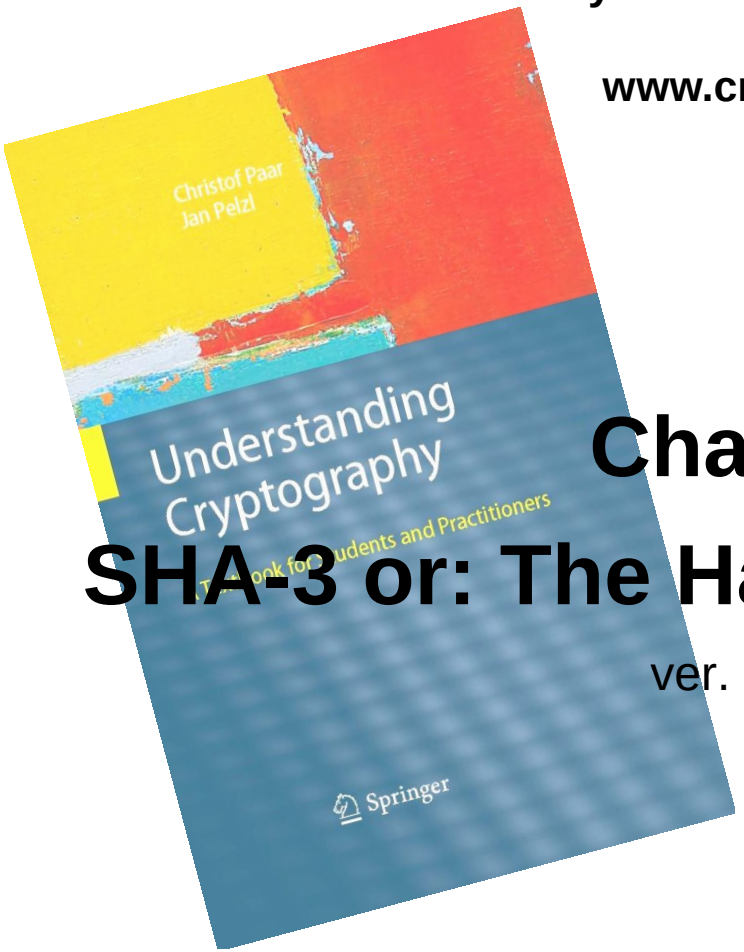
Understanding Cryptography

by Christof Paar and Jan Pelzl

www.crypto-textbook.com



Chapter 10b

SHA-3 or: The Hash Function Keccak

ver. Jun 18, 2013

These slides were prepared by Christof Paar

Some legal stuff (sorry): Terms of Use

- The slides can used free of charge. All copyrights for the slides remain with Christof Paar and Jan Pelzl.
- The title of the accompanying book “Understanding Cryptography” by Springer and the author’s names must remain on each slide.
- If the slides are modified, appropriate credits to the book authors and the book title must remain within the slides.
- It is not permitted to reproduce parts or all of the slides in printed form whatsoever without written consent by the authors.

