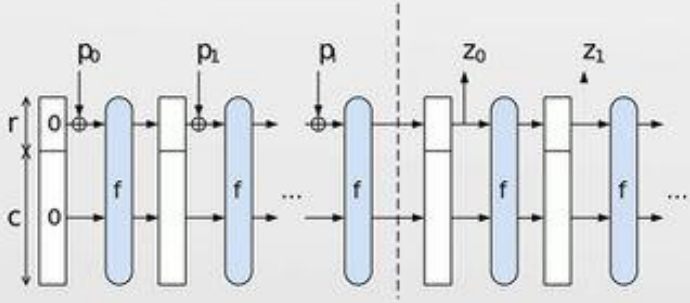


# SHA-3



II4031 Kriptografi dan Koding

# SHA-3 (Keccak)

Oleh: Dr. Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi  
Sekolah Teknik Elektro dan Informatika(STEI)

ITB

Rinaldi Munir/II4031 Kriptografi dan Koding



# Latar Belakang

- Seperti sejarah AES, *National Institute of Standards and Technology* (NIST) menyelenggarakan kompetisi terbuka untuk mengembangkan fungsi *hash* yang baru, bernama SHA-3
- SHA-3 menjadi komplementer SHA-1 dan SHA-2
- Kompetisi diumumkan pada tahun 2007 dan berakhir pada Oktober 2012 dengan memilih pemenang.

# Proses Pemilihan

- Proses pemilihan terdiri dari 2 putaran dan final
- Jumlah *submission* adalah 64 rancangan fungsi *hash*.
  
- Putaran pertama (penyisihan): dipilih 51 *submission*
- Putaran kedua (semi final): dipilih 14 *submission*
- Babak final: 5 finalis

# Finalis

1. BLAKE
2. Grøstl
3. JH
4. Keccak
5. Skein

# BLAKE

- Designers: Jean-Philippe Aumasson, Luca Henzen, Willi Meier, Raphael C.-W. Phan
- Detail: Digest sizes 224, 256, 384 or 512 bits
- Rounds 14 or 16

# Grøstl

- Designers: Praveen Gauravaram, Lars Knudsen, [Krystian Matusiewicz](#), [Florian Mendel](#), [Christian Rechberger](#), [Martin Schlaffer](#), and Søren S. Thomsen
- Detail: Digest sizes 256 and 512

# JH

- Designers: [Hongjun Wu](#)
- Detail: Digest sizes 224, 256, 384, 512

# Keccak

- Designers: [Guido Breton](#), Joan Daemen, [Michaël Peeters](#) and [Gilles Van Assche](#).
- Detail: [Digest sizes](#) arbitrary

