Timing Side Channel Reporting Tool

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

TECHNISCHE FAKULTÄT

February 2, 2012

Contents

List of Figures

1. Results unfiltered

In this chapter the report shows the unfiltered timing measurements. For graphic analysis, the reporting tool uses several types of graphics. These graphics visualize the differences between the timing measurements of the different secrets. The reporting tool helps to analyze the results of a timing measurement by displaying the results in an accessible way.

1.1. Unfiltered Plots, sorted by secret:

1.1.1. Scatterplot

A point in this graphic represents a measured time of a secret. The Y-axis denotes the timing value and the X-axis the n^{th} measurement. Because the measurements are shown in the order they were measured, this representation allows the detection of temporal disturbances during the measurements. Take an example where the timing values suddenly plunge during the measurements, which may result in a bad data set. Another example is when the variance of the measurement changes during the measurements. Both examples can be detected quite well in a scatterplot.

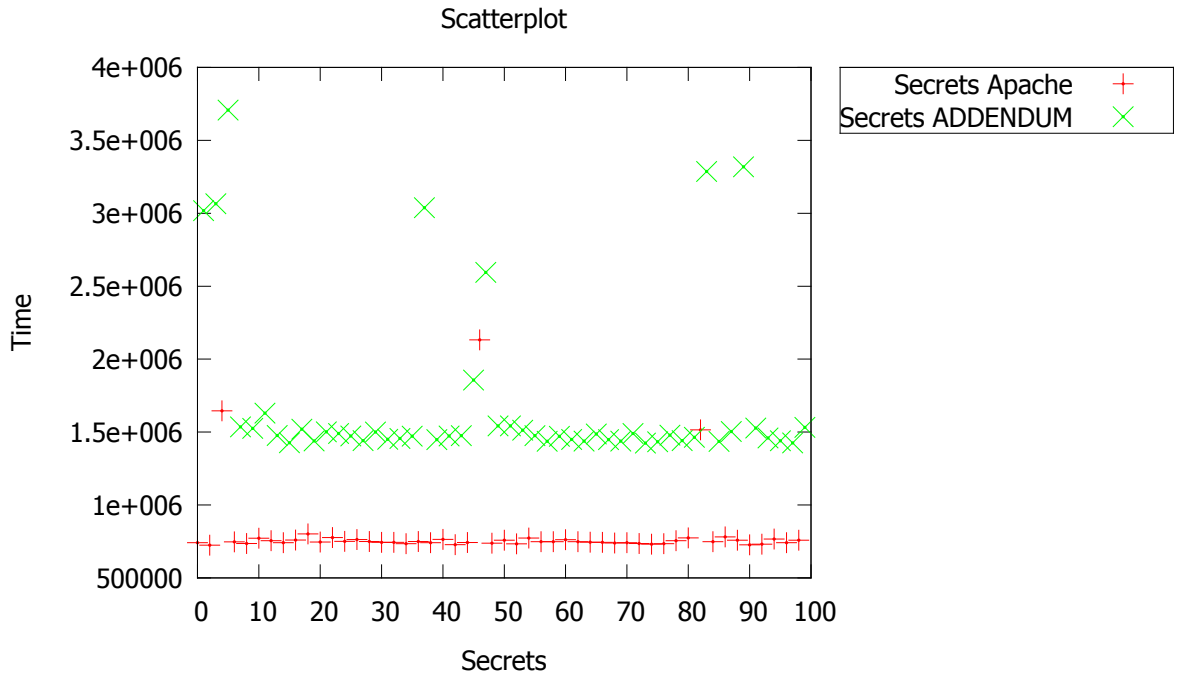

Figure 1.1.: Scatterplot

1.1.2. Whisker Diagram

This *whisker* (also called *Box-Plot*) diagram illustrates three values that provide a good summary on the data set. It shows the upper quartile, the lower quartile, and the median. Given a data set with a reasonable amount of measurements and good quality, this diagram will probably already hint whether or not there are significant timing differences. Note that we do not show the minimum and maximum timing values here, because they tend to have many outliers.

