The World's First USB3.0 Storage Controller

Gideon Intrater

Who are we?

- A fables semiconductor startup
- Based in California and China
- Focusing on SOCs leveraging the new USB 3.0 standard for Personal Storage products

Expand the USE and user EXPERIENCE of CONSUMER STORAGE

Over the past 10 years…

Consumer and PC evolution has accelerated:

- *Hard drives:* *10GB → 100GB → 1TB → 2TB*
- *Flash drives:* *128KB → 100MB → 1GB → 128GB*
- *x86 CPU speed:* *400MHz → 1GHz → 4GHz*
- *Digital cameras* *1 Mpixel → 3 Mpixel → 10 Mpixel*
- *iPODs*
- *External storage*

Access and Consumer Electronic interconnect has evolved:

- Ethernet 10/100 → 10/100/1G → 10/100/1G/10G
- DSL 128Kbps → 1Mbps → 100Mbps
- WiFi 802.11b → 802.11g → 802.11n
- Cellular GPRS → EDGE → UMTS → LTE

But USB has stagnated

- USB USB2.0 → ……..

USB 3.0 – Features and Benefits

- 500MB/s bandwidth capability
  - 4 times faster than gigabit Ethernet, 10 times faster than USB 2.0
- Multiple concurrent data streams
  - Make it possible to operate close to the theoretical throughput
- Improved host hardware and driver (xHCI)
  - Lower CPU burden improves user experience and power efficiency
- Improved peripheral power management
  - Peer-to-peer communication enables much improved device power mgmt.
- Backwards compatible with all legacy USB ports
- Greater operational current for bus powering and charging devices

	Song / Pic	256 Flash	USB Flash	SD-Movie	USB Flash	HD-Movie
	4 MB	256 MB	1 GB	6 GB	16 GB	25 GB
USB 1.0	5.3 sec	5.7 min	22 min	2.2 hr	5.9 hr	9.3 hr
USB 2.0	0.1 sec	8.5 sec	33 sec	3.3 min	8.9 min	13.9 min
USB 3.0	0.01 sec	0.8 sec	3.3 sec	20 sec	53.3 sec	70 sec

USB 3.0 – Adoption Timeline

2009
- External Storage
- ExpressCard, PCIe cards

2010
- Workstation Laptops
- Desktop PCs
- USB HUBS
- External Blu-Ray drives
- Enterprise backup

2011
- PC Port Replicators
- USB Monitors
- Media Players
- Camcorders
- Cameras
- Cell phones
- Printers

2012+
- DTV
- DVR/IPTV
- Game Consoles
- Server Virtualization
- Wireless…

The Challenge – External HDD controller

- High speed bridge from USB3 to dual SATA II HDD
  - Capable of delivering the full throughput of a SATA HDD
  - Even higher bandwidth when running in a RAID configuration
- Security through Authentication and Encryption
- Flexibility to support OEM differentiation
- Minimal external component count
- Telecom grade 5GHz SERDES-based USB3 PHY (for use with very cheap cables….)
- And, all the above at Consumer Electronic prices

