

—>执行

void ISASEBO.execute(byte[] input, byte[] output)

byte[] ISASEBO.execute(byte[] input) —>完成