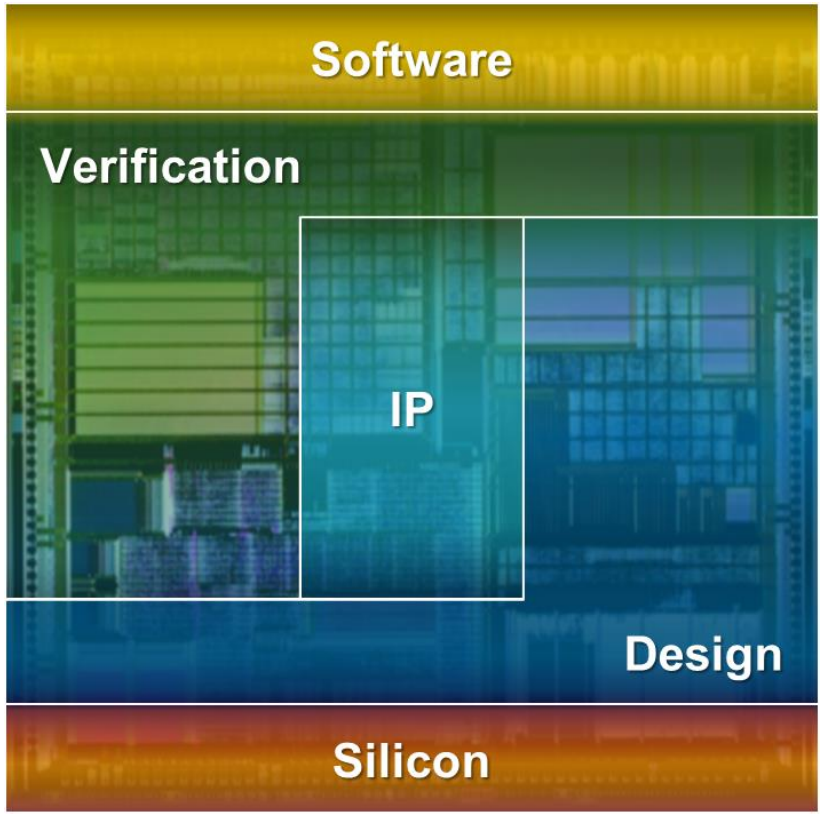
SYNOPSYS®
Silicon to Software™

Security in Standard Interface Protocols

Zongyao Wen

October 3rd, 2019

Synopsys: Silicon to Software



Software
- Application security testing & quality
- Leader in Gartner's Magic Quadrant

Verification
- Fastest engines & unified platform
- HW/SW verification & early SW bring-up

