Shabal

E. Bresson
A. Canteaut
B. Chevallier-Mames
C. Clavier
T. Fuhr
A. Gouget
T. Icart
J.-F. Misarsky
M. Naya-Plasencia
P. Paillier
T. Pornin
J.-R. Reinhard
C. Thuillet
M. Videau

Cryptolog, ANSSI, EADS, France Télécom, Gemalto, INRIA, Sagem

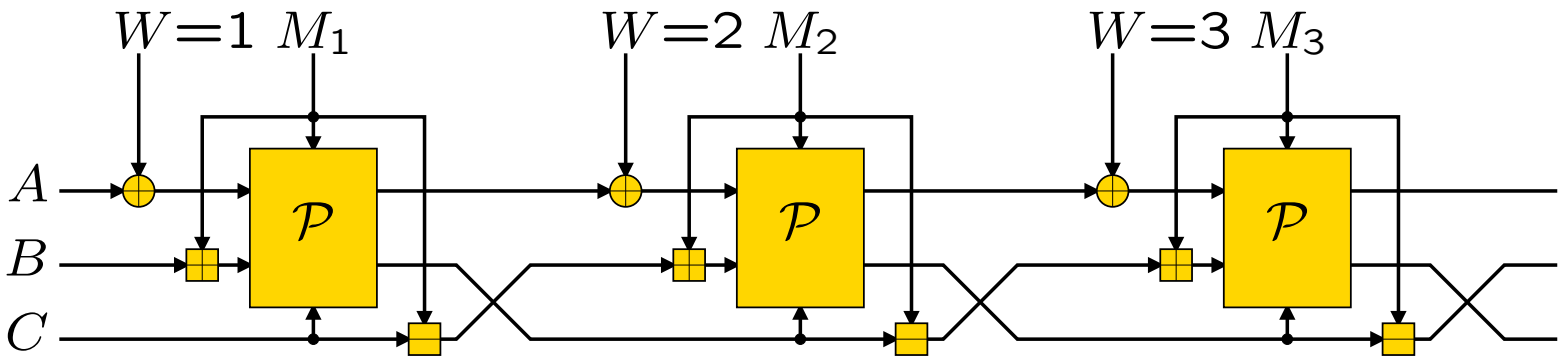
supported by the Saphir2 project

The second SHA-3 Candidate Conference, August 24, 2010

How does Chabal look like?

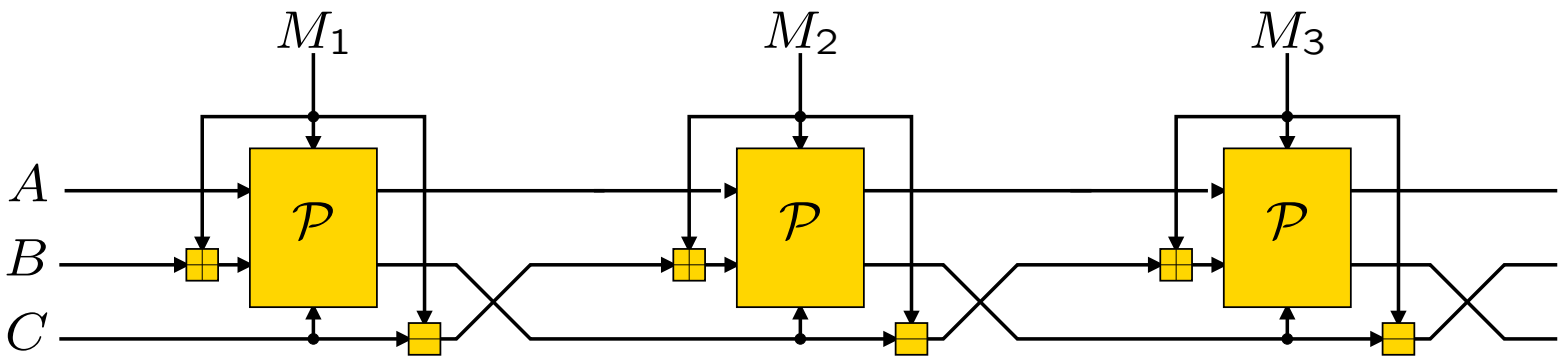
http://commons.wikimedia.org/wiki/File:Sebastien-Chabal_large.jpg

How does Shabal look like?

