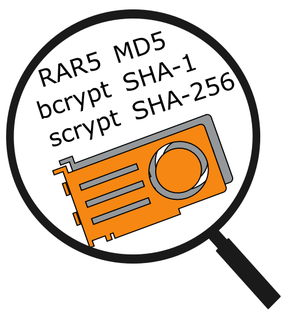
BRNO FACULTY OF INFORMATION TECHNOLOGY
UNIVERSITY OF TECHNOLOGY

Excel@FIT 2019




# Selecting the right GPU for password recovery

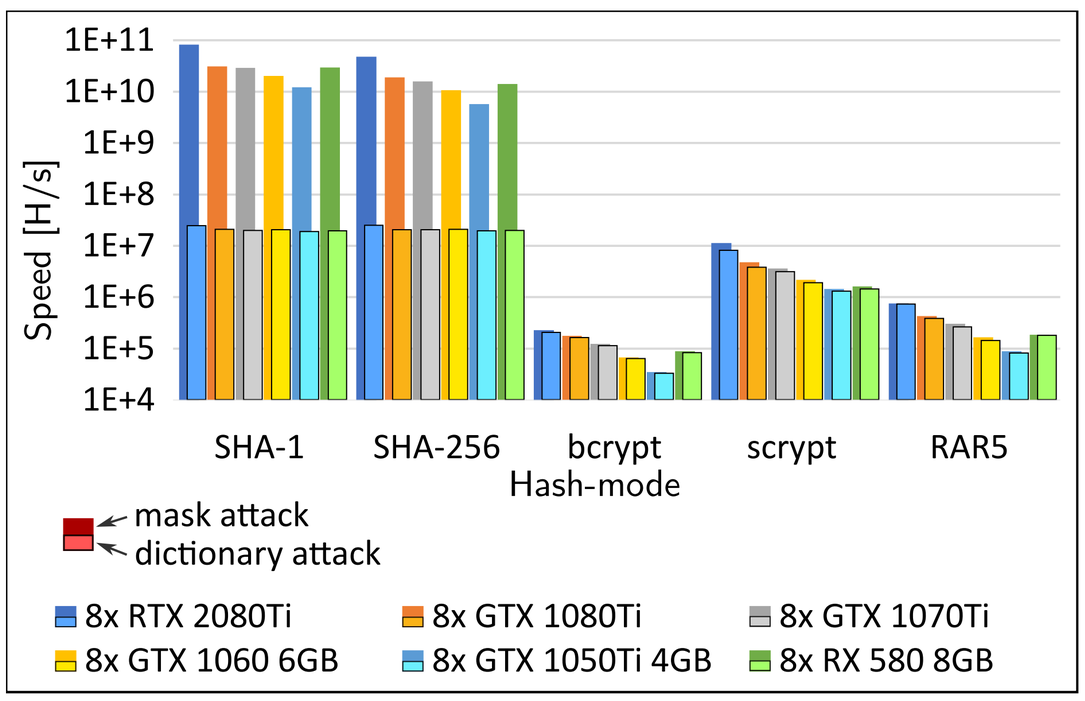
#32

## Motivation

The Graphics Processing Units (GPUs) become more potent with every generation, and they are usable for general purpose computing. The password recovery is a data parallel task and therefore matches the GPU's architecture and designs. Most companies and users compare the GPU performance only using games or rendering benchmarks. Therefore, the password recovery speeds, power consumption and other aspects of interest remain undiscovered or at least are not directly compared under the same conditions.

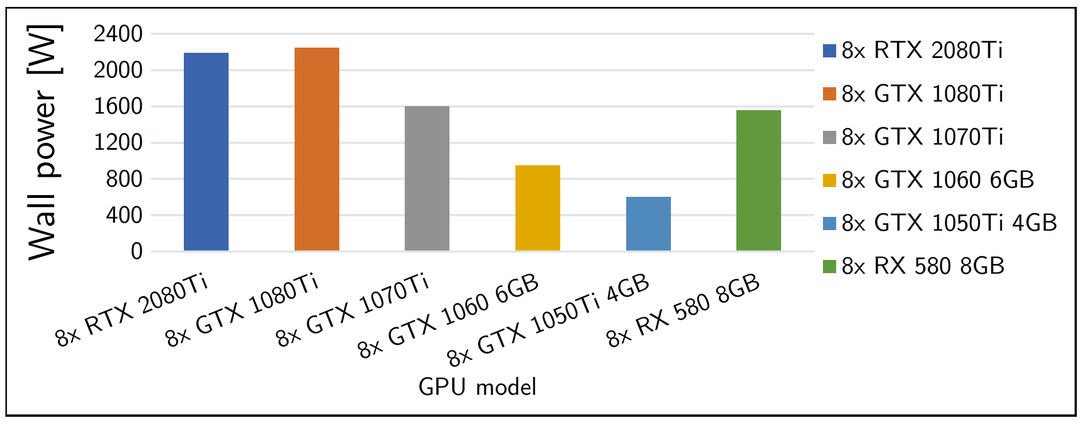
## Dictionary vs. mask attacks

Dictionary and mask (brute-force) are the most basic attacks. A dictionary attack uses files of pre-generated/gathered passwords. On the other hand, the mask attack uses a password generator during the attack. Therefore, mask attacks are generally faster as they are not as CPU <=> GPU communication demanding and the generators can run directly on GPU compared to a dictionary attack where each password has to be transmitted from RAM.



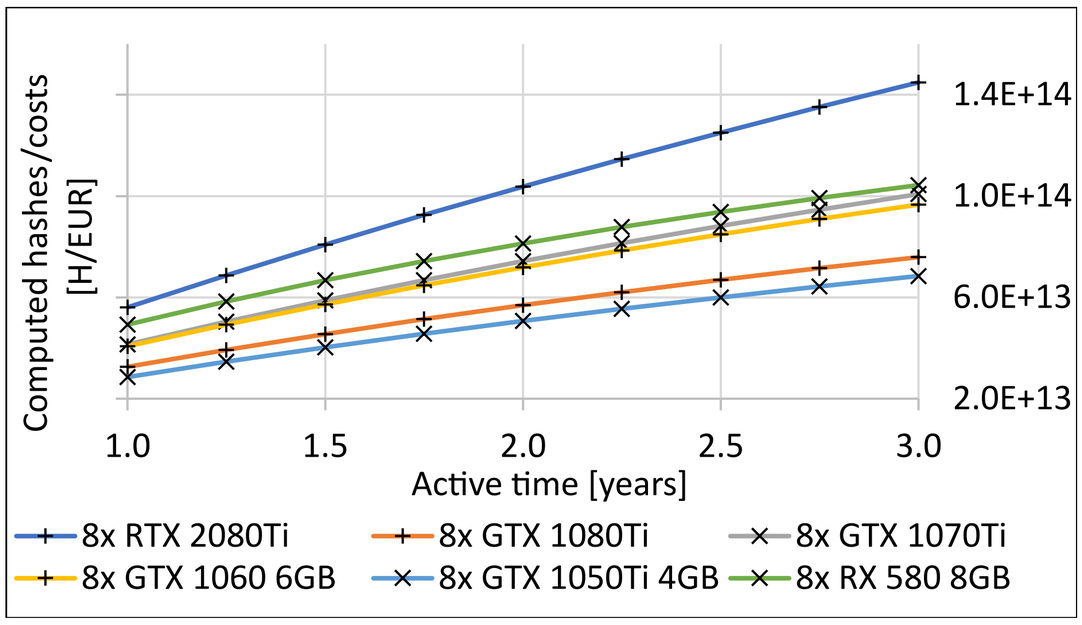

## Power consumption

Power consumption is one of the most critical aspects for such systems as they run in 24/7 mode for several months/years. The consumption generally grows as power increases in the same GPU generation. However, it is interesting to compare the power consumption of models from new to old generations and among different brands.




## Financial aspects

Financial aspects are the final aspect summarizing the relationship between the recovery speeds, power consumption and initial purchase prices. It shows the significance of each considered aspect in some way. Like AMD RX 580 having advantage on Nvidias GTX 1060 and 1070Ti at the start and losing it over time since it has got higher power consumption.




*Author: Bc. Vojtěch Večeřa <xvecer18@stud.fit.vutbr.cz>* | *Supervisor: Ing. Vladimír Veselý, Ph.D.*