AES Encryption over PCI Express

Design Review

Zack Curosh
Matt Swanson
Jevin Sweval

Advanced Encryption Standard (AES)

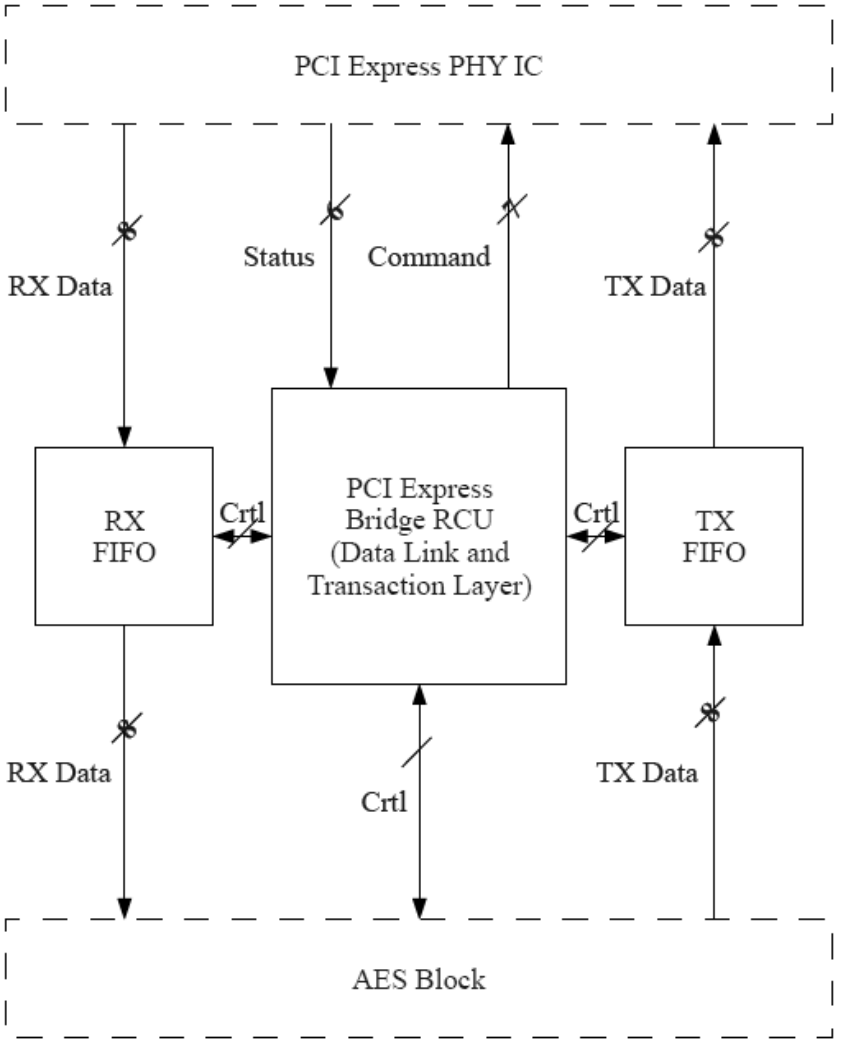
- US government encryption standard since 2002
- Based on Rijndael cipher
- AES is fast in hardware and requires little memory
- User inputs an encryption key and then data in 128-bit blocks
  - Key may be 128, 192, or 256 bits long

Our Design

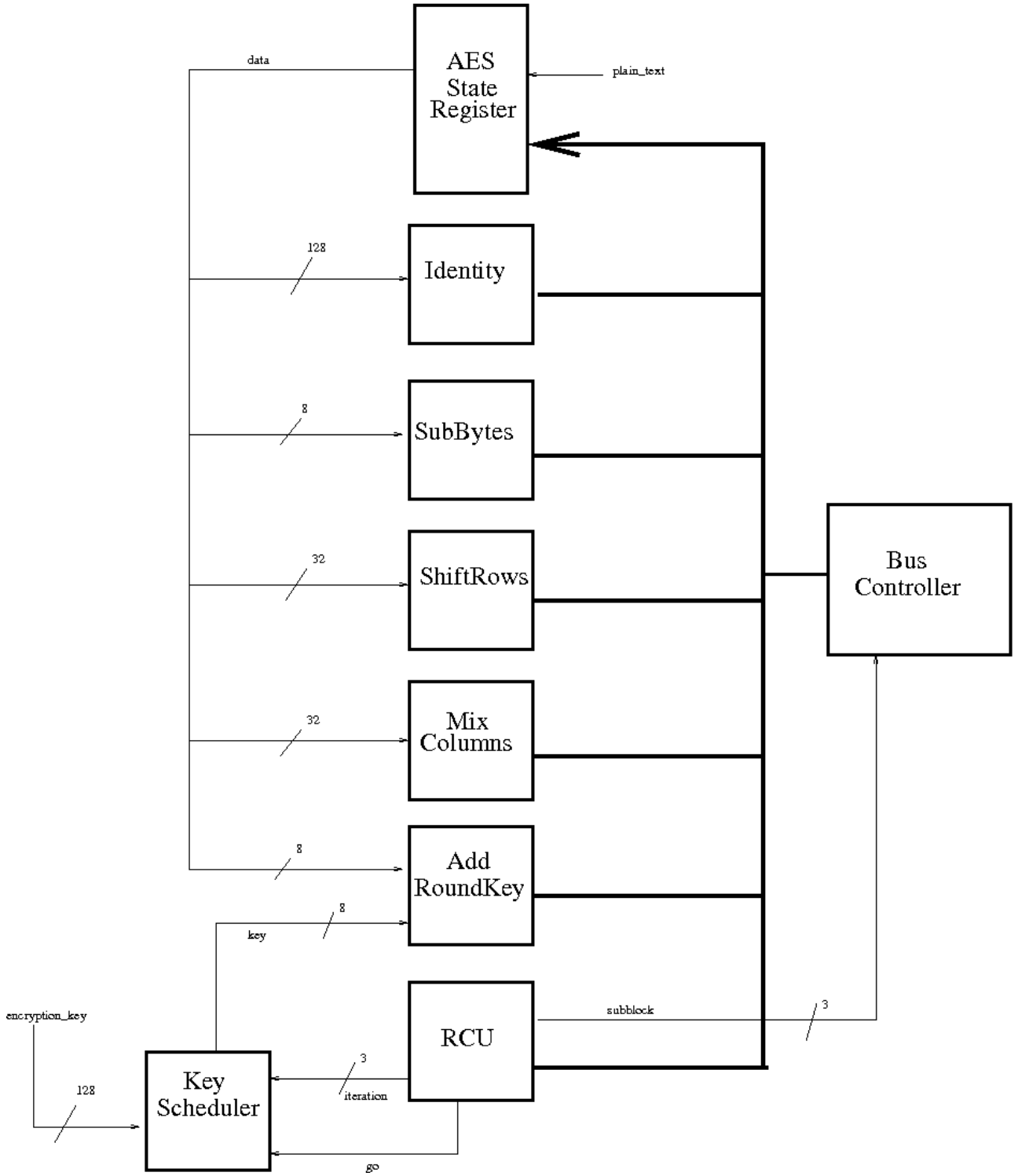
- 128-bit key AES core
- I/O will be done using PCI Express protocol
  - PCI Express bridge: we design
  - TX/RX FIFOs: gold_lib
  - PCI Express transceiver: external hardware
- Hardware implementation gives high-throughput and low power
- PCI Express selected for high performance and widespread use

