Design of A Pre-Scheduled Data Bus for Advanced Encryption Standard Encrypted System-on-Chips

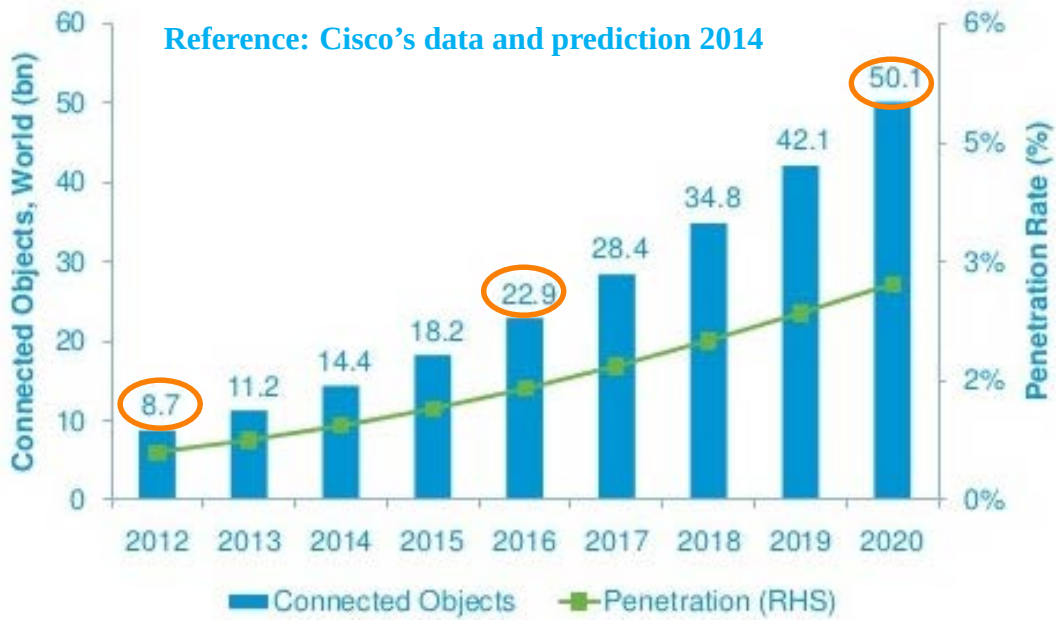
Wujie Wen

Assistant Professor,

ECE Department, FIU,

January, 2017

IoT, The Next Big Thing!



- In 2012:

1.6 T Things, 8.7 B connected (0.6%) .

- By 2016:

1.7 T Things, 23 B connected **(1.3%).**

- **By 2020:**

1.9 T Things,

50 B will be connected (2.7%).

Note: T (trillion) B (billion)

	2013	2014	2015	2016	2017	2018	2019	2020
Per annum (mn)	2,508	3,129	3,849	4,656	5,525	6,414	7,269	8,030
Per day (mn)	6.9	8.6	10.5	12.8	15.1	17.6	19.9	22.0
Per hour (units)	286,350	357,239	439,420	531,558	630,713	732,196	829,825	916,674
Per minute (units)	4,773	5,954	7,324	8,859	10,512	12,203	13,830	15,278
Per second (units)	80	99	122	148	175	203	231	255

- In 2013:

80 things per second.

- **By 2016:**

148 things per second.

- **By 2020:**

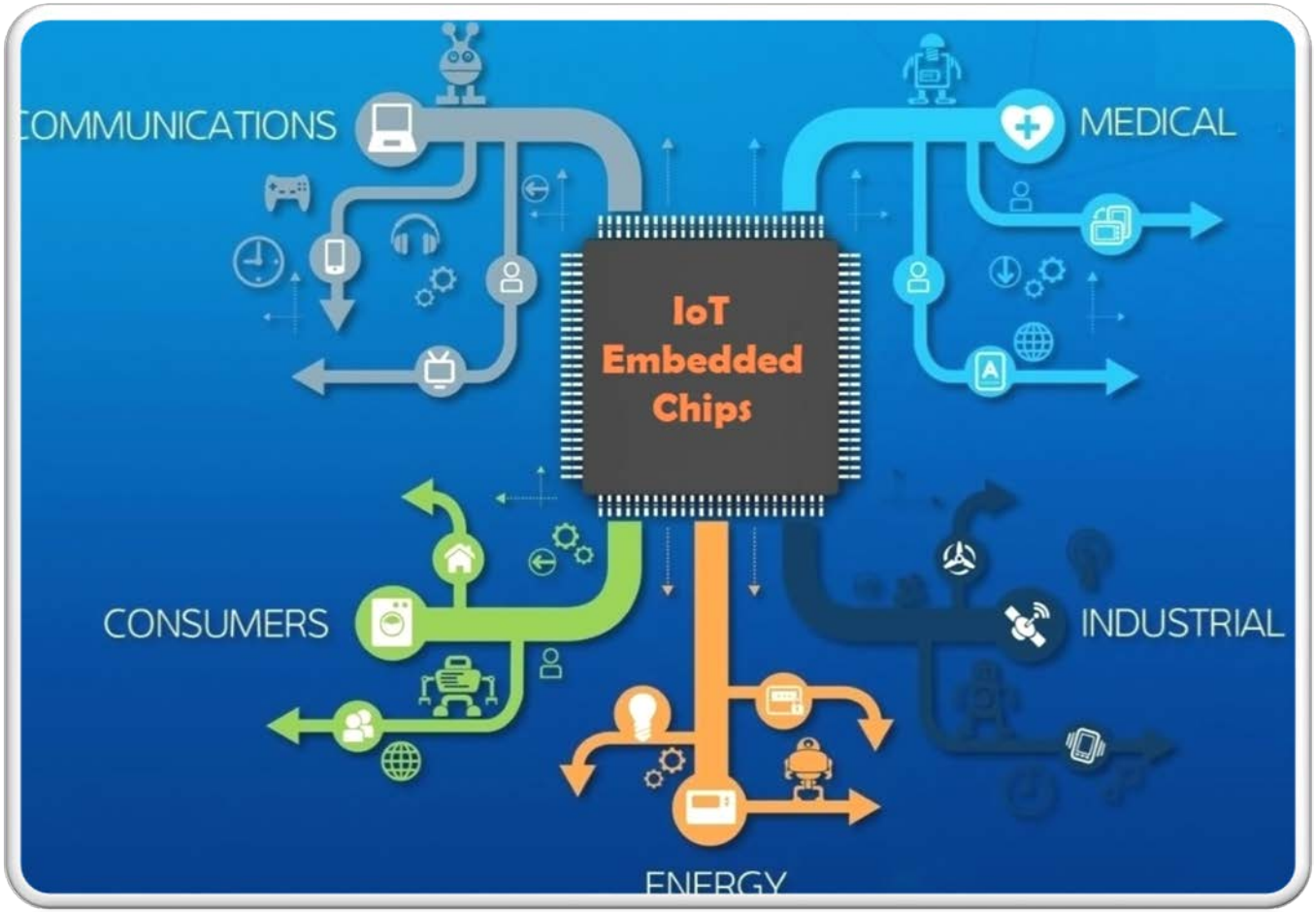
255 things per second.

