

REBEL: REconfigurable Block Encryption Logic for Cyber Security

APPLICATION AREAS

Cyber Security; Cryptography

ABSTRACT

The pervasion of computer-based transactions in every day life has led to an increased need for cryptography to ensure that cyber transactions are secure. Classical methods for encryption/decryption, such as asymmetric RSA encryption/decryption or symmetric block ciphers (for example, NIST standard AES), can take tens of millions of computing cycles that slow the speed of data encryption/decryption. In addition, these systems also suffer from security vulnerabilities through the use of S-boxes, where public knowledge of S-box constants allows for an adversary to develop static statistical models to exploit them. **To overcome these drawbacks, ISU researchers have developed REBEL, or REconfigurable Block Encryption Logic, an alternate method for symmetric encryption/decryption** which uses the secret as truth tables of a reconfigurable gate as opposed to S-boxes; these gates are deployed in a tree circuit whose security properties are extremely strong. In addition, this technology can be implemented in underlying hardware, enabling very fast data encryption and decryption.

BENEFITS

REBEL is:

- Rapid (provides encryption and decryption at data rates 10-20 times higher than currently used methods)
 - Secure (S-boxes are not used so the system is not vulnerable to attack mediated by static statistical models)
 - Versatile (can be included in hardware in embedded processors used in devices such as cell phones, smart cards (ATM cards), wireless routers, etc.)
-

INVENTOR(S)

Drs. Akhilesh Tyagi and Mahadevan Gomathisankaran (Electrical and Computer Engineering)

INTELLECTUAL PROPERTY STATUS

Patent pending

LICENSING ASSOCIATE

Eddie Boylston

E-mail: latinusb@iastate.edu

Phone: 515-294-3621 (Direct Line)
