AURORA

A Cryptographic Hash Algorithm Family

Sony Corporation* Nagoya University†

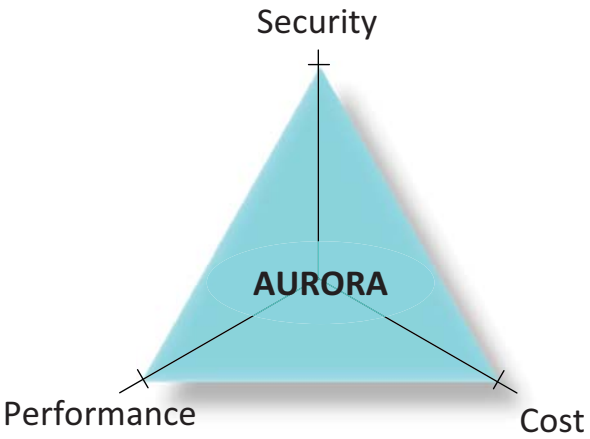
Tetsu Iwata†, Kyoji Shibutani*, Taizo Shirai*,
Shiho Moriai*, Toru Akishita*

Agenda

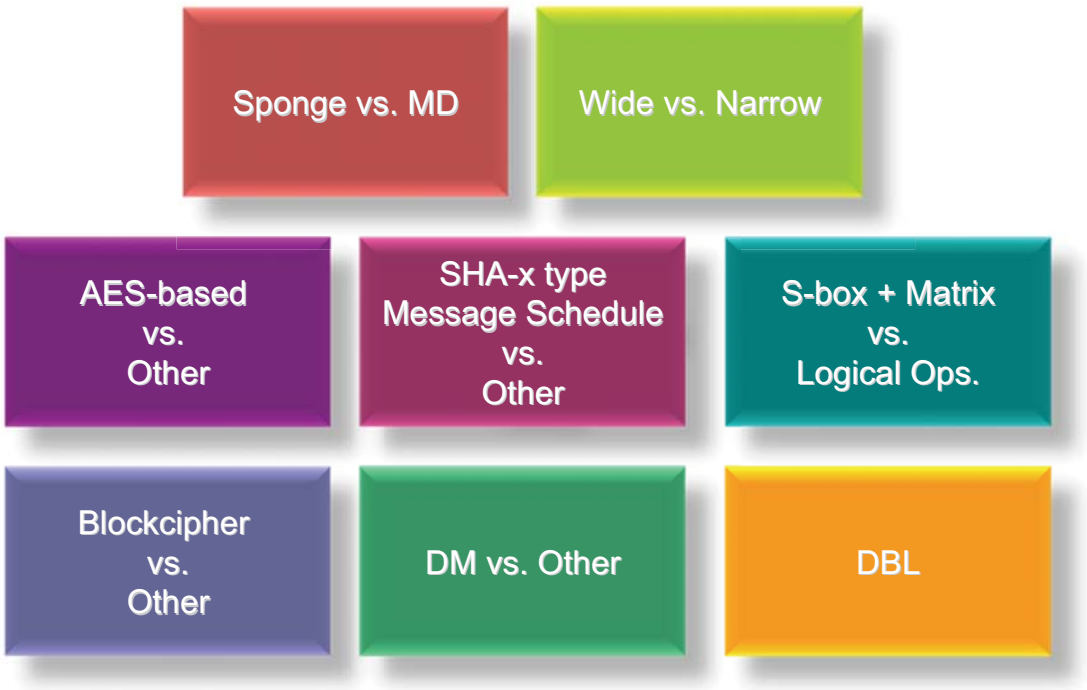
- Design Goals
- AURORA Specification
- Design Rationale
- Security
- Performance

AURORA Design Goal

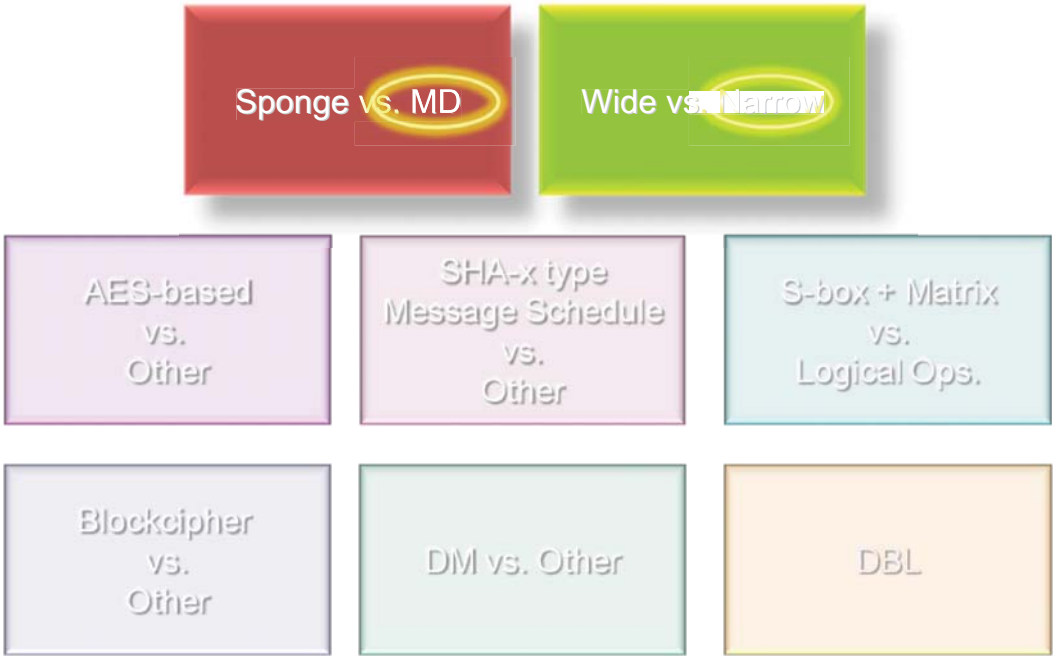
- Our priority: Best balance
- We respect "Selection criteria of AES"!



Design Selections

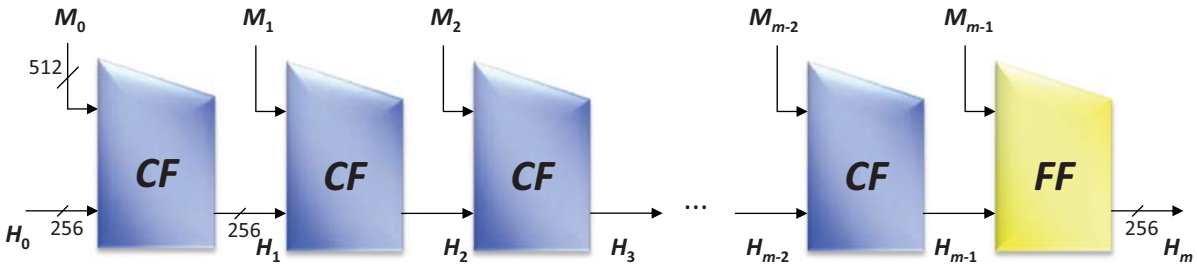


Design Selections (Domain Extension)



AURORA-256: Domain Extension

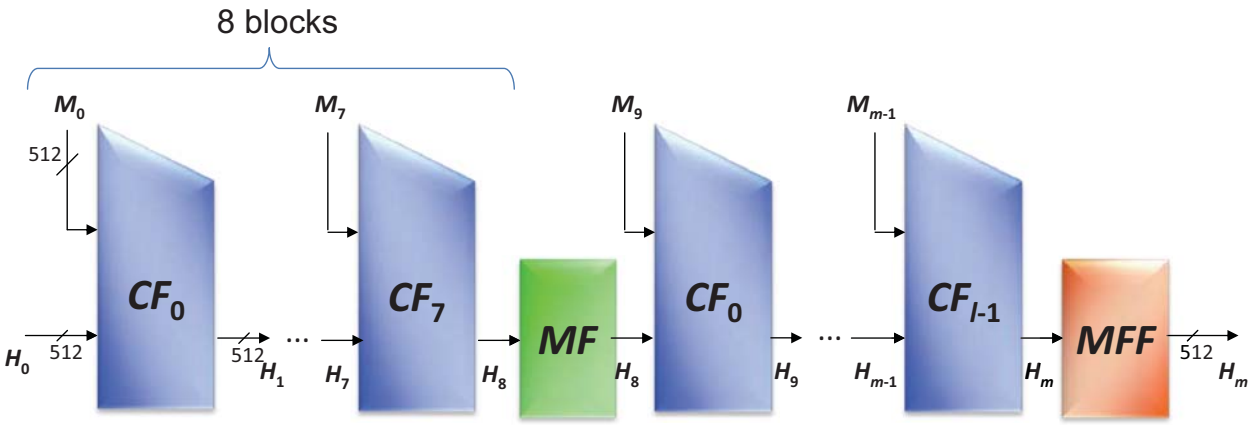
- sMD+ Finalization Function



- ***CF*** : Compression Function
- ***FF*** : Finalization Function

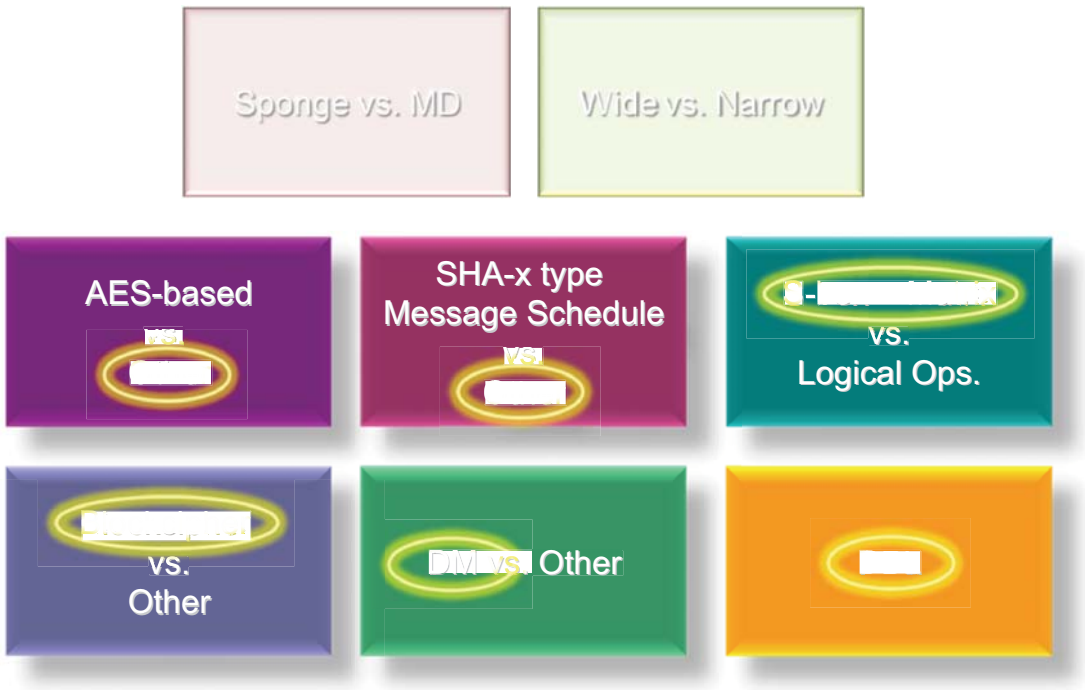
AURORA-512: Domain Extension

- sMD + Mixing Func. + Finalization Func.

