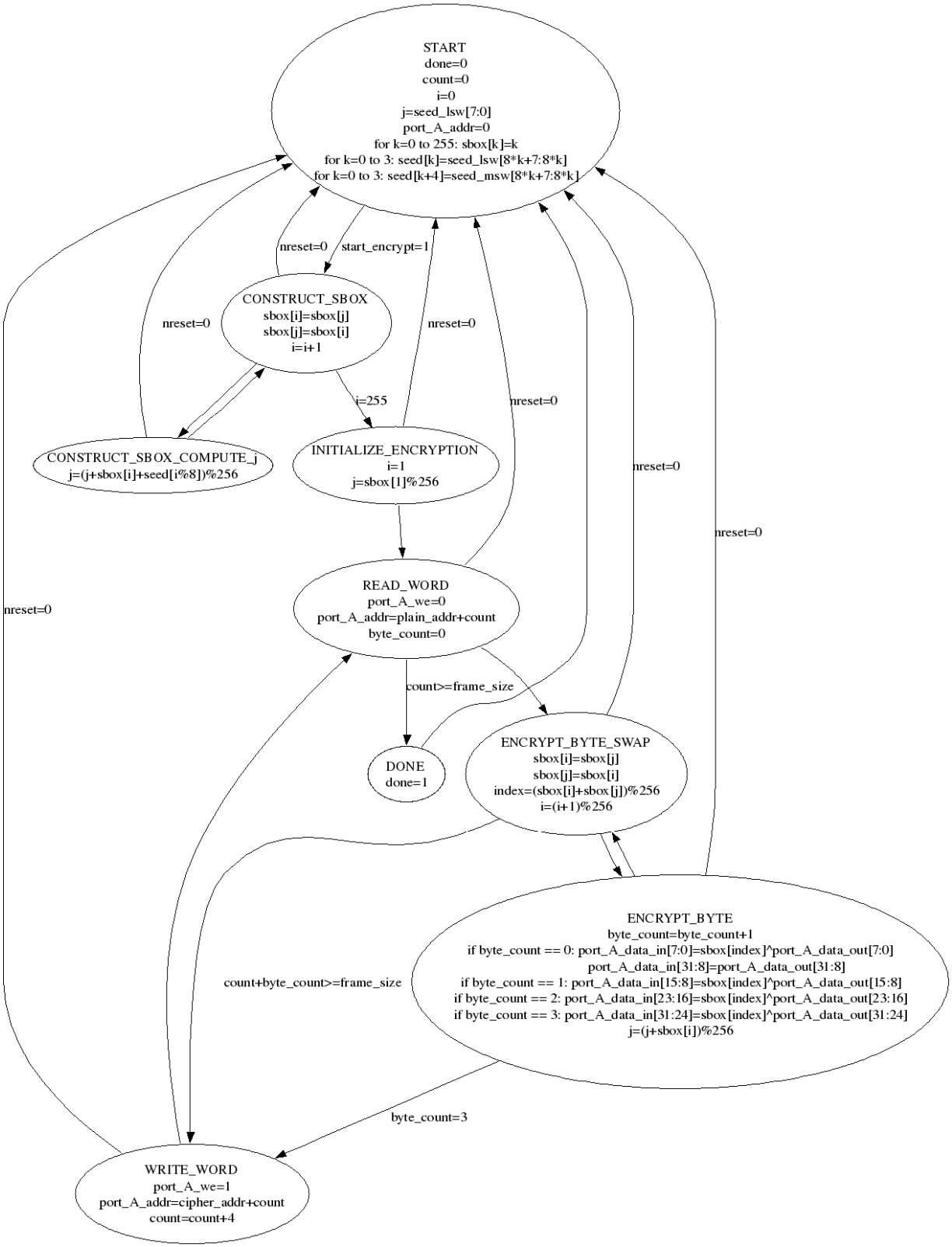
CSE 111
Prof. Sujit Dey
Winter 2007
Project 2

Alvin Jeng
A05409996

Nitay Joffe
A05229402

State diagram:



