Secure Hash Algorithm-3 (SHA-3)

Samer Moein

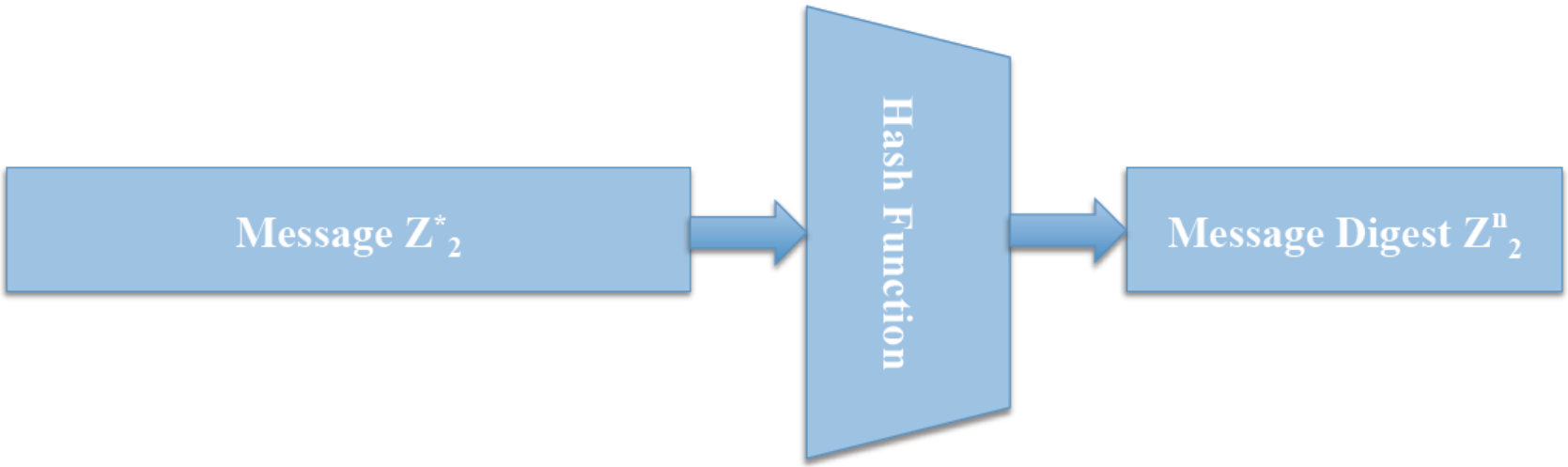
University of Victoria

samerm@uvic.ca

May 18, 2017

Cryptographic Hash Function I

An algorithm that takes an arbitrary block of data (message) and returns a fixed-size bit string (message digest).



- The input to a hash function is called the **message**, and the output is called the **message digest or hash value.**
- The digest often serves as a condensed representation of the message.

Cryptographic Hash Function II

The three security properties of hash functions:

- Pre-image resistant
  - It shall take 2^n effort to given y, find x such that h(x) = y
- 2nd pre-image resistance
  - It shall take 2^n effort to given M and h(M), find another $\overline{M}$ with h($\overline{M}$) = h(M)
- Collision resistance
  - It shall take $2^{n/2}$ effort to find $x_1 \neq x_2$ such that h(x_1) = h(x_2)

SHA-3 (Keccak)

- Selected on October 2012 as the winner of the NIST hash function competition.
- The SHA-3 family consists of four cryptographic hash functions:
  - SHA3-224,
  - SHA3-256,
  - SHA3-384, and
  - SHA3-512.
- The digest lengths in FIPS-approved hash functions are **160**, 224, 256, 384, and 512 bits.
- Built based on the sponge construction.

Sponge Construction

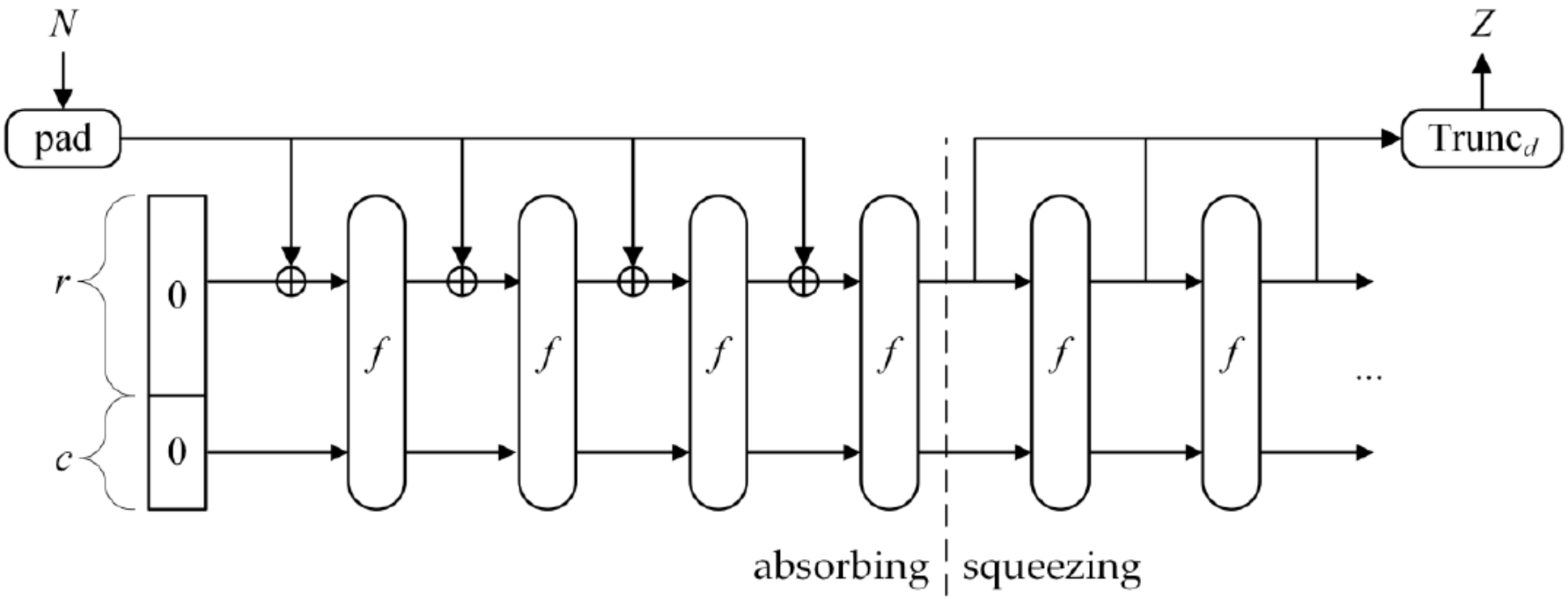
Is a framework for specifying functions on binary data with arbitrary output length.

The construction employs the following three components:

- An underlying function on fixed-length strings, denoted by **f**,
- A parameter called the rate, denoted by **r**, and
- A padding rule, denoted by **pad.**

Sponge Function

- The function that the construction produces from these components is called a sponge function, denoted by: **SPONGE[f, pad, r]**
- A sponge function takes two inputs: a bit string, denoted by N, and the bit length, denoted by d, of the output string, **SPONGE[f, pad, r](N, d).**



KECCAK-p [b, n_r] Permutation I

The KECCAK-p permutations are specified, with two parameters:

1. b: The fixed length of the strings that are permuted, called the **width** of the permutation.
   - The permutation is defined for any b in {25, 50, 100, 200, 400, 800, 1600}
2. n_r: The number of iterations of an internal transformation, called a **round**.
   - n_r can be any positive integer.

- A round of a KECCAK-p permutation, denoted by **Rnd**, consists of a sequence of **five** transformations, which are called the **step mappings.**
- The permutation is specified in terms of an array of values for b bits that is repeatedly updated, called the **state**.

