Research report

Side channel attack

David Zashkolny

During the preparation I have done the next parts:

Organizational part:

* met with the mentors in Telegram
* joined github and copied the project

https://github.com/rnd4u-org/2019-knu-sca

Part1 mathematical:

* Learned block ciphers such DES, DES-3 and AES:

- [https://www.crypto101.io](https://www.crypto101.io/) section 6, ‘Block Ciphers’

- <https://en.wikipedia.org/wiki/Data_Encryption_Standard>

- <https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

- <https://habr.com/ru/post/112733/>

- <https://eprint.iacr.org/2002/157> read article **In How Many Ways Can You Write Rijndael** in order to better understand AES

* Learned some base technologies of machine learning such classifiers.
* Learned side-channel attacks such simple power analysis (SPA), differential power analysis (DPA) and correlation power analysis (CPA):

- <https://www.tandfonline.com/doi/pdf/10.1080/23742917.2016.1231523>

- <https://en.wikipedia.org/wiki/Power_analysis>

* Found some articles about existing attacks for DPA and CPA on the eprint.iarc.org

Part 2 investigate Jupyter:

* installed jupyter on my operation system
* investigated how to use the virtual environment in python
* created demonstration program

Part 2 practice Python:

* Ivestigated Pycryptodome.
* Investigated Numpy (in particular numpy.linalg and numpy.fft).
* Investigated some potentiality of Scipy.
* Investigated matplotlib.pyplot.
* Create some test programs with demonstration of AES and RSA using pycryptodome.
* Create simple program that generates some signal and cleans it from noise.
* Create presentation in Jupyter with previous programs.