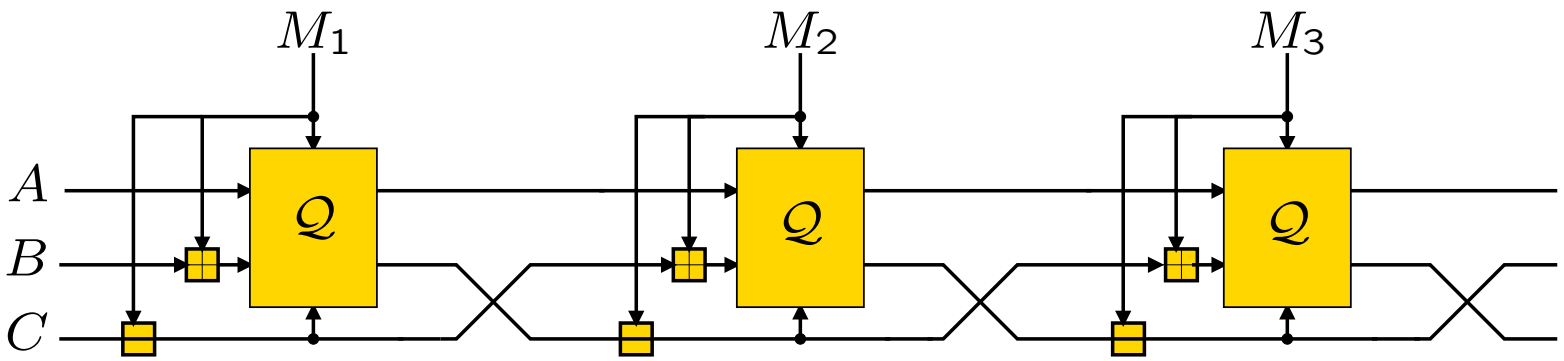


- no tweak;
- same function for all output sizes;
- 1408-bit internal state and 512-bit message blocks;
- 3 additional blank rounds parametrized by the last message block without incrementing the counter;

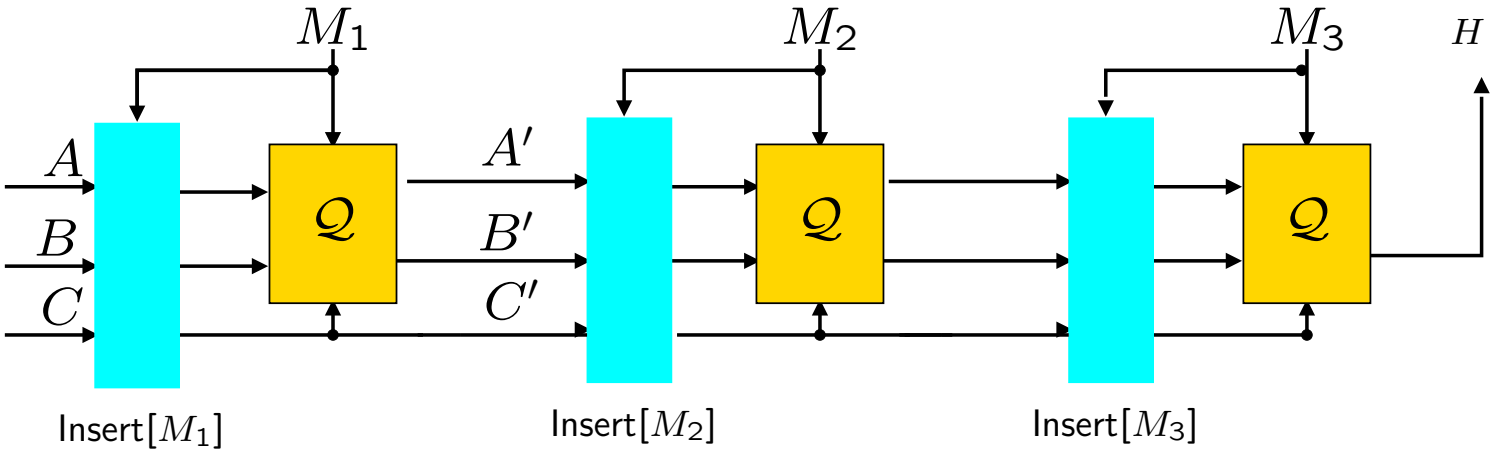
Equivalent mode of operation



Equivalent mode of operation



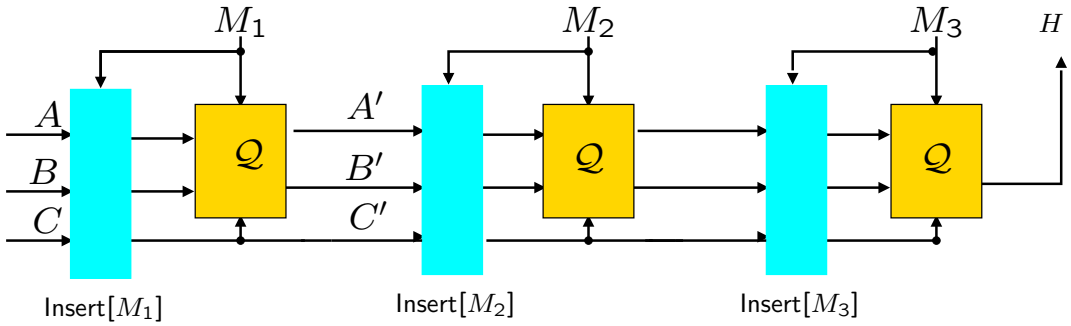
General mode of operation



Example.

For $\ell_{\boldsymbol{c}} = \mathbf{0}$ and **Insert** $= \mathbf{Id}$, it corresponds to chop-MD.

Indifferentiability



Indifferentiability bound.

