Final Project Requirement

Balance You

2020/12/10

PUF security
an eMemory Company

IPR Notice

Date : 1/7/2021

Report time: 20-25 mins

1 **Final Project Task**

2 **Project Content**

3 **Tips**

PUF security
an eMemory Company

Task – Pre-work

- Build an environment for NIST statistical test suite
  - Virtual machine with Ubuntu OS
- Download the test suite
  - Test Suite
  - Read README.md and Chapter 5 in NIST SP800-22 document to learn how to use the suite
- Study the document of NIST SP800-22 to know
  - Proper Input data size
  - Proper setting for parameters

Task – Input Data Size and Parameters Setting

- Input data size
  - Check the Input Size Recommendation in each test in Chapter 2
  - Check Chapter 4.2.2

- Parameters Setting
  - Check the Input Size Recommendation in each test in Chapter 2

- Check Chapter 4.3 (d) and (f)

Task – Analyze TRNG data with Test Suite

- Collect TRNG data with 100*Y*X bits
  - X: size of a bitstream(sequence)
    *should satisfy the minimum size for all test
  - Y: number of bitstreams(sequences)

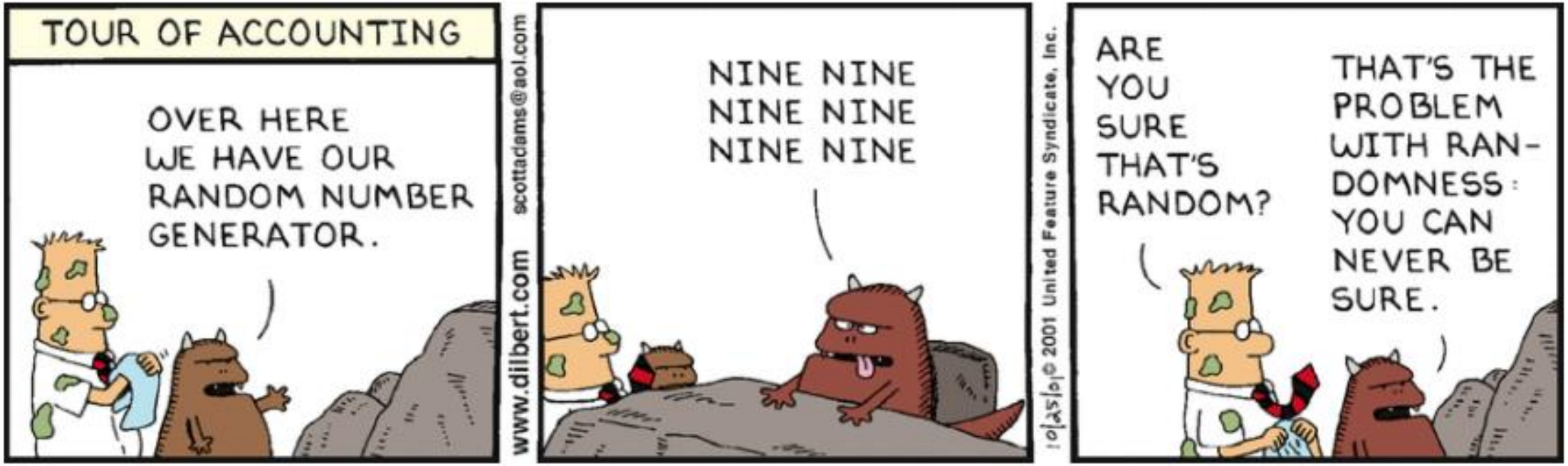
  - You should at least get 100 files with Y*X bits of random number in each file

- Analyze these files with test suite and check the pass rate
  - Compare your pass rate with the ideal one and the pass rate in Table III in the paper:https://ieeexplore.ieee.org/document/7016926

Project content

- How do you choose your input data size and parameter setting?
- What is the pass rate of your 100 random number files?
- Observing “finalAnalysisReport.txt”, find which test fails mostly
  - Try to explain with the result of test and the paper below
    “Study on the Pass Rate of NIST SP800-22 Statistical Test Suite*”*
- How do you judge the TRNG you used in this course?
  - Under the knowledge of “null hypothesis” (NIST document Chapter 1) and the paper you studied

Random?