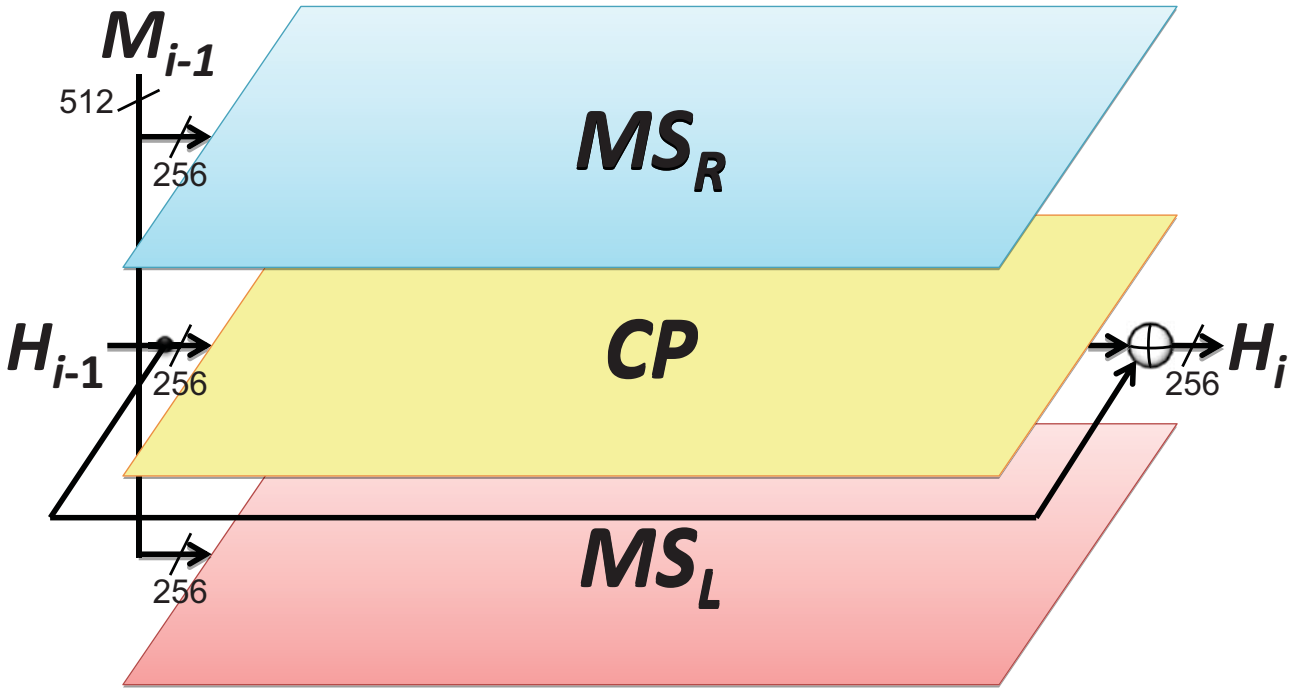


- CF_0 … CF_7 : Compression function
- ***MF*** : Mixing Function
- ***MFF*** : Mixing Function for Finalization

Design Selections (Compression Function)



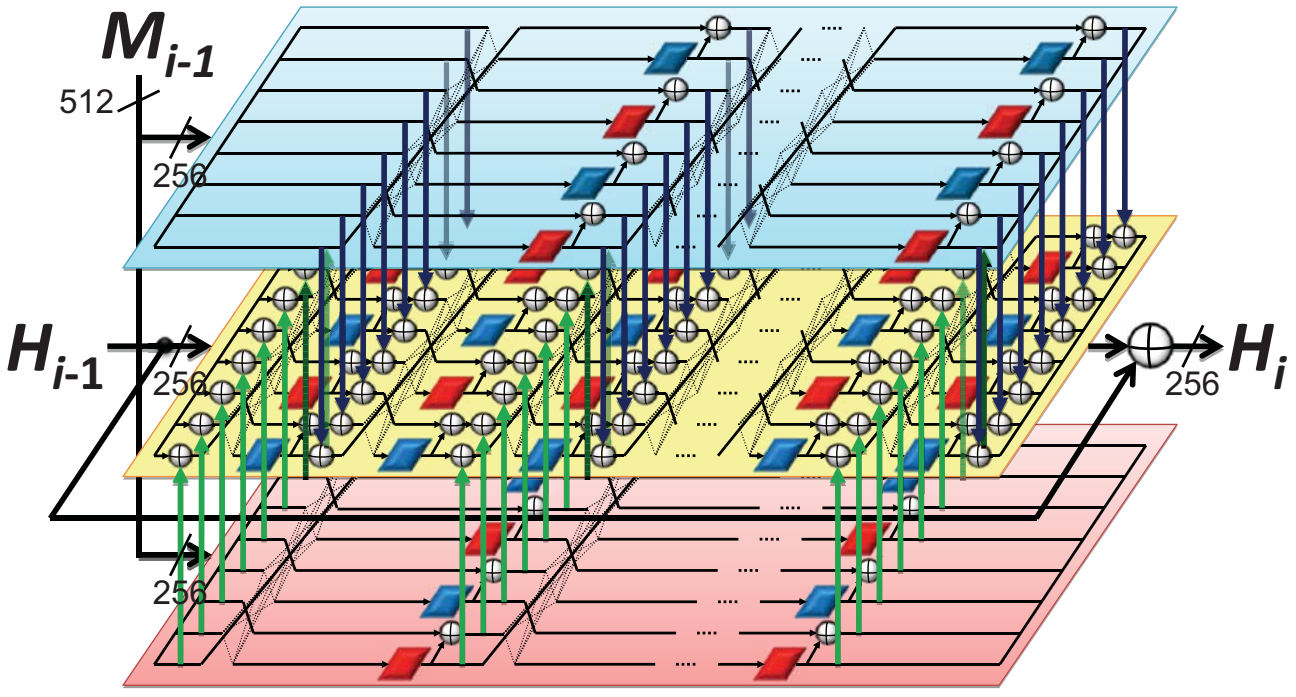
AURORA-256: Compression Func.