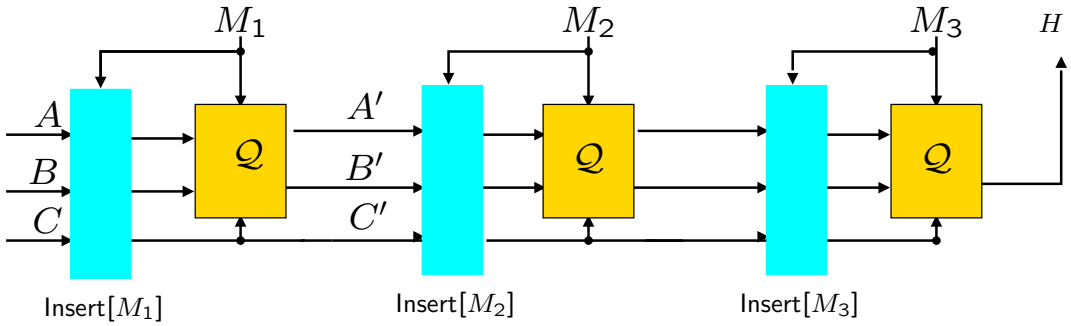
If $\mathcal{Q}$ is an ideal keyed permutation on m-bit inputs,

$$\min\left(2^{\frac{m}{2}},\ \ 2^{m-\ell_h-\log \ell_h}\right).$$

With prefix-free encoding,

$$2^{\frac{m}{2}}$$

Indifferentiability



Indifferentiability bound.

If $\mathcal{Q}$ is an ideal keyed permutation on m-bit inputs,

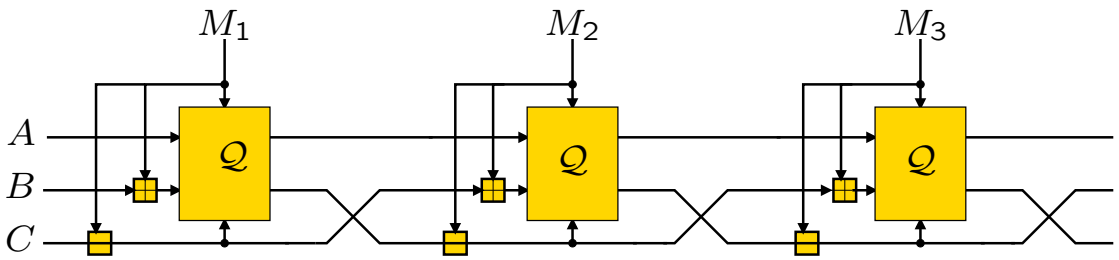
$$\min \quad 2^{\frac{m}{2}}, \quad 2^{m-\ell_h-\log \ell_h} \quad .$$

