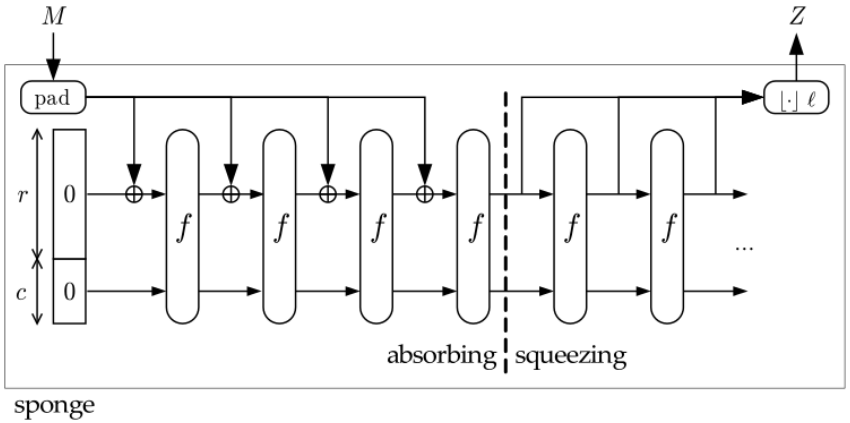


The Sponge Construction

CS 553

CRYPTOGRAPHY

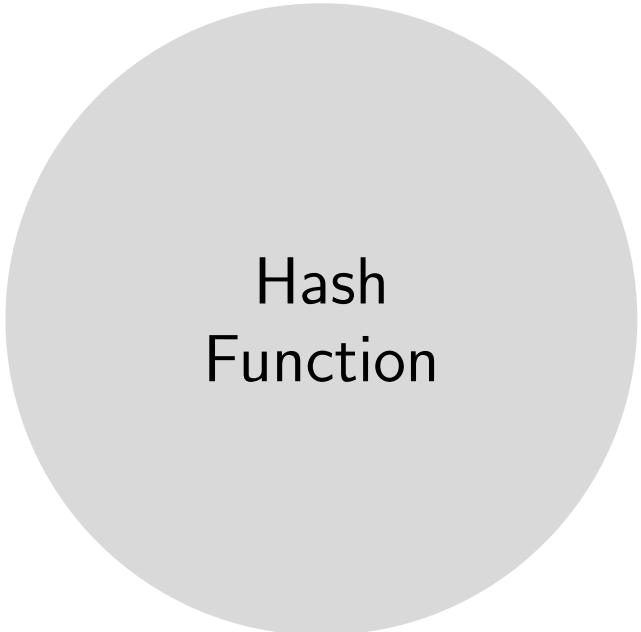
Lecture 20

Hash Constructions

Instructor

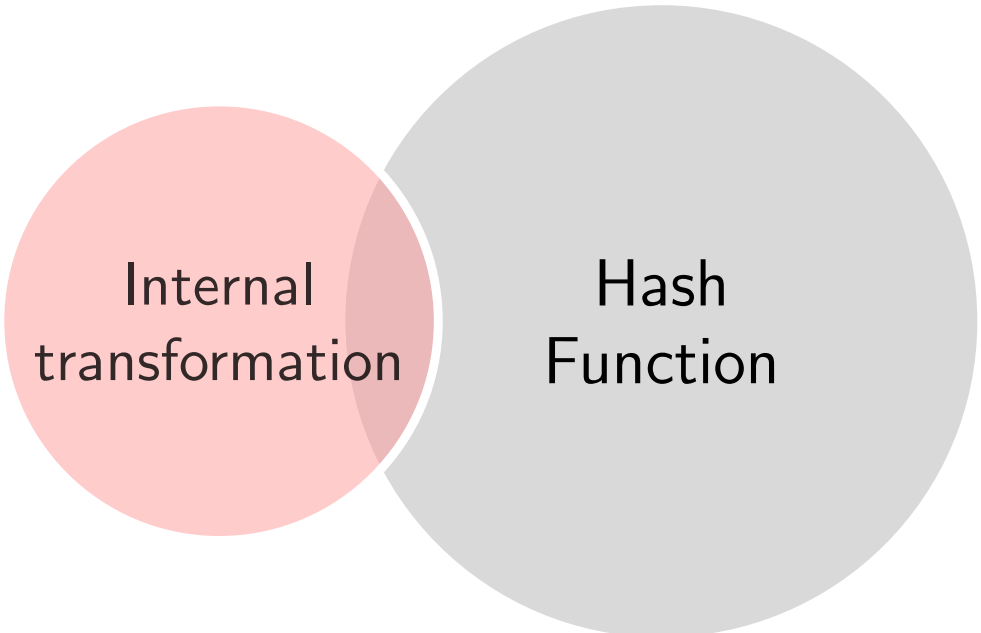
Dr. Dhiman Saha

Image Source: Google



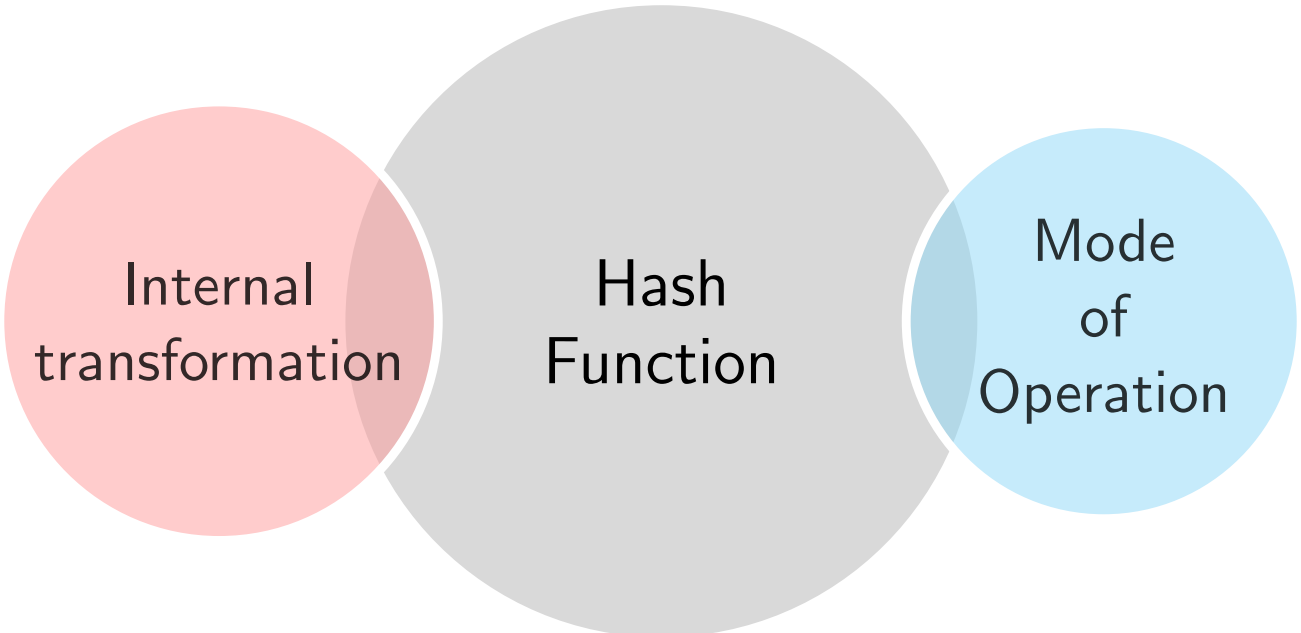
- Compression Function
- Block-Cipher
- Permutation
- etc.

