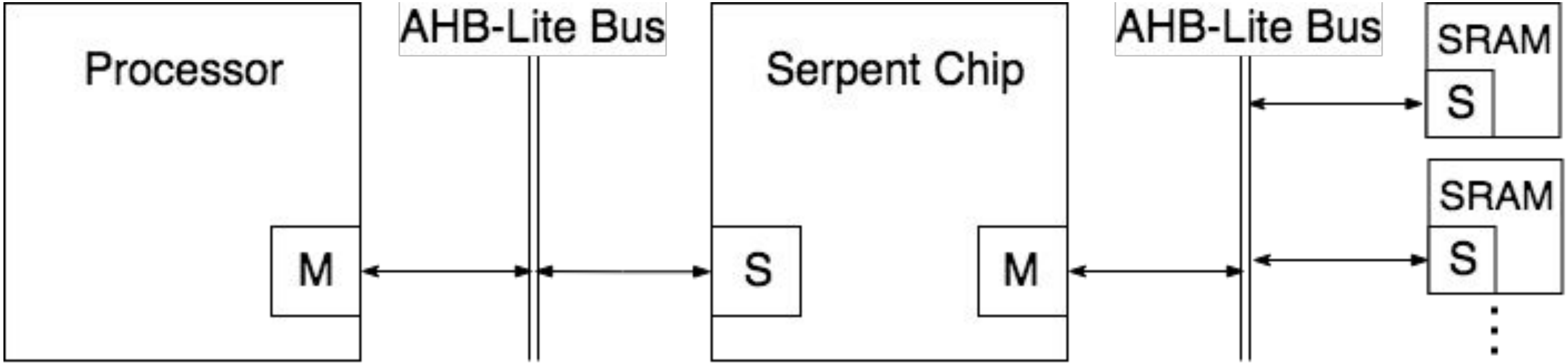
Automatic Encryption: Serpent (AES)

James Weber
Spencer Deak
John Kansky

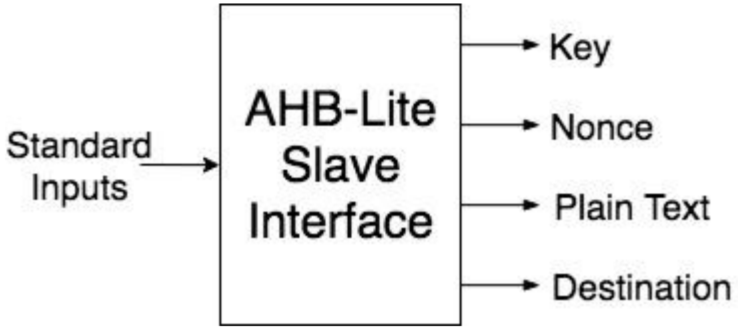
Overview



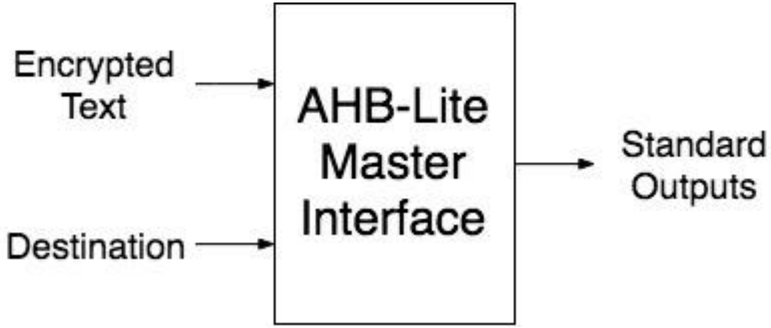
- AHB-Lite I/O for fast, pipelined data transfer.
- Serpent encryption, designed for secure, efficient hardware implementations