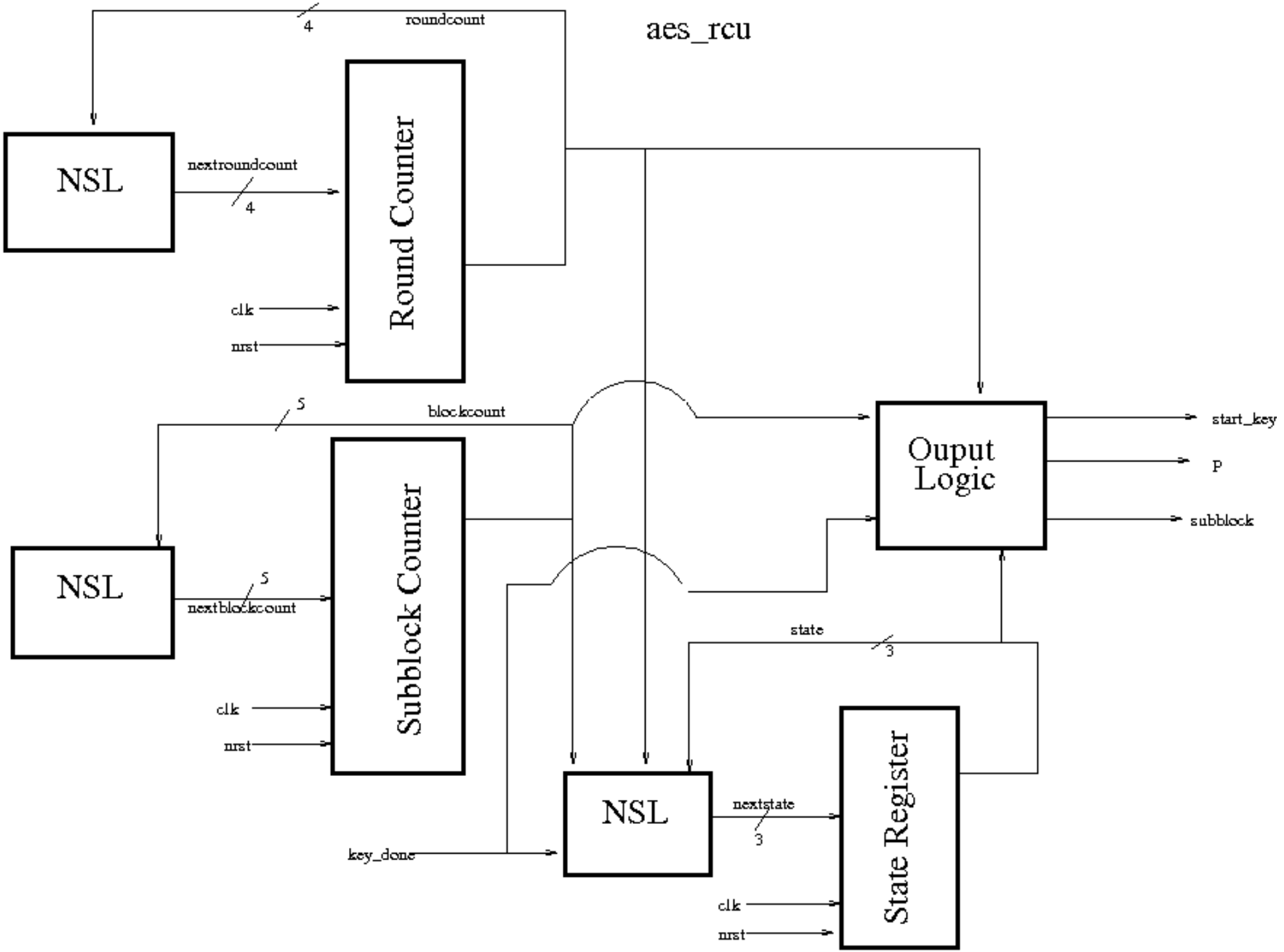
System Level Diagram

NXP PX1011B
PCIe PHY IC

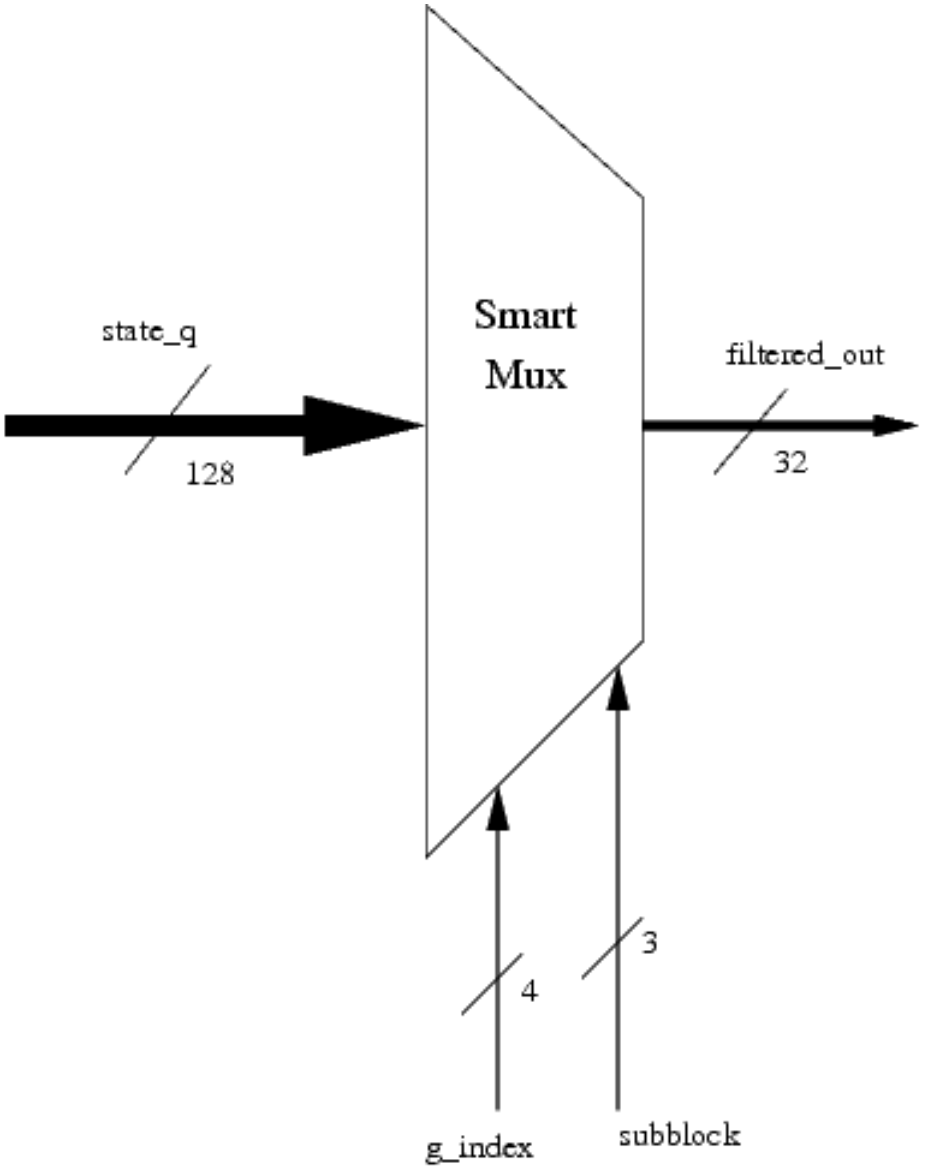


AES Top Level Diagram

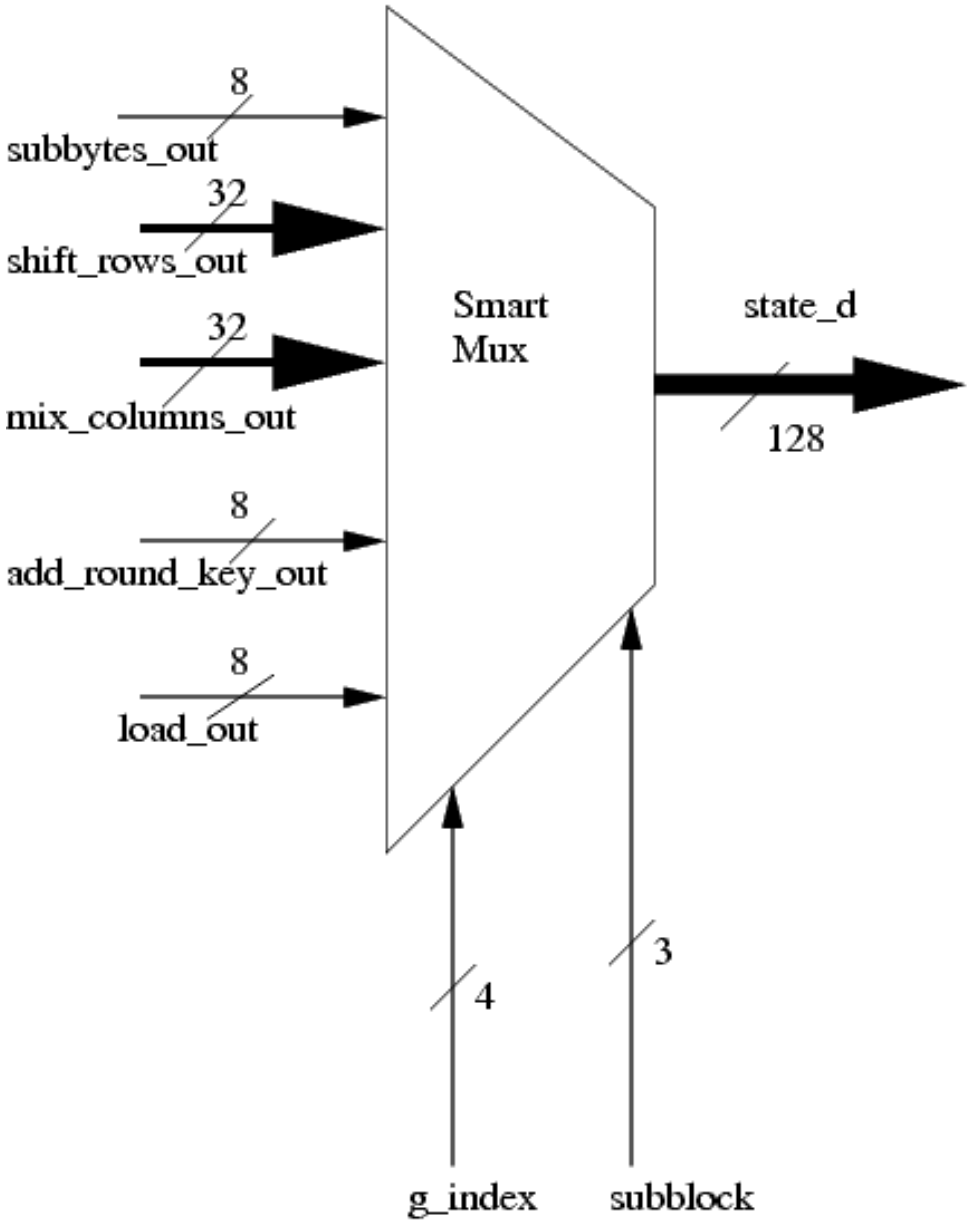



aes_rcu
4
roundcount
NSL
nextroundcount
4