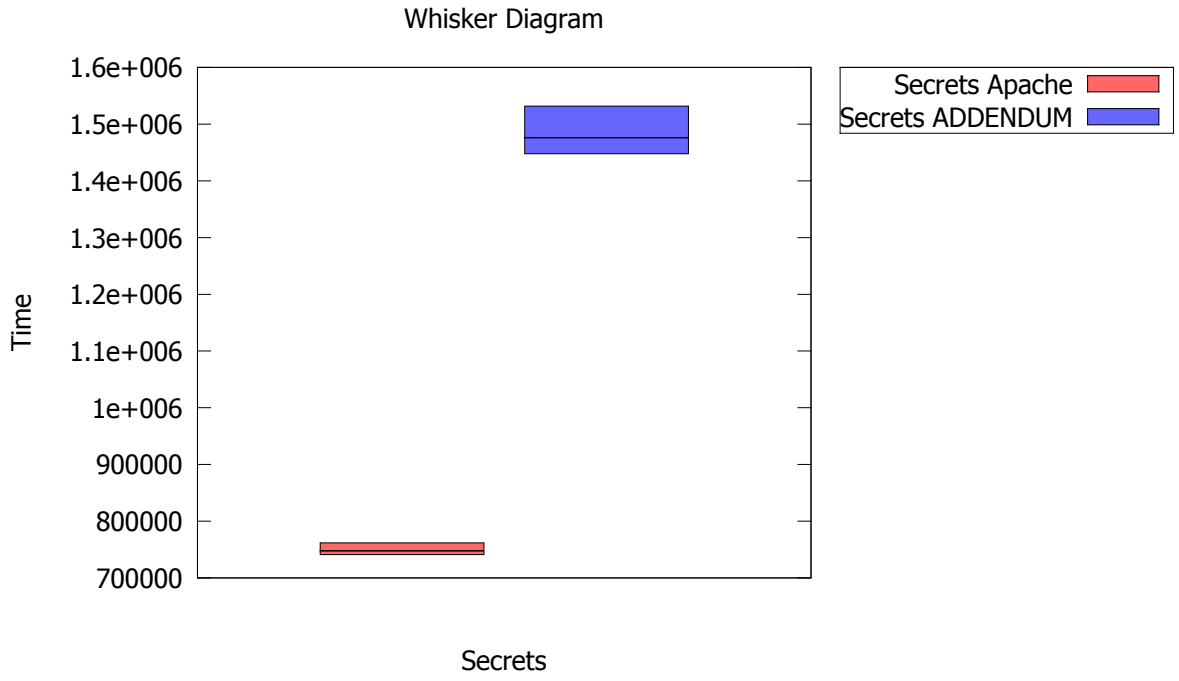

Figure 1.2.: Whisker Diagram

1.1.3. Cumulative Distribution Function

A *CDF (Cumulative Distribution Function)* diagram displays the distribution of the different data sets.

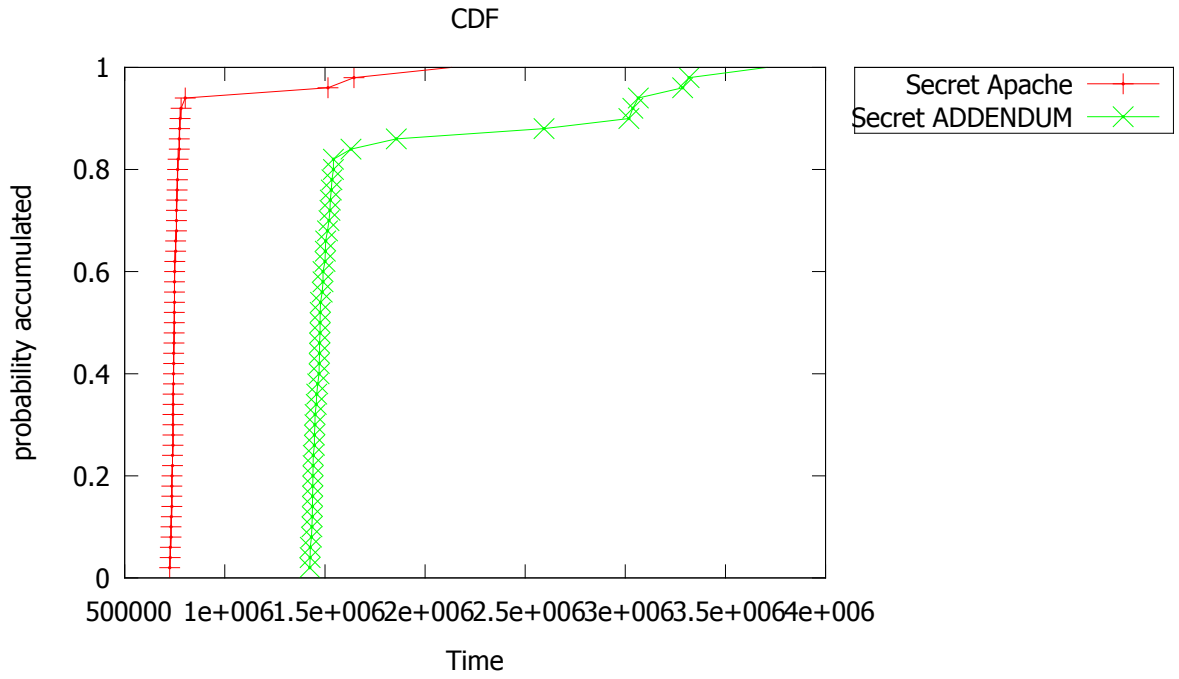

Figure 1.3.: CDF

1.1.4. Histogram

A *Histogram* shows the distribution of the different data sets.

