What happened to LANE?

Krystian Matusiewicz[1], María Naya-Plasencia[2],
Ivica Nikolić[3], Yu Sasaki[4], Martin Schläffer[5]

1: Technical University of Denmark (Denmark)
2: INRIA project-team SECRET (France)
3: University of Luxembourg (Luxembourg)
4: NTT Corporation (Japan)
5: IAIK, Graz University of Technology (Austria)

LANE

- SHA-3 Candidate
- Not appear in 2nd round

What happened to LANE?

Bruce Schneier doesn't know:

"(…) I am (…) most surprised not to see LANE."

What happened to LANE?

Actually, we don't know either…

What happened to LANE?

But, we do know *something*.

Our Results

Semi-free-start collisions on **full** compression function of LANE

	Time	Memory
LANE-256	$\mathbf{2^{96}}$	$\mathbf{2^{80}}$
LANE-512	$\mathbf{2^{224}}$	$\mathbf{2^{128}}$

Attack Impact

Valid

LANE hash function is still secure.

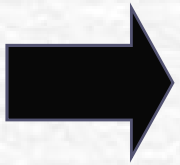
Invalid !!

LANE hash function is provably secure if underlying compression function is secure.

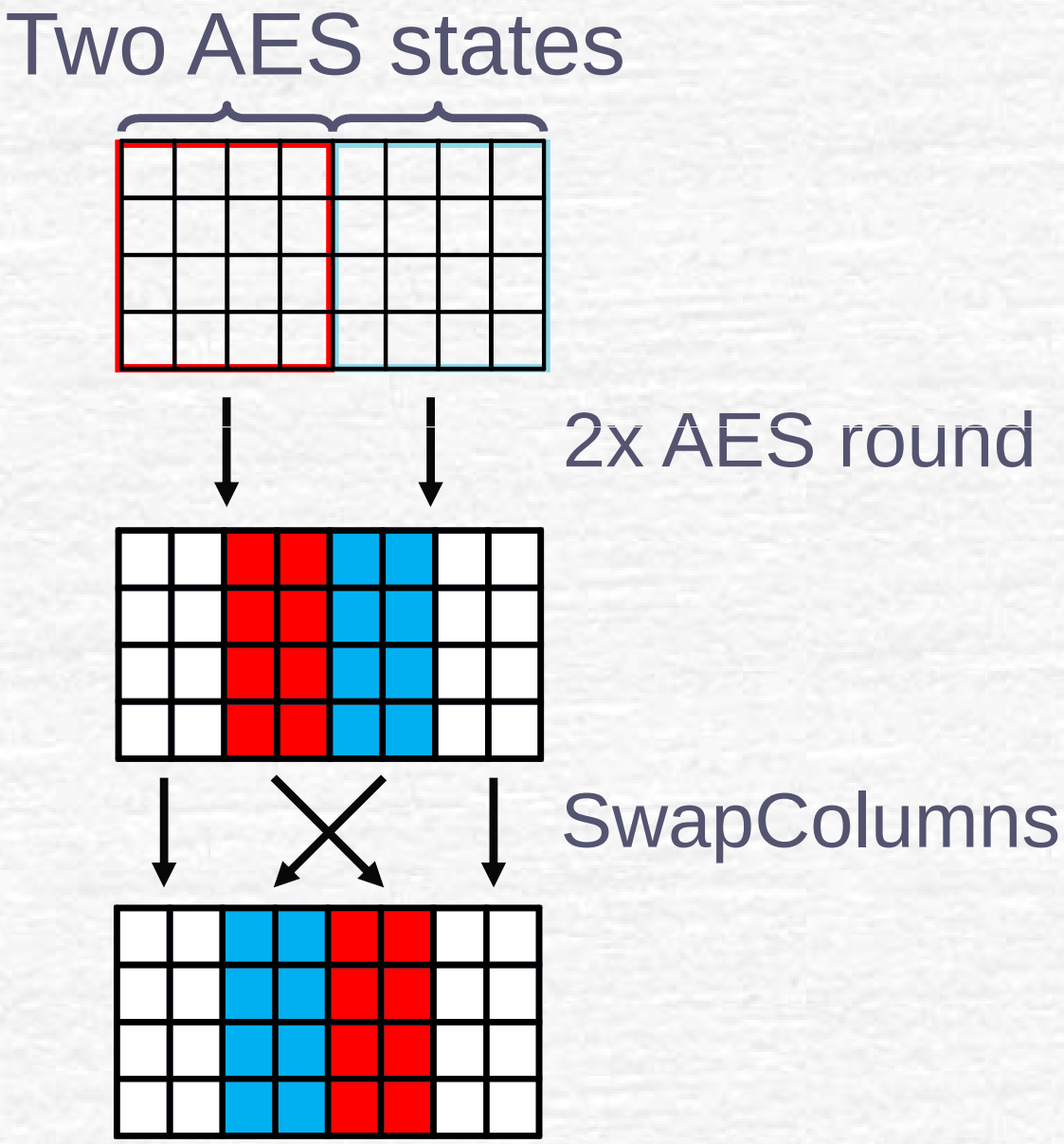
Attack Method

Improved rebound attack

1. Apply inbound phase at several places
2. Merge inbounds
3. Run outbound phase

 can satisfy longer differential path

LANE-256 Round Operation

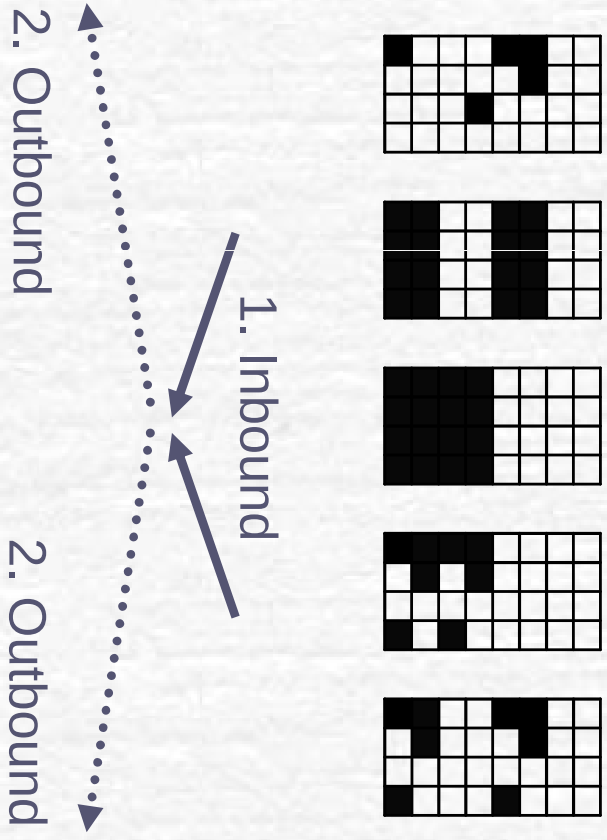


Only dependency in two AES states. (slow diffusion)

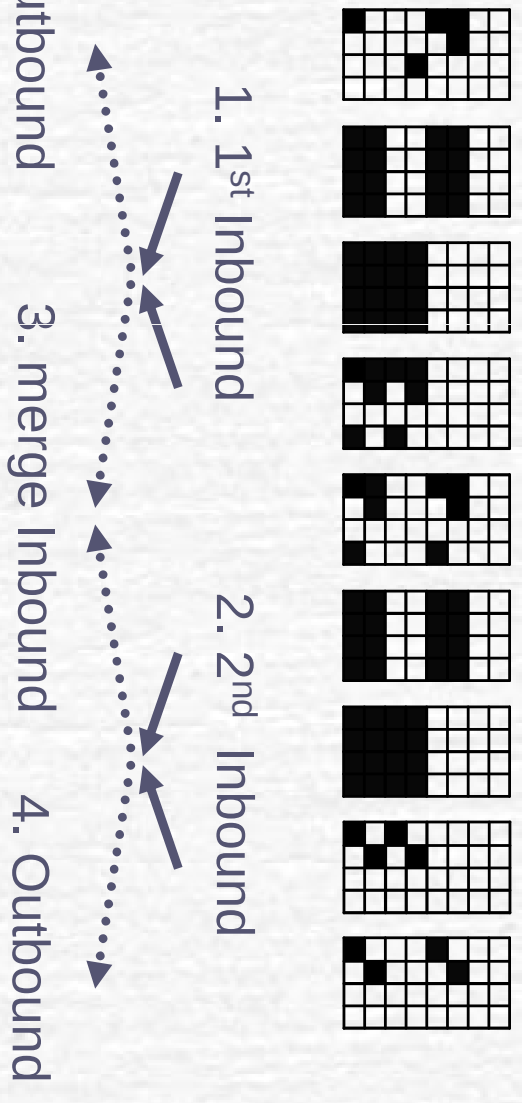
Enables us to merge several inbound phases.