Silicon Vendor Eye the IoT

- **ARM**:
  The ARM IoT subsystem for **Cortex-A, -R, and -M** enables companies to simplify the process and improve time to market. (June**, 2015**)
- **Intel**:
  The **Intel® Quark™** microcontroller brings low-cost connectivity, integration, and compatibility to the latest IoT applications.
  (Intel IoT Insights 2015)
- **Samsung**:
  Samsung revealed a new chip family, **Artik 1, Artik 5 and Artik 10**, to power the IoT, putting it in more direct competition with Intel, Qualcomm and others in the quest to connect everything.
  (May 2015)
- **AMD**:
  Project SkyBridge, designed to fit the various requirements of IoT and embedded solutions, will feature the new family of APUs and SoCs with AMD's GCN core architecture.
  (The new AMD product roadmap in **2015**)

IoT Chip Demands

In the future, most new physical objects will be implanted chips and sensors!



Small Scale

Low Power

High Security

Challenges of IoT Chip Design

Challenges and Problems of IoT Chip Design:

1) AMBA AHB and AXI, Wishbone, OCP, CoreConnect, STBus
   - Define **a large number of signals and complex structures**
   - Transfer data **in linear and row major order**
   - **Limited resources** for tiny chips – **Overhead cost** for complex security algorithms

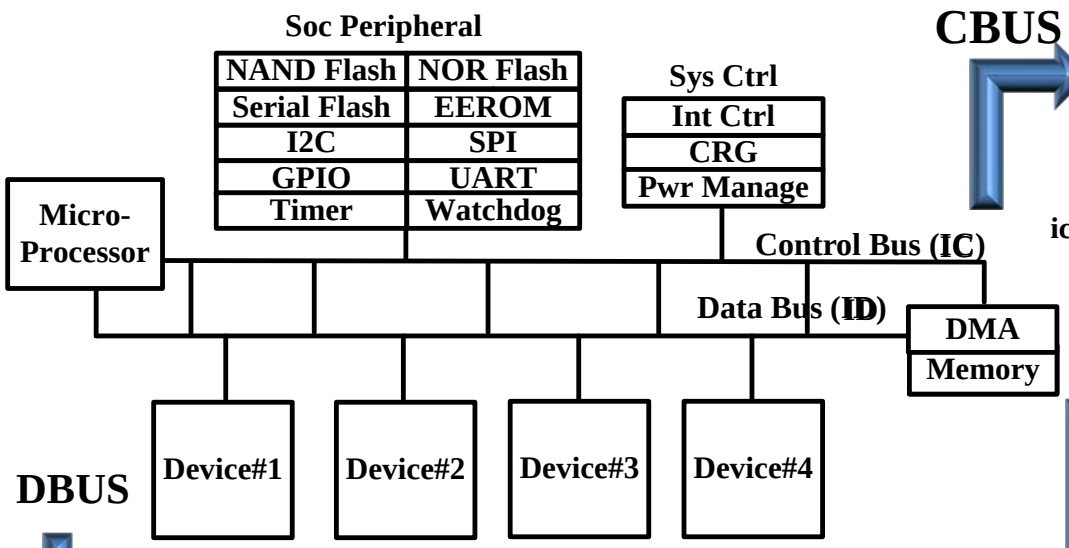
   [Wong_TVLSI'12, Kermani_TC'12, Wang_TVLSI'10]

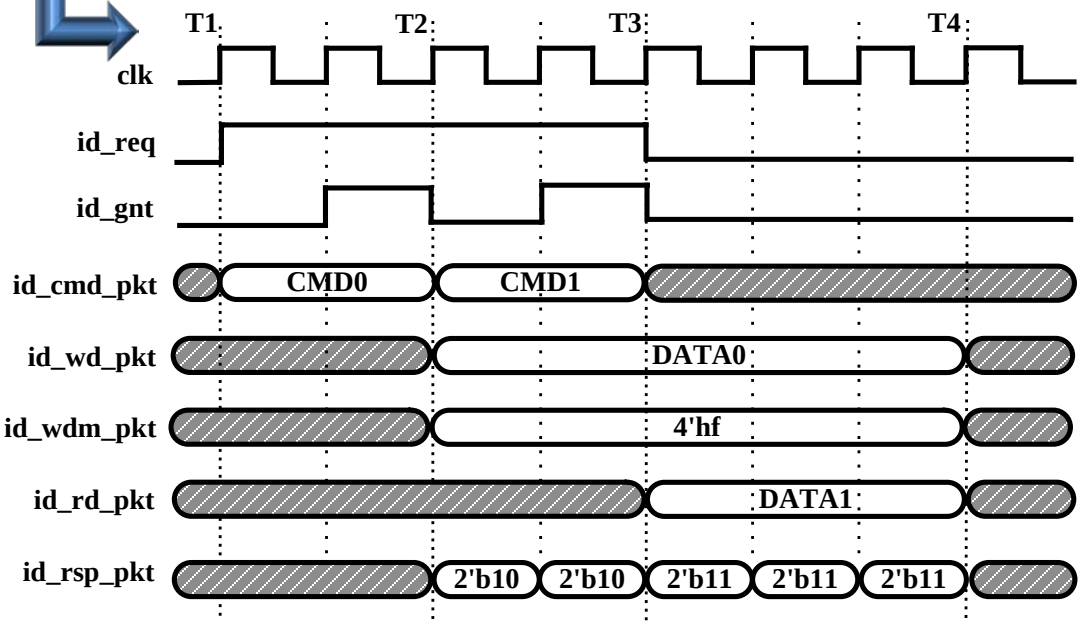
Contributions :

