NIST 14

brief comments on some of the 14 Round 2 NIST SHA-3 hash function candidates

Stanisław Radziszowski
Rochester Institute of Technology
spr@cs.rit.edu

Gdańsk, November 2010

Block cipher based designs

AES based

- ECHO, Gilbert+ FR, wide-pipe
- Fugue, Jutla+ IBM, sponge-like
- Grøstl, Knudsen+ DK, wide-pipe
- SHAvite-3, Dunkelman+ IS, narrow-pipe

Other block cipher based

- BLAKE, Aumasson+ CH, narrow-pipe, ARX
- Hamsi $(+-)$, Küçük BE/TR, narrow-pipe, bitsliced
- Skein, Schneier+ US, narrow-pipe, ARX, Threefish

R·I·T
Department of Computer Science

Keccak

The Keccak Team, BE

Team (from STMicroelectronics and NXP Semiconductors):
Guido Bertoni, Joan Daemen (of AES fame),
Michaël Peeters, Gilles Van Assche

- Elegant, convincing design, ideas from *Grindahl*
- Runs on a $5 \times 5 \times 2^l$ cube of bits,
  recommended 1600-bit state ($l = 6$)
- Nontrivial padding, message schedule
- Same rounds all over, except constants RC
- Sponge construction

This is my favorite hash!

R·I·T
Department of Computer Science

Keccak

single round, only one nonlinear step χ

$$\mathrm{R} = \iota \circ \chi \circ \pi \circ \rho \circ \theta, \text{ with}$$

$$\theta: \quad a[x][y][z] \leftarrow a[x][y][z] + \sum_{y'=0}^{4} a[x-1][y'][z] + \sum_{y'=0}^{4} a[x+1][y'][z-1],$$

$$\rho: \quad a[x][y][z] \leftarrow a[x][y][z-(t+1)(t+2)/2],$$

$$\text{with } t \text{ satisfying } 0 \le t < 24 \text{ and } \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}^t \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \text{ in } \mathrm{GF}(5)^{2\times 2}$$

$$\text{or } t = -1 \text{ if } x = y = 0,$$

$$\pi: \quad a[x][y] \leftarrow a[x'][y'], \text{ with } \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix},$$

$$\chi: \quad a[x] \leftarrow a[x] + (a[x+1]+1)a[x+2],$$

$$\iota: \quad a \leftarrow a + \mathrm{RC}[i_r].$$

Skein

Schneier-Ferguson + team, US-UK

The main designers are well known authors
of cryptography and security books

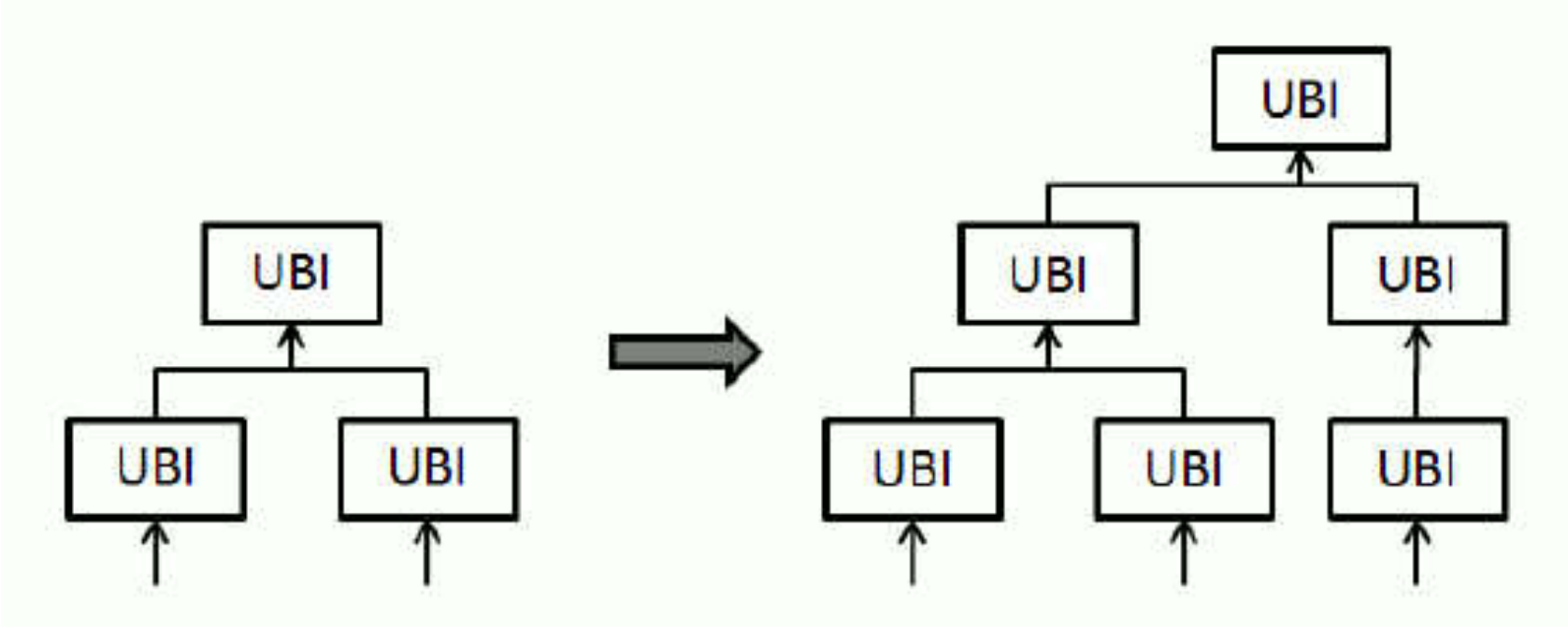
- Based on block cipher Threefish
  (Twofish competed in 2000 to become AES)
- Separate slides by John Hicks with a look inside
- Tree hashing strongly stressed
- Easy parallelizability

The only candidate among remaining 14
with easy and natural parallelizability!

Skein

tree hashing mode, tree growth

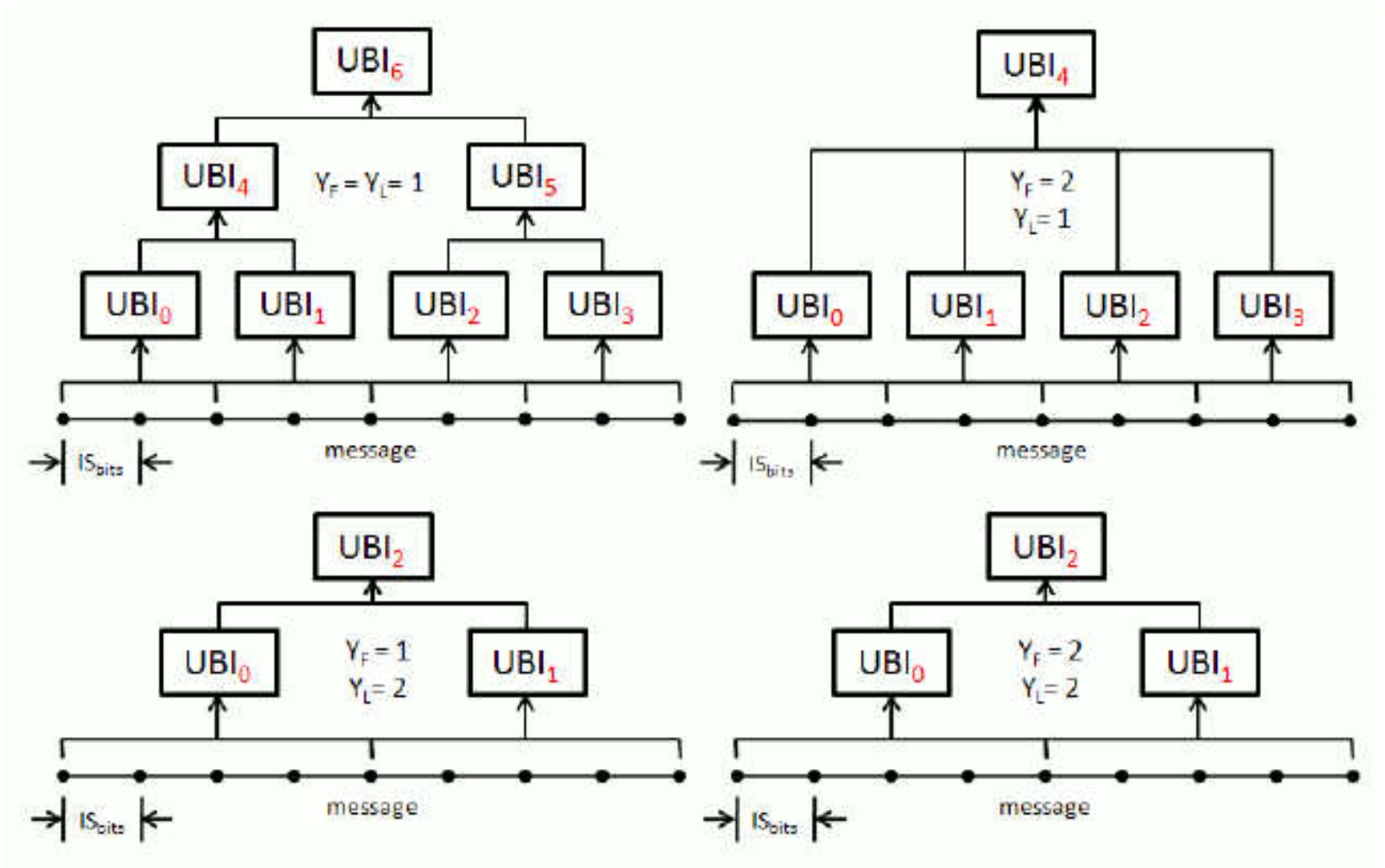
Unique Block Iteration - UBI



[Schorr 2010]

