Hash functions: Properties, an Attack, and an Application

PI: Prof. Qiaoyan Yu of the Electrical and Computer Engineering Department at the University of New Hampshire

Student Researcher: Ranuli Abeysinghe

A ***cryptographic hash function***, *h*, takes an input **message** of arbitrary length and produces as an output a **message digest**, also referred to as a **hash** of fixed length [1].

Key Properties:

- **One-way**: Given a value *y*, it is computationally infeasible to find a value *x* such that *h(x) = y* [2].
- **Preimage resistance:** It must be infeasible to invert a hash or message digest [1].
- **Weak collision resistance**: Given *x* and *h(x)*, it is infeasible to find any *x′*, where *x ≠ x′* and *h(x) = h(x′)* [1, 2].
  - It must be impossible to modify a message without changing its message digest.
- **Strong collision resistance**: It is infeasible to find any *x* and *y* such that *x ≠ y* and *h(x) = h(y)* [2].
  - There are no two inputs that hash to the same output.

SHA-3 (Keccak):

- Keccak-function consists of 24 rounds of 5 sequential steps.
- The output of each round is:

Output = $\iota \circ \chi \circ \pi \circ \rho \circ \theta$(Input), where ι, χ, π, ρ, and θ are sub rounds [3].

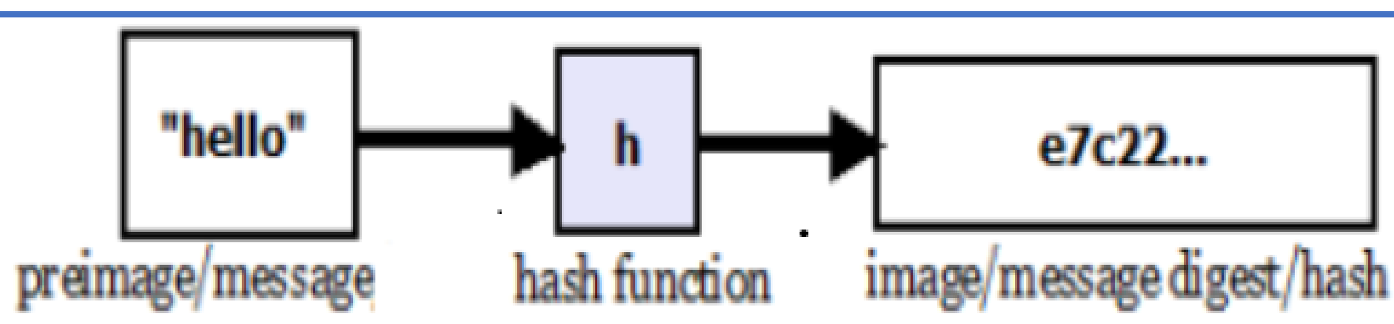


Figure 1. Hash Function Operation

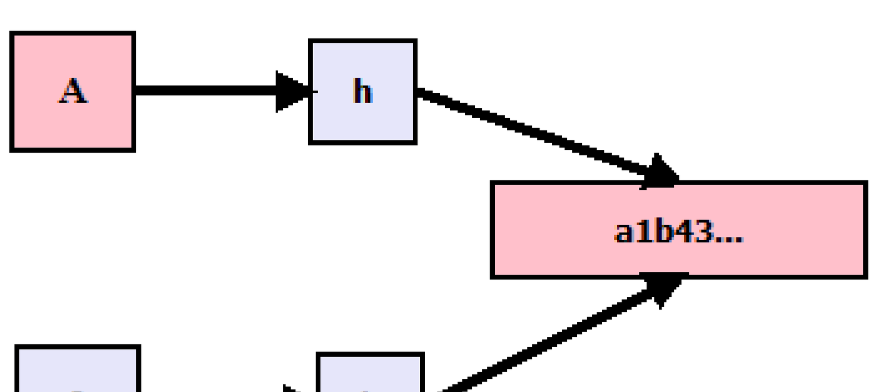
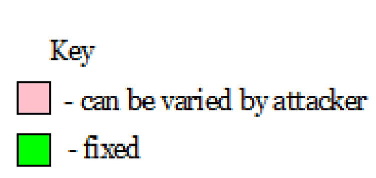