Transcript for the ModelSim run:

```
# //  ModelSim SE 6.2b Jul 31 2006 Linux 2.6.19-gentoo-r5
# //
# //  Copyright 2006 Mentor Graphics Corporation
# //             All Rights Reserved.
# //
# //  THIS WORK CONTAINS TRADE SECRET AND
# //  PROPRIETARY INFORMATION WHICH IS THE PROPERTY
# //  OF MENTOR GRAPHICS CORPORATION OR ITS LICENSORS
# //  AND IS SUBJECT TO LICENSE TERMS.
# //
vlog *.v
# Model Technology ModelSim SE vlog 6.2b Compiler 2006.07 Jul
31 2006
# -- Compiling module testbench_wep_encrypt_v1
# -- Compiling module testbench_wep_encrypt_v3
# -- Compiling module testbench_wep_encrypt_v4
# -- Compiling module wep_encrypt_v1
# -- Compiling module wep_encrypt_v3
# -- Compiling module wep_encrypt_v4
# ** Warning: wep_encrypt_v4.v(105): [RDGN] - Redundant digits
in numeric literal.
#
# Top level modules:
#         testbench_wep_encrypt_v1
#         testbench_wep_encrypt_v3
#         testbench_wep_encrypt_v4
vsim testbench_wep_encrypt_v4
# vsim testbench_wep_encrypt_v4
# ** Note: (vsim-3813) Design is being optimized due to module
recompilation...
# Loading work.testbench_wep_encrypt_v4(fast)


restart -f
# Loading work.testbench_wep_encrypt_v4(fast)
run -all
# Error: memory reference not word aligned!
#
# Error: memory reference not word aligned!
#
# Error: memory reference not word aligned!
#
# ------------
#
# Plaintext 1
#
# ------------
#
# 00000000
#
# 00000000
#
# 00000000
#
# 00000000
#
# 00000000
#
# 00000000
#
# 00000000
#
# 00000000
#
# 00000000
#
# 00000000
#
# 00000028
#
# 864d7f00
#
# ------------
#
# Ciphertext 1
#
# ------------
#
# e7c29474
#
# 79084b10
#
# 53d54b0d
#
# fc1e8f32
#
# 48e81a9b
#
# 773c808e
#
# b7483552
#
# d9cb8c76
#
# 2a8c8bc6
#
# 0967ada8
#
# d4520f74
#
# 568e589d
#
# ------------
#
# Plaintext 2
#
# ------------
#
# 00000000
#
# 12345678
#
# 9abcdef0
#
# 00000000
#
# 00000000
#
# 0f005030
#
# 00000028
#
# 864d7f00
#
# 82367002
#
# 04564530
#
# 45645722
#
# ab56c352
#
# 00555322
#
# Note, most significant byte (00) of last word should not be
encrypted
#
# ------------
#
# Ciphertext 2
#
# ------------
#
# bd10a1a3
#
# 30cf6e1c
#
# 91fd852d
#
# 1c70a490
#
# bb07ccd6
#
# a8e7db9b
#
# edf2a604
#
# e1e7b273
#
# 5938bca6
#
# 0690b62c
#
# 8aa30bd9
#
# c842589f
#
# 0091e22a
#
# Break at testbench_wep_encrypt_v4.v line 144
```

First design with a minimum area:

No. clock cycles	1293
Clock cycle time	100ns
Delay No. cycles * cycle time	129300ns
Area occupied	Ports: 246 Nets: 15334 Cells: 12957 References: 32 Combinational area: 34826.0 Noncombinational area: 15568.0 **Total cell area: 50394.0**
Area * Delay	6515944200

Area

```
Information: Updating design information... (UID-85)
Warning: Design 'wep_encrypt_v4' contains 1 high-fanout nets. A fanout number of 1000 will be
used for delay calculations involving these nets. (TIM-134)

****************************************
Report : area
Design : wep_encrypt_v4
Version: V-2004.06-SP2
Date   : Wed Feb  7 13:59:04 2007
****************************************

Library(s) Used:

    class (File: /acsnfs3/software/synopsys-V-2004.06-SP2/libraries/syn/class.db)

Number of ports:              246
Number of nets:             15334
Number of cells:            12957
Number of references:          32

Combinational area:       34826.000000
Noncombinational area:    15568.000000
Net Interconnect area:      undefined  (Wire load has zero net area)

Total cell area:          50394.000000
Total area:                 undefined
```

Timing

```
****************************************
Report : timing
        -path full
        -delay max
        -max_paths 1
Design : wep_encrypt_v4
Version: V-2004.06-SP2
Date   : Wed Feb  7 13:59:05 2007
****************************************

 # A fanout number of 1000 was used for high fanout net computations.

Operating Conditions:
Wire Load Model Mode: top

  Startpoint: i_reg[1] (rising edge-triggered flip-flop clocked by clk)
  Endpoint: sbox_reg[4][2]
            (rising edge-triggered flip-flop clocked by clk)
  Path Group: clk
  Path Type: max

  Des/Clust/Port     Wire Load Model       Library
  ------------------------------------------------
  wep_encrypt_v4     20x20                 class
```

```
  Point                                                      Incr       Path
  ------------------------------------------------------------------------------
  clock clk (rise edge)                                      0.00       0.00
  clock network delay (ideal)                                0.00       0.00
  i_reg[1]/CP (FD1)                                          0.00 #     0.00 r
  i_reg[1]/Q (FD1)                                          54.62      54.62 r
  C64656/S1 (wep_encrypt_v4_MUX_OP_256_8_8_32)               0.00      54.62 r
  C64656/U2043/Z1 (B2I)                                      0.49      55.12 f
  C64656/U2053/Z (IVI)                                       9.11      64.22 r
  C64656/U1843/Z (MUX21L)                                    0.95      65.17 r
  C64656/U964/Z (MUX21L)                                     0.52      65.69 f
  C64656/U1840/Z (MUX21L)                                    0.55      66.24 r
  C64656/U958/Z (MUX21L)                                     0.52      66.76 f
  C64656/U1829/Z (MUX21L)                                    0.55      67.30 r
  C64656/U936/Z (MUX21L)                                     0.52      67.82 f
  C64656/U1786/Z (MUX21L)                                    1.56      69.38 r
  C64656/Z_5 (wep_encrypt_v4_MUX_OP_256_8_8_32)              0.00      69.38 r
  U12276/Z (ND2I)                                           25.95      95.33 f
  U2449/Z (NR2I)                                             0.80      96.14 r
  U2448/Z (AO1P)                                             0.36      96.50 f
  U12193/Z (EON1)                                            1.31      97.80 r
  sbox_reg[4][2]/D (FD1)                                     0.00      97.80 r
  data arrival time                                                    97.80

  clock clk (rise edge)                                    100.00     100.00
  clock network delay (ideal)                                0.00     100.00
  sbox_reg[4][2]/CP (FD1)                                    0.00     100.00 r
  library setup time                                        -0.80      99.20
  data required time                                                   99.20
  ------------------------------------------------------------------------------
  data required time                                                   99.20
  data arrival time                                                   -97.80
  ------------------------------------------------------------------------------
  slack (MET)                                                          1.40
```

