KECCAK/SHA3 CRYPTOGRAPHIC HASHING

Josh Wretlind

MATH 440 – Parallel Scientific Computing

11/21/2013

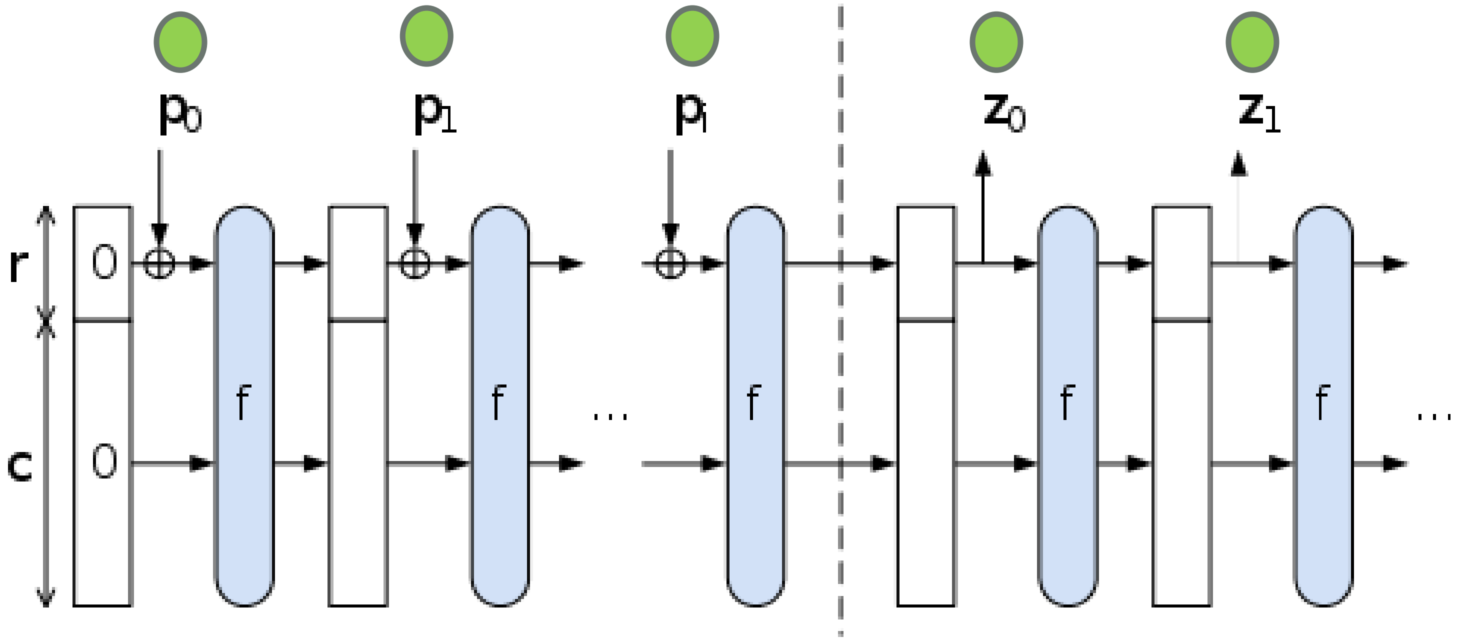
Overview

- What cryptographic hashing is
    - Performance vs Security tradeoff
- What hash functions are there, why SHA3/Keccak?

