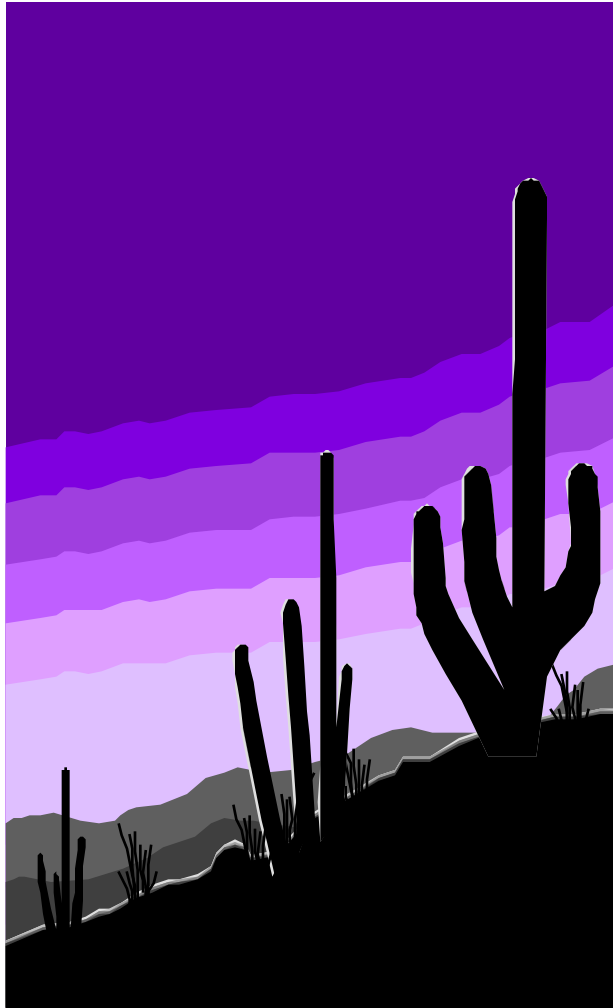
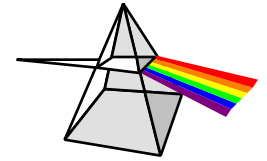
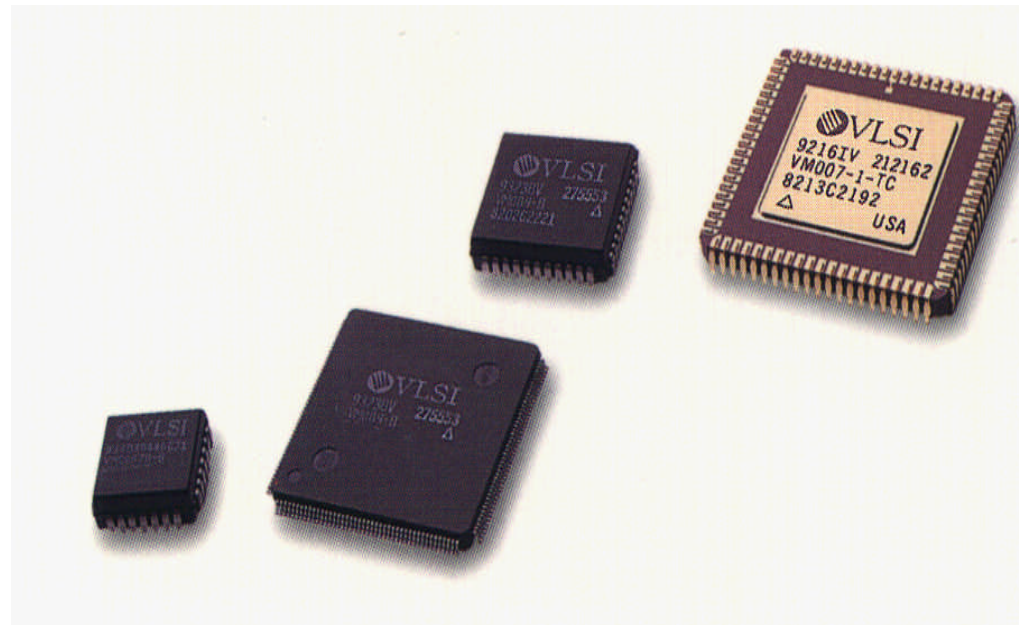