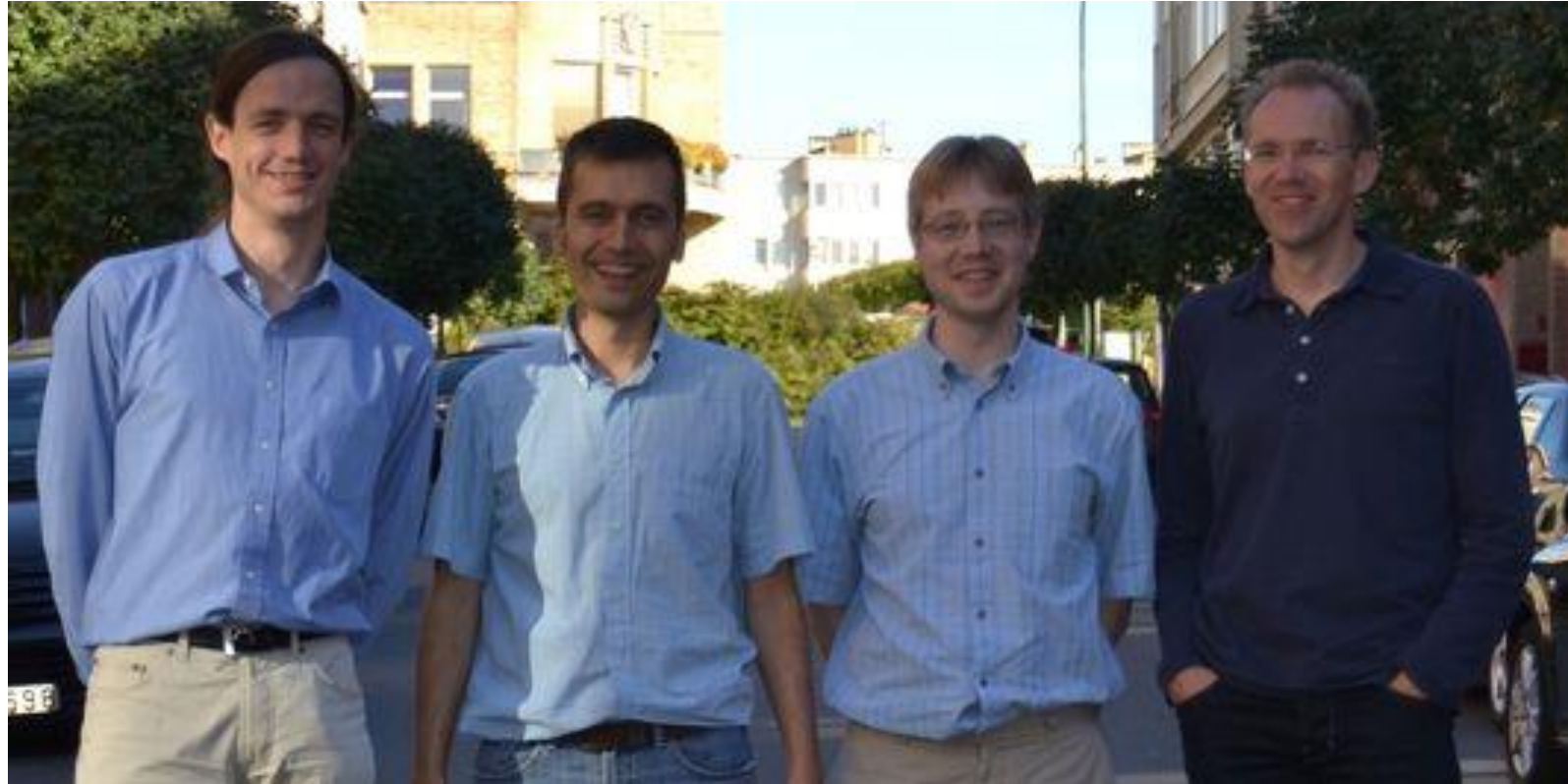


# SKEIN

- Designers: [Bruce Schneier](#), [Stefan Lucks](#), [Niels Ferguson](#), [Doug Whiting](#), [Mihir Bellare](#), [Tadayoshi Kohno](#), [Jon Callas](#) and [Jesse Walker](#).
- Detail: [Digest sizes](#) arbitrary
- Rounds: 72 (256 & 512 block size), 80 (1024 block size)

dan pemenangnya adalah...

## Keccak



[Guido Breton](#), Joan Daemen, [Michaël Peeters](#) and [Gilles Van Assche](#).