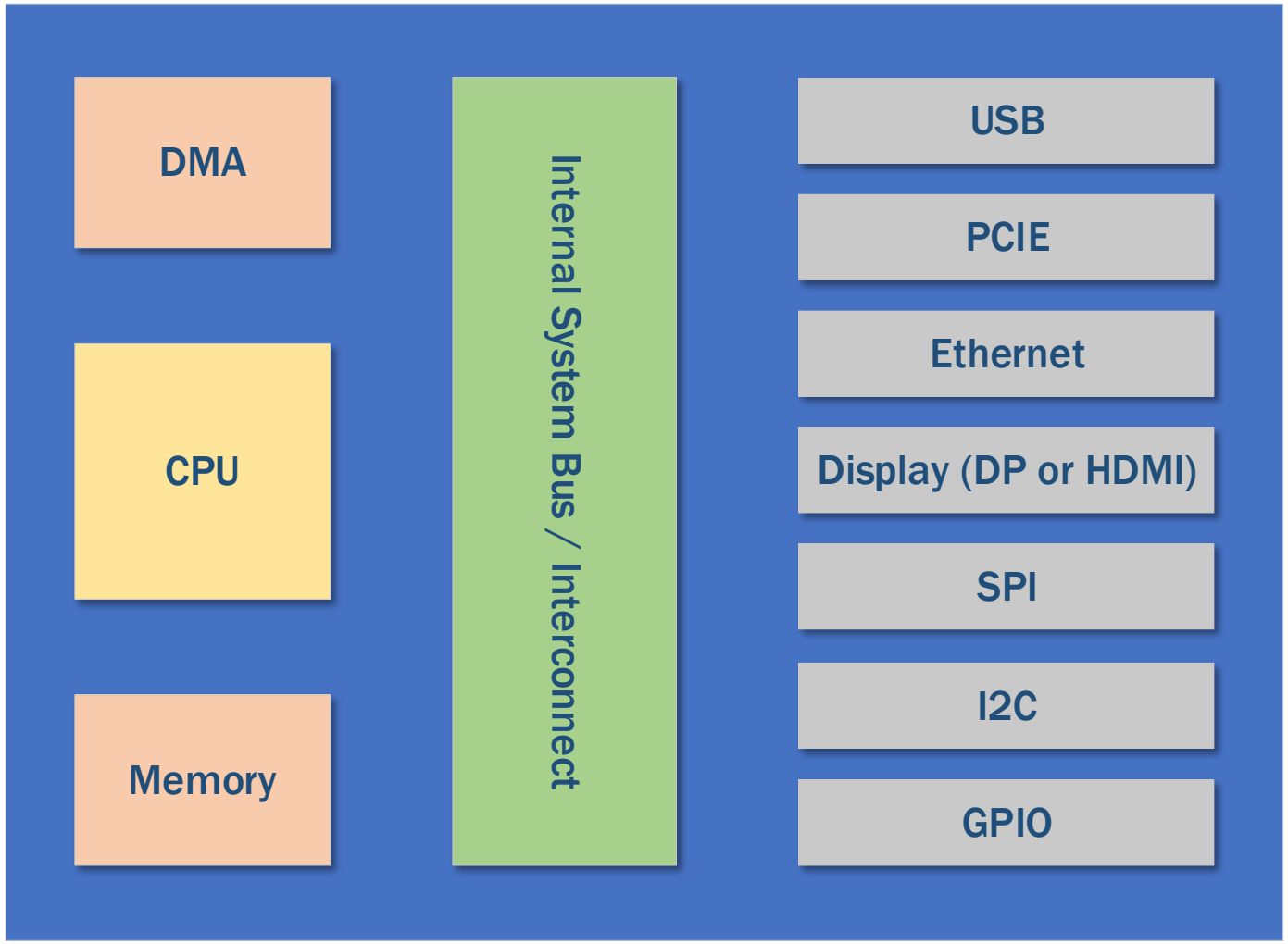
IP
- Broadest portfolio of silicon-proven IP
- #1 interface, analog, embedded mem. & phys. IP

Design
- Digital & custom AMS platforms
- Best quality of results & highest productivity

Silicon
- TCAD, lithography tools & yield optimization
- Down to 5nm & below

Protocol Standards

- Increasing number of internal and external interfaces in a SoC design
- Each interface is an access point into the system and can be a security risk
- IP usages are high to reduce TTM and cost



Security Features and Research in Standard Protocols

	Protocols	Security Features and Research
Internal Bus	AMBA	AXI, AHB and APB *PROT signals and secure memory ranges
	OCP	Security Parameters & MSecure Bits
External	USB	USB Authentication Protocol (R1.0)
System Bus	PCIE	Process Address Space ID (PASID w/ privileged), Access Control Services (ACS)
Storage	NVME	Sanitize, Write Protect, Authentication, TCG* defined locking/encryption
	SATA	ATA security commands
	SAS	SCSI Security Protocol, TCG reserved Types, Encryption and authentication
Display	DP, HDMI	HDCP
Memory	DDR	ECC (against rowhammering), research in SecureDIMM, ORAM
	NVDIMM	TCG has persistent memory group
Automotive	CAN/LIN	Nothing built-in, but there are researches and industry solutions, e.g. CANcrypt
Networking	Ethernet	MACsec Encryption

