CRII: SaTC: Automated Proof Construction and Verification for Attribute-based Cryptography

SUNY Polytechnic Institute

Challenge:

- Building cryptographic proofs complex and error-prone process
- More so for advanced areas of cryptography such as pairing-based cryptosystems
- Would be nice to partially or fully automate the process…

All use Cryptographic Constructs/Protocols

Need strong security guarantees!

- Standard Assumptions, e.g, factoring, discrete log
- PKE schemes, RSA, ElGamal, DH, etc.
- We know how to automate proofs of *some* of these

- Non-standard assumptions, e.g., pairings in bilinear groups
- Attribute-based cryptography
- No automation for proofs up until now. Seek to fill this gap.

cientific Impact:

Project will help build proof assistants for a new, upcoming area of cryptography: attribute-based cryptosystems

- Will provide a foundation for building proof assistants for similar areas, e.g. Non-interactive zero knowledge proofs, identity based cryptosystems, etc.

Solution:

- Extend existing proof assistants with support for *attribute-based cryptosystems*
- Our Contributions: Build libraries of commonly-used abstractions, strategies, and tactics for pairing-based cryptography and attribute-based cryptosystems

Broader Impact:

- Will make life easier for cryptographers, designers of crypto protocols
- Edu. Goals: Creation of course on pairing-based crypto, and proof automation tools

Award # 1566297, SUNY Polytechnic.
PI: Roopa Vishwanathan
vishwar@sunyit.edu