Apr 15th, 1:00 PM - 3:00 PM

Cryptographic accumulators

Ilker Ozcelik
University of Tennessee at Chattanooga

Sai Medury
University of Tennessee at Chattanooga

Justin Broaddus
University of Tennessee at Chattanooga

Recommended Citation

Ozcelik, Ilker; Medury, Sai; and Broaddus, Justin, "Cryptographic accumulators". *ReSEARCH Dialogues Conference proceedings*. https://scholar.utc.edu/research-dialogues/2020/day2_presentations/54.

Cryptographic Accumulators

Ilker Ozcelik, Sai Medury, Justin Broaddus
SimCenter – Center of Excellence in Applied Computational Science and Engineering

Outline

- Motivation & Problem Statement
- Cryptographic Accumulator Definition and Classification
- Cryptographic Accumulator Architectures
- Cryptographic Accumulator Properties - Security
- Cryptographic Accumulator Properties – Optional Features
- Current and Potential Applications
- Q&A

Motivation & Problem Statement

- A cryptographic accumulator is a **space and time efficient** data structure that is used for **set membership tests**
- It is possible to phrase any *computational problem where the answer is yes or no as set membership problem*.
- Common Example: Access Control List in User Account Management
  - **Approach 1**: compare each credential and look for a match
    - Lookup - linear (O(n)) with the size (n) of the list
  - **Approach 2**: compare each credential in the ordered list
    - Lookup - sublinear (O(logn))
    - Sort - could be anywhere between O(nlogn) to O(n2)
    - Memory - (O(n))
  - **Approach 3** - constructing auxiliary data structures like hashmaps.
    - Lookup- Constant
    - Memory - (O(n))
  - **Approach 4 - Cryptographic Accumulators**
    - **Lookup – constant**
    - **Memory – constant***

Cryptographic Accumulator Classification

- Asymmetric Cryptographic Accumulator
  - **Requires a witness** creation and update for dynamic verification of set membership
  - Built on asymmetric cryptographic primitives
  - Require the underlying hash algorithm to exhibit the quasi-commutative property
    - Generalization of the commutative property
    - h(h(x,y1),y2) = h(h(x,y2),y1)

- Symmetric Cryptographic Accumulator
  - **Does not require a witness** for verification
  - Built on symmetric cryptographic primitives
  - Underlying hash algorithm <u>does not</u> exhibit the quasi-commutative property
  - Provides a limited representation of set-membership with a **false positive rate**

Cryptographic Accumulator Architectures

- One-way Accumulators (Benaloh and de Mare)
  - A family of one-way hash functions with the additional quasi-commutative property
  - One-way hash function (H)
    - accept an arbitrarily large message (M)
    - returns a constant size output called a message digest (MD)

- Collision-Free Accumulators (Barić and Pfitzmann)
  - More general constructs that are defined as a 4-tuple of polynomial time algorithms
    - Generate
    - Evaluation
    - Witness Extraction
    - Verification

- One-way Accumulators (**Implemented**) / Collision-Free Accumulators (**Theoretical**)

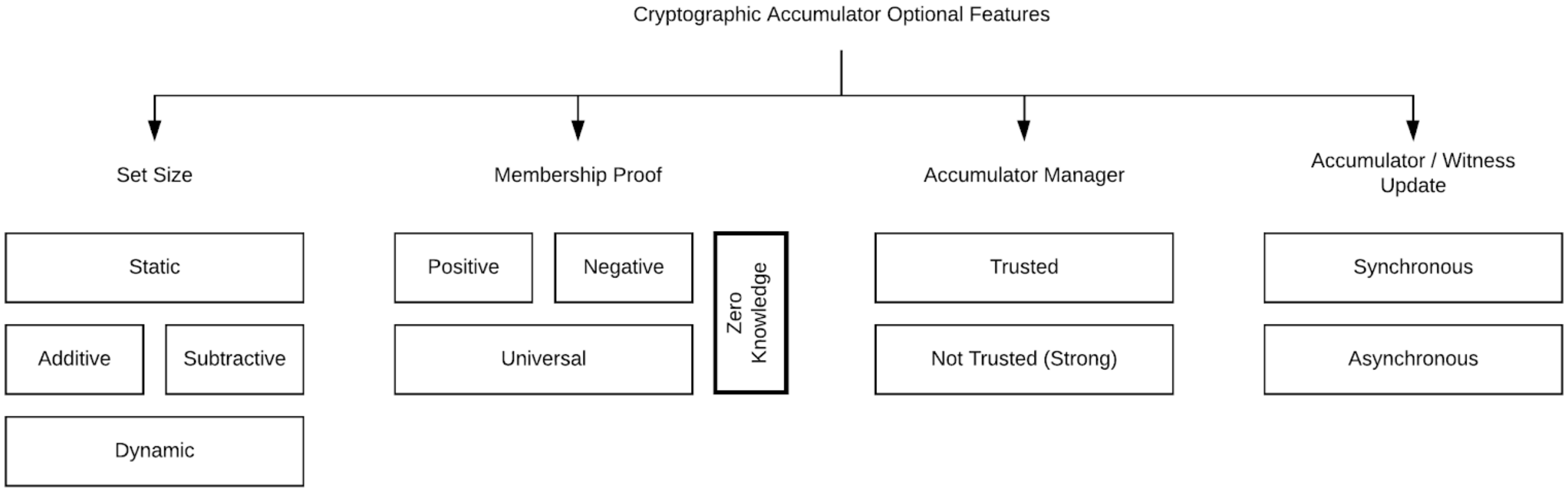
Cryptographic Accumulator Properties (Security)

- Soundness (Collision-Freenes)
    - **Cannot generate** membership/*non-membership* witnesses for non-set members/*set members*
- Completeness
    - **Should be able to prove membership** by using accumulator and witness value
- Undeniability
    - **Cannot generate** membership and non-membership witness for the same element **at the same time**
- Indistinguishability
    - Privacy related property
    - Neither the accumulator nor the witness **leak information** about the accumulated set

Cryptographic Accumulator Properties (Optional Features)

- Input Set Size Change
- Membership Proof

- Accumulator Manager Trust
- Accumulator / Witness Update



Current and Potential Applications

- Known & Potential Areas
  - Time Stamping and Membership testing.
  - Privacy and anonymity-conscious applications/data sharing
  - Authentication systems
  - Revocation Lists
- Applications
  - In Cryptocurrency
    - Bitcoin – Bloom Filter for set membership testing of transactions
    - Bitcoin – Merkle Block to confirm validity of transactions
    - Zerocoin – CL-RSA-B based accumulator for privacy preserving cryptocurrency operations
  - In Industry (Potential)
    - Any access-controlled systems
    - Finance
    - Smart and autonomous systems

Ilker Ozcelik, PhD

SimCenter

ilker-ozcelik@utc.edu

ozcelikilker@ieee.org

Sai Medury, PhD Candidate

SimCenter

Sai-medury@utc.edu

Justin Broaddus

SimCenter

dzt972@mocs.utc.edu