Identify Trusted Devices

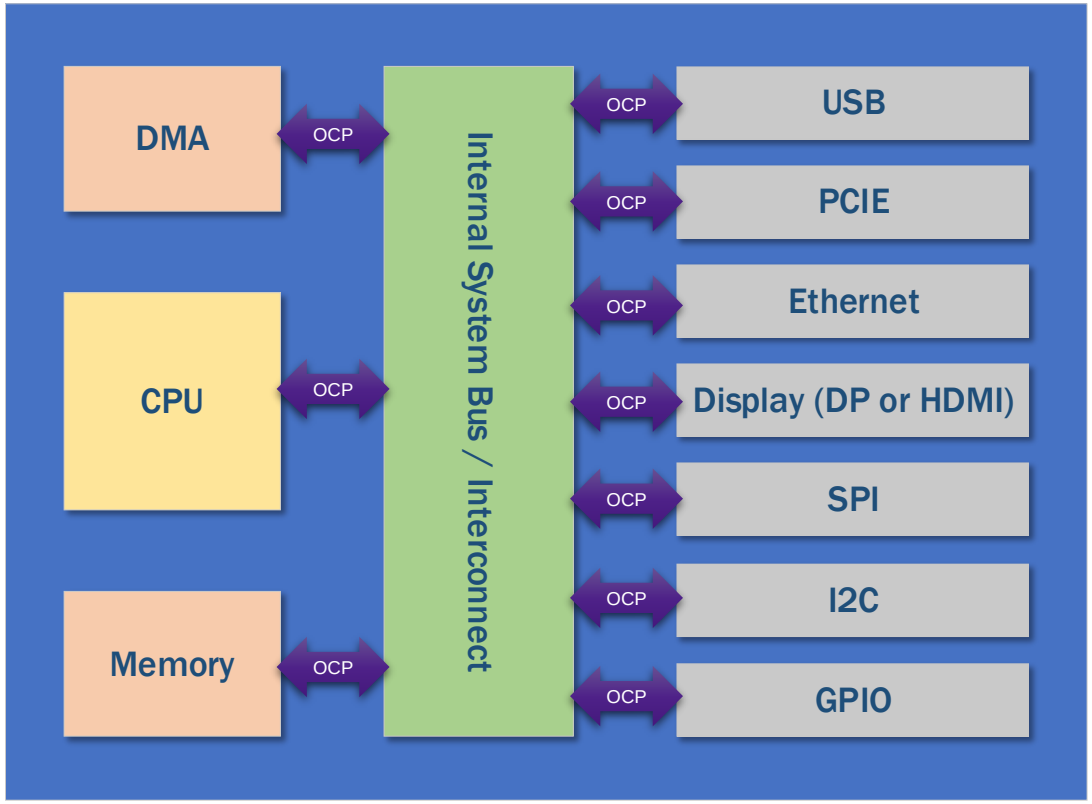
- USB Authentication Protocol

- 128-bit security
- Certificate based authentication
- Up to 8 slots (certificate changes)
  - 0-3 are USB-IF rooted certificate chains
  - 4-7 are additional certificate chains
- Three type of operations
  - Query: GET_DIGESTS <- DIGESTS
  - Read: GET_CERTIFICATE <- CERTIFICATE
  - Challenge; CHALLENGE <- CHALLENGE_AUTH
- Protocol encapsulations
  - USB PowerDelivery Extended Messages
  - USB Control Transfers, AUTH_IN and AUTH_OUT

Part of a Secure System

- OCP MSecure Bit Codes

- Open Core Protocol is a point-to-point interface that is bus interconnect independent
- Can connect to high performance processors
- Built-in fields to help identify secure vs. non-secure accesses
- Different access modes to help OS protect different memory regions



Bit	Value 0	Value 1
0	non-secure	secure
1	user mode	privileged mode
2	data request	instruction request
3	user mode	supervisor mode
4	non-host	host
5	functional	debug

