World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

Accelerating Side Channel Analysis with Distributed and Parallelized Processing

Authors : Kyunghee Oh, Dooho Choi

Abstract : Although there is no theoretical weakness in a cryptographic algorithm, Side Channel Analysis can find out some secret data from the physical implementation of a cryptosystem. The analysis is based on extra information such as timing information, power consumption, electromagnetic leaks or even sound which can be exploited to break the system. Differential Power Analysis is one of the most popular analyses, as computing the statistical correlations of the secret keys and power consumptions. It is usually necessary to calculate huge data and takes a long time. It may take several weeks for some devices with countermeasures. We suggest and evaluate the methods to shorten the time to analyze cryptosystems. Our methods include distributed computing and parallelized processing.

Keywords : DPA, distributed computing, parallelized processing, side channel analysis
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020