# Embedded Security Solutions

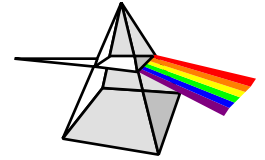


**“Driving Security into the Commercial World”**



# **Embedded Security Solutions**

## ***VLSI Mission Statement***

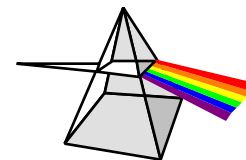


### **Secure Products Mission Objective:**

***Provide multi-grade hardware security products  
and services to our customers***

## **Embedded Security Solutions**

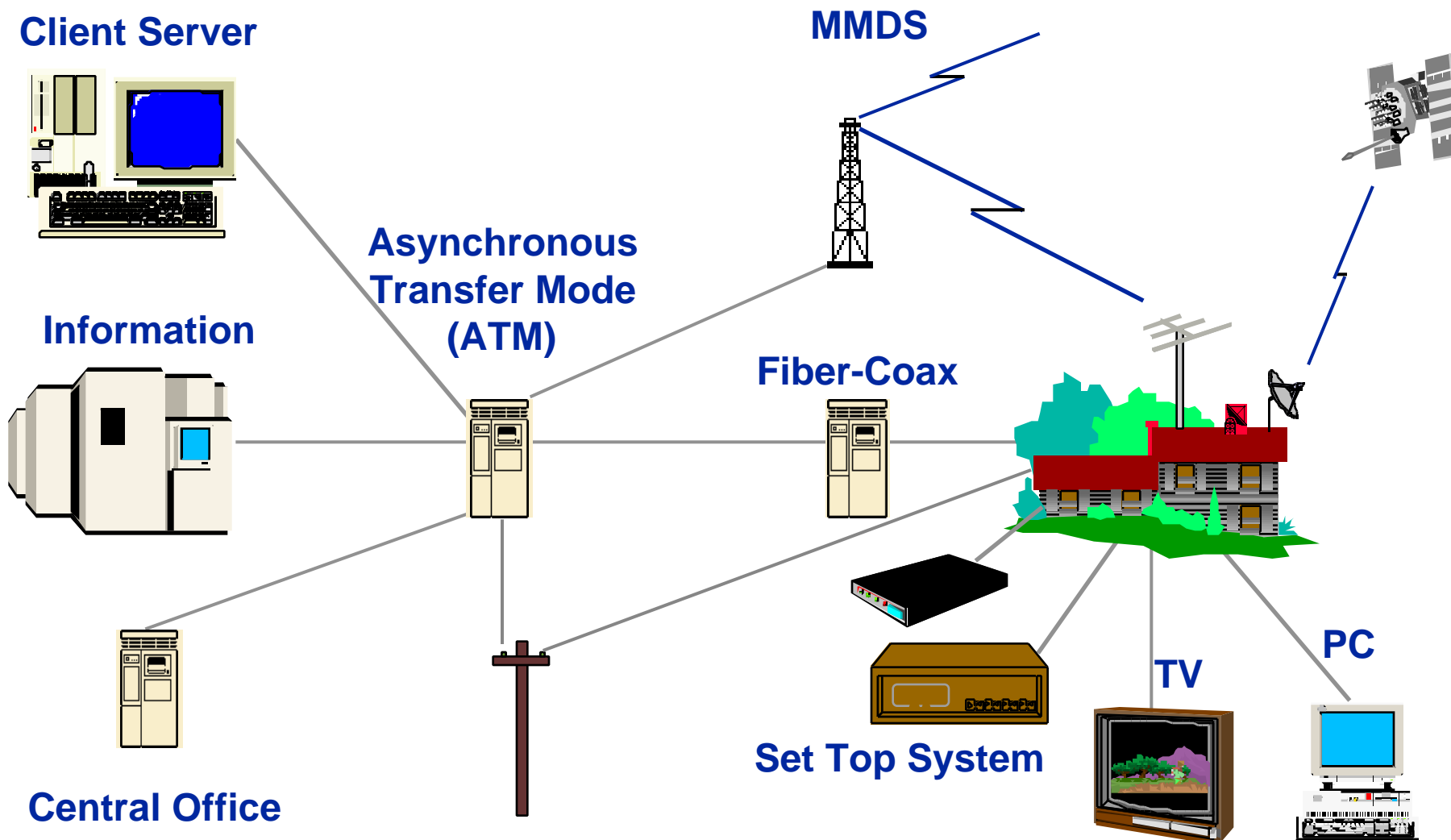
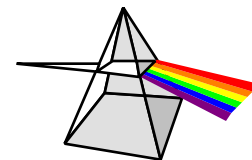
### ***VLSI Technology Background***



- ◆ **VLSI is a leading company in the development of system-on-a-chip technologies and integrated circuit manufacturing**
  - **1995 Revenue - \$720M**
- ◆ **World-Wide presence**
  - **World-Wide Sales and Technology Center coverage**
  - **Manufacturing in San Jose, CA, Tempe, AZ, and San Antonio, TX**
  - **Approximately 3000 employees**
- ◆ **VLSI's target markets are high growth computing, communications, and digital entertainment**
- ◆ **VLSI has been providing its customers with silicon security solutions since 1991**
- ◆ **VLSI is the leading supplier of key escrow products to the U.S. Government**

# Embedded Security Solutions

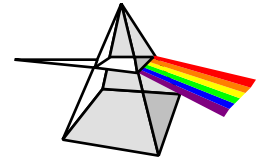
## *Pervasive Commercial & Personal Security Needs*



RSA Data Security Conference 1997

# **Embedded Security Solutions**

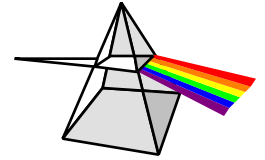
## ***Why Encrypt?***



- ◆ **Public (Internet) and private computer networks and telephone systems are wide open to hacker access**
- ◆ **There is a need for data authentication, integrity, and privacy on the various networks**
- ◆ **Foreign governments and hackers are motivated to intrude Electronic Commerce Networks**
- ◆ **Protection of intellectual property**
- ◆ **Theft of service is cable industries largest problem**

# **Embedded Security Solutions**

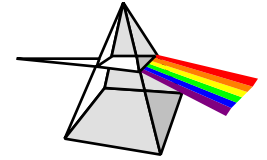
## ***Hardware or Software Security?***



- ◆ **Hardware security is much faster than software security**
  - **SW algorithms can use major amounts of CPU bandwidth, slowing throughput of entire system**
- ◆ **Software algorithms are susceptible to disassembly, modification, and, or replacement in a way that may be difficult to detect.**
  - **Hardware is difficult to attack without physical destruction**
- ◆ **Hardware key management is more robust, private/secret keys are easier to protect**
- ◆ **Hardware lends itself to embedded solutions where space, MIPS, and battery life are at a premium**

