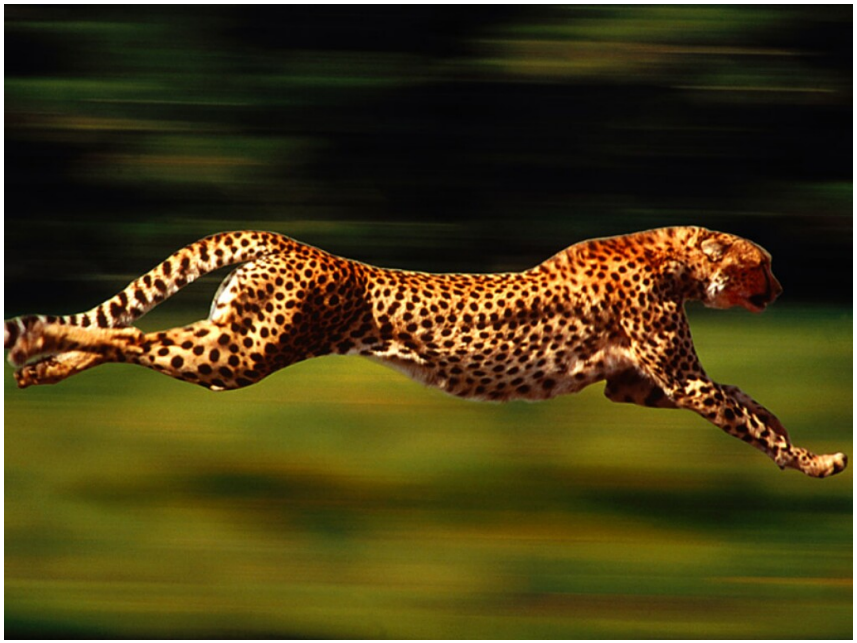


# Cheetah — the fastest AES-based hash function

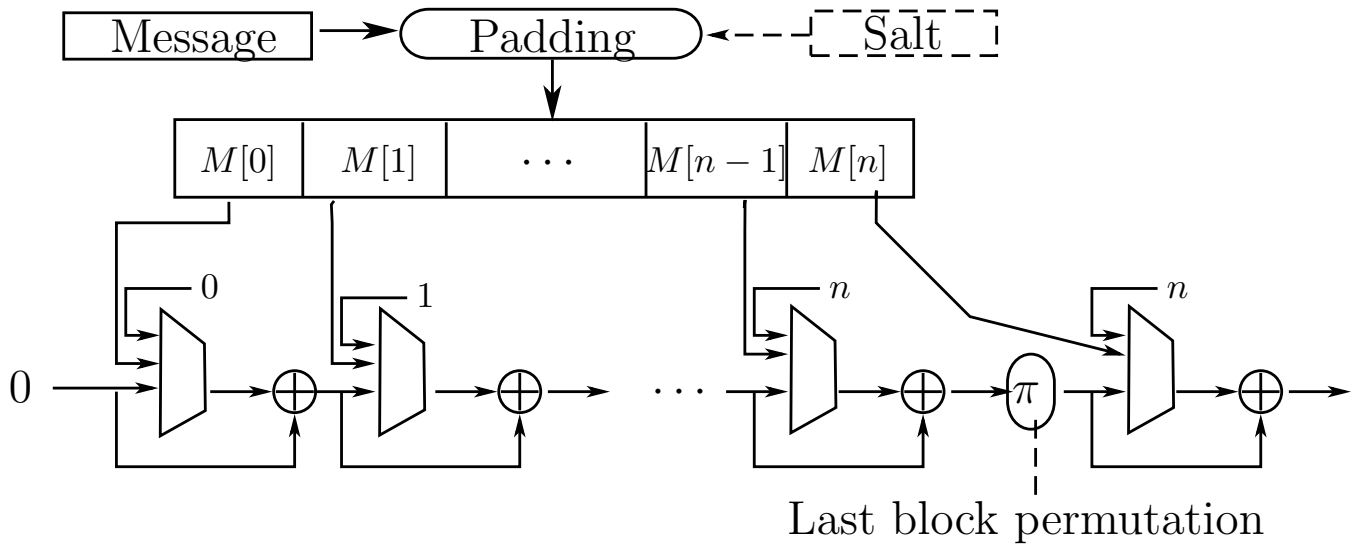
Dmitry Khovratovich, Alex Biryukov, Ivica Nikolić