Resources

```
****************************************
Report : resources
Design : wep_encrypt_v4
Version: V-2004.06-SP2
Date   : Wed Feb  7 13:59:07 2007
****************************************

Resource Sharing Report for design wep_encrypt_v4 in file ./wep_encrypt_v4.v

===============================================================================
|          |               |            | Contained     |                      |
| Resource | Module        | Parameters | Resources     | Contained Operations |
===============================================================================
| r1168    | DW01_inc      | width=8    |               | add_380 add_420      |
| r1169    | DW01_add      | width=8    |               | add_1_root_add_390_2 |
|          |               |            |               | add_447              |
| r1189    | DW01_add      | width=8    |               | add_0_root_add_390_2 |
| r1191    | DW01_add      | width=16   |               | add_406              |
| r1193    | DW01_cmp2     | width=32   |               | gte_409              |
| r1195    | DW01_add      | width=8    |               | add_419              |
| r1197    | DW01_add      | width=32   |               | add_422              |
| r1199    | DW01_cmp2     | width=32   |               | gte_422              |
| r1201    | DW01_inc      | width=2    |               | add_430              |
| r1203    | DW01_add      | width=16   |               | add_458              |
| r1205    | DW01_add      | width=32   |               | add_459              |
===============================================================================


Implementation Report

===============================================================================
|                  |                  | Current          | Set              |
```

Cell	Module	Implementation	Implementation
add_0_root_add_390_2	DW01_add	rpl	
add_406	DW01_add	rpl	
add_419	DW01_add	rpl	
add_422	DW01_add	rpl	
add_458	DW01_add	rpl	
add_459	DW01_add	rpl	
gte_409	DW01_cmp2	rpl	
gte_422	DW01_cmp2	rpl	
r1168	DW01_inc	rpl	
r1169	DW01_add	rpl	

Multiplexor Report

Cell	Width	Data	Select	Reference
C64655	8	256	8	wep_encrypt_v4_MUX_OP_256_8_8_33
C64656	8	256	8	wep_encrypt_v4_MUX_OP_256_8_8_32
C64657	8	256	8	wep_encrypt_v4_MUX_OP_256_8_8
C64658	8	8	3	wep_encrypt_v4_MUX_OP_8_3_8

References

```
****************************************
Report : reference
Design : wep_encrypt_v4
Version: V-2004.06-SP2
Date   : Wed Feb  7 13:59:06 2007
****************************************

Attributes:
    b - black box (unknown)
   bo - allows boundary optimization
    d - dont_touch
   mo - map_only
    h - hierarchical
    n - noncombinational
    r - removable
    s - synthetic operator
    u - contains unmapped logic
```

Reference	Library	Unit Area	Count	Total Area	Attributes
AN2I	class	2.000000	282	564.000000	
AN3	class	2.000000	66	132.000000	
AO1P	class	2.000000	341	682.000000	
AO2	class	2.000000	18	36.000000	
AO7	class	2.000000	39	78.000000	
EOI	class	3.000000	1	3.000000	
EON1	class	3.000000	72	216.000000	
FD1	class	7.000000	2224	15568.000000	n
IVDA	class	1.000000	2	2.000000	
IVI	class	1.000000	367	367.000000	
ND2I	class	1.000000	908	908.000000	
ND4	class	2.000000	1	2.000000	
ND5	class	4.000000	1	4.000000	
NR2I	class	1.000000	6347	6347.000000	
NR3	class	2.000000	16	32.000000	
OR2P	class	2.000000	240	480.000000	
OR3	class	2.000000	1031	2062.000000	
OR4	class	3.000000	987	2961.000000	
wep_encrypt_v4_DW01_add_8_0		100.000000	1	100.000000	h
wep_encrypt_v4_DW01_add_8_1		99.000000	1	99.000000	h
wep_encrypt_v4_DW01_add_8_2		105.000000	1	105.000000	h
wep_encrypt_v4_DW01_add_16_0		151.000000	1	151.000000	h
wep_encrypt_v4_DW01_add_16_1		151.000000	1	151.000000	h
wep_encrypt_v4_DW01_add_32_0		191.000000	1	191.000000	h

```
wep_encrypt_v4_DW01_add_32_1    168.000000       1    168.000000  h
wep_encrypt_v4_DW01_cmp2_32_0   200.000000       1    200.000000  h
wep_encrypt_v4_DW01_cmp2_32_1   200.000000       1    200.000000  h
wep_encrypt_v4_DW01_inc_8_0      37.000000       1     37.000000  h
wep_encrypt_v4_MUX_OP_8_3_8     146.000000       1    146.000000  h
wep_encrypt_v4_MUX_OP_256_8_8  6126.000000       1   6126.000000  h
wep_encrypt_v4_MUX_OP_256_8_8_32
                               6140.000000       1   6140.000000  h
wep_encrypt_v4_MUX_OP_256_8_8_33
                               6136.000000       1   6136.000000  h
--------------------------------------------------------------------------------
Total 32 references                                 50394.000000
```