Round Counter
clk
nrst
5
blockcount
Ouput Logic
start_key
P
subblock
NSL
5
nextblockcount
Subblock Counter
clk
nrst
state
3
NSL
nextstate
3
State Register
key_done
clk
nrst

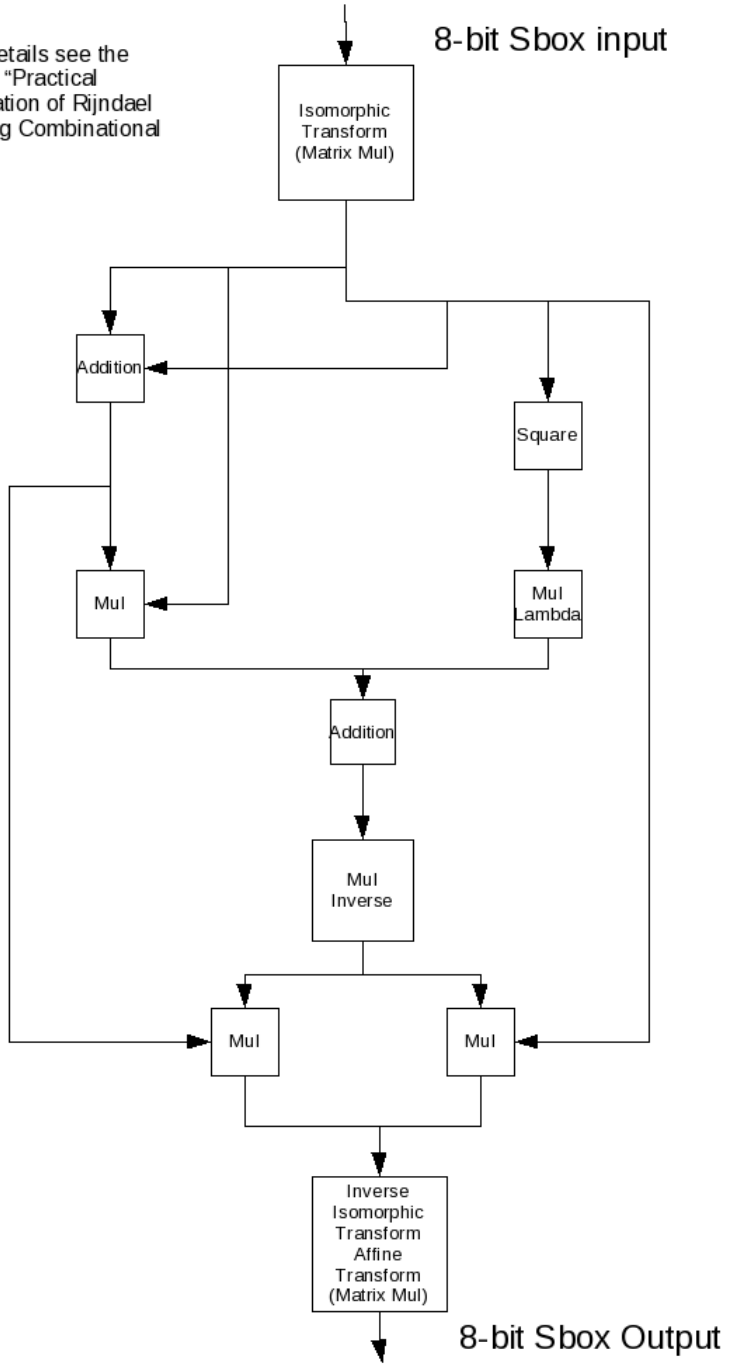
bus_controller (from state)