System Design: AHB Lite

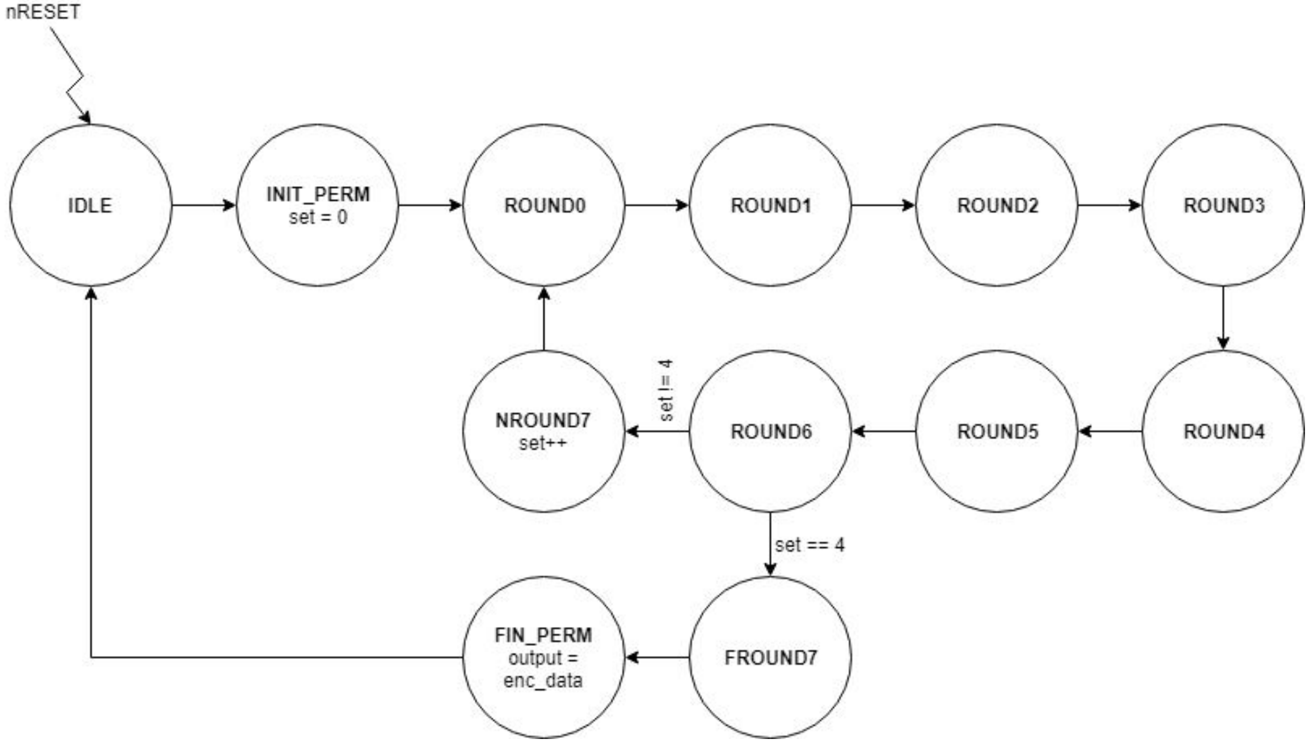
Slave



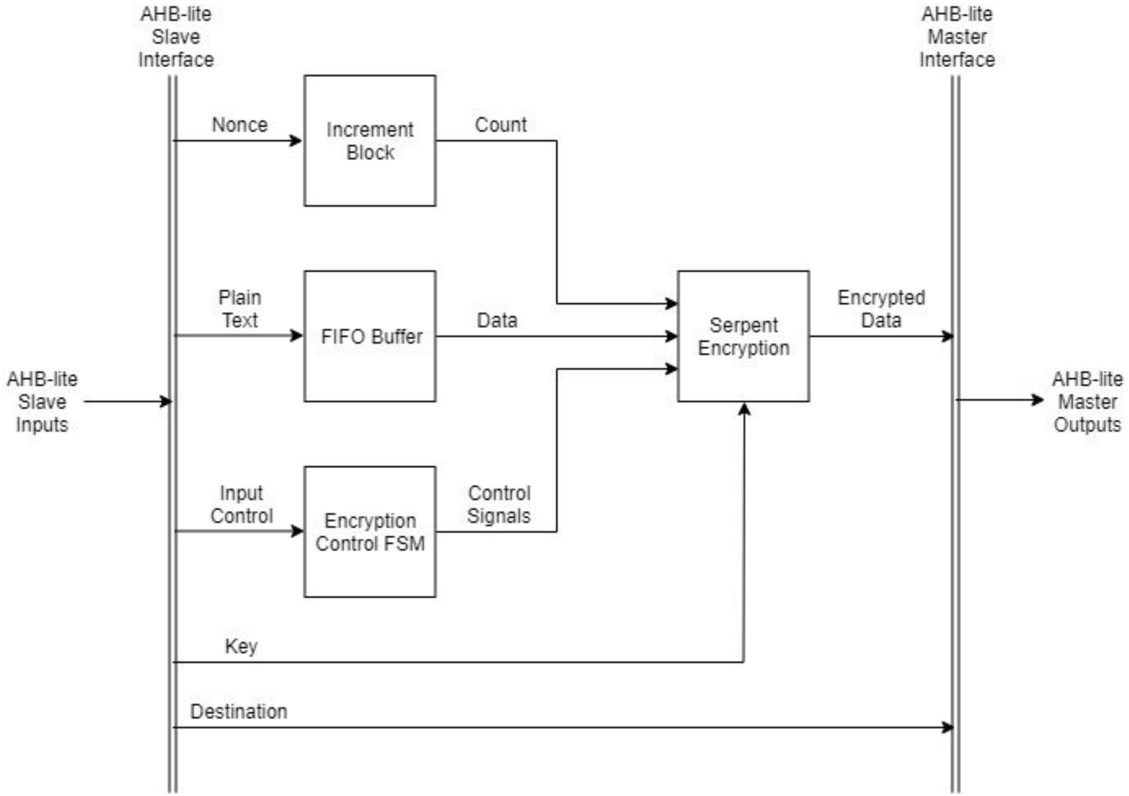
Master



System Design: Encryption



System Design: Integration

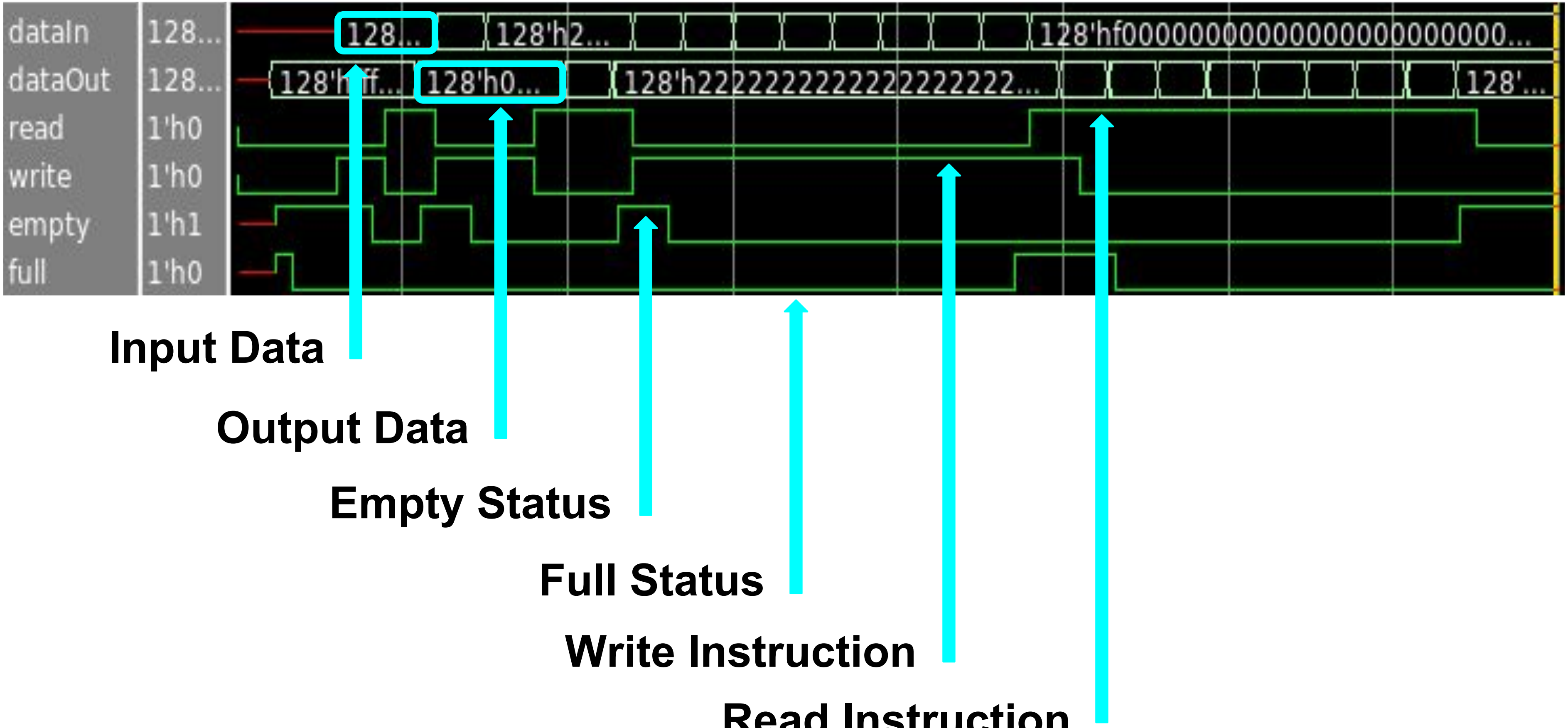


Success Criteria and Results

Test Benches	All top level modules have test benches that adequately demonstrate the functionality of the module in both source and mapped situations.
Proper Synthesis	All modules compile and synthesize without error, do not generate latches, and do not raise any warnings.
Source and Mapped	All modules operate as intended in source, and generate proper netlists in mapped versions that do not yield timing errors.