Realistic model for the finalization: with blank rounds, if the insertion function is well-chosen (e.g. in Shabal),

$$\min \quad 2^{\frac{m}{2}}, \quad 2^{m+\ell_c-\ell_h-\log \ell_h} \quad .$$

Indifferentiability up to 2^{448} queries compared to 2^{128} or 2^{256} for single-pipe designs [Blake, Hamsi, SHAvite-3, Skein].

Second-preimage resistance



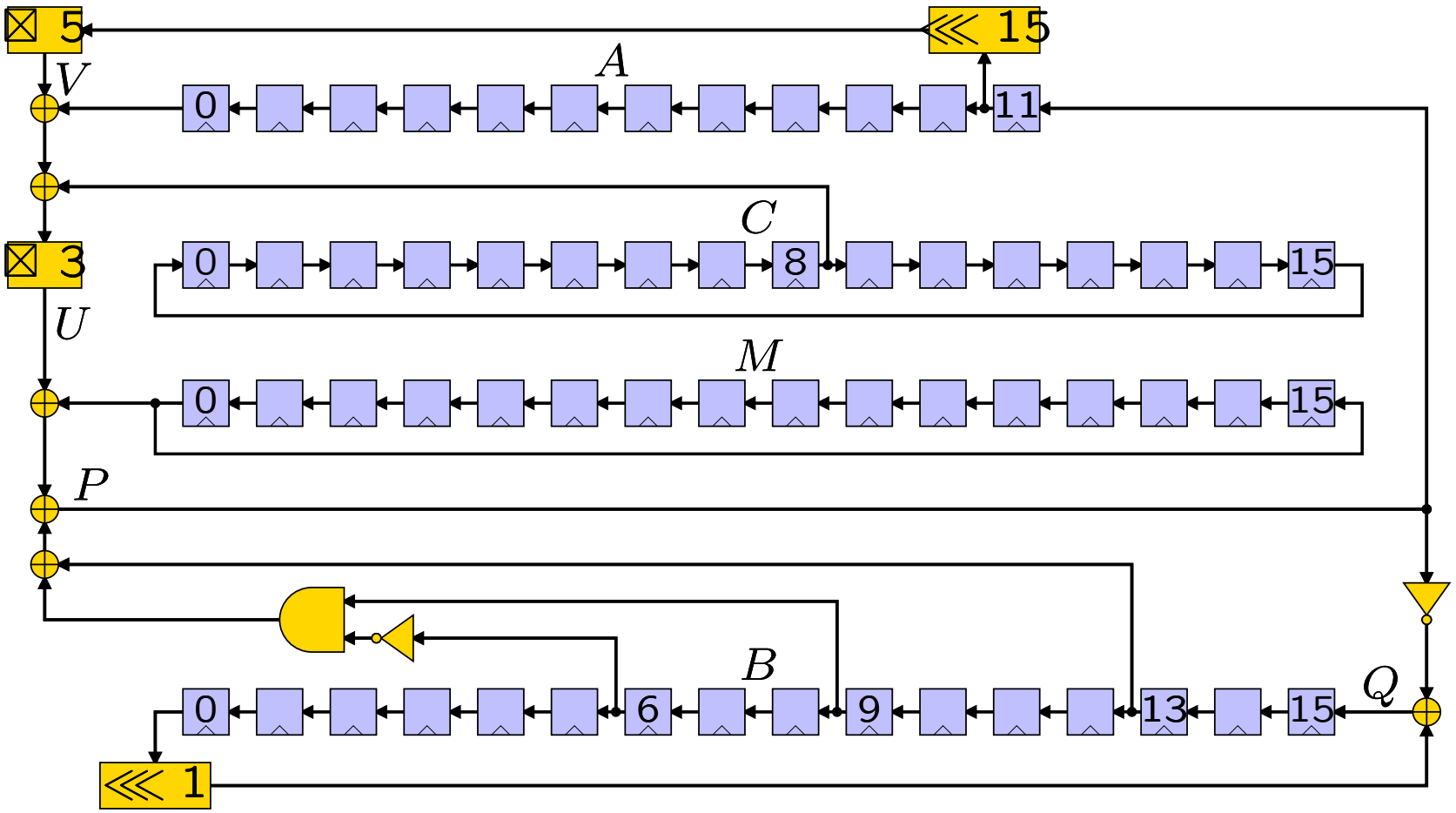
Bound on second-preimage resistance (besides the generic preimage attack).

