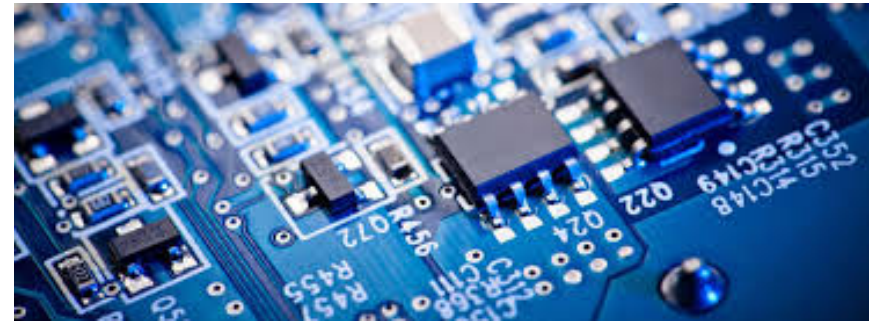
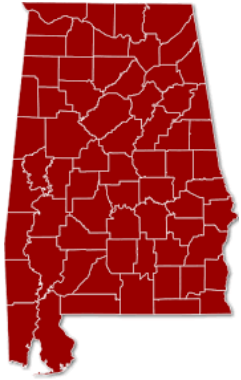


FAU REU Summer Project

BRAXTON MCLEAN

About Me – Braxton McLean



Cryptography

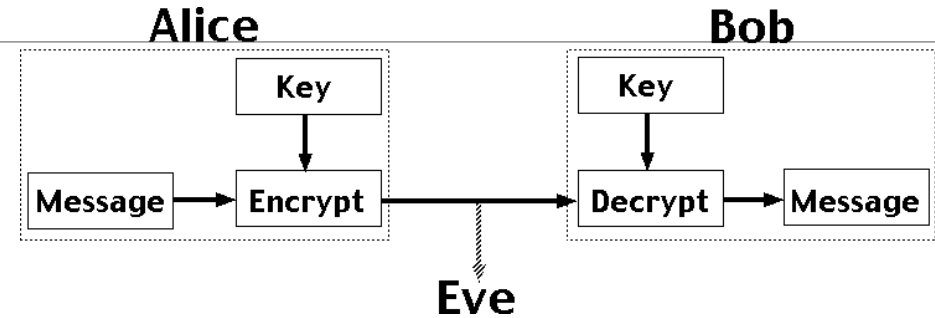
Information or communication secure

“One way math,” i.e. Discrete Logarithm Problem

Current encryption: large, prime integers (RSA, ECC)

Small devices and security

Quantum computers and encryption



```
01110101100011101100011001100111110101100001101111000001101111
0000001001011111000000000000100001011111100011100101110100
01100001110110100110100101000010011001110100011010010101011100
01010011010101110001011101011110101111010001010001011001011011
10011001100010111001000100010110000101011001100000100001011101
1111000101011101101101101101001001000111111111111110010011010
11000101000101101001101001000000010010001000010010011111000110
1101110001111111000001101110010011000001101110001111000001100
00000100001101110001111001010010001010101000111101101011001100
00111110100111001010011010001011010001011000001000110110010011
01100110111010111010011110001111101010011100101101010111000110
11010100110011001001010111100110100111110100100101110101111010
1100001101100100000000100000011001110100100101101011100111000
00101100110011010111100011100100110010111110001010001111001010
1111111011011011011111111111111111110000000110001000100010000
01111001100100010110101001100100100010001111101010010000011011
1101011100000001101010000000100101111100000000000100100101111
001110001011100001010101010100100100010011000101000110010010
10001110111010100001011010010110011011100101010111011001111111
```

Post-Quantum Cryptography and IoT

Public-key encryption vulnerable

Quantum resistant encryption = “Post-Quantum Cryptography”

New methods, same premise

Search for usability, efficiency, and scalability

IoT security - Incredibly dependent

Device resources are limited

My Work - Multiplier Design in VHDL

Exponentiation – large portion of the work in cryptographic schemes

Multiplier efficiency – small improvements lead to great efficiency gain

Task: multiplier implementation and improvements

First steps – Theory, math, research papers

Following – VHDL and circuitry design

Final – Available improvements