



Encryption Engine



TECHNOLOGY SUMMARY

In the past, traditional encryption engines utilized a mode of encryption that was vulnerable to certain attacks and not capable of running at full capacity. Sandia has created an invention that provides a solution to the problem of keeping an encryption engine pipeline full so that the encryption engine can run at full capacity in CBC mode or other encryption modes requiring feedback from previous computation.

Cipher Block Chaining, CBC, is the preferred mode in practice because CBC mode encryption requires feedback from the previous computation. Previous concern with the CBC mode was that the pipeline has the possibility of being flushed or run dry, however this invention allows the encryption engine pipeline to be kept full, allowing full-rate operation.

BENEFITS

Engine pipeline kept full, allowing full-rate operation

Modes of encryption able to run at full capacity

Advanced Computing

INTELLECTUAL PROPERTY

US PATENT #7,362,859
SD# 6769

POTENTIAL MARKET APPLICATIONS

Computing

Software

Cyber Security

TECHNOLOGY READINESS LEVEL

Sandia estimates this technology at TRL 5. Key elements have been demonstrated in relevant environments.

Craig Smith | 925.294.3358 | casmith@sandia.gov



Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration. SAND # 2011-4639P