SAND2009-4649P

Summer 2009 STAR Program

Alex Baker

Center for Cyber Defenders

Who am I?

- My Name is Alex Baker
- From Rio Rancho, NM
- Go to Rio Rancho High School
- Will be a senior next year, graduating in 2010
- Taken several computer science classes

Where I work

- Work at the Sandia National Lab's Center for Cyber Defenders (CCD)
- Even though I am in the CCD, I do work for the Sandia National Laboratories Cryptography Department
- Outside of the Tech or restricted Area

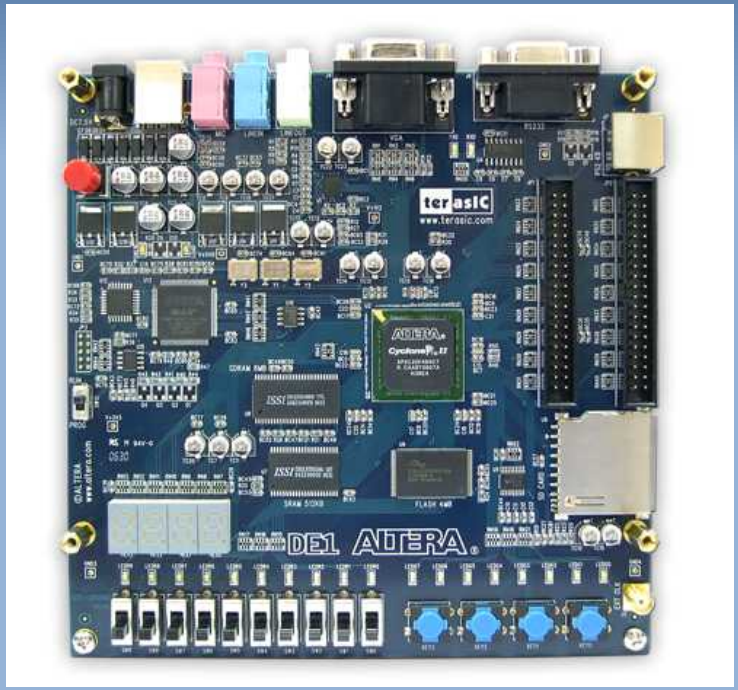
What I work on

- Project:
  - Work with an FPGA (**F**ield **P**rogrammable **G**ate **A**rray)
  - Put AES (**A**dvanced **E**ncryption **S**tandard) onto the FPGA and then optimize the FPGA for power consumption
    - Encryption is important for keeping your data safe. A good encryption will allow only people who have a "Need to Know" to be able to look at your data. AES is approved by for the encryption of unclassified but sensitive information.
  - Goal is to use the least amount of power while executing the encryption on the FPGA

FPGA

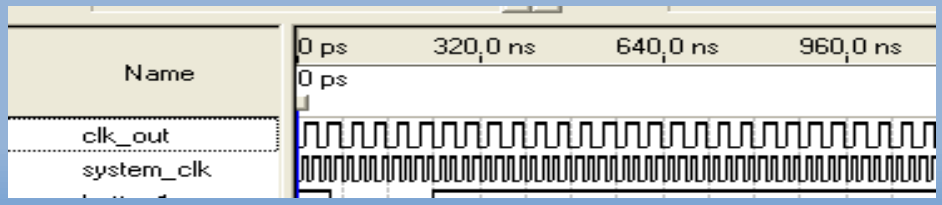
- An FPGA is hardware, similar to a processor
  - A FPGA is different than a processor in that it is reprogrammable
    - This means that the gates can be reconfigured, or reprogrammed
- FPGA's are very useful in the development of silicon chips
  - Can test the program on the FPGA and fix it as needed before putting it into silicon

- The Altera Cyclone II board was used for these tests
- Hardware description languages are used to program the FPGA
- Altera's Quartus II software and VHDL were used to program the board



Power Optimization

- Power optimization is usually a trade off with performance.
  - Less power means less speed
- There are two main types of power that are looked at for power optimization
  - Dynamic power:
    - This is power used to change the state of a gate from 0 to 1 or vice versa
    - A major source of this power is the clock, because it is constantly switching between 0 and 1

