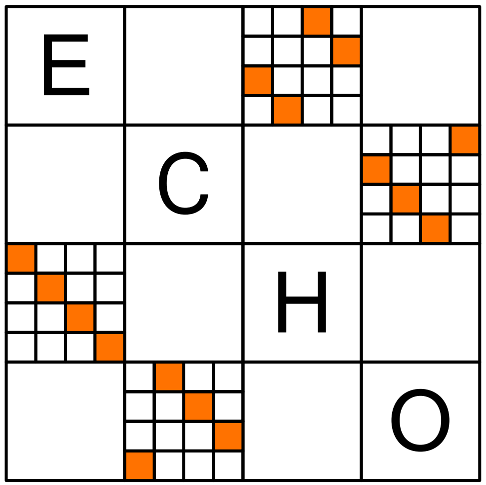


Ryad Benadjila

Olivier Billet

Henri Gilbert

Gilles Macario-Rat

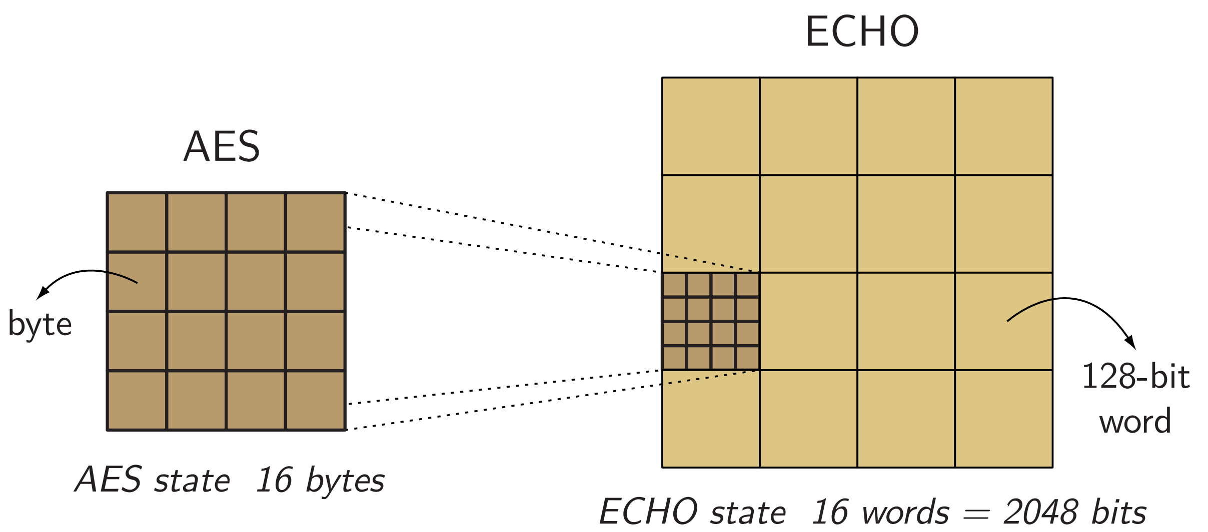
Thomas Peyrin *

Matt Robshaw

Yannick Seurin

*(* Ingenico, all other authors at Orange Labs)*

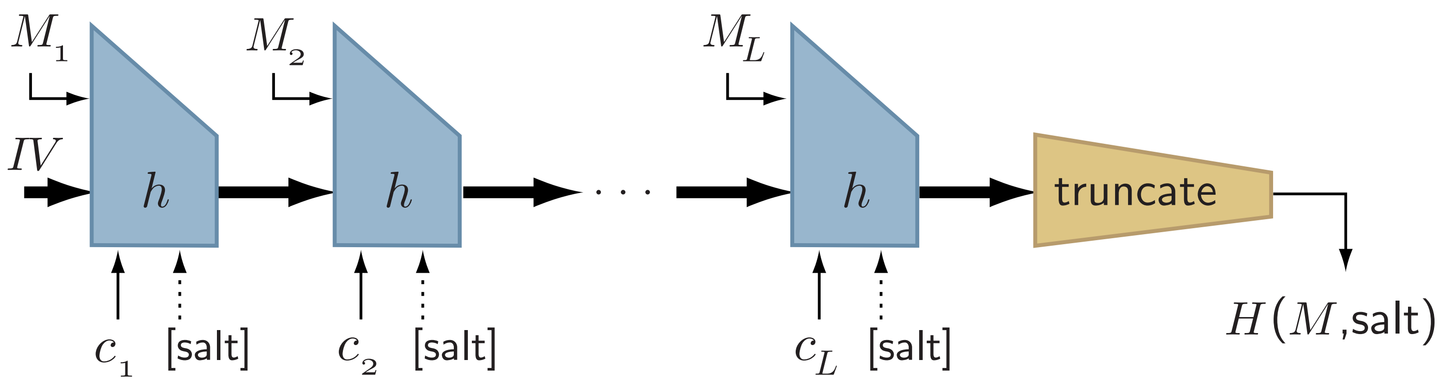
design principles



- simple to describe: echoing the AES design
- simple to analyze: exceptionally strong security proofs
- lessons from recent cryptanalytic advances
  - domain extension: HAIFA + double-pipe
  - compression function: input neutral