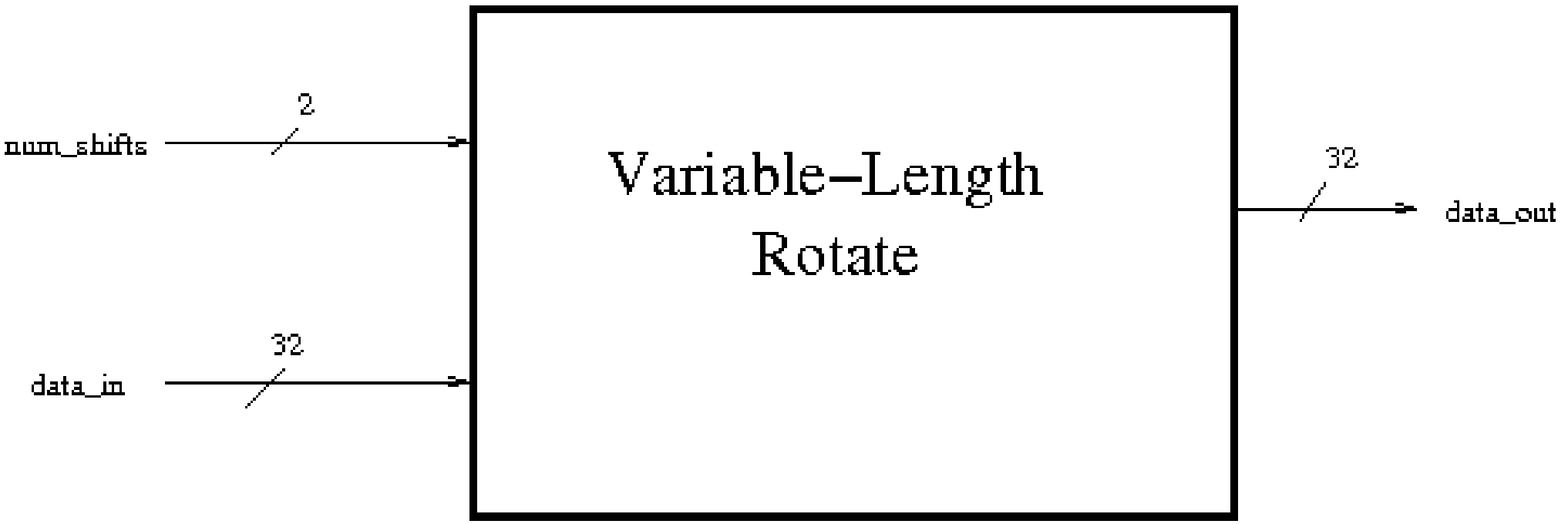
bus_controller (to state)



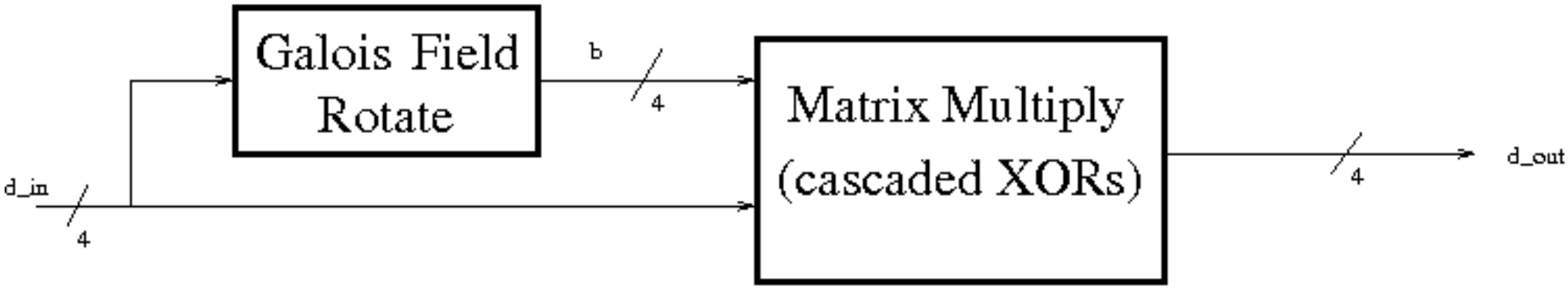
For more details see the paper titled “Practical Implementation of Rijndael S-Box Using Combinational Logic”