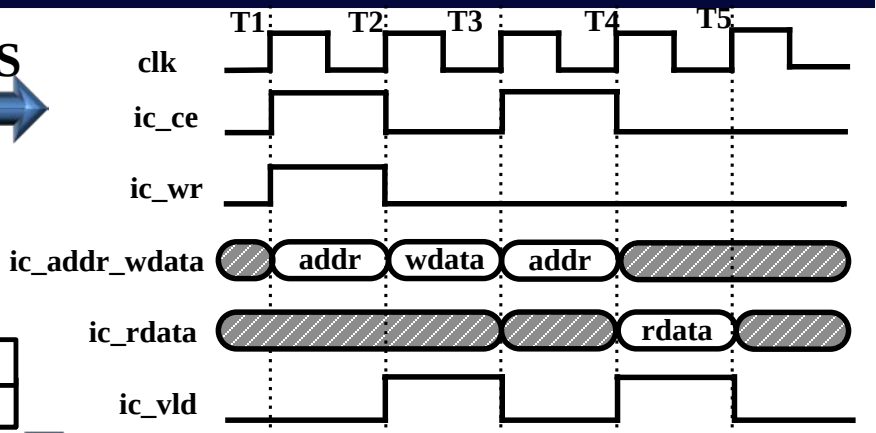
A Low-Cost and Low-Power Data Bus (DBUS) which provides three transfer modes:

