Merkle Tree based Mobile Remote Storage

Capstone Project by Anzhe Zu (azu)
Advisor: Bernardo Palazzi
Problem

- Mobile Phones are used extensively
- Portable, Mobile
- LIMITED computation power, storage
Demand

• People have a lot of files — documents, music, photos, movies, etc.

• People want their files available by hand all the time
Trivial Solution

- 4G, LTE technology
- Dump the files to a server, and retrieve them when needed
• Security concern

• Verification of retrieved files
Verification

- Hash?
- Merkle Tree
My Project

- Phone — Upload/Retrieve
- Server — Storage

Merkle Tree Verification
Merkle Hash Tree

- Balanced binary tree defining a hierarchical hashing scheme.
- Root hash is a hierarchical digest of the entire set.
Proof of Membership

- Path from the item to the root hash + hashes of the sibling nodes
- Example: block 2
- (Hash 0-0, Left), (Hash 1, right)
Advantage

- Client need root hash only, $O(1)$
- Verification takes $\log(n)$, $n$ is # of files despite the file size
Modern Usage

- Proof of absence
- Prove $x_{7.5}$ does not exist
- Provide $x_6$ & $x_8$, and the proof of them
Industry Use Cases

• Version Control — Git
• Secure File Synchronization — FileRock
• Transaction History — Bitcoin Protocol
• Streaming Data — Netflix
Demo

• Server: django w/ mysql on heroku
• Client: iOS