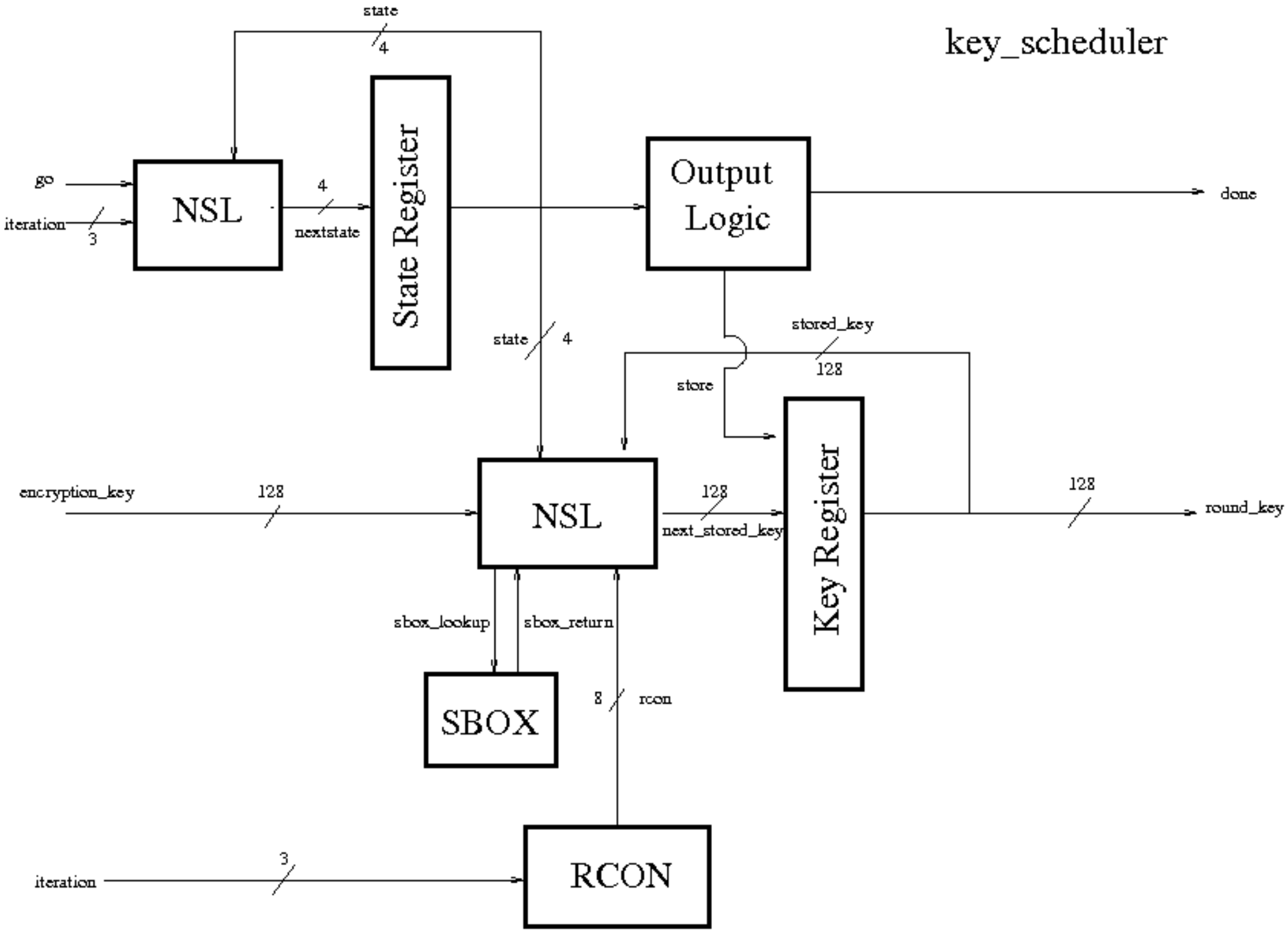


shift_rows

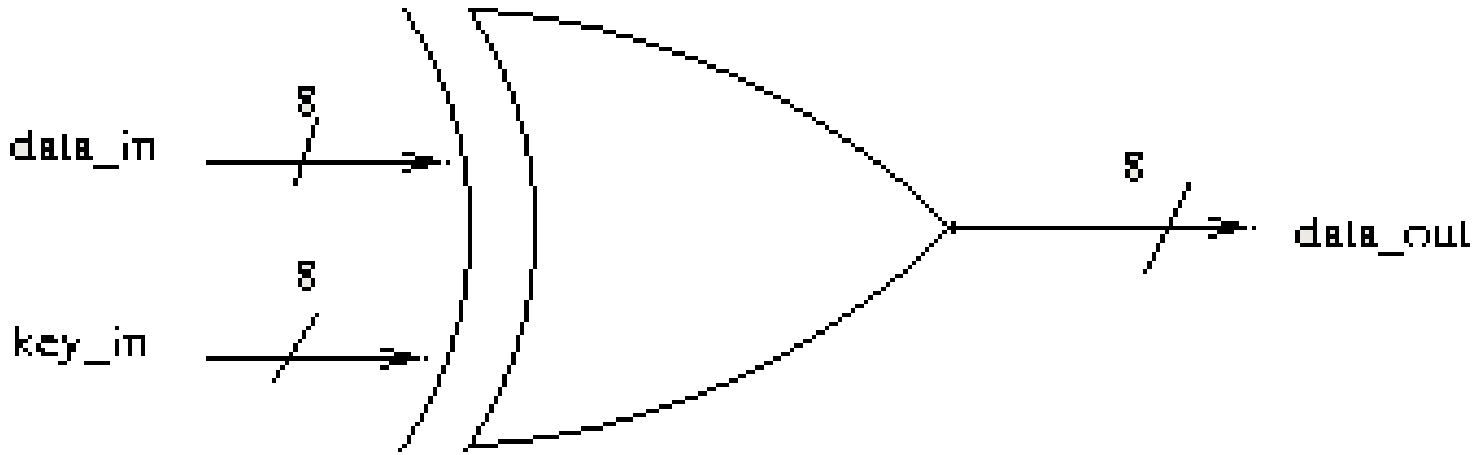


mix_columns

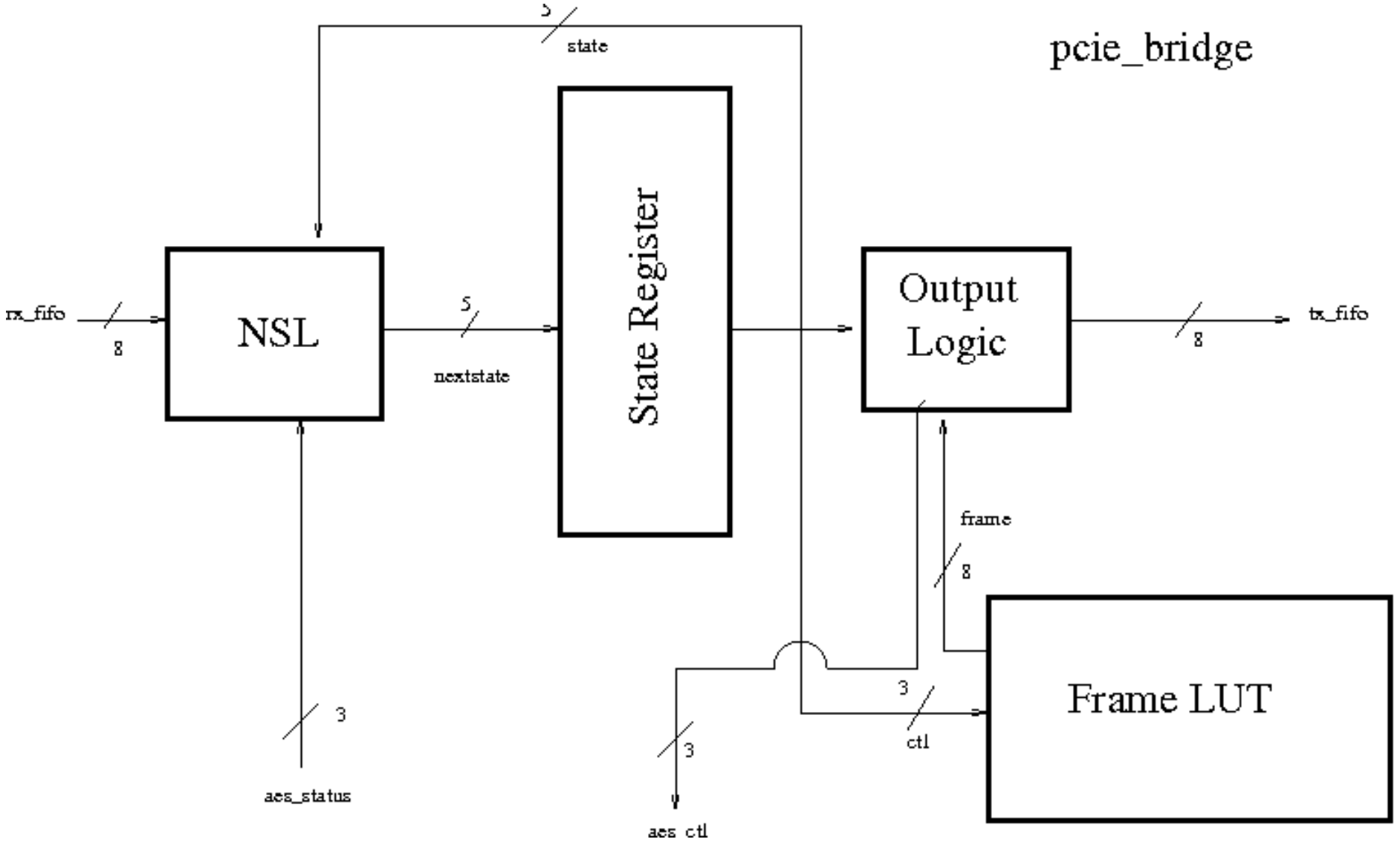

Galois Field
Rotate
b
4
Matrix Multiply
(cascaded XORs)
d_in
4
4
d_out


key_scheduler
state
4
NSL
go
iteration
3
4
nextstate
State Register
Output Logic
done
state
4
stored_key
128
store
encryption_key
128
NSL
128
next_stored_key
Key Register
128
round_key
sbox_lookup
sbox_return
SBOX
8
rcon
iteration
3
RCON