Improved Rebound Attack

Previous

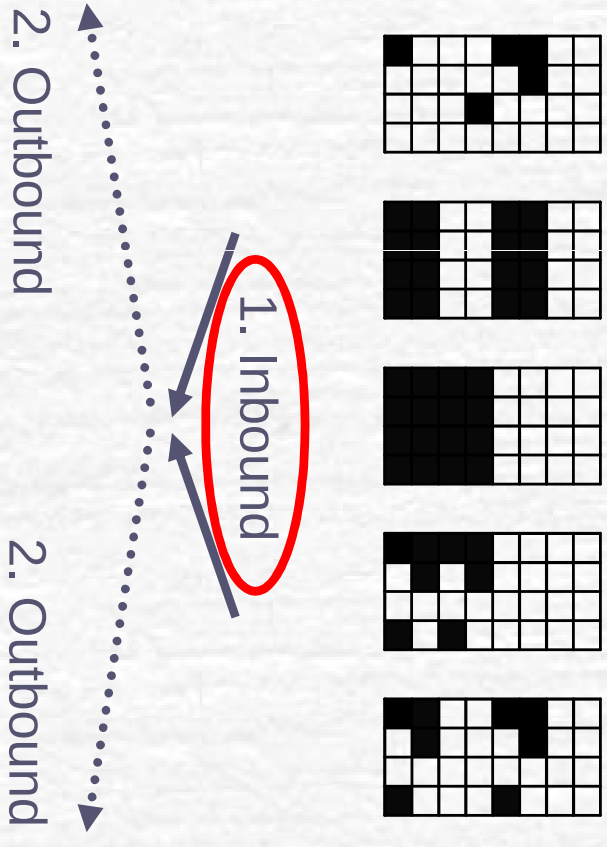


Ours

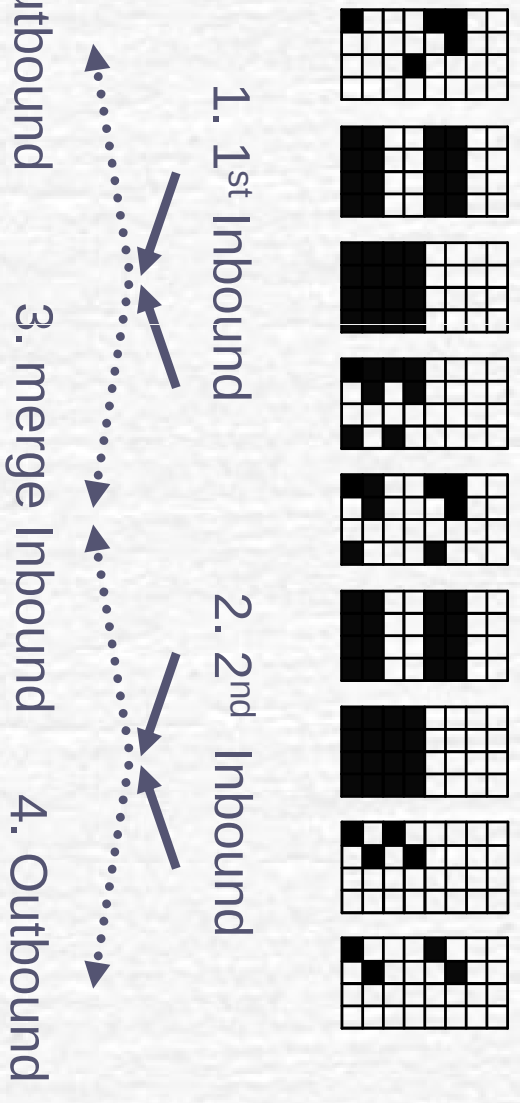


Improved Rebound Attack

Previous



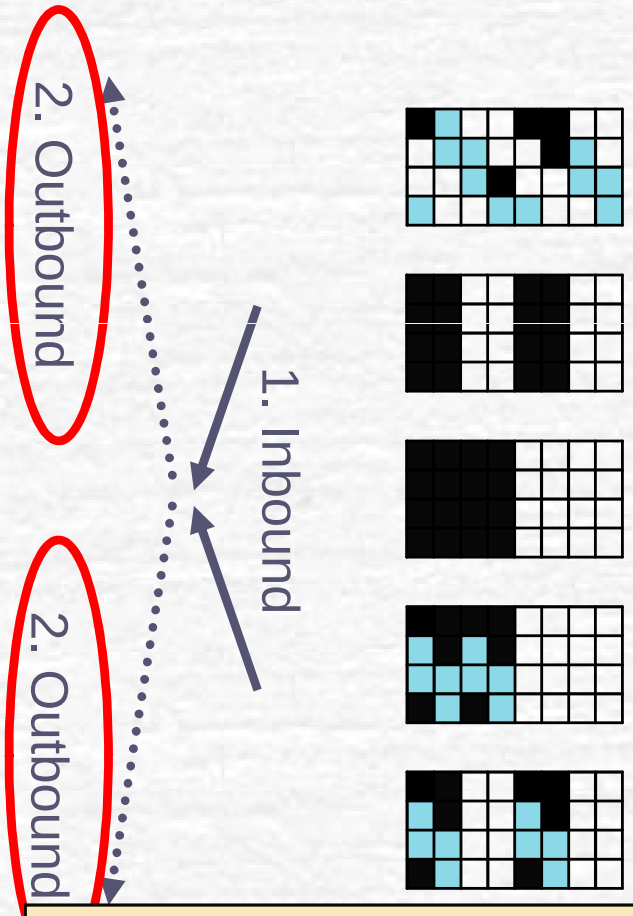
Ours



Match the differences.