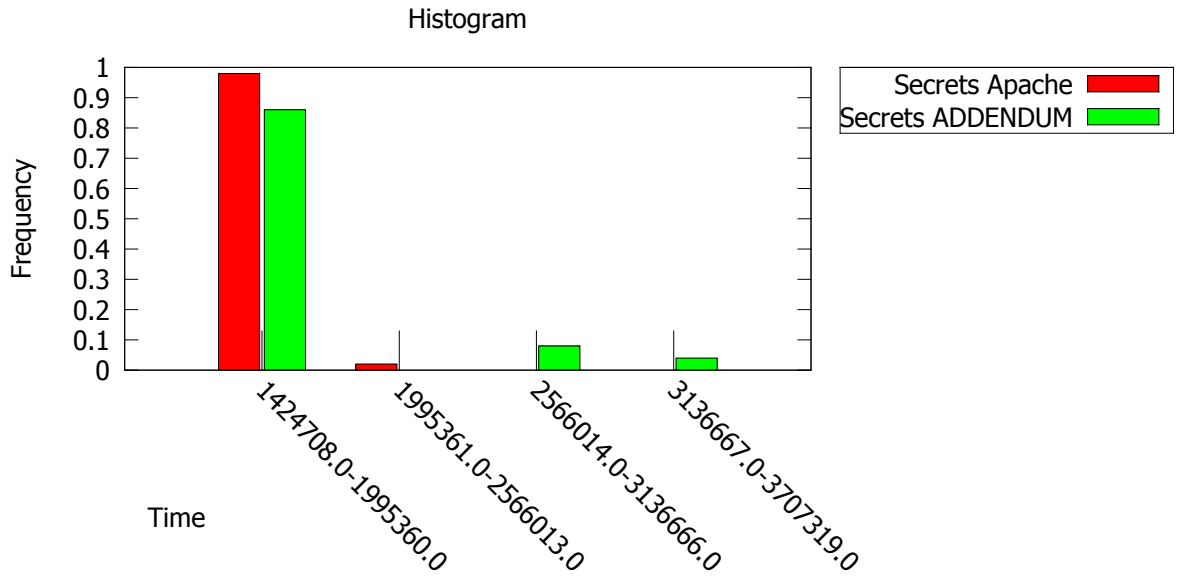

Figure 1.4.: Histogram

1.1.5. Secrets in Detail

Summary

2. Results filtered

2.1. Statistical Evaluation

2.2. Filtered Scatterplot

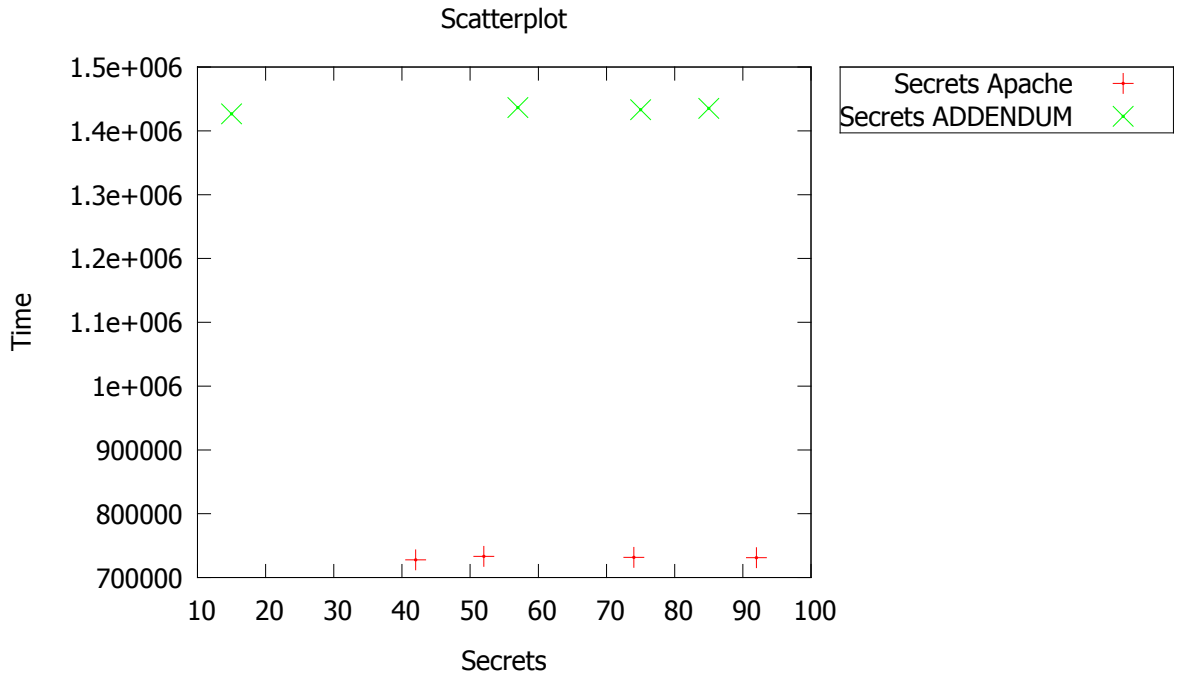

Figure 2.1.: Filtered Scatterplot

2.3. Filtered Whisker Diagram

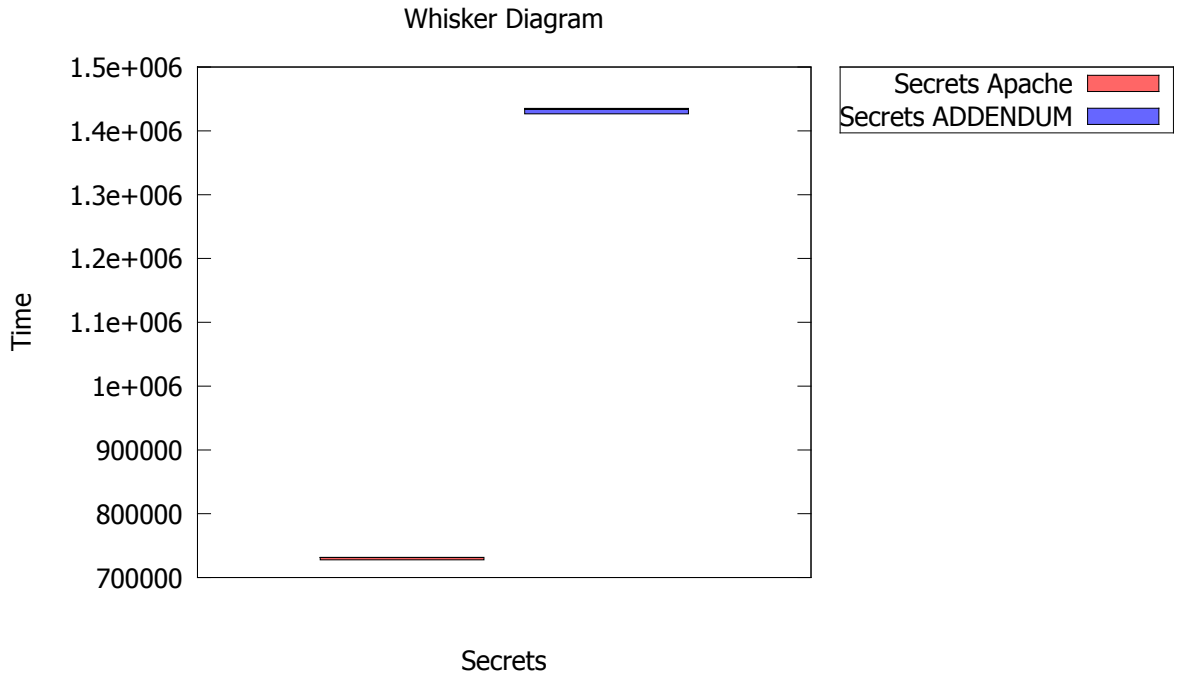

Figure 2.2.: Filtered Whisker Diagram