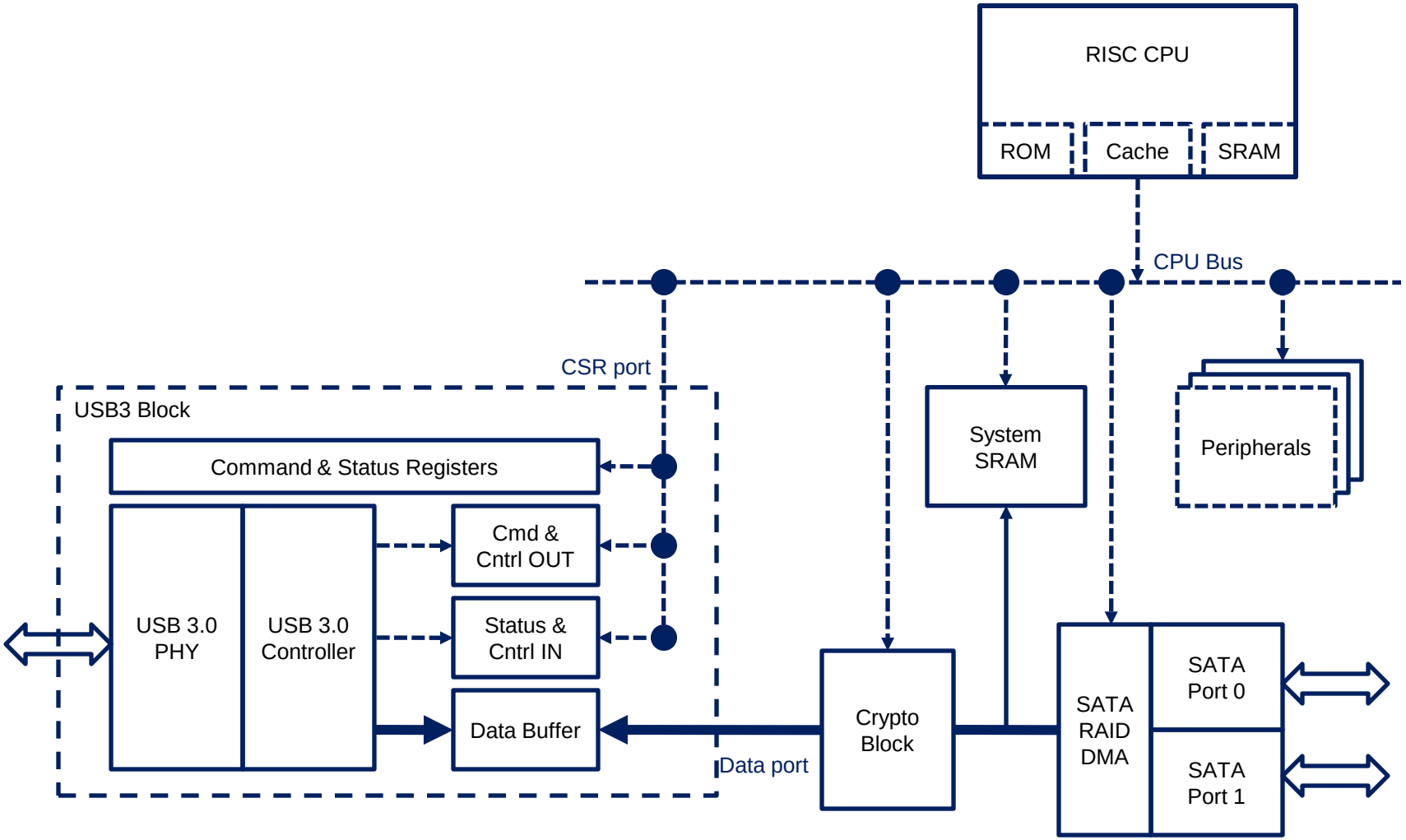
Performance Challenges

- Get as close as possible to 500MBytes/s, the maximum theoretical speed of USB 3.0
- On-the-fly translation of the USB Attached SCSI Protocol (UASP) to the ATA protocol
- Maintain the Out-Of-Order capabilities of USB/UASP and SATA/NCQ
- Control two storage devices in RAID mode to double the throughput achievable with a single drive
- Stay within USB BUS powering budget when combined with a single SSD/HDD!