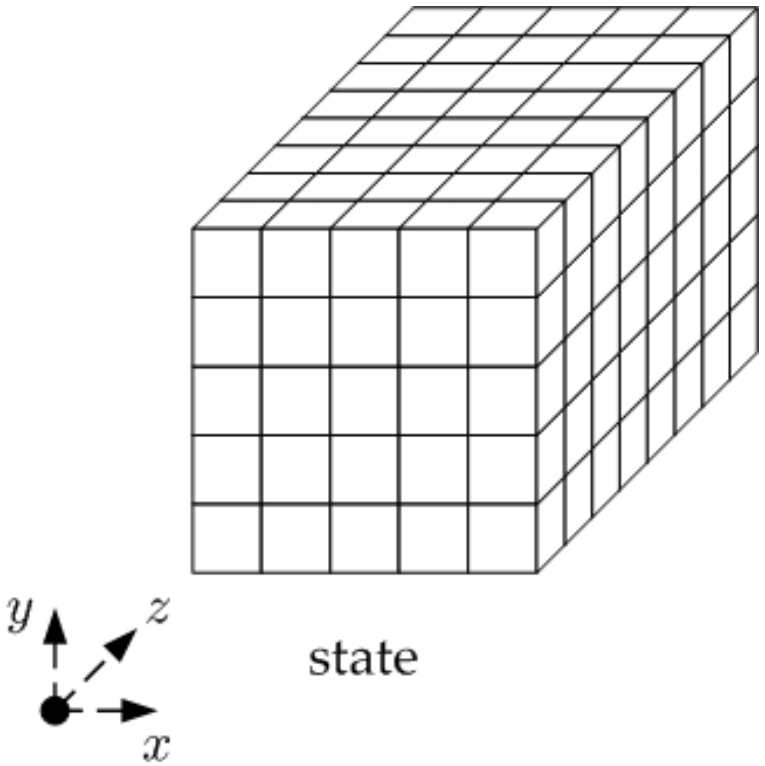
KECCAK-p [b, n_r] Permutation II

Given a state array **A** and a round index i_r, the round function **Rnd** is the transformation that results from applying the step mappings θ, ρ, π, χ, **and** ι, in that order, i.e.,:

$$Rnd(A, i_r) = \iota(\chi(\pi(\rho(\theta(A)))), i_r)$$

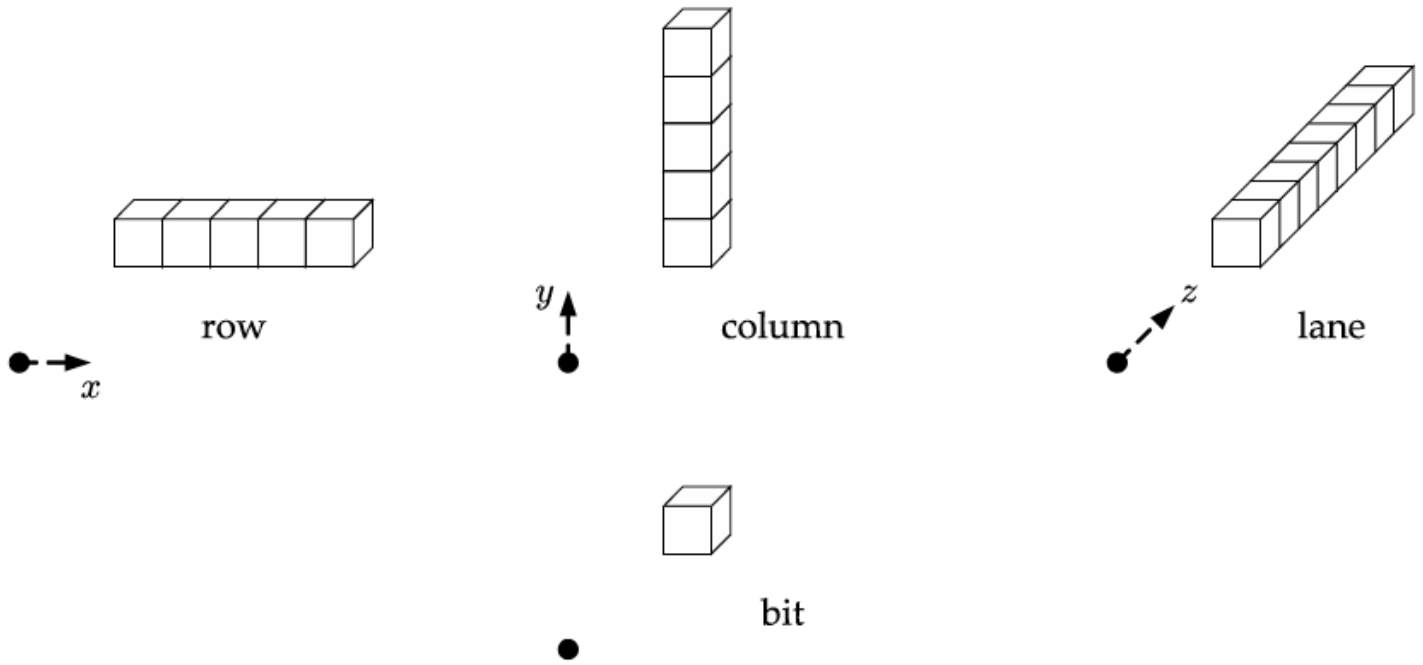
State I

An array of $5 \times 5 \times 2^{\ell}$ bits $\equiv 5 \times 5 \times \omega$ bits,
where $\omega = b/25$, $\ell = log_2(b/25)$



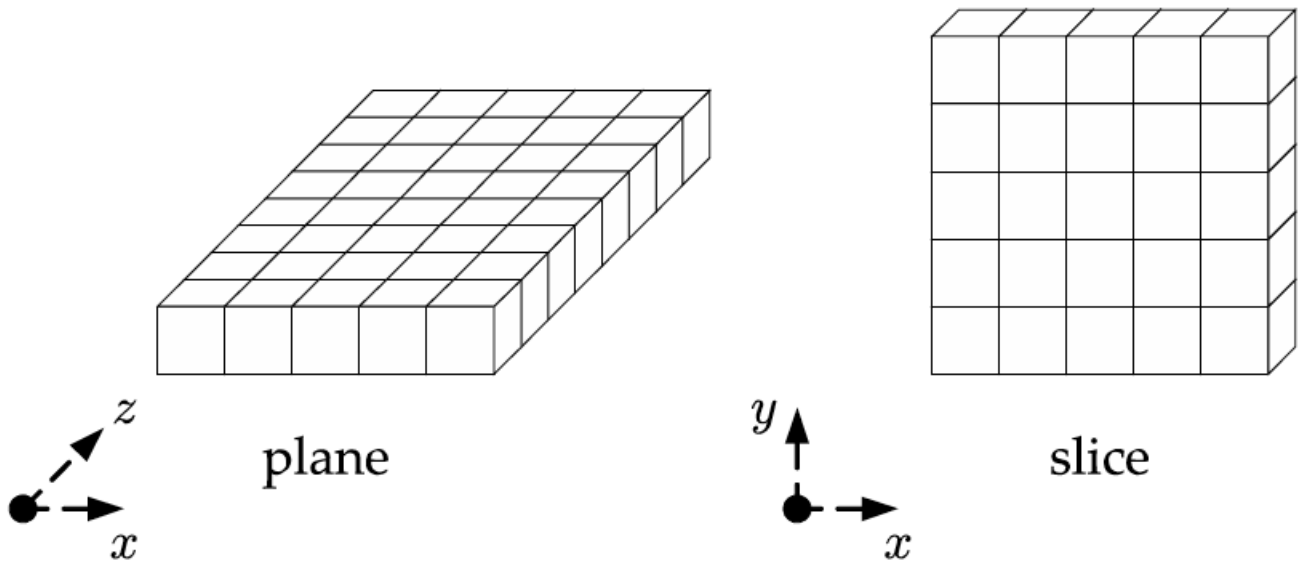
State II

An array of $5 \times 5 \times 2^{\ell}$ bits $\equiv 5 \times 5 \times \omega$ bits,
where $\omega = b/25$, $\ell = log_2(b/25)$