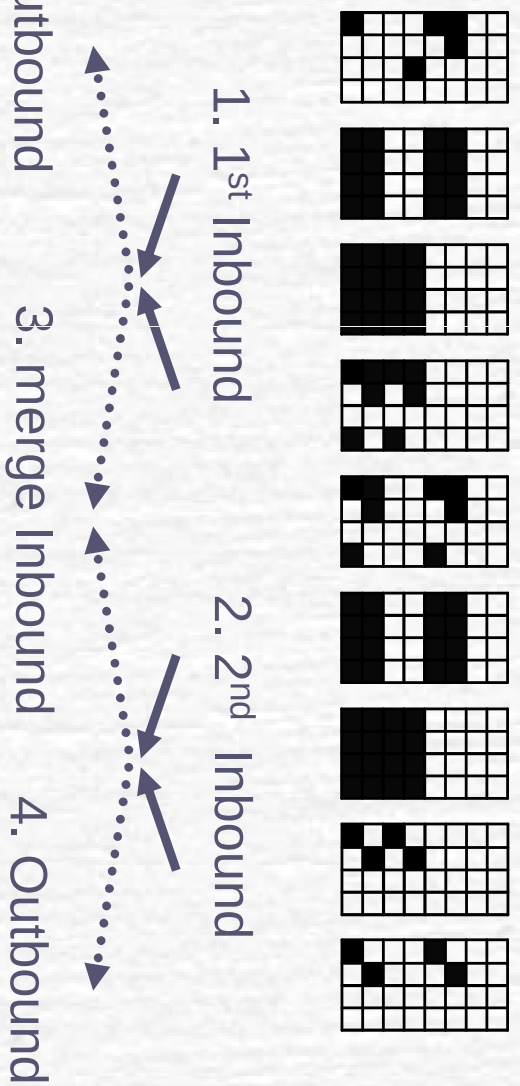
Improved Rebound Attack

Previous



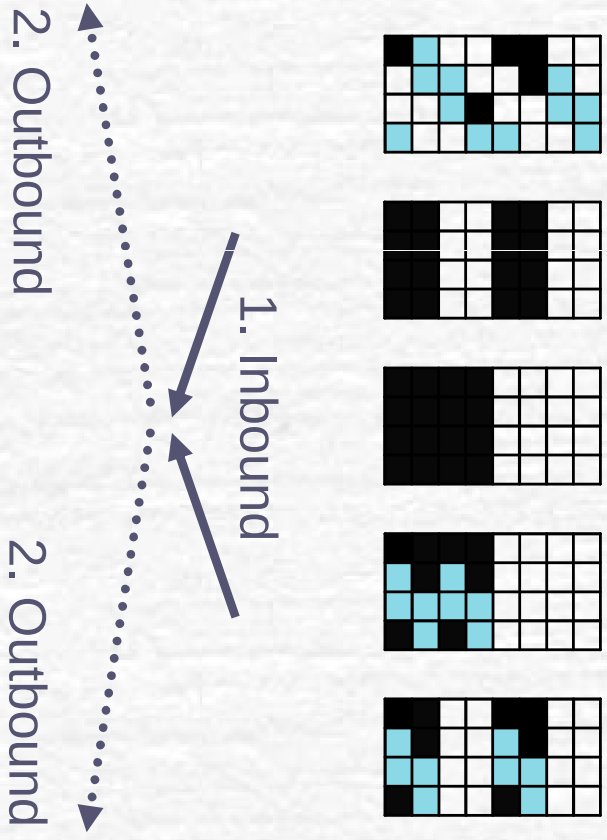
Obtain many values satisfying matched diffs.

