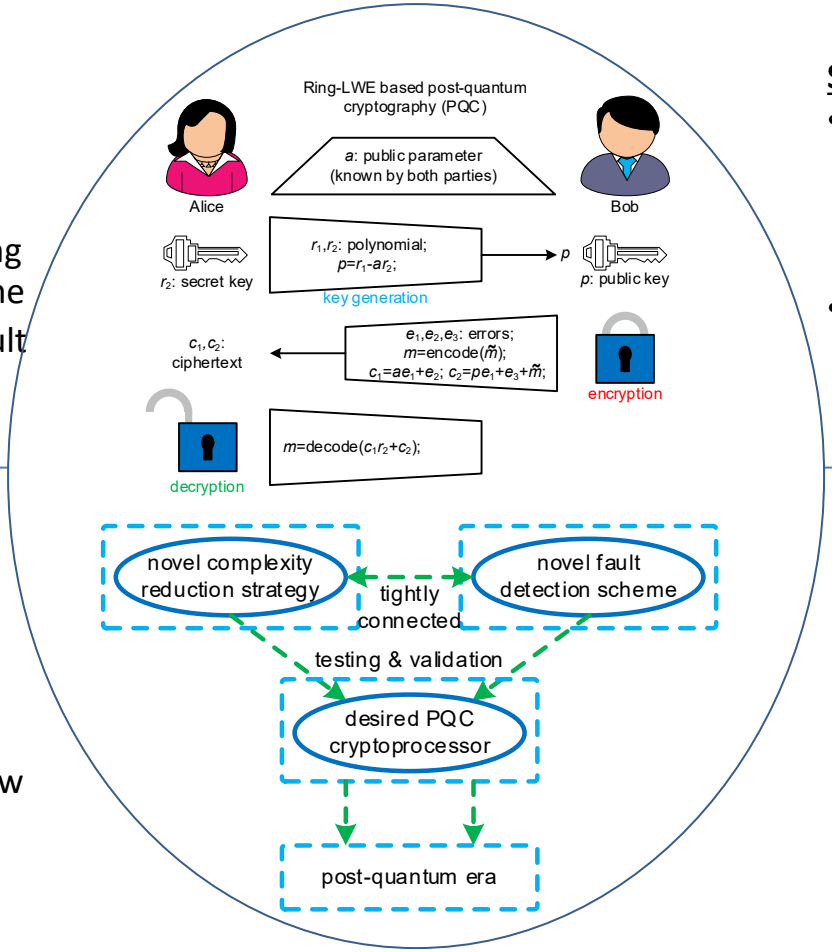
SaTC: CORE: Small: Fast Algorithm Originated Fault Detection Scheme for Ring-LWE based Cryptographic Hardware

Challenge:

- How to reduce the complexity overhead brought by the equipping of fault detection scheme
- How to develop new fault detection scheme for Ring-LWE based PQC



Solution:

- Propose novel fast algorithm to reduce the complexity of the fault detection scheme
- Develop complexity reduction originated new fault detection scheme

NSF Award SaTC 2020625

PI: Jiafeng Xie (Villanova University)
Contact: jiafeng.xie@villanova.edu

Scientific Impact:

- First attempt to develop novel fast algorithm to reduce the overhead for fault detection module of Ring-LWE based PQC
- Inspire the hardware security society to explore new countermeasures for PQC implementation

Broader Impact and Broader Participation:

- Provide significant impacts on PQC security technology advancement
- Facilitate PQC standardization process
- Independent study and undergraduate
- SIGDA Electronic Newsletter “What is” Column
- Course module