- Iterates the internal transformation
- Also called the **Domain Extension Algorithm**



- Compression Function
- Block-Cipher
- Permutation
- etc.

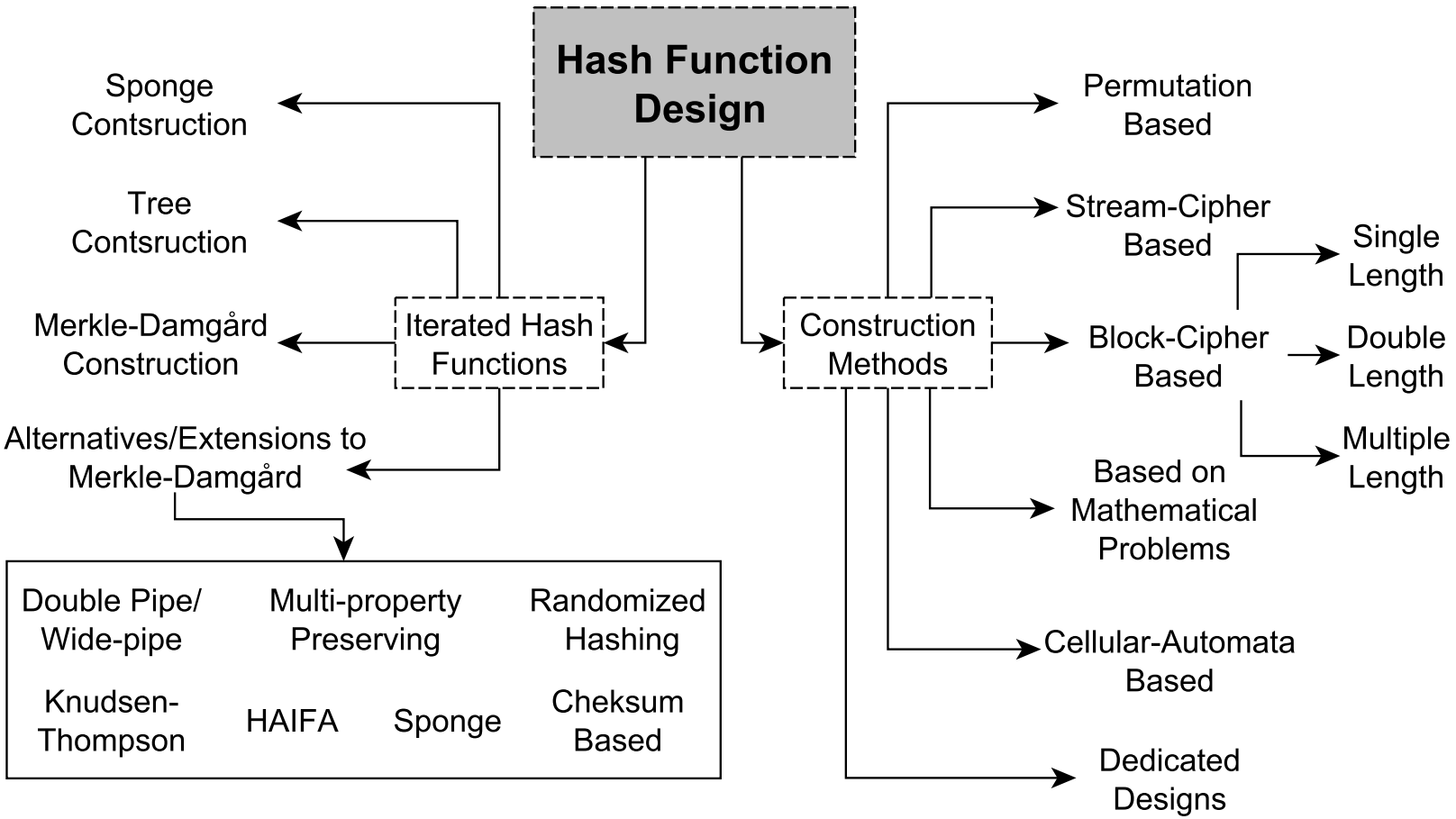
- Iterates the internal transformation
- Also called the **Domain Extension Algorithm**



- Compression Function
- Block-Cipher
- Permutation
- etc.

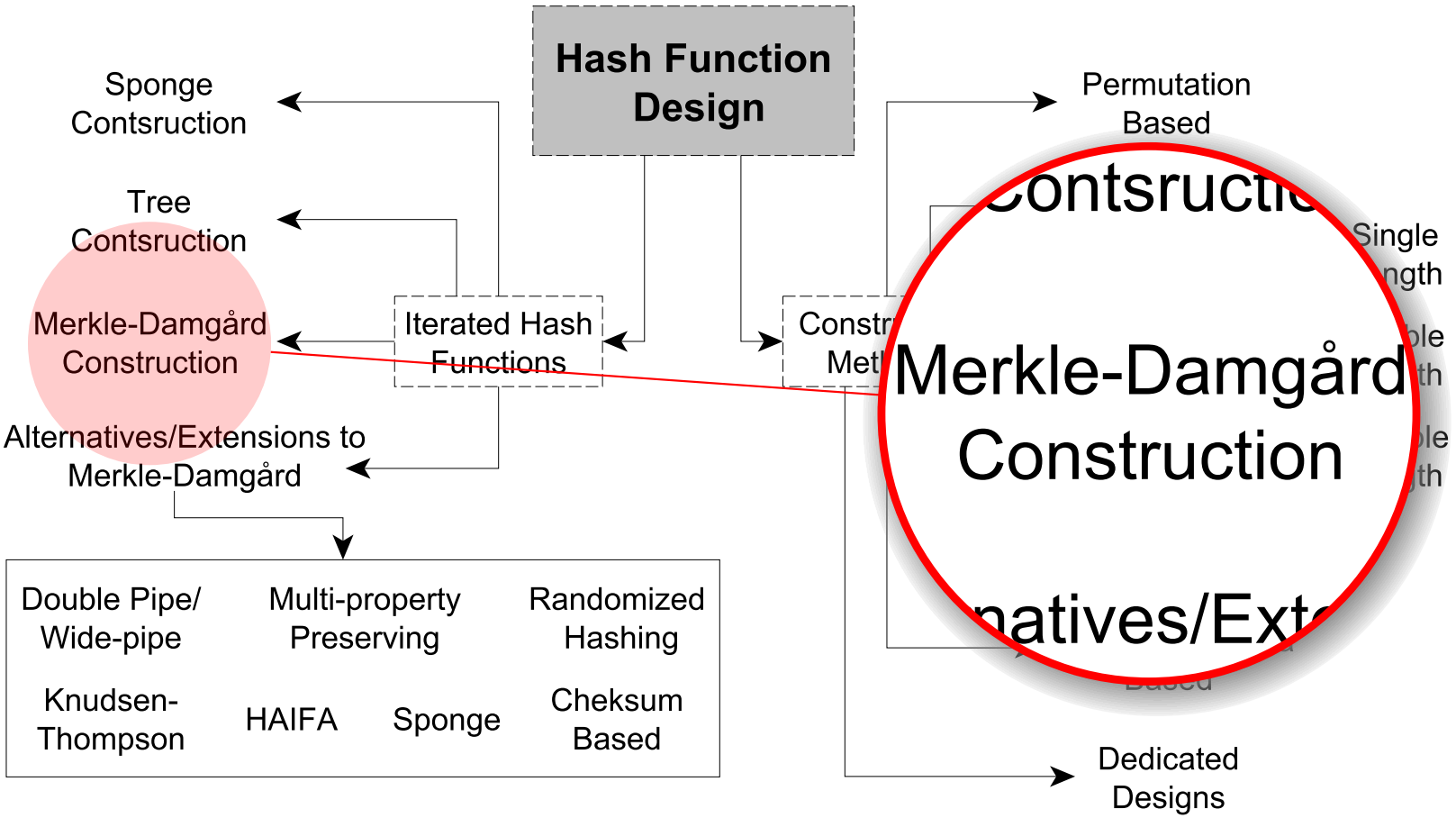
- Iterates the internal transformation
- Also called the **Domain Extension Algorithm**