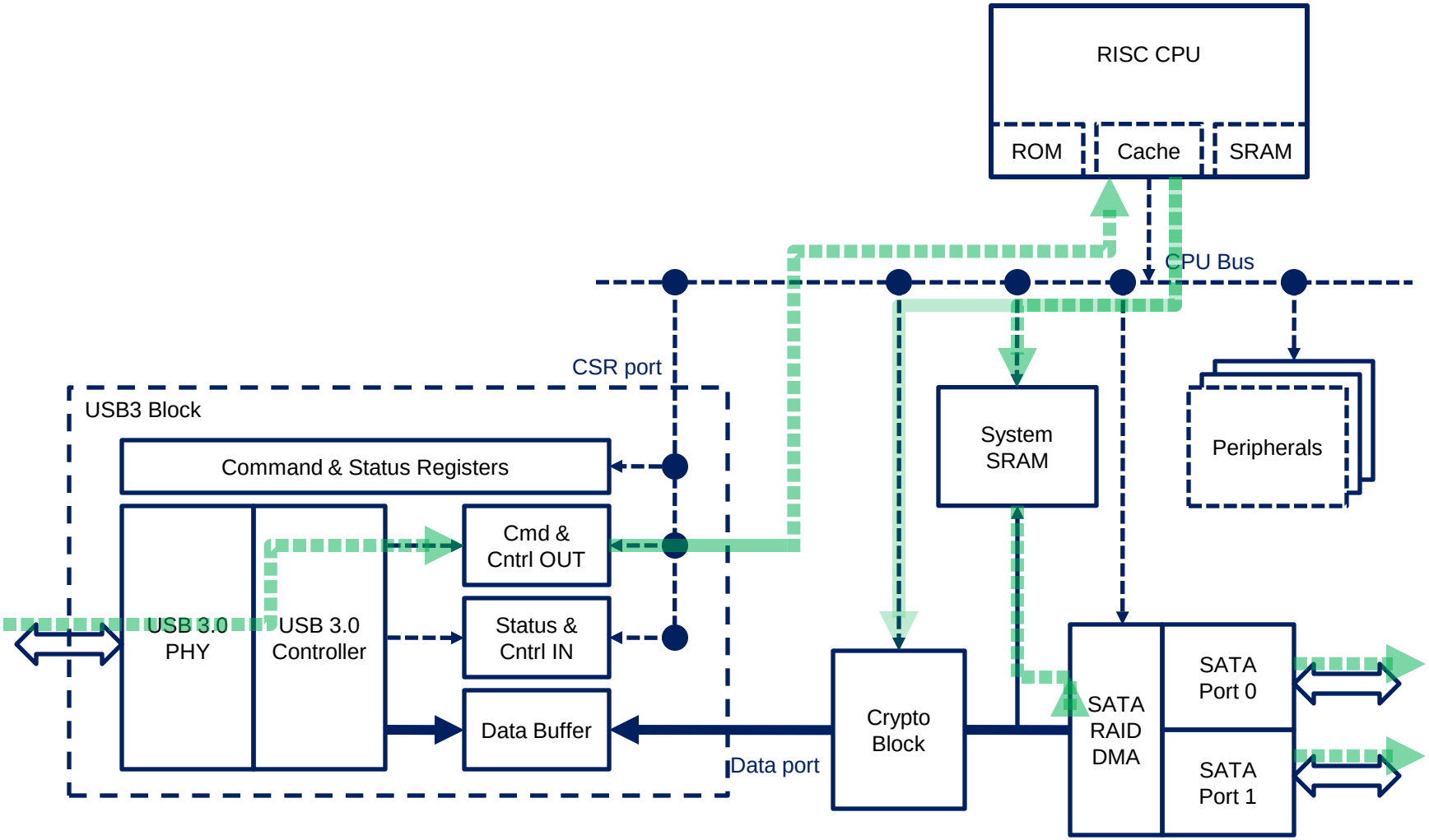
Performance Solution

- Operate a traditional control- and data-path split
- Control path:
  - Utilizes a RISC CPU for real time protocol conversion
- Data path:
  - Data is transferred with fast DMA engines while maintaining Out-of-Order on both sides
  - Hardware support for automatic RAID support