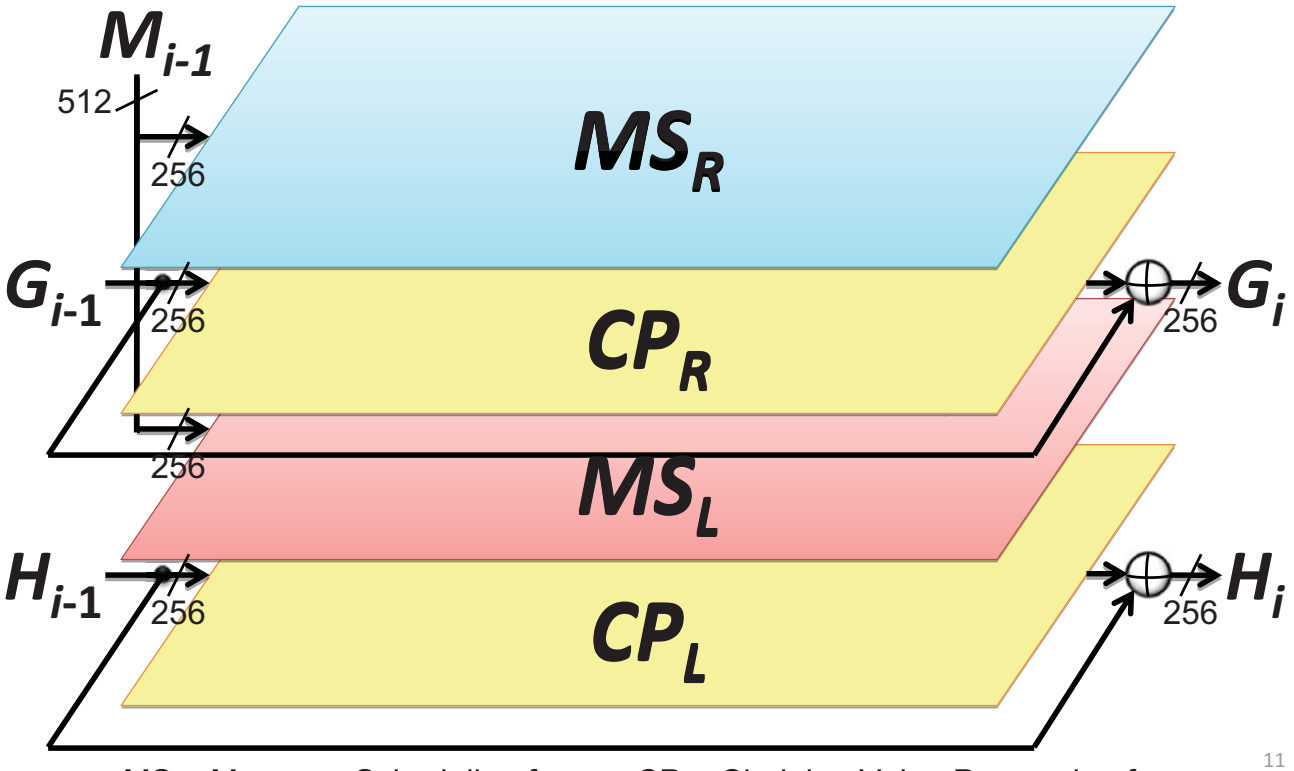
MS = Message Scheduling func.
CP = Chaining Value Processing func.

AURORA A Cryptographic Hash Algorithm Family

AURORA-256: Compression Func.

