Hash Function Collision Searching
Team Mordor

Alex Young & Emmanuel Dodoo

September 24, 2018
Outline

- Introduction
- Computational Problem
- Sequential Algorithm
- Parallel Algorithm
- Conclusion
Merkle-Damgard Construction

MD5

- Takes in any length string text
  - Breaks message into 512-bit blocks
- Hash function outputs 128-bit value
- As of Dec. 2008 the US Government discourages further use of MD5 for cryptographic hashing

Source: https://www.k-ict.org/v4/online-security/md5-hash/

Computational Problem

Investigate & quantify collision time of attack using sequential and parallelized approaches
Sequential Algorithm

```java
while (collision == false) {
    generate input string
    output = MD5 hash (input string)
    check for collision in hashmap
    if (collision == true) {
        print Inputs & output hash
        Exit program
    } else {
        record input & hash output in hashmap
    }
}
```
Parallel Algorithm

while (collision == false)
{
    parallelFor start_idx to end_idx do
        generate input string
        output = MD5 hash (input string)
        check for collision in hashmap
        if (collision found) {
            print Input & output hash
            break
        }
        else {
            record input & hash output in hashmap
        }
}
Conclusion

We believe having a cluster of nodes working in parallel we will be able to find a collision much faster.
THANK YOU

QUESTIONS ?