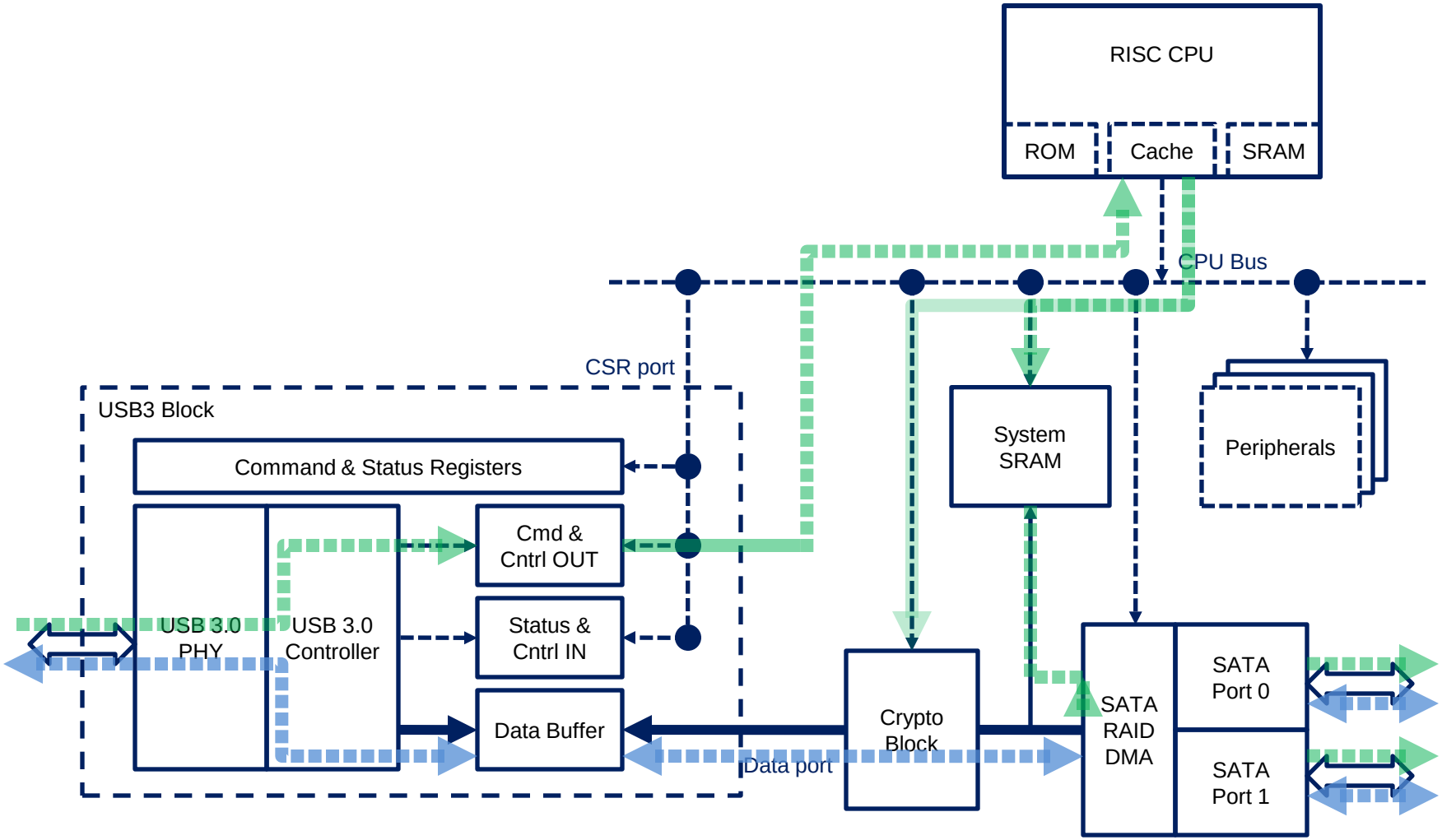
Control and Data Paths



Control Path

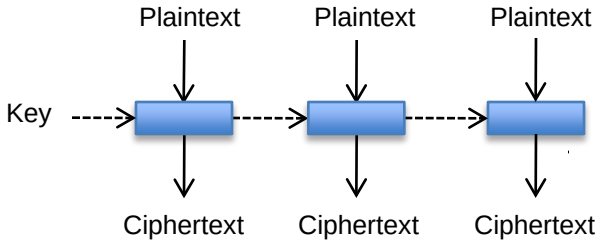


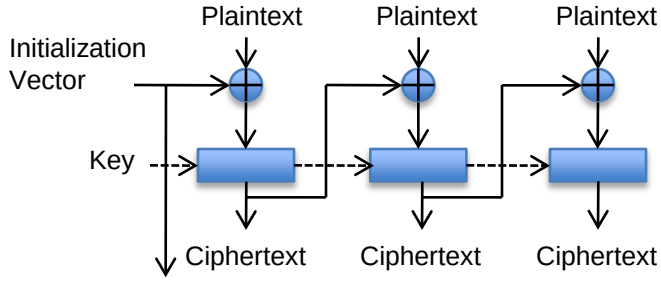
Data Path

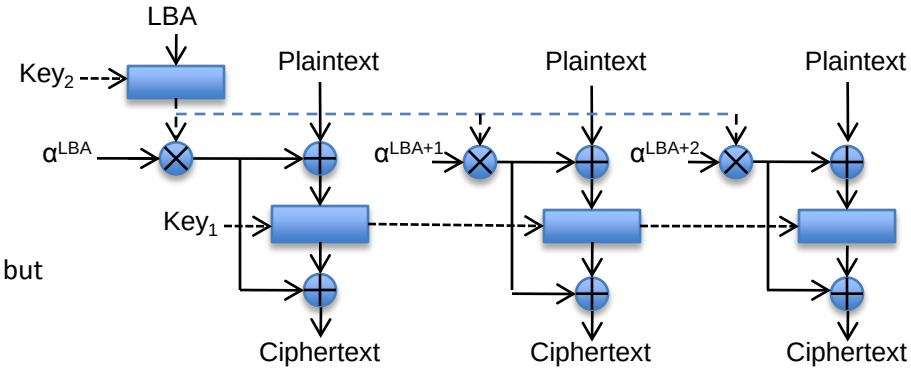


Data Encryption Standards in Storage

- AES-ECB
  - The simplest mode of AES
  - Easily scaled by using parallel engines
  - Vulnerable, as multiple locations use the same key
- AEC-CBC
  - XORs the results of the previous encryption with the plaintext of current block
  - Not scalable due to data-dependency
  - Requires storing the IV with each block
- AES-XTS (IEEE 1619)
  - Tweaks the key based on the address
    - Requires one complex operation per sector, but minimal complexity for consecutive blocks
  - Can easily scale