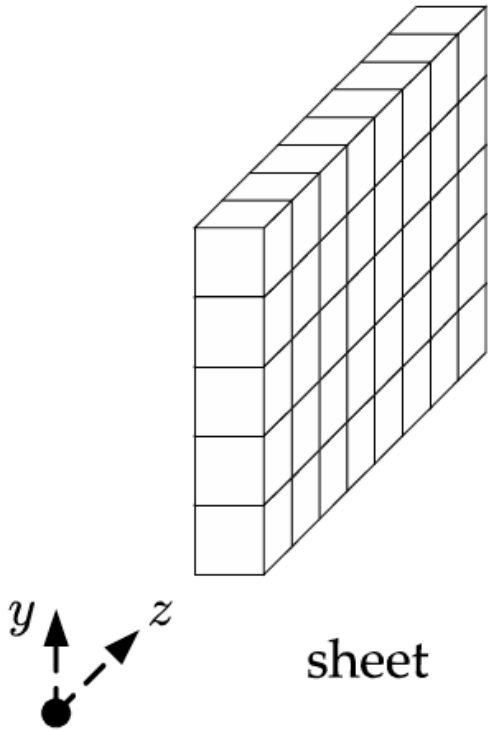
State III

An array of $5 \times 5 \times 2^{\ell}$ bits $\equiv 5 \times 5 \times \omega$ bits,
where $\omega = b/25$, $\ell = log_2(b/25)$



State IV

An array of $5 \times 5 \times 2^{\ell}$ bits $\equiv 5 \times 5 \times \omega$ bits,
where $\omega = b/25$, $\ell = log_2(b/25)$



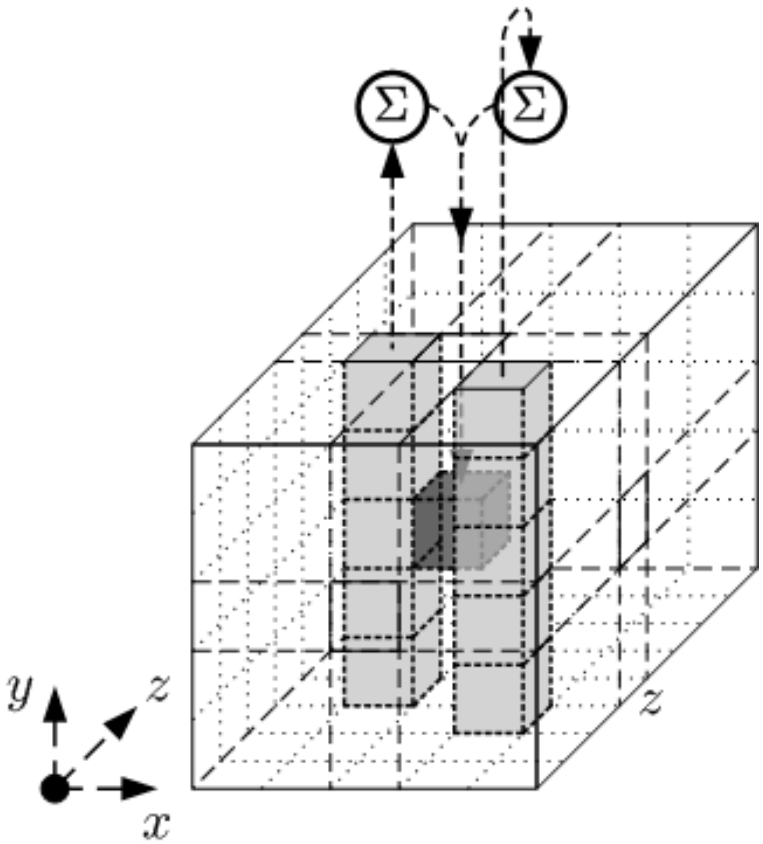
Step Mappings

The five step mappings that comprise a round of KECCAK-p[b, n_r] are denoted by:

- Theta (θ)
- Rho (ρ)
- Pi (π)
- Chi (χ)
- Iota (ι)

