09.11.2021

CMSE353 Fall 2021

Lab 2. Implementation of Merkle hash tree

Due date : Lab 2 period: 11.11.2021-16.12.2021 Gr2, reporting on 16.12.2021; 15.11.2021-20.12.2021 Gr1, reporting on 20.12.2021

Merkle hash tree is used in block-chain technology. This laboratory supports Term project on block-chain technolgy.

Task:

1. Implement Merkle hash tree [1] as an application taking as input variable number of records, and outputting a Merkle hash tree (see Fig. 1 built according to (1), (2) from [1]).
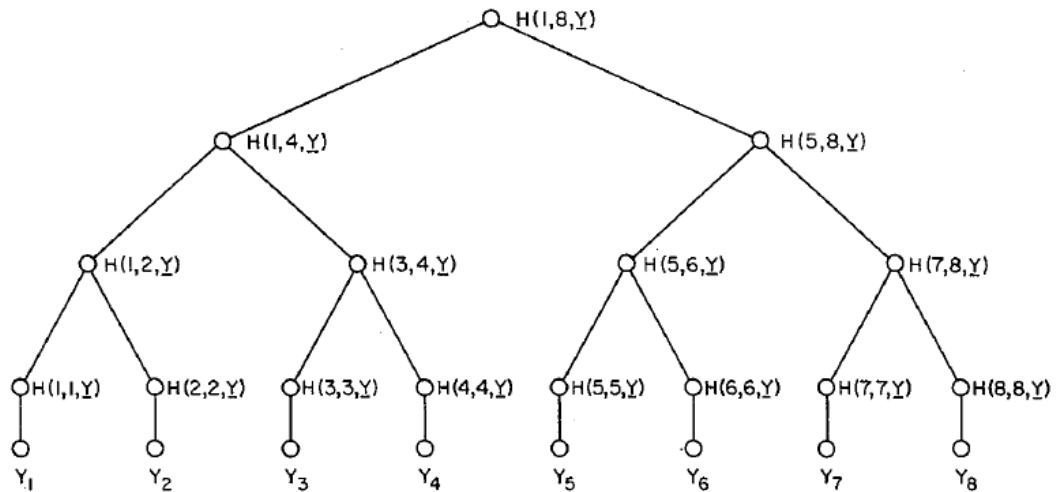

Fig. 1. Merkle hash tree [1]

2. Any hash function can be used, borrowed or implemented yourself.
3. Any programming tools can be used.
4. Conduct tests with your application to validate its correctness
5. Prepare (in Word) a **report** on your assignment having:
   - ☐ Cover page
   - ☐ outline,
   - ☐ problem definition,
   - ☐ description of your team work (meetings, discussions, work break down, team members' responsibilities)
   - ☐ description of the data structures and algorithms for solving your problem,
   - ☐ description of tools you used for implementation of your problem and the details of their installation and preparation for usage
   - ☐ description of the developed program (parts of the program, ways of interaction, synchronization, etc.)
   - ☐ user guide (how to use your program – what and where should be installed, launched, how it should be interpreted)
   - ☐ description of conducted tests and their results with screenshots of the runs
   - ☐ conclusion
   - ☐ references on used sources (books, articles, web-sites, etc.)

6. Supply the report as a Winrar file having all the Lab-related materials: doc-file with your report, sources and executables of your application, results of your tests, and instructions how to use your program
7. Copies are not allowed and will deserve 0 points

Grading policy: report – 40%, explanations – 60%

References

1. R.C. Merkle, Method of providing digital signatures, US patent 4,309,569, Jan. 5, 1982,
   https://patentimages.storage.googleapis.com/69/ab/d9/2ff9f94fada6ea/US4309569.pdf