# **Embedded Security Solutions**

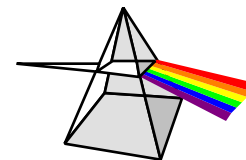
## ***VLSI Technology Capabilities***



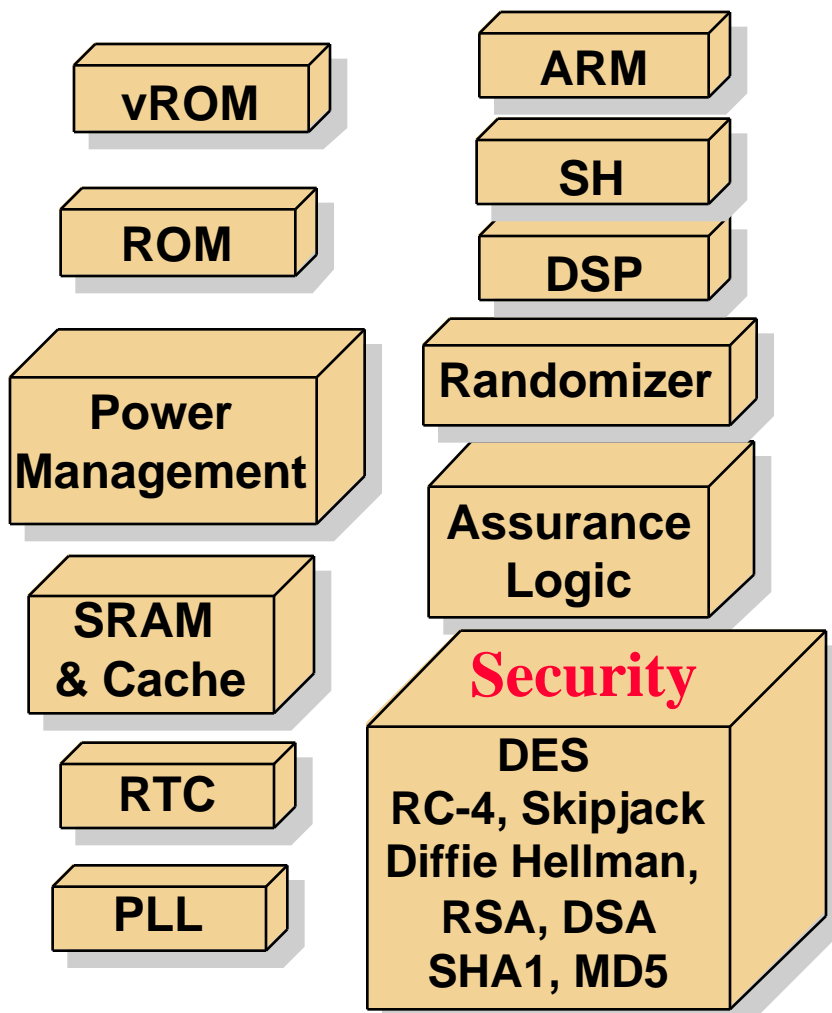
- ◆ **Security Expertise**
  - High-performance standard products
  - Architecture and chip designs for embedded applications
  - Customizable system solutions
  - Security related Functional System Blocks (FSB™)
- ◆ **Integrated technology applicable to system-on-a-chip solutions with unique embedded security features**
  - FSB design methodology and cell libraries for communications, computing, and digital entertainment applications
  - HDL design methodology for multiple CAE platforms
- ◆ **World-wide support available through VLSI's network of Technology Centers**