Compiling

```
Information: Evaluating DesignWare library utilization. (UISN-27)

============================================================================
| DesignWare Building Block Library       |      Version       | Available |
============================================================================
| Basic DW Building Blocks                |                    |           |
                                          | V-2004.06-DWF_0406 |     *     |
| Licensed DW Building Blocks             |                    |           |
                                          |                    |           |
============================================================================
  Beginning Pass 1 Mapping
  ------------------------
  Processing 'wep_encrypt_v4'
  Updating timing information
  Beginning Implementation Selection
  ----------------------------------
  Processing 'wep_encrypt_v4_DW01_inc_8_0'
  Processing 'wep_encrypt_v4_DW01_add_8_0'
  Processing 'wep_encrypt_v4_DW01_add_8_1'
  Processing 'wep_encrypt_v4_DW01_add_16_0'
  Processing 'wep_encrypt_v4_DW01_cmp2_32_0'
  Processing 'wep_encrypt_v4_DW01_add_8_2'
  Processing 'wep_encrypt_v4_DW01_add_32_0'
  Processing 'wep_encrypt_v4_DW01_cmp2_32_1'
  Processing 'DW01_inc_2_0'
  Processing 'wep_encrypt_v4_DW01_add_16_1'
  Processing 'wep_encrypt_v4_DW01_add_32_1'
  Beginning Mapping Optimizations  (High effort)
  -------------------------------
                           ELAPSED
CPU SEC MBYTES   AREA      TIME
------- ------ --------- ---------
   1537  287.4   53284.0   0:33:19
   1555  287.4   51852.0   0:33:38
  Beginning Delay Optimization Phase
  ----------------------------------
------- ------ --------- ---------
   1555  287.4   51852.0   0:33:38
  Beginning Area-Recovery Phase  (max_area 0)
  ---------------------------
------- ------ --------- ---------
   1555  287.4   51852.0   0:33:38
   1557  287.4   51852.0   0:33:40
   1625  287.4   51679.0   0:34:53
Information: Complementing port 'S0' in design 'wep_encrypt_v4_MUX_OP_256_8_8'.
           The new name of the port is 'S0_BAR'. (OPT-319)
Information: Complementing port 'S1' in design 'wep_encrypt_v4_MUX_OP_256_8_8'.
           The new name of the port is 'S1_BAR'. (OPT-319)
Information: Complementing port 'S2' in design 'wep_encrypt_v4_MUX_OP_256_8_8'.
           The new name of the port is 'S2_BAR'. (OPT-319)
Information: Complementing port 'S3' in design 'wep_encrypt_v4_MUX_OP_256_8_8'.
           The new name of the port is 'S3_BAR'. (OPT-319)
Information: Complementing port 'S4' in design 'wep_encrypt_v4_MUX_OP_256_8_8'.
           The new name of the port is 'S4_BAR'. (OPT-319)
   1690  287.4   50851.0   0:36:00
   1739  287.4   50542.0   0:36:52
   1746  287.4   50542.0   0:36:59
   1884  287.4   50508.0   0:39:25
   1919  287.4   50428.0   0:40:02
   1958  287.4   50398.0   0:40:42
   1972  287.4   50394.0   0:40:58
  Optimization Complete
  ---------------------
Warning: Design 'wep_encrypt_v4' contains 1 high-fanout nets. A fanout number of 1000 will be
used for delay calculations involving these nets. (TIM-134)
     Net 'port_A_clk': 2225 load(s), 1 driver(s)
  Transferring design 'wep_encrypt_v4' to database 'wep_encrypt_v4.db'
Current design is 'wep_encrypt_v4'.
```

Elaborate

```
Running PRESTO HDLC
Loading db file '/acsnfs3/software/synopsys-V-2004.06-SP2/libraries/syn/standard.sldb'
Loading db file '/acsnfs3/software/synopsys-V-2004.06-SP2/libraries/syn/gtech.db'
Loading db file '/acsnfs3/software/synopsys-V-2004.06-SP2/libraries/syn/class.db'

Statistics for case statements in always block at line 94 in file
         './wep_encrypt_v4.v'
===============================================
|           Line           |  full/ parallel  |
===============================================
|            98            |    auto/auto     |
|           431            |    auto/auto     |
===============================================
Warning:  ./wep_encrypt_v4.v:390: Potential simulation-synthesis mismatch if index exceeds size
of array 'seed'. (ELAB-349)

Inferred memory devices in process
         in routine wep_encrypt_v4 line 94 in file
                  './wep_encrypt_v4.v'.
================================================================================
|    Register Name    |   Type    | Width | Bus | MB | AR | AS | SR | SS | ST |
================================================================================
|    port_A_we_reg    | Flip-flop |   1   |  N  | N  | N  | N  | N  | N  | N  |
| port_A_data_in_reg  | Flip-flop |  32   |  N  | N  | N  | N  | N  | N  | N  |
|        j_reg        | Flip-flop |   8   |  Y  | N  | N  | N  | N  | N  | N  |
|   port_A_addr_reg   | Flip-flop |  16   |  Y  | N  | N  | N  | N  | N  | N  |
|   byte_count_reg    | Flip-flop |   2   |  Y  | N  | N  | N  | N  | N  | N  |
|      sbox_reg       | Flip-flop | 2048  |  N  | N  | N  | N  | N  | N  | N  |
|        i_reg        | Flip-flop |   8   |  Y  | N  | N  | N  | N  | N  | N  |
|      done_reg       | Flip-flop |   1   |  N  | N  | N  | N  | N  | N  | N  |
|      seed_reg       | Flip-flop |  64   |  Y  | N  | N  | N  | N  | N  | N  |
|      index_reg      | Flip-flop |   8   |  Y  | N  | N  | N  | N  | N  | N  |
|  current_state_reg  | Flip-flop |   4   |  N  | N  | N  | N  | N  | N  | N  |
|      count_reg      | Flip-flop |  32   |  Y  | N  | N  | N  | N  | N  | N  |
================================================================================
Statistics for MUX_OPs
============================================================
|  block name/line   | Inputs | Outputs | # sel inputs | MB |
============================================================
| wep_encrypt_v4/378 |  256   |    8    |      8       | N  |
| wep_encrypt_v4/379 |  256   |    8    |      8       | N  |
| wep_encrypt_v4/433 |  256   |    8    |      8       | N  |
| wep_encrypt_v4/390 |   8    |    8    |      3       | N  |
============================================================
Presto compilation completed successfully.
Current design is now 'wep_encrypt_v4'
```

