Exploring Throughput Oriented Cryptographic Systems

*Raj Parihar and Jay Geagan
Email: {rpariha, jgeagan}@us.ibm.com
Content Protection Group, IBM Research – Almaden
*University of Rochester, Rochester, NY 14627

Objective
Explore and analyze high throughput oriented hardware and software based encryption/decryption platforms to maximize crypto operations/sec/$. 

Algorithmic view of AES-128 Encryption

AES Forward Cipher Flow Graph

GPU Based Encryption Platform

FPGA Based Encryption Platform

FPGA based systems are the fastest among all which provide up to ~600 trillion encryptions/sec in 1 million dollar budget.

ASIC IP Based Encryption Platform

ASIC based systems provide about 1.5x higher throughput compare to FPGA based solution. 
ASIC based systems have much higher NRE cost which ranges 3 – 5 million dollars easily.

Summary
FPGA based cryptographic systems are the fastest among all except custom based ASIC based systems.

For a budget < 5 million dollars FPGA based systems would maximize # of encryptions/sec/$.

ASIC based systems would be best if the budget is >5 million dollars.

GPU and hardware accelerator increase computing power of large scale systems by an order in similar power budget.

Biological systems are also shown to provide high throughput encryptions which are still in very primitive age.