CS554 Homework

Cryptographic Hashing

Instructions:

- *Assigned date: Thursday April 6th, 2023*
- *Due date: 11:59PM on Wednesday April 12th, 2023*
- *Maximum Points: 3*
- *This assignment must be done individually*
- *Please post your questions to BB*
- *Only a softcopy submission is required to BB*
- *No late submission will be allowed on this assignment*

Overview

You are to read the BLAKE3 paper that discusses in detail the BLAKE3 cryptographic hashing algorithm and its performance compared to SHA256 as well as other cryptographic hashing algorithms.

https://github.com/BLAKE3-team/BLAKE3-specs/blob/master/blake3.pdf

Your review must be written in a narrative form, with bullets when appropriate. You are to generate a PDF file and submit it on BB before the deadline. You must do these reviews individually.

Your review should include the following information:

- Reviewer name (that is you)
- Paper title
- Paper authors
- Publication venue (conference, workshop, or journal name)
- Year of publication
- Paper summary (150~300 words); Clearly state the nature of the work (e.g. implementation of a real system, simulation, theoretical, empirical performance evaluation, survey, etc)
- What are the core contributions of this paper (1~3 items)
- How is this work/solution different than related work (<300 words)?
- Pros: Identify 3 things that this paper does well
- Cons: Identify 3 things that this paper could do better
- Identify 1 thing that the author could do that would make the paper better
- Identify 1 thing that someone could pursue as future work (that is not identified in the paper already)

Your review should be 1 to 2 pages long. It is expected that you spend several hours for each paper to read and writeup this review.