Second design with a 25ns constraint:

No. clock cycles	1293
Clock cycle time	25ns
Delay No. cycles * cycle time	43425ns
Area occupied	Ports: 246 Nets: 15675 Cells: 13216 References: 32 Combinational area: 35120.0 Noncombinational area: 15568.0 **Total cell area: 50688.0**
Area * Delay	2201126400

Area

```
Information: Updating design information... (UID-85)
Warning: Design 'wep_encrypt_v4' contains 1 high-fanout nets. A fanout number of 1000 will be
used for delay calculations involving these nets. (TIM-134)

****************************************
Report : area
Design : wep_encrypt_v4
Version: V-2004.06-SP2
Date   : Wed Feb  7 15:41:13 2007
****************************************

Library(s) Used:

    class (File: /acsnfs3/software/synopsys-V-2004.06-SP2/libraries/syn/class.db)

Number of ports:              246
Number of nets:             15675
Number of cells:            13216
Number of references:          37

Combinational area:       35120.000000
Noncombinational area:    15568.000000
Net Interconnect area:      undefined  (Wire load has zero net area)

Total cell area:          50688.000000
Total area:                 undefined
```

Compile

```
Information: Evaluating DesignWare library utilization. (UISN-27)

============================================================================
| DesignWare Building Block Library       |      Version       | Available |
============================================================================
| Basic DW Building Blocks                |                    |           |
                                          | V-2004.06-DWF_0406 |     *     |
| Licensed DW Building Blocks             |                    |           |
                                          |                    |           |
============================================================================


  Beginning Pass 1 Mapping
  ------------------------
  Processing 'wep_encrypt_v4'

  Updating timing information

  Beginning Implementation Selection
  ----------------------------------
  Processing 'wep_encrypt_v4_DW01_inc_8_0'
  Processing 'wep_encrypt_v4_DW01_add_8_0'
  Processing 'wep_encrypt_v4_DW01_add_8_1'
  Processing 'wep_encrypt_v4_DW01_add_16_0'
```

```
  Processing 'wep_encrypt_v4_DW01_cmp2_32_0'
  Processing 'wep_encrypt_v4_DW01_add_8_2'
  Processing 'wep_encrypt_v4_DW01_add_32_0'
  Processing 'wep_encrypt_v4_DW01_cmp2_32_1'
  Processing 'DW01_inc_2_0'
  Processing 'wep_encrypt_v4_DW01_add_16_1'
  Processing 'wep_encrypt_v4_DW01_add_32_1'

  Beginning Mapping Optimizations  (High effort)
  -------------------------------

                          ELAPSED
CPU SEC MBYTES   AREA      TIME
------- ------ --------- ---------
   1627  282.4   53912.0   0:34:35
   1638  282.4   51945.0   0:34:47
   1675  282.4   52182.0   0:35:26
   1714  282.4   51964.0   0:36:06


  Beginning Delay Optimization Phase
  ----------------------------------

                          ELAPSED
CPU SEC MBYTES   AREA      TIME
------- ------ --------- ---------
   1714  282.4   51964.0   0:36:06


  Beginning Area-Recovery Phase  (max_area 0)
  ------------------------------

                          ELAPSED
CPU SEC MBYTES   AREA      TIME
------- ------ --------- ---------
   1714  282.4   51964.0   0:36:06
   1715  282.4   51964.0   0:36:08
   1781  282.4   51723.0   0:37:16
   1791  282.4   51702.0   0:37:27
Information: Complementing port 'S0' in design 'wep_encrypt_v4_MUX_OP_256_8_8'.
          The new name of the port is 'S0_BAR'. (OPT-319)
Information: Complementing port 'S2' in design 'wep_encrypt_v4_MUX_OP_256_8_8'.
          The new name of the port is 'S2_BAR'. (OPT-319)
Information: Complementing port 'S3' in design 'wep_encrypt_v4_MUX_OP_256_8_8'.
          The new name of the port is 'S3_BAR'. (OPT-319)
Information: Complementing port 'S4' in design 'wep_encrypt_v4_MUX_OP_256_8_8'.
          The new name of the port is 'S4_BAR'. (OPT-319)
   1853  282.4   51276.0   0:38:33
   1923  282.4   50823.0   0:39:47
   1941  282.4   50823.0   0:40:05
   1946  282.4   50823.0   0:40:11
   1964  282.4   50823.0   0:40:30
   2113  282.4   50793.0   0:43:09
   2146  282.4   50707.0   0:43:44
   2178  282.4   50689.0   0:44:19
   2193  282.4   50688.0   0:44:34

  Optimization Complete
  ---------------------
Warning: Design 'wep_encrypt_v4' contains 1 high-fanout nets. A fanout number of 1000 will be
used for delay calculations involving these nets. (TIM-134)
     Net 'port_A_clk': 2225 load(s), 1 driver(s)
  Transferring design 'wep_encrypt_v4' to database 'wep_encrypt_v4.db'

Current design is 'wep_encrypt_v4'.
```