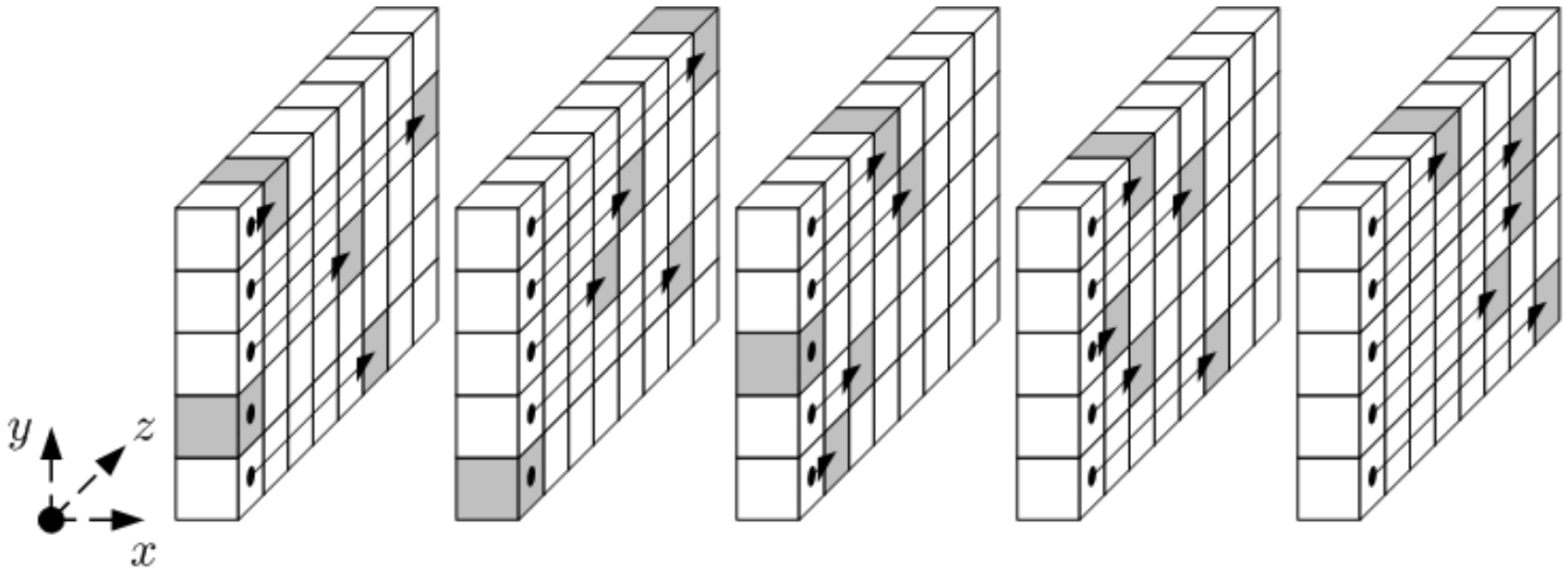
Theta (θ)

The effect of θ is to XOR each bit in the state with the parities of two columns in the array.