Encryption Challenges

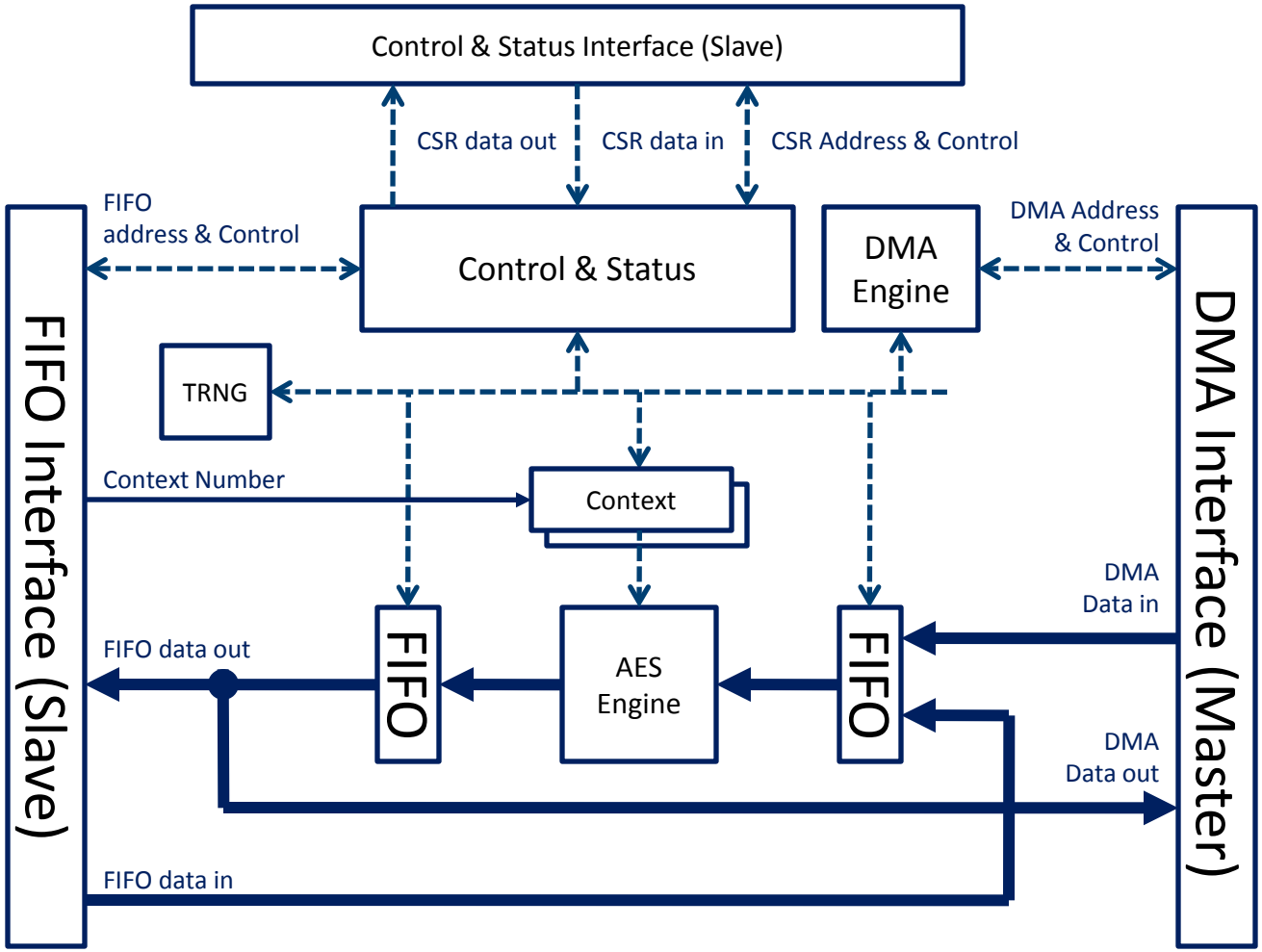
- Encrypting the HDD reduces the data exposure risk if the HDD is lost or stolen
- The state-of-the-art in storage encryption is the IEEE 1619 standard utilizing the AES-XTS protocol
  - The encryption key is tweaked based on the sector address
    - This is expensive in cycles for a random sector address, but quite efficient for sequential sectors
  - Supporting two concurrent data streams in and out of the RAID storage system
  - Minimal intervention from the CPU to maintain control and data-path separation

Encryption Solution

- A multi-threaded multi-core AES block with an integrated DMA unit
  - Multiple concurrent AES computational cores deliver the raw bandwidth
  - Multi-threading enables keeping the state of both HDD channels and appearing to the AES engine as if the sectors are sequential

Note: the definition and the design of the crypto block were done in collaboration with Discretix Technologies