Elaborate

```
Running PRESTO HDLC
Loading db file '/acsnfs3/software/synopsys-V-2004.06-SP2/libraries/syn/standard.sldb'
Loading db file '/acsnfs3/software/synopsys-V-2004.06-SP2/libraries/syn/gtech.db'
Loading db file '/acsnfs3/software/synopsys-V-2004.06-SP2/libraries/syn/class.db'

Statistics for case statements in always block at line 94 in file
         './wep_encrypt_v4.v'
===============================================
|           Line           |  full/ parallel  |
===============================================
|            98            |    auto/auto     |
|           431            |    auto/auto     |
===============================================
Warning:  ./wep_encrypt_v4.v:390: Potential simulation-synthesis mismatch if index exceeds size
of array 'seed'. (ELAB-349)

Inferred memory devices in process
         in routine wep_encrypt_v4 line 94 in file
                  './wep_encrypt_v4.v'.
================================================================================
|    Register Name    |   Type    | Width | Bus | MB | AR | AS | SR | SS | ST |
================================================================================
|    port_A_we_reg    | Flip-flop |   1   |  N  | N  | N  | N  | N  | N  | N  |
| port_A_data_in_reg  | Flip-flop |  32   |  N  | N  | N  | N  | N  | N  | N  |
|        j_reg        | Flip-flop |   8   |  Y  | N  | N  | N  | N  | N  | N  |
|   port_A_addr_reg   | Flip-flop |  16   |  Y  | N  | N  | N  | N  | N  | N  |
|   byte_count_reg    | Flip-flop |   2   |  Y  | N  | N  | N  | N  | N  | N  |
|      sbox_reg       | Flip-flop | 2048  |  N  | N  | N  | N  | N  | N  | N  |
|        i_reg        | Flip-flop |   8   |  Y  | N  | N  | N  | N  | N  | N  |
|      done_reg       | Flip-flop |   1   |  N  | N  | N  | N  | N  | N  | N  |
|      seed_reg       | Flip-flop |  64   |  Y  | N  | N  | N  | N  | N  | N  |
|      index_reg      | Flip-flop |   8   |  Y  | N  | N  | N  | N  | N  | N  |
|  current_state_reg  | Flip-flop |   4   |  N  | N  | N  | N  | N  | N  | N  |
|      count_reg      | Flip-flop |  32   |  Y  | N  | N  | N  | N  | N  | N  |
================================================================================
Statistics for MUX_OPs
============================================================
|  block name/line   | Inputs | Outputs | # sel inputs | MB |
============================================================
| wep_encrypt_v4/378 |  256   |    8    |      8       | N  |
| wep_encrypt_v4/379 |  256   |    8    |      8       | N  |
| wep_encrypt_v4/433 |  256   |    8    |      8       | N  |
| wep_encrypt_v4/390 |   8    |    8    |      3       | N  |
============================================================
Presto compilation completed successfully.
Current design is now 'wep_encrypt_v4'
```

Reference

```
****************************************
Report : reference
Design : wep_encrypt_v4
Version: V-2004.06-SP2
Date   : Wed Feb  7 15:41:16 2007
****************************************

Attributes:
    b - black box (unknown)
   bo - allows boundary optimization
    d - dont_touch
   mo - map_only
    h - hierarchical
    n - noncombinational
    r - removable
    s - synthetic operator
    u - contains unmapped logic

Reference          Library       Unit Area   Count    Total Area   Attributes
--------------------------------------------------------------------------------
```

```
AN2I                class          2.000000     284    568.000000
AN3                 class          2.000000      35     70.000000
AO1                 class          2.000000       3      6.000000
AO1P                class          2.000000     330    660.000000
AO2                 class          2.000000      18     36.000000
AO3                 class          2.000000       8     16.000000
AO4                 class          2.000000      67    134.000000
AO7                 class          2.000000      16     32.000000
B2I                 class          2.000000       8     16.000000
EOI                 class          3.000000       1      3.000000
EON1                class          3.000000       5     15.000000
FD1                 class          7.000000    2224  15568.000000  n
IVDA                class          1.000000      34     34.000000
IVDAP               class          2.000000       3      6.000000
IVI                 class          1.000000     549    549.000000
IVP                 class          1.000000       1      1.000000
ND2I                class          1.000000     969    969.000000
ND3                 class          2.000000       9     18.000000
NR2I                class          1.000000    6352   6352.000000
NR3                 class          2.000000      29     58.000000
OR2P                class          2.000000     230    460.000000
OR3                 class          2.000000    1038   2076.000000
OR4                 class          3.000000     989   2967.000000
wep_encrypt_v4_DW01_add_8_0     110.000000       1    110.000000  h
wep_encrypt_v4_DW01_add_8_1     104.000000       1    104.000000  h
wep_encrypt_v4_DW01_add_8_2     110.000000       1    110.000000  h
wep_encrypt_v4_DW01_add_16_0    151.000000       1    151.000000  h
wep_encrypt_v4_DW01_add_16_1    151.000000       1    151.000000  h
wep_encrypt_v4_DW01_add_32_0    191.000000       1    191.000000  h
wep_encrypt_v4_DW01_add_32_1    168.000000       1    168.000000  h
wep_encrypt_v4_DW01_cmp2_32_0   199.000000       1    199.000000  h
wep_encrypt_v4_DW01_cmp2_32_1   205.000000       1    205.000000  h
wep_encrypt_v4_DW01_inc_8_0      37.000000       1     37.000000  h
wep_encrypt_v4_MUX_OP_8_3_8     148.000000       1    148.000000  h
wep_encrypt_v4_MUX_OP_256_8_8  6148.000000       1   6148.000000  h
wep_encrypt_v4_MUX_OP_256_8_8_31
                               6189.000000       1   6189.000000  h
wep_encrypt_v4_MUX_OP_256_8_8_32
                               6163.000000       1   6163.000000  h
------------------------------------------------------------------------------
Total 37 references                                  50688.000000
```