Content of this Chapter

Fig.. 1.2 Absorbing and squeezing phase of Keccak

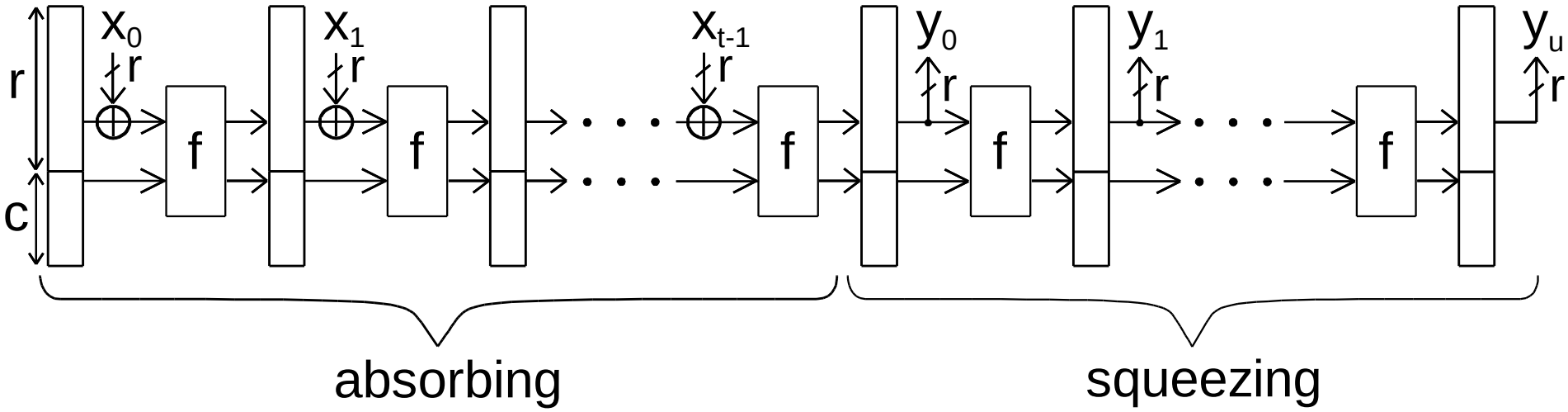


Fig. 1.3 The internal structure of Keccak

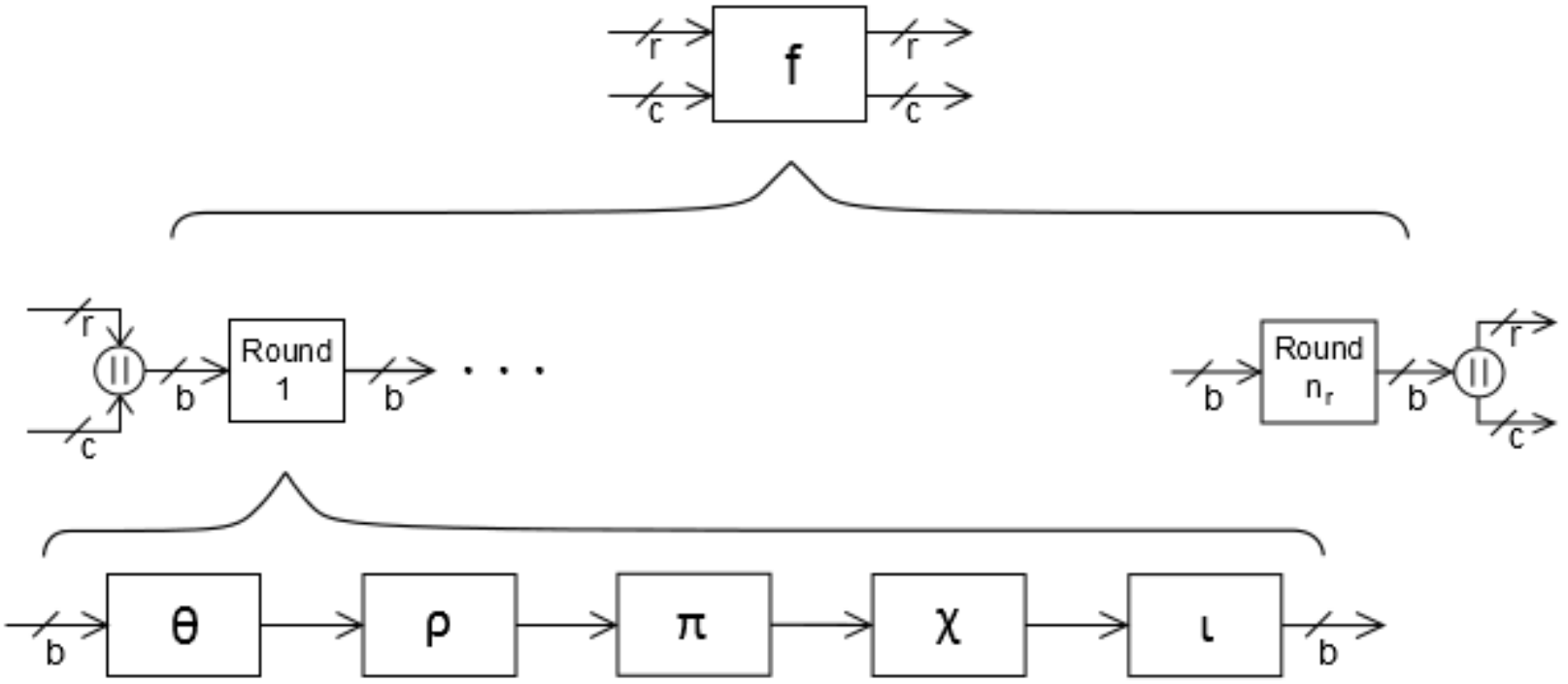


Fig. 1.4 The state of Keccak

