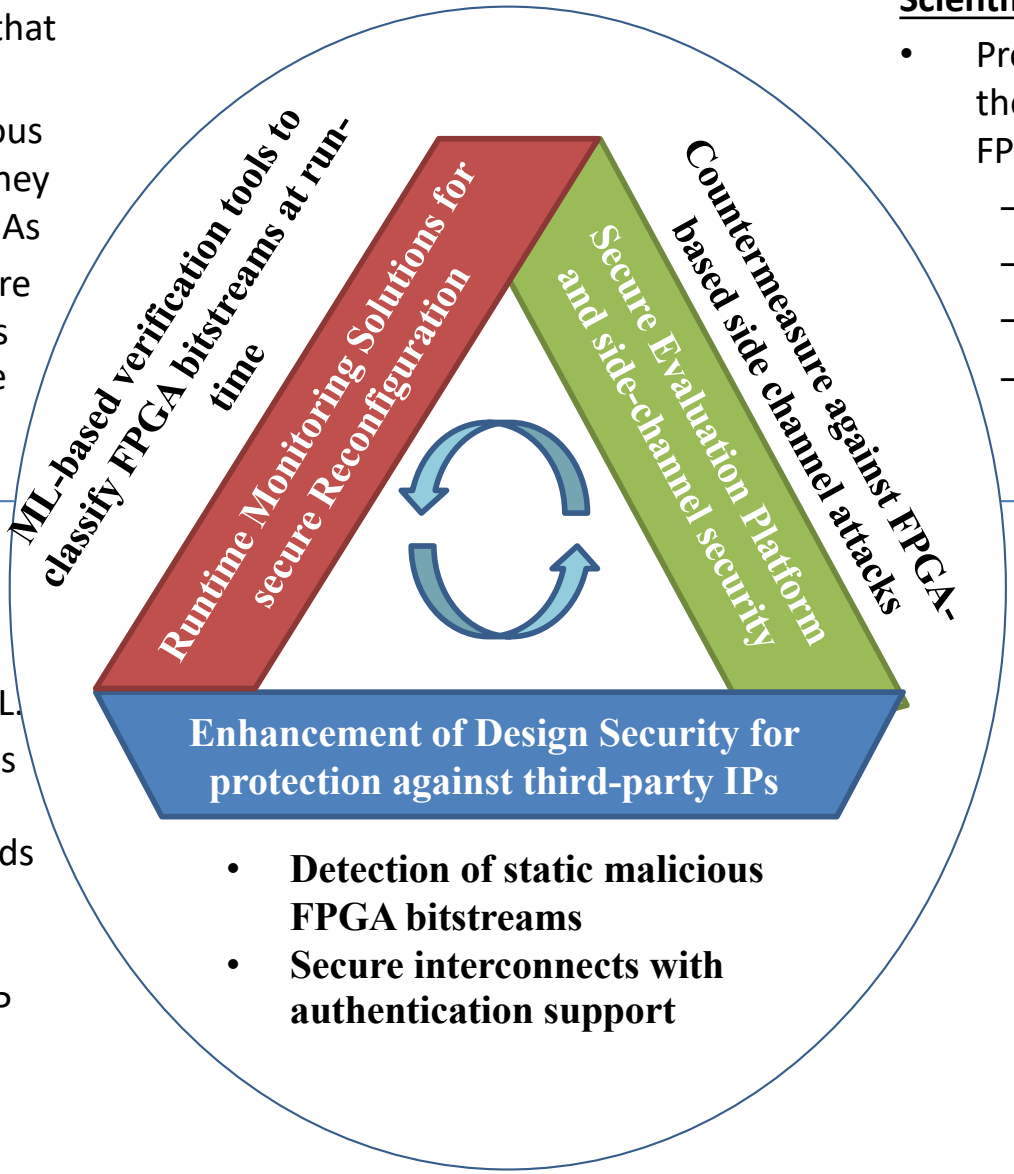
# Security of FPGA-as-a-Service Reconfigurable Systems
# Award #2011561

**Challenge:**

- Study of security threats that target FPGA-as-a-Service
- Static detection of malicious FPGA bitstreams before they are used to configure FPGAs
- Countermeasures to secure SoCs against untrusted IPs that launch attacks on the trusted IPs

**Solution:**

- Static analysis and detection of malicious FPGA bitstreams using ML.
- Detect potential malicious attacks on FPGA using feature extraction methods
- Dynamic cryptographic authentication and obfuscation support for IP security.




**Scientific Impact:**

- Proposed framework supports the following in context of FPGA-as-a-Service:
  - Vulnerability assessment
  - Attack Modeling
  - Prediction and Detection
  - IP Protection

**Broader Impact and Broader Participation:**

- Research relevant to national cyber security
- Collaboration with industry (Intel, IBM, AMD), technology transfers and two patents
- Outreach among broader scientific community through workshops at MEST, SRC, etc.
- Supporting female PhD student