Resources

```
****************************************
Report : resources
Design : wep_encrypt_v4
Version: V-2004.06-SP2
Date   : Wed Feb  7 15:41:17 2007
****************************************

Resource Sharing Report for design wep_encrypt_v4 in file ./wep_encrypt_v4.v

================================================================================
|          |              |            | Contained     |                       |
| Resource | Module       | Parameters | Resources     | Contained Operations  |
================================================================================
| r1168    | DW01_inc     | width=8    |               | add_380 add_420       |
| r1169    | DW01_add     | width=8    |               | add_1_root_add_390_2  |
|          |              |            |               | add_447               |
| r1189    | DW01_add     | width=8    |               | add_0_root_add_390_2  |
| r1191    | DW01_add     | width=16   |               | add_406               |
| r1193    | DW01_cmp2    | width=32   |               | gte_409               |
| r1195    | DW01_add     | width=8    |               | add_419               |
| r1197    | DW01_add     | width=32   |               | add_422               |
| r1199    | DW01_cmp2    | width=32   |               | gte_422               |
| r1201    | DW01_inc     | width=2    |               | add_430               |
| r1203    | DW01_add     | width=16   |               | add_458               |
| r1205    | DW01_add     | width=32   |               | add_459               |
================================================================================
```

Implementation Report

Cell	Module	Current Implementation	Set Implementation
add_0_root_add_390_2	DW01_add	rpl	
add_406	DW01_add	rpl	
add_419	DW01_add	rpl	
add_422	DW01_add	rpl	
add_458	DW01_add	rpl	
add_459	DW01_add	rpl	
gte_409	DW01_cmp2	rpl	
gte_422	DW01_cmp2	rpl	
r1168	DW01_inc	rpl	
r1169	DW01_add	rpl	

Multiplexor Report

Cell	Width	Data	Select	Reference
C64655	8	256	8	wep_encrypt_v4_MUX_OP_256_8_8_32
C64656	8	256	8	wep_encrypt_v4_MUX_OP_256_8_8_31
C64657	8	256	8	wep_encrypt_v4_MUX_OP_256_8_8
C64658	8	8	3	wep_encrypt_v4_MUX_OP_8_3_8

Timing

```
****************************************
Report : timing
        -path full
        -delay max
        -max_paths 1
Design : wep_encrypt_v4
Version: V-2004.06-SP2
Date   : Wed Feb  7 15:41:15 2007
****************************************

 # A fanout number of 1000 was used for high fanout net computations.

Operating Conditions:
Wire Load Model Mode: top

  Startpoint: j_reg[0] (rising edge-triggered flip-flop clocked by clk)
  Endpoint: sbox_reg[11][1]
            (rising edge-triggered flip-flop clocked by clk)
  Path Group: clk
  Path Type: max

  Des/Clust/Port     Wire Load Model       Library
  ------------------------------------------------
  wep_encrypt_v4     20x20                 class

  Point                                                    Incr       Path
  ---------------------------------------------------------------------------
  clock clk (rise edge)                                    0.00       0.00
  clock network delay (ideal)                              0.00       0.00
  j_reg[0]/CP (FD1)                                        0.00 #     0.00 r
  j_reg[0]/Q (FD1)                                         1.47       1.47 f
  U12349/Z (IVI)                                           0.31       1.77 r
  U11923/Z (IVP)                                           0.83       2.61 f
  C64655/S0 (wep_encrypt_v4_MUX_OP_256_8_8_32)             0.00       2.61 f
  C64655/U2295/Z (IVI)                                     0.67       3.28 r
  C64655/U2269/Z (IVI)                                    11.39      14.67 f
  C64655/U1121/Z (MUX21L)                                  0.95      15.62 r
```

```
C64655/U1922/Z (MUX21L)                                  0.52      16.14 f
C64655/U1118/Z (MUX21L)                                  0.55      16.68 r
C64655/U2195/Z (MUX21L)                                  0.52      17.20 f
C64655/U1107/Z (MUX21L)                                  0.55      17.75 r
C64655/U2129/Z (MUX21L)                                  0.52      18.27 f
C64655/U1106/Z (MUX21L)                                  0.55      18.82 r
C64655/U2061/Z (MUX21L)                                  0.87      19.69 f
C64655/Z_6 (wep_encrypt_v4_MUX_OP_256_8_8_32)            0.00      19.69 f
U10734/Z (ND2I)                                          0.62      20.31 r
U12396/Z (IVI)                                           0.95      21.26 f
U12386/Z (IVI)                                           1.22      22.48 r
U9725/Z (NR2I)                                           0.22      22.70 f
U9724/Z (OR4)                                            1.50      24.20 f
sbox_reg[11][1]/D (FD1)                                  0.00      24.20 f
data arrival time                                                  24.20

clock clk (rise edge)                                   25.00      25.00
clock network delay (ideal)                              0.00      25.00
sbox_reg[11][1]/CP (FD1)                                 0.00      25.00 r
library setup time                                      -0.80      24.20
data required time                                                 24.20
-----------------------------------------------------------------------------
data required time                                                 24.20
data arrival time                                                 -24.20
-----------------------------------------------------------------------------
slack (MET)                                                         0.00
```

Comparison

The state machine is what was concluded upon after several revisions. Not only did we aim at simplifying the encrypt machine, we also focused on reducing the number of states to make it more efficient. We adjusted the script files accordingly for synopsys with a 25ns restraint. As seen from the above timing diagram, it seems that the data required time was less than the 25ns clock time set (at 24.20 ns). The result from running two different scripts on the same state machines was as suspected. The number of adders and muxes remains the same since no changes to that will occur without changing the actual verilog code with states.