2.4. Filtered CDF

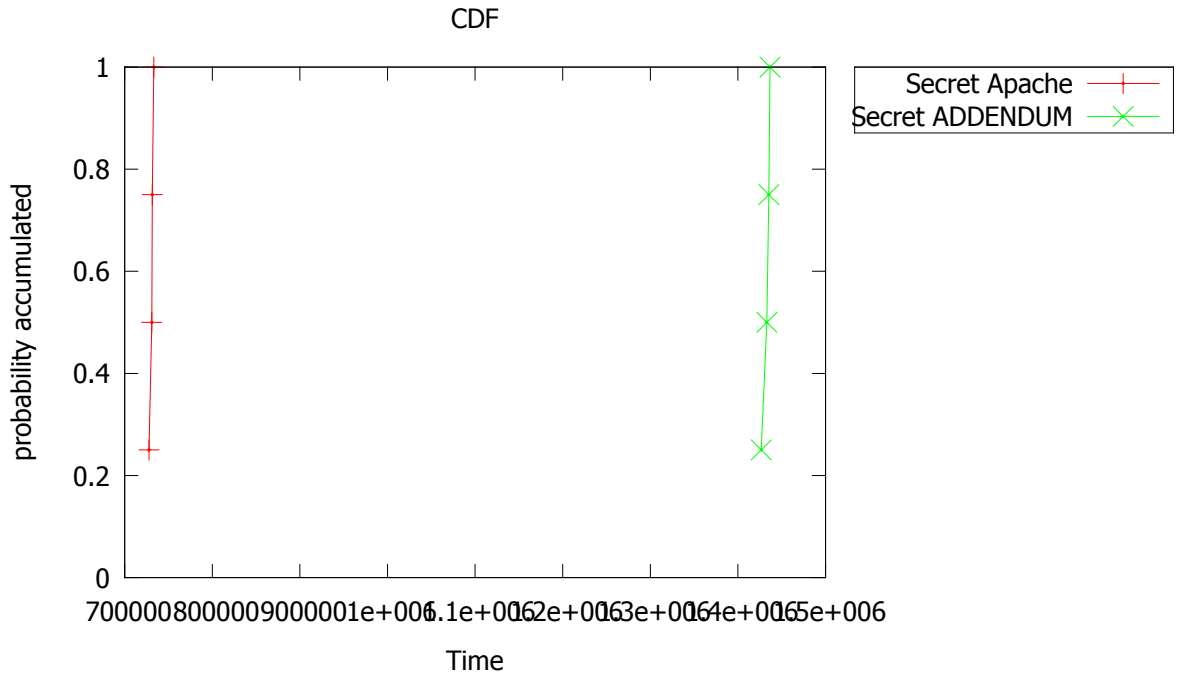

Figure 2.3.: Filtered CDF

2.5. Filtered Histogram

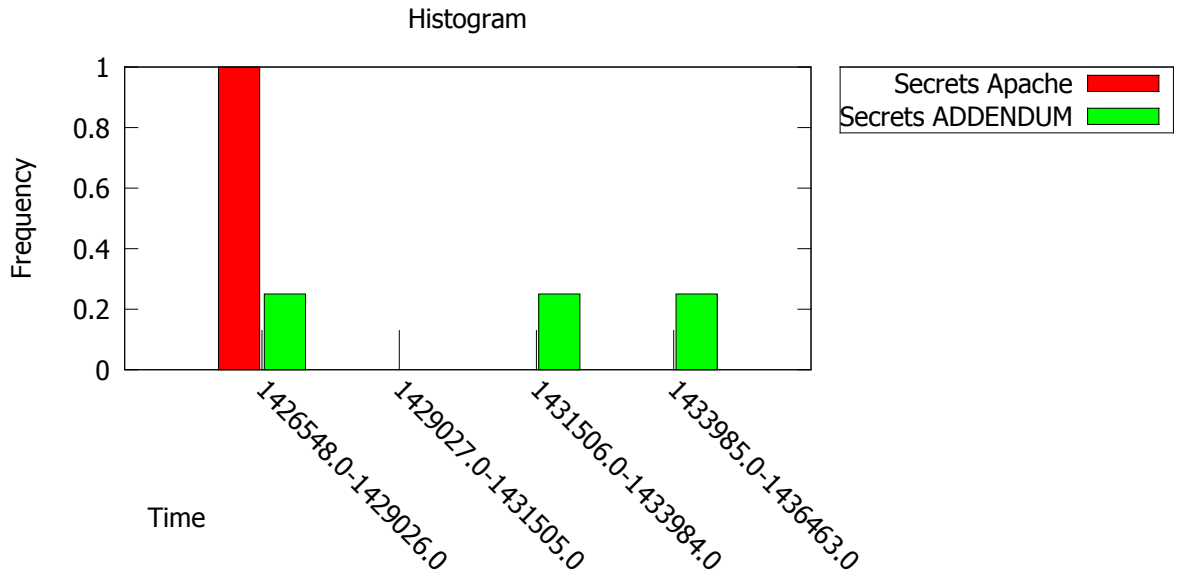

Figure 2.4.: Filtered Histogram

3. Measurement

3.1. Table

Demo-Example1

Secret	Amount Measurement	MIN	MAX	Median	AVG
Apache	50	725063	2132263	747837	810565
ADDENDUM	50	1424708	3707322	1476127	1718263