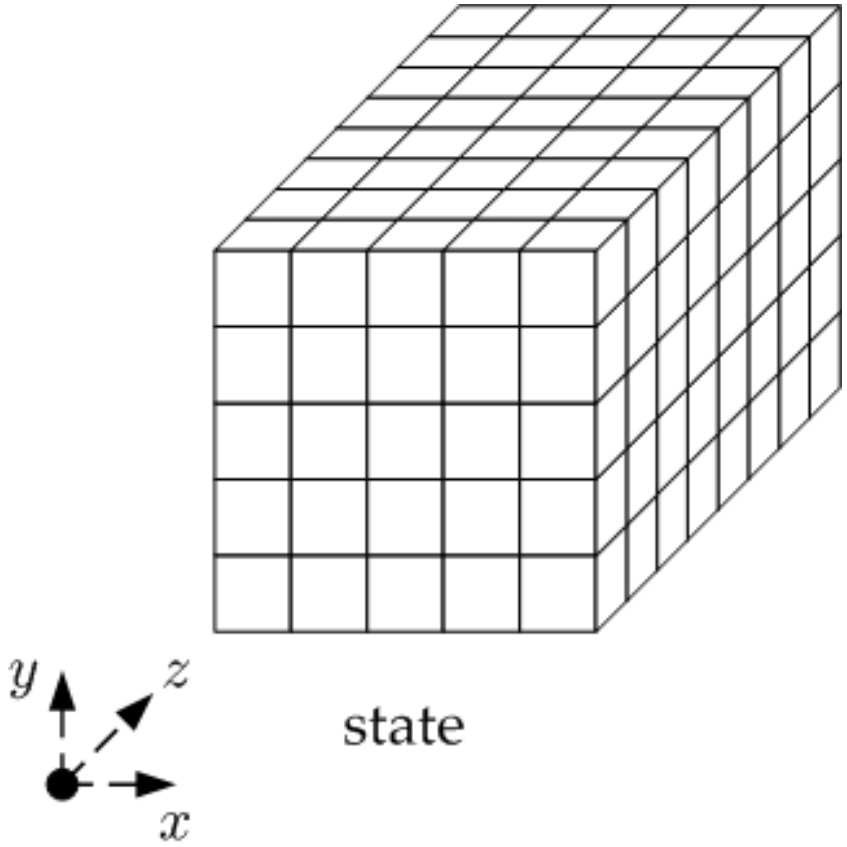


Fig. 1.5 The Theta Step of Keccak – visually

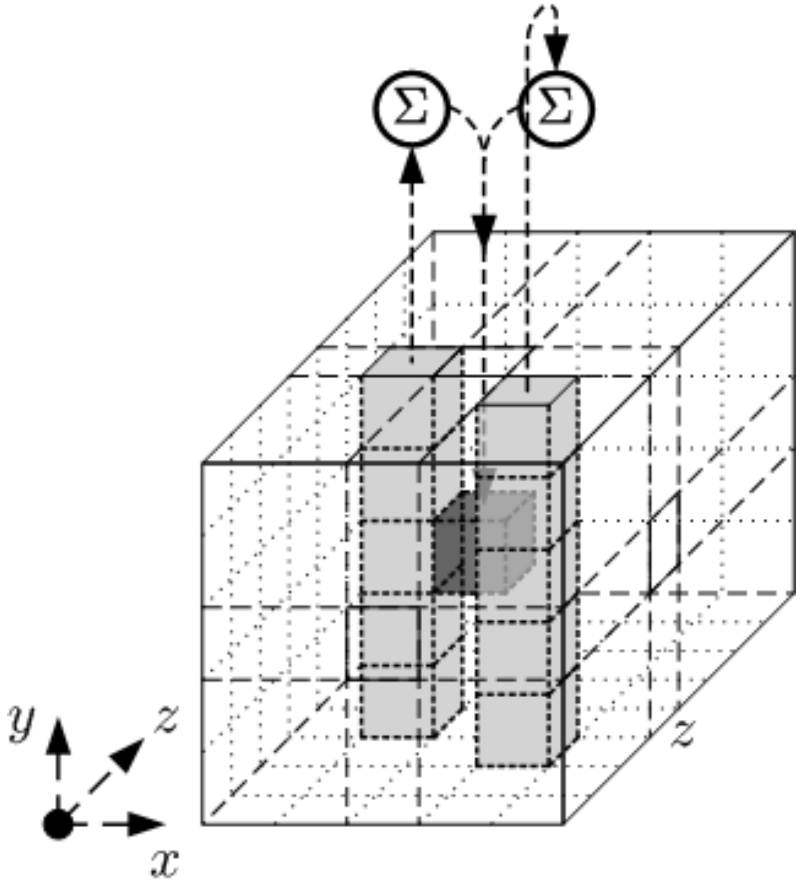


Fig. 1.5 The Theta Step of Keccak – pseudo code

- Input: state array A[x,y]
- Output: manipulated state array A[x,y]