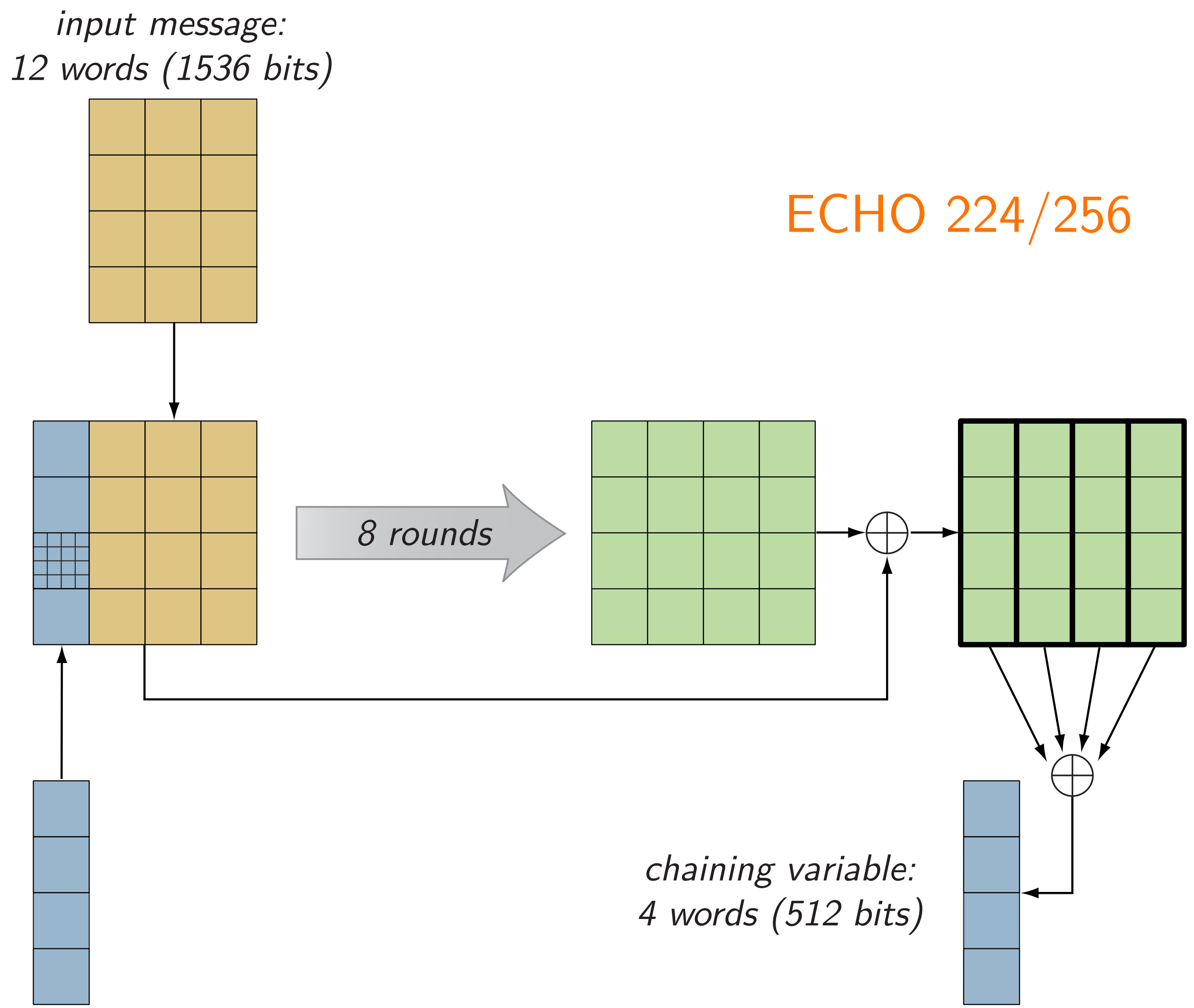
domain extension: double pipe

message + padding : $M_1 | M_2 | \cdots | M_L$

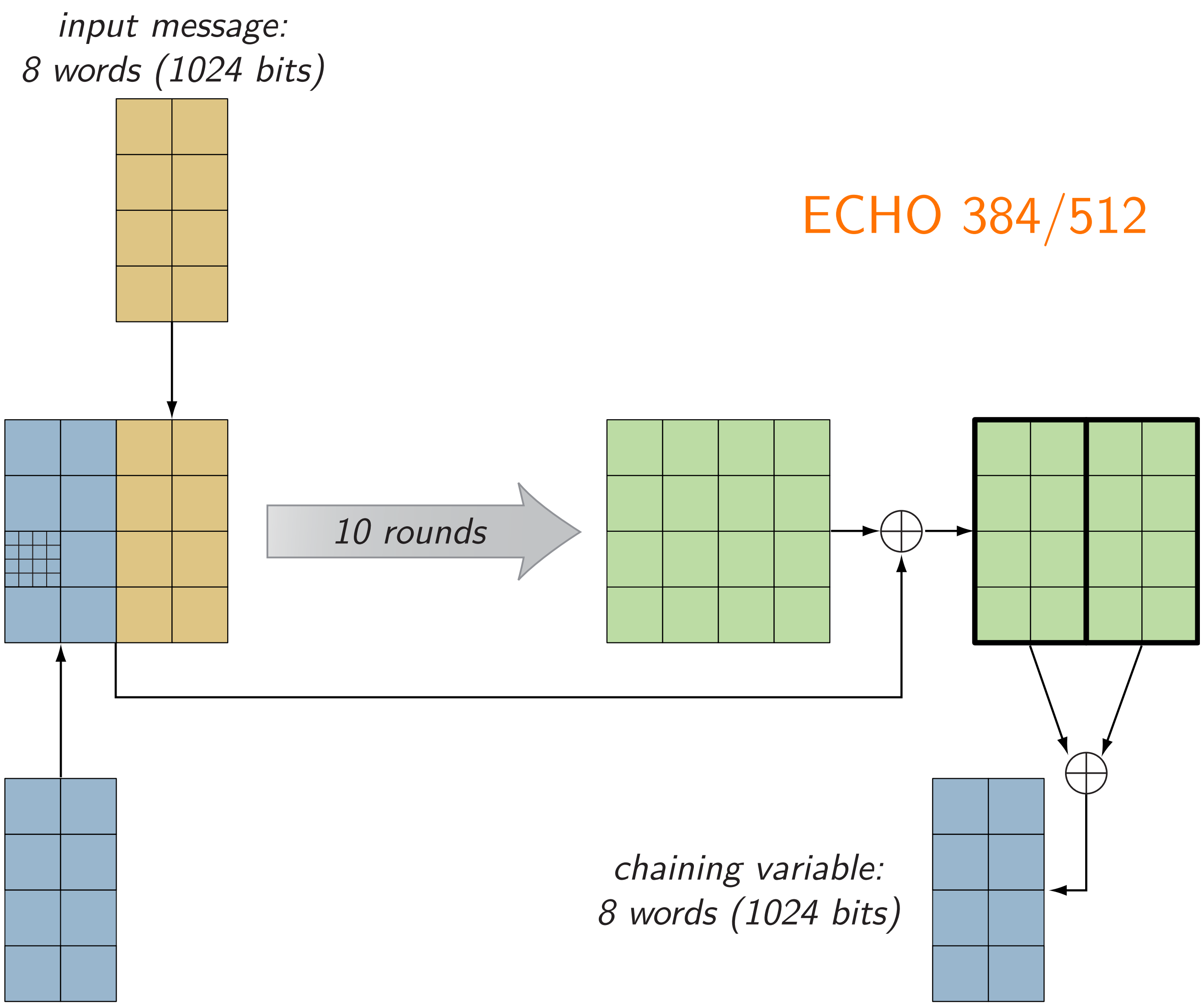


- double size chaining variable (avoid multicollisions)
- we also use HAIFA features:
  - pad the message with message length and hash length
  - use a bit counter as a compression function input
  - integrate the salt as an optional compression function input