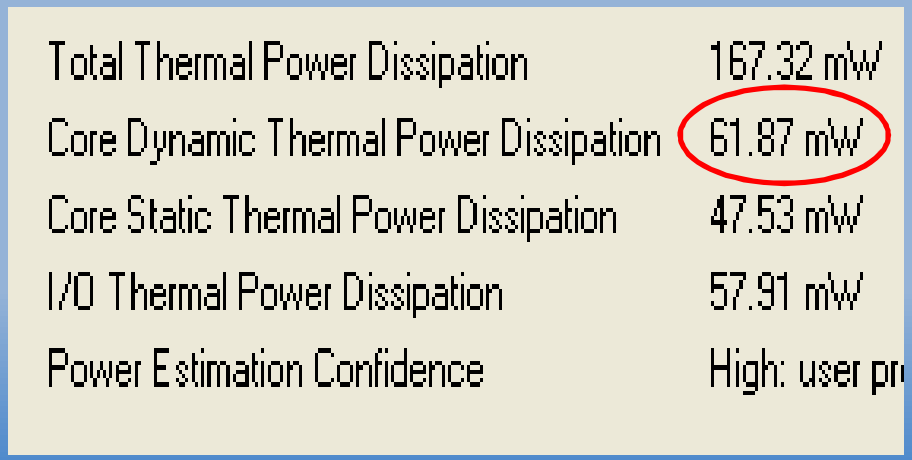


  - Static power
    - Power that is lost while a gate is at rest.

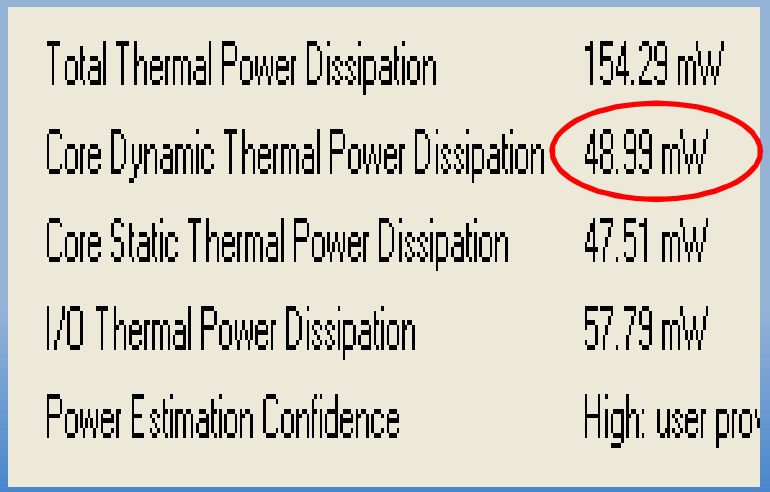
Fixes

- Settings can be made during Analysis and Synthesis to optimize for power
  - This reduces the dynamic power some