- $C[x] = A[x,0] \oplus A[x,1] \oplus A[x,2] \oplus A[x,3] \oplus A[x,4]$ $\quad x = 0 \ldots 4$
- $D[x] = C[x-1] \oplus \text{rot}(C[x+1],1)$ $\quad x = 0 \ldots 4$
- $A[x,y] = A[x,y] \oplus D[x]$ $\quad x,y = 0 \ldots 4$

Table 1.3 The rotation constants of Keccak

	x = 3	x = 4	x = 0	x = 1	x = 2
y=2	25	39	3	10	43
y=1	55	20	36	44	6
y=0	28	27	0	1	62
y=4	56	14	18	2	61
y=3	21	8	41	45	15

Fig. 1.6 The Chi Step of Keccak

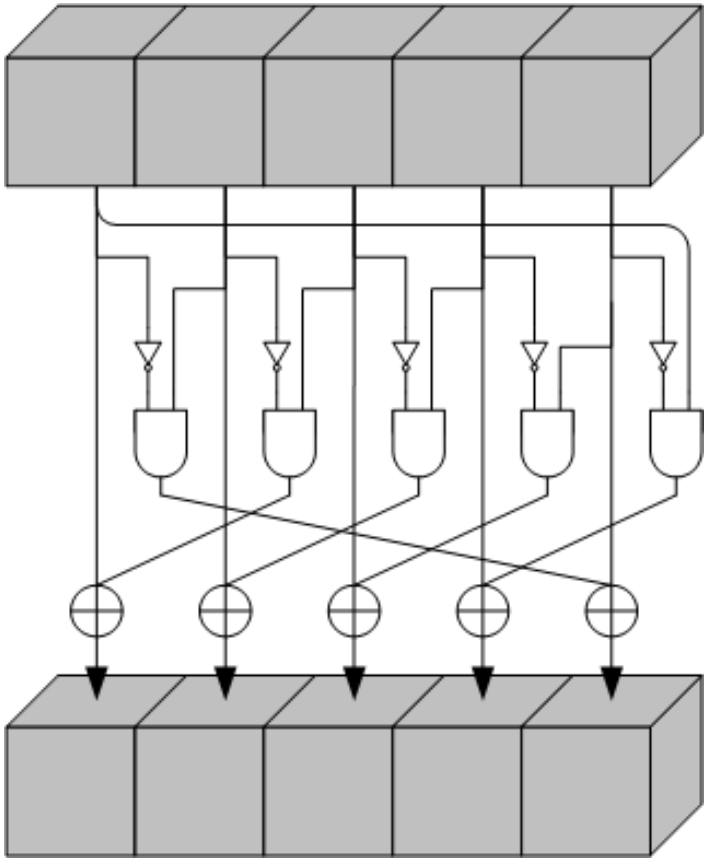


Table 1.4 The round constants of Keccak

RC[0] = 0x0000000000000001	RC[12] = 0x000000008000808B
RC[1] = 0x0000000000008082	RC[13] = 0x800000000000008B
RC[2] = 0x800000000000808A	RC[14] = 0x8000000000008089
RC[3] = 0x8000000080008000	RC[15] = 0x8000000000008003
RC[4] = 0x000000000000808B	RC[16] = 0x8000000000008002
RC[5] = 0x0000000080000001	RC[17] = 0x8000000000000080
RC[6] = 0x8000000080008081	RC[18] = 0x000000000000800A
RC[7] = 0x8000000000008009	RC[19] = 0x800000008000000A
RC[8] = 0x000000000000008A	RC[20] = 0x8000000080008081
RC[9] = 0x0000000000000088	RC[21] = 0x8000000000008080
RC[10] = 0x0000000080008009	RC[22] = 0x0000000080000001
RC[11] = 0x000000008000000A	RC[23] = 0x8000000080008008