If $\mathcal{Q}$ is an ideal keyed permutation on m-bit inputs, for κ-block messages, the number of queries for a 2nd-preimage attack is at least

$$\frac{1}{8}\min\left(2^{m-\log \ell_c},\ 2^{m+\ell_c-\log \kappa},\ 2^{\frac{m+\ell_c}{2}}\right).$$

Proven 2nd-preimage resistance (besides the generic attack) up to 2^{702} queries compared to existing 2nd-preimage attacks with complexity 2^{513} for Keccak-512, 2^{453} for Cubehash 16/32...

Shabal keyed permutation

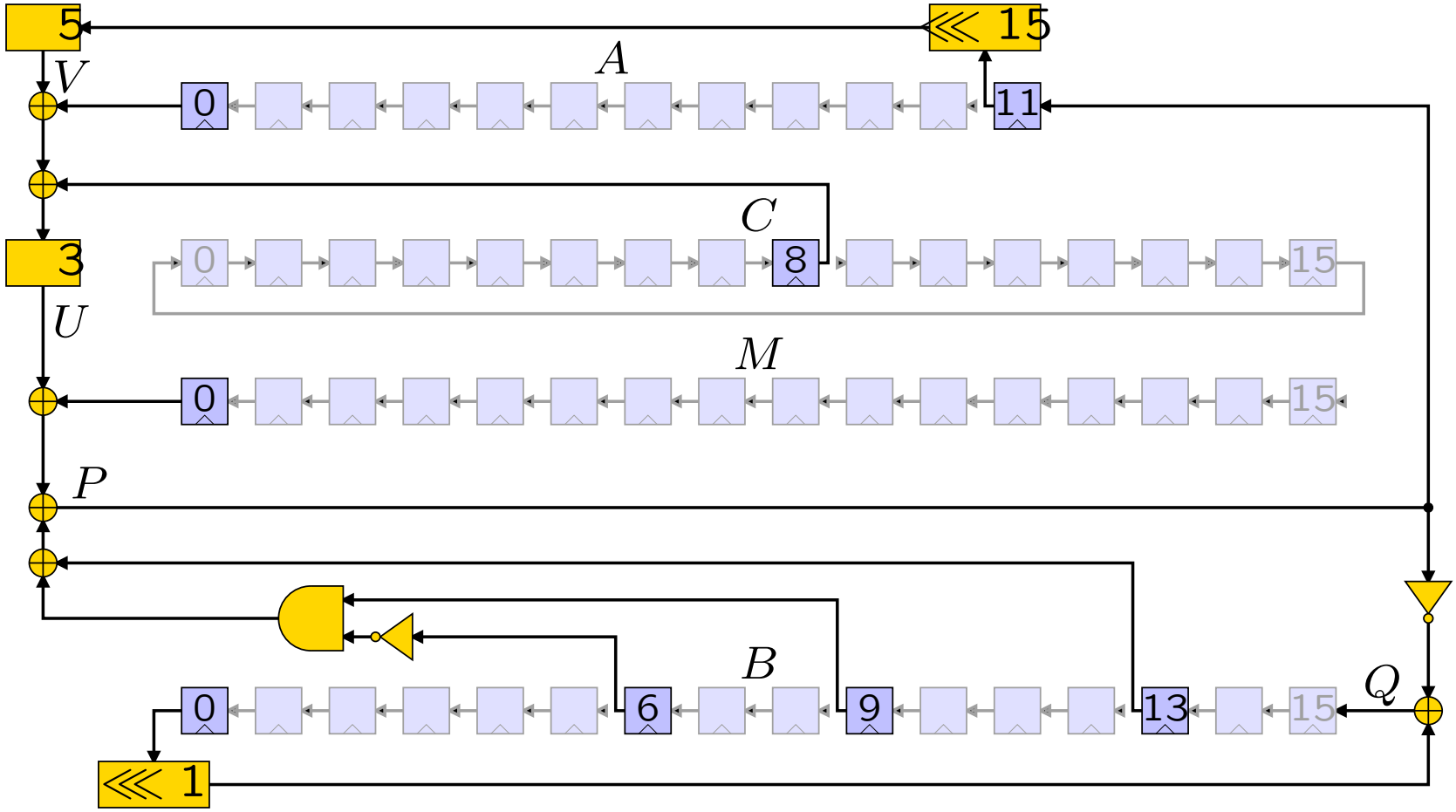


For $i = 0, \ldots, 15$: $B[i] \leftarrow B[i] \lll 17$

Apply 48 *steps*

For $i = 0, \ldots, 35$: $A[i \bmod 12] \leftarrow A[i \bmod 12] \boxplus C[(i+3) \bmod 16]$

Shabal keyed permutation



For $i = 0, \ldots, 15$: $B[i] \leftarrow B[i] \lll 17$

Apply 48 *steps*

For $i = 0, \ldots, 35$: $A[i \bmod 12] \leftarrow A[i \bmod 12] \boxplus C[(i+3) \bmod 16]$

Can you find him?

Distinguishers on the inner permutation

Non-dependencies of the inverse permutation [Shabal 08]
[Aumasson 09],[Shabal 09].
The number of preimages for a given (y, M) may be only 2^{m-96}.

Differential distinguishers [Aumasson et al. 09],
[Novotney 10],[Isobe-Shirai 10].
Let Δ be a difference on the msb of each word of M.
Then, (X, M) and $(X \oplus f(\Delta), M \oplus \Delta)$ are related.

Rotational distinguisher [van Assche 10].

$$\mathcal{P}(X \lll 1, M \lll 1) = \mathcal{P}(X, M) \lll 1$$

with probability 2^{-159}.

Fixed points [Knudsen et al. 09].

New indifferentiability proof for a "biased" permutation

New framework [eprint 09].
It assumes that $\mathcal{Q}$ is drawn uniformly at random from $\mathbf{FUNC}' \subset \mathbf{FUNC}$.

Types of distinguishers which can be included:

- bias in the distribution of the output [eprint 09];
- related (input, output) pairs, *e.g.* differential and rotational distinguishers [this paper];
- weak inputs, *e.g.* fixed points [eprint 09].

New indifferentiability bound taking into account all known distinguishers.
Shabal is indifferentiable from a random oracle up to 2^{332} queries.