Ours

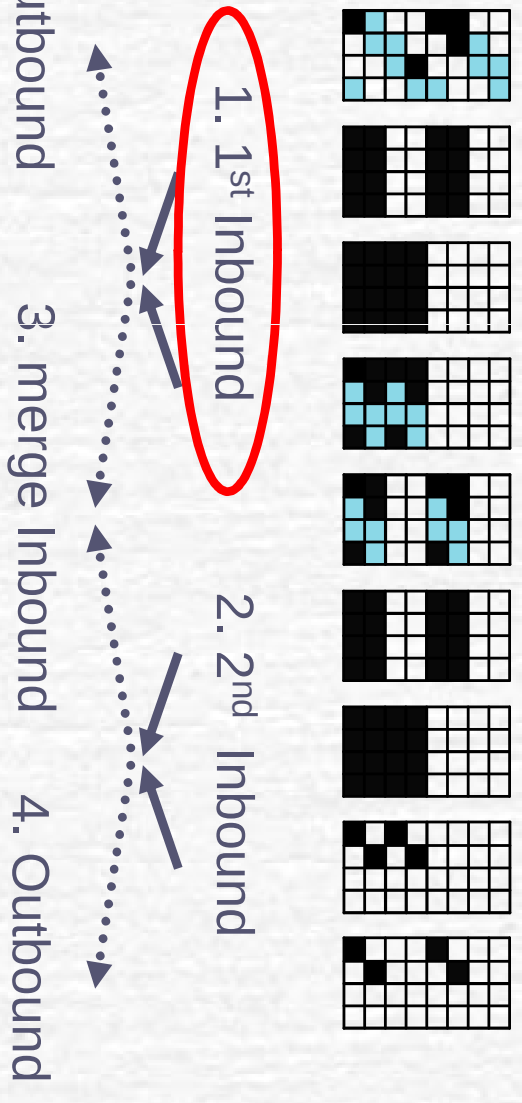


Improved Rebound Attack

Previous

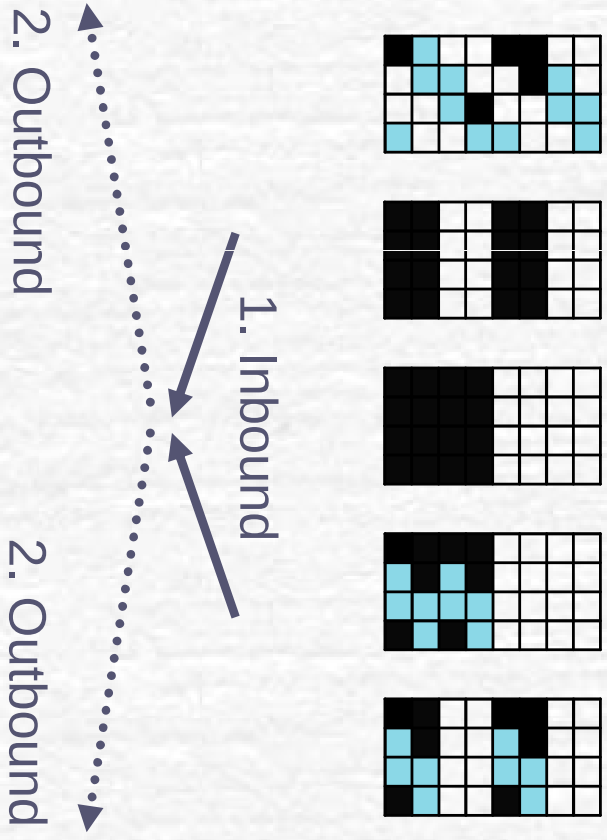


Ours

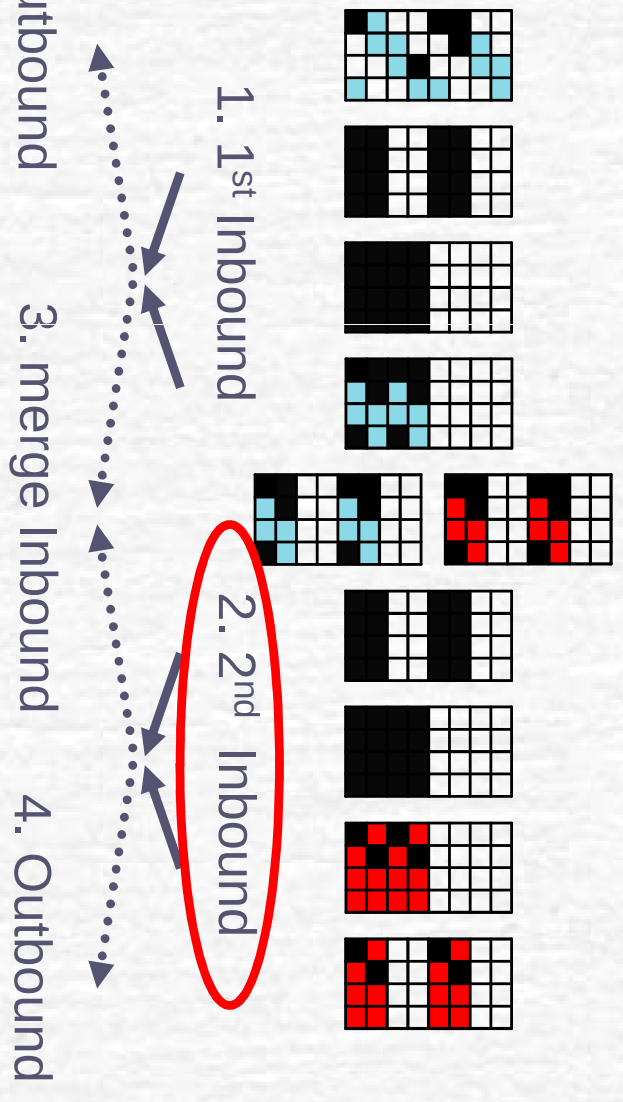


Improved Rebound Attack

Previous

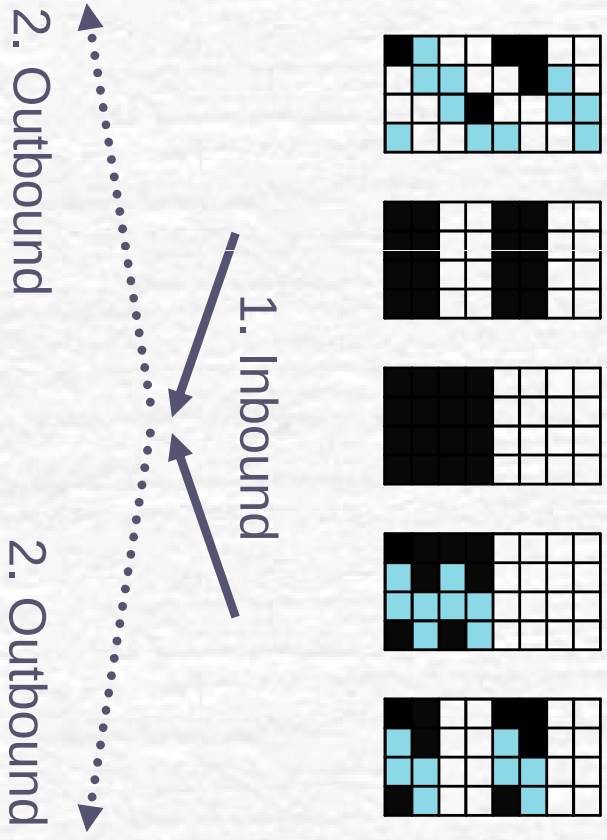