# Embedded Security Solutions

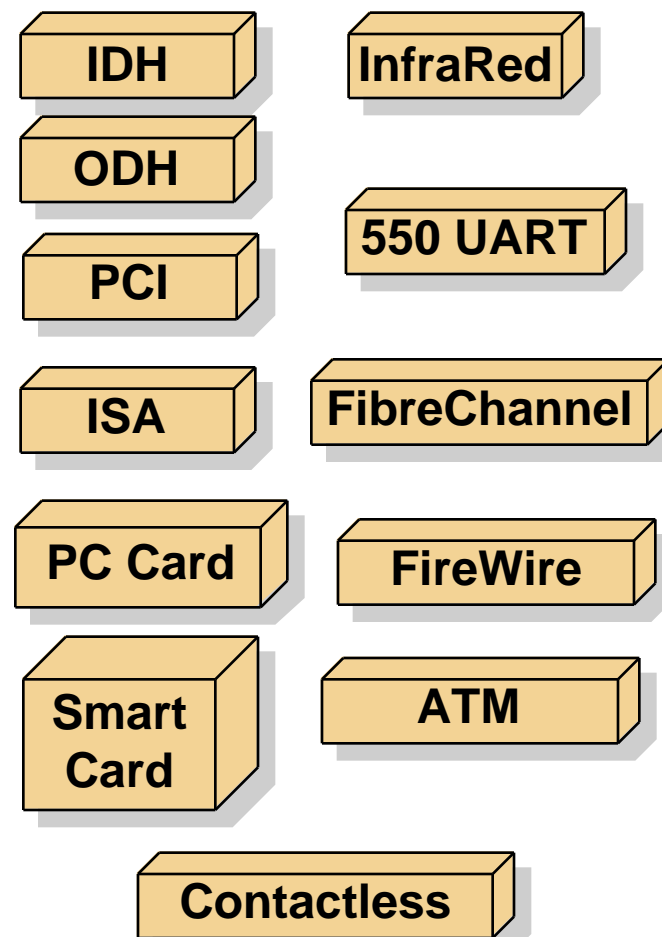
## FSB Building Blocks



### VLSI FSB's

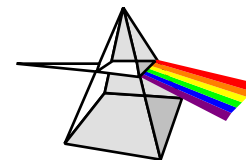


### VLSI FSB I/O's

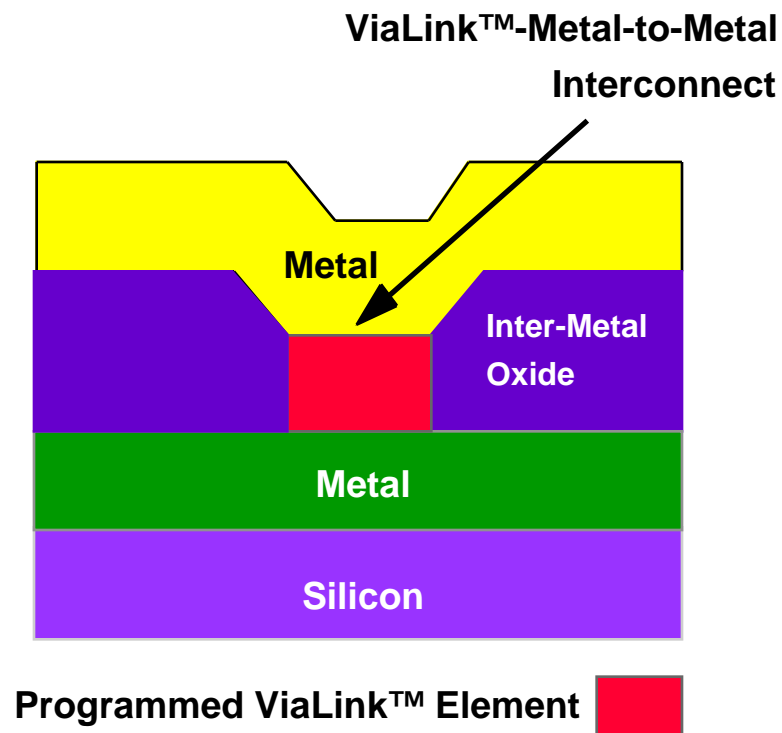


# Embedded Security Solutions

## **VIALINK™ Antifuse Technology**

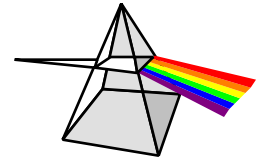


- ◆ One-Time Programmable, Non-Volatile Memory
  - 512 x N vROM
- ◆ Field-programmable by customer
- ◆ Inherent secure features



## **Embedded Security Solutions**

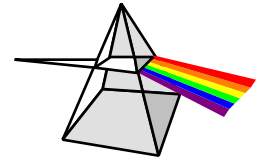
### ***VLSI'S Crypto Features***



- ◆ Complete cryptographic system & boundary on a chip
- ◆ ARM 32-bit RISC processor based
  - Secure and general purpose processing
  - Integrated JumpStart™ development tools for PC and Unix based systems plus “Black ICE™” hardware emulator
- ◆ On-chip key generation: “Key never sees the light of day”
  - Self-programming vROM™
- ◆ Full range of hashing algorithms based on SHA-1 and MD5
- ◆ Public key algorithms:
  - Diffie-Hellman, RSA
- ◆ Digital Signature & Verification
  - RSA, DSA
- ◆ Complete cryptographic primitives
  - Software protected by O/S using cryptographic checksum
- ◆ Anti-cloning and anti-spoofing features

## Embedded Security Solutions

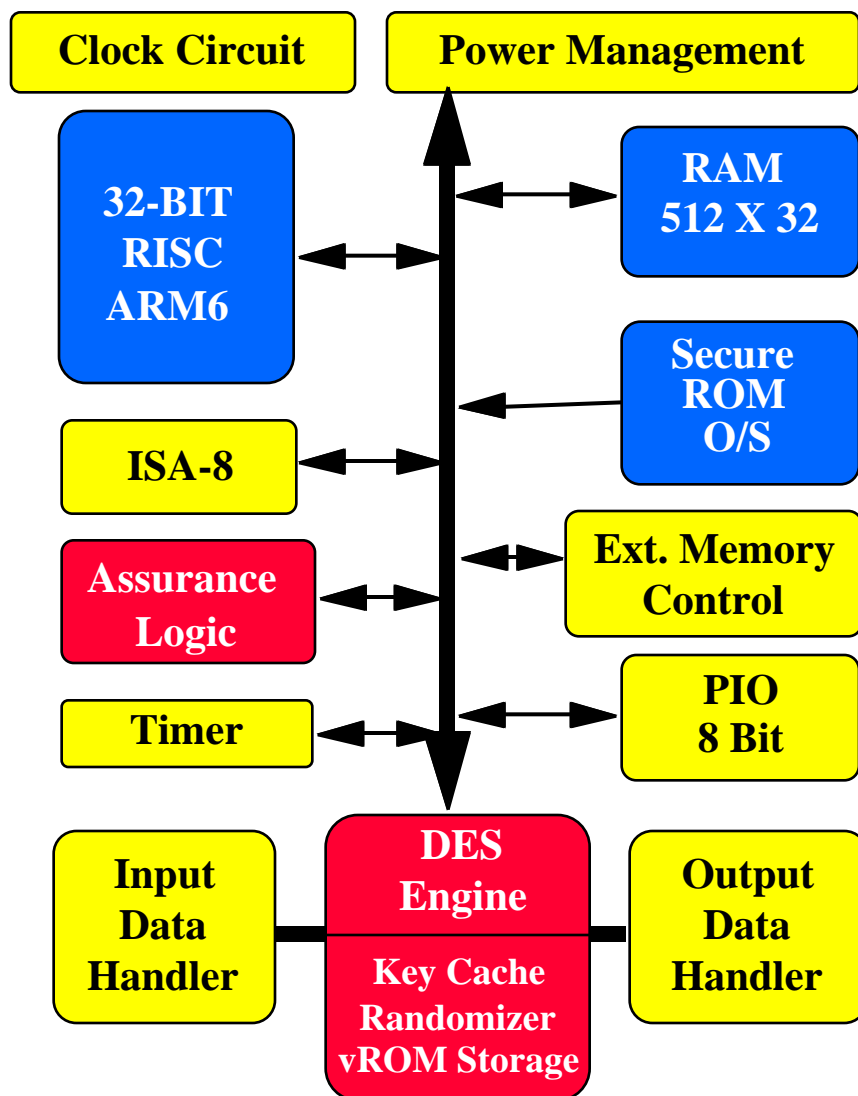
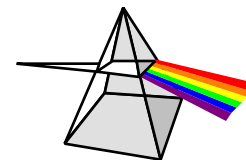
### *VMS210 - Set top box security*