Figure 2. A Preimage Attack



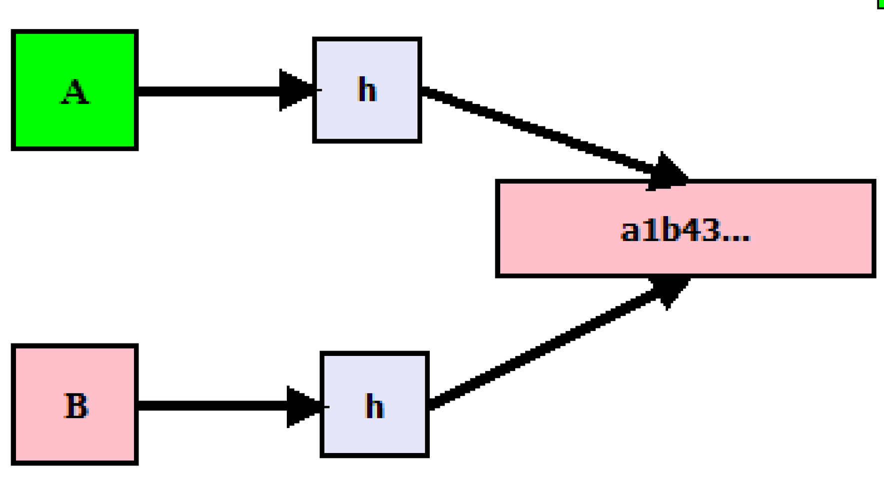


Figure 3. A Second Preimage Attack

Differential Fault Analysis:

- DFA utilizes the dependency of output faults on internal intermediate variables to recover messages, then a limited observable digest is used to recover part of the input of the last round χ operation to launch an attack [5].
- DFA is a powerful and efficient attack method, and has been used to break various cryptographic algorithms [5].

Sponge Construction:

- Sponge construction constructs a function SPONGE[*f, pad, r*].
  - *f* is a fixed-length transformation
  - *pad* is a padding rule
  - *r* is the bitrate
- The process of producing a hash occurs in three steps:
  1. The state bits are initialized to zero.
  2. The *absorbing* phase: The *r-b* input message blocks are XORed into the outer part of the state and treated with *f* [4].
  3. The *squeezing* phase: the outer part of the state is iteratively returned as an output blocks, after being treated by *f* [4].