Taxanomy of Hash Designs

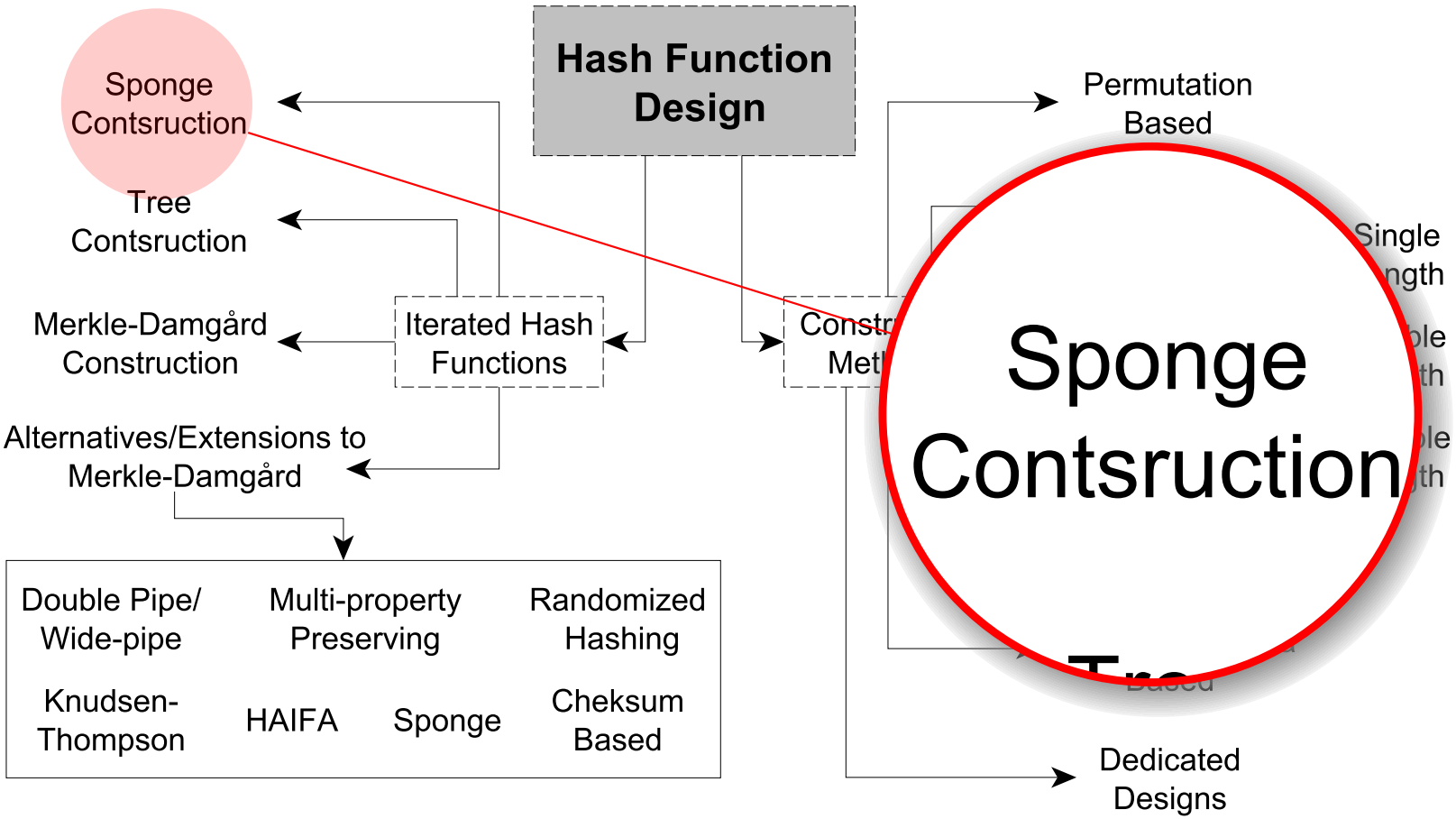


Most Popular: Iterated Hashing

Our Focus - Historical Importance



Our Focus - Latest



Idea

The simplest way to hash a message is to split it into chunks and process each chunk consecutively using a similar algorithm.

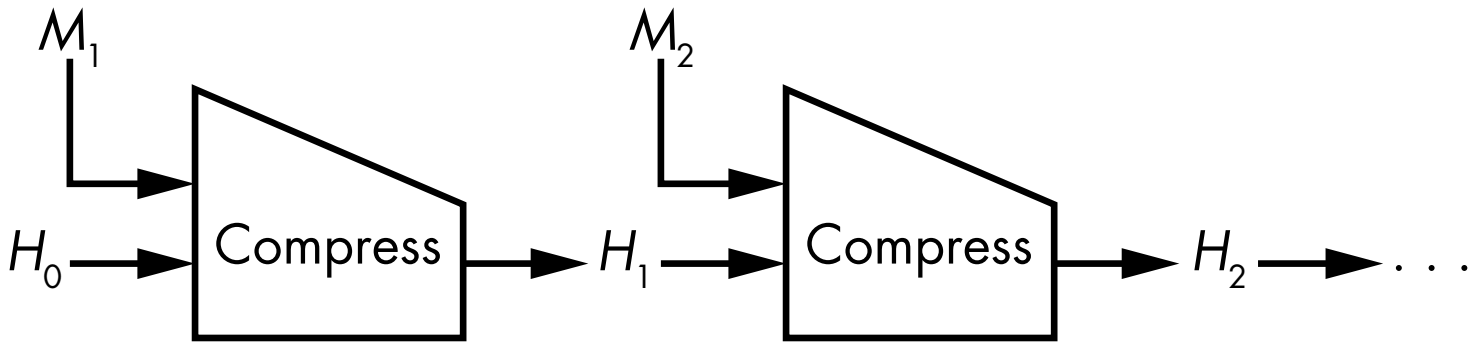
Compression Function Based

- Uses a **compression function** that transforms an input to a smaller output.
- AKA the MerkleDamgård construction
- Named after the Ralph Merkle and Ivan Damgård