- ◆ VMS210 is an advanced crypto-processor and controller architecture consisting of :
  - 32-bit (22 MIPS) ARM 6 RISC processor
  - Special hardware DES engine with integrated key cache
    - Supports ECB, CBC, OFB, 1-, 2-, 3-DES
  - All digital non-deterministic randomizer (patent pending)
  - High speed I/O handler for packetized data
  - Flexible external memory interface
- ◆ VMS210 is optimized for packet data encryption/decryption specifically for MPEG2 transport streams
- ◆ VMS210 includes a flexible security kernel, masked ROM, and is customizable for specific applications
- ◆ Each chip is programmable for anti-cloning and device ID
- ◆ In production now

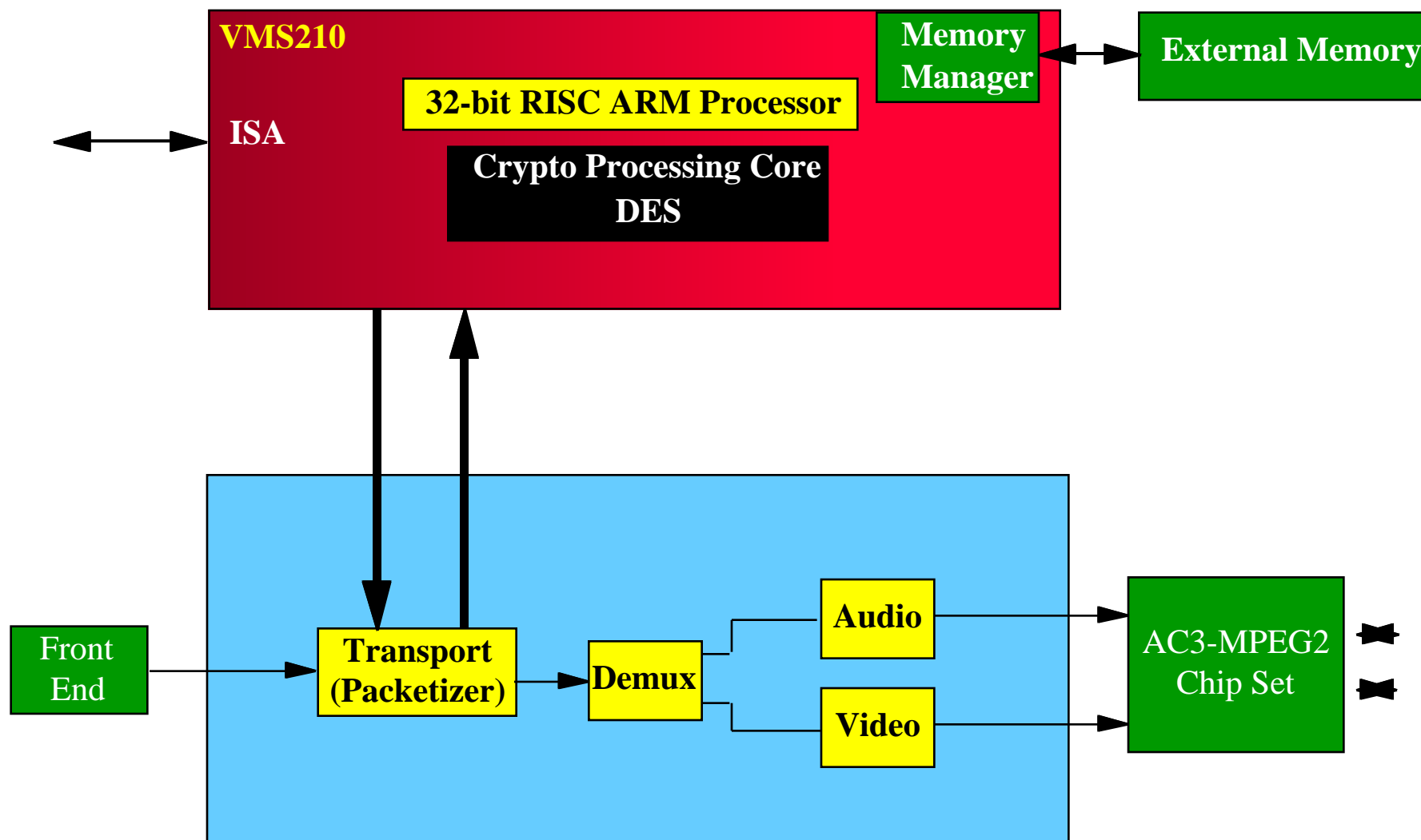
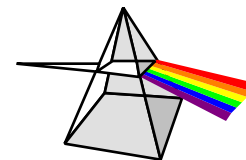
# Embedded Security Solutions