Part of a Secure System

- PCIE ACS and Authentication

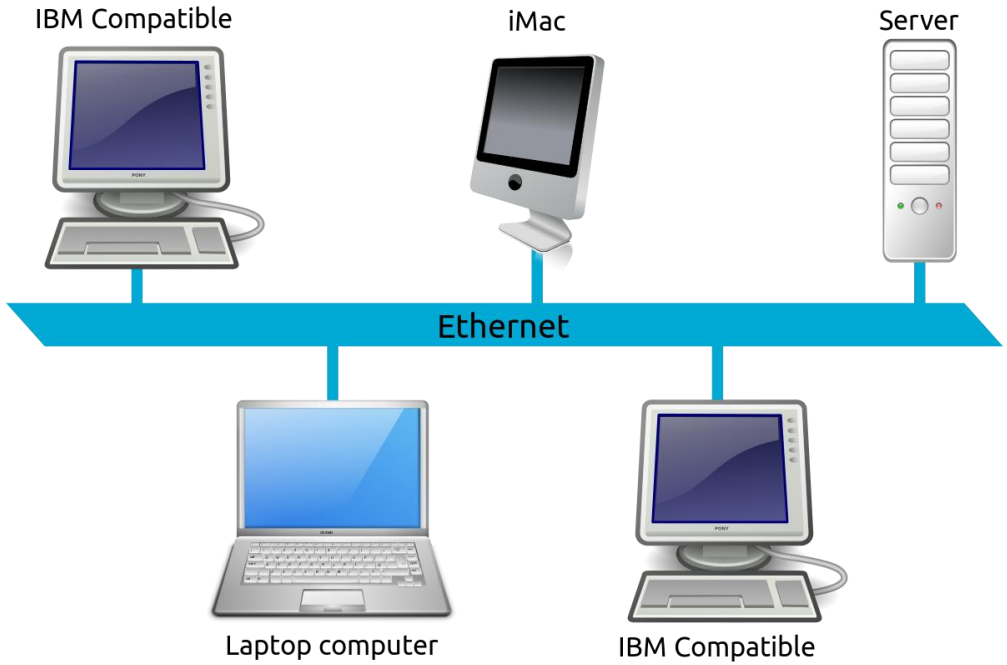
- ACS can be used to set up access protections over PCIE
  - ACS Source Validation
  - ACS Translation Blocking
  - ACS P2P Request Redirect
  - ACS P2P Completion Redirect
  - ACS Upstream Forwarding
  - ACS P2P Egress Control
  - ACS Direct Translated P2P
  - ACS I/O Request Blocking
  - ACS DSP Memory Target Access
  - ACS USP Memory Target Access
  - ACS Unclaimed Request Redirect

  Limitations
  - Optional
  - Multiple function device is not supported by all ACS features
- PCIE security specification being proposed
  - Certificate based authentication, similar to USB Authentication Protocol
  - Minimum security level higher than USB Authentication Protocol
  - Added more message types on top of USB Authentication Protocol

Network Protection In Hardware

- Ethernet MACsec (IEEE 802.1AE-2018)

- Encrypt data on Layer 2 point-to-point connection
  - Higher throughput than IPSec (Layer 3), but less flexible
- Rely on key agreement protocol IEEE 802.1X
  - MACsec is not standalone and it is part of architecture
- Protects a whole frame except Destination and Source Addresses
- Support multiple cipher suites with a clear default
  - Default Cipher Suite is (GCM-AES-128)



Protect Digital Content

- Introduction to HDCP

- Designed to securely transmit Audio & Visual Content between a Stream Transmitter and Stream Receiver(s)
- Each HDCP Device has a Unique Keyset provided by Digital Content Protection LLC (DCP).
- Content owners can confidently broadcast media products to set top boxes and the Blu-ray players that can only transmit to HDCP licensed devices, which don’t copy their content.
- Display port and HDMI HDCP protocols are similar but not identical. They do have different protocol documents

Protect Digital Content

- HDCP 1.3 in DisplayPort

Authentication

- An 64 – bit Pseudo-random value
- KSV (KEY selection vector) 40 bit value, has 20 one's and 20 zero's
- Km is private key
- Mi is 32 bit o/p of CM
- RI/RO is Mi
- Run for 105 clocks

Ciphers

- **HDCP block cipher**: run over CM0 for 108 and load to CM1 after 128 clocks
- **HDCP Re-key cipher**: run over CM0 for 55 clock and load on CM1 after 64 clocks
- **HDCP stream cipher** : run over CM0 & CM1 for every clock between CPSR and SR.