Ours

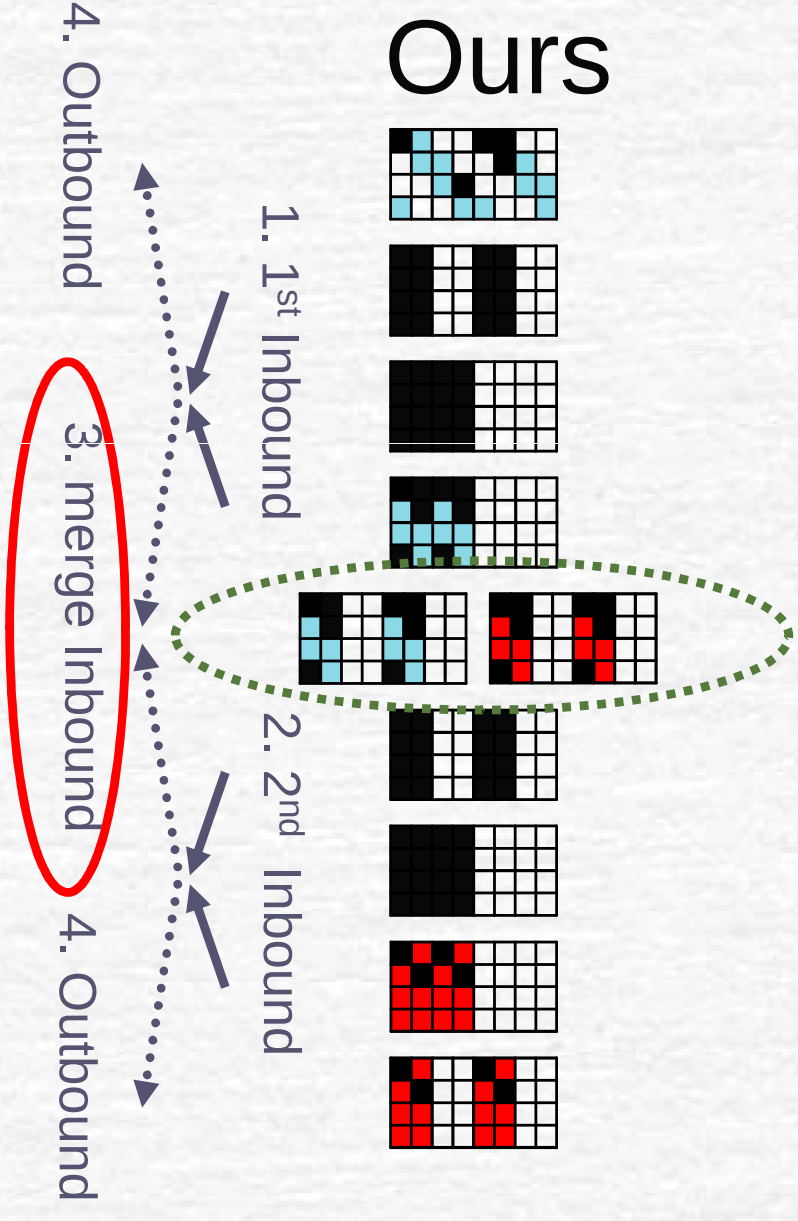


Improved Rebound Attack

Previous

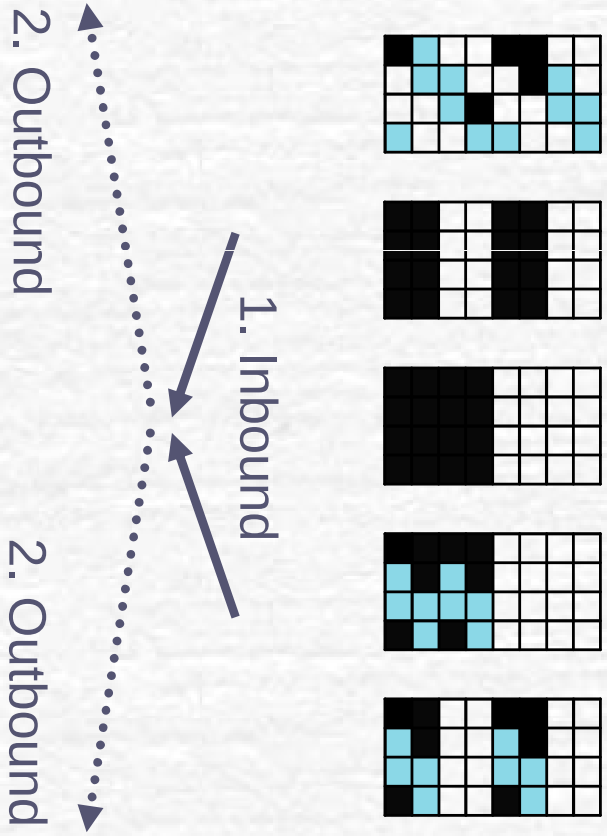


Ours

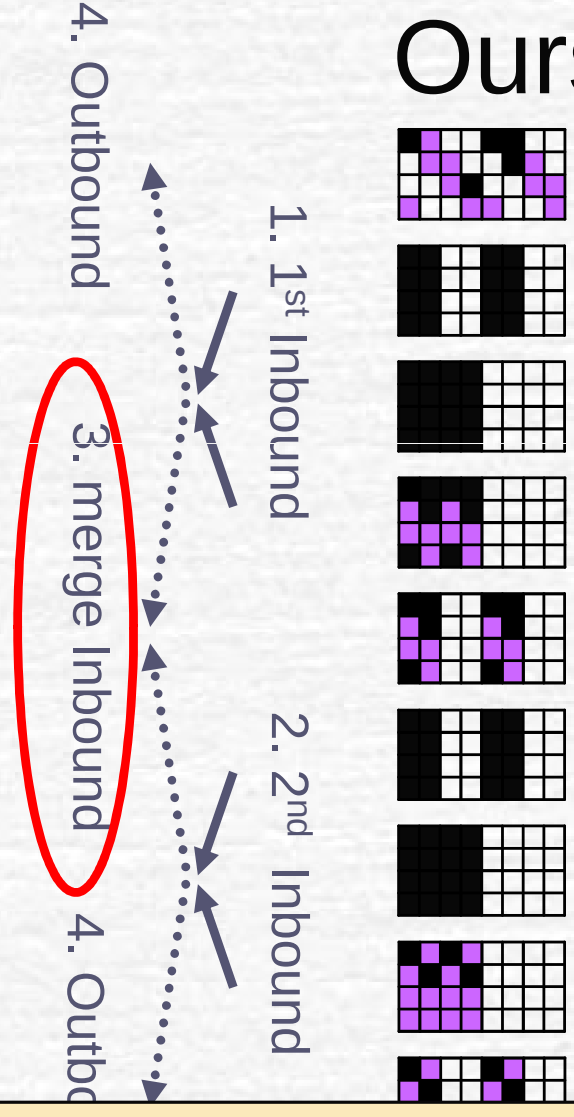


Improved Rebound Attack

Previous