Crypto Block



Authentication

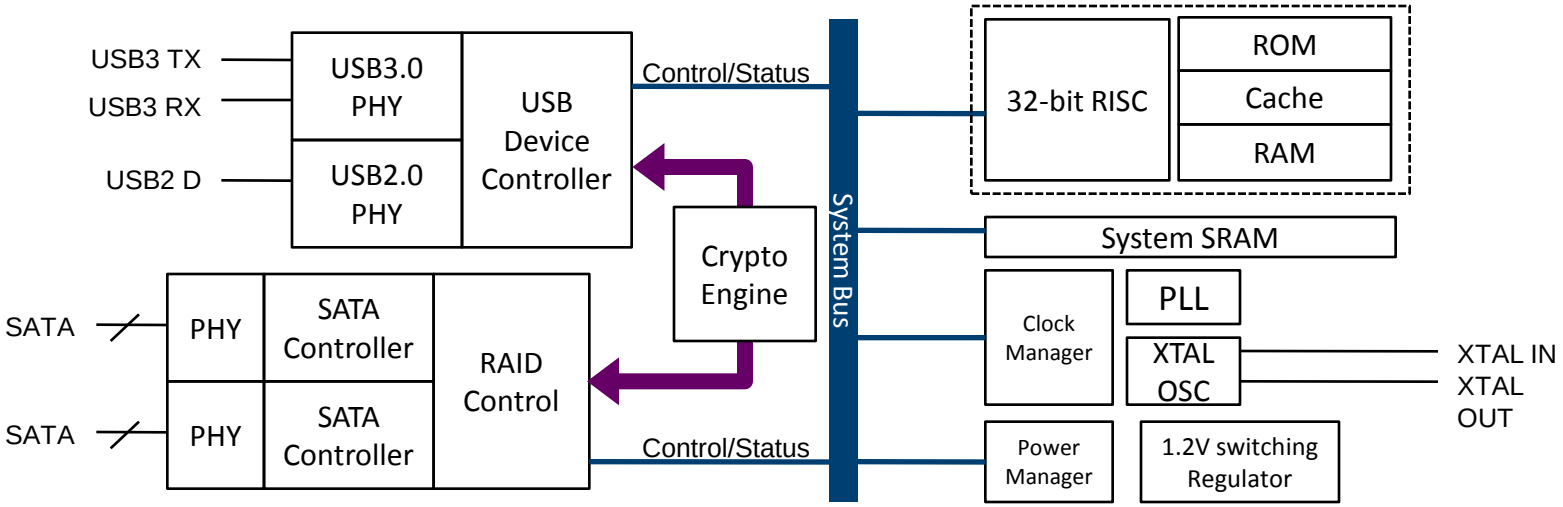
- Challenge: support IEEE 1667
  - A public-key based authentication protocol for transient storage devices
  - The public-key authentication is a complex algorithm that executes infrequently
- Solution:
  - A perfect fit for our RISC processor which implements the whole algorithm in software
  - The only HW assist is a True Random Number Generator (TRNG)

Hitting the Low-Cost Target

- Use the lowest-cost process that can carry a 5GHz USB 3.0 PHY – a 130nm generic process
- Process selection that balances I/O to core logic and; Balances speed to power dissipation
- Integrate on chip all the auxiliary circuitry to reduce BOM:
  - Voltage regulators
  - Oscillators and PLLs
  - I/O controllers

SW6318 - USB 3.0-to-SATA Bridge

- USB 3.0 device controller and PHY
  - USB Attached SCSI Protocol (UASP)
- Dual SATA-II host controller and PHY
  - Native Command Queuing (NCQ)
- High Performance RISC CPU
- IEEE 1619 hardware AES engine
- IEEE 1667 Authentication
- Standard I/O controllers
- Voltage regulator and PLL



Key Performance Attributes

- Enables UASP based Out-of-Order command processing for nearly 2X throughput improvement over BOT
- Throughput – USB is no longer is the bottleneck
  - Non-blocking performance for today's SSD/HDD drives
  - Near doubling of performance utilizing RAID 0 mode
- CPU resources – Customer oriented optimizations
  - Extensive development tools, SDK, clocking/power management
  - Tightly coupled SRAM
  - Adequate onboard ROM for FLASH-less operation
- 0.13u CMOS provides balance of I/O count, die size & power

Die Photo

Summary

- In just one year, we took a USB 3.0-to-SATA Bridge from concept to an implementation
- To achieve product success multiple engineering challenges including performance, security and cost were overcome
- Balancing all of these, the SW6318 SOC delivers uncompromised performance at consumer electronic prices

Thank You!

www.symwave.com