Skein

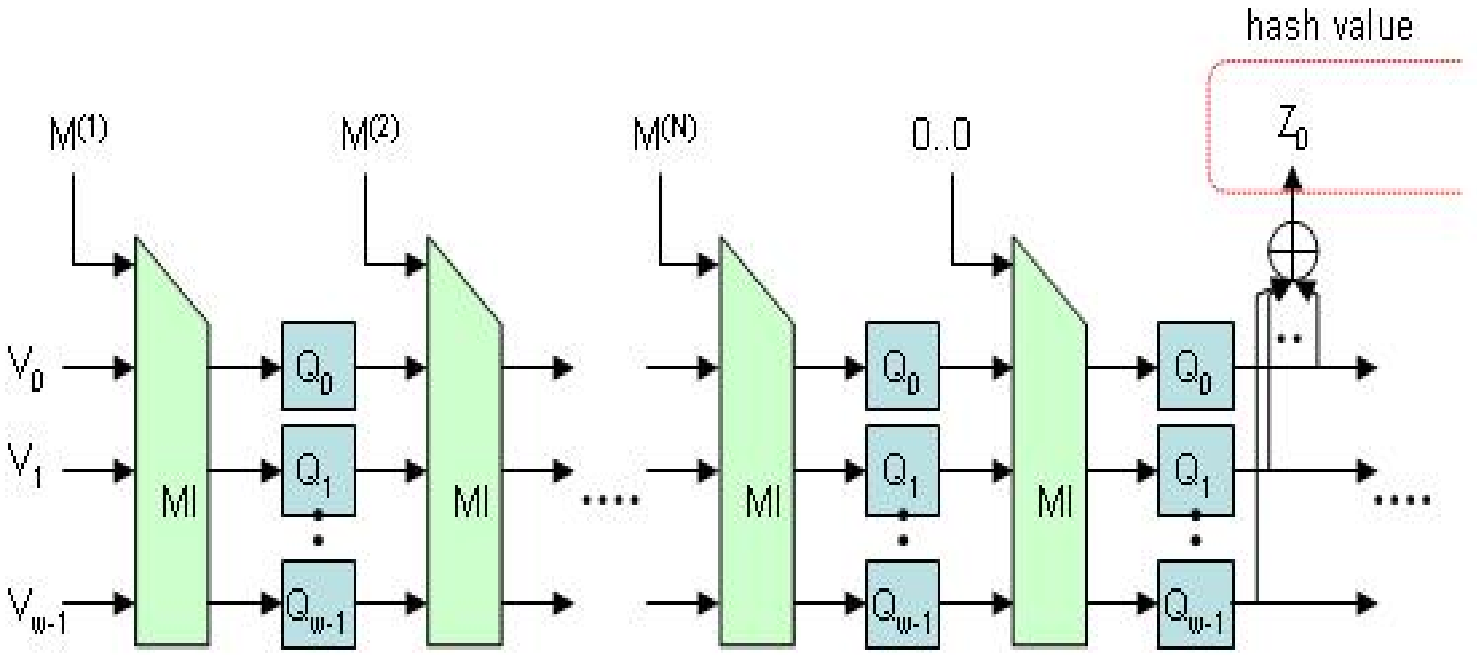
tree hashing mode, various parameters



[Schorr 2010]

Luffa

Watanabe-Sato-DeCarniere, JP/BE



- MI linear maps, Q perms, sponge-like
- Small s-boxes motivated by Serpent (almost AES to be 10 years ago)
- Black horse?

Grøstl

Knudsen+team, DK

Strong among AES based candidates

- Detailed slides by Joel Lathrop
- Wide-pipe Merkle-Damgård design
- Wide-trail design (not that clear how different from the latter)
- (512 or 1024)-bit blocks and chaining values
- (10 or 14) AES-type rounds on
  8 by (8 or 16) array of bytes
- AES S-box

Hamsi

Özgül Küçük, KU Leuven, BE

hamsi = sardela = anchovy

- Small message blocks, 32 and 64 bits
- Internal state size 512 and 1024 bits
- Message expansion via linear codes over $GF(4)$
  32 to 256 bits via [128,16,70] code
  64 to 512 bits via [256,32,131] code
  provides strong diffusion
- Sponge-like construction
- Small S-box from *Serpent*
- XOR of constants and a counter

CubeHash $r/b - h$

Daniel Bernstein, Chicago

- r rounds per each b-byte block, h-bit hash
  recommended $r = 16, b = 32$, sponge construction

  new tweak on initialization/finalization with less rounds

- Nicely coded with 5-dimensional (cube) arrays

  $$x[2][2][2][2][2] = y[32]$$

  a round has ten simple steps manipulating

  $$x_{ijklm} = x[i][j][k][l][m]$$

  with addition modulo 2^{32},
  word rotation, swap and XOR.

- Subject of vigorous discussions on the NIST hash-forum,
  perhaps the most studied among all candidates

BMW - Blue Midnight Wish

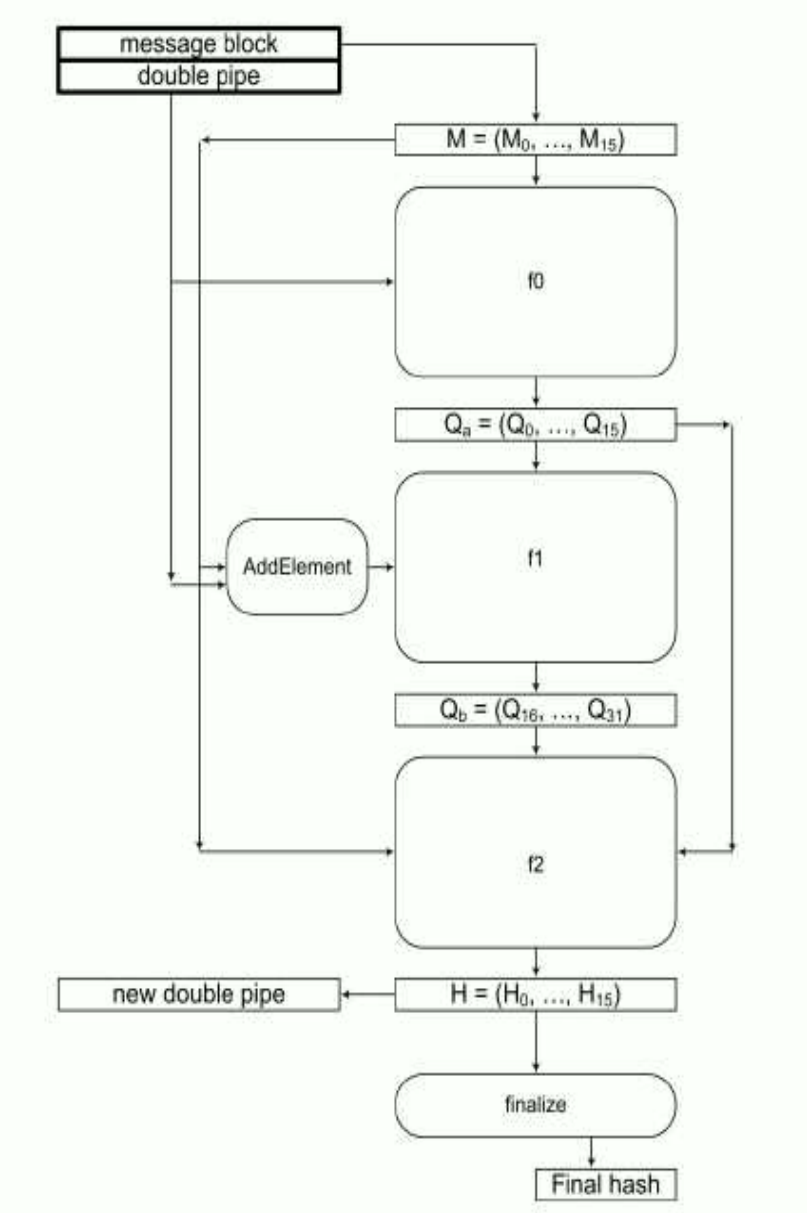
team from NTNU Trondheim, NO

Danilo! Gligoroski, Vlastimil Klima,
Svein Johan Knapskog and the team from
the Norwegian University of Science and Technology

- Double-pipe expansion
- Very complicated details of specification
- Compression: non-linear expansion followed by folding

BMW - Blue Midnight Wish

structure



References

containing pointers to many other references

- NIST report NISTIR 7620, Status Report on the First Round of the SHA-3 Cryptographic Hash Algorithm Competition, September 2009
  `http://csrc.nist.gov/groups/ST/hash`
- The Second SHA-3 Candidate Conference, Santa Barbara, CA, Aug. 23-24, 2010
  `http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/Aug2010`
- ECRYPT SHA-3 Zoo
  `http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo`
- eBASH: ECRYPT Benchmarking of All Submitted Hashes
  `http://bench.cr.yp.to/ebash.html`