## VMS210 Architecture



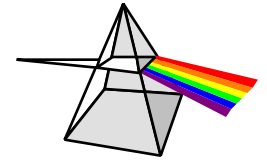
# Embedded Security Solutions

## VMS210 Set Top Box Connection



## **Embedded Security Solutions**

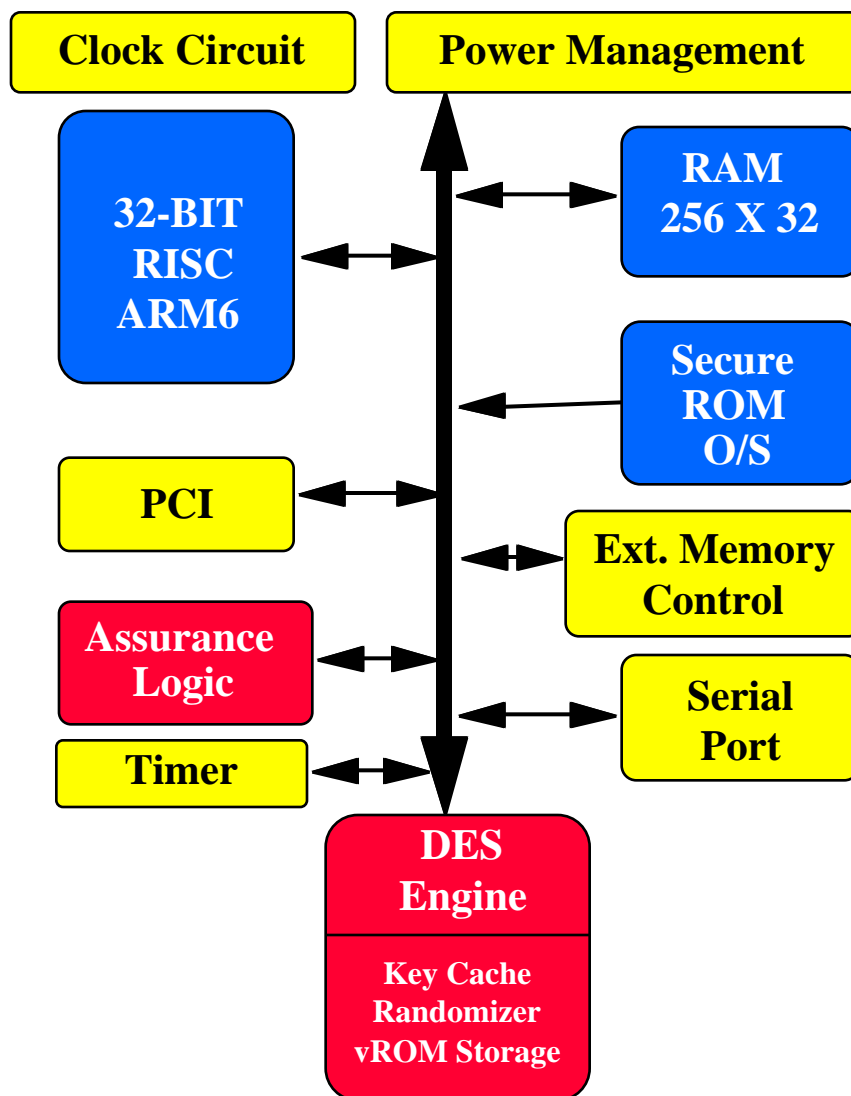
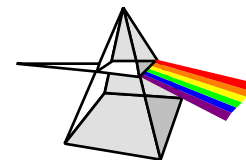
### ***VMS230 - Satellite Video and Data Security***

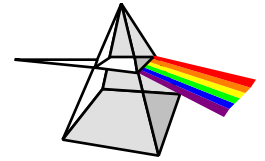


- ◆ **VMS230 is designed for secure PC connectivity**
  - **Software and valued content distribution**
- ◆ **Customizable internal O/S for specific requirements**
- ◆ **PCI (master & slave modes) to move data between host and peripherals**
- ◆ **32-bit ARM RISC processor**
- ◆ **Special hardware DES engine with key cache**
- ◆ **Special packet handler with CRC**
- ◆ **RSA key management algorithm**
- ◆ **All digital non-deterministic randomizer**
- ◆ **Multiple communication ports**
- ◆ **Samples 1Q97, production 3Q97**

