CRII: SaTC: Award #1800088: Automated Proof Generation and Verification for Attribute-based Cryptography

- Proposed methods to automate proofs of well-known signature schemes: Boneh-Boyen strong and weak signatures, and Boneh Boyen Shacham group signatures, in the standard model
- Extended tool – AutoGnP to support EUF-CMA for signature security
- Extended AutoGnP supports rich set of data structures: monotone access structures, pairing-based assumptions, and other building blocks
- Also investigated blockchain-based applications
- Broader impact: Women’s groups at NMSU (NCWIT, YWiC), and CAHSI initiative