University of Luxembourg

# Design of Cheetah

# Upper level

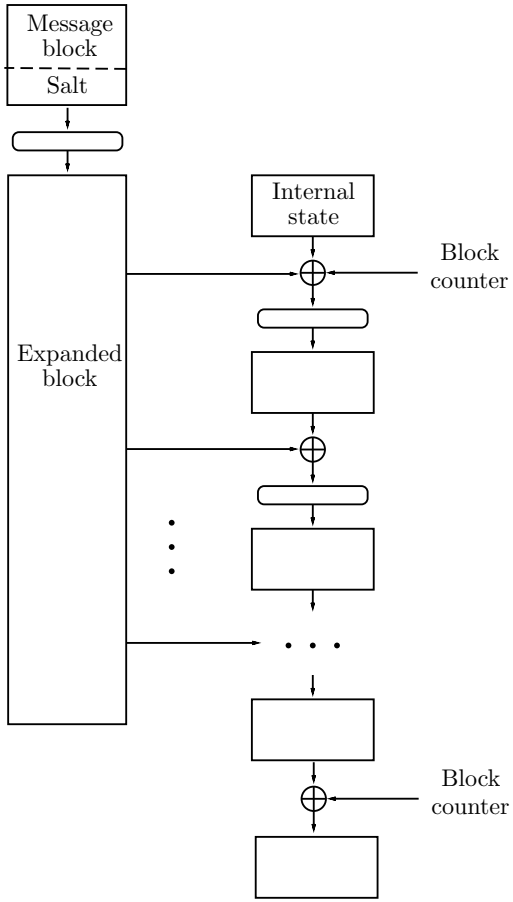
Strengthened Merkle-Damgard:




- Davies-Meyer mode for the compression function;
- Salt for randomized hashing (thx to HAIFA);
- Block counter against generic attacks;
- Permutation against length-extension attacks.

# Lower level-I

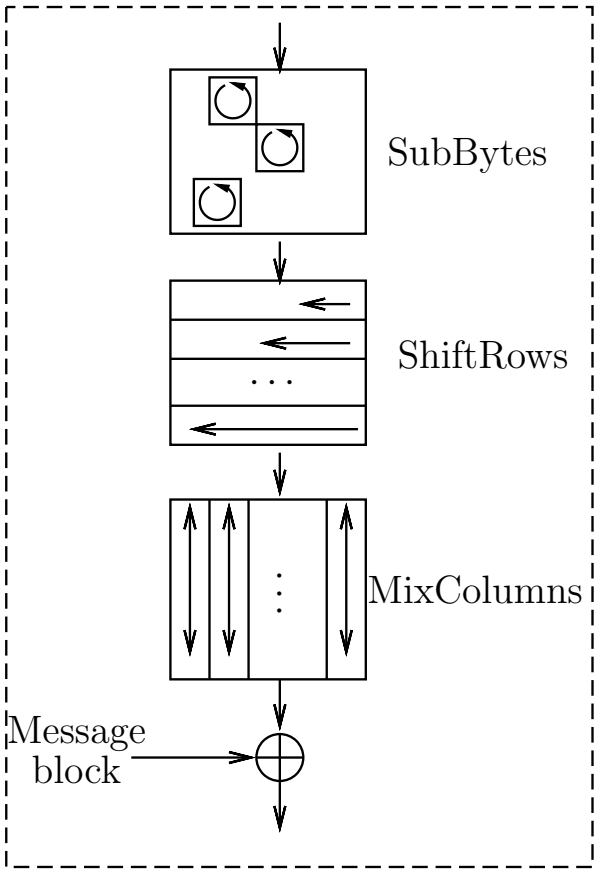
Compression function: AES speed + AES security.




- AES round function $\longrightarrow$ internal rounds;
- AES round function $\longrightarrow$ message expansion;
- 1024-bit message block;
- Cheetah-256,224: 256-bit internal state, 16 rounds;
- Cheetah-512,384: 512-bit internal state, 12 rounds.

