# A parallel XTS encryption mode of operation

## ABSTRACT

Securing data stored inside the storage devices is becoming an important concern in computer security now. It is known that the most efficient techniques to protect storage devices are using cryptography. Developing newer and more secure encryption algorithms and modes of operation might be critically important to protect these devices since conventional disk encryption algorithms, such as CBC mode, have shown serious security flaws. In this paper, the newly standardized IEEE XTS encryption mode of operation for storage encryption (P1619 standard) has been implemented using parallel design. A performance comparison between the sequential and parallel algorithms of XTS mode has been presented. The parallel XTS algorithm has shown a speedup of 1.80 (with 90% efficiency) faster than the sequential algorithm. In these simulations, AES is used as encryption algorithm with 256-bit encryption key.

**Keyword:** Disk encryption; Encryption modes; Parallel processing; XTS mode