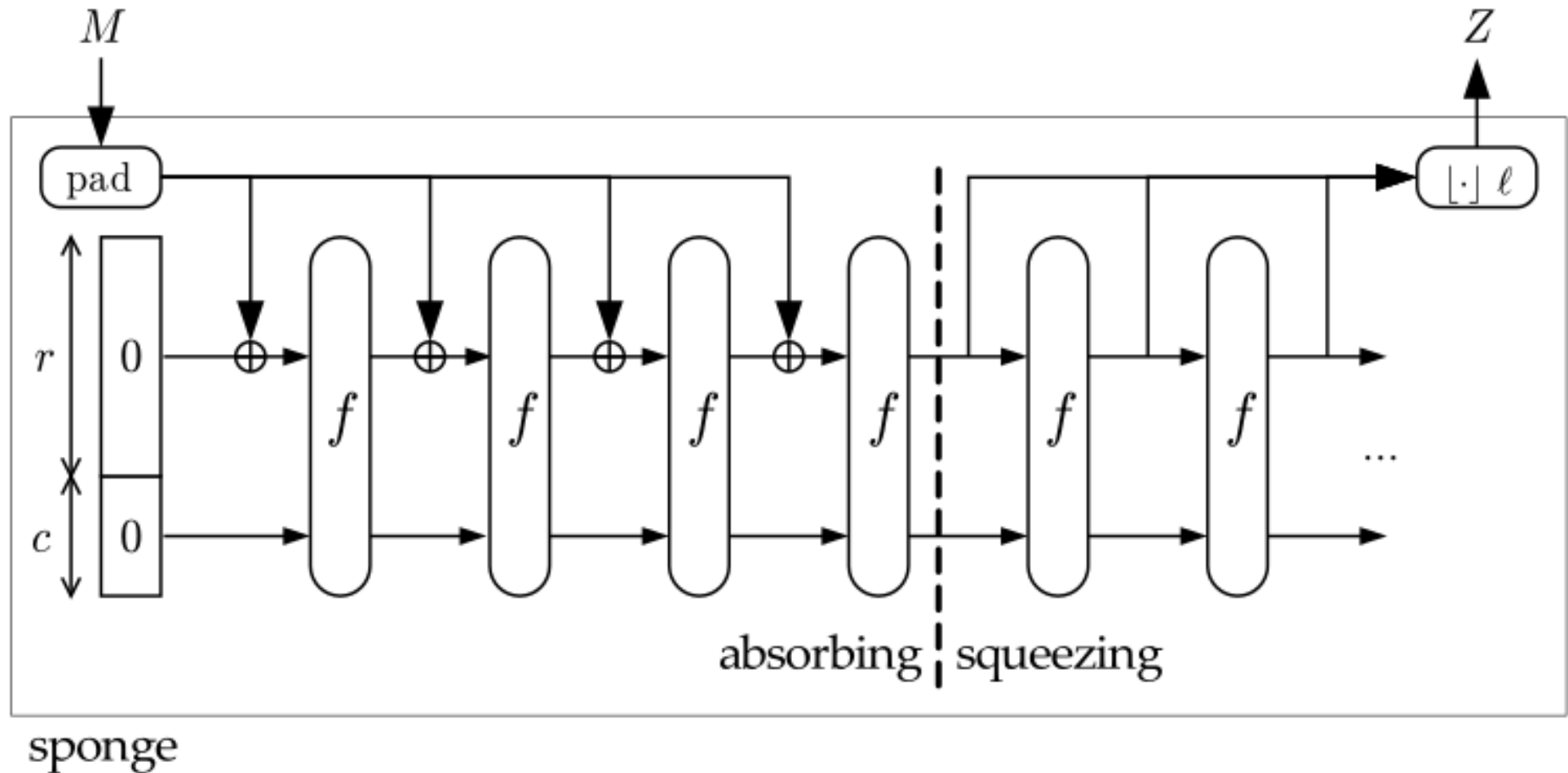
Keccak terpilih sebagai SHA-3

# Sekilas Keccak

- Nama 'Keccak' berasal dari kata 'Kecak', sebuah tari dari Bali.
- Keccak berbeda dari finalis SHA3 lainnya dalam hal menggunakan konstruksi 'spons' (*sponge construction*). Jika desain lainnya bergantung pada 'fungsi kompresi, Keccak menggunakan fungsi non-kompresi untuk menyerap dan kemudian 'memeras' *digest*.
- Desain Keccak berbeda dari pendekatan yang ada. NIST merasa bahwa dalam kasus ini, yang berbeda adalah lebih baik.