A. Scatterplot

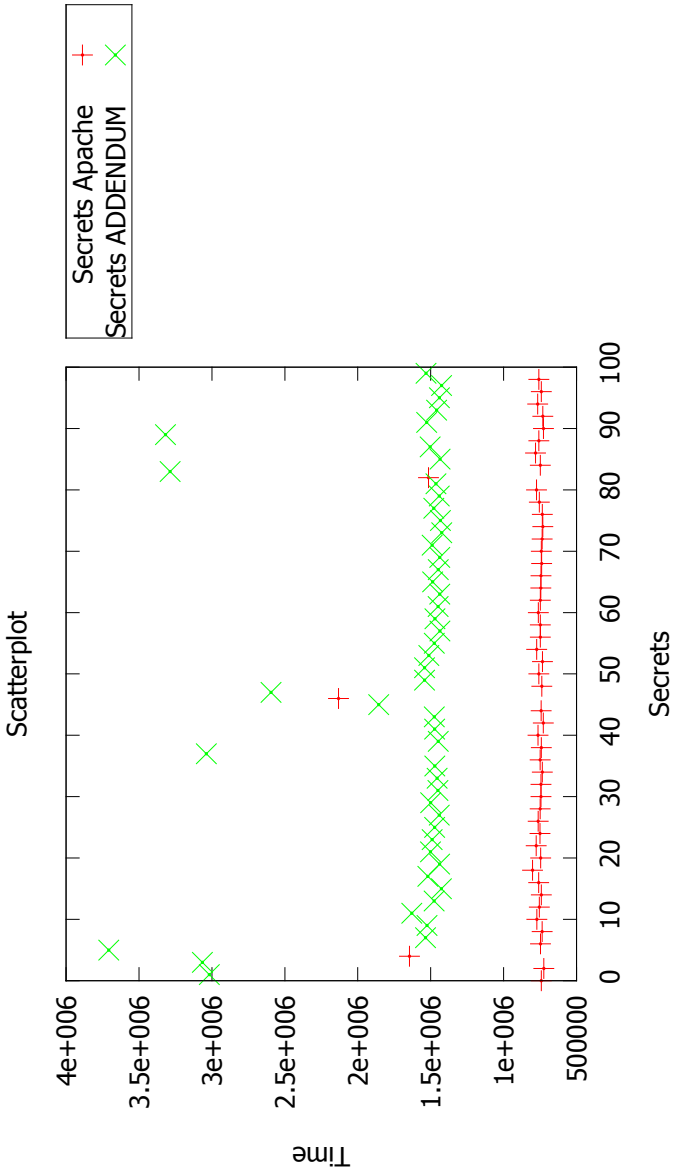

Figure A.1.: Scatterplot

B. Whisker Diagram

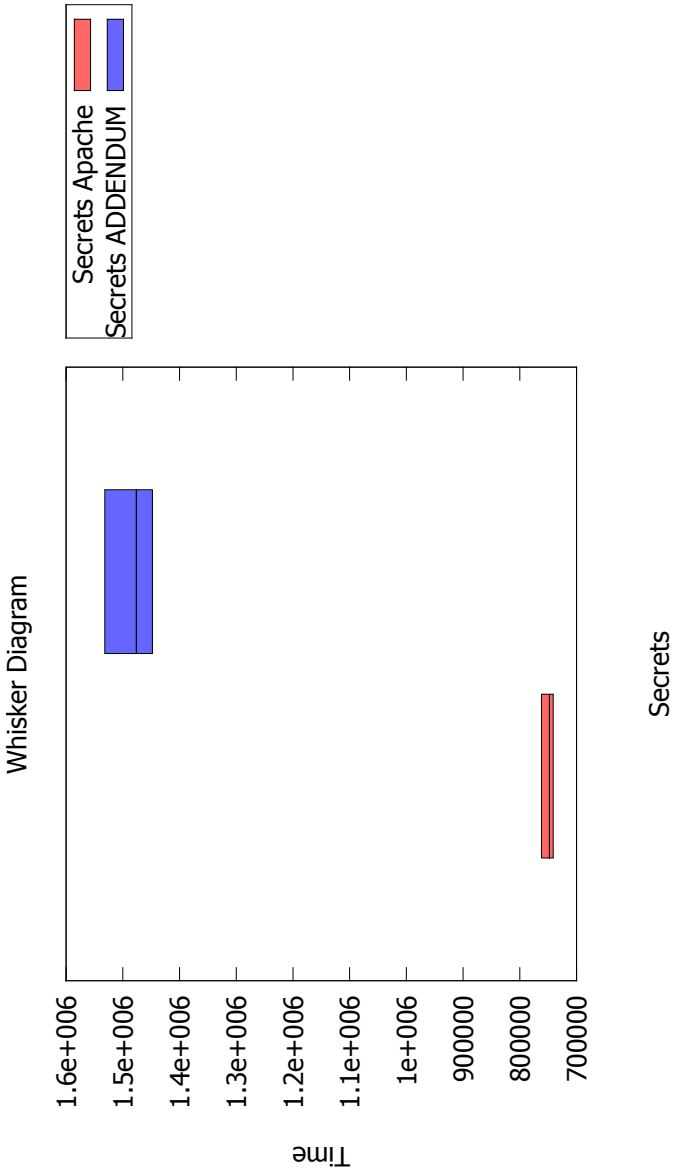

Figure B.1.: Whisker Diagram