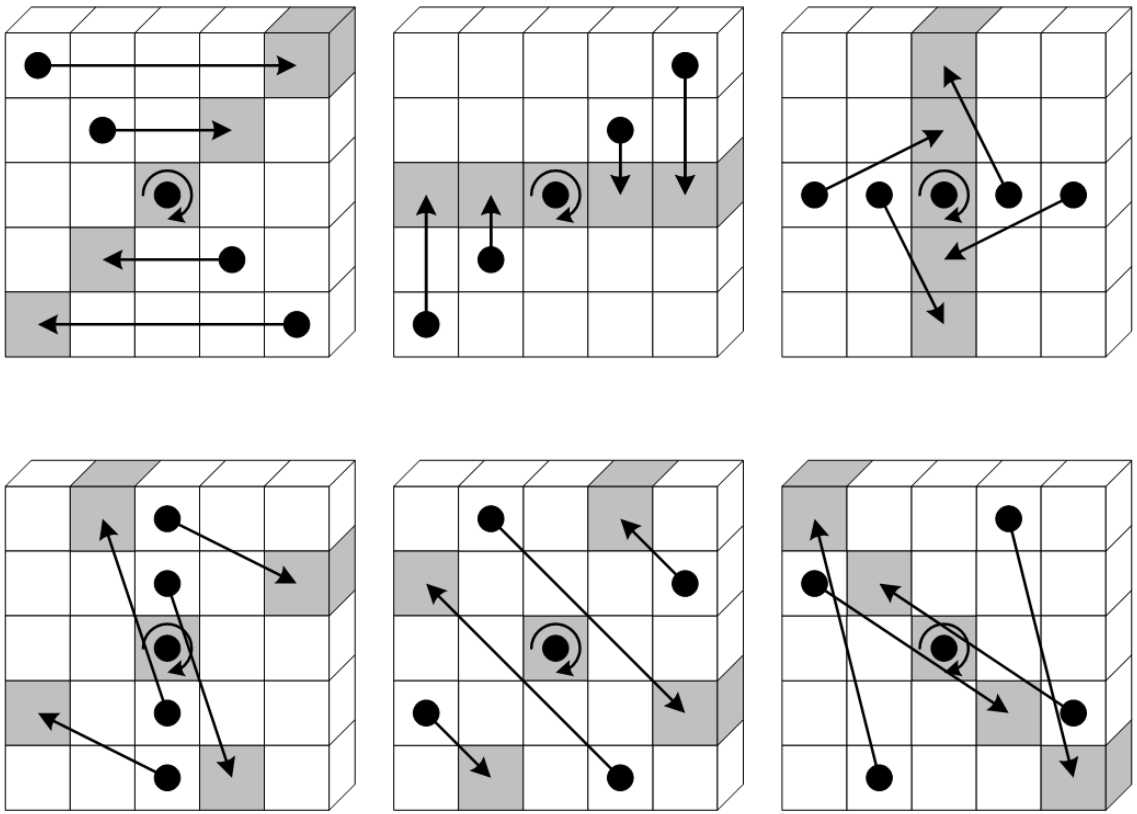
Rho (ρ)

The effect of ρ is to rotate the bits of each lane by a length, called the offset, which depends on the fixed x and y coordinates of the lane.



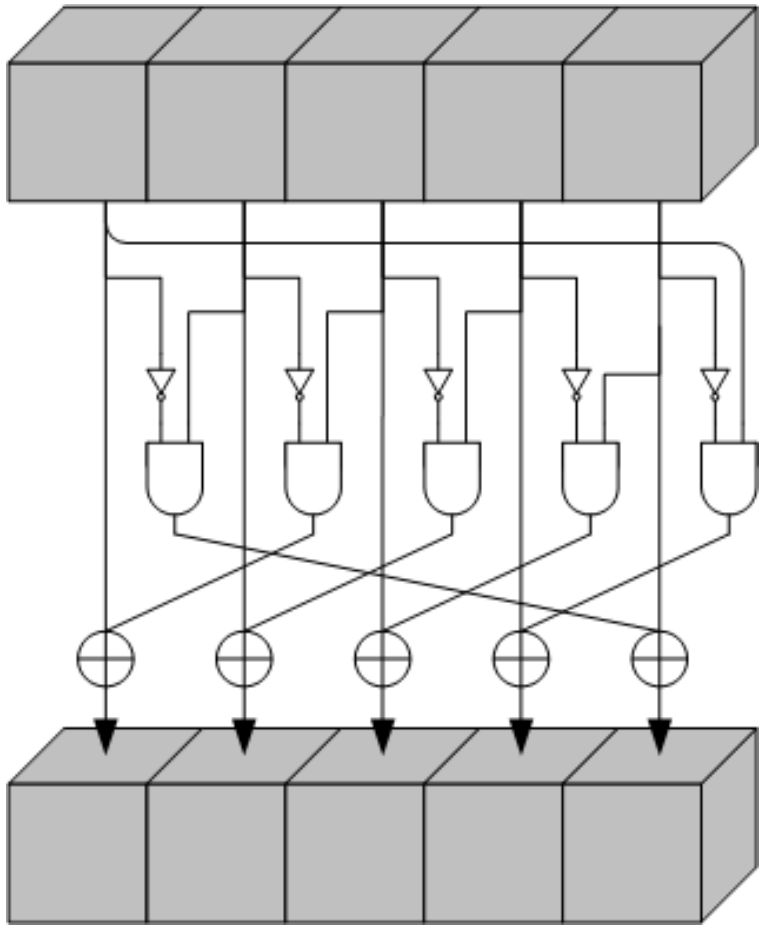
Pi (π)

The effect of π is to rearrange the positions of the lanes.