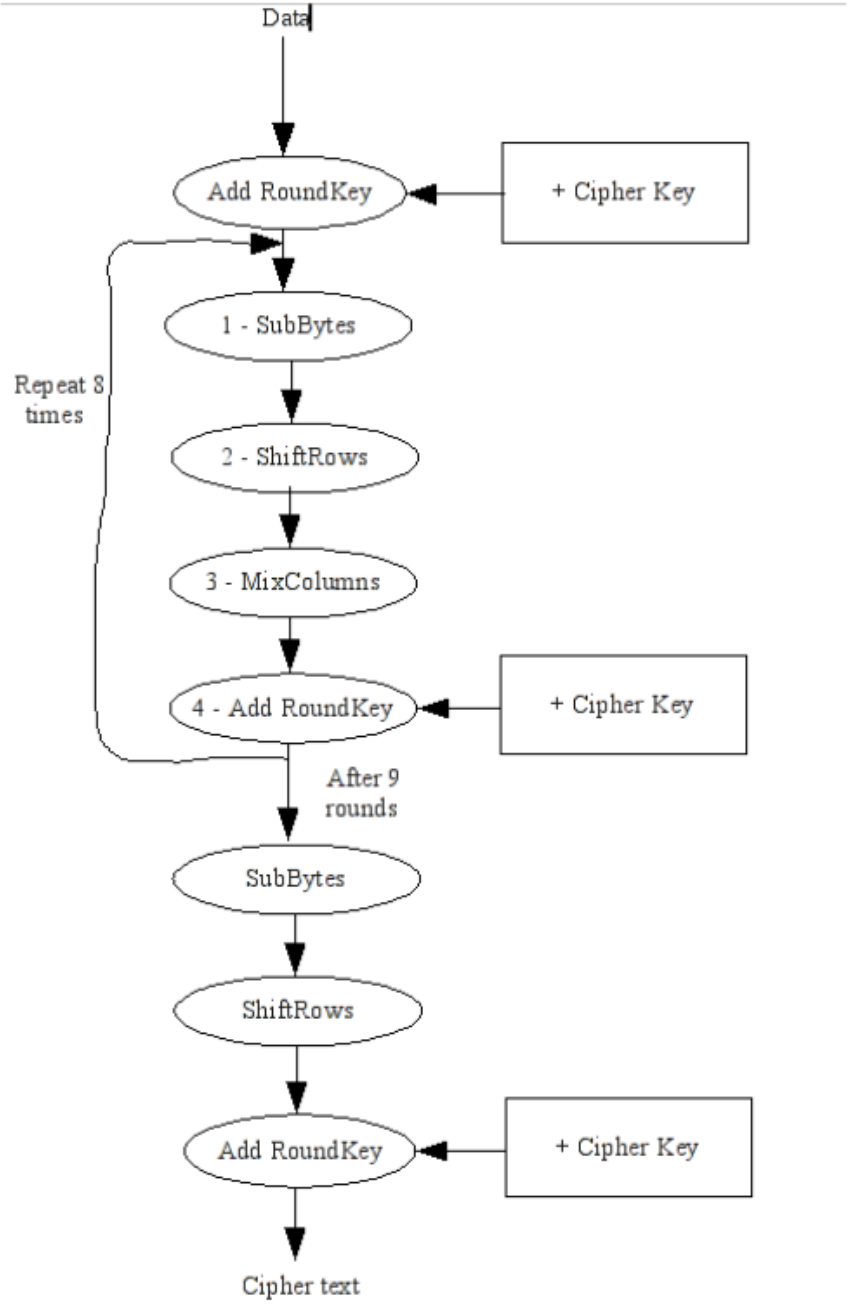
add_round_key



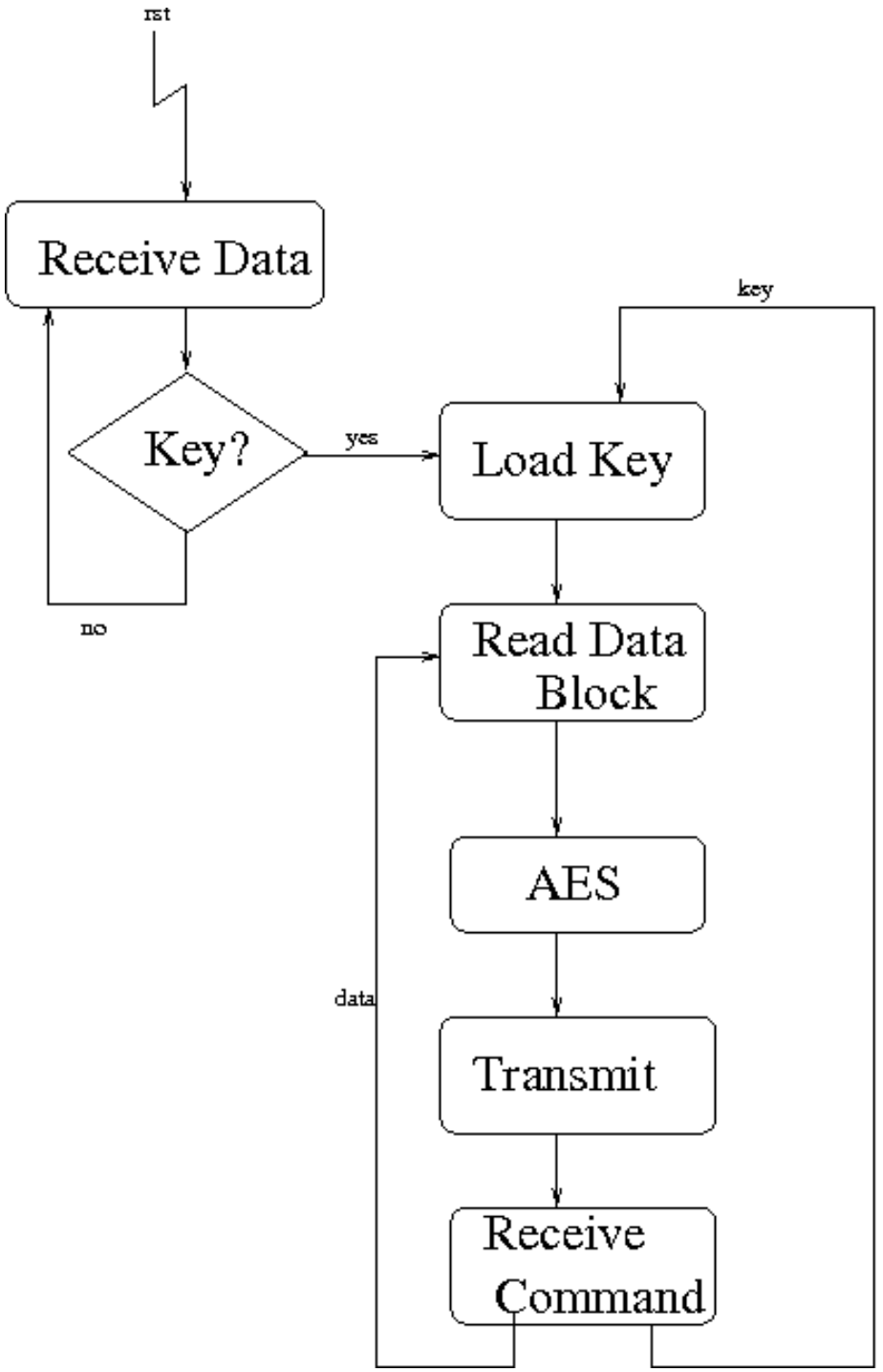
PCIe Bridge Diagram



AES Flowchart



PCIe Bridge Flowchart



AES Encryption over PCI Express

Design Review

Zack Curosh
Matt Swanson
Jevin Sweval

Advanced Encryption Standard (AES)

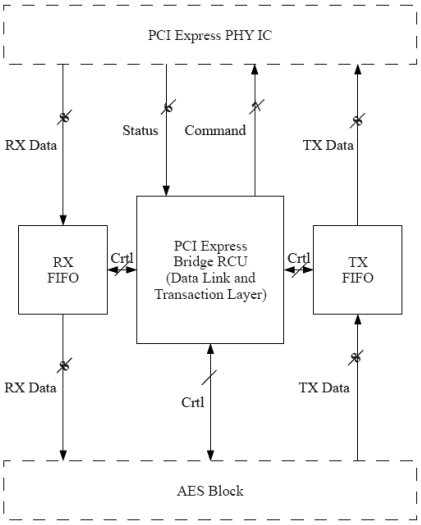
- US government encryption standard since 2002
- Based on Rijndael cipher
- AES is fast in hardware and requires little memory
- User inputs an encryption key and then data in 128-bit blocks
  - Key may be 128, 192, or 256 bits long

Our Design

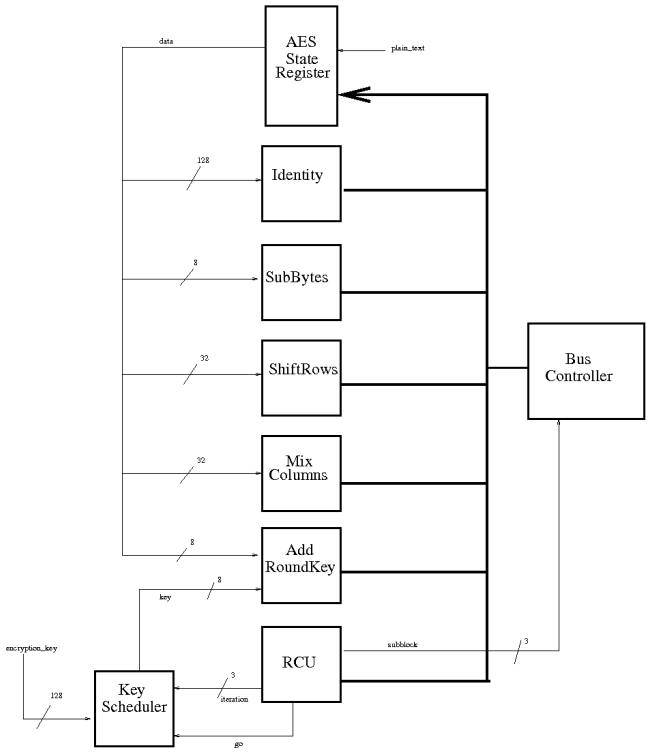
- 128-bit key AES core
- I/O will be done using PCI Express protocol
  - PCI Express bridge: we design
  - TX/RX FIFOs: gold_lib
  - PCI Express transceiver: external hardware
- Hardware implementation gives high-throughput and low power
- PCI Express selected for high performance and widespread use