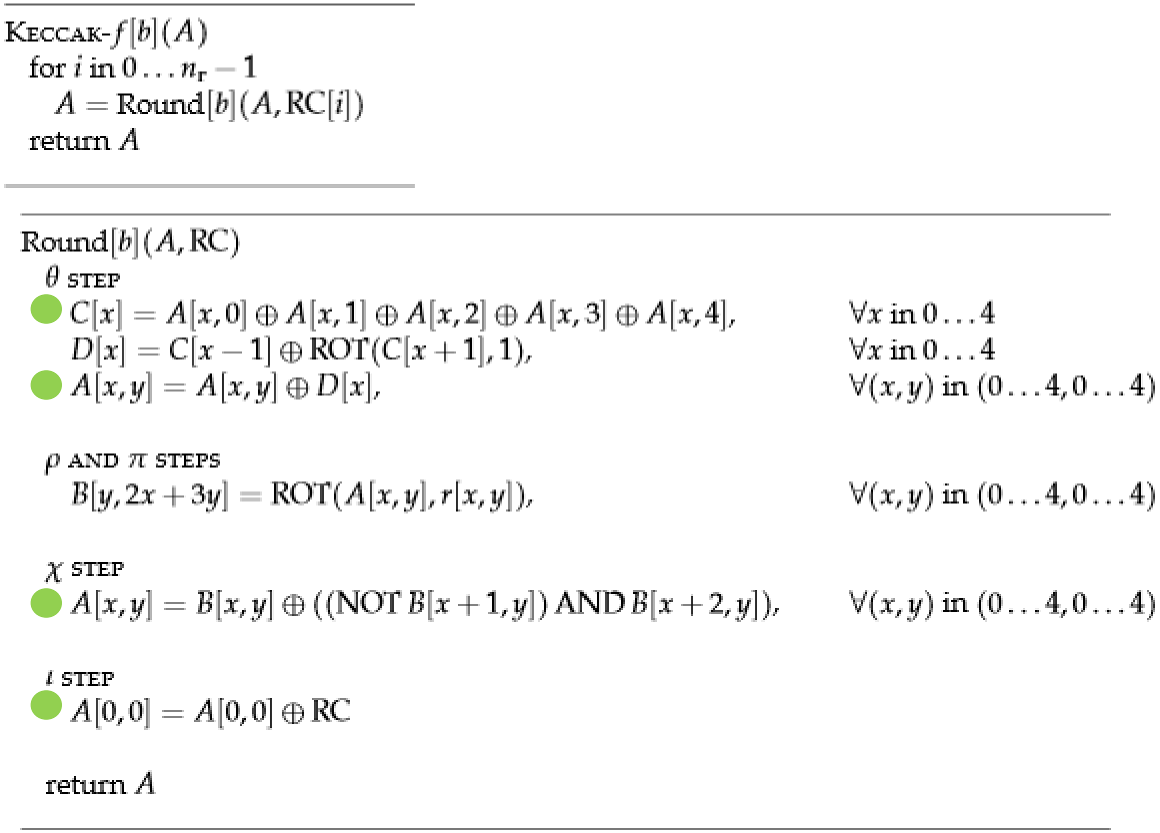
Overall SHA3

- Main driver is output width and lane size
- SHA3-X represents SHA3 with output length of X
    - Typically 256 or 512
- Lane width = 2^(lane size)
- SHA3 specifies a state array of 5*5*lane width
- Capacity is double the output width
- The rate at which bits are taken into the state is 5*5*lane width – capacity

How does SHA3 work?