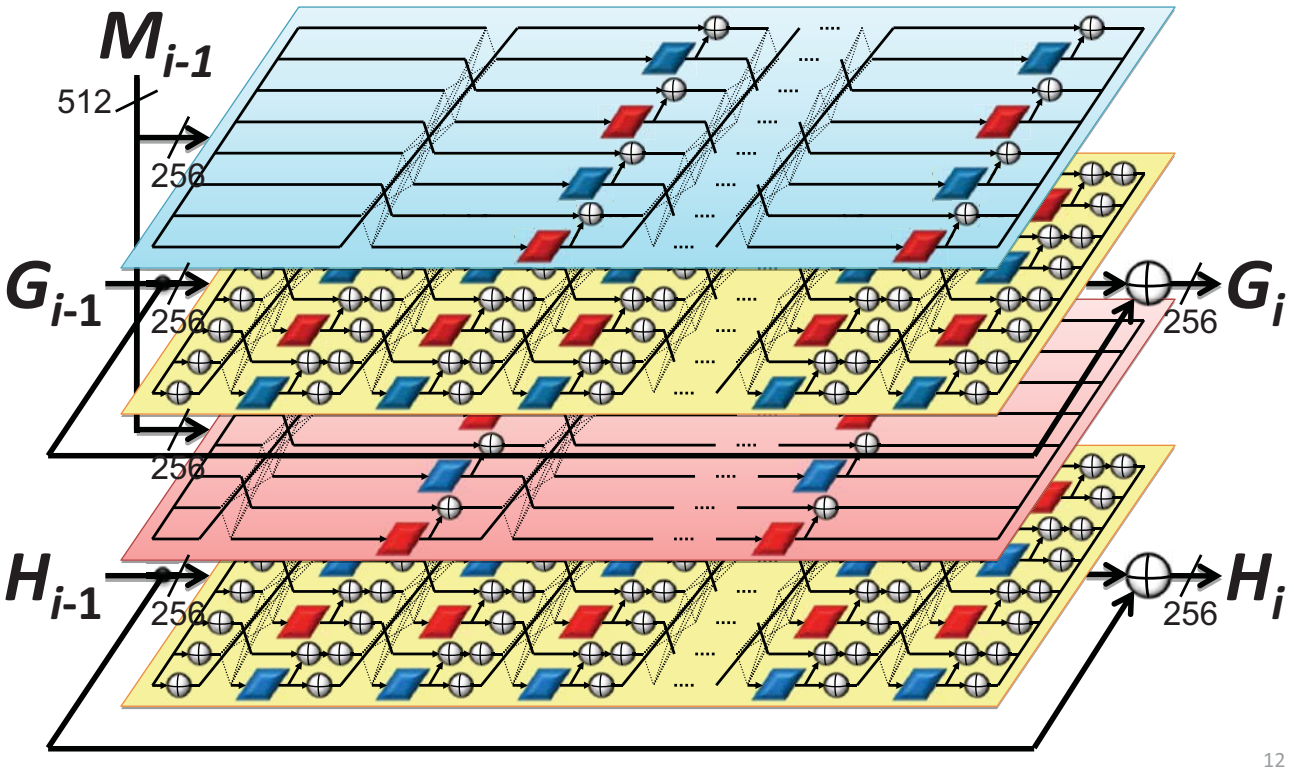


AURORA-512: Compression Func.

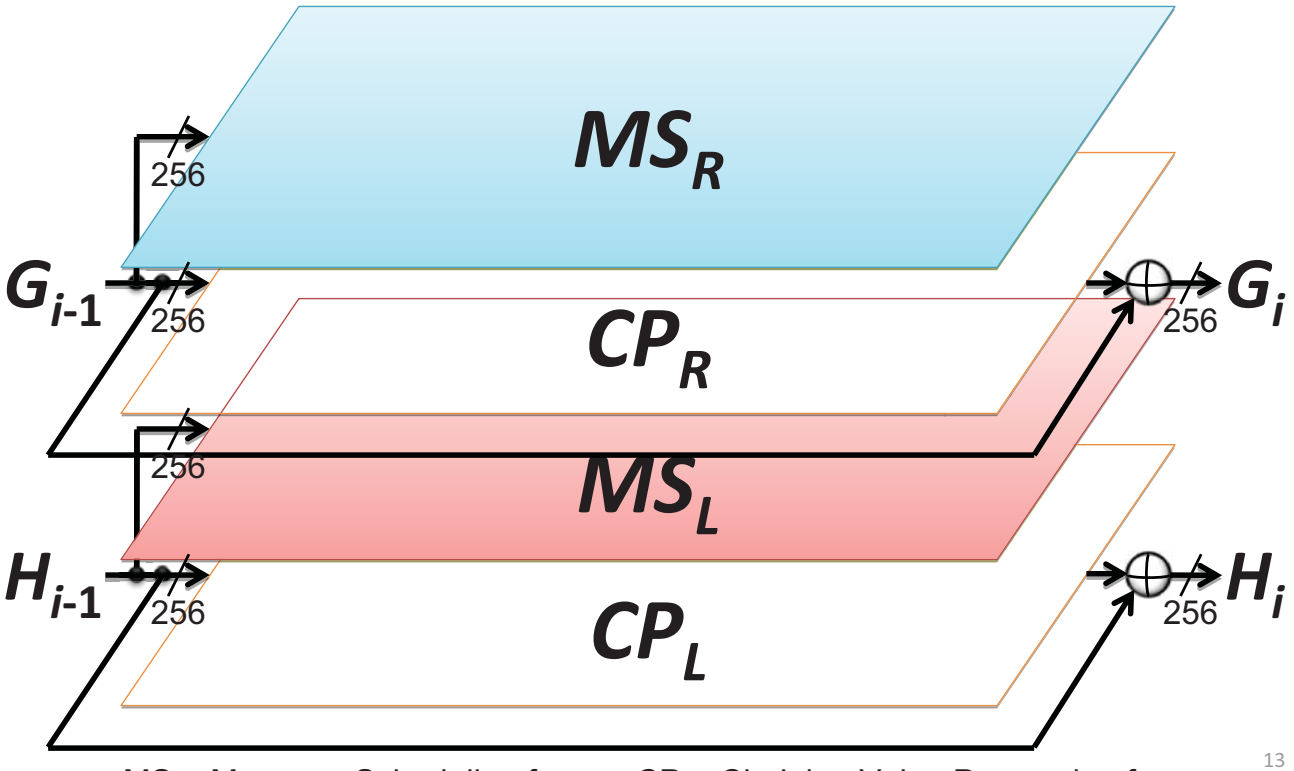


MS = Message Scheduling func. CP = Chaining Value Processing func.

