Andy Getzendanner

ENGR3410: Computer Architecture

PIPELINED SHA256 IN VERILOG

SHA256: A CRYPTOGRAPHIC HASH FUNCTION

- Compresses an arbitrary message to a 256-bit fingerprint
- Impossible to reverse
- Difficult to create a collision
- Confirms data integrity
- Demonstrates knowledge of a password, without keeping the cleartext password
- One of a class of functions useful for passwords, file verification, and more

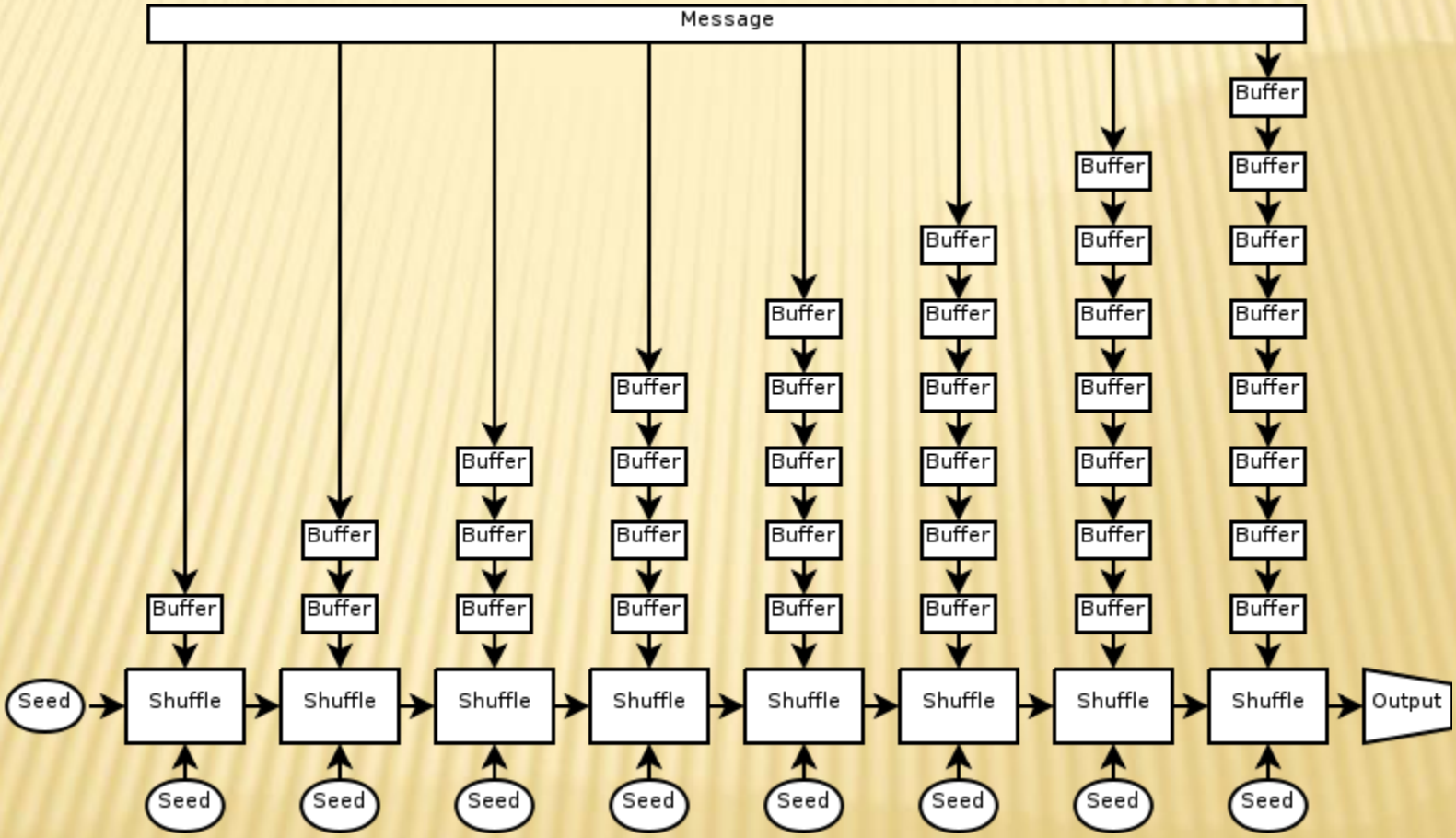
HASHING IN HARDWARE

- Computationally expensive on general-purpose CPUs
- Lots of iterations needed to hash a big file or… crack a password
- ASICs have been used in the past to crack passwords [1]
- Generally, cryptographic accelerators for cracking, SSL, full-disk encryption

PIPELINING SHA256

- 64 iterations of a single shuffle operation applied to mix seed data with message
- Extra shuffler modules can work on additional messages
- If enough messages need to be hashed, scaling in linear with the number of shuffler modules

PIPELINING SHA256



REFERENCE

1. Wikipedia: Custom hardware attack