Block, State, and Linear

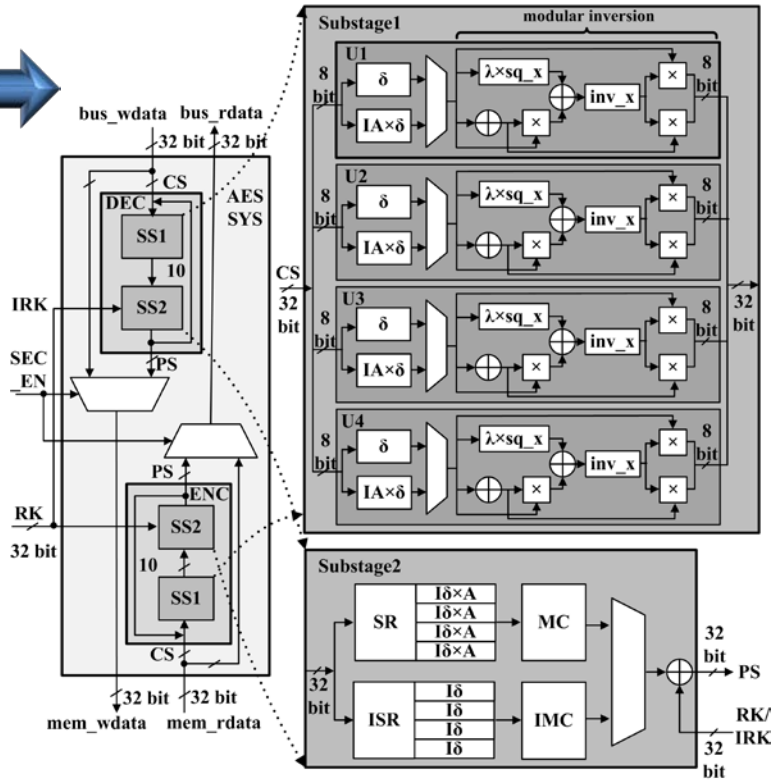
CBUS-DBUS Architecture



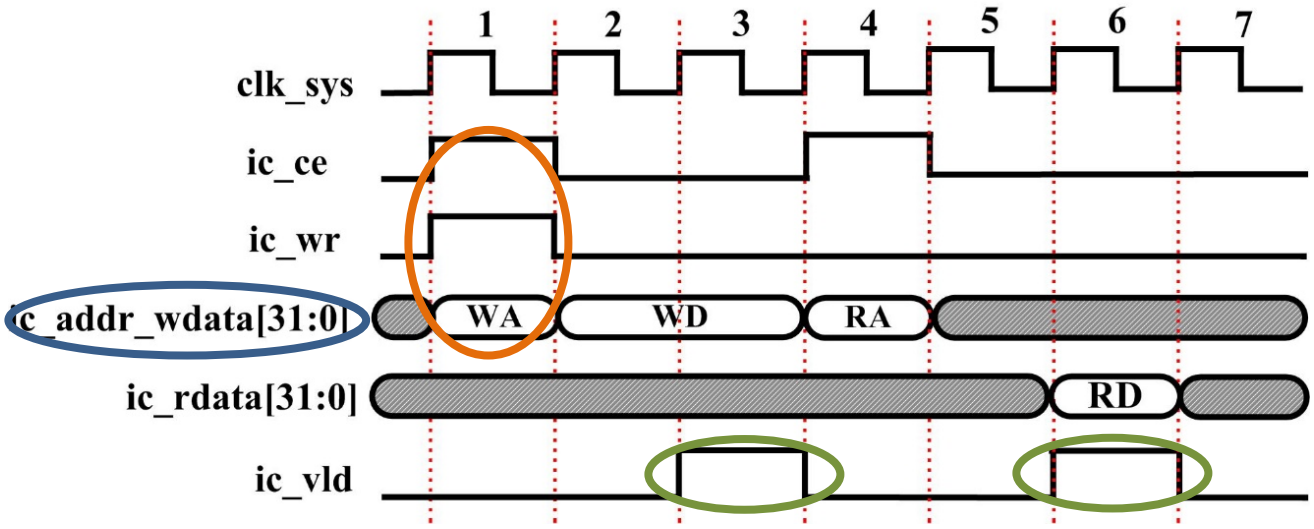




CBUS: 69, APB : 103, AHB: 119



CBUS Protocol



CBUS Protocol

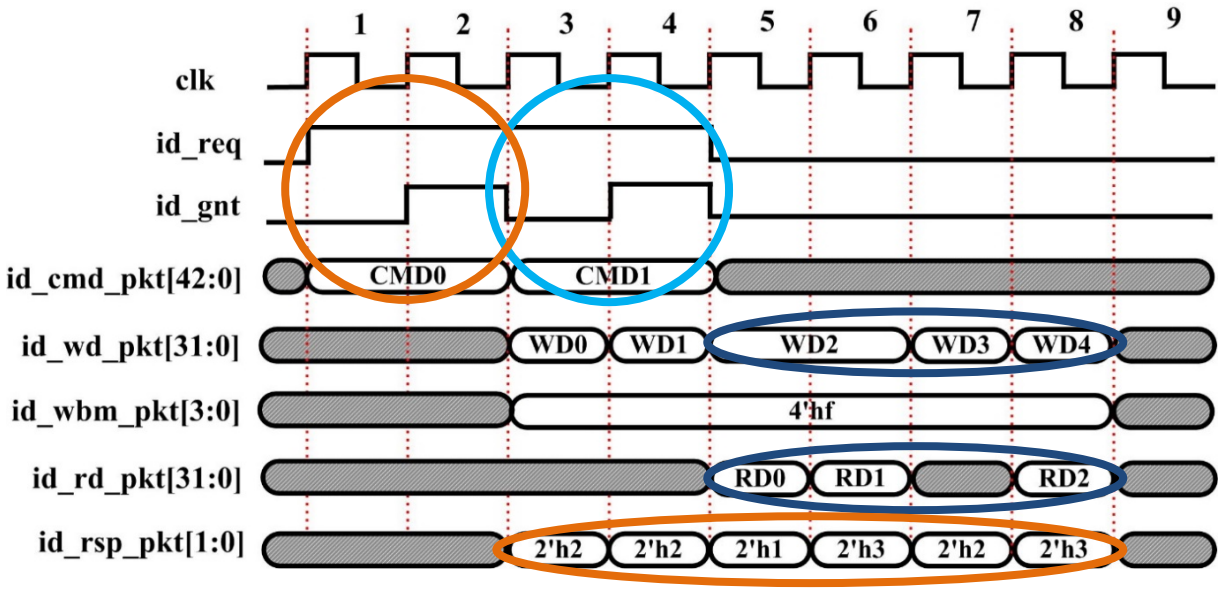
- ✓ **Wire Efficiency**
- ✓ **One-cycle Command**
- ✓ **Vld/Ack/Sync**
- ✓ **Response Timer**

ERROR/RETRY/DISCARD

CBUS: 69 wires, APB : 103 wires, AHB: 119 wires

Name	Source	Description
c_en	Micro-processor	CBUS request enable
c_wr	Micro-processor	CBUS transfer Direction
c_addr_wdata[31:0]	Micro-processor	**Shared signals: write address, read address, and write data**
c_rdata[31:0]	CBUS slaves	CBUS read data
c_vld[1:0]	CBUS slaves	CBUS data valid

DBUS Protocol



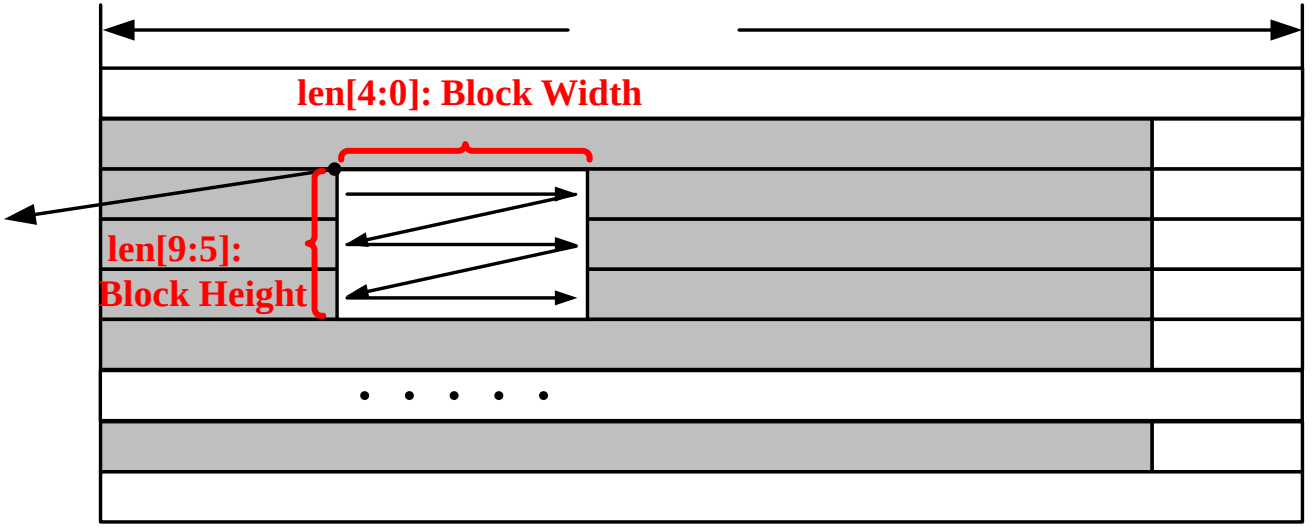
DBUS Protocol

- ✓ **CMD Preprocessing**
- ✓ **Full-duplex Bus**
- ✓ **Two-Cycle cmd/resp**

Name	Source	Description
d_req_x	Masters	DBUS Request.
d_gnt_x	DMA	DBUS Grant
d_addr[31:0]	Masters	**Address, Transfer Direction, and Transfer Mode/Size.**
d_wr (id_cmd_pkt[42:0])		**id_len[11:10]: 2'b00 Linear, 2'b01 Block, 2'b10 State.**
d_len[11:0] (id_cmd_pkt[42:0])		**2'b11 Reserved**
d_wd_pkt[31:0]	Masters	DBUS Write Packet
d_wbm_pkt[3:0]	Masters	DBUS Write Data Bye Mask
d_rd_pkt[31:0]	DMA	DBUS Read Packet
d_rsp_pkt[1:0]	DMA	DBUS Write and Read Packet Valid.