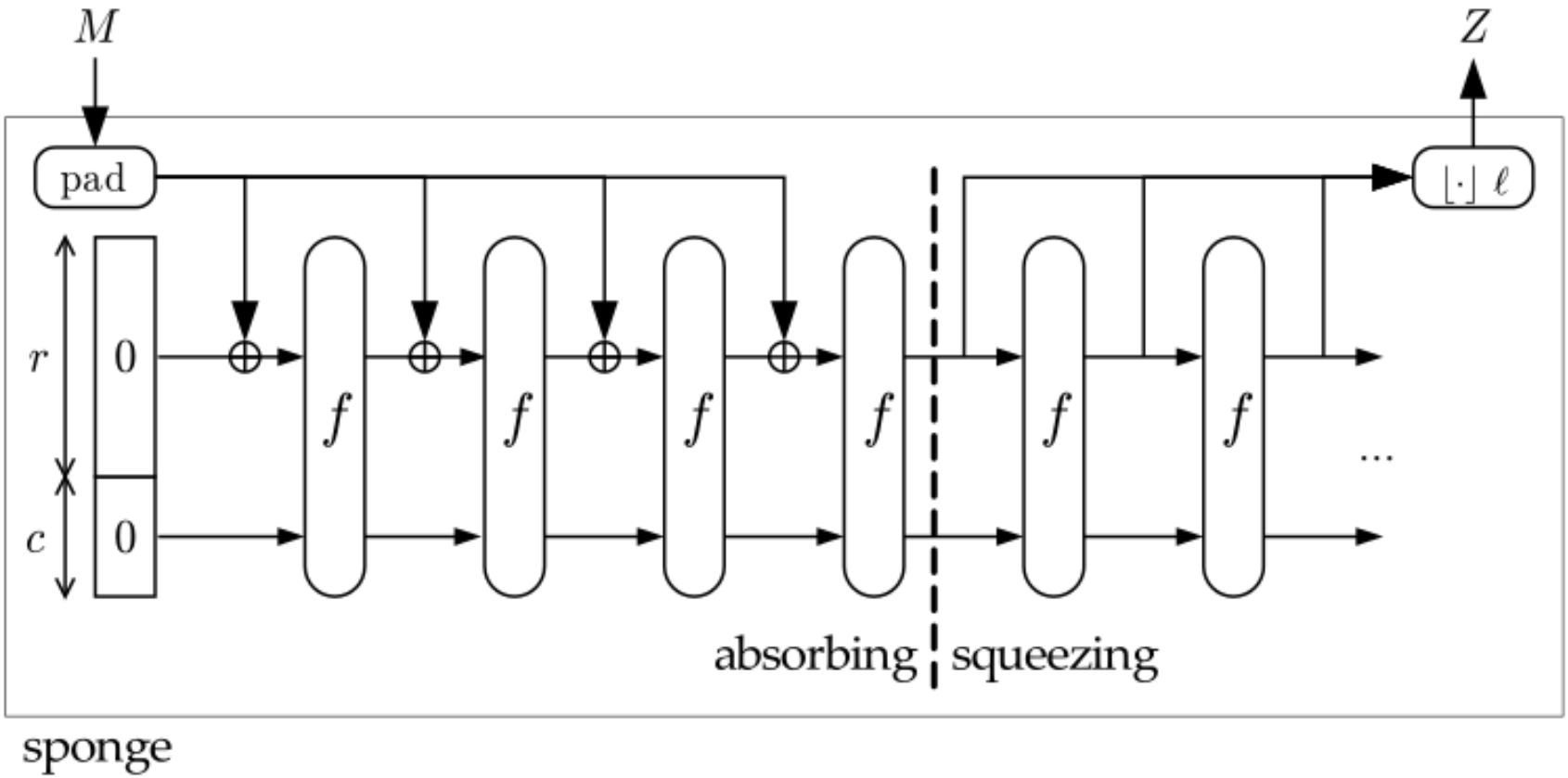
Permutation Based

- Transforms an input to an output of the same size
- AKA **sponge** functions.

Merkle-Damgård



Sponge



sponge

Why? Homework

If a **compression function** is preimage and collision resistant, then a **hash function** built on it using the **M-D** construction will also be preimage and collision resistant.

Finding Multi-collisions

How much more difficult than finding a collision?

Why?

If you know $Hash(M)$ for some unknown message, M, composed of blocks M_1 and M_2 (after padding), you can determine $Hash(M_1||M_2||M_3)$ for **any** block, M_3.

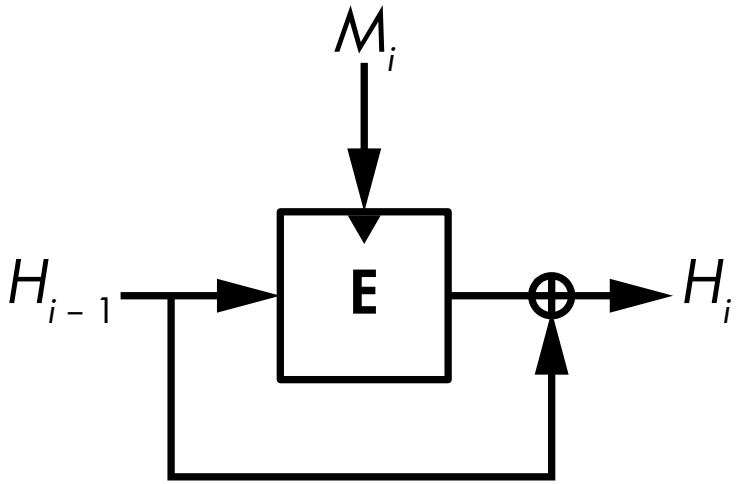
- A side-effect of M-D Construction.

A Practical Example

Proof of storage protocols

The Davies-Meyer construction

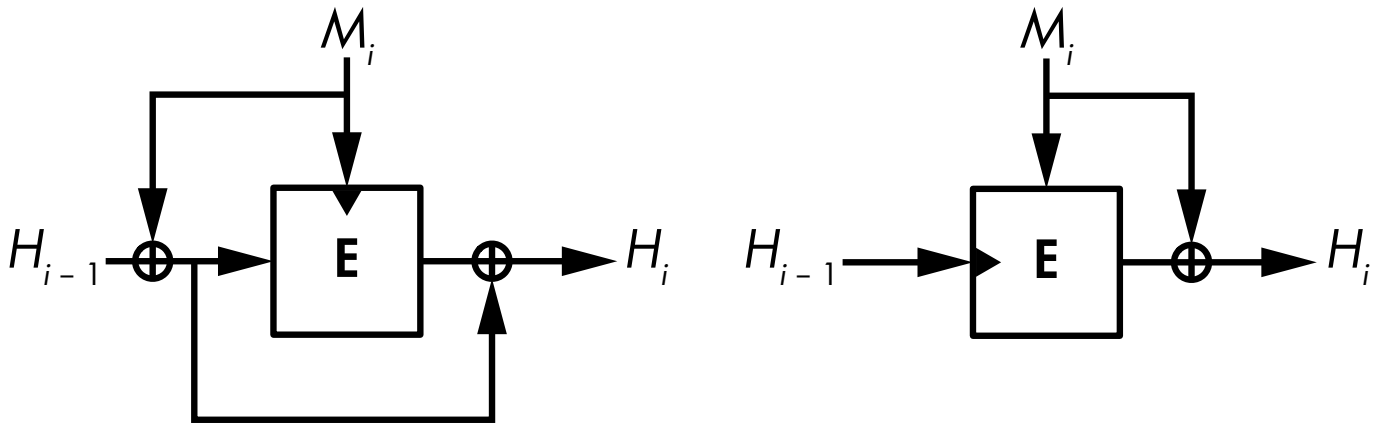
The most common of the block cipher-based compression functions



Fixed Points — An Interesting Property

You can find fixed points, or chaining values, that are unchanged after applying the compression function with a given message block.

Other Compression Function Constructions



Less Popular

- More complex or
- Require the message block to be the same length as the chaining value.

- Hash functions are the same everywhere

Implication User re-uses the same password on two sites

- What if both sites use same hash function?
- The values in the password database will be the same.

- Further, many passwords are extremely common (`password`), so many users will use the same one.

The Rainbow Table

What if we simply try many of those passwords, creating huge tables mapping passwords to their hash values?

Definition (Salt)

Random data that is added to a cryptographic primitive like

- A one-way function such as a cryptographic hash function
- Or a key derivation function

Customizes such functions to produce different outputs (provided the salt is different)

- Can be used to prevent e.g. **dictionary attacks**
- Typically **does not** have to be **secret**, but secrecy may improve security properties of the system.