AURORA-512: Compression Func.

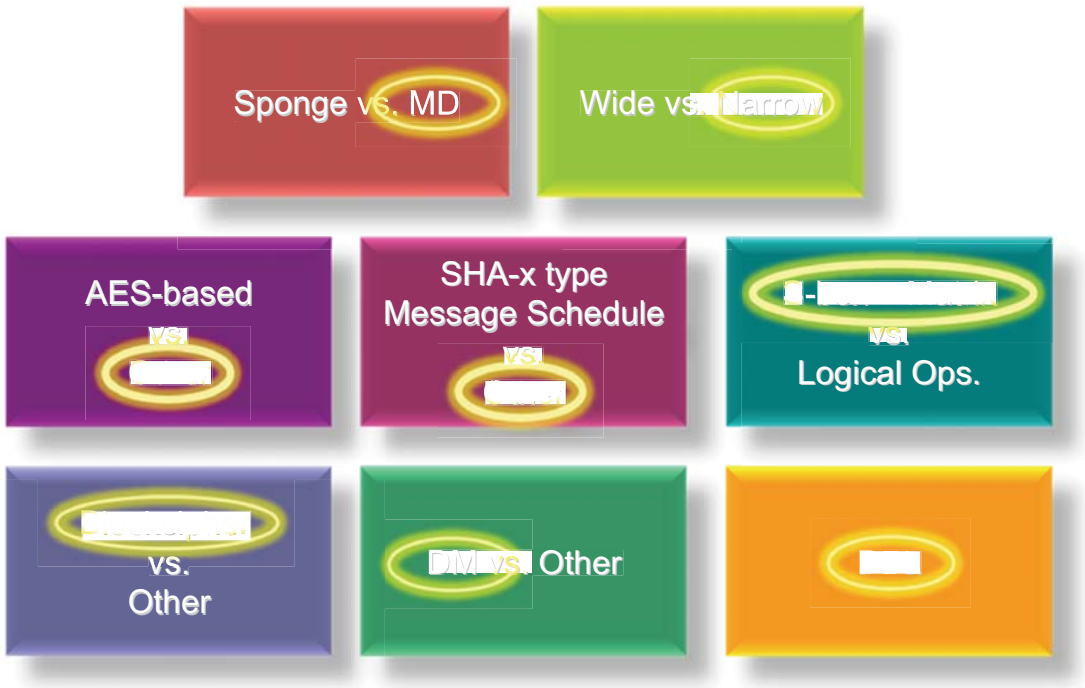


AURORA-512: Mixing Func., Finalization Func.



MS = Message Scheduling func. CP = Chaining Value Processing func.

Design Selections (Summary)



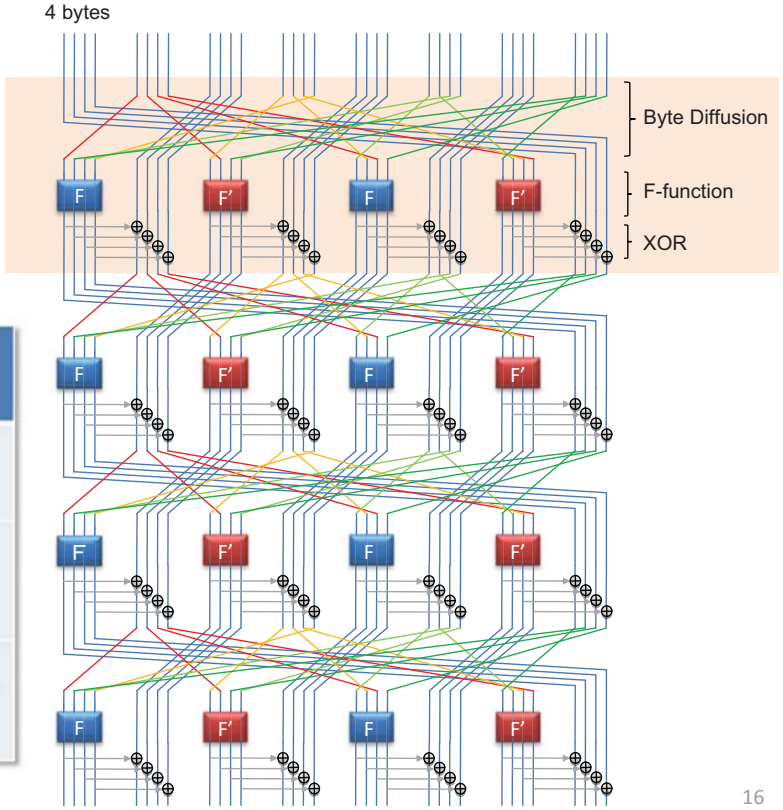
Main Features of Design Aspect

- S-box + Matrix design
  - S-box-based design is easy to evaluate.
  - AURORA structure
- Non AES-based
  - allows the use of DSM (Diffusion Switching Mechanism)
    - fast diffusion
    - can reduce the number of rounds
  - Our S-box is chosen considering hardware efficiency
- Strong Message Schedule
  - To prevent recent attacks on MDx/SHAx family.