We attempted to test and analyze another encrypt mechanism by splitting states that had multiple addition logic in one statement. Although this would increase the number of states, and therefore increase the number of clock cycles required, it would allow for the circuit to REUSE the adder. Adders consist of many parts, and we suspect that it would minimize the design by taking out long mathematical logic. However, the consequence of adding an additional, single mathematical expression state was that sythesys would often run out of memory during compile (it would get through elaborate and such fine). We believe that it is the machine due to the number of synthesys programs running from other groups. We have also tried different servers, but ending with the same result as other groups are attempting this. Although we tried figuring out a solution (contacting staff, making new state diagrams/machines, etc), we could just not be successful in doing so. We were successful upon adding a single state by splitting the “construct sbox” state that computed j. We predicted that by splitting this state, we could REUSE the adder since it would be on 2 different clock cycles. After analyzing the data, it seemed that there was very little noticeable difference. The timing seemed the same, except the data arrival time went from -97.80 to -99.18 with the additional state. The area expanded- and it is possible with the increase of flipflops and mux size. The area, however, was a difference of about 200 (total cell area), which is quite insignificant to the overall size (50500). (Less nets, and more cells with the additional of a state).

We do feel, however, that the state machine above is one that has been well thought and implements a correct algorithm with fewer states. With that, we feel that adding additional states to minimize area (reuse adders and such, and increase delay) would be to verify our projections for the results rather than to further the development of our wep encrypt mechanism.

With an additional state:

```
****************************************
Report : timing
        -path full
        -delay max
        -max_paths 1
Design : wep_encrypt_v4
Version: V-2004.06-SP2
Date   : Thu Feb  8 01:46:37 2007
****************************************

 # A fanout number of 1000 was used for high fanout net computations.

Operating Conditions:
Wire Load Model Mode: top

  Startpoint: i_reg[2] (rising edge-triggered flip-flop clocked by clk)
  Endpoint: sbox_reg[0][4]
            (rising edge-triggered flip-flop clocked by clk)
  Path Group: clk
  Path Type: max

  Des/Clust/Port     Wire Load Model       Library
  ------------------------------------------------
  wep_encrypt_v4     20x20                 class

  Point                                                   Incr       Path
  --------------------------------------------------------------------------
  clock clk (rise edge)                                   0.00       0.00
  clock network delay (ideal)                             0.00       0.00
  i_reg[2]/CP (FD1)                                       0.00 #     0.00 r
  i_reg[2]/Q (FD1)                                       72.36      72.36 r
  C64662/S2 (wep_encrypt_v4_MUX_OP_256_8_8_31)            0.00      72.36 r
  C64662/U2045/Z2 (B2I)                                   3.19      75.54 r
  C64662/U2044/Z (IVDA)                                  11.18      86.73 r
  C64662/U576/Z (MUX21L)                                  0.72      87.45 f
  C64662/U1649/Z (MUX21L)                                 0.55      87.99 r
  C64662/U575/Z (MUX21L)                                  0.52      88.51 f
  C64662/U1638/Z (MUX21L)                                 0.55      89.06 r
  C64662/U511/Z (MUX21L)                                  0.52      89.58 f
  C64662/U1616/Z (MUX21L)                                 1.35      90.94 r
  C64662/Z_3 (wep_encrypt_v4_MUX_OP_256_8_8_31)           0.00      90.94 r
  U10709/Z (ND2I)                                         4.00      94.93 f
  U12339/Z (IVI)                                          0.61      95.54 r
  U12337/Z (IVI)                                          2.25      97.79 f
  U10708/Z (NR2I)                                         0.65      98.43 r
  U10706/Z (OR3)                                          0.75      99.18 r
  sbox_reg[0][4]/D (FD1)                                  0.00      99.18 r
  data arrival time                                                 99.18

  clock clk (rise edge)                                 100.00     100.00
  clock network delay (ideal)                             0.00     100.00
  sbox_reg[0][4]/CP (FD1)                                 0.00     100.00 r
  library setup time                                     -0.80      99.20
  data required time                                                99.20
  --------------------------------------------------------------------------
  data required time                                                99.20
  data arrival time                                                -99.18
  --------------------------------------------------------------------------
  slack (MET)                                                       0.02


Information: Updating design information... (UID-85)
Warning: Design 'wep_encrypt_v4' contains 1 high-fanout nets. A fanout number of 1000 will be
used for delay calculations involving these nets. (TIM-134)

****************************************
Report : area
Design : wep_encrypt_v4
Version: V-2004.06-SP2
Date   : Thu Feb  8 01:46:36 2007
****************************************

Library(s) Used:

    class (File: /acsnfs3/software/synopsys-V-2004.06-SP2/libraries/syn/class.db)

Number of ports:              246
Number of nets:             15457
Number of cells:            13069
```

```
Number of references:          32

Combinational area:       34932.000000
Noncombinational area:    15568.000000
Net Interconnect area:      undefined  (Wire load has zero net area)

Total cell area:          50500.000000
Total area:                 undefined
```