C. CDF

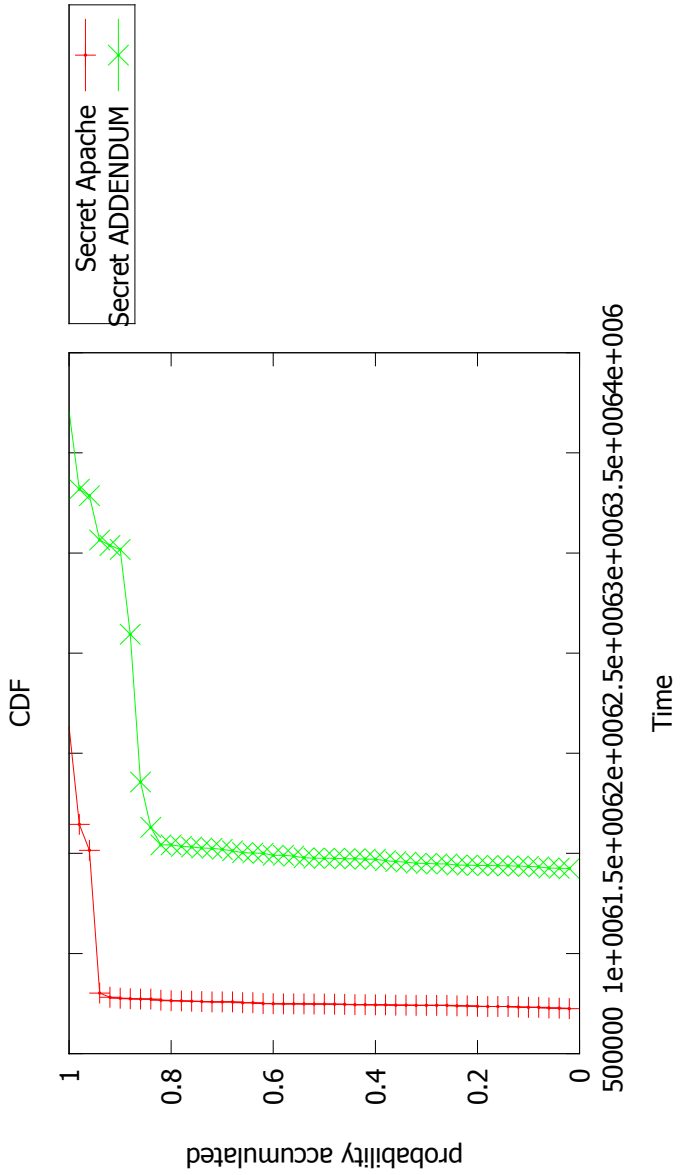

Figure C.1.: CDF

D. Histogram

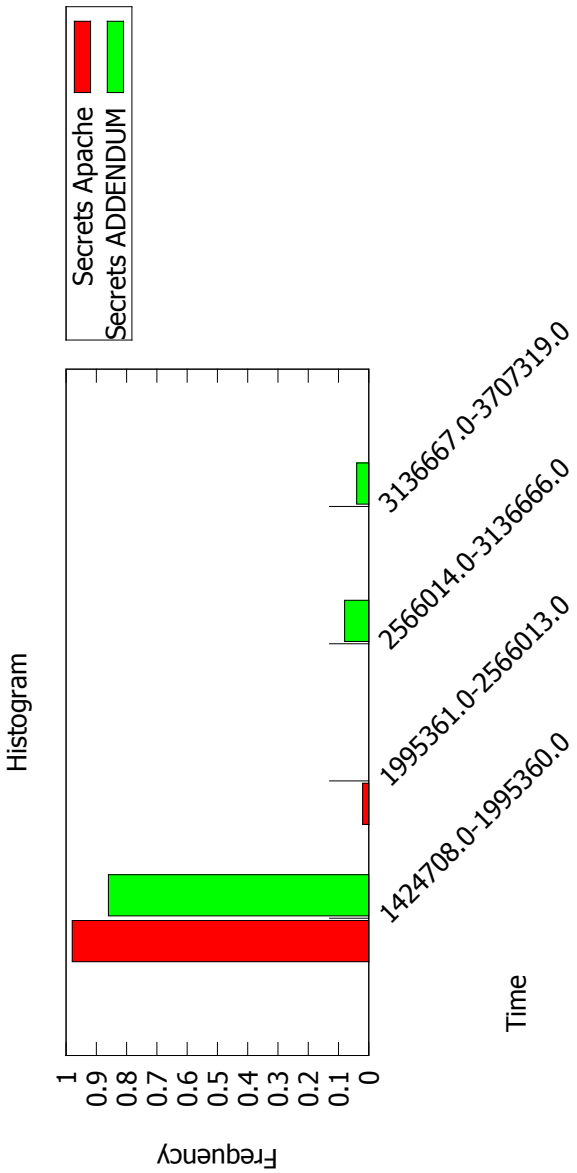

Figure D.1.: Histogram