# Lower level-II

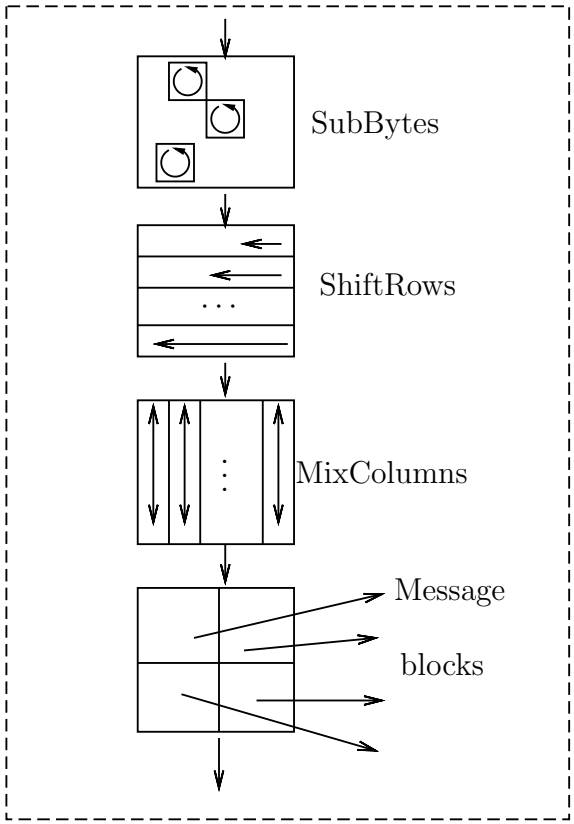
Internal round:




- Cheetah-256:
  - 16 rounds;
  - State $8 \times 4$.
- Cheetah-512:
  - 12 rounds;
  - State $8 \times 8$.
- *SubBytes* from AES;
- Adapted *ShiftRows* and *MixColumns*;
- Full diffusion after 4 rounds.

# Lower level-III

Message round:



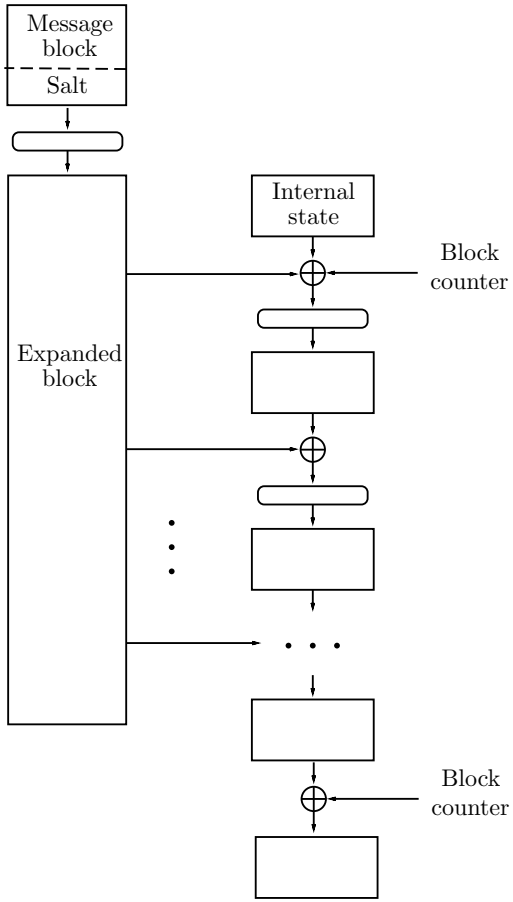

- 1024-bit block: $8 \times 16$.
- Cheetah-256:
  - 3 rounds;
  - 4 new message blocks per round.
- Cheetah-512:
  - 5 rounds;
  - 2 new message blocks per round.
- *SubBytes* from AES;
- Adapted *ShiftRows* and *MixColumns*;
- Full diffusion after 3 rounds.

# Why it is secure

# Hash function

| **Attack** | **Countermeasure** |
|---|---|
| Herding | Salt |
| Fast second preimage | Block counter |
| Length-extension | Permutation before the last block |
| Randomized hashing | Salt |