DBUS Linear and Block Modes

DBUS Block Transfer Mode



Linear Mode:
ADDR: 32'h00
LEN: 12'h20

↳ {2'b00, 10'h10}
bits: 11:10, 9:0

0x00	0x04	0x08	0x0c	...	0x38	0x3c	...	0x3fc
...	...							
0xfc00	0xfc04	0xfc08	0xfc0c	...	0xfc38	0xfc3c	...	0xfffc

Block Mode:
ADDR: 32'h00
LEN: 12'h284

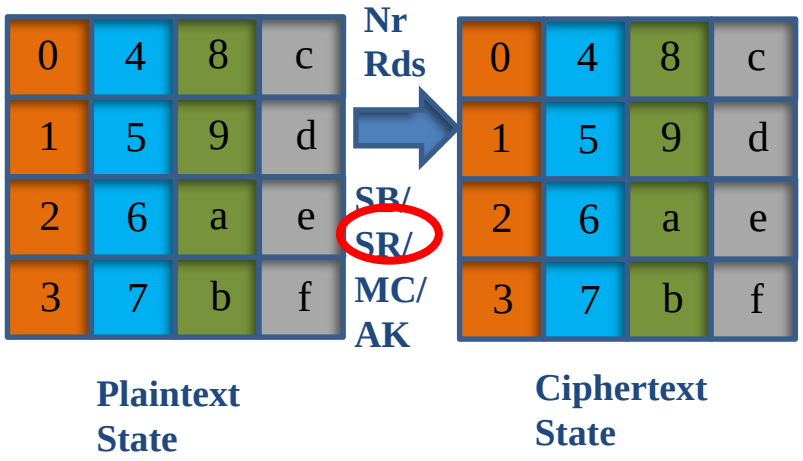
↳ {2'b01, 5'h4, 5'h4}
bits: 11:10, 9:5 4:0

0x00	0x04	0x08	0x0c	...	0x38	0x3c	...	0x3fc
0x400	0x404	0x408	0x40c	...	0x438	0x43c	...	0x7fc
0x800	0x804	0x808	0x80c	...	0x838	0x83c	...	0xbfc
0xc00	0xc04	0xc08	0xc0c	...	0xc38	0xc3c	...	0xffc
...	...							
0xfc00	0xfc04	0xfc08	0xfc0c	...	0xfc38	0xfc3c	...	0xfffc

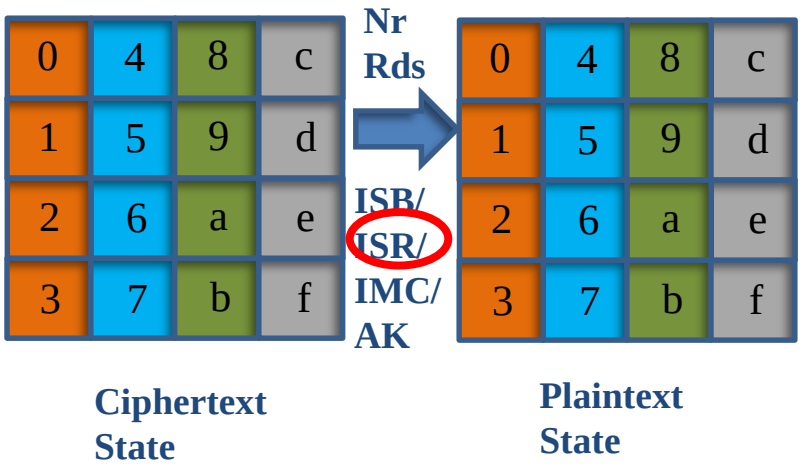
AES Mathematical Preliminary

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
   byte  state[4,Nb]

   state = in

   AddRoundKey(state, w[0, Nb-1])

   for round = 1 step 1 to Nr-1
      SubBytes(state)
      ShiftRows(state)
      MixColumns(state)
      AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
   end for

   SubBytes(state)
   ShiftRows(state)
   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

   out = state
end
```

AES Encryption



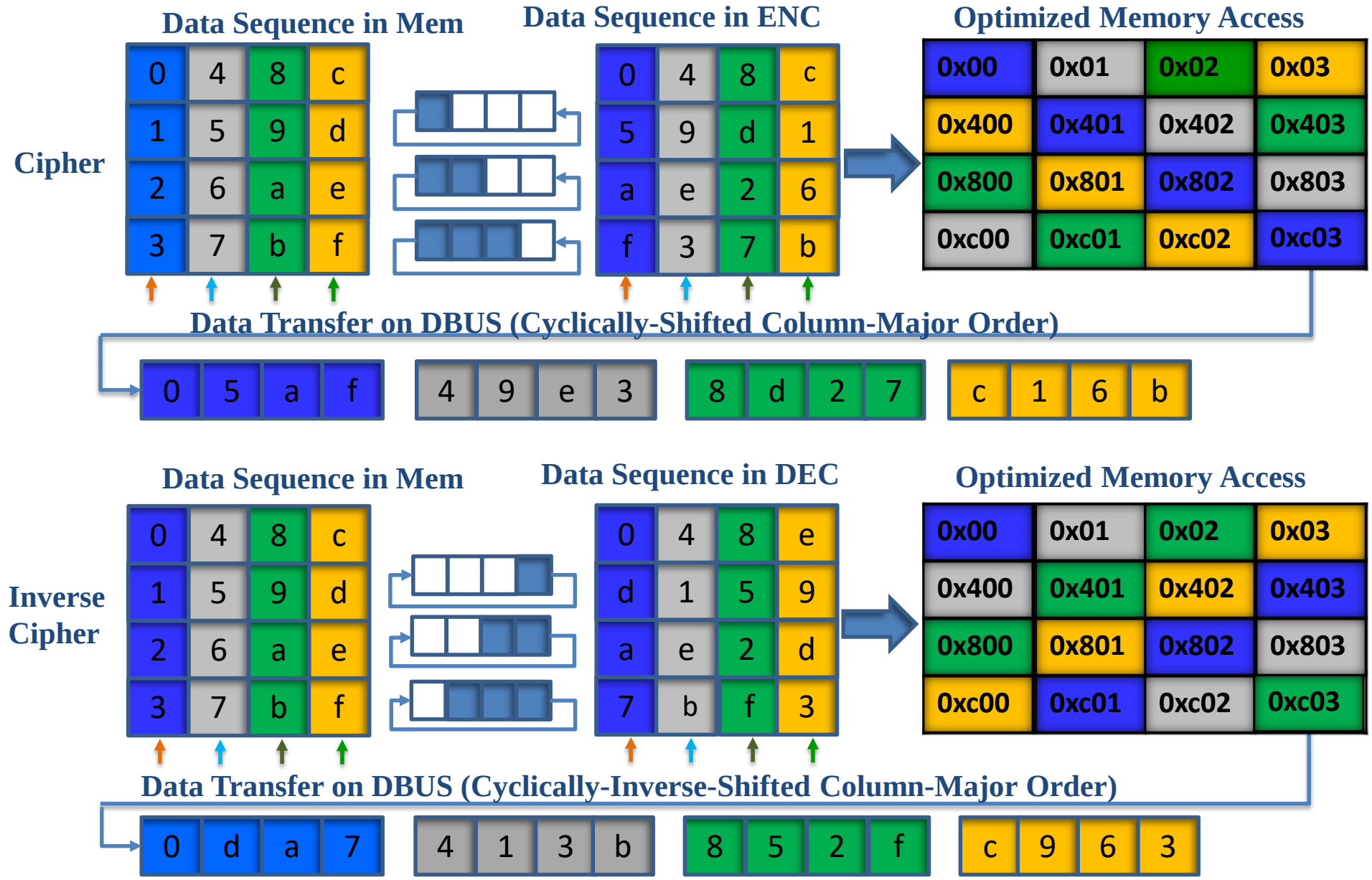
AES Decryption




