

TECHNOLOGY READINESS LEVEL: 5

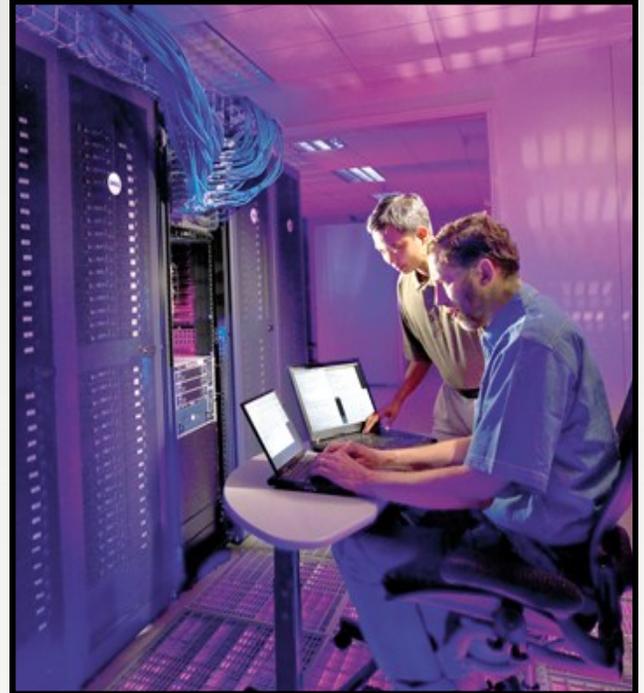
US PATENT # 7,362,859

KEY ELEMENTS HAVE BEEN DEMONSTRATED IN RELEVANT ENVIRONMENTS.

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.



POTENTIAL APPLICATIONS

- Computing
- Software
- Cyber security

TECHNOLOGICAL BENEFITS

- Engine pipeline kept full, allowing full-rate operation
- Modules of encryption able to run at full capacity
- Advanced computing

TECHNOLOGY INQUIRY?

For more information or licensing opportunities contact us at

ip@sandia.gov

Refer to SD # 6769

or visit

<https://ip.sandia.gov>