E. Scatterplot

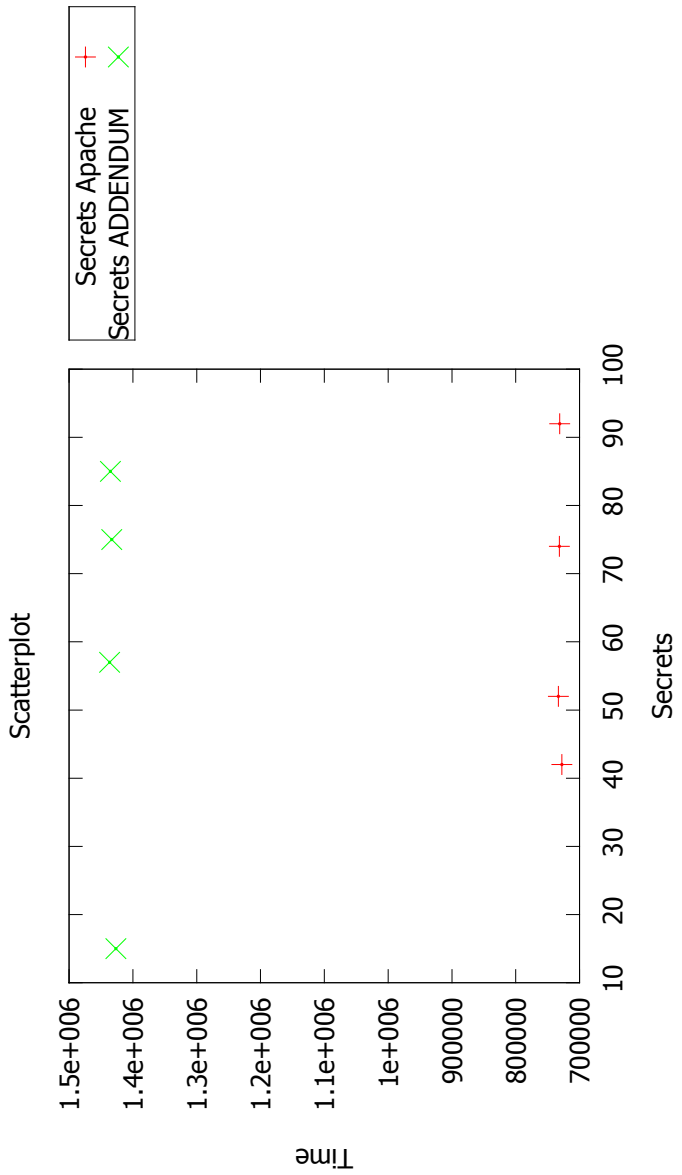

Figure E.1.: Scatterplot

F. Whisker Diagram

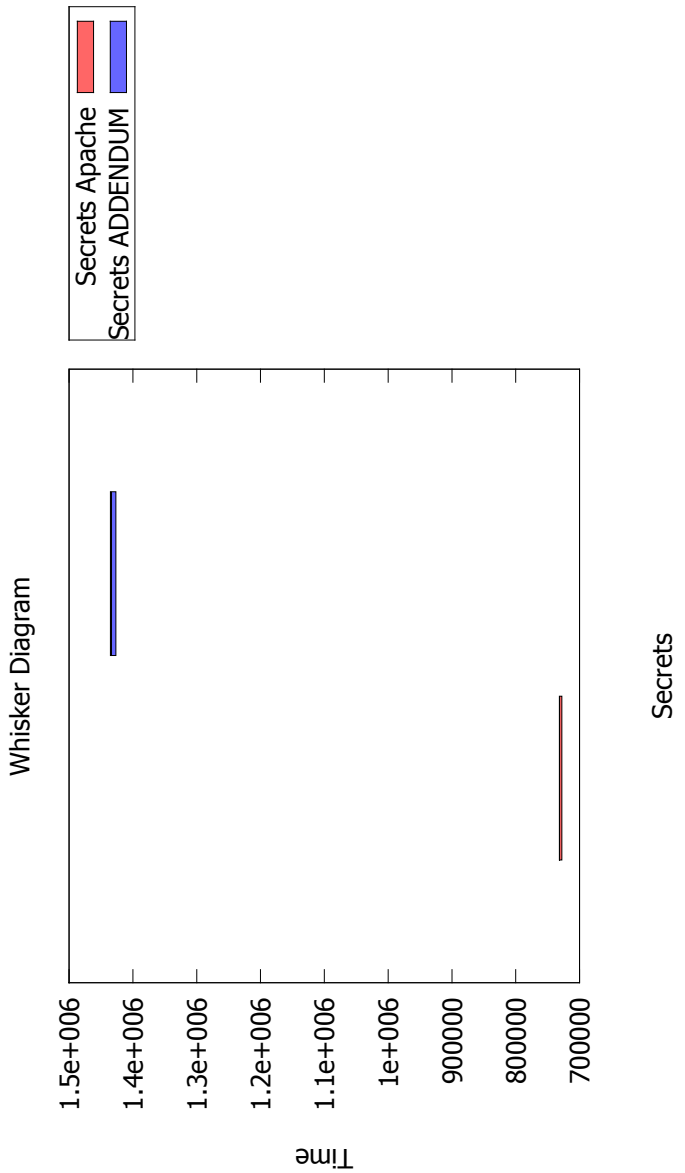

