COMP.SEC.220 Security Protocols: Helping Alice and Bob to Share Secrets

Coursework 2: experimental results

Sami Jakonen

Experimental results

Let’s evaluate the performance of the AinQ *(Arrows in a Quiver)* scheme. The scheme was developed according to the algorithm description in the original paper [1] and the evalution is done following the experimental section of the same paper. As it was not required to use a resource constrained device, a quite average desktop PC was used for this experiment. All, the KGC, the team leader drone and the edge drones were run on the same machine.

- Fedora Workstation 37
- AMD Ryzen 5 1600X
- 16 GB RAM

Instructions for running the code can be found in the README.md file in the project root. Also, a video demo of the program can be found in README.md.

Performance of Core Cryptographic Functions

In this section, the performance of the cryptographic functions of the AinQ scheme is studied by measuring their execution times. For each part of the program the relevant functions were tested, following the experiments in the AinQ paper [1].

Edge drone

The EC multiplication execution time was observed with Python time and with the test system the execution time was 0.014 seconds. The system executed the GenSecretValue function in 0.016 seconds and KeyRetrieval in 0.015 seconds.

	EM	TIME (SEC)
EC MULTIPLICATION	0	0.014
GENSECRETVALUE	1	0.016
KEYRETRIEVAL	1	0.015

Table 1. Edge drone performance

Table 1 shows the results for each measured part of the program. The measurements were taken 50 times each while the whole program was running normally.

Team leader

The relevant functions of the team leader drone are GenGroupKey and Re-Key. In this experiment, the number of edge drones was varied from 1 to 2000. When measuring the execution time of GenGroupKey for one drone, we measured a time of 0.043 seconds. For 2000 drones the execution time was 59.386 seconds. When this is compared to 0.043 multiplied by 2000 drones (85.6 seconds), we can observe that the execution time was about 70 % of the expected value.

The Re-Key function is also instrumental in the performance of the team leader drones. In this experiment its execution times are first tested when a key expires. The times were measured again ranging from 1 to 2000. The different measurements for GenGroupKey and Re-Key are shown in Figure 1. For one drone the Re-Key execution time was 0.014 seconds and for 2000 drones 0.067 seconds.

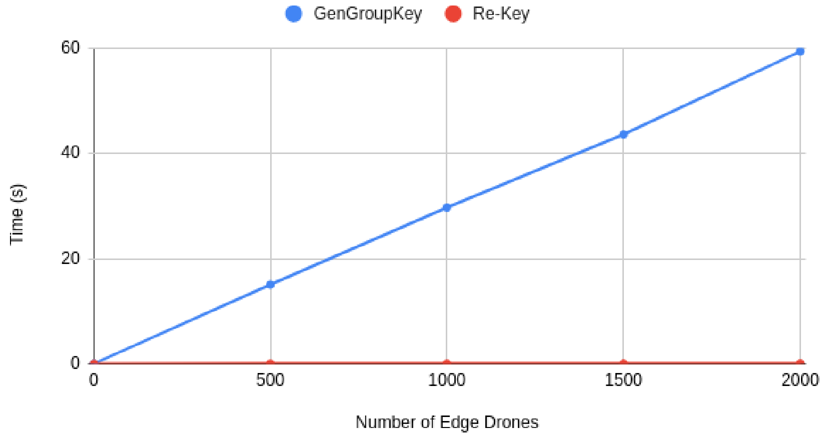

Figure 1. Performance of the Team Leader

The execution times of the Re-Key function were measured also for different numbers of edge drones added. Table 1 shows the different execution times of Re-Key.

Existing Group Members	New Group Members	Time (s)
1	1	0.044
1	100	2.917
1	500	14.370
1	1000	29.135
100	1	0.046
100	100	3.013
100	500	14.575
100	1000	29.333
500	1	0.056
500	100	2.970
500	500	14.423
500	1000	29.381
1000	1	0.071
1000	100	3.200
1000	500	14.719
1000	1000	29.659

Table 1. Group Re-Key Function

For one new drone on top of one existing drone, the Re-Key function finished in 0.044 seconds. For 1000 new drones joining a group of 1000 existing drones, the time was 29.659 seconds. Not all measurements did grow relative to one another. This can be explained with the program being run on a regular desktop PC with other programs taking up resources.

Comparison of results

The results are quite comparable to the results of the original AinQ paper [1]. The program implemented in Python in this report falls short in many execution time measurements, but this can be accounted to the actual implementation being coded in a more efficient language on dedicated hardware. The differences of the results follow similar patters however, which proves that the AinQ scheme provides good implementation for especially the Re-Key function.

References

[1] Frimpong, E. et al. (2021) ‘Arrows in a Quiver: A Secure Certificateless Group Key Distribution Protocol for Drones’, in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). [Online]. Cham: Springer International Publishing. pp. 31–48.