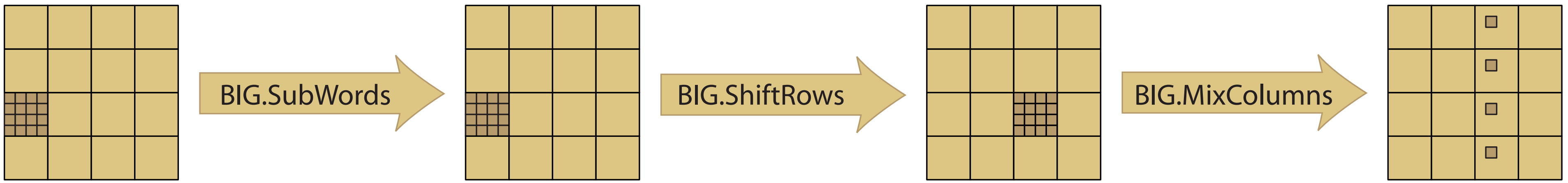
compression function up to 256 bits



compression function up to 512 bits

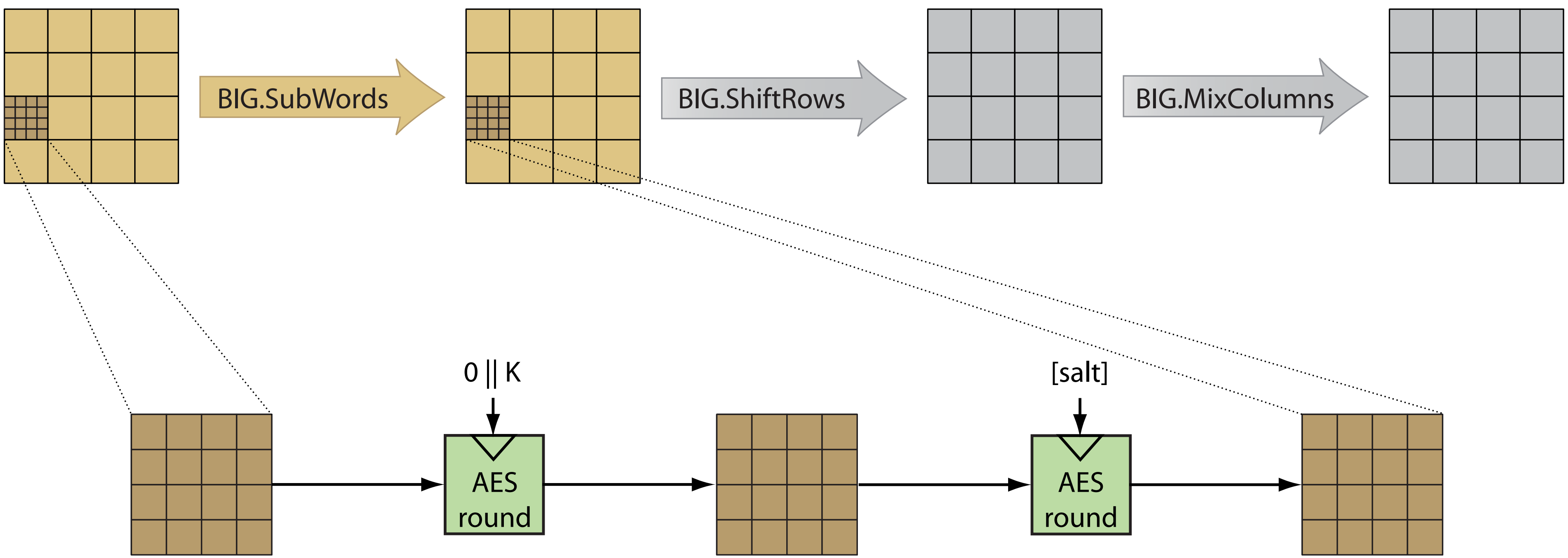


round function



- ROUND = BIG.SubWords + BIG.ShiftRows + BIG.MixColumns

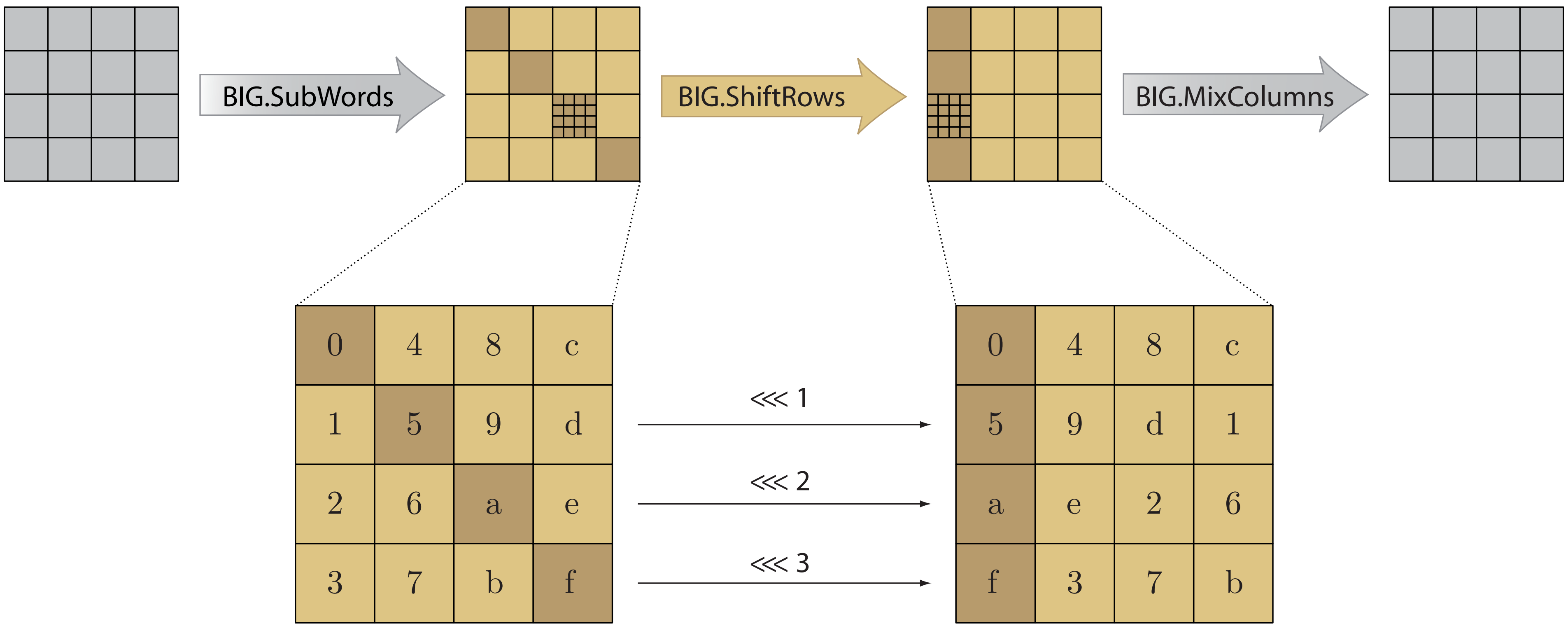
round function



BIG.SubWords

- K is an internal counter incremented each time it is used

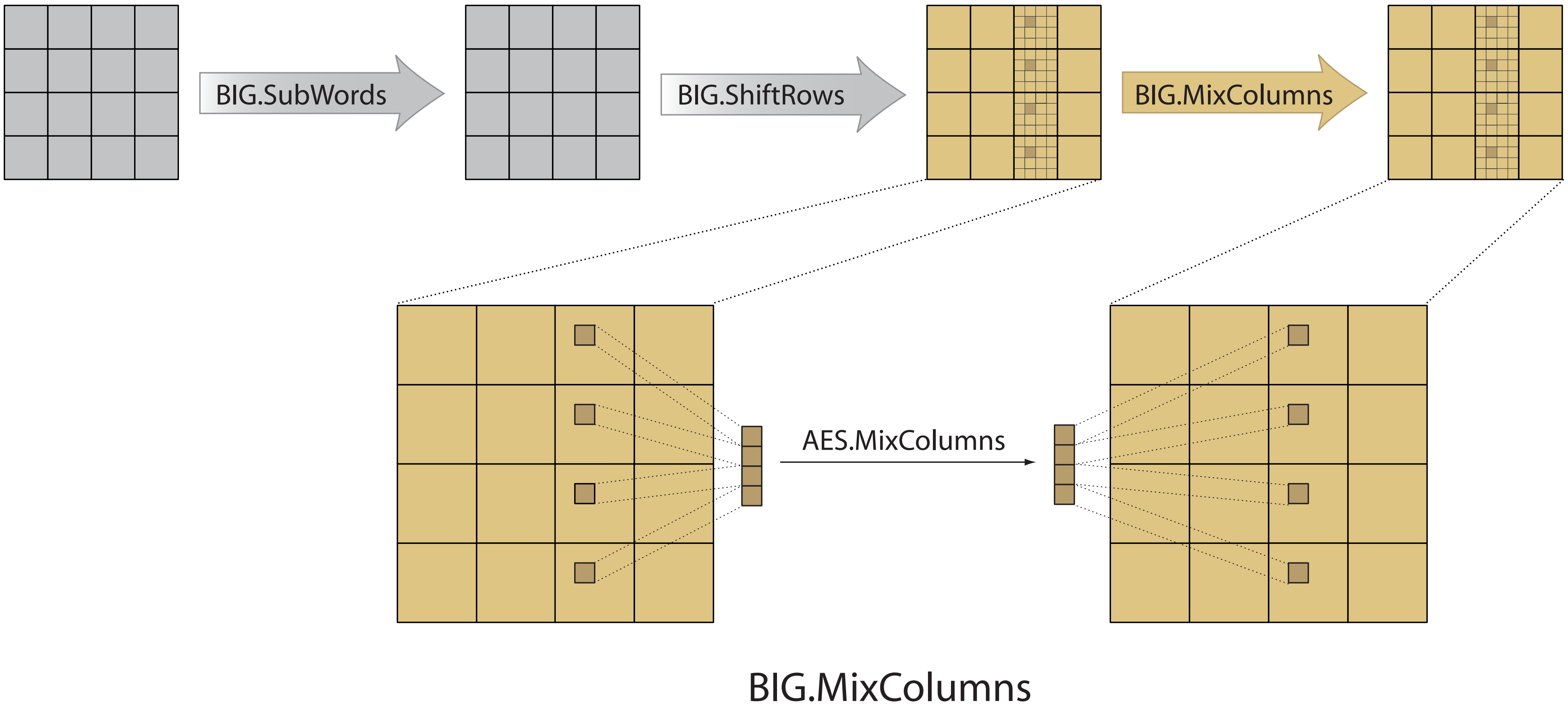
round function



BIG.ShiftRows

- apply the usual ShiftRows transformation on 128-bit words

round function



- apply the MixColumns of AES to 4-tuples of bytes throughout the state

design philosophy

- avoid related key attacks
  - the keys used for the 2-round AES are fixed
  - no message expansion:
    attacker can only control the beginning of the computation
- input neutral
  - message and chaining inputs are handled similarly
- leveraging AES security
  - by using AES rounds as a component
  - by using AES structure: ECHO is a BIG AES

differential proofs

- probability of differential characteristics
  - ECHO 256: $p \leqslant 2^{-1500}$ (at least 250 active AES S-boxes)
  - ECHO 512: $p \leqslant 2^{-1650}$ (at least 275 active AES S-boxes)
  - proof sketch
    - at least 25 active S-boxes for 4 rounds of AES

