VLSI Design and Implementation of PQC Algorithm

UG SEMINAR

Department of Electrical Engineering

MENTORED BY

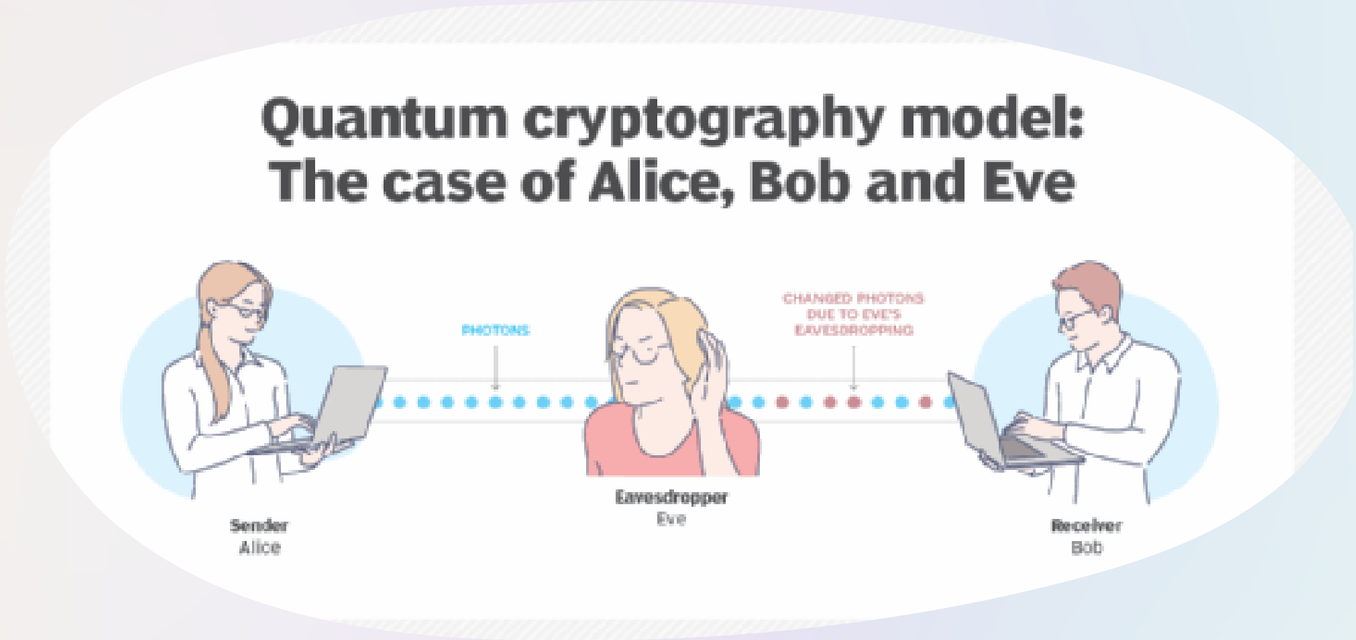
ROHIT B. CHAURASIYA

PRESENTED BY

Y.Ram Narayana Reddy
(2021UEE0161)

Agenda

1	Objective of Study
2	Problem Statement
3	Algorithm Selection and Success Criteria
4	Design of Hardware Model
5	RTL to GDS Flow
6	Conclusion
7	References and Discussion



Objective of the Study

Cryptography has evolved to combat emerging threats. Traditional methods rely on math, while quantum cryptography offers unbreakable security using principles like entanglement. Post-quantum crypto addresses vulnerabilities to quantum computing attacks, ensuring security in this era. Quantum crypto provides unconditional security based on physics, while post-quantum adapts to quantum advancements.

Back to Agenda

Problem Statement

Scope of the study

Explain the parameters of your study here.

Relevance of the study

Explain the impacts of your study here.