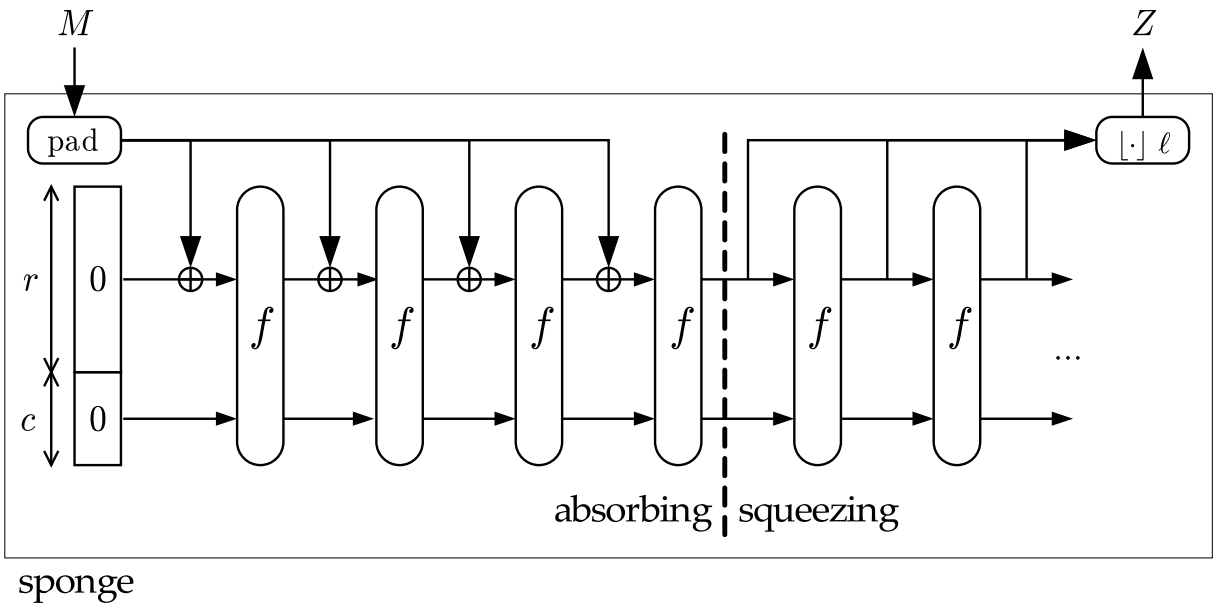
Compare salt with nonce, initialization vector.

Instantiates a fixed-length permutation

An interesting alternative to *hard-to-build* structures:

Compression functions, Block ciphers

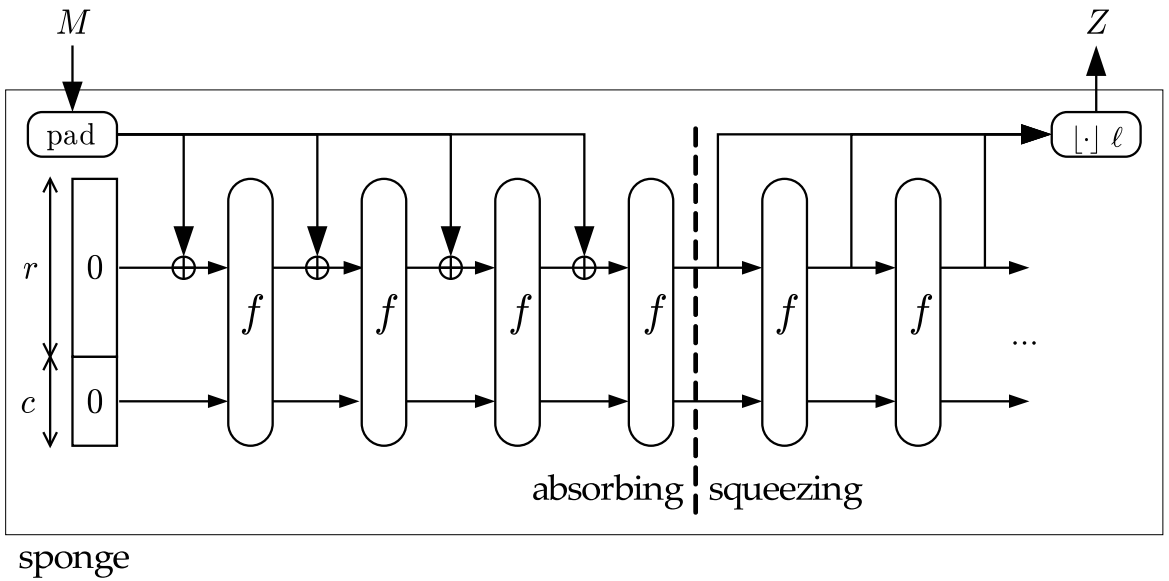
$b = r + c$
b = width
r = bitrate
c = capacity



Note

The output length is **variable** $\Longrightarrow$ classical notion fails

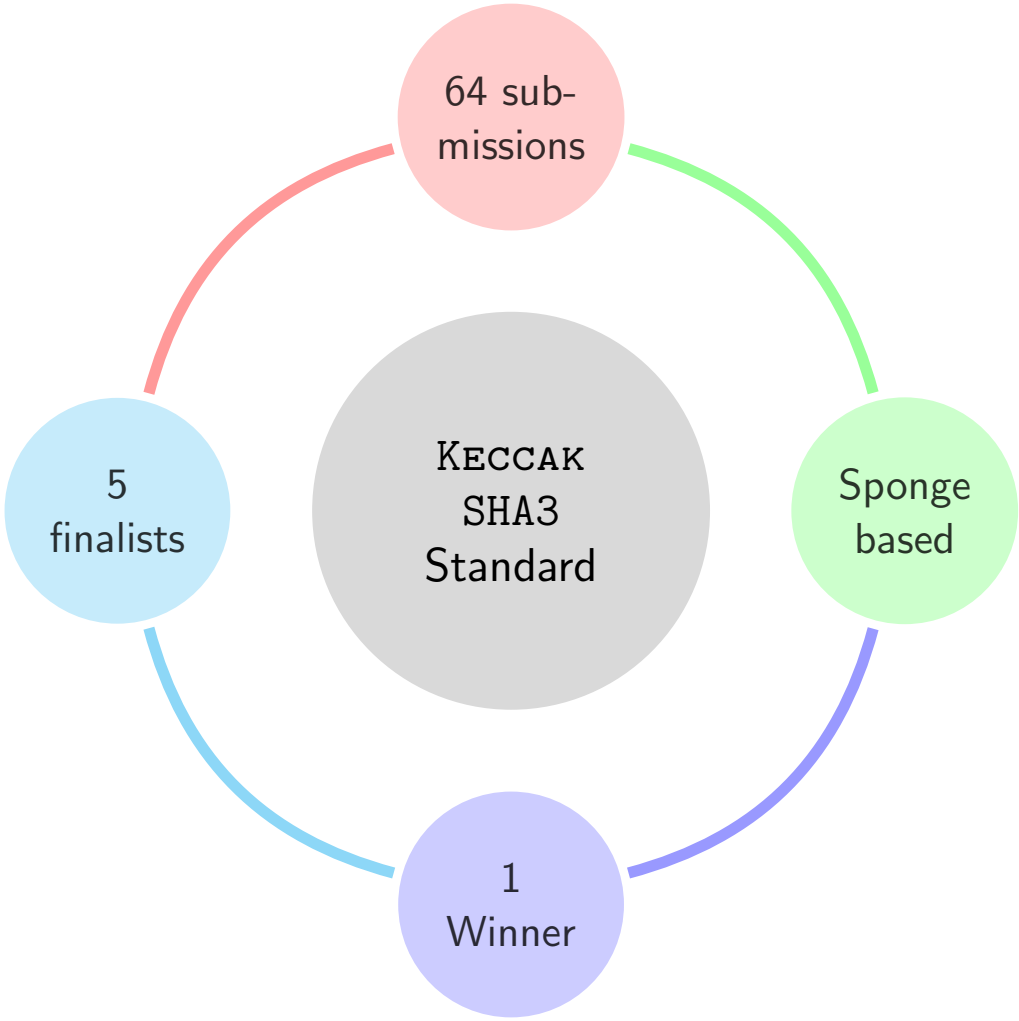
New notion: Security defined in terms of **capacity**