Chi (χ)

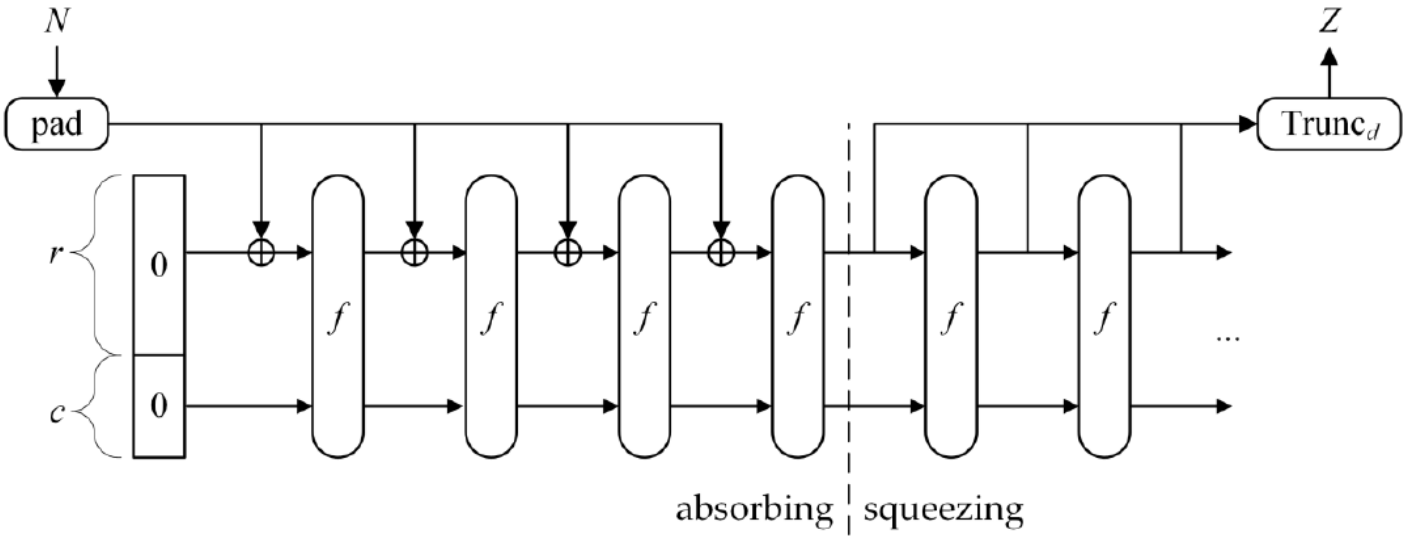
The effect of χ is to XOR each bit with a non-linear function of two other bits in its row.



Iota (ι)

The effect of ι is to modify some of the bits of Lane (0, 0) in a manner that depends on the round index i_r. The other 24 lanes are not affected by ι.

KECCAK I



KECCAK

$$KECCAK[c](N, d) = SPONGE[KECCAK - p[b, n_r], pad, b - c](N, d)$$

KECCAK II

KECCAK

$$KECCAK[c](N, d) = SPONGE[KECCAK - p[b, n_r], pad, b - c](N, d)$$

Project - Pre-image

$$KECCAK[160](N, 80) = SPONGE[KECCAK - p[200, 2], pad, 40](N, 80)$$

Project - Collision

$$KECCAK[160](N, 160) = SPONGE[KECCAK - p[200, 2], pad, 40](N, 160)$$

References

FIPS PUB 202

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

http://dx.doi.org/10.6028/NIST.FIPS.202

The End