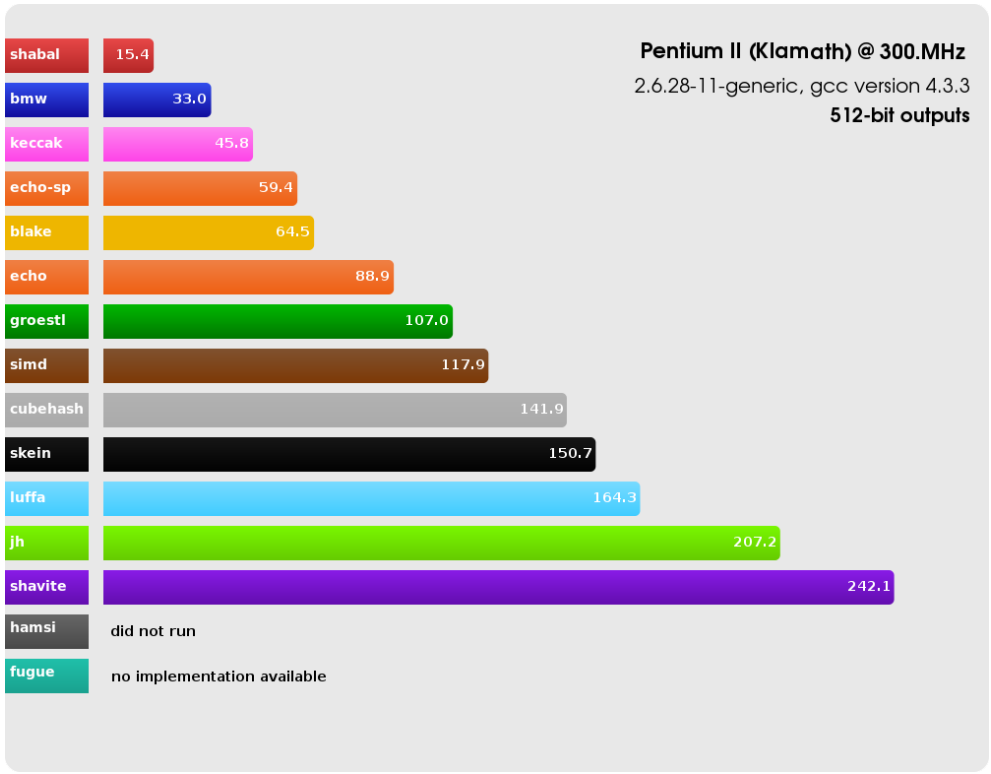
Analysis of weakened variants

- (second)-preimage attack in $\mathbf{2^{497}}$ in time and $\mathbf{2^{400}}$ in memory for 32 out of 48 rounds and without the final transformation in the inner permutation [Shabal team 09][Isobe, Shirai 10];
- (second)-preimage attack in $\mathbf{2^{497}}$ in time and $\mathbf{2^{272}}$ in memory for 24 out of 48 rounds and for a permutation with 768-bit inputs (instead of 896) [Isobe, Shirai 10].

Software performances

Smallest number of 32-bit arithmetic instructions per hashed bit [Jos, Stefan 10]

$\longrightarrow$ Among the fastest two candidates on almost any platform



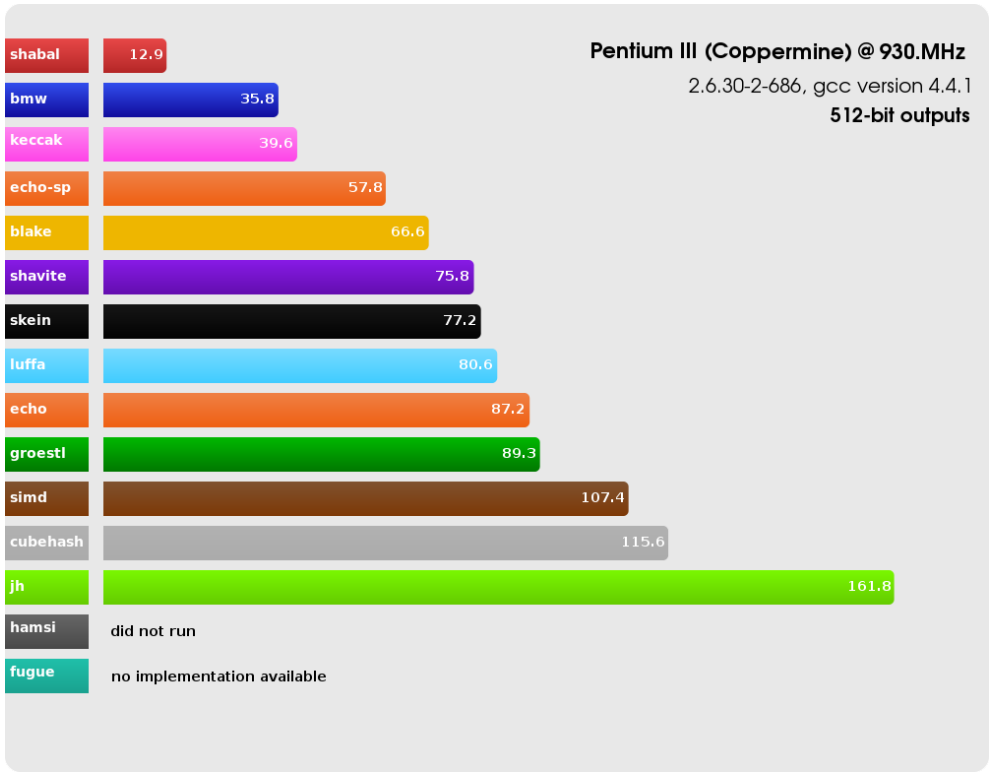
512-bit output, Pentium II `http://crypto.rd.francetelecom.com/ECHO/sha3/`

without 64-bit/AES/SIMD instructions.

Software performances

Smallest number of 32-bit arithmetic instructions per hashed bit [Jos, Stefan 10]