Allows trade-off between $\left\{ \begin{array}{c} \text{speed} \\ \& \\ \text{security} \end{array} \right. \rightarrow \begin{array}{c} \text{rate} \\ \& \\ \text{capacity} \end{array}$

SHA3 Competition

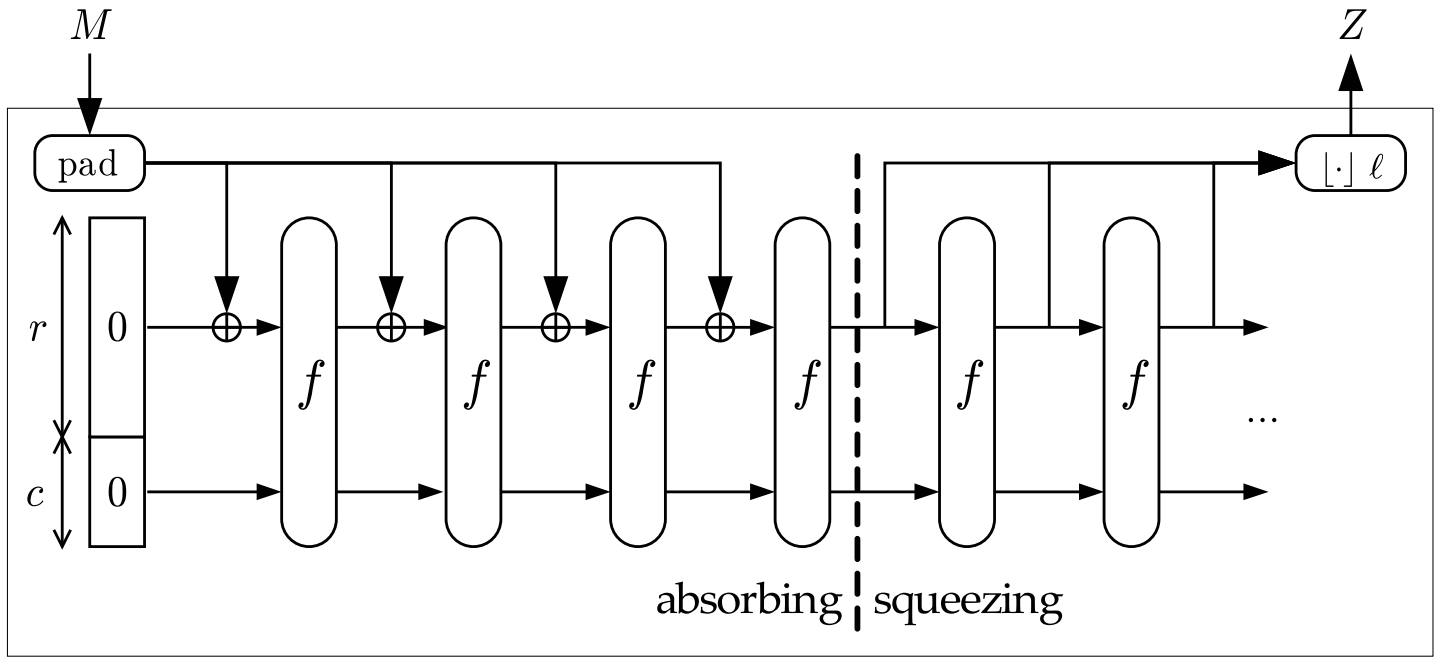
- Announced by NIST in 2007
- Search for the next generation (S)ecure (H)ash (A)lgorithm
- Follows philosophy of AES Competition
- 5 years of intense cryptanalysis
- Keccak declared winner in Oct 2012



- Follows SPONGE construction
- Internal permutation called KECCAK-f/KECCAK-p
- SHA3 Family