Research Questions

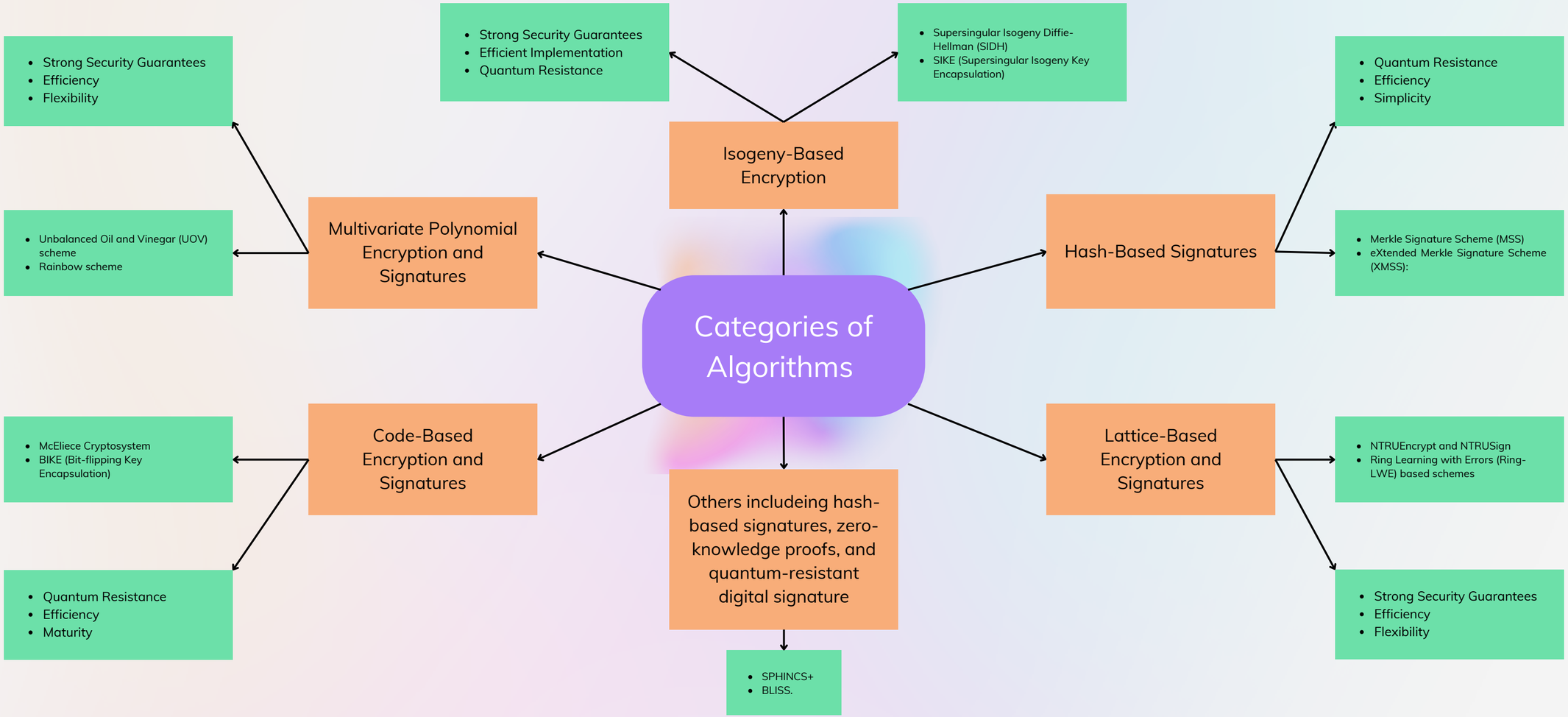
List the research questions relevant to your problem.

Key Parameters

Key Parameters	
• Security Guarantees	• Performance Characteristics
• Suitability for Cryptographic Primitives	• Standardization Potential

Back to Agenda

Algorithm Selection



Algorithm Selection

Success Criteria
• **Security:** Robust protection against cryptographic attacks, including those from quantum adversaries, based on strong mathematical principles. • **Performance:** Efficient cryptographic operations for practical deployment without excessive computational overhead or latency. • **Area Efficiency:** Optimized resource utilization, minimizing hardware or software requirements for implementation. • **Power Efficiency:** Reduced power consumption, particularly crucial for energy-constrained environments or battery-powered devices. • **Toolchain Compatibility:** Seamless integration with Electronic Design Automation (EDA) tools for efficient implementation and manufacturing processes.

Back to Problem Statement

NIST 2022 Finalists

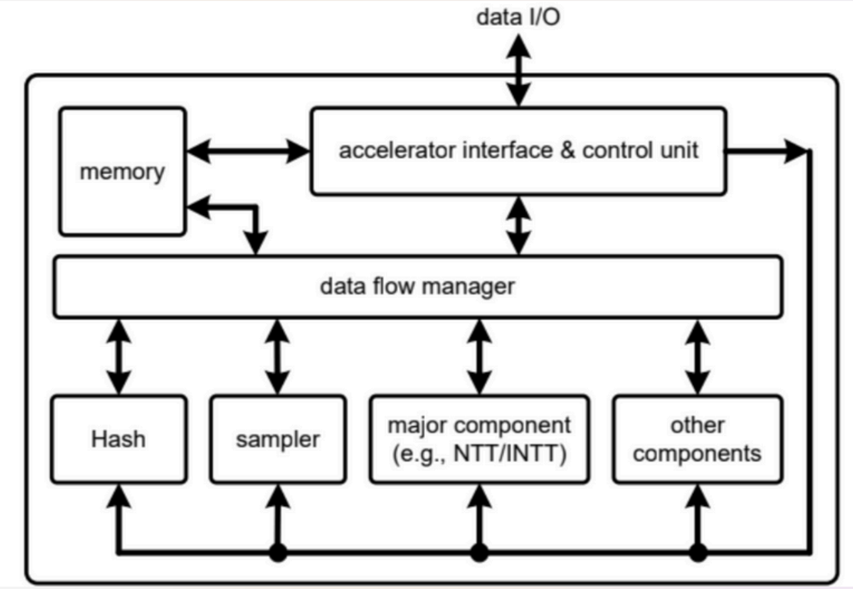
Crystals KYBER is a lattice-based algorithm for robust security against quantum adversaries, offering efficient encryption and key establishment. Finalist in NIST's Post-Quantum Cryptography Standardization project, it's flexible for various security needs.

Crystals DILITHIUM is a lattice-based digital signature algorithm ensuring robust security, chosen as a finalist by NIST. Efficient and scalable, it seamlessly integrates into existing cryptographic systems.

FALCON is a lattice-based digital signature algorithm providing robust security and efficiency. Selected as a finalist by NIST, it offers flexibility and seamless integration into cryptographic infrastructures.

SPHINCS+ is a hash-based algorithm for digital signatures, resistant to quantum adversaries. Recognized for efficiency and suitability for post-quantum cryptography, it's a contender for standardization.

Digital VLSI Architecture Design for PQC Accelerator



PQC hardware accelerator's system-level design efforts are not trivial even all the required components are well-designed.
In general, hardware PQC's system-level design needs to take care of multiple aspects including memory setup, data flow management, performance, resource-oriented specific design, etc.

Using this General Architecture of PQC acclerator we will focussing on particular block to optimize the Algorithm

ASIC Chip Design (RTL to GDS-II)

RTL to GDS flow, also known as Register Transfer Level (RTL) to Graphic Data System (GDS) flow, is a process in integrated circuit (IC) design that involves translating a digital design description written in RTL code (such as Verilog or VHDL) into a physical layout represented in GDSII format. Here's a brief overview of the steps involved in the RTL to GDS flow

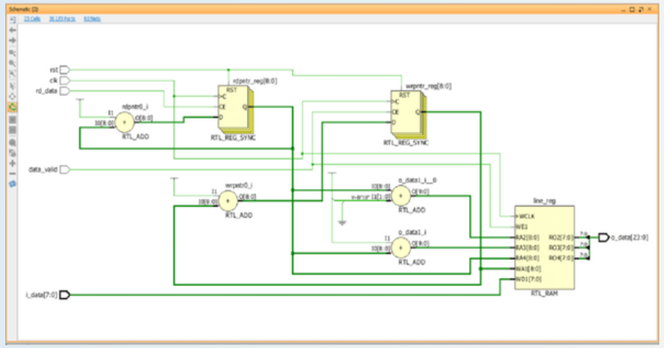
Back to Agenda

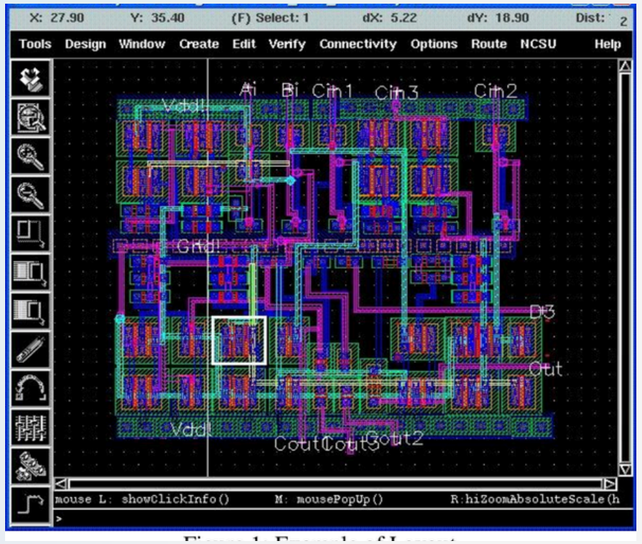
RTL Design

Function Verification

Synthesis And Optimization

Floor Planning





ASIC Chip Design (RTL to GDS-II)

Overall, the RTL to GDS flow involves a series of steps to translate a digital design from its functional description in RTL code to a physical layout represented in GDSII format, ready for semiconductor fabrication. Each step in the flow requires careful consideration and optimization to ensure that the final design meets the desired performance, area, power, and manufacturability requirements.

