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

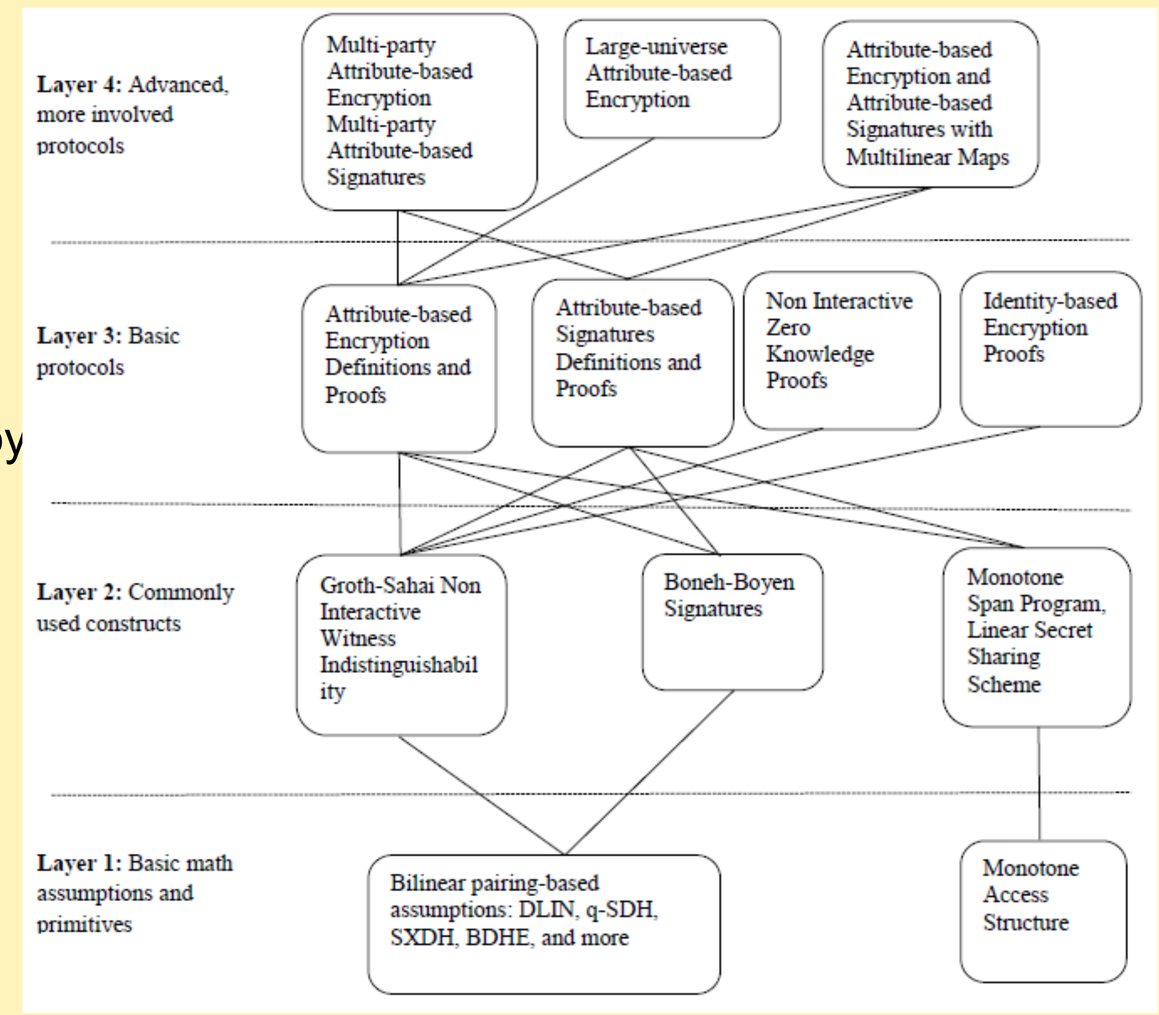
PIs: Roopa Vishwanathan. SUNY Polytechnic, vishwar@sunyit.edu

Objective

Proofs of crypto protocols complex and involved. A proof-assistant would be a handy tool!

Our Objective: Build a proof assistant for helping with constructing proofs of a well-defined family of cryptosystems: attribute-based cryptography.

Figure shows activities organized by hierarchical layers



Approach

- Start with existing proof-assistants, see if we can extend their capabilities to attribute-based cryptography
- Build libraries of tactics, algebraic manipulations, strategies, and common abstractions
- Build a tool that can eventually be used across various families of cryptosystems that are based on pairing-based assumptions

Progress so Far

- Looked at various proof assistants: CryptoVerif, CertiCrypt, EasyCrypt, etc.
- Picked one – *AutoGnP*, which is designed only for pairing-based crypto

Progress so Far

- Coded up basic math assumptions in AutoGnP
- Coded up proofs of Boneh-Boyen pairing-based signature scheme in AutoGnP

Next Steps

- Use our signature proofs to construct proof of an attribute-based *signature* scheme
- Next, look at attribute-based *encryption* proofs

Stretch Goals

- So far, focused only on bilinear pairings, extend into multilinear or k-linear pairings
- Look at asymmetric parings, instead of just simple symmetric pairings

Interested in meeting the PIs? Attach post-it note below!