# Embedded Security Solutions

## VMS230 Architecture

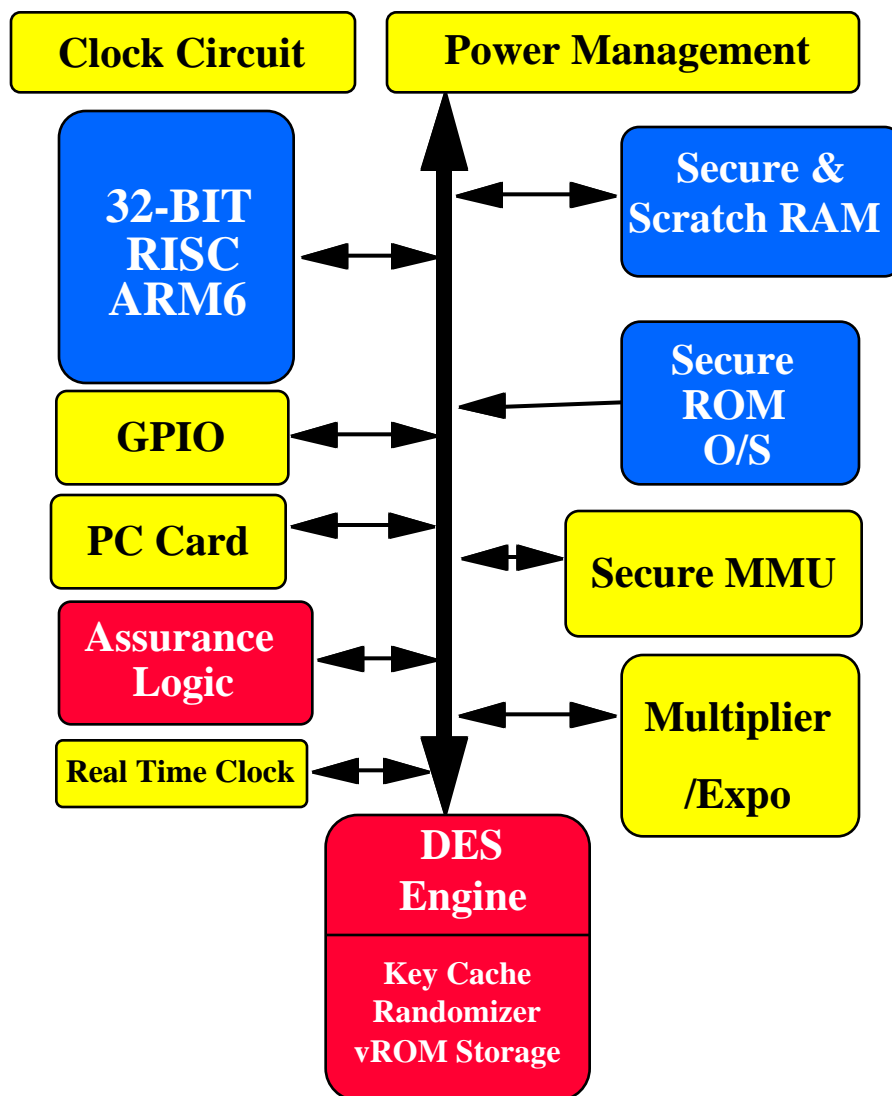
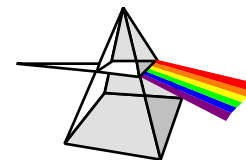




- ◆ PC Card (PCMCIA 2.1) interface
- ◆ 32-bit ARM RISC processor
- ◆ Key security features:
  - Special hardware DES engine with integrated key cache
  - All digital non-deterministic randomizer
  - Real time clock for secure time stamping
  - Key management: RSA - 1024 bits, Diffie-Hellman - 1024 bits with hardware assist
  - Signature: DSS, RSA
  - Hash: MD5, SHA1
  - Secure memory management unit (encrypted external code)
  - Physical logic protection designed to meet NIST level 3
- ◆ Samples 3Q97, production 3Q97