Back to Agenda

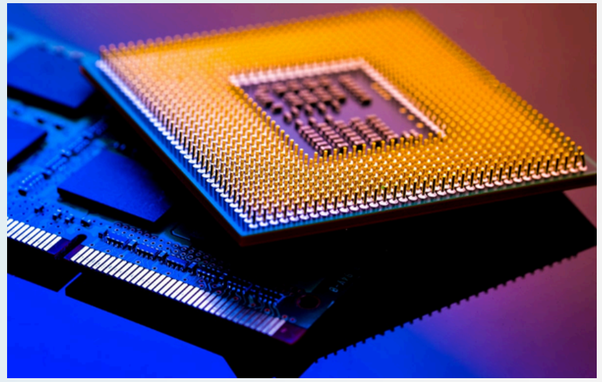
Placement &Routing

CTS(Clock Tree Synthesis)

Physical Verification

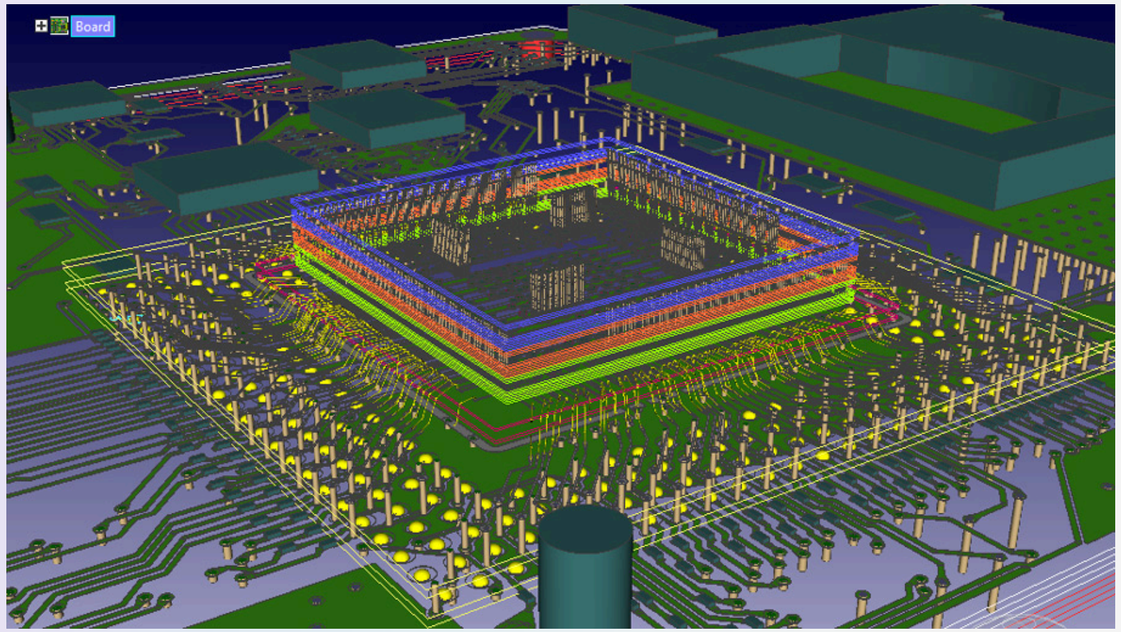
Design for Manufacturing (DFM)

GDSII Generation



Conclusion

- We will focus on Component level designing, which can be optimized from the PQC architecture.
- We will perform the required operations and mathematics to find the relation that holds good to perform.
- After obtaining the best module design, we will start designing our module using Verilog to perform testing and validation on it.
- After Designing the module, we will start the complete RTL to GDS generation for the chip designing.



References

Add more text

1. Jiafeng Xie, Wenfeng Zhao, Hanho Lee, Debapriya Basu Roy and Xinmiao Zhang “Hardware Circuits and Systems Design for Post-Quantum Cryptography – A Tutorial Brief”-Research Paper
2. Jiafeng Xie, Kanad Basu, Kris Gaj, Ujjwal Guin “The Recent Advance in Hardware Implementation of Post-Quantum Cryptography” -Research Paper
3. Daniel J. Bernstein, Johannes Buchmann Erik Dahmen “Post Quantum Cryptography”-Book
4. Some Required websites etc

THANK YOU

It is a simple feat of scientific electrical engineering – only expensive – blind, faint-hearted, doubting world.-Tesla