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

Pls: 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.

Multi-party Large-universe Attribute-based Attribute-based Attribute-based Encryption and Layer 4: Advanced, Encryption Encryption Attribute-based more involved Multi-party Signatures with protocols Attribute-based Multilinear Maps Signatures Non Interactive Identity-based Attribute-based Attribute-based Encryption Signatures Layer 3: Basic Encryption Knowledge Proofs Definitions and Definitions and protocols Proofs Proofs Proofs Monotone Boneh-Boyen Groth-Sahai Non Layer 2: Commonly Span Program, Signatures Interactive used constructs Linear Secret Witness Sharing Indistinguishabil Scheme Layer 1: Basic math Monotone Bilinear pairing-based assumptions and Access assumptions: DLIN, q-SDH, primitives Structure SXDH, BDHE, and more

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 pairingbased 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!





