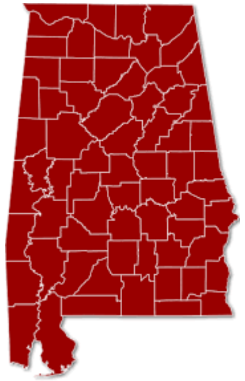
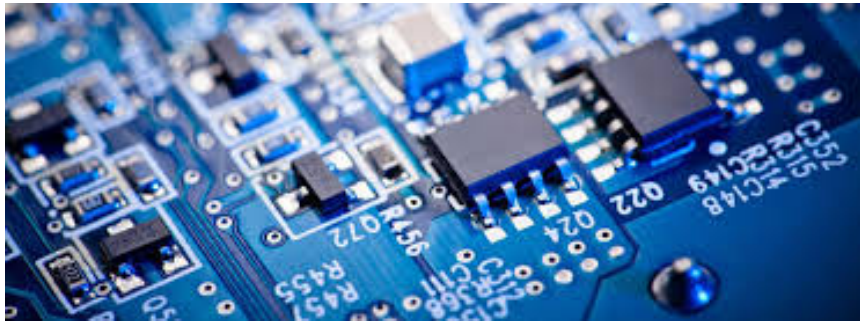
FAU REU Summer Project

BRAXTON MCLEAN

About Me – Braxton McLean





Georgia State University | COLLEGE OF ARTS & SCIENCES

GEORGIA STATE UNIVERSITY GSURC UNDERGRADUATE RESEARCH CONFERENCE

FAU™ I-SENSE Division of Research Florida Atlantic University

Cryptography

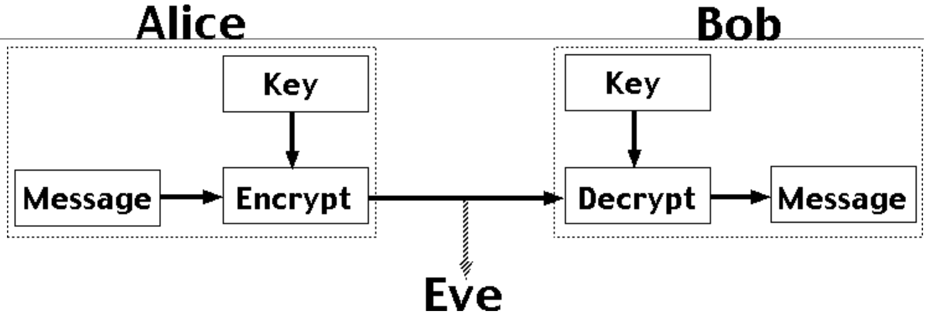
Information or communication secure

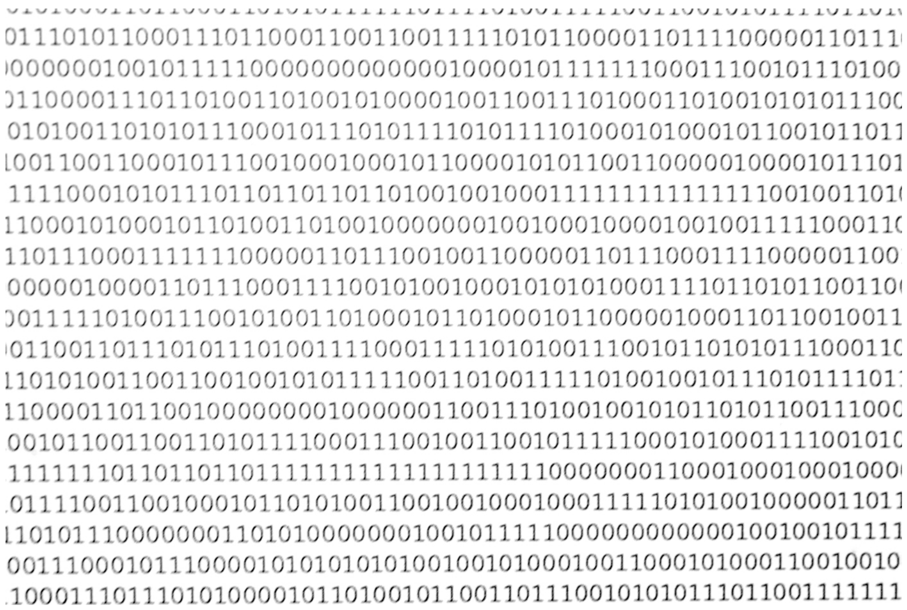
“One way math,” i.e. Discrete Logarithm Problem

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

Small devices and security

Quantum computers and encryption





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 circuity design

Final – Available improvements