



## ABOUT ENCRYPTTEK

Encryptek's patented Radium product-line provides the world's fastest RSA cryptographic acceleration.

Encryptek merges mathematical theory and state of the art engineering to drive super-high performance hardware cryptography solutions. The Encryptek founders set out to re-define hardware cryptographic acceleration by applying a unique, yet adaptable, and highly parallel solution to Modular Exponentiation, resulting in a patented system for RSA encryption and decryption acceleration.

Encryptek focuses on flexibility: IP optimizations can be selected for encryption strength, hardware architecture, power constraints, embedded devices, and high performance computing. The key to such parameter tuning is Encryptek's scalable design, leveraging highly parallel primitives, that can be applied on 1024, 2048, 4096-bit computations, and beyond.

At a cost per transaction basis, the Encryptek products deliver value not seen in any competitor products.

## ENCRYPTTEK RADIUM IP CORE

- Patented IP core for very fast and secure asymmetric encryption
  - RSA, DH, DSA, EC, any modular exponentiation encryption/decryption
- Public key and PKI
  - Has been a standard for many years, but limited by speed/cost
- Encryptek IP is fastest known implementation
  - With similar/smaller area as existing designs
- Scalable bit word solution
  - Flexible for 1024/2048/4096/etc. bit encryption on FPGA or ASIC
- Implemented and proved in previous products
  - Low power, realtime, high throughput, embedded systems

## TECHNICAL APPLICATIONS AND MARKET

- Key Exchange
  - Web and email servers
  - VoIP
  - SAN encryption
  - TCG, FIPS, and embedded markets
  - Assist in generation of public/private key pairs
- Reuse of insecure media
  - Wireless
  - Satellite
- Many more enterprise environments