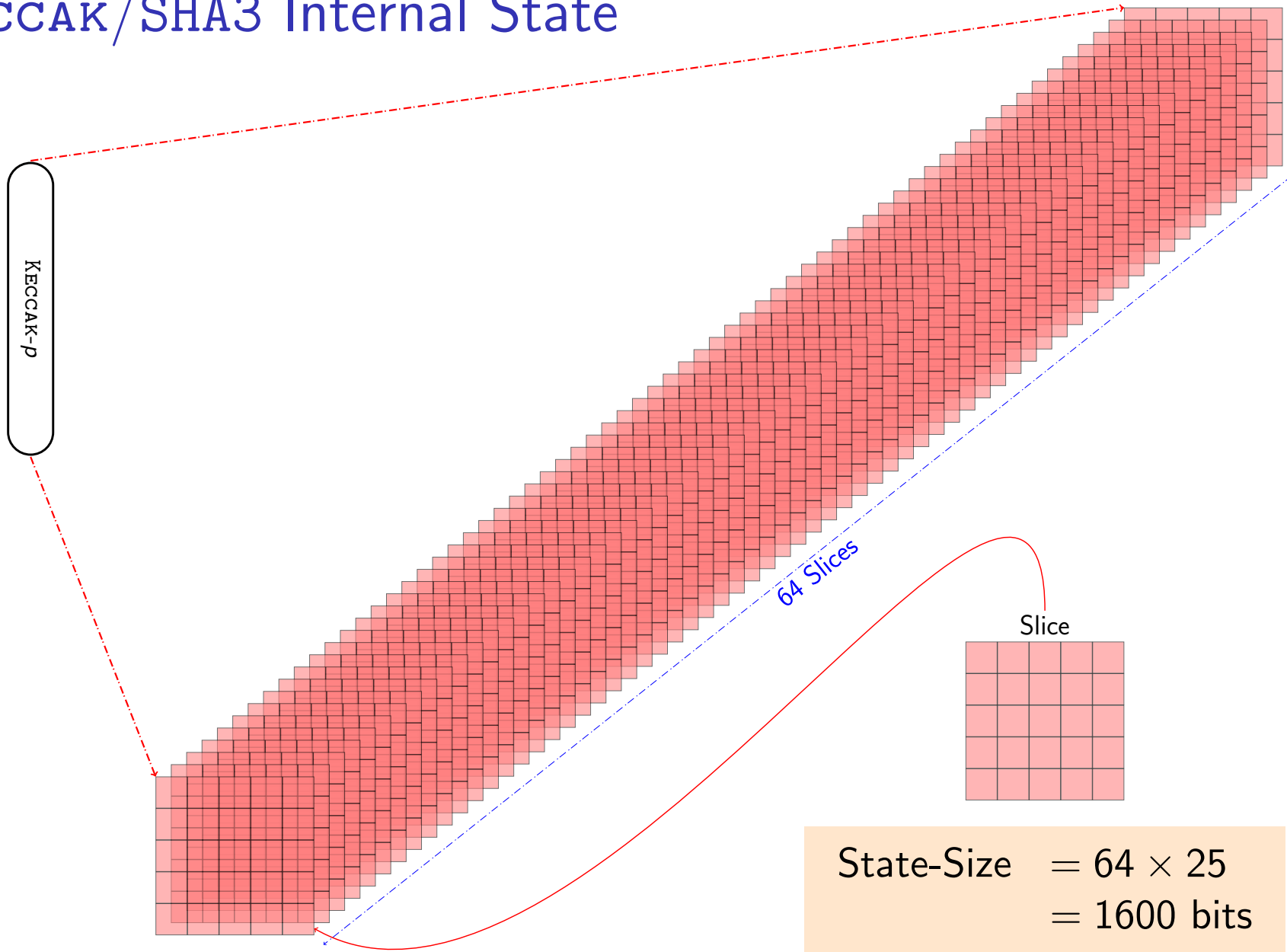
Fixed-Length → SHA3-224/256/384/512

XOF → SHAKE128/256



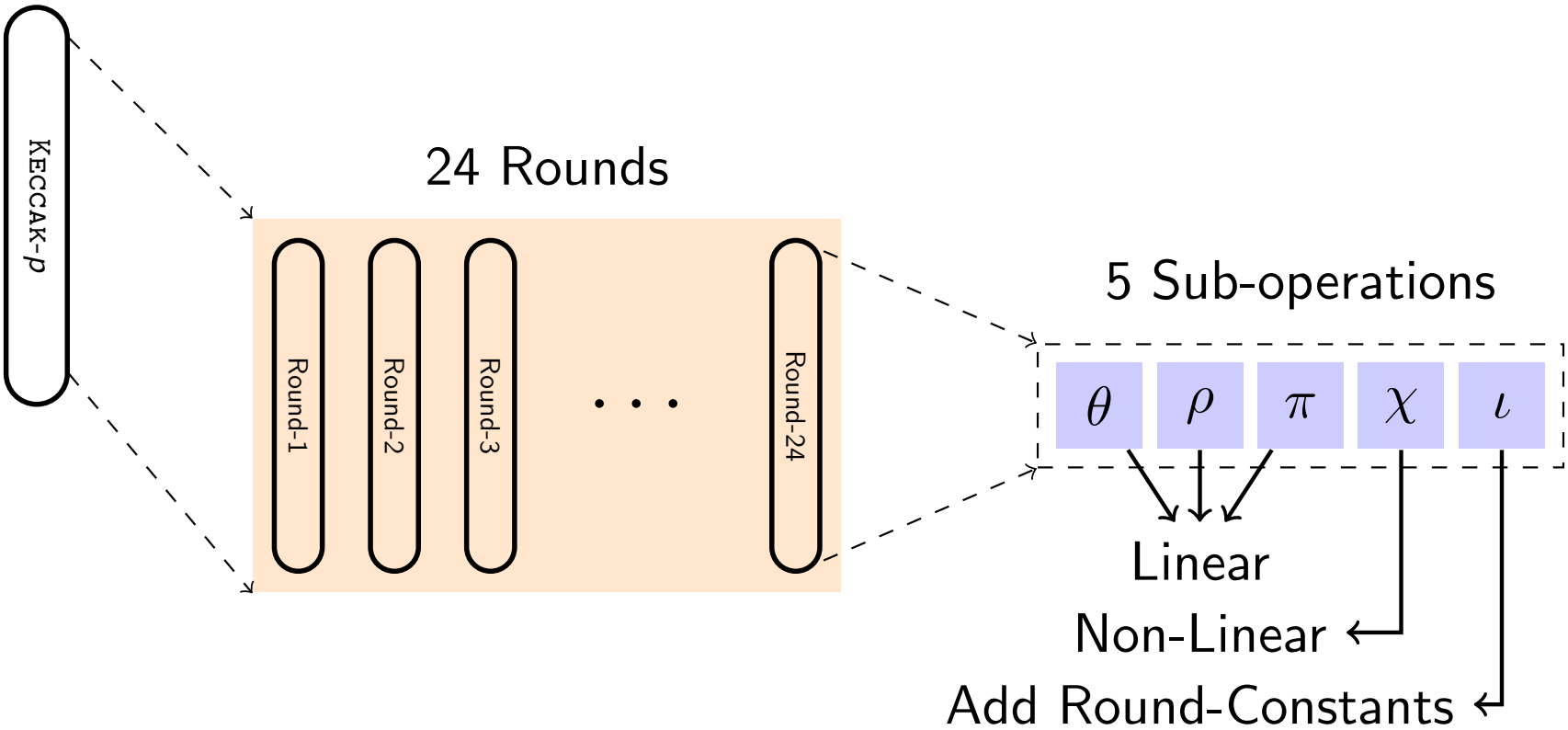
sponge

Keccak/SHA3 Internal State



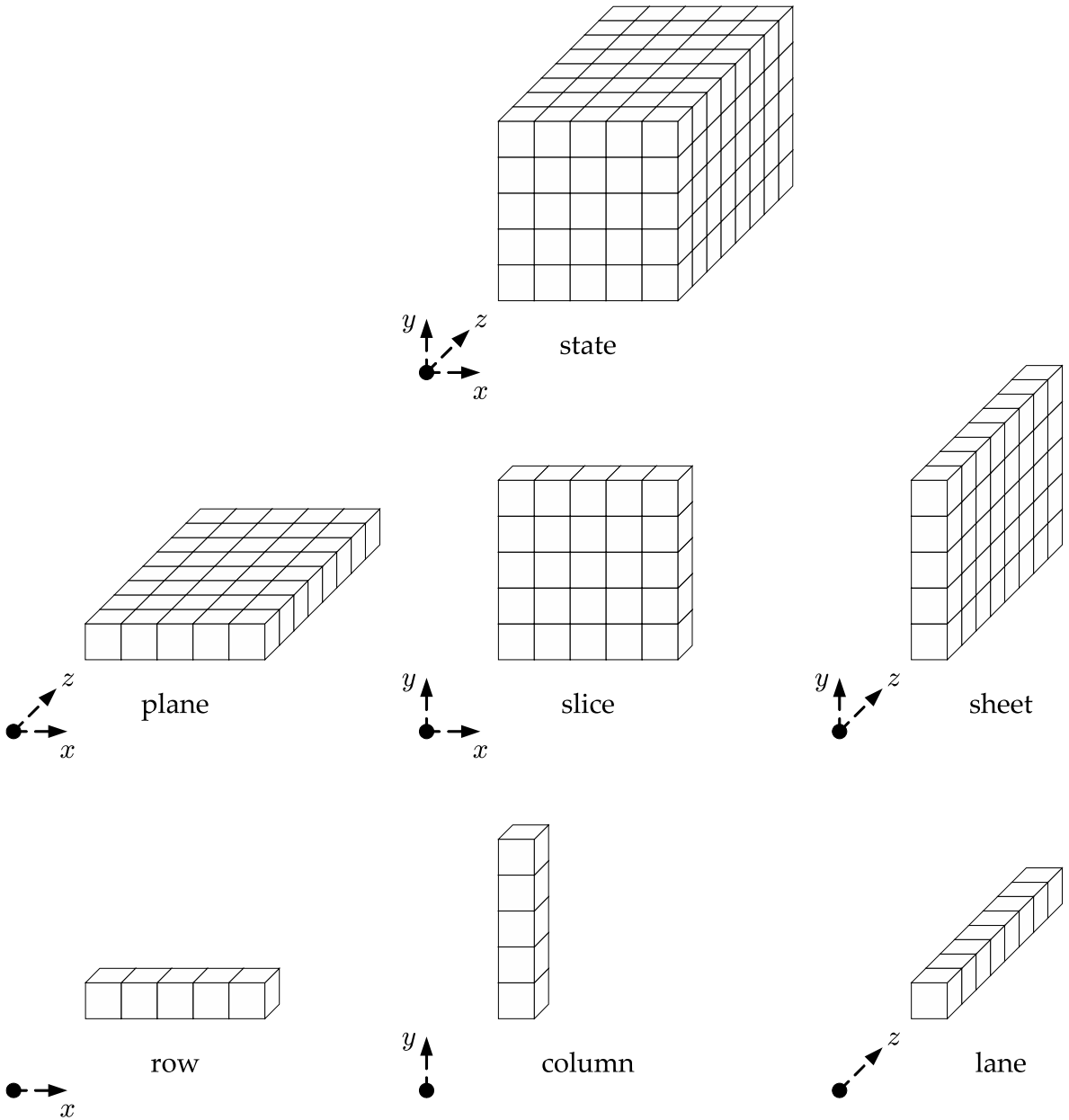
State-Size $= 64 \times 25$
$= 1600$ bits