https://dilbert.com/strip/2001-10-25

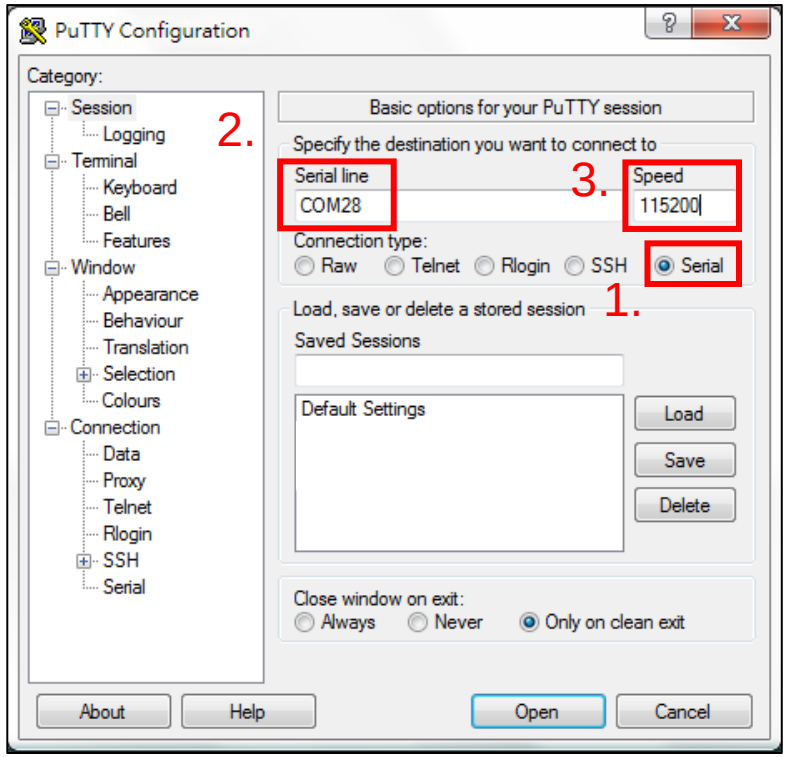
PUF security
an eMemory Company

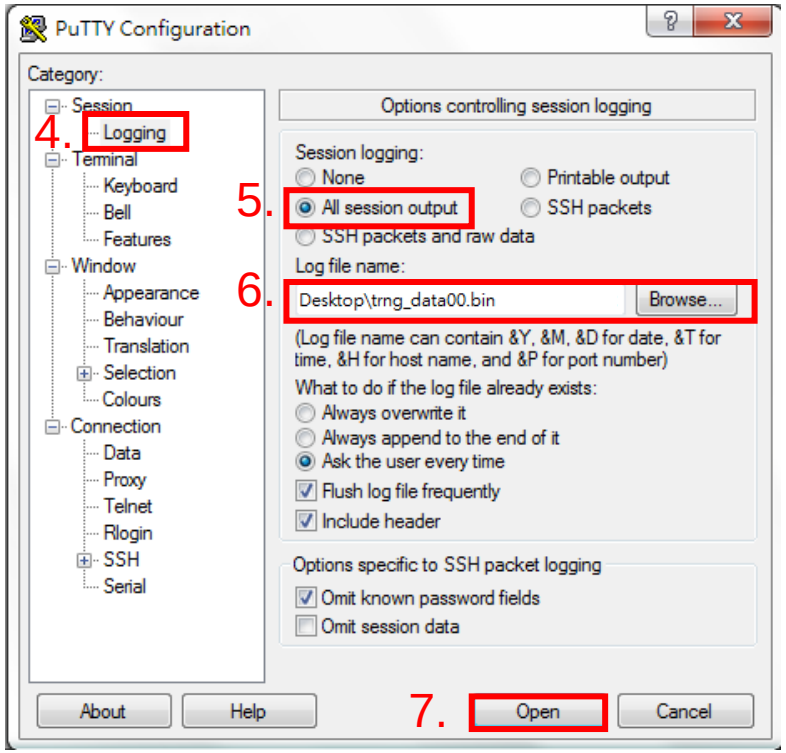
Tips – Store data into file with PUTTY (1/3)

- To accelerate data collection, you can change the baud rate of DUE from “9600” to “115200”
- Output the 8-bit random umber (outputdata) in binary format:
  - Serial.write((outputdata&0xFF));
- Program your code for RN collection into the DUE w/o testchip and open serial monitor to check the operation
- Keep pressing “Reset” button on DUE and setting PUTTY to store data into file
- PUTTY download:
  - https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Tips – Store data into file with PUTTY (2/3)

