Practical Preimages for Maraca

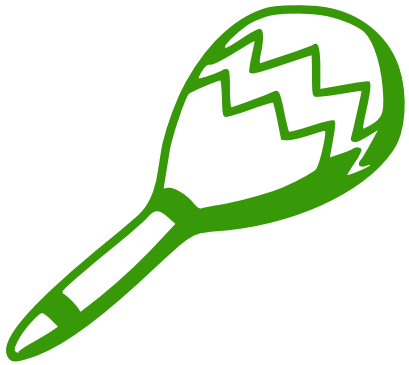
Sebastiaan Indesteege
sebastiaan.indesteege@esat.kuleuven.be

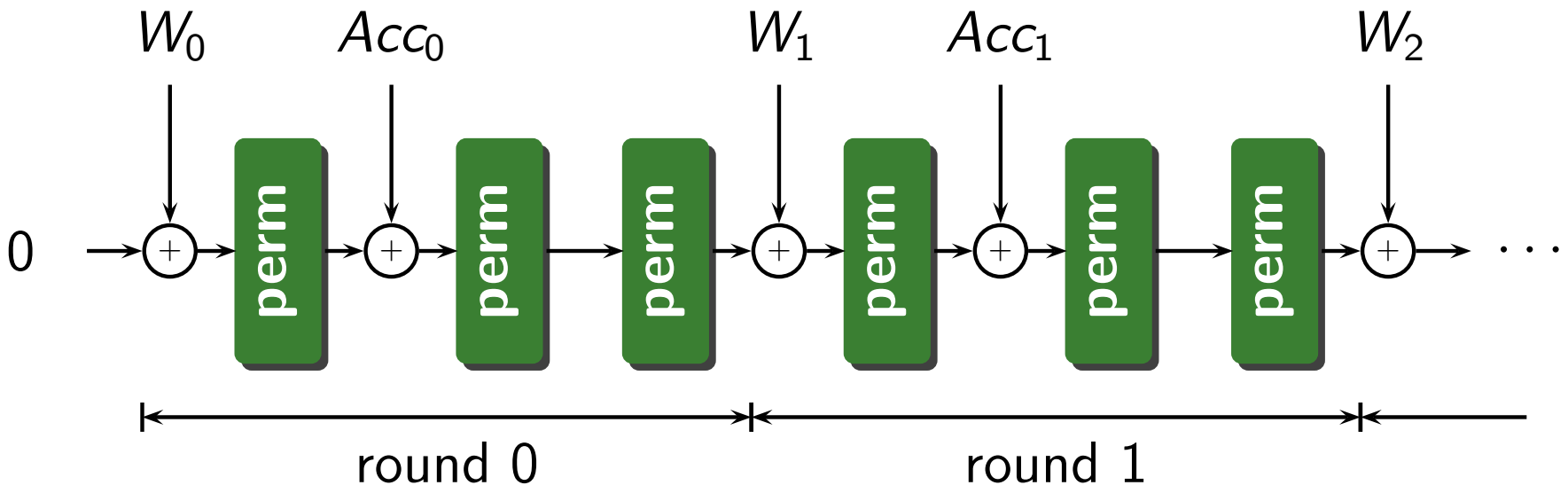
COSIC, ESAT, K.U. Leuven, Belgium

FSE 2009 Rump Session

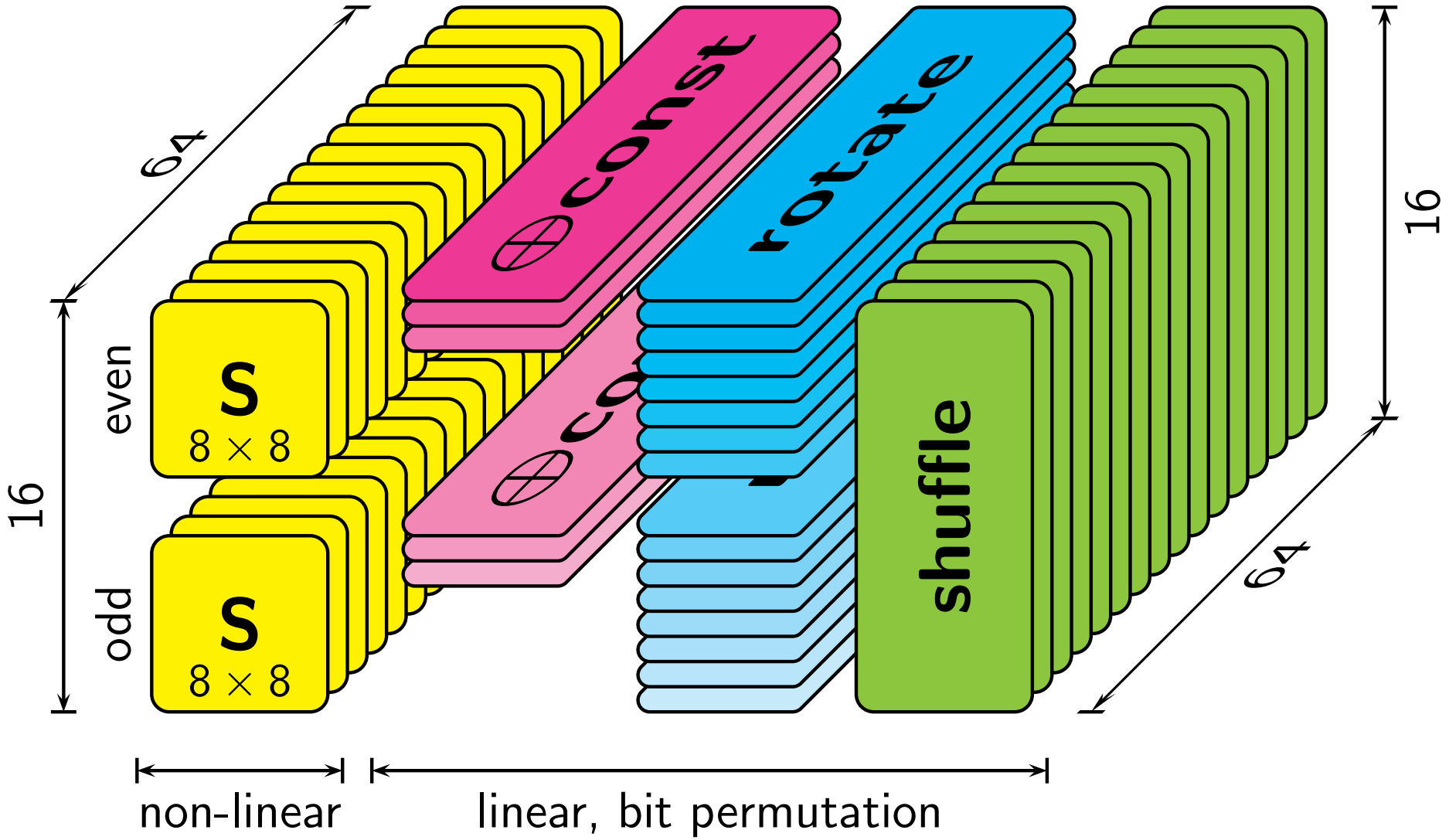
Maraca

- SHA-3 submission
  (not selected for round 1)
- Designer: Robert J. Jenkins Jr.





The Maraca permutation



A Preimage Attack on Maraca

Maraca's S-box

- 8×8 bit S-box
- Three output bits are **linear** functions of input bits
- And not very non-linear otherwise, either...

Idea

- Impose affine conditions on the S-box inputs
- **S-box $\rightsquigarrow$ affine function**
- Any 8×8 S-box: 7 conditions, trivial
- Maraca S-box: **only 3 conditions** required

A Preimage Attack on Maraca

Fast Forward

A Preimage Attack on Maraca

Result

- When restricted to a carefully chosen affine message space, Maraca becomes a **linear function**...

Practice

1. Precomputation
   - 32-node cluster *(AMD Opteron + Infiniband)*
   - 10.7 CPU-days, 20 GB of RAM *(distributed)*
   - **Result:** a 94 MB data file
2. Online Phase
   - **Live demo** *(available online the SHA-3 zoo)*