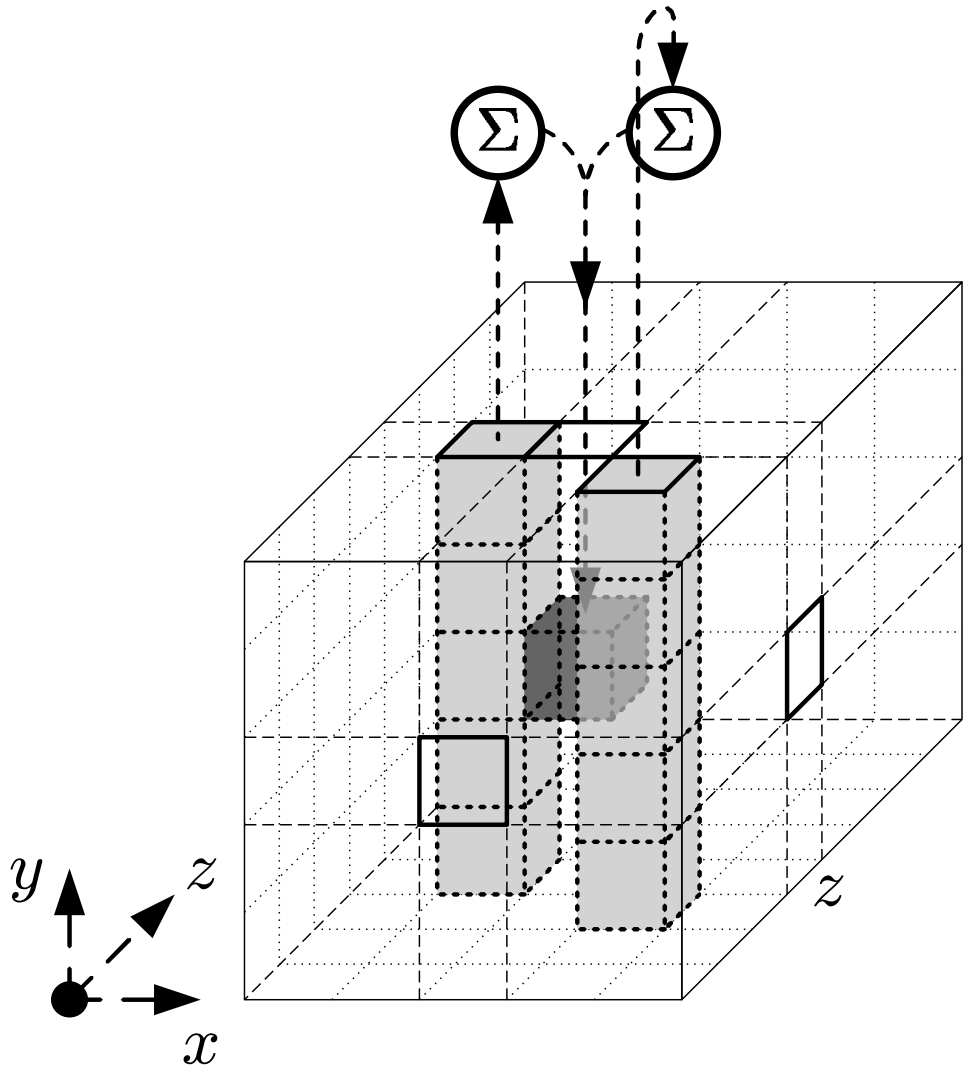
Inside KECCAK-p Permutation

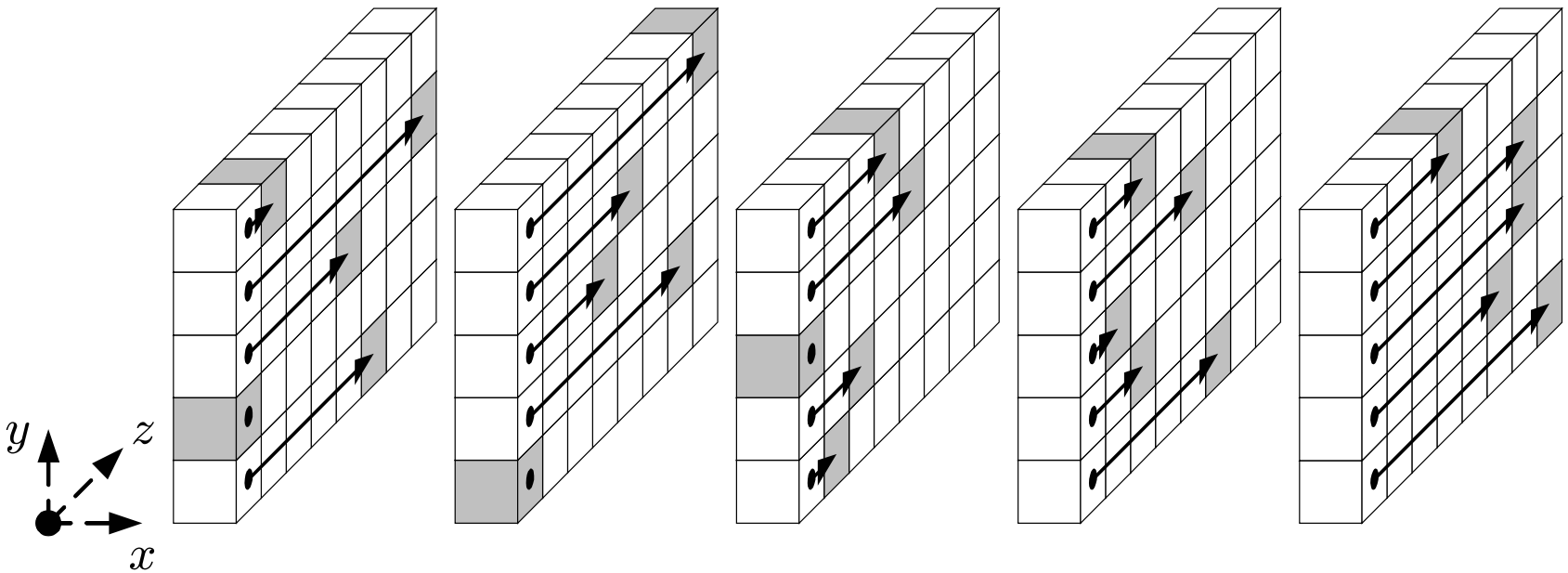


Round Constants added to destroy symmetry

Pieces of the Keccak Internal State




Σ
Σ
y
z
x
z


y
z
x