SaTC: CORE: Small: Formal Verification Techniques For Microprocessor Security Vulnerabilities and Trojans

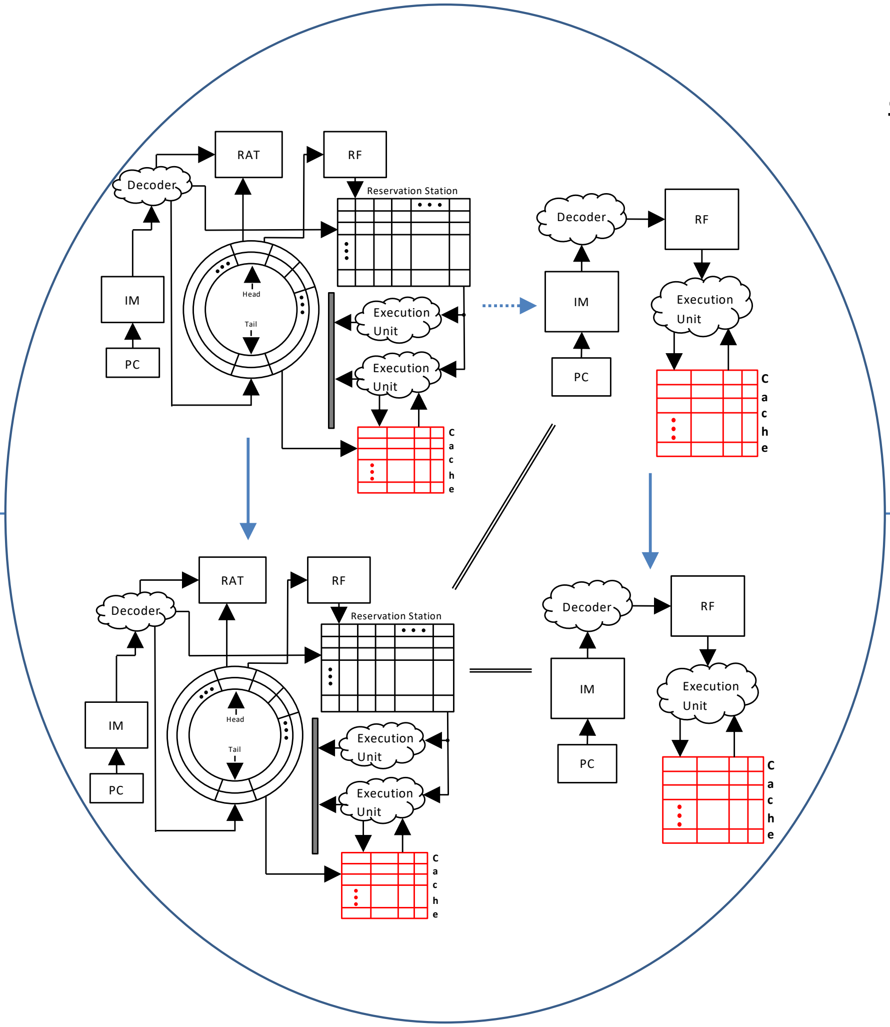
Challenge:

- Invulnerability verification for processor microarchitecture design against Spectre, Meltdown, and other transient execution attacks
- Without invulnerability guarantees, bugs and trojans can be exploited to circumvent mitigations

Solution:

- Refinement-based formal verification
- Key Idea: Expose microarchitecture attack instrument to architecture in refinement verification

Award No: 2117190
Institution: North Dakota State University
PI: Sudarshan Srinivasan



Scientific Impact:

- Project will transition 30 years of formal techniques for microprocessor design correctness to security invulnerability verification
- A set of formal properties will be developed that will enhance understanding of the microarchitecture design behaviors that need to be thwarted to prevent these attacks

Broader Impact and Broader Participation:

- Microprocessors are used pervasively in society and their security has become fundamental to keeping societal systems functioning
- Defense against cyberwarfare
- Recruitment and Retention of Native American Students of ND to ECE at NDSU
- Summer Course for Native American Students