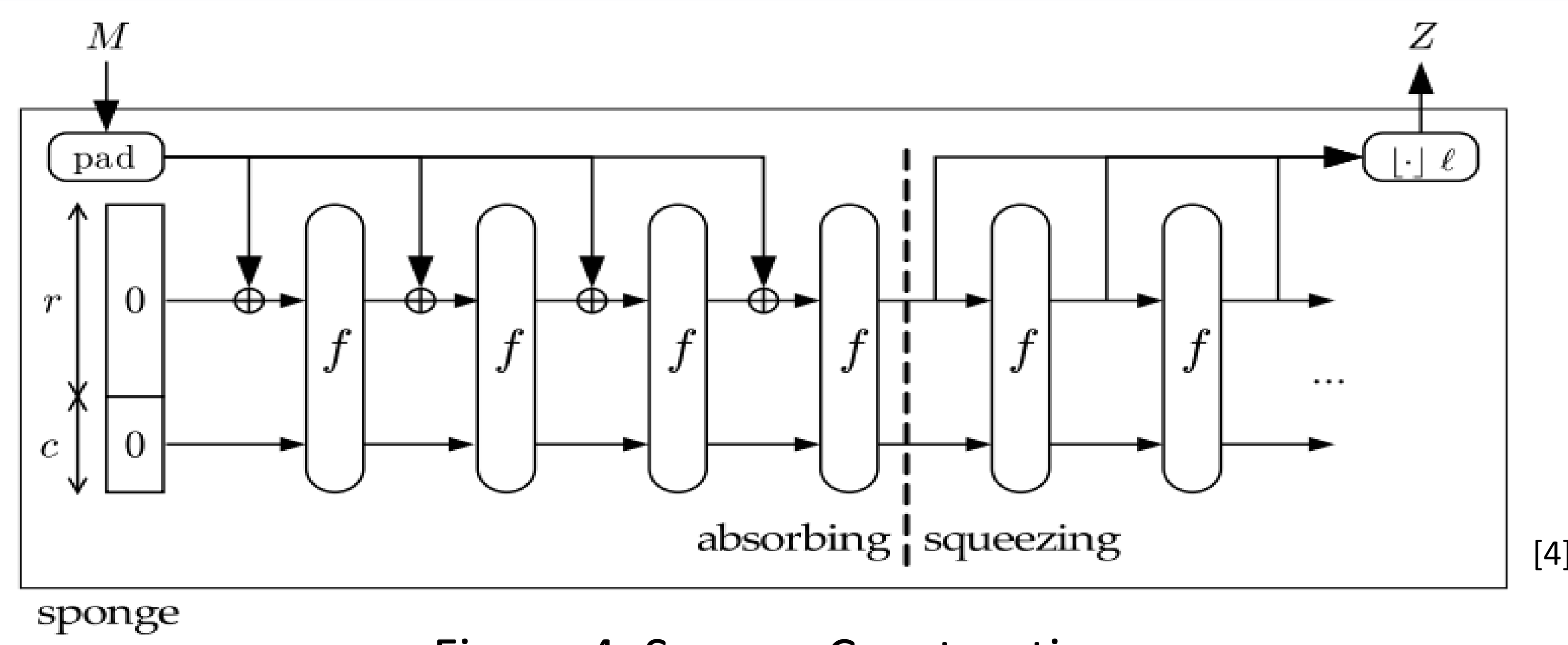


Figure 4. Sponge Construction

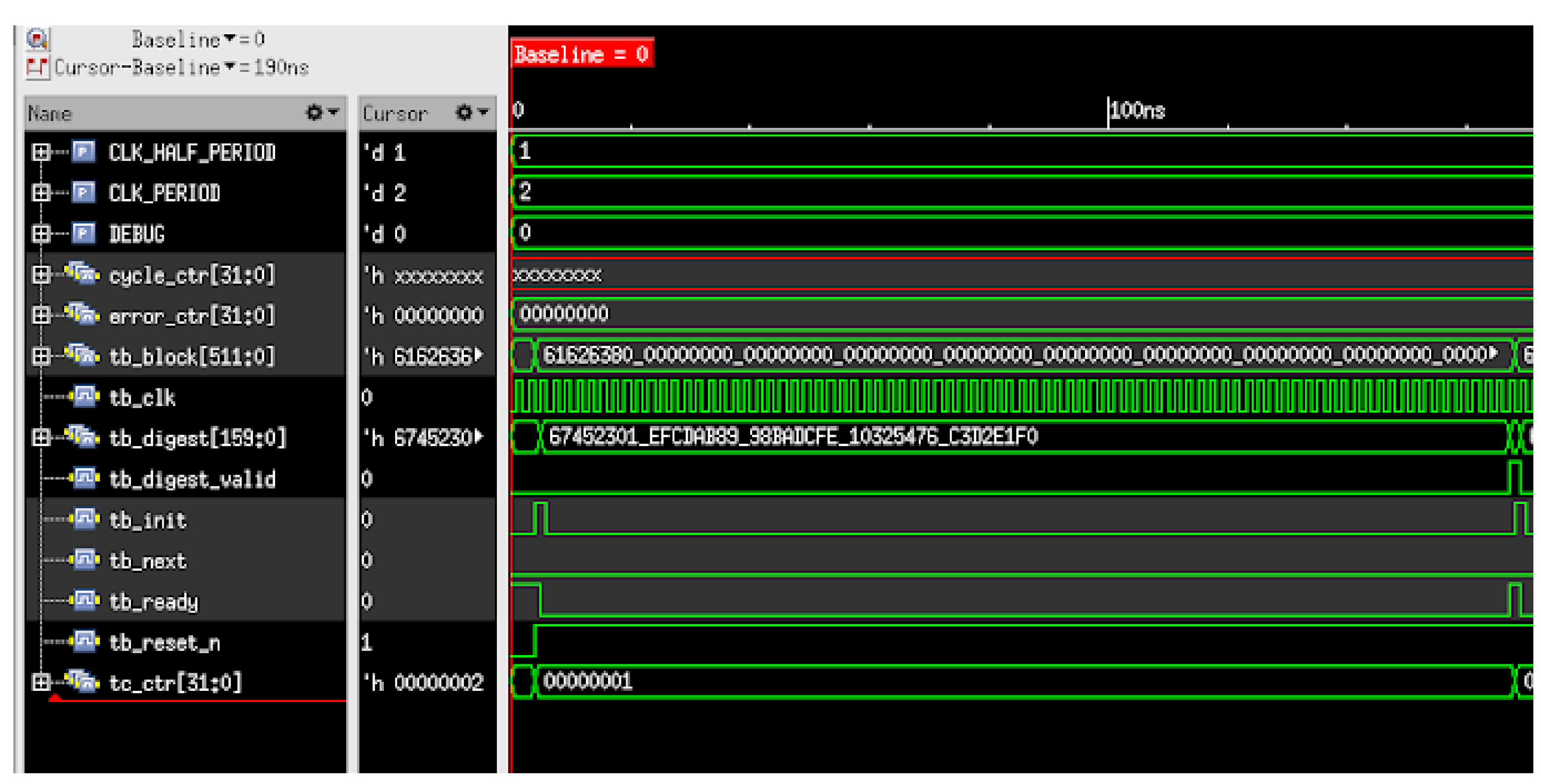


Figure 5. Waveform Depicting SHA-1 in Verilog

Future Work:

1. Produce waveforms of an executed hash in SHA-3
2. Implement SHA-3 on an FPGA
3. Launch a DFA attack

Broader Impact of Project:

- The ultimate goal of this project is to apply the SHA-3 as a security measure in a sensor network.

Citations:

[1]W. Trappe and L.C. Washington, *Introduction to Cryptography with Coding Theory*. Upper Saddle River: Pearson, 2006. P. 218-239.
[2]Stamp, M. (2011). *Information Security Principles and Practice*. 2nd ed. Hoboken: John Wiley & Sons, pp.125-153.
[3]M. Taha and P. Schaumont, "Differential Power Analysis of MAC-Keccak at Any Key-Length", *Lecture Notes in Computer Science*, vol. 8231, pp. 68-82, 2013. Available: https://link.springer.com/chapter/10.1007%2F978-3-642-41383-4_5. [Accessed 12 June 2019].
[4]G. Bertoni, J. Daemen, M. Peeters and G. Van Assche, "Cryptographic sponge functions", 2011. [Online]. Available: https://keccak.team/files/CSF-0.1.pdf. [Accessed: 21 Aug 2019].
[5]P. Luo, Y. Fei, L. Zhang and A. Ding, "Differential Fault Analysis of SHA3-224 and SHA-256", *Eprint.iacr.org*, 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7774477. [Accessed: 24- Oct 2019].

Award ID#: 1652474

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting)
October 28-29, 2019 | Alexandria, Virginia