Specifications for RSA Efficiency Research

George Wood

Last Modified: 3/7/2018

1 Misc. Hardware Info

1. Raspberry Pi
   - Use Raspbian OS
   - There may be implementation issues with Raspbian.
2. Arduino
   - Will probably melt.
3. Build hardware list, priority on RAM, processor, OS, and possibly GPU.

2 RSA Specs

1. Don't worry about randomness - data will be pre-generated and consistent across trials.
2. Don't worry about padding for same reason
3. Use data of sizes: 64B, 1kB, 32kB, 64kB, 128kB, 1MB
4. Use keys of size: 512b, 1024b, 2048b, 4096b

3 Measurements

1. Power consumption
   - Kill-A-Watt for physical measurements
   - Software such as MS's Joulemeter
2. Cache/RAM IO Speed (Transfers/second)
   - Determined largely by RAM, info released by manufacturers
3. Keep track of RAM usage and CPU usage

4 To-Dos/Deadlines

1. Deadlines
    - Thursday, 3/8/2018: Kill-A-Watt arrives, configure and test.
    - Sunday, 3/11/2018: Complete UI for performing tests/collecting data.
    - Monday, 3/12/2018 - Tuesday, 3/13/2018: Perform tests and collect data on all available machines.
    - Friday, 3/16/2018: Complete preliminary organization of all data collected up to this point.
    - Friday, 3/30/2018 - Saturday, 3/31/2018: Perform tests and collect data on all remaining machines.
    - Tuesday, 4/3/2018: Complete remaining organization of all data. Perform and record statistical analysis of data.
    - Thursday, 4/5/2018: Complete first draft of paper.

5 Etc

1. Other Papers
    - Wyatt Yost
    - Thomas Graves