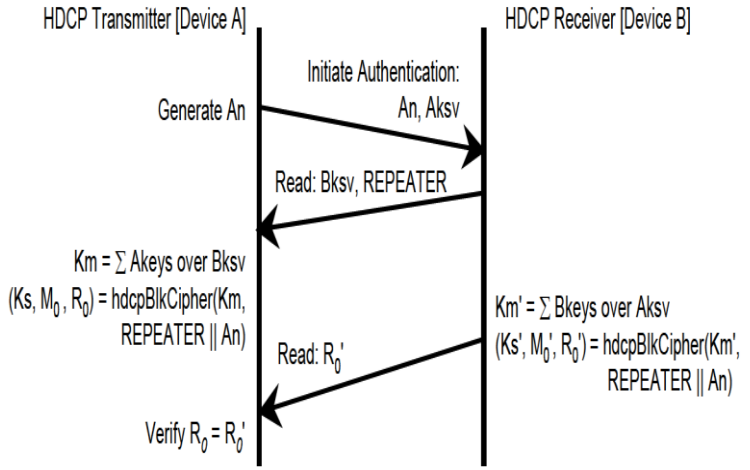


Figure 2-1. First Part of Authentication Protocol

4.1 Overview

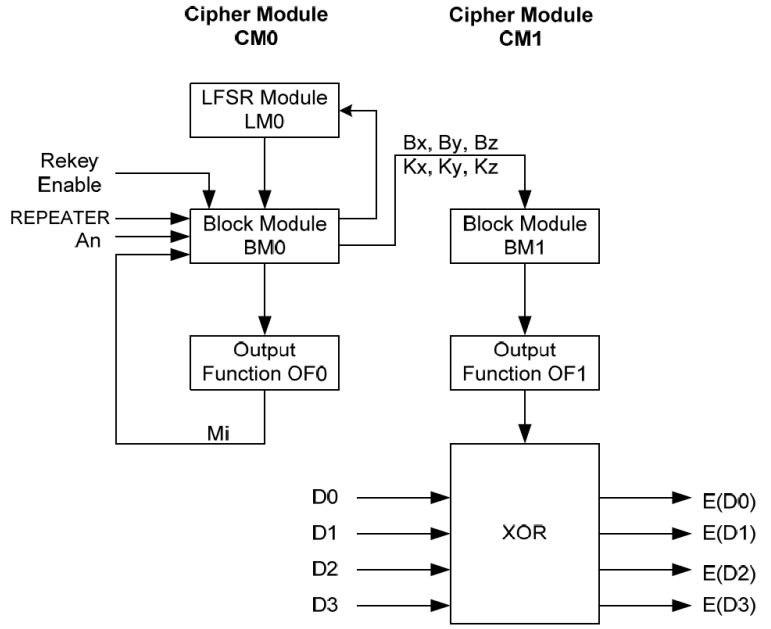


Figure 4-1. HDCP Cipher Structure

DP HDCP 2.2 overview

HDCP TX port has following parameters :

- lc128 Global Constance.
- 3072-bit RSA public key of DCP LLC denoted by kpubdcp.
- rtx: a 64-bit pseudo-random value.

HDCP RX port has following parameters :

- **lc128** : All HDCP Devices contain a 128-bit secret Global Constant denoted by lc128.
- **Receiver ID**. A 40-bit value that uniquely identifies the HDCP Receiver. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes
- **Receiver Public Key.** A 1048-bit Unique RSA public key of HDCP Receiver denoted by *kpubrx*.
- **DCP LLC Signature**: A 3072-bit A cryptographic signature calculated over all preceding fields of the certificate

Authentication Flow :

- Authentication and Key Exchange (AKE) – The HDCP Receiver's public key certificate is verified by the HDCP Transmitter. A Master Key *km* is exchanged.
- Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 7 ms.
- Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key *ks* with the HDCP Receiver.
- Authentication with Repeaters – The step is performed by the HDCP Transmitter only with HDCP Repeaters. In this step, the repeater assembles downstream topology information and forwards it to the upstream HDCP Transmitter.

Summary and Challenges

- Functional verification of protocol security features
  - Synopsys Verification IP (VIP) already supports many security features
  - For example, HDCP 1.3 to 2.0 are supported by Synopsys DisplayPort and HDMI VIP, PCIE ACS and Ethernet MACsec.
- Trust worthy IPs of the standard interfaces
  - Synopsys pre-verified IP and VIP
- Reliable implementation of cryptographic algorithms, random number generation and PUF to support the authentication and encryption protocols
  - Synopsys Secure IP provides Root of Trust modules, security algorithms, true random number generator, PUF and Non-Volatile Memory
- Not all protocols has security features
  - Require security community be more involved with protocol spec working groups. Add encryption of data into more protocols.

SYNOPSYS®
Silicon to Software™

Thank You