```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
   byte  state[4,Nb]

   state = in

   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

   for round = Nr-1 step -1 downto 1
      InvShiftRows(state)
      InvSubBytes(state)
      AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
      InvMixColumns(state)
   end for

   InvShiftRows(state)
   InvSubBytes(state)
   AddRoundKey(state, w[0, Nb-1])

   out = state
end
```

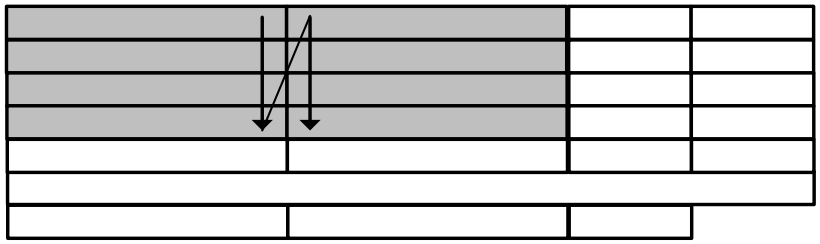
AES Data Sequence

State Mode:
LEN: 12'h284
{2'b10, 10'h1}
bits: 11:10, 9:0

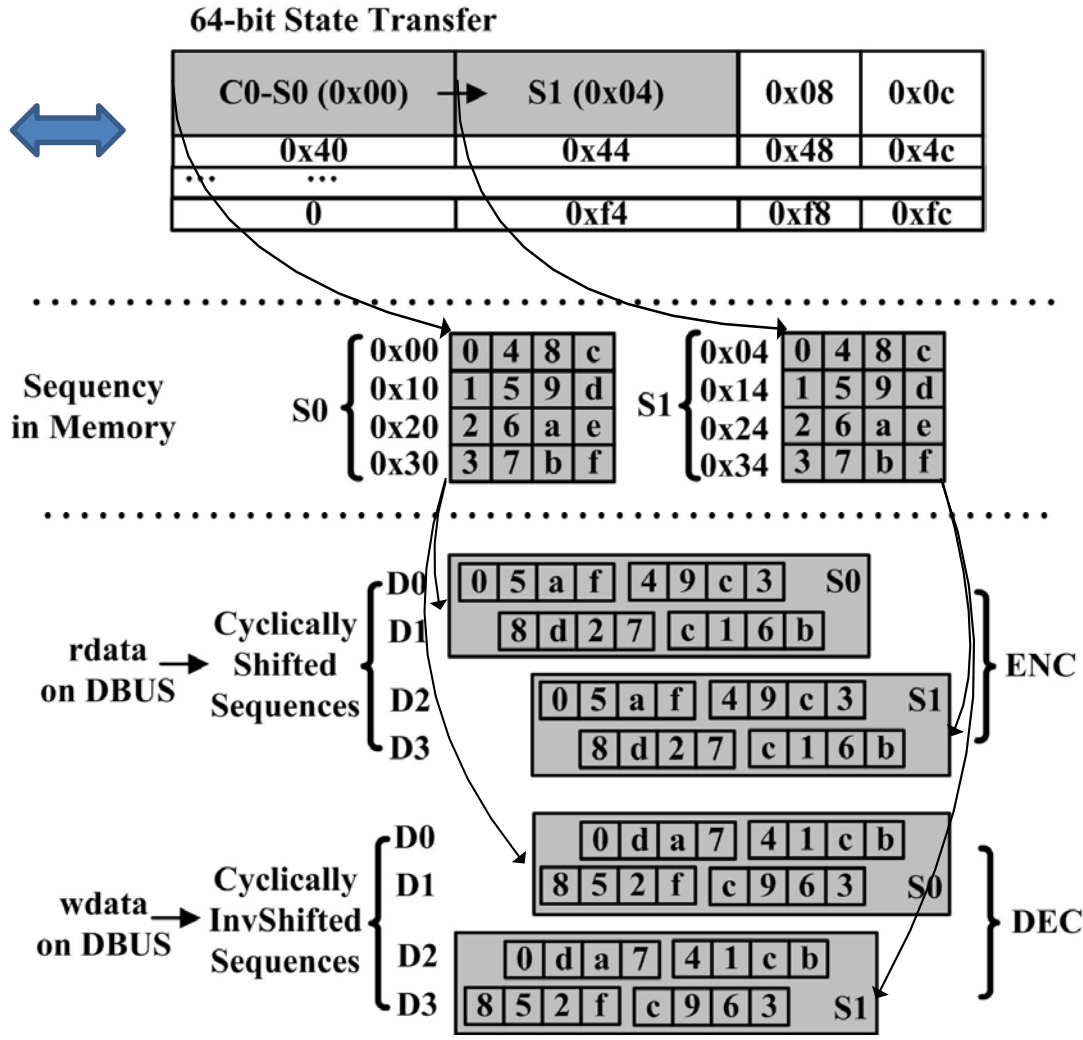


DBUS State Mode

Block Transfer Mode



AES State Transfer Mode



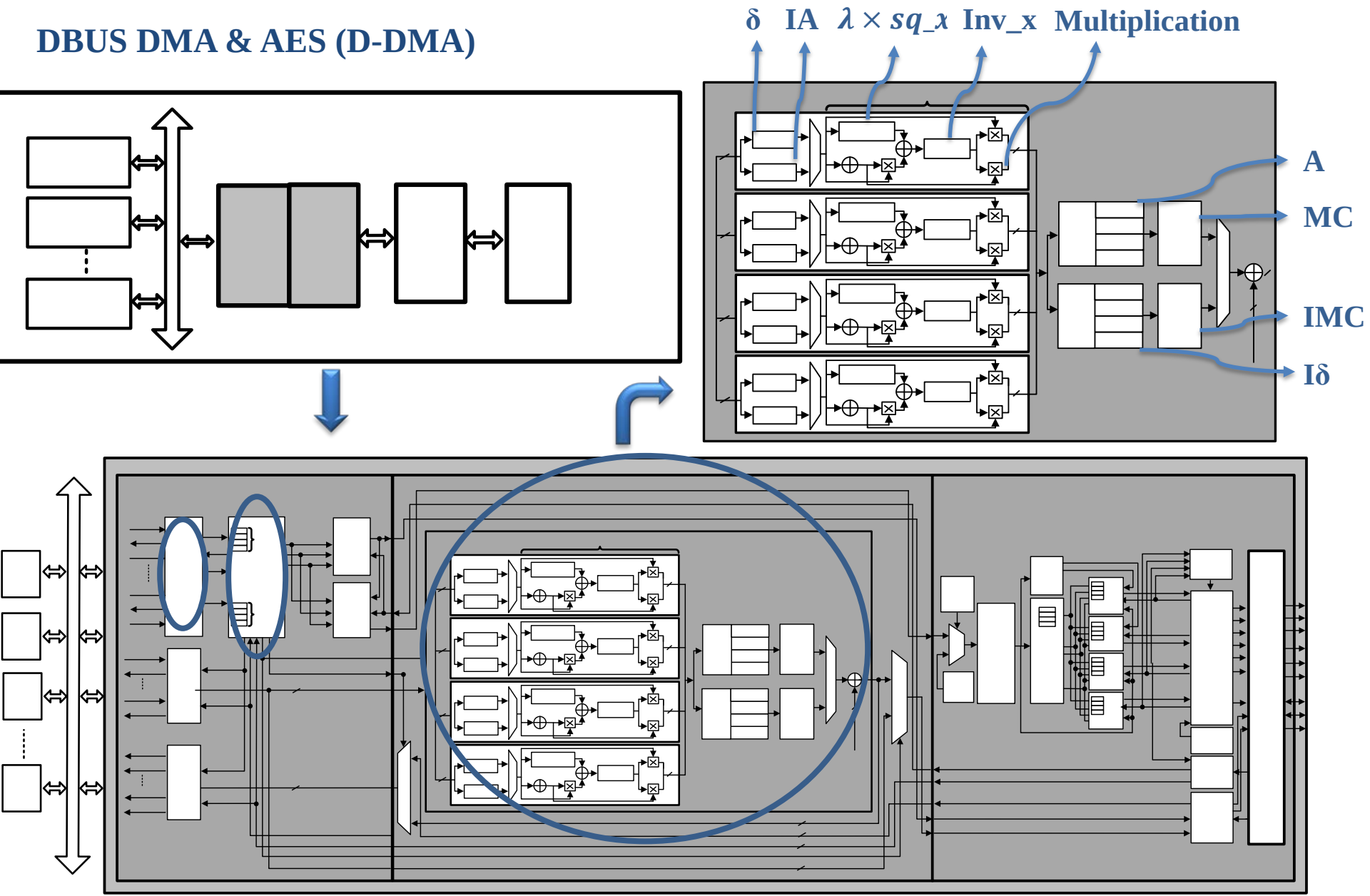
{2'b10, 10'h02}
bits: 11:10, 9:0

C0: {addr, len, wr}={32'h00, 12'h802, 1'b0}
D0: rdata->{0x00, 0x11,0x22,0x33, 0x01, 0x12, 0x23, 0x30}
D1: rdata->{0x02, 0x13,0x20,0x31, 0x03, 0x10, 0x21, 0x32}
D2: rdata->{0x04, 0x15,0x26,0x37, 0x05, 0x16, 0x27, 0x34}