IC Layout	A complete IC layout has been generated that contains valid geometry and connectivity.

Success Criteria and Results

Successful Encryption	Encrypts and decrypts data, but does not adhere to Serpent-1 standard.
AHB-Lite Master	Correctly transfers data from the encryption module to the SRAM as specified by standard protocol.
AHB-Lite Slave	Adequately passes data from the processor to the FIFO buffer while following AHB-List standards.
FIFO Buffer Operation	Enqueues and dequeues data in one clock cycle for fast data storage and retrieval by the chip.
Round Key Generation	Successfully generates 33 unique round keys for one encryption in compliance with Serpent.



Input Data

Output Data

Empty Status

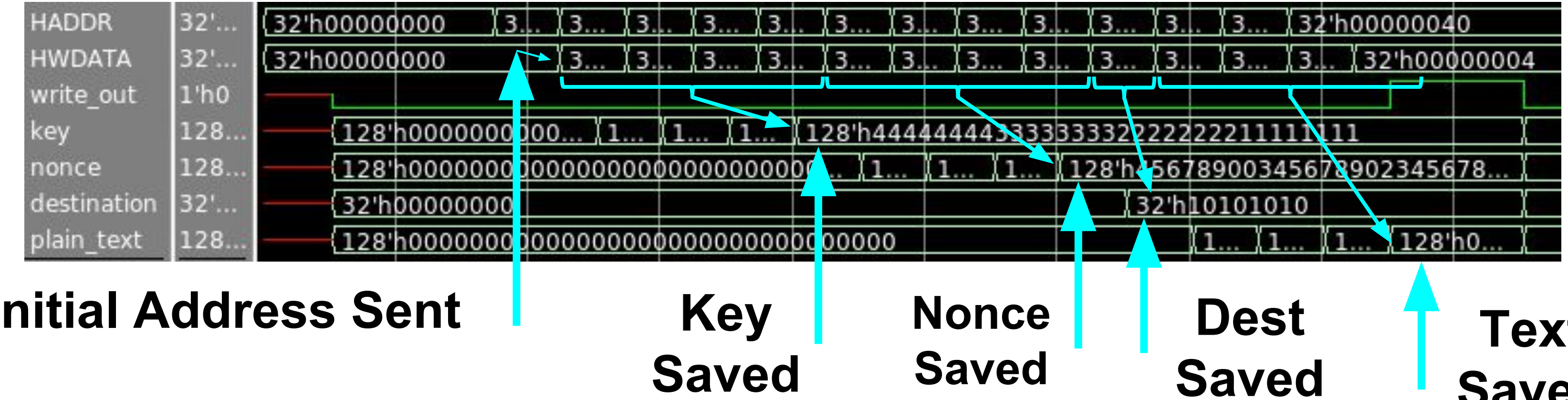
Full Status

Write Instruction

Read Instruction

Specific Criteria: FIFO Buffer

Slave


HADDR 32'... 32'h00000000 32'h00000040
HWDATA 32'... 32'h00000000 32'h00000004
write_out 1'h0
key 128... 128'h0000000000... 128'h44444444333333332222222211111111
nonce 128... 128'h00000000000000000000000000000... 128'h4567890034567890234567 8...
destination 32'... 32'h00000000 32'h10101010
plain_text 128... 128'h00000000000000000000000000000000 128'h0...