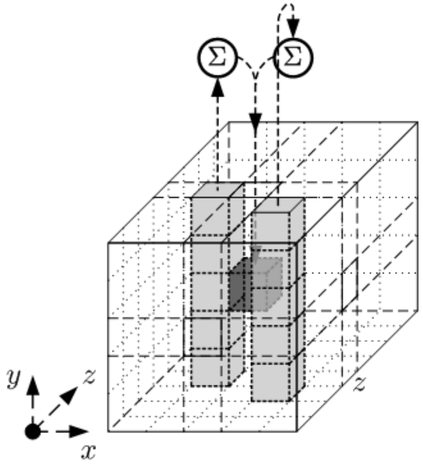
How SHA3 works pt 2

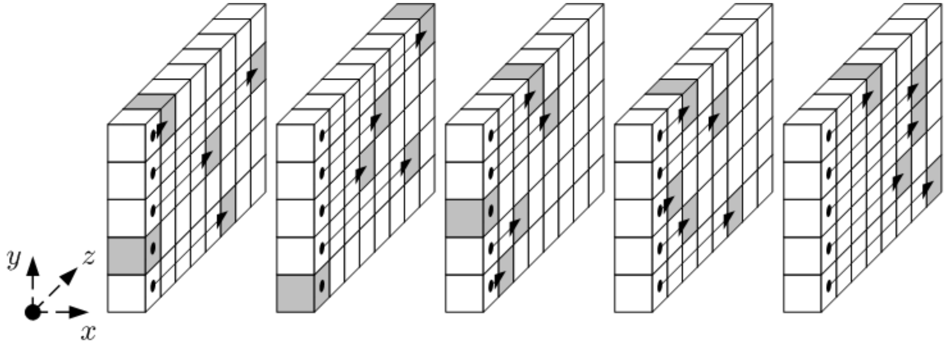


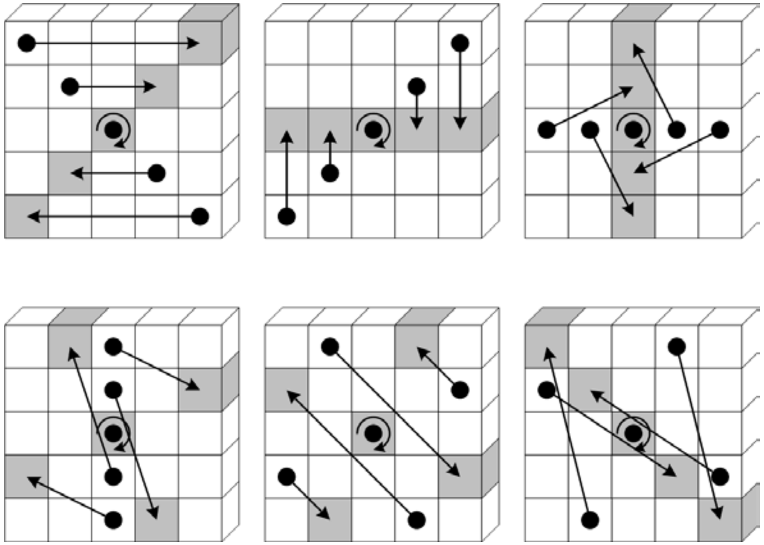
```
KECCAK-$f[b](A)$
  for $i$ in $0 \ldots n_r - 1$
    $A = \text{Round}[b](A, \text{RC}[i])$
  return $A$
```

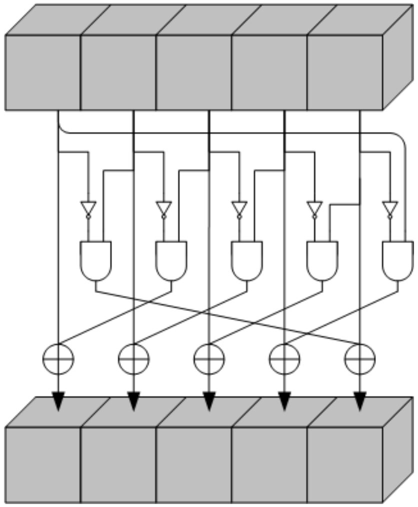
```
Round$[b](A, \text{RC})$
  $\theta$ STEP
● $C[x] = A[x,0] \oplus A[x,1] \oplus A[x,2] \oplus A[x,3] \oplus A[x,4]$,      $\forall x$ in $0 \ldots 4$
    $D[x] = C[x-1] \oplus \text{ROT}(C[x+1], 1)$,                             $\forall x$ in $0 \ldots 4$
● $A[x,y] = A[x,y] \oplus D[x]$,                                              $\forall (x,y)$ in $(0 \ldots 4, 0 \ldots 4)$

  $\rho$ AND $\pi$ STEPS
    $B[y, 2x+3y] = \text{ROT}(A[x,y], r[x,y])$,                               $\forall (x,y)$ in $(0 \ldots 4, 0 \ldots 4)$

  $\chi$ STEP
● $A[x,y] = B[x,y] \oplus ((\text{NOT } B[x+1,y]) \text{ AND } B[x+2,y])$,    $\forall (x,y)$ in $(0 \ldots 4, 0 \ldots 4)$

  $\iota$ STEP
● $A[0,0] = A[0,0] \oplus \text{RC}$

  return $A$
```