Figure F.1.: Whisker Diagram

G. CDF

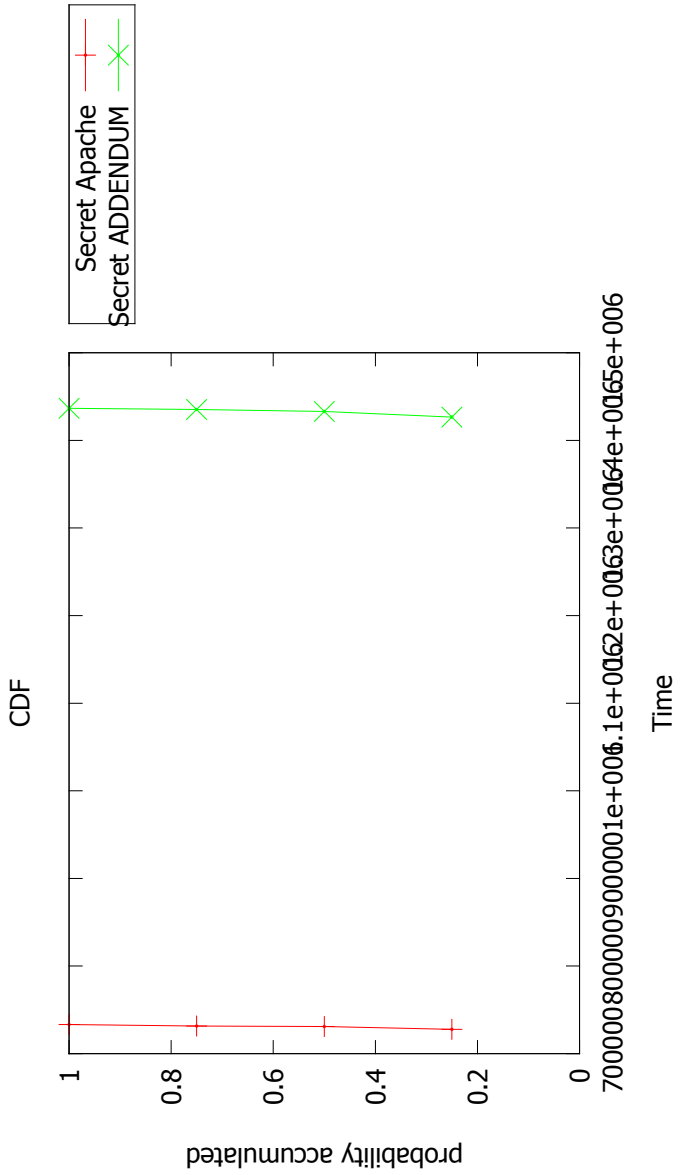

Figure G.1.: CDF

H. Histogram

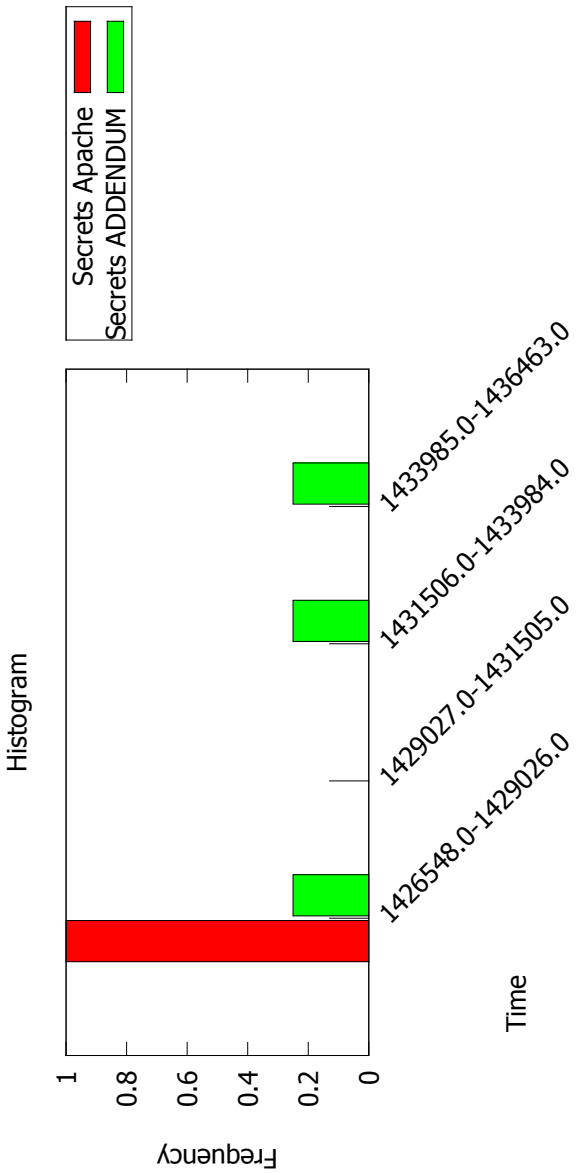

Figure H.1.: Histogram