Initial Address Sent

Key Saved

Nonce Saved

Dest Saved

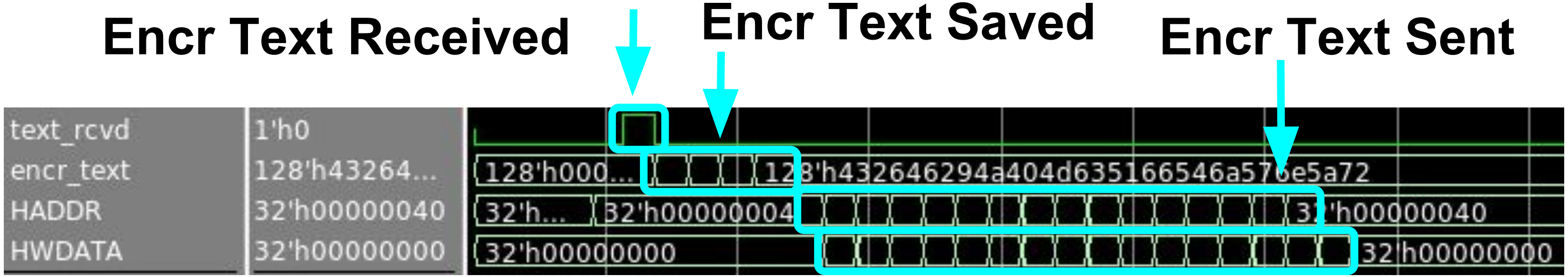
Text Saved

Encr Text Received

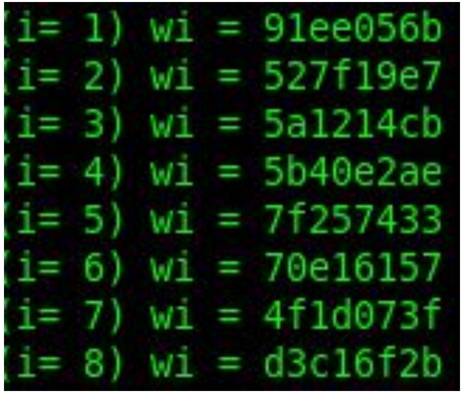
Encr Text Saved

Encr Text Sent

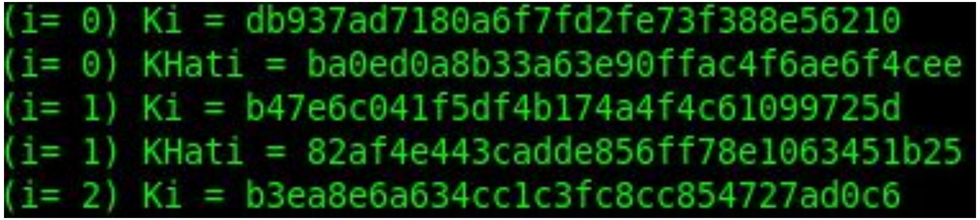
Master


text_rcvd 1'h0
encr_text 128'h43264... 128'h000... 128'h432646294a404d635166546a576e5a72
HADDR 32'h00000040 32'h... 32'h00000004 32'h00000040
HWDATA 32'h00000000 32'h00000000 32'h00000000