SHA3 round steps



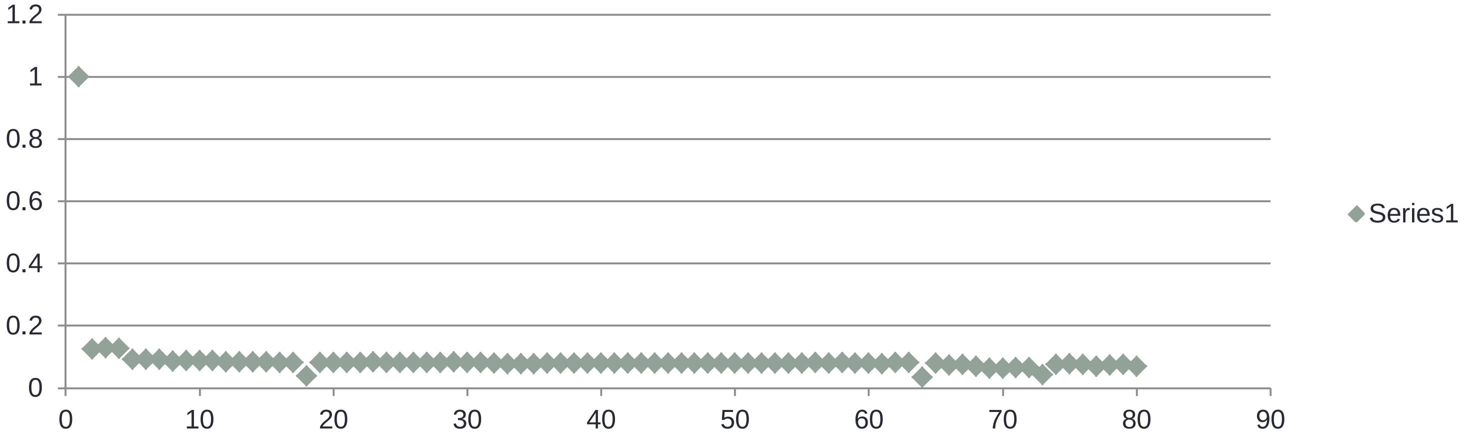


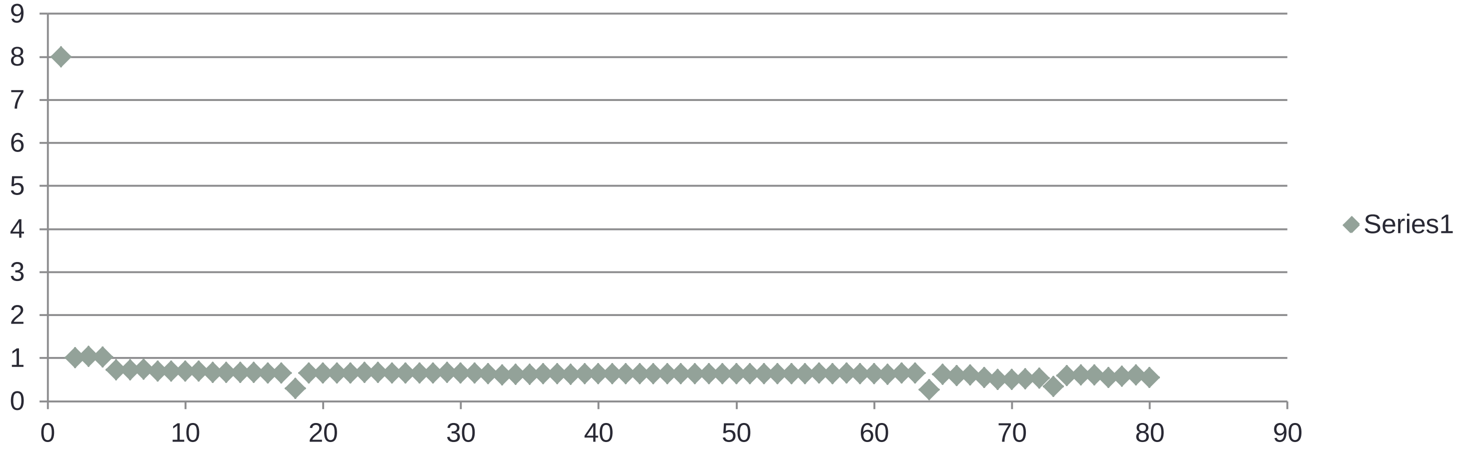




Performance Results

- Speedup using SHA256 and 1MB of input:


◆ Series1


◆ Series1