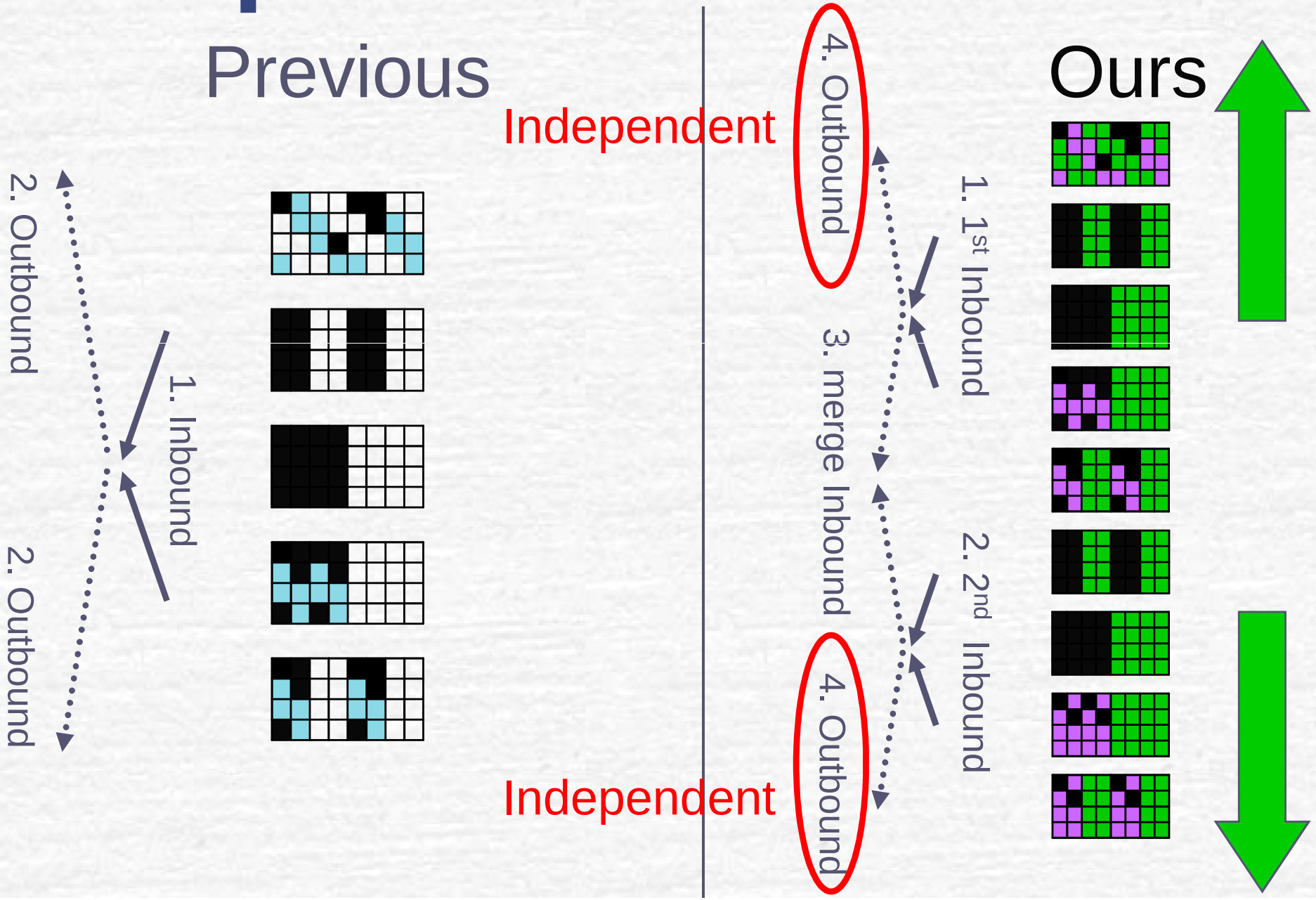


Ours



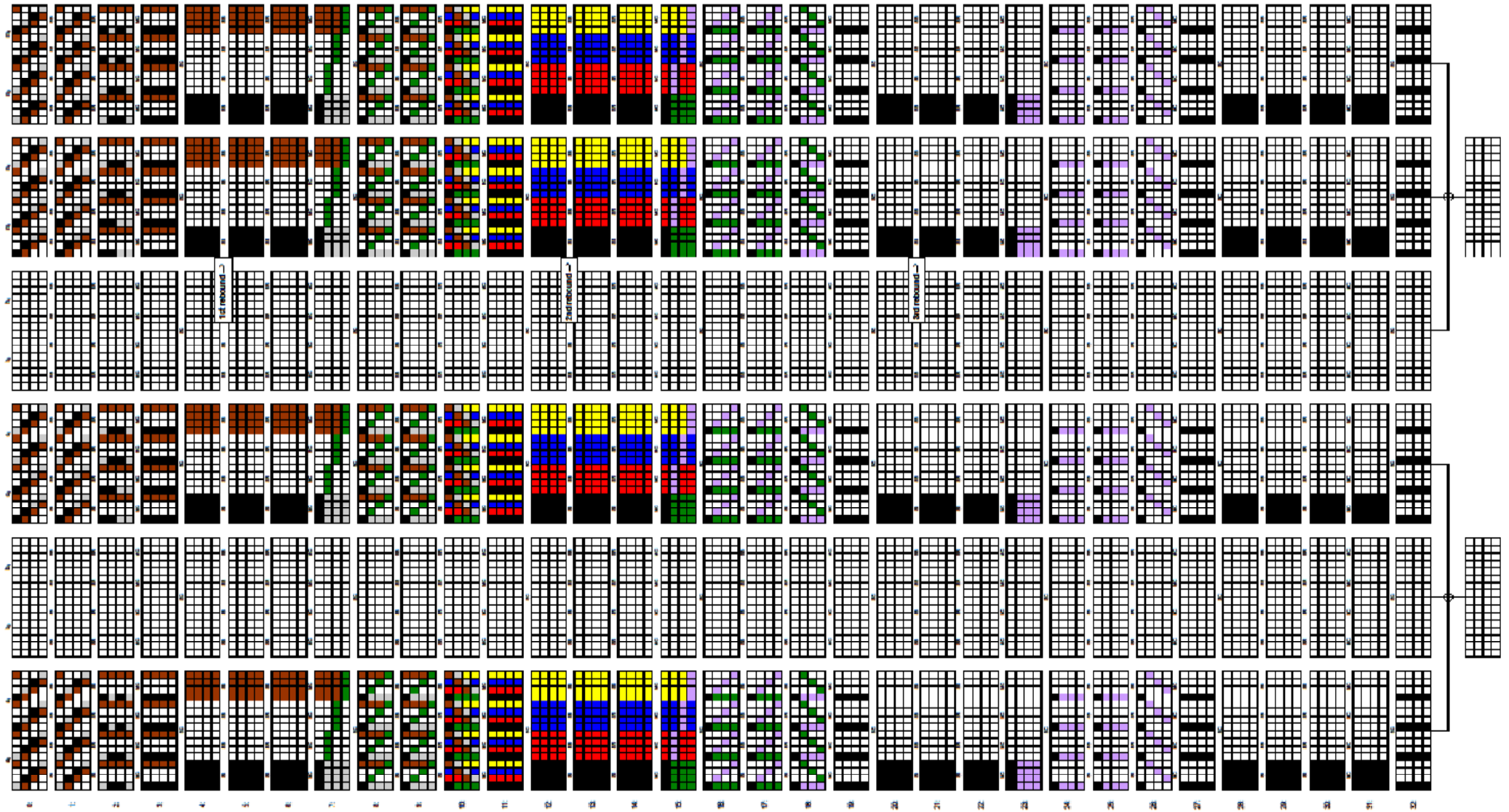
Lots of freedom remains.

Improved Rebound Attack



It's even easier for LANE-512

It's even easier for LANE-512



Summary

- Semi-free-start collision attacks on full LANE-256 and LANE-512.
- More details in the ASIACRYPT'09 paper:

Rebound Attack on the Full LANE Compression Function

Kristian Matusiewicz, María Naya-Plasencia, Ivica Nikolić, Yu Sasaki, Martin Schläffer

Thanks for your attention !