Regular Synthesis

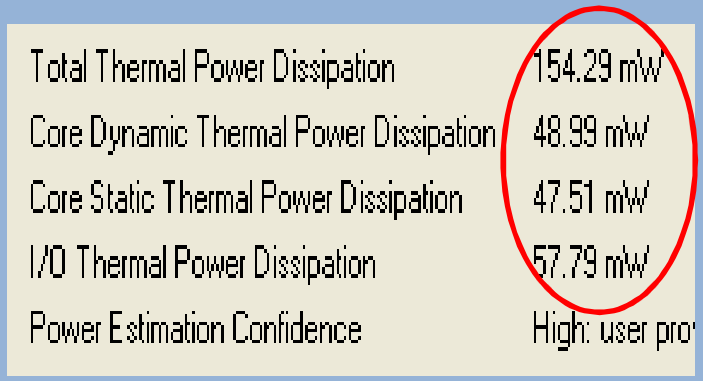


Optimized synthesis

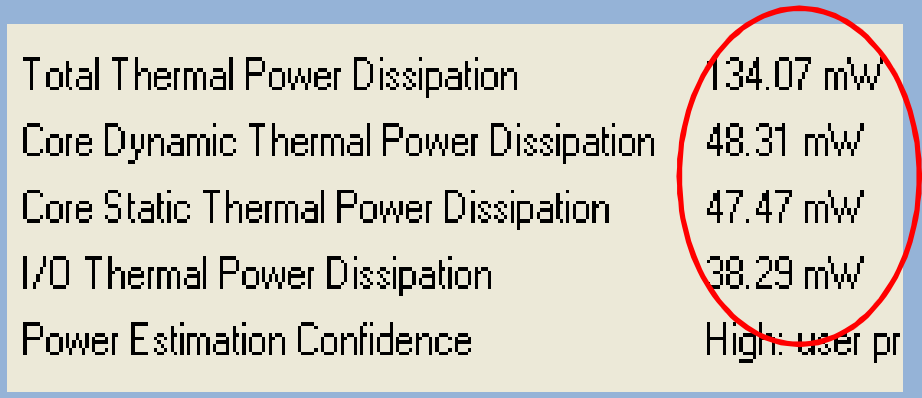


- Reducing the number of input and output also helps the power usage as a whole

Power optimized Synthesis



Optimized synthesis with less I/O ports

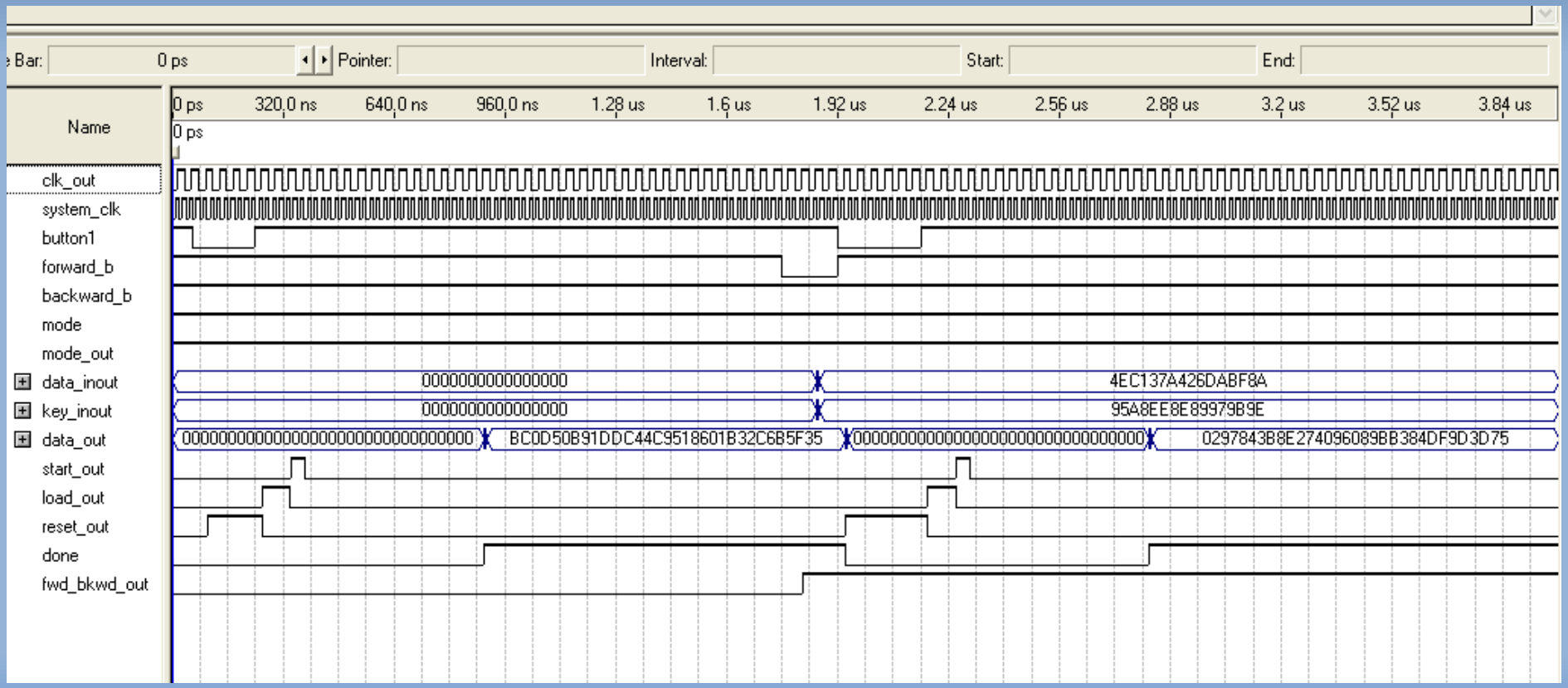


Advanced Encryption Standard

- Also Known as Rijndael
- In 1997, the US Government issued a call for a new encryption standard to be created
- In 2001, the Rijndael algorithm was chosen by The **N**ational **I**nstitute of **S**tandards and **T**echnology (NIST) to be the Advanced Encryption Standard
- AES is a symmetric block cipher
  - Meaning the it deals with data in blocks, usually 16 byte blocks
  - AES also uses symmetric keys, meaning that both the sender (encoder) and the receiver (decoder) use the same secret key