Security of AURORA structure

- The DSM technique
- Guaranteed number of active S-boxes in AURORA structure

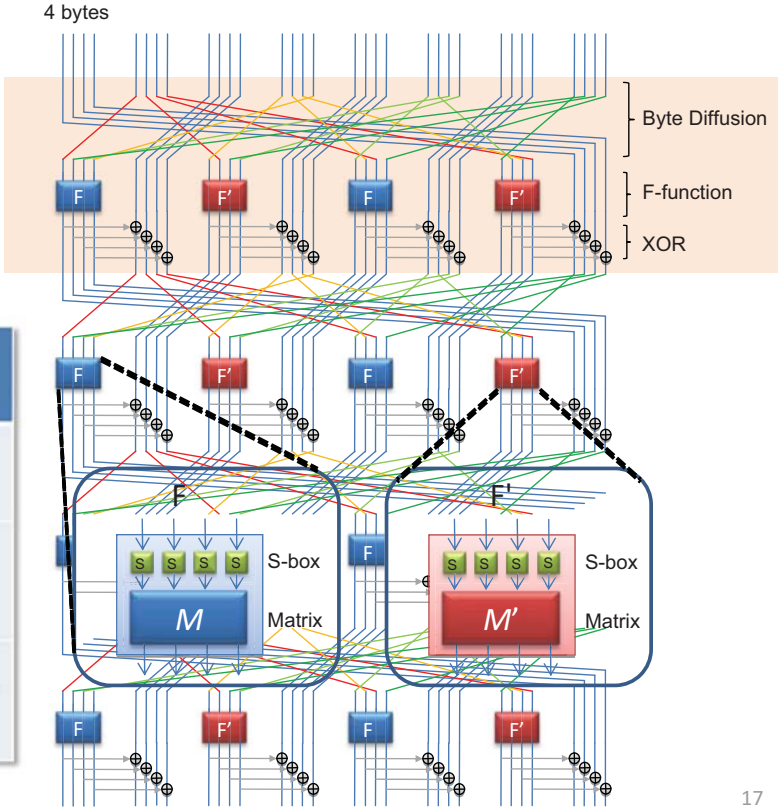
	CP	MS
#rounds	17	8
#active S-boxes	56	26
Max. Diff. Char. Prob.	$< 2^{-256}$	$< 2^{-128}$



Security of AURORA structure

- The DSM technique
- Guaranteed number of active S-boxes in AURORA structure

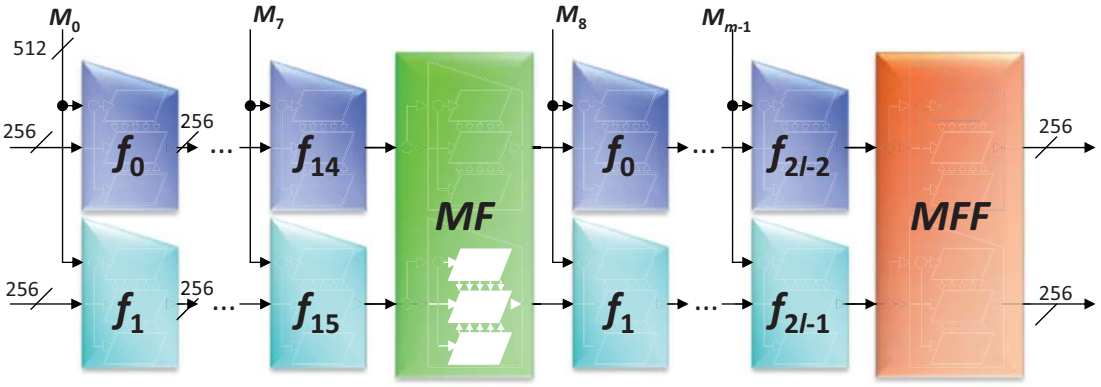
	CP	MS
#rounds	17	8
#active S-boxes	56	26
Max. Diff. Char. Prob.	$< 2^{-256}$	$< 2^{-128}$



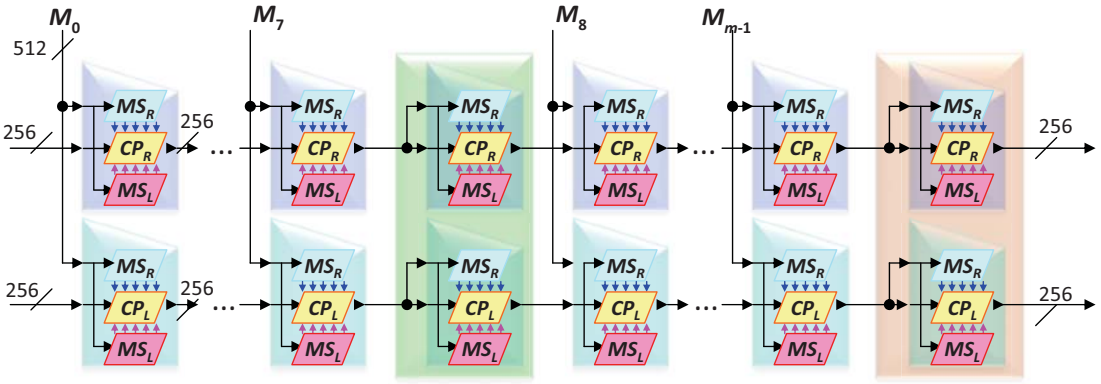
Security of Domain Extension

- AURORA-256
  - sMD + Finalization func.
    - indifferentiability, collision resistance-preserving, …
- AURORA-512
  - sMD + Mixing func. + Finalization func.
  - DMMD (Double-Mix Merkle-Damgaard) transform
  - Enhanced DBL of Compression function