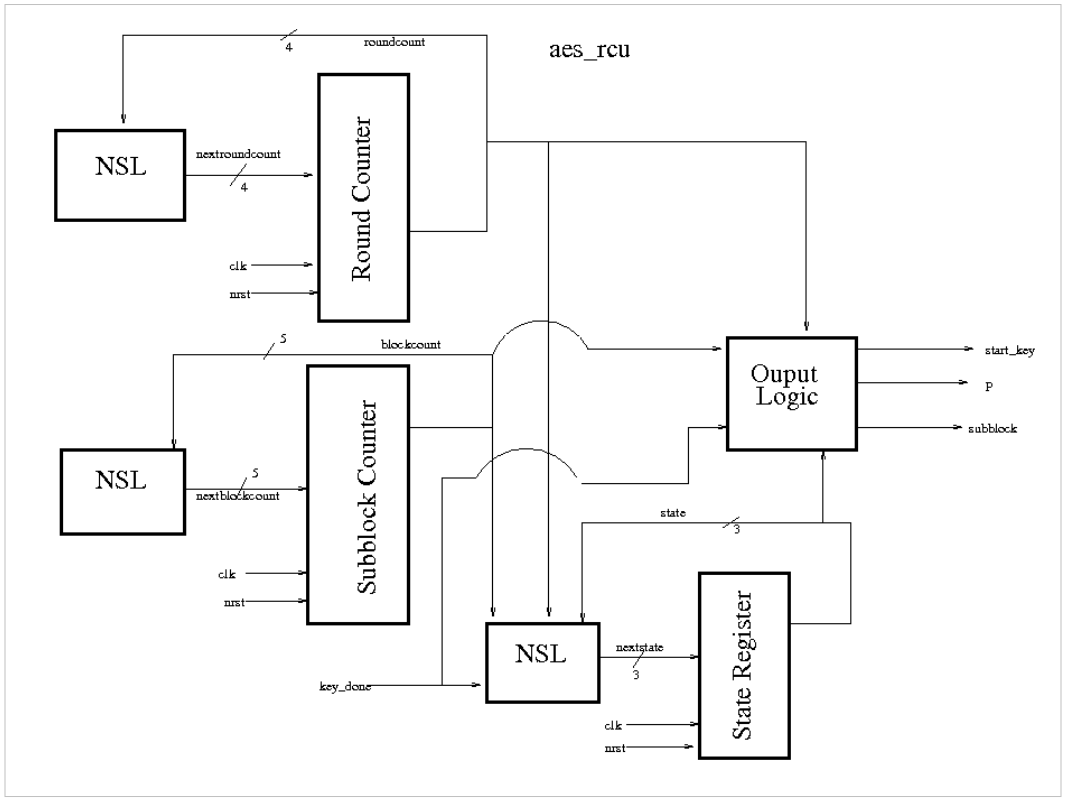
System Level Diagram

NXP PX1011B
PCIe PHY IC

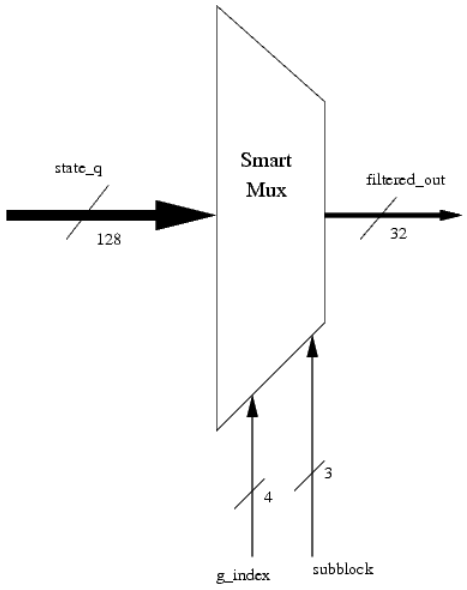


AES Top Level Diagram

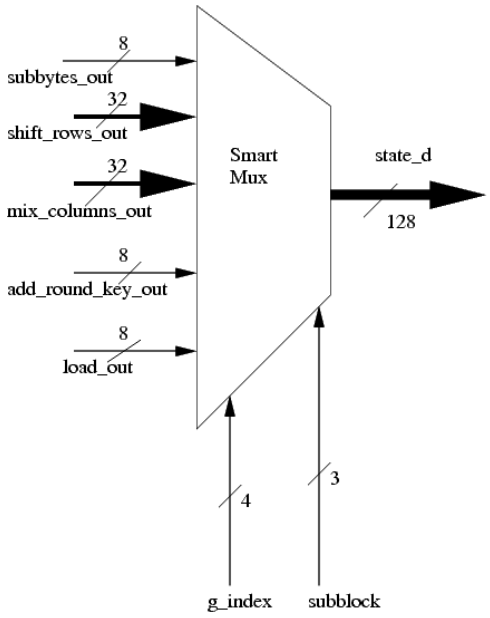



aes_rcu
roundcount
4
NSL
nextroundcount
4
Round Counter
clk
nrst
blockcount
5
Ouput Logic
start_key
p
subblock
NSL
5
nextblockcount
Subblock Counter
clk
nrst
state
3
NSL
nextstate
3
State Register
key_done
clk
nrst

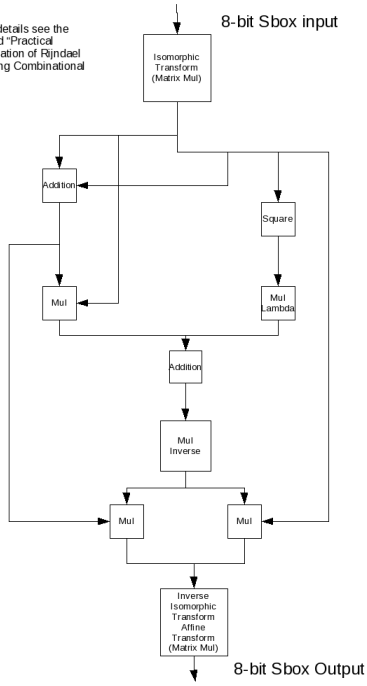
bus_controller (from state)



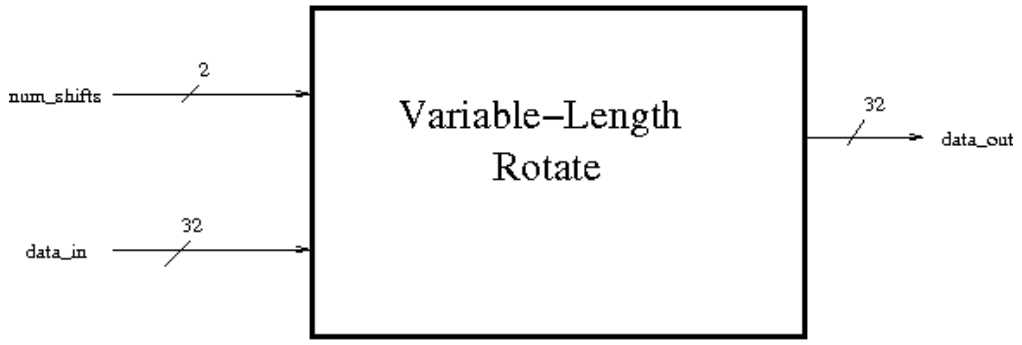
bus_controller (to state)