Specific Criteria: AHB

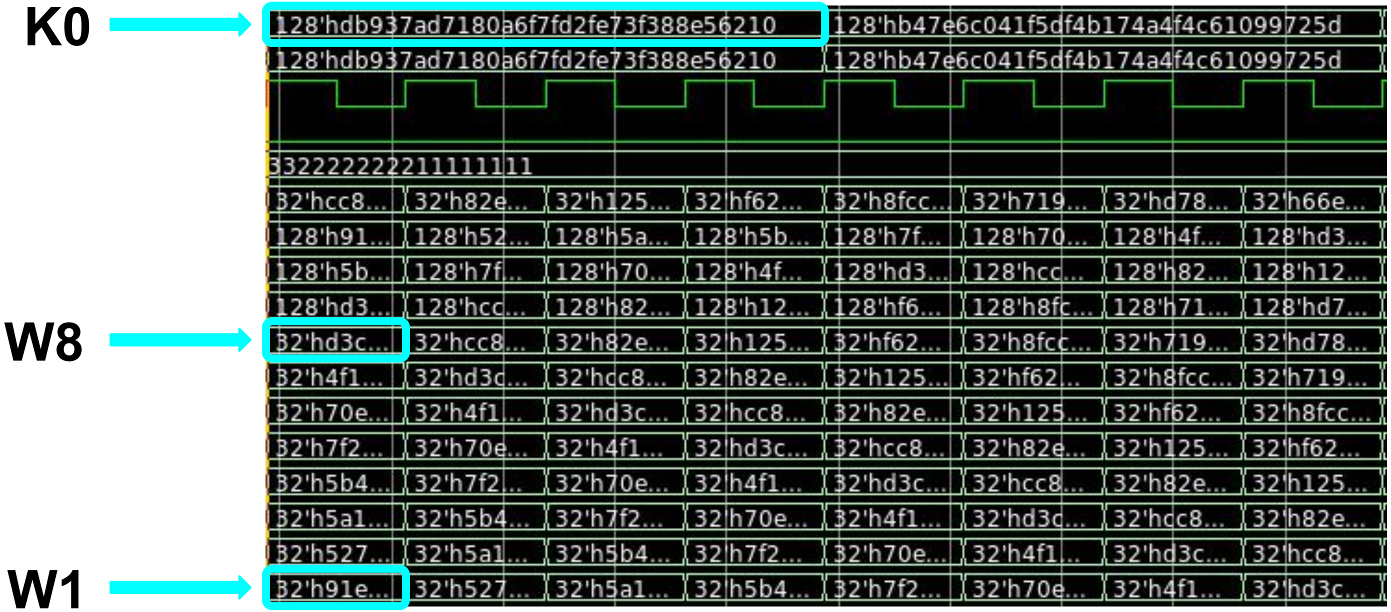


```
(i= 1) wi = 91ee056b
(i= 2) wi = 527f19e7
(i= 3) wi = 5a1214cb
(i= 4) wi = 5b40e2ae
(i= 5) wi = 7f257433
(i= 6) wi = 70e16157
(i= 7) wi = 4f1d073f
(i= 8) wi = d3c16f2b
```



```
(i= 0) Ki = db937ad7180a6f7fd2fe73f388e56210
(i= 0) KHati = ba0ed0a8b33a63e90ffac4f6ae6f4cee
(i= 1) Ki = b47e6c041f5df4b174a4f4c61099725d
(i= 1) KHati = 82af4e443cadde856ff78e1063451b25
(i= 2) Ki = b3ea8e6a634cc1c3fc8cc854727ad0c6
```

