Dragon-2: Fast Stream Cipher Encryption

Description

In our world of billions of interconnected computers, transmitting or storing data requires the use of encryption, to prevent unauthorized parties from snooping or modifying the data.

The Dragon-2 stream cipher provides efficient symmetric encryption, using state of the art techniques to achieve maximum throughput of 5 cycles/byte while retaining 256 bits of security. It leverages the extensive analysis on the eSTREAM Dragon cipher to provide confidence in its security.

The core of the cipher can be customized to clients’ needs, or replaced with a round of the Advanced Encryption Standard (AES) to provide the highest level of assurance. Whether providing Dragon-2 or a fresh design, we also deliver a methodical and complete cryptanalysis.

Features

- Extremely fast (5 cycles/byte)
- 256-bit security
- Can incorporate AES technology
- Utilizes single-instruction multiple-data

Applications

- End-to-end Encryption
- Disk Encryption
- Proprietary Security

References


Department of Infocomm Security, Institute for Infocomm Research (http://icsd.i2r.a-star.edu.sg)
1 Fusionopolis Way, #21-01 Connexis (South Tower), Singapore 138632
Contact: Eunice Pee (IDM)  Tel: (65) 64082180 Email: eunice-pee@i2r.a-star.edu.sg