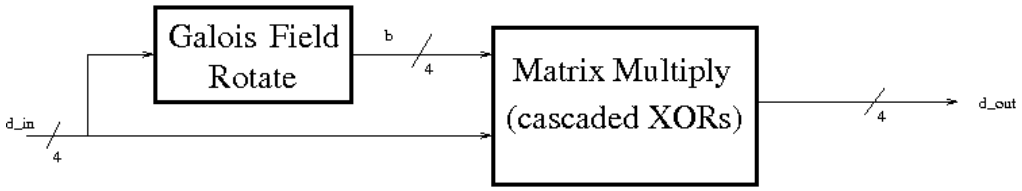
For more details see the paper titled "Practical Implementation of Rijndael S-Box Using Combinational Logic"

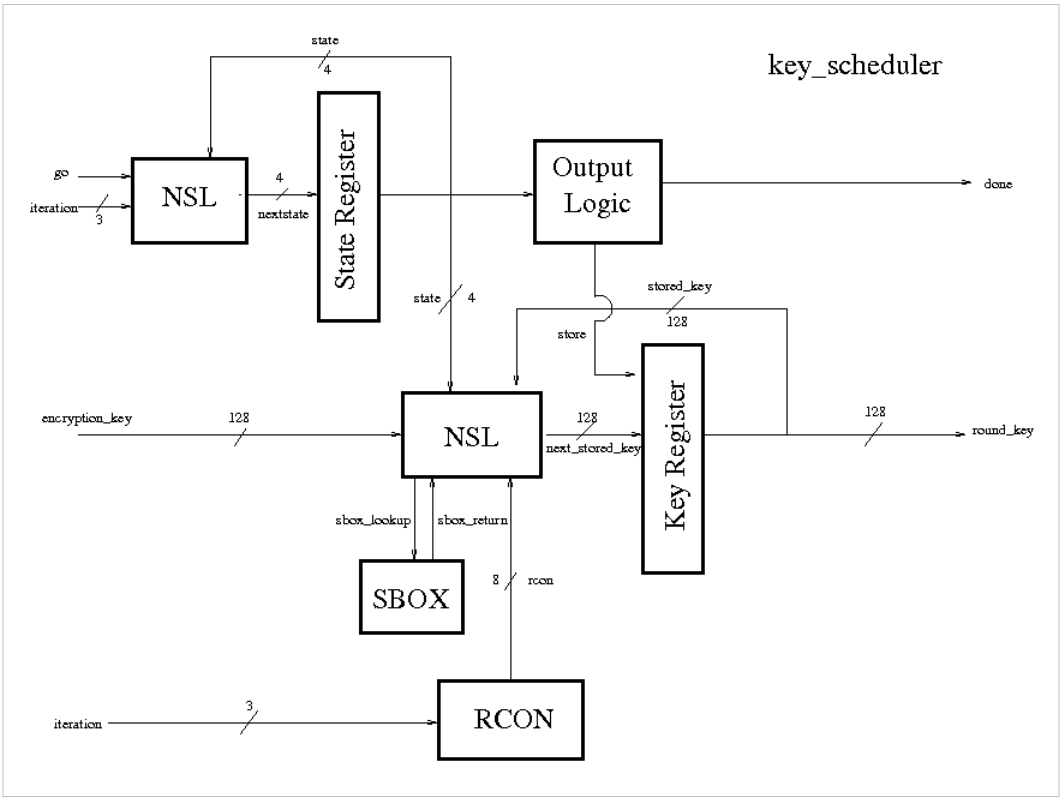


shift_rows

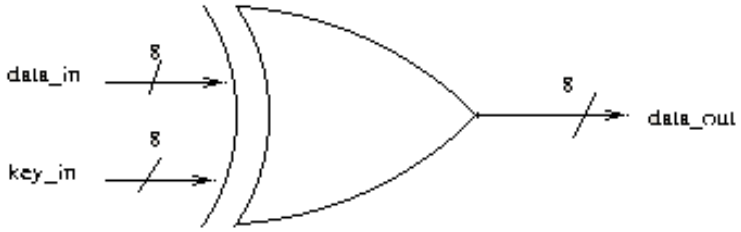


mix_columns

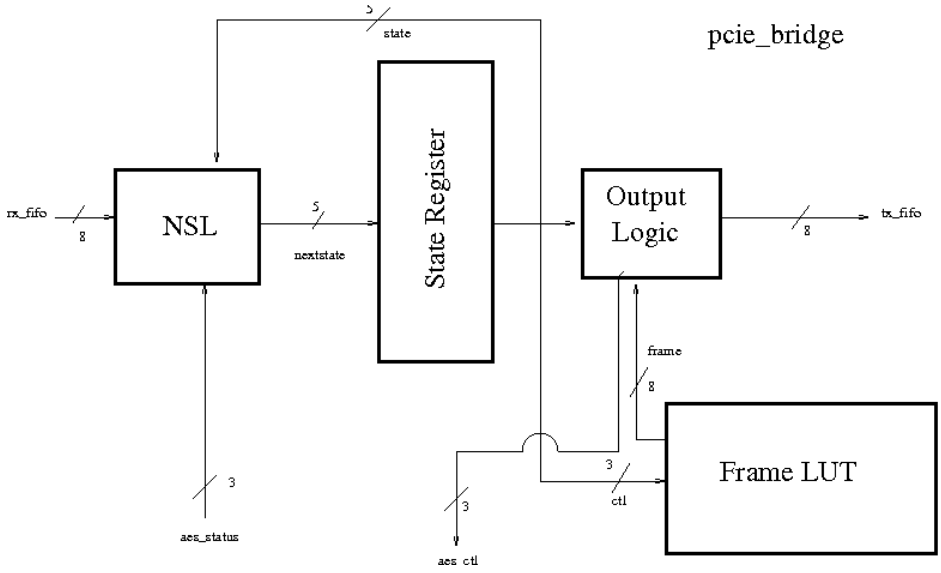

Galois Field
Rotate
b
4
Matrix Multiply
(cascaded XORs)
4
d_out
d_in
4


key_scheduler
state
4
go
iteration
3
NSL
4
nextstate
State Register
Output Logic
done
state
4
stored_key
128
store
encryption_key
128
NSL
128
next_stored_key
Key Register
128
round_key
sbox_lookup
sbox_return
SBOX
8
rcon
iteration
3
RCON

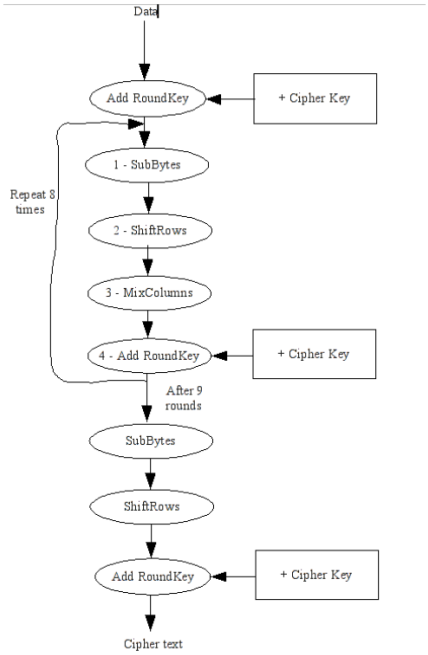
add_round_key



PCIe Bridge Diagram



AES Flowchart



PCIe Bridge Flowchart