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

PI: Jiafeng Xie; Dept. Electrical and Computer Engineering, Villanova University

https://www.ece.villanova.edu/~jxie02/lab/

This project aims to deliver a breakthrough in the novel fast algorithm originated fault detection scheme for Ring-LWE based post-quantum cryptography (PQC). The research goal is to develop low-complexity hardware Ring-LWE based PQC equipped with novel fault detection scheme, with the purpose of becoming new cryptosystem implementation standard.

So far, we have conducted successful research to design low-complexity Ring-LWE based PQC, and the developing of fault detection scheme for targeted PQC is ongoing.

Major Challenges and Significance:

- Challenge-I: How to develop novel strategy to reduce the potential complexity overhead brought by the equipping of fault detection scheme
- Challenge-II: How to develop novel fault detection scheme to achieve high detection capability
- Significance: Ring-LWE based cryptoprocessor with low-complexity and high fault detection is critical for practical applications

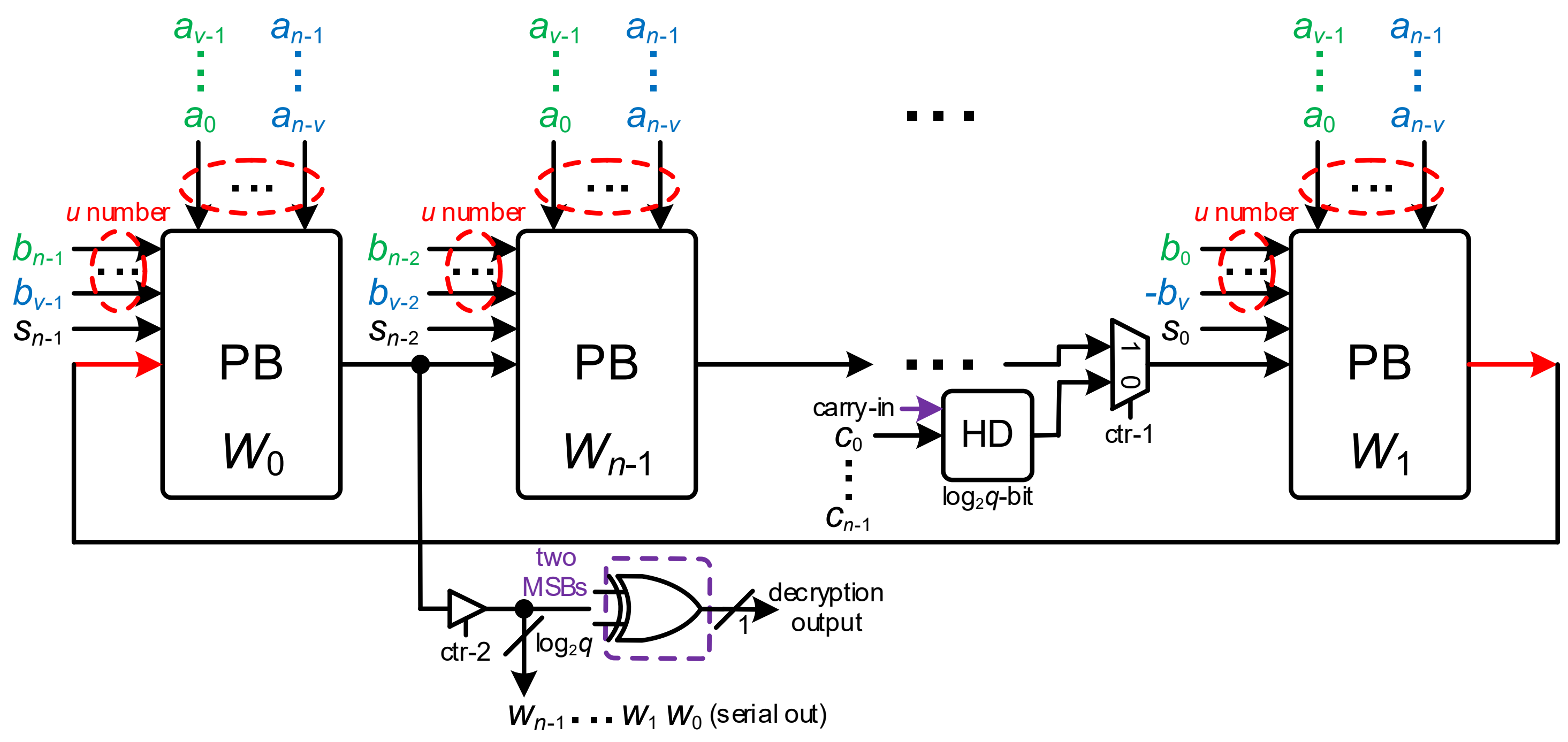
Scientific Impact:

- First attempt to develop novel fast algorithm to reduce the overhead of the fault detection module, which will inspire the cryptographic community to design efficient cryptosystem on hardware
- Fault detection originated Ring-LWE based cryptoprocessor, which will revolutionize the hardware security society to explore new countermeasures for cryptosystem implementation

Technical Approach:

- Propose novel fast algorithm to reduce the complexity of the fault detection module as well as the Ring-LWE based PQC scheme
- Design complexity reduction strategy based novel fault detection scheme for the Ring-LWE based cryptographic hardware

- **Key Innovation (e.g., accepted in IEEE TETC):**



Broader Impact (society):

- Provide significant impacts on national PQC security science and technology advancement
- Bring significant impact on the development of Ring-LWE based PQC
- Facilitate the PQC standardization process

Broader Impact (education):

- Offer independent study options for students
- Develop PQC related course modules
- Involve undergraduate students on PQC related research
- SIGDA Electronic Newsletter "What is"

Broader Impact and Broader Participation:

- One undergraduate female student for summer internship
- A group of five undergraduate students (one female) for lightweight Ring-LWE based PQC project

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2022 SaTC PI Meeting)
June 1-2, 2022 | Arlington, Virginia