Advanced encryption standard-XTS implementation in field programmable gate array hardware

ABSTRACT

In recent years, security has been a common concern for the data in-transit between communication networks as well as data at rest in storage devices. The Institute of Electrical and Electronics Engineers P1619 Security in Storage Working Group proposed a standard for the security of static data. One of the components of this standard is the cryptographic protection of data on block storage devices. This standard uses Advanced Encryption Standard-XEX weakable block cipher with ciphertext stealing as a building block for the protection of data. Few field programmable gate array-based implementations of this mode that achieve sustainable throughput for block storage devices exist. This work proposes and demonstrates a different scheme that achieves better efficiency compared with current implementations.

Keyword: Cryptography; Disk encryption; FPGA; AES-XTS