# Collisions for compression function

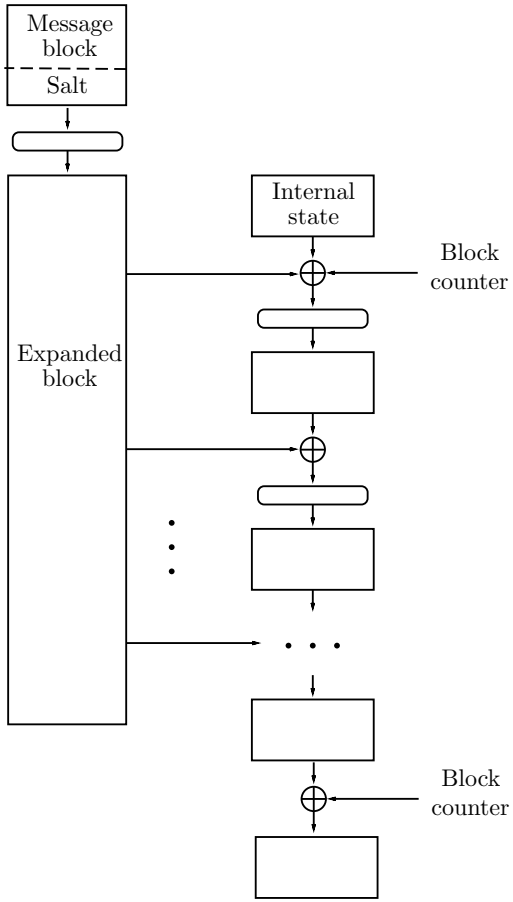



Cheetah-256:

- At least 81 active S-boxes in message expansion;
- At least 17 active S-boxes in internal rounds;
- Truncated differentials have high weight.

Similar bounds for Cheetah-512.

# Preimages for compression function




- Compression function is an AES-based block cipher;
- Search for a preimage is equivalent to key-recovery;
- Key recovery is expected to be hard.

# Why it is fast

# Speed estimates

Cycles per byte on reference platforms:

| | **256/224** | **512/384** |
|---|---|---|
| 32-bit | 15 | 15 |
| 64-bit | 9.3 | 13.6 |

# Main points

- "Message block"/"Internal state" ratio: 4 for Cheetah-256, 2 for Cheetah-512;
- Reasonable number of rounds;
- AES optimization tricks are applied.

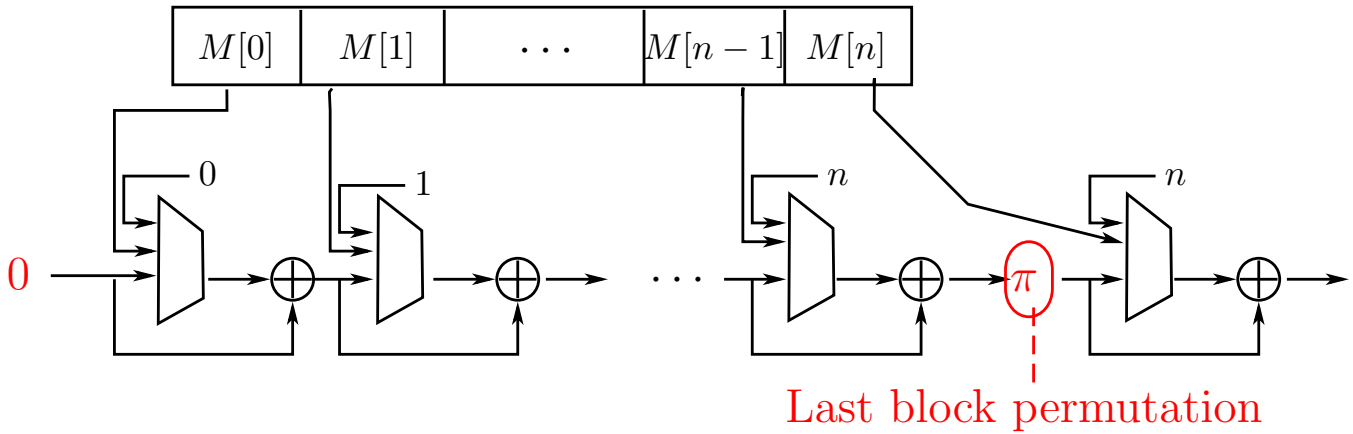
# Attacks

# Current attacks on Cheetah

- Mendel et al.: attack on 8.5 (of 12) rounds of Cheetah-512;
- Observation by Gligoroski on the length-extension resistance.

# Length-extension observation

- $\pi(a||b) = b||a$.
- $\pi(IV) = IV$, which is bad for short messages.




Trivially fixed by using $\pi'(x) = \pi(x) \oplus 1$.

- No effect on speed.
- No effect on the security of other elements.

# Summary

- The fastest AES-based proposal;
- Easy-to-understand design;
- No attacks on compression function.

# Questions?

Visit cryptolux.org/cheetah !