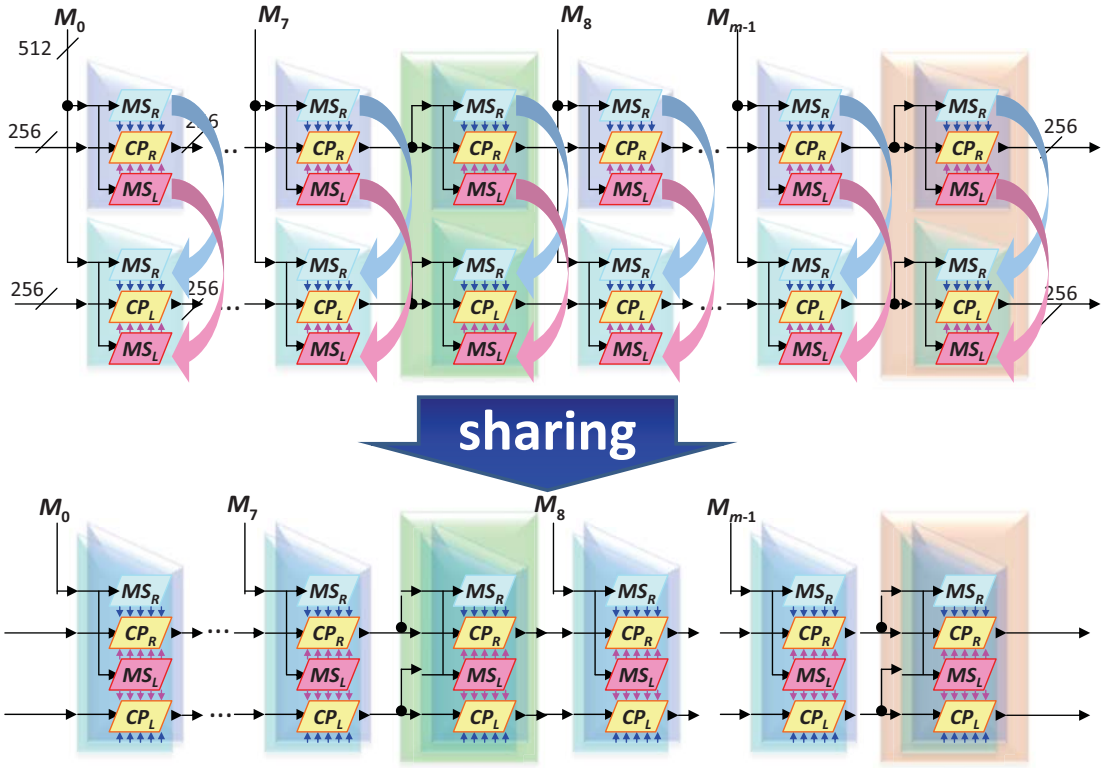
Instantiation of DMMD



Instantiation of DMMD



Instantiation of DMMD



Security of DMMD

- Security Proofs
  - collision/preimage resistance in RO
- Theorem: For any adversary A that makes at most q queries,

  $\Pr(\text{A finds a collision}) \leq O(q/2^{201})$

  $\Pr(\text{A finds a preimage}) \leq O(q/2^{512})$
  - does not imply collision attack with $q=2^{201}$
  - bound is expected to be improved
  - generic attacks failed

Algorithm Analysis

- Claimed security
  - Collision resistance : n/2 bits
    - An attack up to 3 round of AURORA-256/512
  - Preimage resistance : n bits
    - An attack up to 3 round of AURORA-256
  - 2nd Preimage resistance for 2^k block messages

AURORA-224	AURORA-256	AURORA-384	AURORA-512
Min{224,256-k}	256-k	384	512-k

  - Length extension attack: not possible

Software Performance

Good performance in ANSI C

	CPU	Language	Speed (cycles/byte)	
			Visual Studio*	Intel C
AURORA-256	Core 2 Duo (32-bit)	ANSI C	24.3	19.8
	Core 2 Duo (64-bit)	ANSI C	15.4	15.0
AURORA-512	Core 2 Duo (32-bit)	ANSI C	46.9	35.5
	Core 2 Duo (64-bit)	ANSI C	27.4	26.9

*NIST reference platform and compiler

- High performance in ANSI C is important.
  - Assembly implementations are not always chosen for the cases where portability is important.

AURORA A Cryptographic Hash Algorithm Family

Hardware Performance

Candidate of Best HW performance

	Optimization	Area [gates]	Frequency [MHz]	Speed [Mbps]	Efficiency [Kbps/gate]
AURORA-256	Area*	8,870	304.8	1,084	122.2
	Speed	35,016	363.9	10,352	295.6
	Efficiency	20,825	252.1	7,171	344.3
SHA-256	Area	11,484	154.1	1,096	95.4
	Speed	15,329	333.3	2,370	154.6
AURORA-512	Area*	12,134	290.2	590	48.6
	Speed	56,748	361.2	9,132	160.9
	Efficiency	31,746	244.7	6,187	194.9
SHA-512	Area	23,146	125.0	1,455	62.8
	Speed	27,297	250.0	2,909	105.6

Using a 0.13 um CMOS ASIC Library, fully autonomous implementation * Details will be published soon.

AURORA A Cryptographic Hash Algorithm Family

Conclusions

- Security
  - supported by security proofs/arguments
  - based on established blockcipher design/analysis techniques
- Efficiency and Flexibility
  - good SW performances across many platforms
  - flexible HW implementations with wide variety of area/speed trade-offs

Thank you for your attention