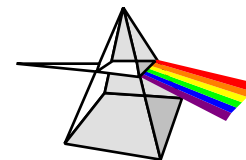
# Embedded Security Solutions

## VMS310 Architecture

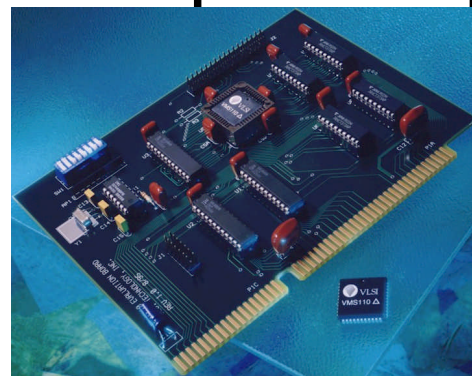


## Embedded Security Solutions

### VMS110 /VMS110E / VMS113 - Standalone DES

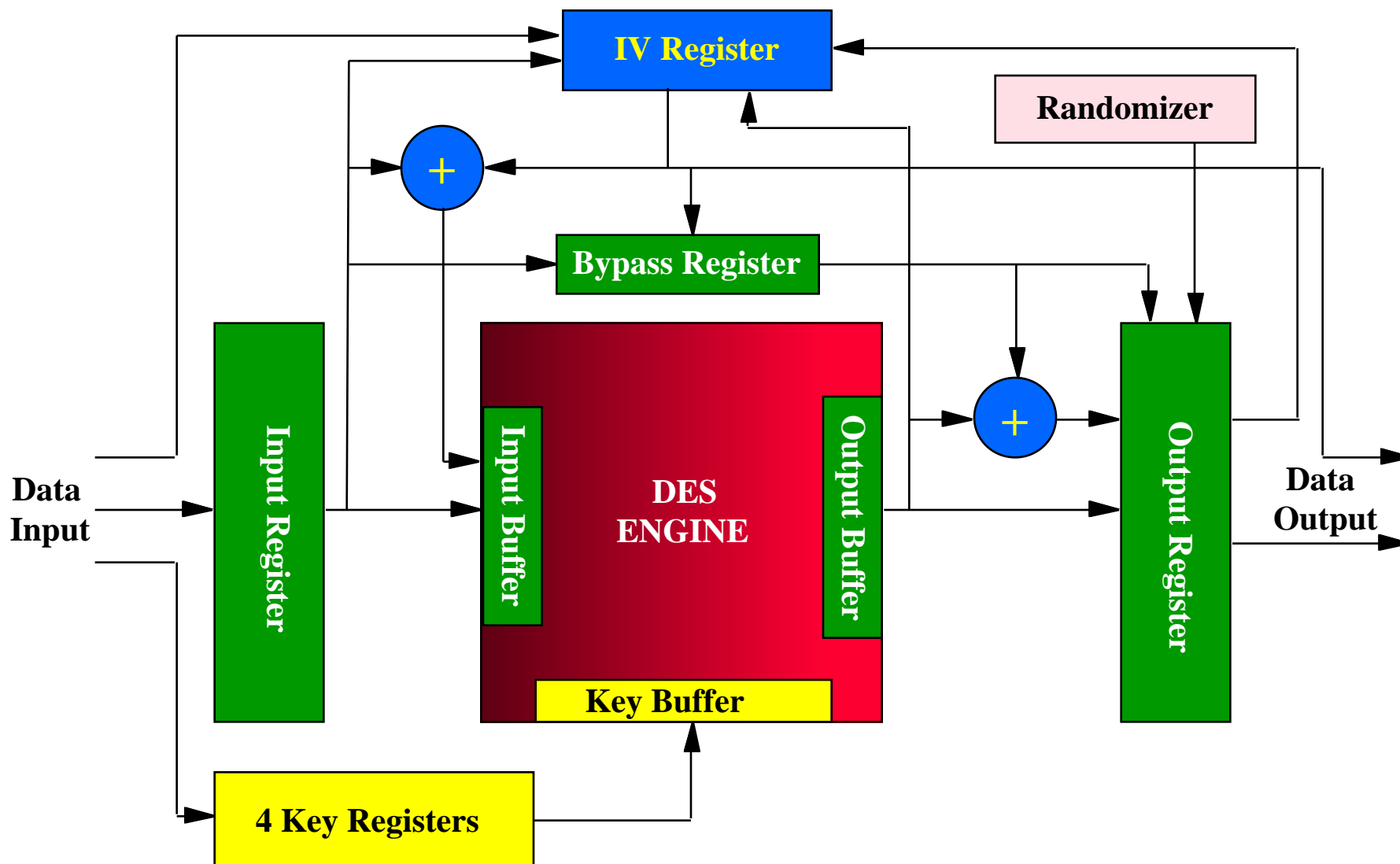
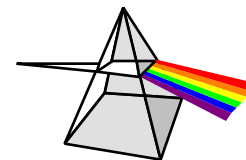


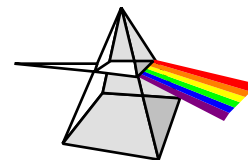
- ◆ NIST certified to FIPS-PUB Standard 46-2 Data Encryption Standard (DES)
- ◆ High speed single DES Electronic Codebook (ECB) and Cipher-Block-Chaining (CBC)
  - 284 Mbps at 40Mhz
  - Simple register interface for low firmware overhead
  - Built-in all digital, non-deterministic randomizer
  - Built-in key cache for high speed cryptographic context switching
- ◆ VMS110 samples and production now.
- ◆ VMS113 adds pin and register compatible triple DES capability
  - Samples now
- ◆ VMS110E is an exportable VMS110
  - Samples 1/97, Production 6/97
- ◆ Evaluation boards, software, and documentation available



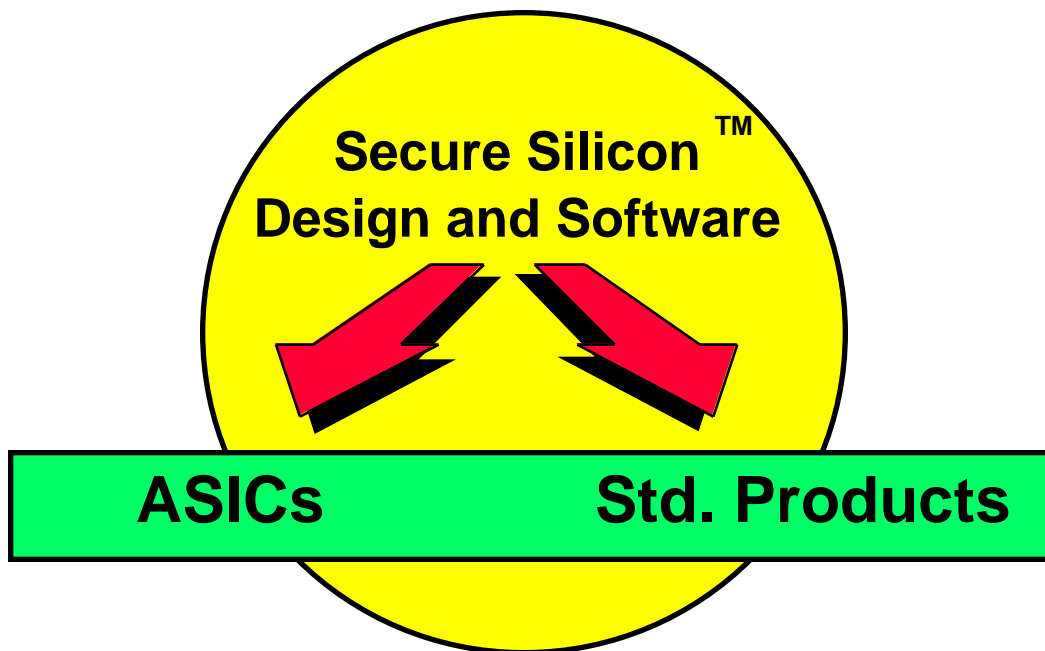
# Embedded Security Solutions

## VMS110 /VMS110E/ VMS113 Architecture





Leveraging ASIC & Crypto Expertise to Help Our Customers Succeed



- Time-to-market
- Price/Performance
- Integration
- Risk Reduction