D3: rdata->{0x06, 0x17,0x24,0x35, 0x07, 0x14, 0x25, 0x36}

{2'b10, 10'h02}
bits: 11:10, 9:0

C0: {addr, len, wdata_vld, wr}={32'h00, 12'h802, 8'hff, 1'b1}
D0: wdata->{0x00, 0x13,0x22,0x31, 0x01, 0x10, 0x23, 0x32}
D1: wdata->{0x02, 0x11,0x20,0x33, 0x03, 0x12, 0x21, 0x30}
D2: wdata->{0x04, 0x17,0x26,0x35, 0x05, 0x14, 0x27, 0x36}
D3: wdata->{0x06, 0x15,0x24,0x37, 0x07, 0x16, 0x25, 0x34}

DBUS DUT (DMA and AES)



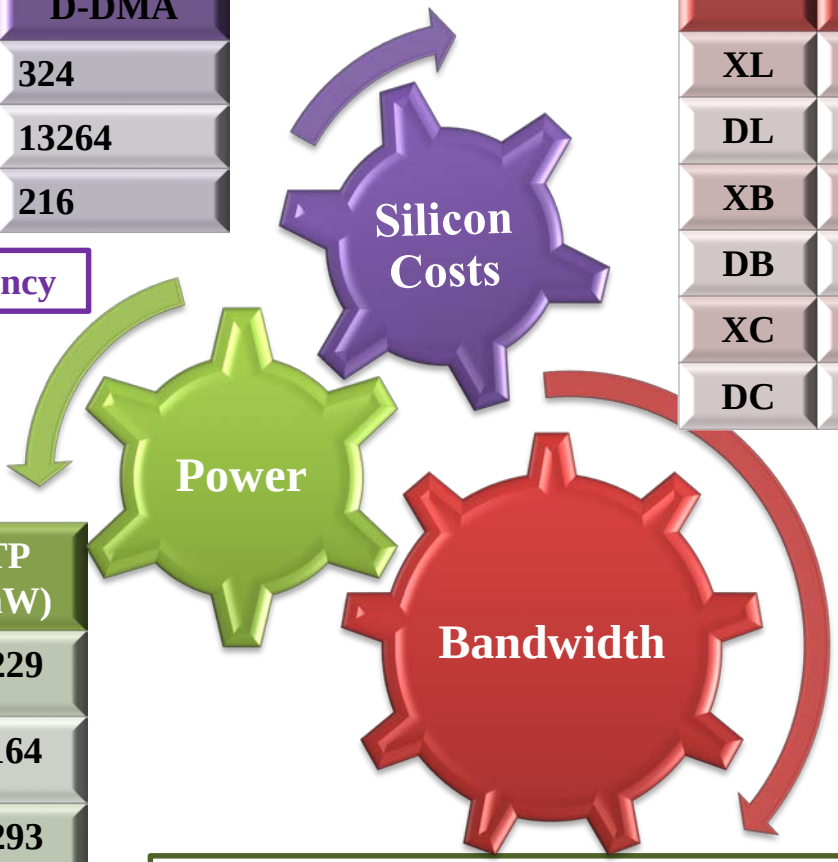
Performance Comparison

X-DMA: AXI DMA+AES
D-DMA: DBUS DMA+AES

DUTs	X-DMA	D-DMA
IOs Count	533	324
Slices Count	15028	13264
MOF (MHz)	167	216

MOF: Max Operational Frequency

Test Cases	VB (Gbps)	DE (uJ)	SE (KBps /Slice)	DEE (GBPS /J)
XL	1.04	0.29	69.46	2.19
DL	1.17	0.23	88.26	2.83
XB	0.98	0.35	65.21	1.84
DB	1.17	0.25	88.26	2.56
XC	0.56	0.68	37.15	0.94
DC	0.73	0.46	54.83	1.40



SP: Static Power
DP: Dynamic Power
TP: Total Power

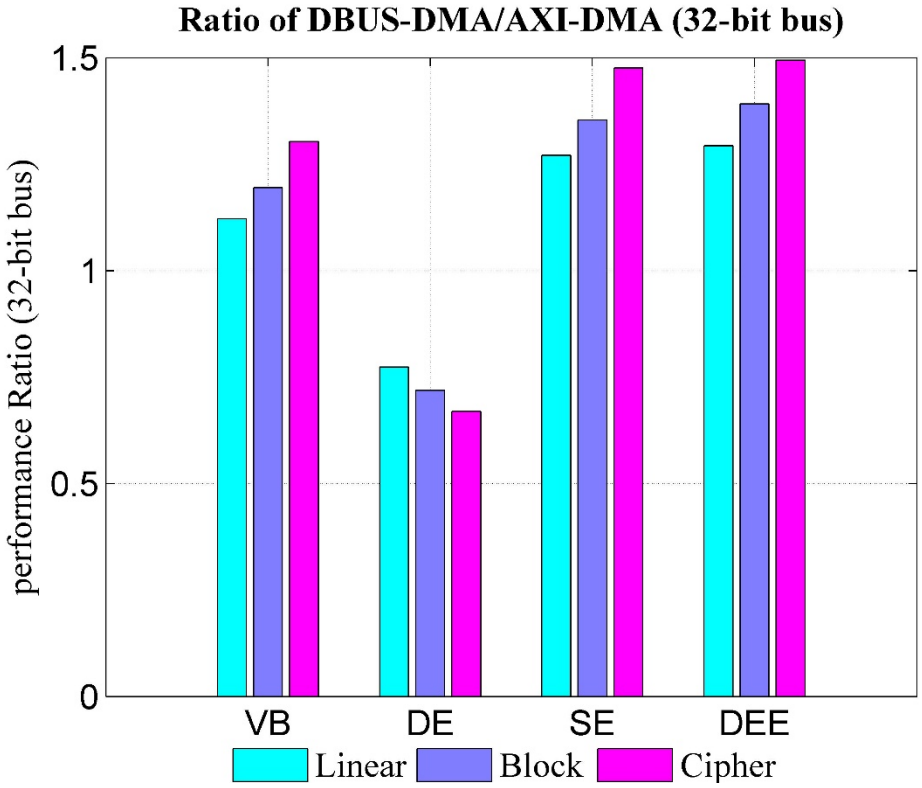