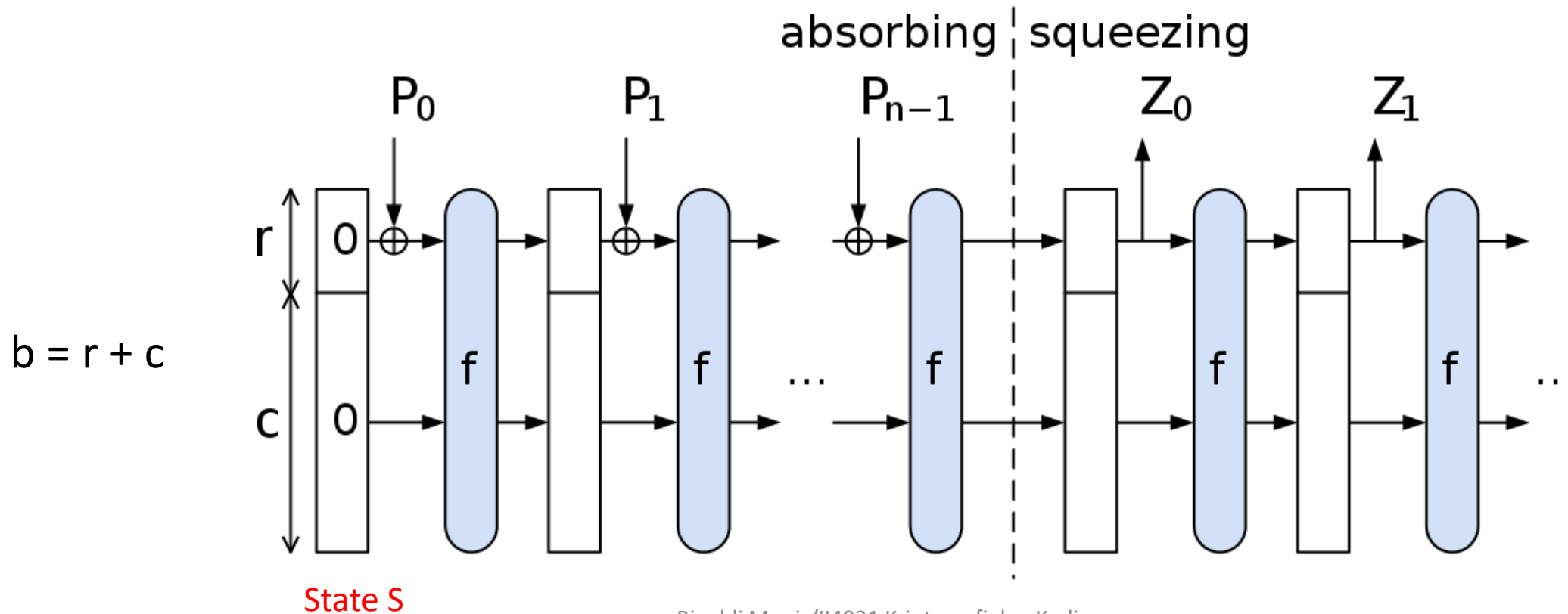
## Konstruksi spon



Praproses:

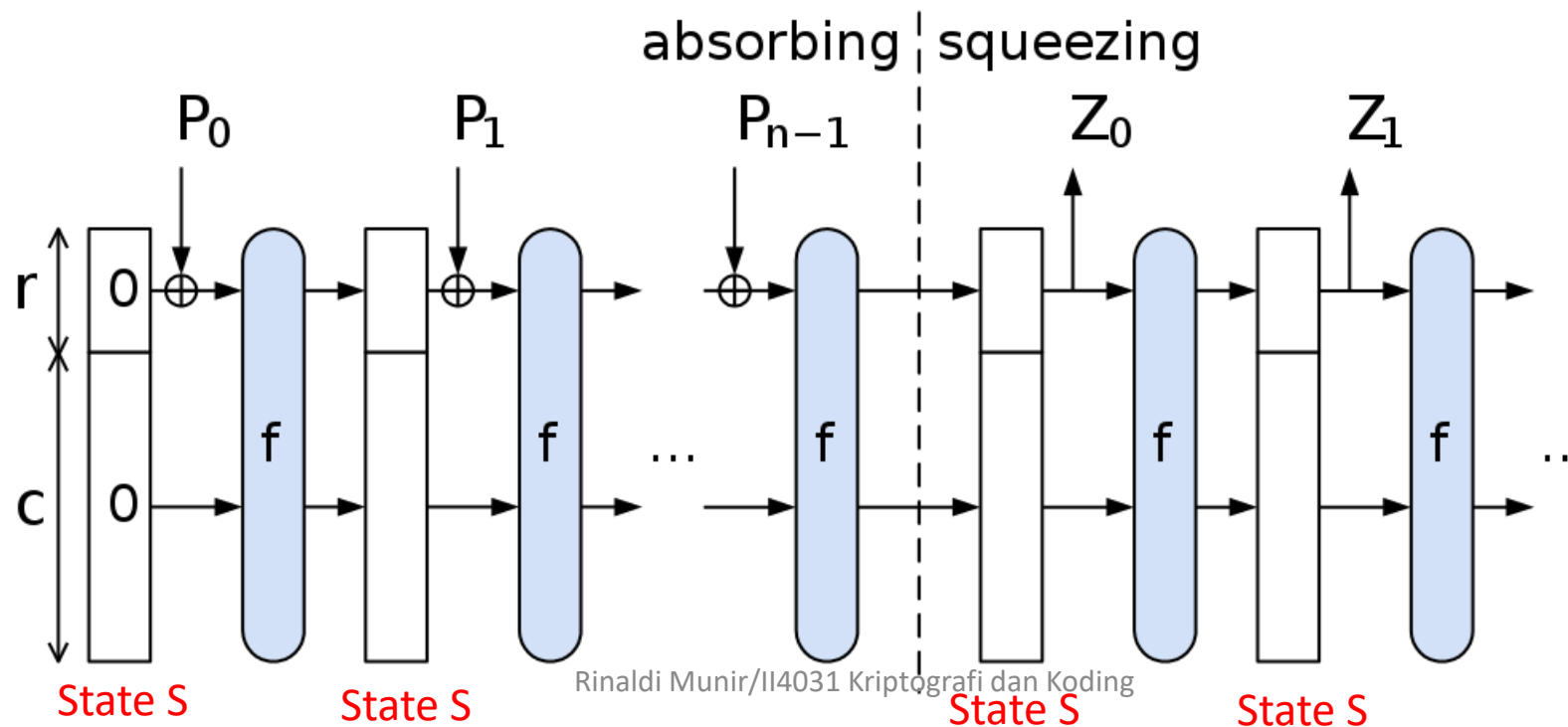
- Misalkan panjang *digest* yang diinginkan adalah  $d$  bit.
- Pertama, pesan  $M$  ditambah dengan bit-bit pengganjal (*padding*) menjadi string  $P$  sehingga habis dibagi dengan  $r$  atau  $n = \text{length}(P)/r$