$\longrightarrow$ Among the fastest two candidates on almost any platform



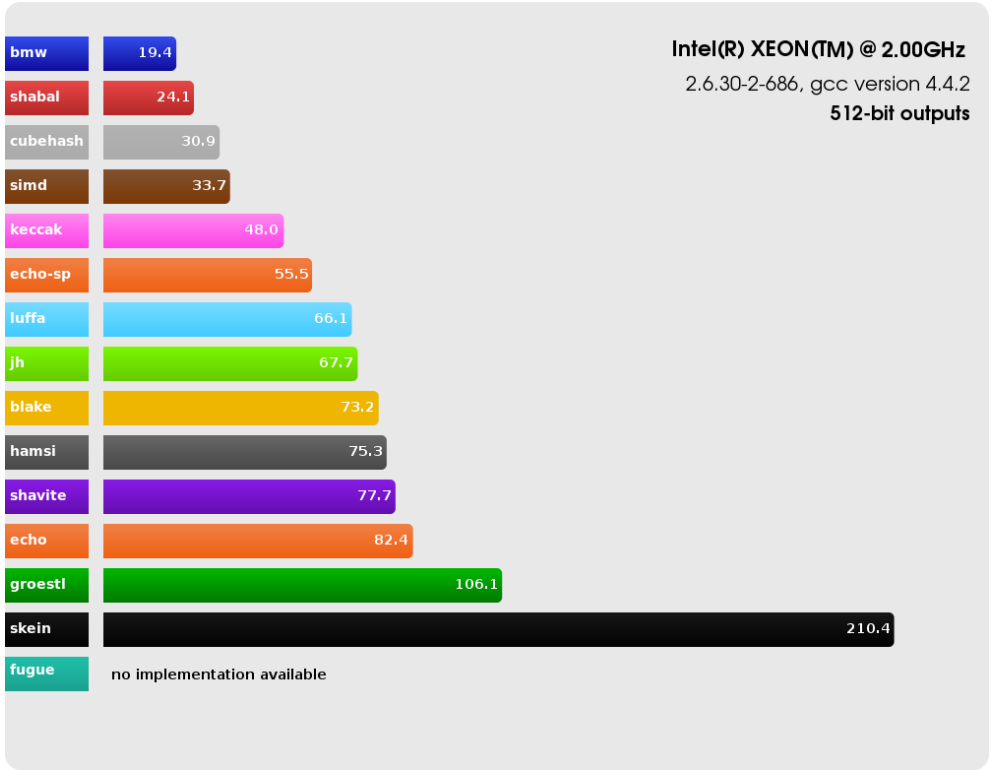
512-bit output, Pentium III `http://crypto.rd.francetelecom.com/ECHO/sha3/`

without 64-bit/AES/SIMD instructions.

Software performances

Smallest number of 32-bit arithmetic instructions per hashed bit [Jos, Stefan 10]

$\longrightarrow$ Among the fastest two candidates on almost any platform



512-bit output, Xeon `http://crypto.rd.francetelecom.com/ECHO/sha3/`

without 64-bit/AES/SIMD instructions.

Shabal can be made very small

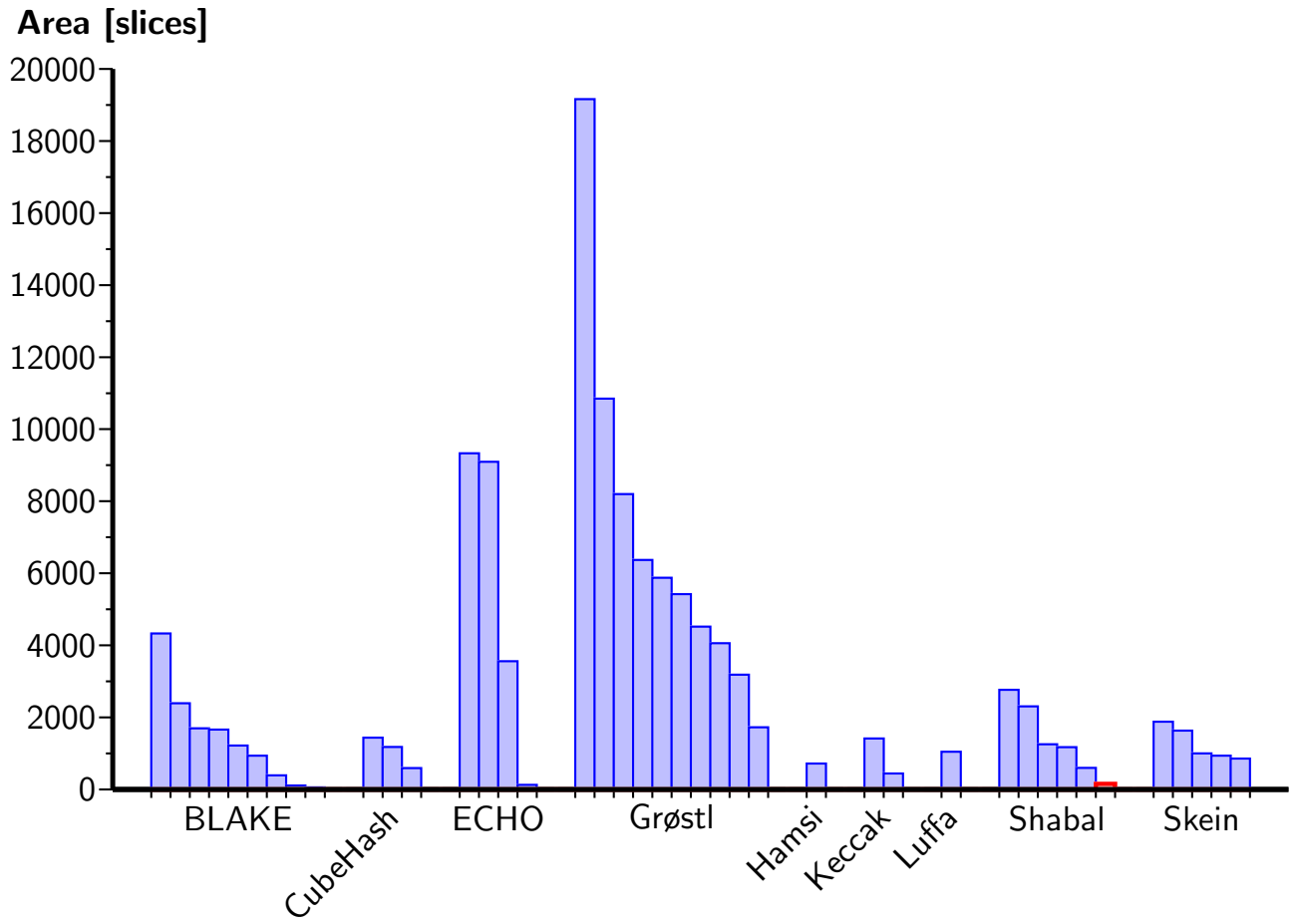
Compact implementation [Pornin 10].

