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

Cryptography, Security and Privacy Research (CrySPR) Lab, CS Dept., New Mexico State University. https://sites.google.com/view/crysprlabnmsu/home

Roopa Vishwanathan, Dept. Of Computer Science, New Mexico State University

roopav@nmsu.edu

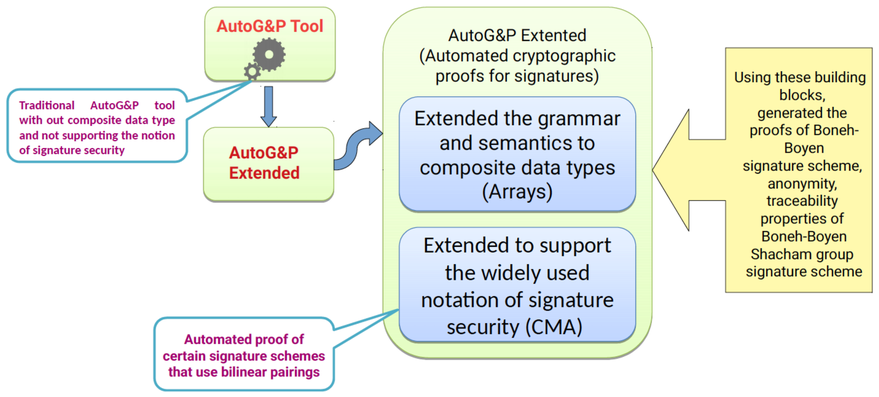
INTRODUCTION

- Cryptographic schemes proven secure in rigorous frameworks
- Security based on computational hardness assumptions, e.g., DDH, CDH, qSDH, DLIN, etc.
- A given scheme proven secure by reducing the hardness of breaking it to one or more assumptions – can be complex, tedious process

Observation: Cryptographic protocols need automated tools to help construct and verify proofs

MOTIVATION

- Not enough work done in area of automating proofs of cryptographic primitives and less so in advanced areas, e.g., pairing-based cryptography (PBC)
- PBC forms the basis of numerous encryption and signature scheme such as IBE, NIZKP, ABE, ABS, and more
- Proofs in **standard model** more desirable (as opposed to random oracle model)
- Automated proofs should produce proofs in well-known frameworks, e.g., IND CPA, IND-CCA2, EUF-CMA, etc.



OBJECTIVES

- To propose libraries of simple transformations, algebraic manipulations, commonly used abstractions and constructs, and proof strategies, to help in generation and verification of proofs in ABE/ABS, in standard model

CONTRIBUTIONS

- We propose methods to automate and construct cryptographic proofs in **standard model** using AutoG&P – a tool first proposed by Barthe et al. [ACM CCS'15]
- Improve scope of AutoG&P by supporting rich set of data types, monotone-access structures and linear secret sharing schemes
- Include support for ABE/ABS and related infrastructure: pairing-based assumptions, signature schemes, other building blocks

WORK SO FAR

- Boneh-Boyen weak signature scheme [Eurocrypt'04]
- Boneh-Boyen strong signature scheme [Eurocrypt'04]
- Boneh-Boyen-Shacham group signature scheme, anonymity [Crypto'04]
- Boneh-Boyen-Shacham group signature scheme, traceability [Crypto'04]
- Lewko et al. ABE scheme [Eurocrypt"10]
- Waters' CPABE scheme [PKC'11]

PUBLICATIONS

- Subramanian, L. M. and Vishwanathan, R. Attribute Based Signatures: The Case for Automation. In Proceedings of the 15th International Conference on Security and Cryptology (SECRYPT) 2018, pp. 703–708.
- Eswaraiah, G., Vishwanathan, R., and Nedza, D. Automated Proofs of Signatures using Bilinear Pairings. In 16th Annual Conference on Privacy, Security and Trust (PST) 2018, pp. 1–10.
- Eswaraiah, G., Subramanian, L.M., and Vishwanathan, R. Exploring Automation in Proofs of Attribute-based Encryption in Standard model. 17th International Conference on Privacy, Security and Trust (PST) 2019.

Research supported by NSF award #1800088

BROADER IMPACT (EDUCATION AND OUTREACH)

- PI introduced 2 new courses at CS@NMSU:
  - CS 479/579: Intro to Cryptography
  - CS 579: Advanced Cryptography
- Both courses well received, enrolment up!
- 2 current PhD students
- 2 MS students (1 graduated)
- 2 undergrads (both graduated)

BROADER IMPACT (QUANTIFY POTENTIAL IMPACT)

- New **BS in Cybersecurity** program in NMSU, crypto courses part of it
- Young Women in Computing (**YWiC**) club at NMSU
- **NCWIT** group at NMSU
- NMSU part of Computing Alliance of Hispanic Serving Institutions (**CAHSI**)