- Selanjutnya,  $P$  dipotong menjadi blok-blok  $P_i$  berukuran  $r$ -bit.
- Kemudian,  $b$ -bit dari peubah status (*state*)  $S$  diinisialisasi menjadi nol dan konstruksi spons berlangsung dalam dua fase:



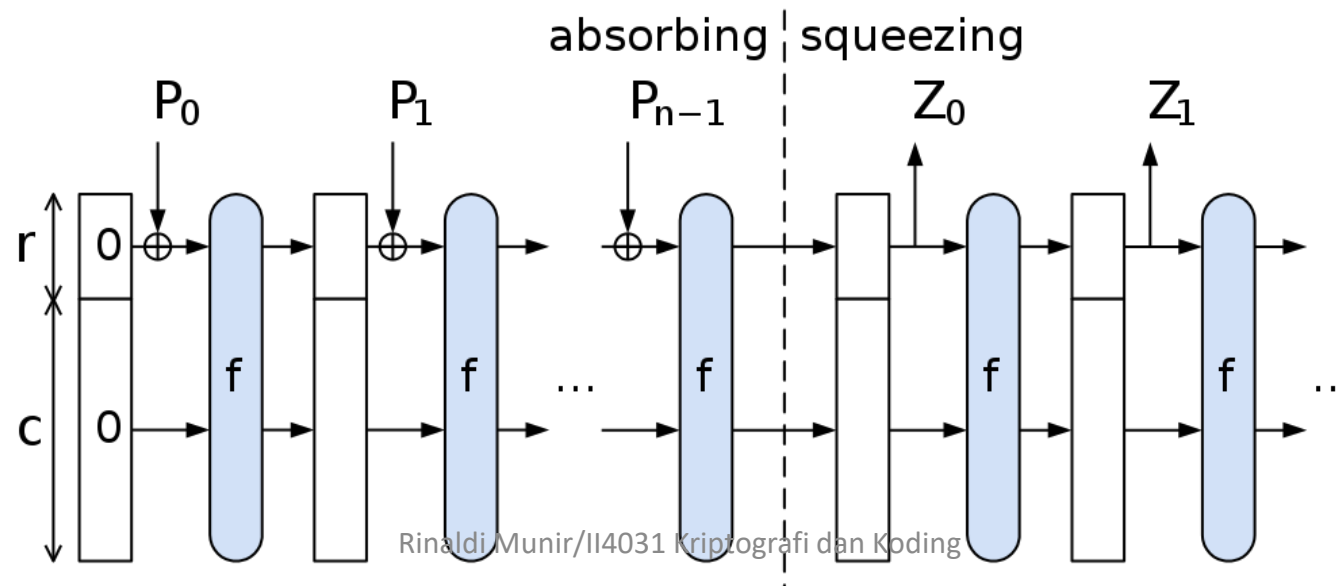
## Fase penyerapan (*absorbing*)

- Untuk setiap blok masukan  $P_i$  berukuran  $r$ -bit, XOR-kan dengan  $r$ -bit pertama dari *state*  $S$ , lalu hasilnya dimasukkan ke dalam fungsi permutasi  $f$  untuk menghasilkan *state* baru  $S$ .
- Bila semua blok masukan selesai diproses, konstruksi spons beralih ke fase pemerasan (*squeezing*).