- Close serial monitor
- Set PUTTY with DUE port



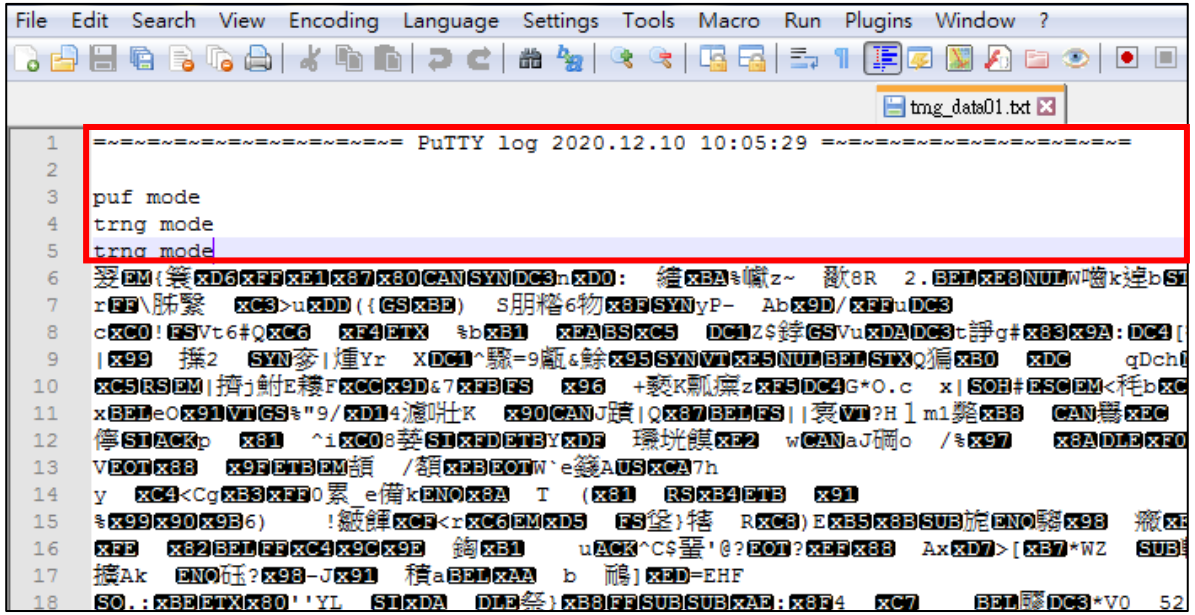


File name:
XXX.bin

8. Release
Reset button

Tips – Store data into file with PUTTY (3/3)

- Delete the header and debug message from the data file



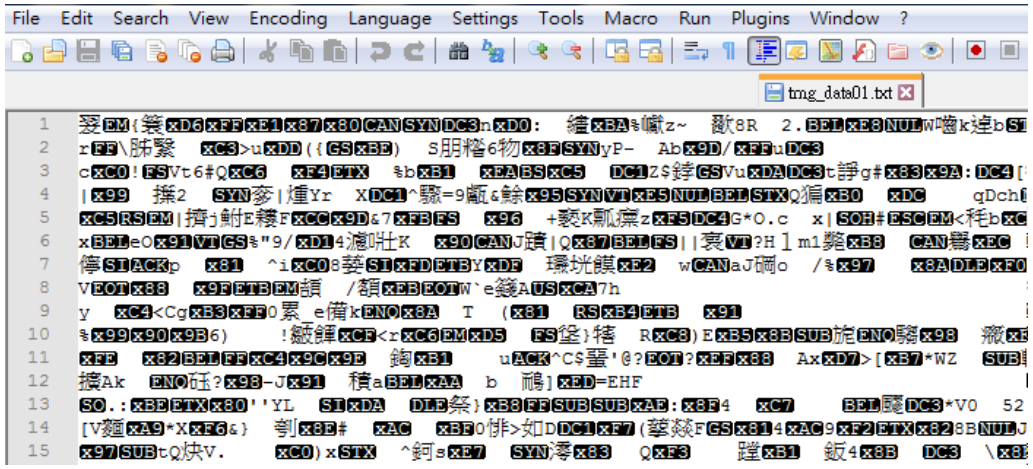
PUF security an eMemory Company

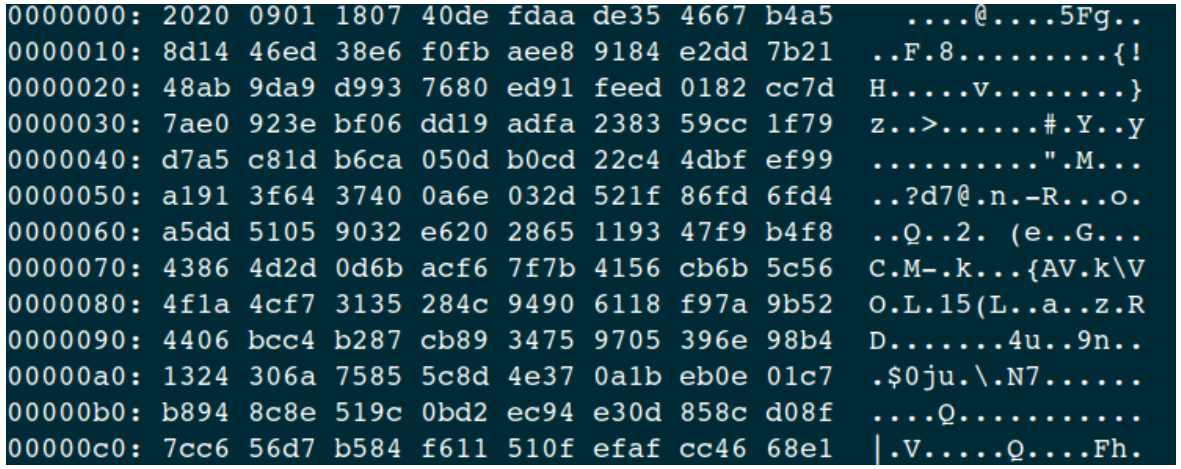
Tips – Others (1/2)

- Virtual Machine with Ubuntu
  - Vmwave: https://www.kjnotes.com/linux/18
  - Virtualbox: https://www.kjnotes.com/linux/29
- You can transfer data files from your OS to virtual machine by:
  - Share folder (google the key word with your virtual machine software)
  - Internet

Tips – Others (2/2)

- Use “xxd” command on Ubuntu to check your data.bin file
  - xxd data.bin |less





THANK YOU

PUF security

Secure the connected world

PUF security
an eMemory Company