Test Cases	SP (mW)	DP (mW)	TP (mW)
XL	753	476	1229
DL	751	413	1164
XB	761	532	1293
DB	758	457	1215
XC	764	594	1358
DC	759	518	1277

VB: Valid Bandwidth
DE: Dynamic Energy
SE: Slice Efficiency
DEE: Dynamic Energy Efficiency

XL: AXI Linear / XB: AXI Block / XC AXI Cipher
DL: DBUS Linear / DB: DBUS Block / DC: DBUS Cipher

Performance of Silicon Costs, Power and Bandwidth

Performance Comparison (DDAM/XDAM)



Linear Tests:

- **VB: 1.13 / DE: 79.31%**
- **SE: 1.27 / DEE: 1.29**

Block Tests:

- **VB: 1.19 / DE: 71.43%**
- **SE: 1.35 / DEE: 1.39**

Cipher Tests:

- **VB: 1.30 / DE: 66.93%**
- **SE: 1.48 / DEE: 1.49**

VB: Valid Data Bandwidth, DE: Dynamic Energy, SE/DEE: Slice/Dynamic Energy Efficiency

Linear and Block Transfer Contributions:

X. Yang, J. Andrian, "A High Performance On-Chip Bus (MSBUS) Design and Verification," IEEE Trans. On VLSI Syst. (**TVLSI**), Vol. 23, Issue: 7, PP. 1350-1354, Jul. 2014.