A framework for GPU-accelerated AES-XTS encryption in mobile devices

ABSTRACT

Attacks on data stored in mobile devices are increasingly getting more efficient and successful, especially with the use of advanced cryptanalysis techniques and high-tech systems. Encryption using the IEEE XTS-AES algorithm might be an attractive solution for this problem, but it comes with a significant impact on the performance of these limited-resources devices. The emergence of the potential Graphical Processing Units (GPUs), as a general purpose non-graphical computational power, has gained a great interest in both industry and academia. Recently, GPUs have presented higher performance for parallel programming than conventional CPUs while they continue gaining reduced cost. One important application area that can benefit from GPUs power is storage encryption in mobile devices. In this paper, we introduce a GPU-accelerated framework for storage encryption in mobile devices using the XTS-AES encryption algorithm. The Google's Android is targeted in this work as a mobile operating system.

Keyword: Data security in mobile devices; Google's Android OS; GPU computing; Massive parallel processing; XTS-AES