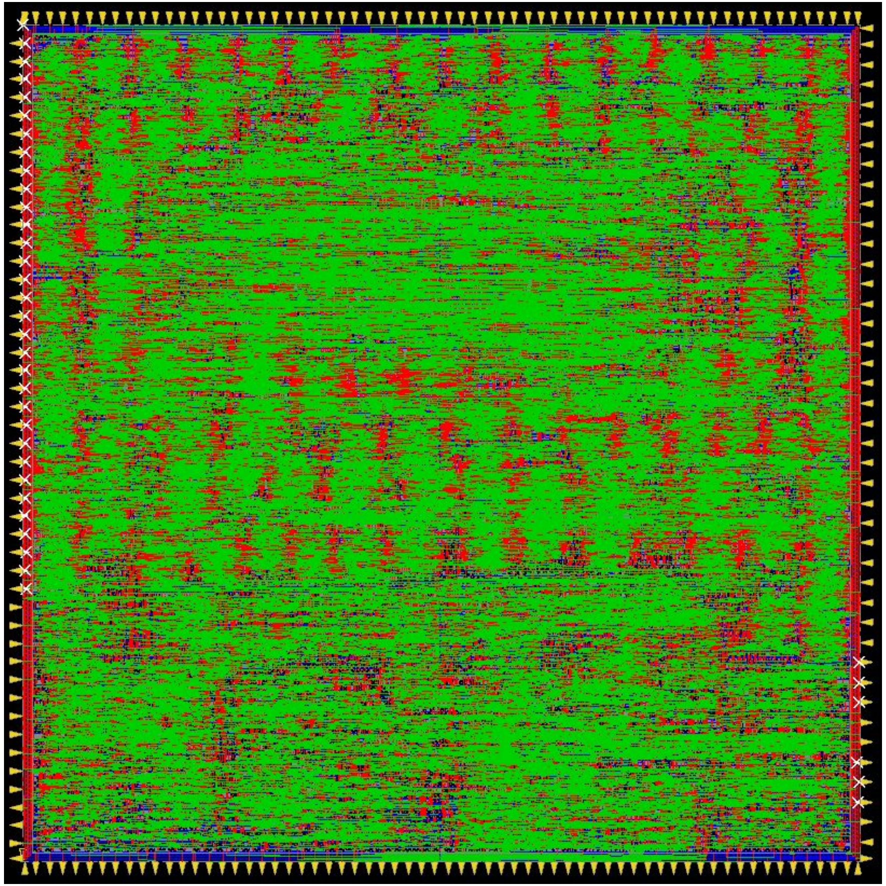
Wi - Prekeys
Ki - Round Keys



```
128'hdb937ad7180a6f7fd2fe73f388e56210                    128'hb47e6c041f5df4b174a4f4c61099725d
128'hdb937ad7180a6f7fd2fe73f388e56210                    128'hb47e6c041f5df4b174a4f4c61099725d

33222222221111111
32'hcc8...  32'h82e...  32'h125...  32'hf62...  32'h8fcc... 32'h719...  32'hd78...  32'h66e...
128'h91...  128'h52...  128'h5a...  128'h5b...  128'h7f...  128'h70...  128'h4f...  128'hd3...
128'h5b...  128'h7f...  128'h70...  128'h4f...  128'hd3...  128'hcc...  128'h82...  128'h12...
128'hd3...  128'hcc...  128'h82...  128'h12...  128'hf6...  128'h8fc... 128'h71...  128'hd7...
32'hd3c...  32'hcc8...  32'h82e...  32'h125...  32'hf62...  32'h8fcc... 32'h719...  32'hd78...
32'h4f1...  32'hd3c...  32'hcc8...  32'h82e...  32'h125...  32'hf62...  32'h8fcc... 32'h719...
32'h70e...  32'h4f1...  32'hd3c...  32'hcc8...  32'h82e...  32'h125...  32'hf62...  32'h8fcc...
32'h7f2...  32'h70e...  32'h4f1...  32'hd3c...  32'hcc8...  32'h82e...  32'h125...  32'hf62...
32'h5b4...  32'h7f2...  32'h70e...  32'h4f1...  32'hd3c...  32'hcc8...  32'h82e...  32'h125...
32'h5a1...  32'h5b4...  32'h7f2...  32'h70e...  32'h4f1...  32'hd3c...  32'hcc8...  32'h82e...
32'h527...  32'h5a1...  32'h5b4...  32'h7f2...  32'h70e...  32'h4f1...  32'hd3c...  32'hcc8...
32'h91e...  32'h527...  32'h5a1...  32'h5b4...  32'h7f2...  32'h70e...  32'h4f1...  32'hd3c...
```

Specific Criteria: Encryption Round Keys



Design Area: 4,610 μm x 4,610 μm
21,252,100 μm^2

Layout Critical Path: 9.58 ns
CLK -> CLK

Synthesis Critical Path: 4.66 ns
CLK -> HWRITE

Estimated Critical Path: 2.40 ns
R_STA -> R_STA

Chip Layout

Conclusion

- Serpent is worthwhile and secure cipher, but documentation is somewhat scarce.
- Break AHB interfaces into smaller modules to avoid monolithic debugging.
- More efficient S-box implementation can reduce the chip area by a significant factor.