Keccak Thesis

Alexander Scheel

Iowa State University

TODO

MATH 490 | Advisor: Dr. Clifford Bergman | SHA-3 | hash_framework

1. A Series of Introductions

This paper presents the work of the author towards the completion of the requirements for the MATH 490 Independent Study course under Dr. Clifford Bergman at Iowa State University of Science and Technology. This work was an extension of the author's Honors Project under Dr. Eric Bergman and utilized the resulting hash_framework project. Additional artifacts related to this project can be seen in the keccak-attacks repository.

Within this section are a series of introductions which provide necessary background on the topics of cryptography, hash functions, the development of Keccak/SHA-3, and its structure. While certain sections can be skipped if the reader has the prerequisite knowledge, hopefully all readers find the material engaging and useful. Following these introductions, this paper presents the analysis of the Keccak/SHA-3 hash function before concluding with a final evaluation and further work.

Introduction on the Topics of Cryptography. While there have been many applications of mathematics, few are as demanding and shrouded in secrecy as that of cryptography. Cryptography exists because of the fundamental need of civilizations, governments, and individuals to keep secrets secure from devoted adversaries.

Introduction on the Topics of Hash Functions. Within cryptography's collection of algorithms, few are are as useful as hash functions have proven to be to cryptographers and non-cryptographers alike. A hash function maps arbitrary length binary strings to binary strings of a fixed length.

Introduction on the Development of Keccak/SHA-3. FIPS 202 [1].

Introduction on the Structure of SHA-3. SHA-3 consists of two parts: a core permutation function, KECCAK-f, and a domain extender, the KECCAK sponge function.

2. Mathematical Properties of the Five Round Functions

Bijectivity.

Of θ.

E-mail: alexander.m.scheelgmail.com

Of ρ.

Of π.

Of χ.

Of ι.

Order of the Permutation.

Evaluation of the Orders of Composition of Permutations.

Inverse of the Permutation.

XOR ($\oplus$) Distributivity.

Generalizations of θ and χ.

Choice of Parameters and Ordering of Composition.

3. Marginal and Differential Properties of the Five Round Functions

Margin Properties.

Differential Properties.

Input Margin Impact on Differential Properties.

Output Margin Impact on Differential Properties.

4. Exhaustive Collision Searches

5. Fixed Point Attacks

Full Fixed Points.

Partial Fixed Points.

6. Conclusions and Further Work

7. Bibliography

1. (2015) Fips pub 202, sha-3 standard: Permutation-based hash and extendable-output functions. U.S.Department of Commerce/National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf.