Grøstl

Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz,
Florian Mendel, Christian Rechberger,
Martin Schläffer, Søren S. Thomsen

www.groestl.info

First SHA-3 Candidate Conference, 2009

MAT, DTU
IAIK, TU Graz

The Grøstl Hash Function

- Grøstl is FAST
- Grøstl is PROVABLY SECURE
- Grøstl is SIDE-CHANNEL RESISTANT
- Grøstl is SIMPLE
- …

The Grøstl Hash Function

- Grøstl is FAST
- Grøstl is PROVABLY SECURE
- Grøstl is SIDE-CHANNEL RESISTANT
- Grøstl is SIMPLE
- …
- Grøstl TASTES GOOD and is CO_2 NEUTRAL
- Grøstl is THE ANSWER to
  the question on life, the universe and everything.

What sets Grøstl apart:

- The team
  - Hash design experience
  - Hash cryptanalysis experience
- Solid at every level
  - Hash function → compression function → two permutations
- Simplicity of Grøstl
  - Simplicity of design
  - Simplicity of analysis
- Balanced implementation characteristics

What sets Grøstl apart:

- The team
  - Hash design experience
  - Hash cryptanalysis experience
- Solid at every level
  - Hash function → compression function → two permutations
- Simplicity of Grøstl
  - Simplicity of design
  - Simplicity of analysis
- Balanced implementation characteristics

The Grøstl Design Team





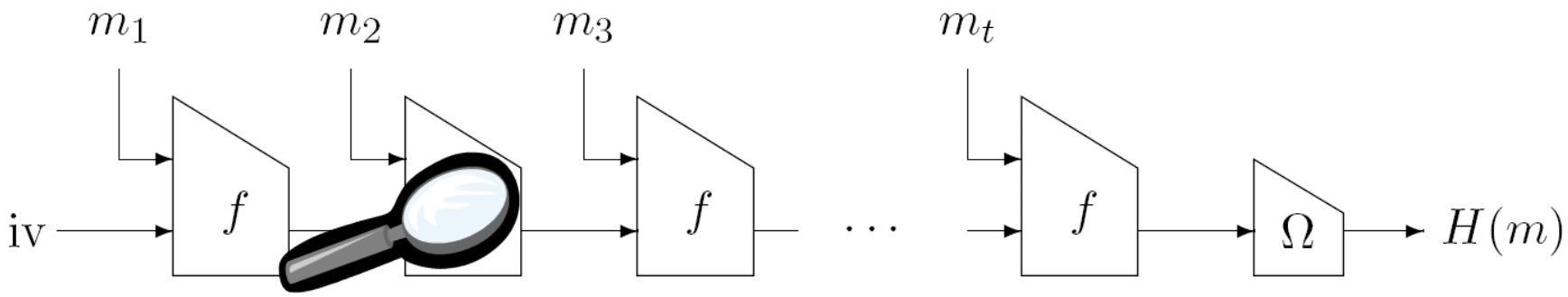


What sets Grøstl apart:

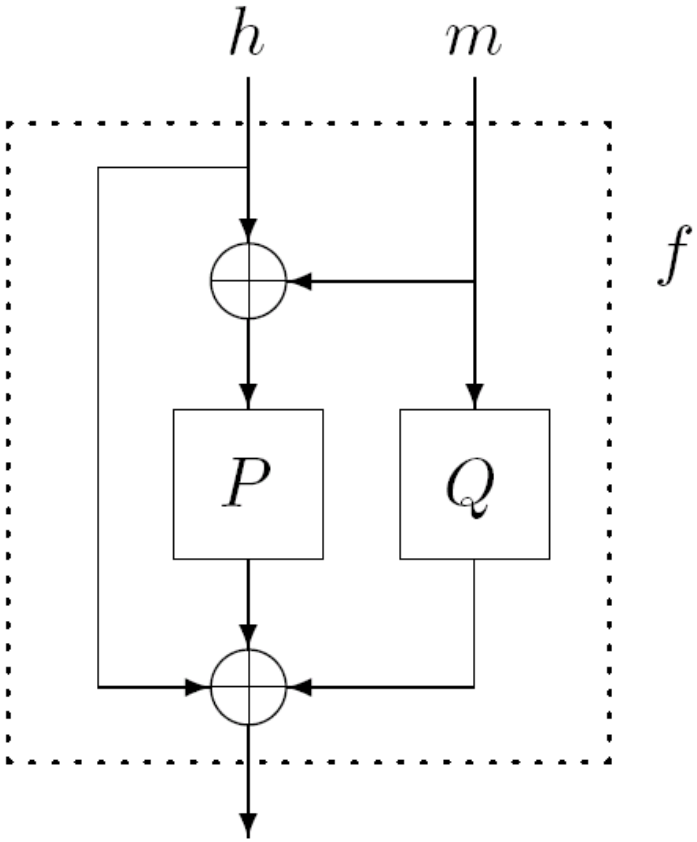
- The team
  - Hash cryptanalysis experience
  - Hash design experience
- Solid at every level
  - Hash function → compression function → two permutations

- Simplicity of Grøstl
  - Simplicity of design
  - Simplicity of analysis
- Balanced implementation characteristics

The Grøstl Hash Function



The Grøstl Compression Function

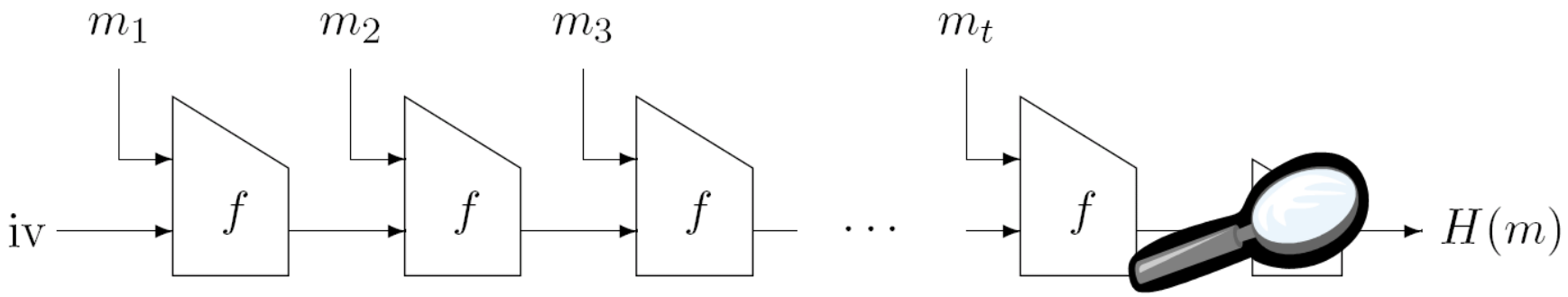


Grøstl-256:
512-bit permutations

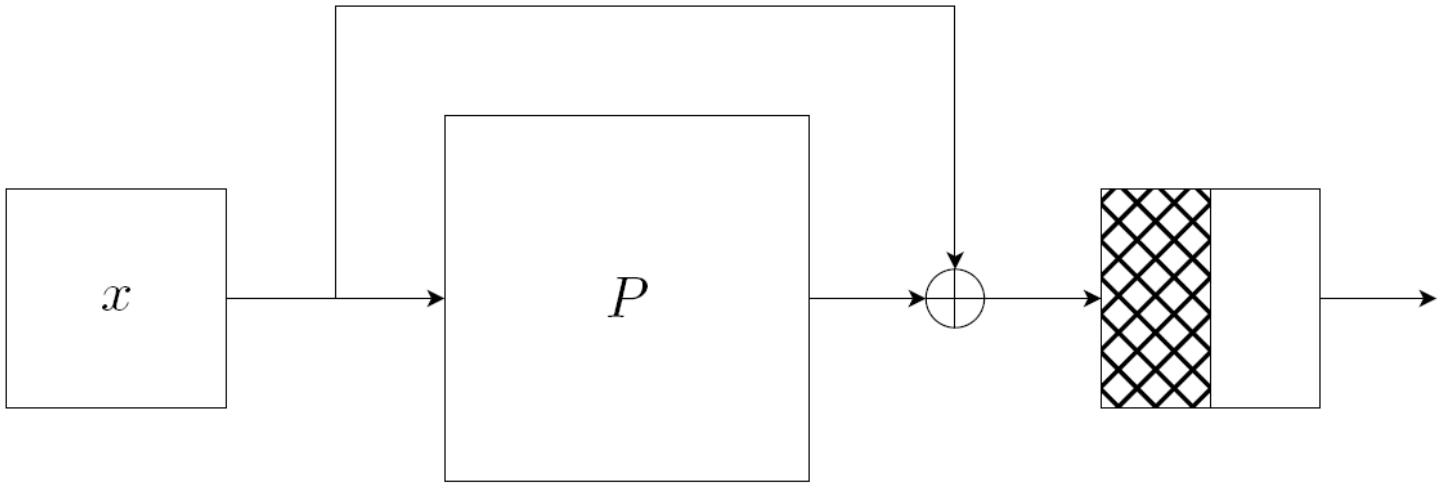
Grøstl-512:
1024-bit permutations

$$f(h, m) = P(h \oplus m) \oplus Q(m) \oplus h$$

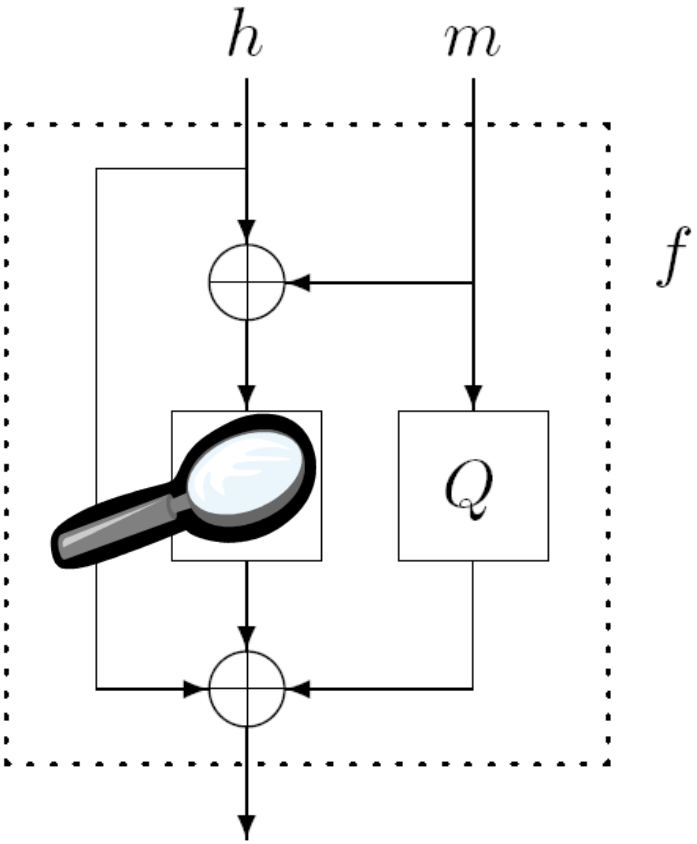
The Grøstl Hash Function



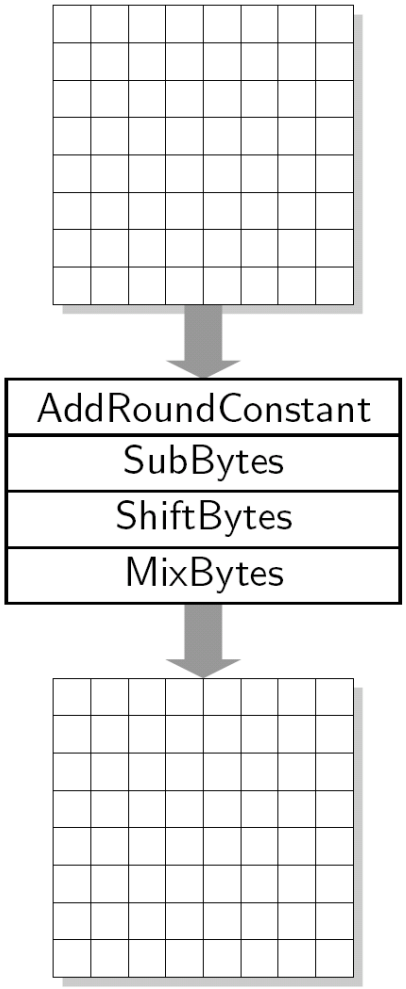
The Output Transformation



The Grøstl Compression Function



The State / Round Transformation



AES-like

Grøstl-256:
8x8 geometry
10 rounds

Grøstl-512:
8x16 geometry
14 rounds

Simple and proven solid

- Iteration
  - wide-pipe + MD + output transform
- Compression function
  - two permutations in well studied construction
- Permutation
  - “wide trail” design strategy → bounds on various attacks
  - undergone serious cryptanalysis

- Reduction proofs for collisions/preimages: done
- Reduction proofs for RO-indifferentiability: to be done

What sets Grøstl apart:

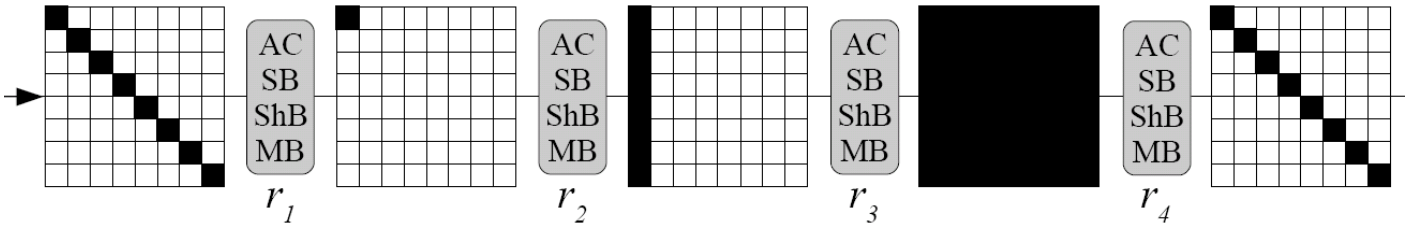
- The team
  - Hash design experience
  - Hash cryptanalysis experience
- Solid at every level
  - Hash function → compression function → two permutations
- Simplicity of Grøstl
  - Simplicity of design
  - Simplicity of analysis

- Balanced implementation characteristics

What sets Grøstl apart:

- The team
  - Hash design experience
  - Hash cryptanalysis experience
- Solid at every level
  - Hash function → compression function → two permutations
- Simplicity of Grøstl
  - Simplicity of design
  - **Simplicity of analysis**
- Balanced implementation characteristics

Simplicity of Analysis



- Grøstl allows to construct optimal (truncated) differentials, and prove bounds on them

➔Bounds on “standard” differential attack

Internal Cryptanalysis

- **Rebound-Attacks** on the compression function
  6 rounds out of 10 (FSE 2009)

- Side-effects of this work
  - Practical collision attack on Twister compress
  - Compression function attack on Cheetah-512 (8.5 out of 12)
  - Compression function attack on Maelstrom (8.5 out of 10)
  - Compression function attack on Whirlpool (7.5 out of 10)

- Freedom left for attacks on block ciphers based hashes
  - But not for Grøstl

What sets Grøstl apart:

- The team
  - Hash design experience
  - Hash cryptanalysis experience
- Solid at every level
  - Hash function → compression function → two permutations
- Simplicity of Grøstl
  - Simplicity of design
  - Simplicity of analysis
- Balanced implementation characteristics

Balanced implementation characteristics

- No preference for particular platform
- No preference for particular wordsize

- Allows table based implementations

- Allows implementation techniques without tables
  - Bit-sliced
  - Special instructions (e.g. Intel)

No Cache Attacks

Performance

	Grøstl 256	Grøstl 512
AMD Opteron (64-bit)	19,50	
Intel Core2Duo (64-bit)	21,45	30,45
Intel Core2Duo (32-bit)	23,11	36,70
Intel Pentium M 760 (32-bit)	28,90	67,40
ATMega 163 (8-bit), estimates	415,00	580,00

Numbers are cycles/byte for long messages

Further speed-ups to be expected

Hardware: many trade-offs possible, see Appendix

Summary

Summary of Grøstl

- Solid construction at every level
  - Iteration
    wide-pipe + MD + output transform
  - Compression function
    provable query complexities for collision/preimage
  - Permutation
    - “wide trail” design strategy → bounds on various attacks
    - undergone serious cryptanalysis
- More flexible implementation characteristics than SHA-2
- Easier to get confidence in

Grøstl Q&A

www.groestl.info

Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz,
Florian Mendel, Christian Rechberger,
Martin Schläffer, Søren S. Thomsen

MAT, DTU
IAIK, TU Graz

Supporting slides

The name Grøstl

An open call

What would be the name/pronunciation
of the DISH „hash“
in YOUR language/country?

- Examples:
  - Austrian/Austria: Gröstl
  - Danish/Denmark: Biksemad
  - Swiss-German/Switzerland: Rösti

Security claims / attacks

- The Grøstl hash function:

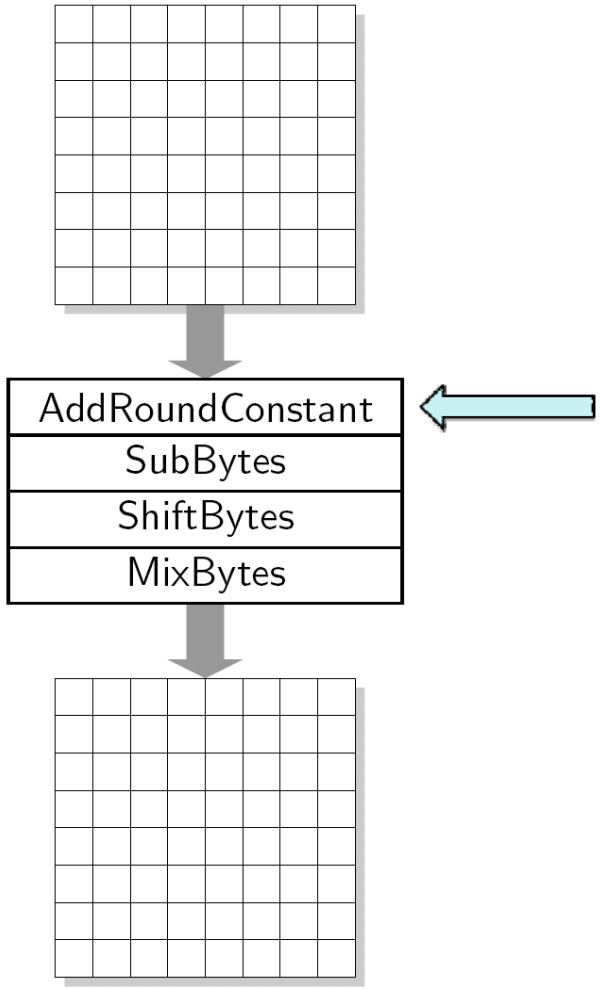
Attack type	Claimed complexity	Best known attack
Collision	$2^{n/2}$	$2^{n/2}$
d-collision	$\lg(d) \cdot 2^{n/2}$	$(d!)^{1/d} \cdot 2^{n(d-1)/d}$
Preimage	2^n	2^n
Second preimage	2^{n-k}	2^n

- The Grøstl compression function:

Attack type	Claimed complexity	Best known attack
Collision	$2^{\ell/4}$	$2^{\ell/3}$
Preimage	$2^{\ell/2}$	$2^{\ell/2}$

Supplementary Illustration for the Permutations P & Q

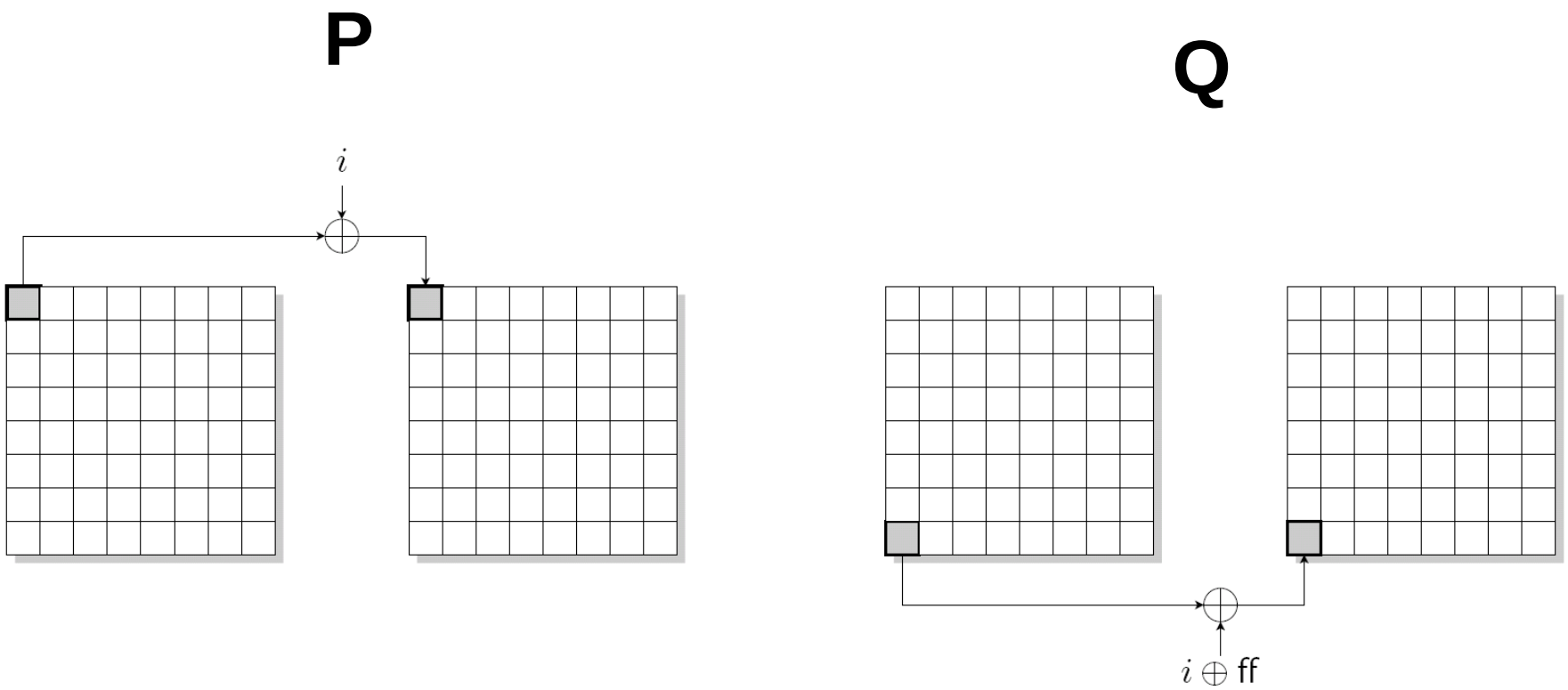
The State / Round Transformation



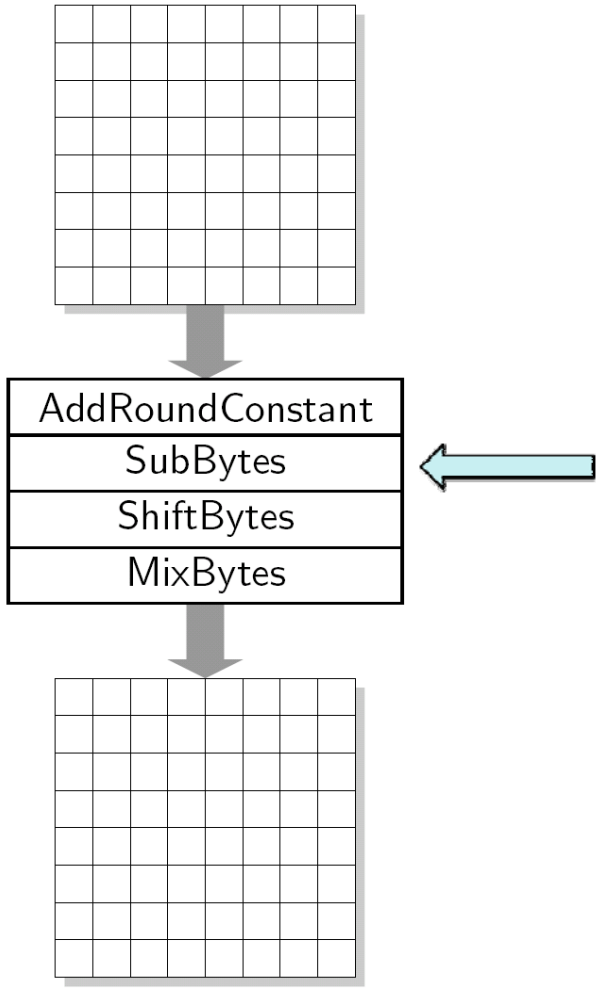
Grøstl-256:
8x8 geometry

Grøstl-512:
8x16 geometry

AddRoundConstant



The State / Round Transformation

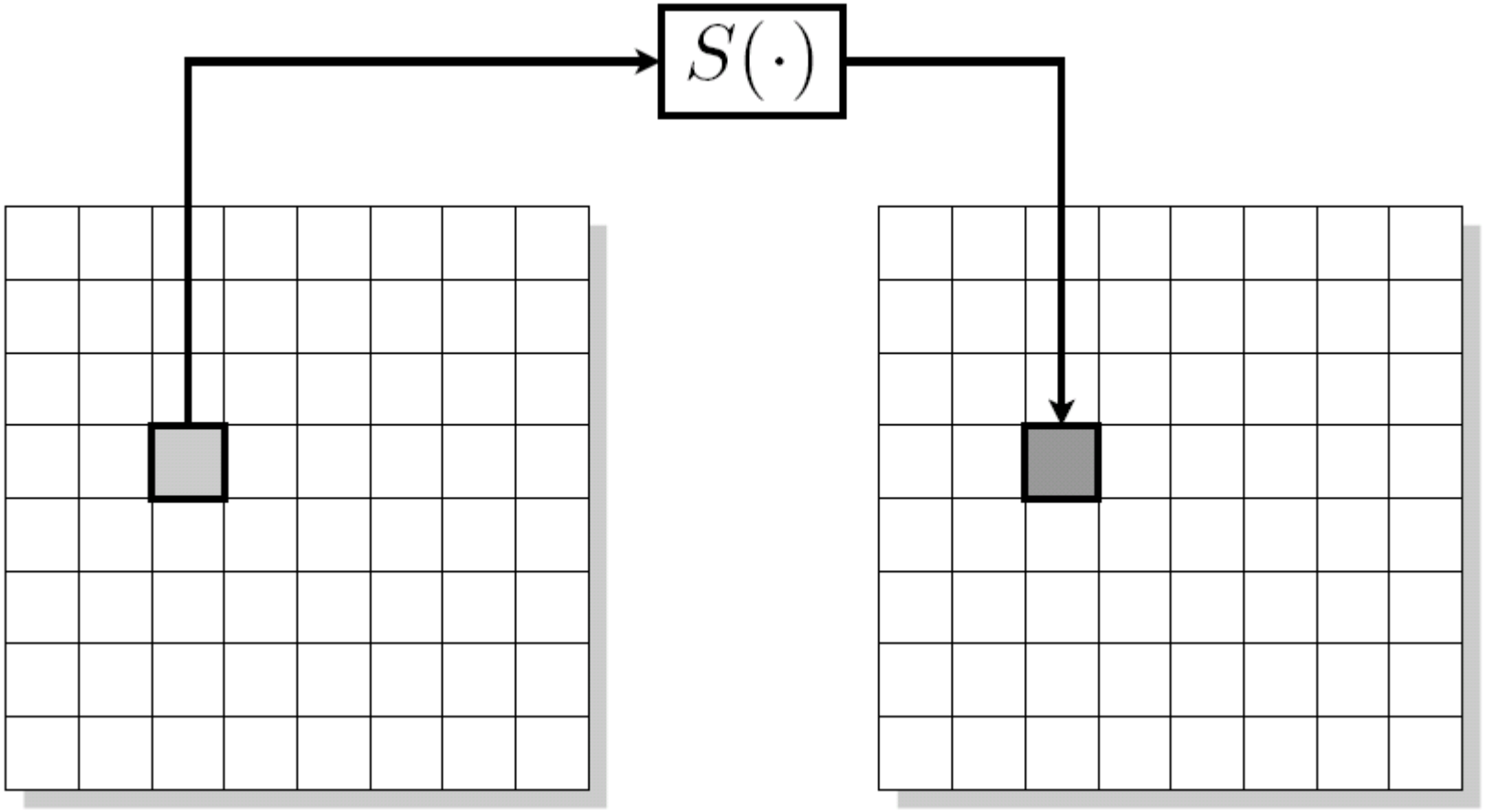


Grøstl-256:
8x8 geometry

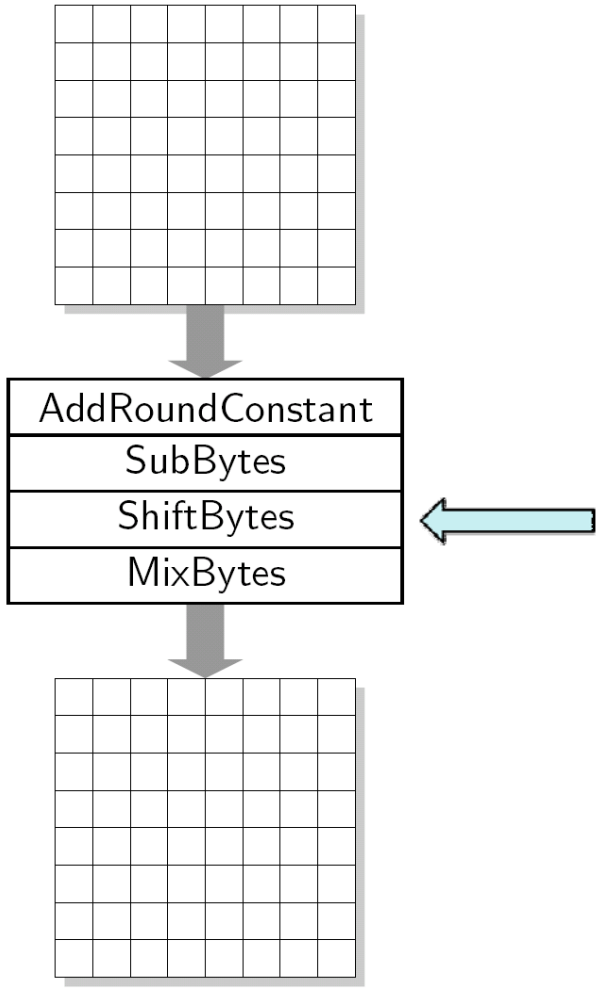
Grøstl-512:
8x16 geometry

SubBytes

same as the 8-bit AES Sbox



The State / Round Transformation

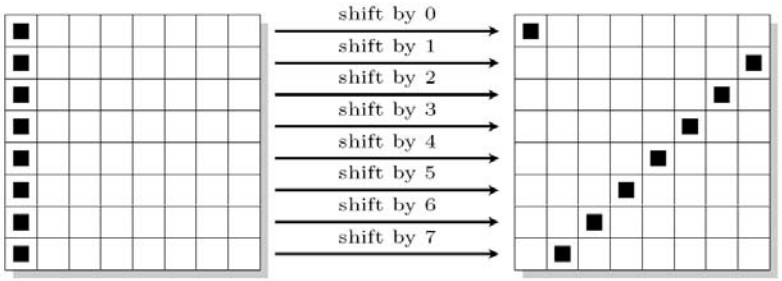


Grøstl-256:
8x8 geometry

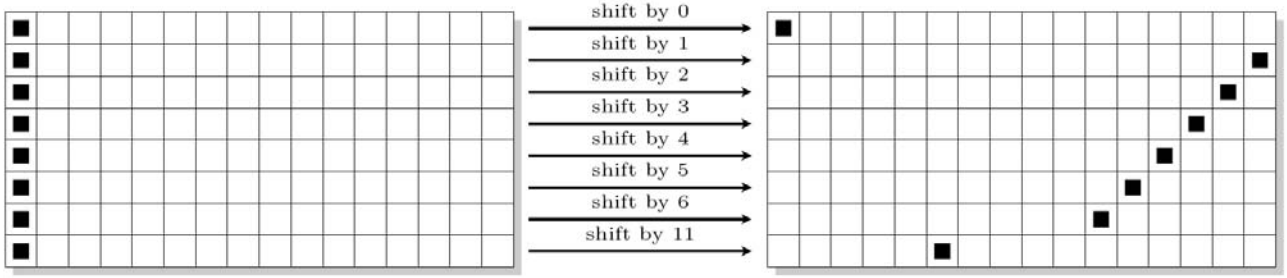
Grøstl-512:
8x16 geometry

ShiftBytes / ShiftBytesWide

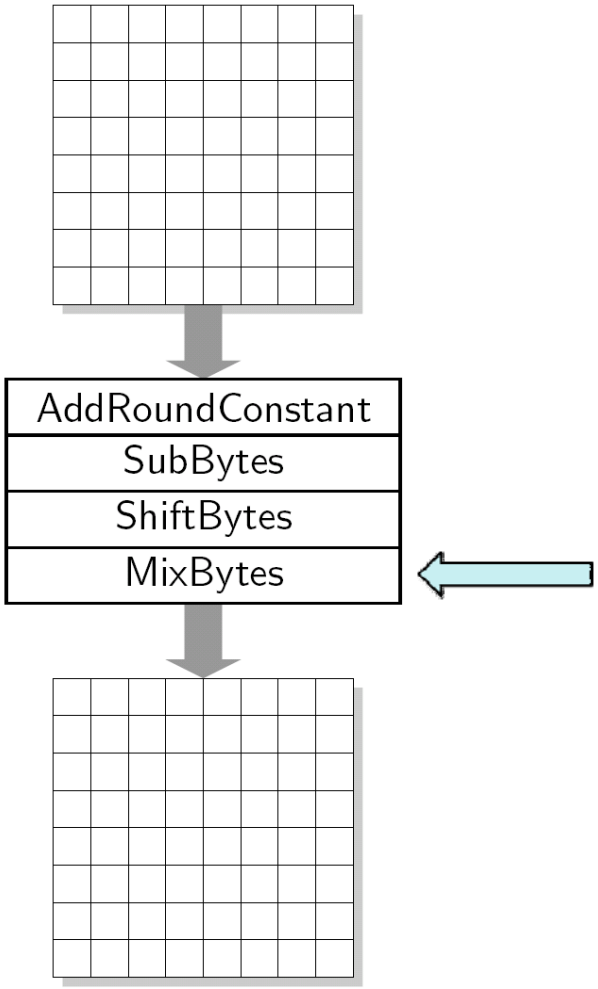
Grøstl-256



Grøstl-512



The State / Round Transformation

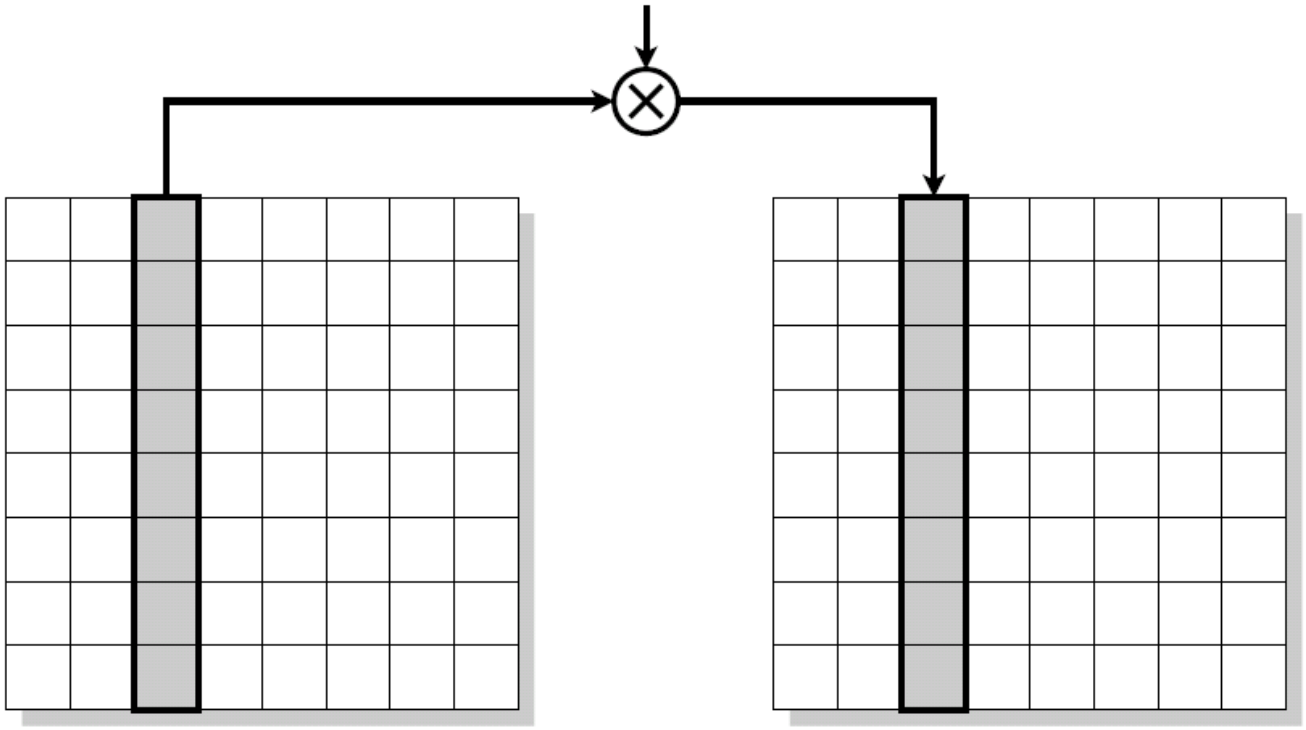


Grøstl-256:
8x8 geometry

Grøstl-512:
8x16 geometry

MixBytes

$$B = \mathrm{circ}(02, 02, 03, 04, 05, 03, 05, 07)$$



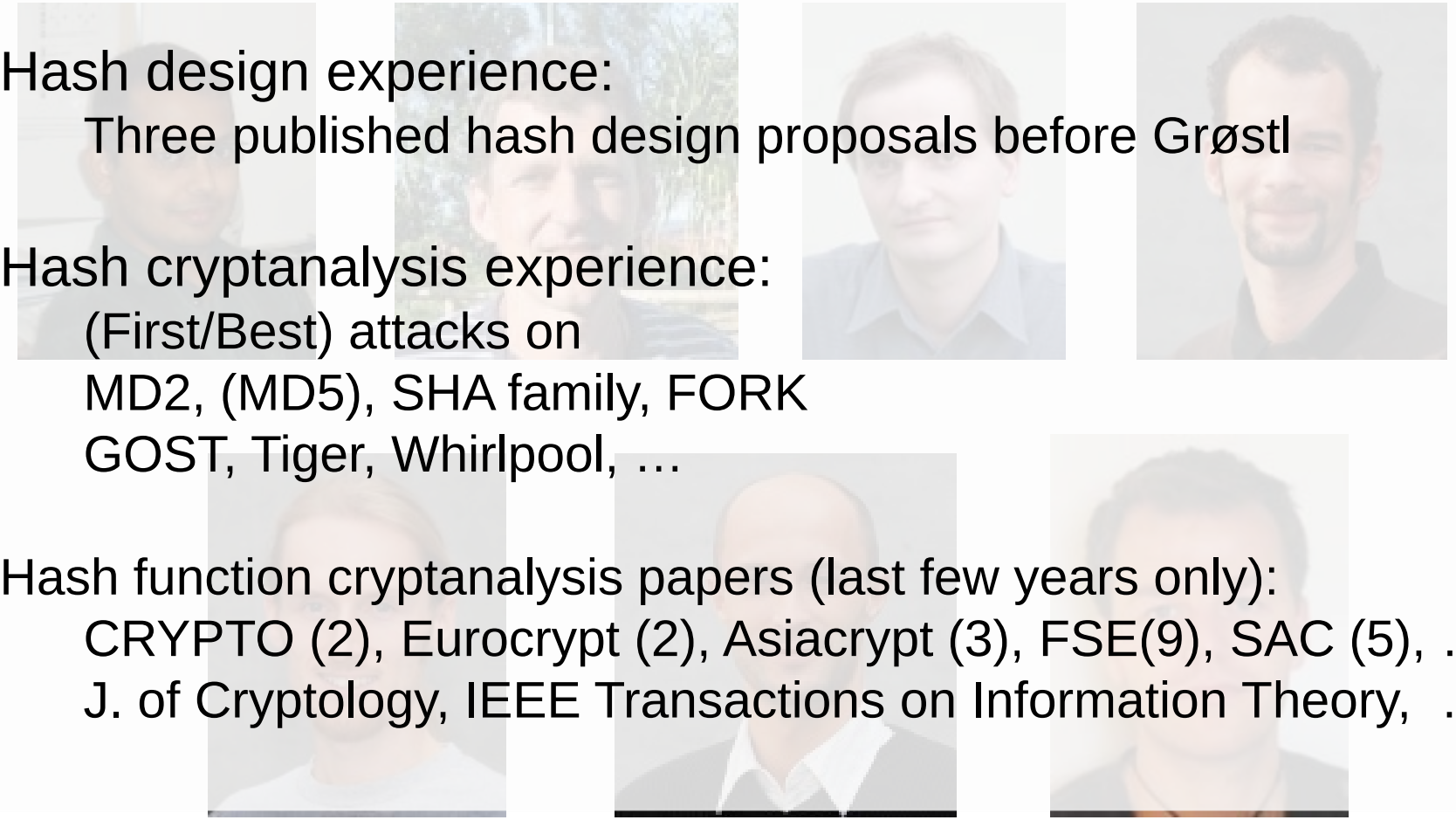
Hardware Performance:

- Grøstl allows extremely flexible implementations
  various memory/gates/throughput/latency/… trade-offs

Some implementation results:

	Area	Throughput(Gbits/s)
High throughput ASIC (0,18µm)	58 kGates	6,30
High throughput ASIC (0,18µm)	50 kGates	2,70
Low cost ASIC (0,18µm)	19 kGates	0,90
Low cost ASIC (0,18µm)	16 kGates	0,33
Spartan 3 FGPA	6.5 kSlices	4,40
Virtex 5 FGPA	1,7 kSlices	10,20

Proven track record:



Hash design experience:

Three published hash design proposals before Grøstl

Hash cryptanalysis experience:

(First/Best) attacks on
MD2, (MD5), SHA family, FORK
GOST, Tiger, Whirlpool, …

Hash function cryptanalysis papers (last few years only):

CRYPTO (2), Eurocrypt (2), Asiacrypt (3), FSE(9), SAC (5), …
J. of Cryptology, IEEE Transactions on Information Theory, …

Grøstl SHA-3 cryptanalysis

Recent SHA-3 related breaks/cryptanalysis of the Grøstl team:

- Blender, JH, Sarmal, TIB3, Twister, Vortex, Boole, DCH, SHAMATA
- BMW, Essence, JH, Vortex, MeshHash, Tangle