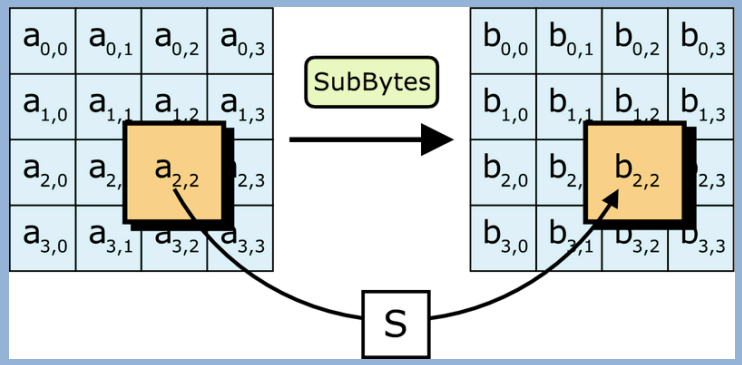
- Each of these blocks are then considered a state
- Each State then goes through multiple transformations, consisting of Byte Substitution, Shift Row, Mix Column, and AddRoundyKey
- All of these transformations make 1 round in the algorithm. Depending on key size, the state goes through 10-14 rounds
- The round key is generated separately, but through a similar process

Working Simulation of AES in Altera Quartus II Software



Steps to Encryption

- Byte Substitution
  - This is the first step in the round.
  - It consist of replacing the bytes in the state in a look up table
    - This table is called an S-Box
    - S-Box is derived using special mathematics in a finite field GF(2^8)
    - The S-Box never changes, so a simple table can be used without using any math