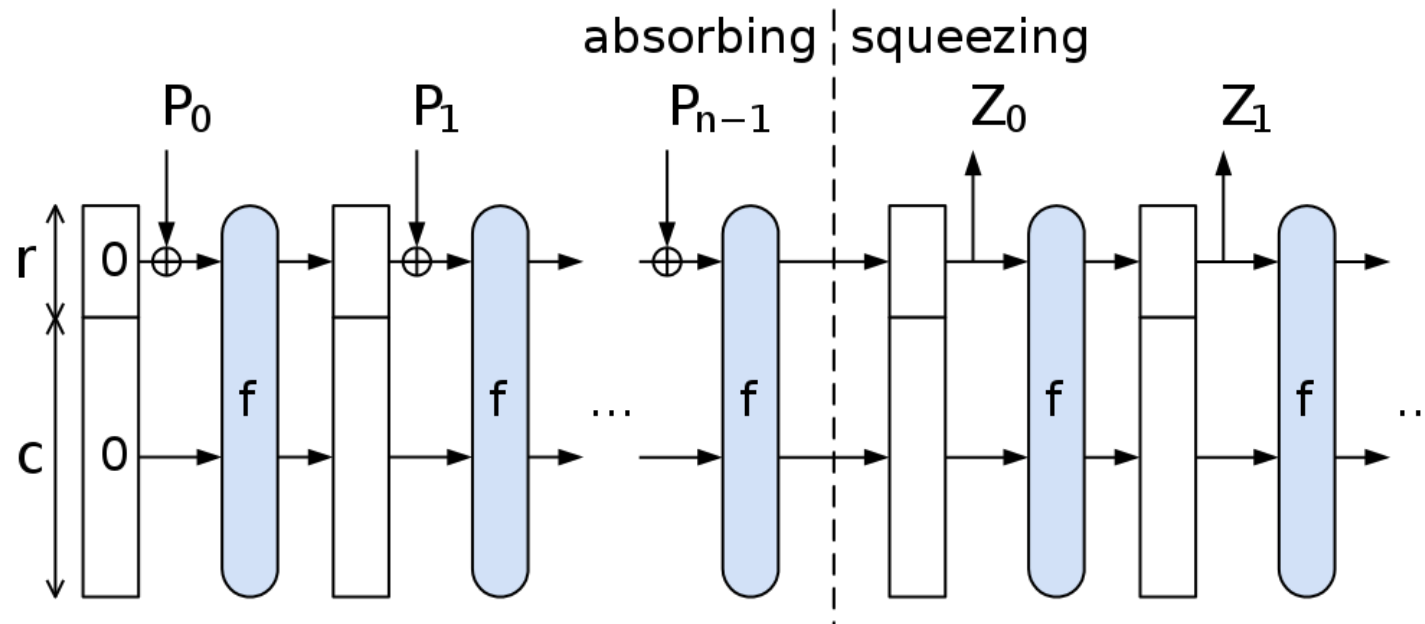
## Fase pemerasan (*squeezing*)

- *Message digest* akan disimpan di dalam  $Z$ .
- Inisialisasi  $Z$  dengan string kosong (*null string*).
- Selagi panjang  $Z$  belum sama dengan  $d$ ,  $r$ -bit pertama dari *state*  $S$  disambungkan (*append*) ke  $Z$ .
- Jika panjang  $Z$  masih belum sama dengan  $d$ , masukkan ke dalam fungsi permutasi  $f$  menghasilkan *state* baru  $S$ .





- Perhatikan bahwa  $c$  bit terakhir dari *state* tidak pernah terpengaruh secara langsung oleh blok masukan dan tidak pernah mengeluarkan luaran selama fase pemerasan. Hal ini untuk mencegah terjadinya kolisi.



- Spesifikasi Keccak (termasuk *source code*) dapat dilihat di: [http://keccak.noekeon.org/specs\\_summary.html](http://keccak.noekeon.org/specs_summary.html)

## Contoh *message digest* dengan Keccak-256

keccak256("halo")=

51e5ddea5dcdaa85bc8623b8ac163bed5c3b00e9e2ceaeca78f7f3cd8016d836

keccak256("halu")=

beccbf92062e8427947bfed81a546d4ccebba76d3f002bc254e19a6d3359d144

keccak256("halo, apa kabar teman? ") =

0055d097fad321072610be3f16147533355cd1d370577a21ffae735f9da47c48

keccak("The quick brown fox jumps over the lazy dog") =

4d741b6f1eb29cb2a9b9911c82f56fa8d73b04959d3d9d222895df6c0b28aa15

**SELAMAT BELAJAR**