Code size: 698 bytes

109 MB/s on a 2.4 GHz Core2 machine.

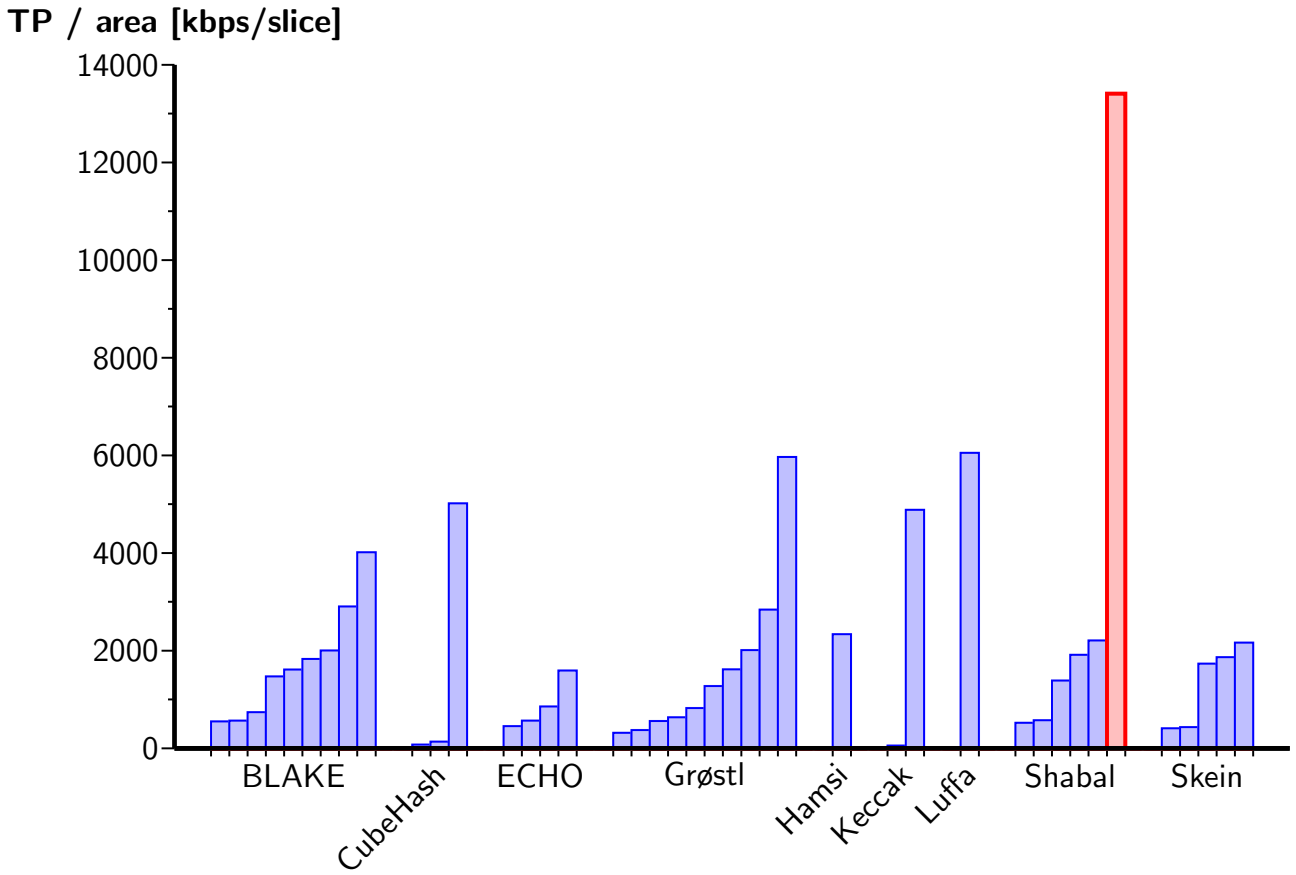
Hardware performances on Xilinx

[Detrey-Gaudry-Khalfallah 10, presented at SAC 2010]



Hardware performances on Xilinx

[Detrey-Gaudry-Khalfallah 10, presented at SAC 2010]



Why choosing Shabal?

- it has security proofs (indifferentiability, collision resistance and second-preimage resistance) which provide important safety margins;
- it has been studied by many external teams;
- single function for all output lengths;
- very fast software implementations (without any tricks);
- small footprint (in software and hardware).

Why choosing Shabal?

Otherwise, he won't be happy...