      $\Rightarrow$ at least 25 active “ECHO S-boxes” for 4 rounds of ECHO
    - an “ECHO S-box” is 2 rounds of AES

      $\Rightarrow$ at least 5 active AES S-boxes
    - therefore, at least 125 active AES S-boxes for 4 rounds of ECHO
  - even attackers who entirely control 4 rounds of ECHO have a success probability lower than 2^{-750}

- probability of differentials
  - for 4 rounds of ECHO: $p \leqslant 2^{-452}$
  - we can reuse AES proofs to get differentials bounds for ECHO

other attacks

- truncated differentials (e.g. Grindahl cryptanalysis)
  - do not endanger ECHO because of the strong diffusion
  - achieved through many MixColumns transformations
- related salt/counter attacks
  - prevented by strong lower bounds on the number of active S-boxes
  - even when salt/counters are under full control of the attacker
- structural cryptanalysis
  - very well studied for the AES (square, partial sum, bottleneck)
  - far from being a threat for ECHO with the current state-of-the-art
- algebraic cryptanalysis
  - much larger algebraic system than in the case of the AES

security claims

attack	MD single pipe	HAIFA single pipe	ECHO
collision	✓	✓	✓
preimage	✓	✓	✓
2^{nd} preimage	✗	✓	✓
multicollision	✗	✗	✓

ECHO is (multi-)collision and (2nd-)preimage resistant

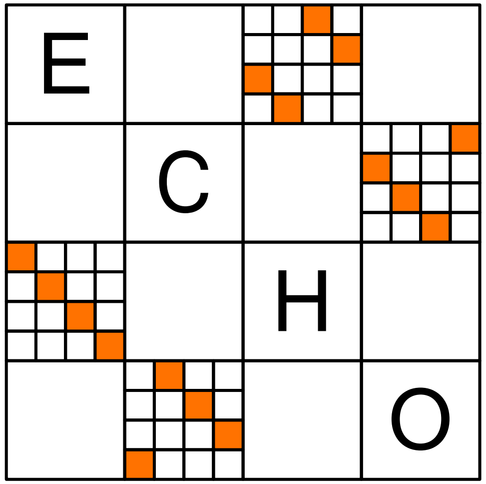
implementation

- flexible design gives the same implementation for all variants
- hardware parallelism
- take full advantage of Intel AES instructions set
  - implementation for Intel emulator available on web site
  - no dependency between AES instructions calls
- leverage existing AES implementations
  - benefit from AES countermeasures against side-channel attacks
  - benefit from speed improvements of AES implementations
- good performances on legacy CPUs
  - low cache overhead (four AES lookup tables)

comparisons

		AES rounds per 128 bits (256 / 512)	256 bits speed (c/B)			512 bits speed (c/B)		
			64 bits	32 bits	intel AES	64 bits	32 bits	intel AES
multicollision resistant	ECHO	21 / 40	28.5	32.5	$\leqslant 6$ *	53.5	61.0	$\leqslant 12$ *
	FUGUE	N/A	33.3	38.0	✗	75.5	78.2	✗
	Grøstl	N/A	22.4	22.9	✗	30.1	37.5	✗
single pipe	ECHO-SP	18 / 27	24.4	27.8	$\leqslant 5$ *	35.7	40.7	$\leqslant 8$ *
	LANE	21 / 28	25.7	40.5	5	145.3	152.2	?
	SHAvite-3	13 / 21	26.7	35.3	$\leqslant 8$	38.2	55.0	$\leqslant 12$

* code for Intel emulator available from ECHO web page



- a simple and clean design
- strong security arguments
- full flexibility in a single primitive
- support of the Intel AES instructions set

http://crypto.rd.francetelecom.com/echo/