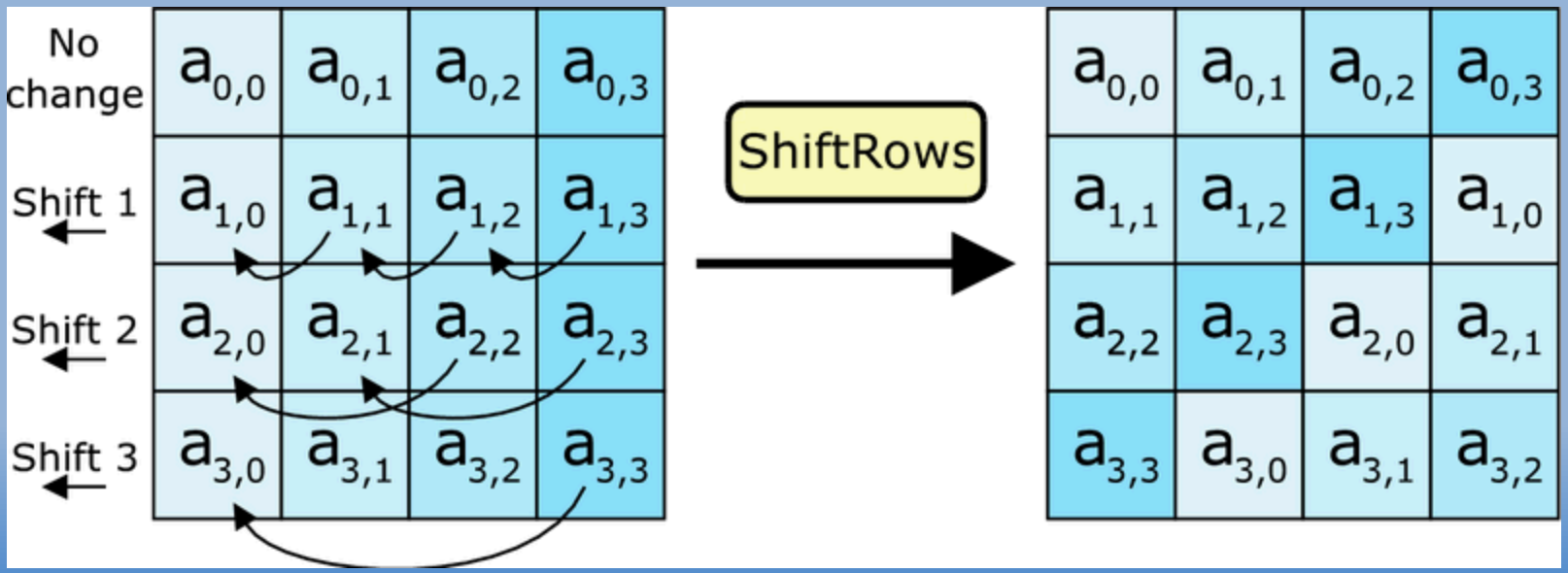


S-Box

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

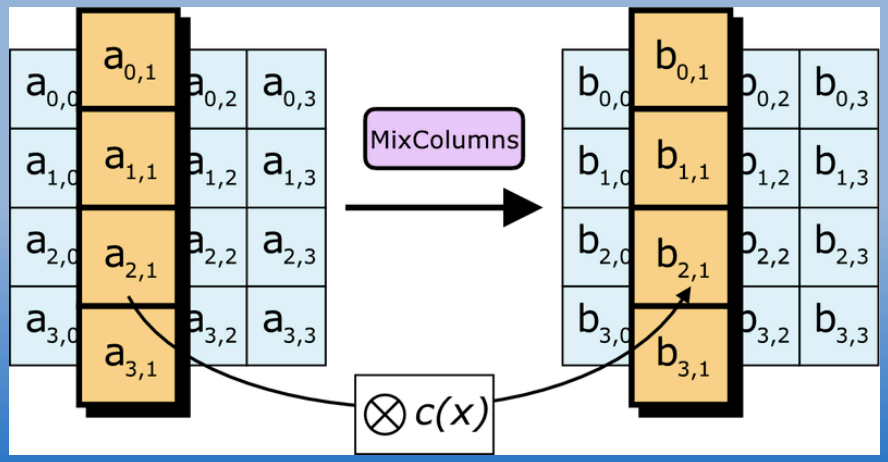
Shift Rows

- Shift rows is simple, each consecutive row is shifted one more to the left



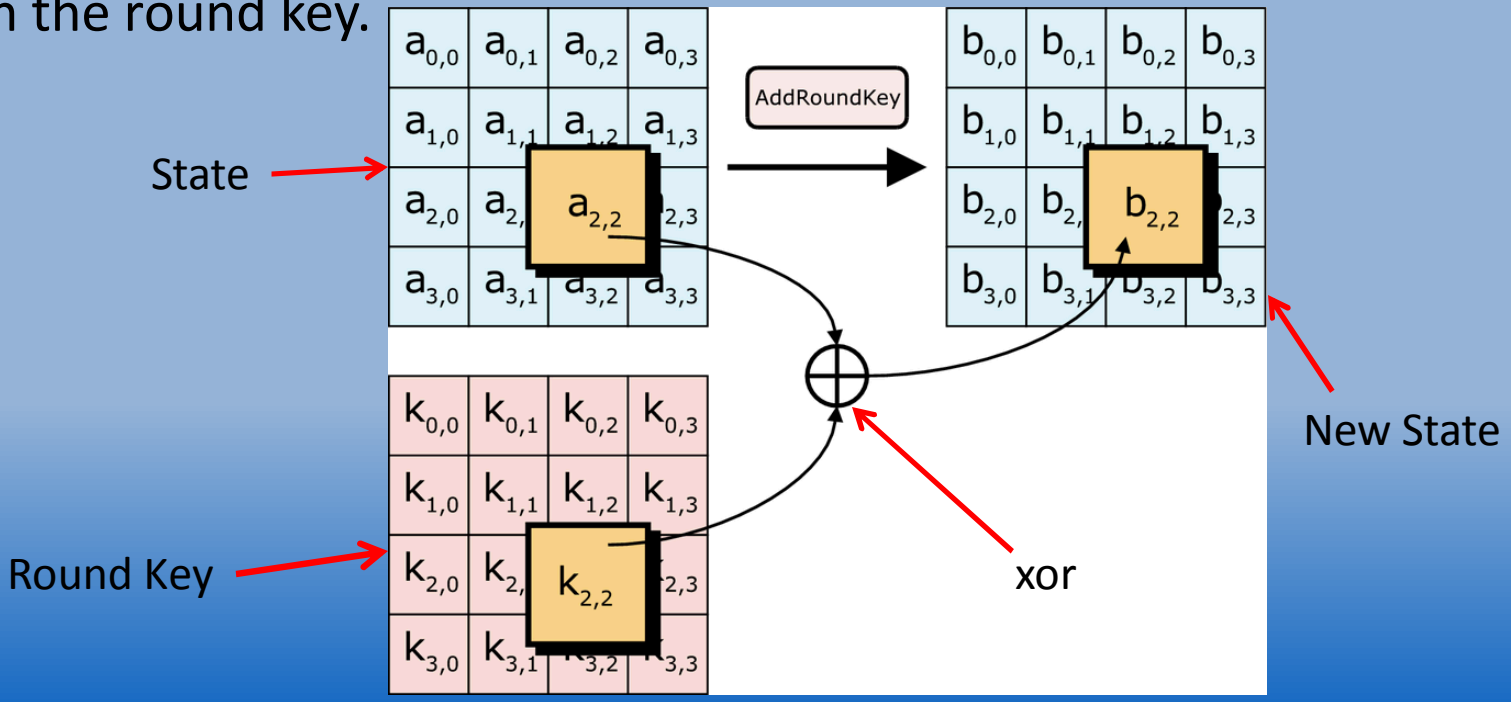
Mix Column

- Each column is assorted into a polynomial of degree 3 – A(x). This is then multiplied by a fixed polynomial C(x) = 3x^3 + x^2 + x + 2.
- The result of A(x) * C(x) is multiplied modulo x^4 + 1. The purpose of this is to get the polynomial back to degree 3.
- Modulo is simply a remainder function. In mix columns, it finds the remainder of A(x) * C(x) / x^4 + 1
- The coefficients of the modulo function then get put back into the state column



AddRoundKey

- The Round Key is generated separately from the state, called Key Expansion.
- A different Round Key is used for each round.
- The Round Key is the same size as the state.
- During the Round Key step, each byte in the state is xor with each byte in the round key.



- This process is done 10 – 14 times depending on key size.
- AES Accepts Key sizes of 128 bits, 192 bits, and 256 bits.
- Decryption goes through the same process, only inverses of the functions are used.

Results

- AES code from opencores.com was successfully modified for the Altera Cyclone II FPGA
- Decreased dynamic power dissipation from 61 mW to 48 mW
- Static power hardly changed
- By decreasing I/O ports, I/O power dissipation went from 57 to 38 mW

Conclusion

- AES was successfully optimized for power on the Altera Cyclone II FPGA board
- This was successfully done by changing synthesis settings for power optimization and reducing the number of I/O ports used in the program
- Future Measures: In the future, less power could be used by turning off part of the circuit that is no longer in use. An example would be turning off the sub bytes part of the circuit after the sub byte transformation is completed.

Questions?

Resources

- www.opencores.com
- www.nist.gov
- www.altera.com
- www.xilinx.com
- Sandia National Labs Cryptography Course Power Point
- - **The Laws of Cryptography:**
  Advanced Encryption Standard:
  - ***By: Neal R. Wagner***
  - http://www.cs.utsa.edu/~wagner/laws/SBoxes.html
- Java AES Example:
  http://people.eku.edu/styere/Encrypt/JS-AES.html
- Pictures and diagrams courtesy of Google Images

Special Thanks

- Karen Shanklin
- Marty Murphy
- Andrea Walker
- Michael Berg
- Katie Dellaquila