Rotational Rebound Attack on Reduced Skein

Dmitry Khovratovich, University of Luxembourg
Ivica Nikolić, University of Luxembourg
Christian Rechberger, KU Leuven

Content of this talk

- Background
  - Rotational attacks
  - Rebound approach
- Skein
- Rotational property + Rebound approach =
  Attack on reduced Skein
  (almost 80% of the rounds)
- Discussion

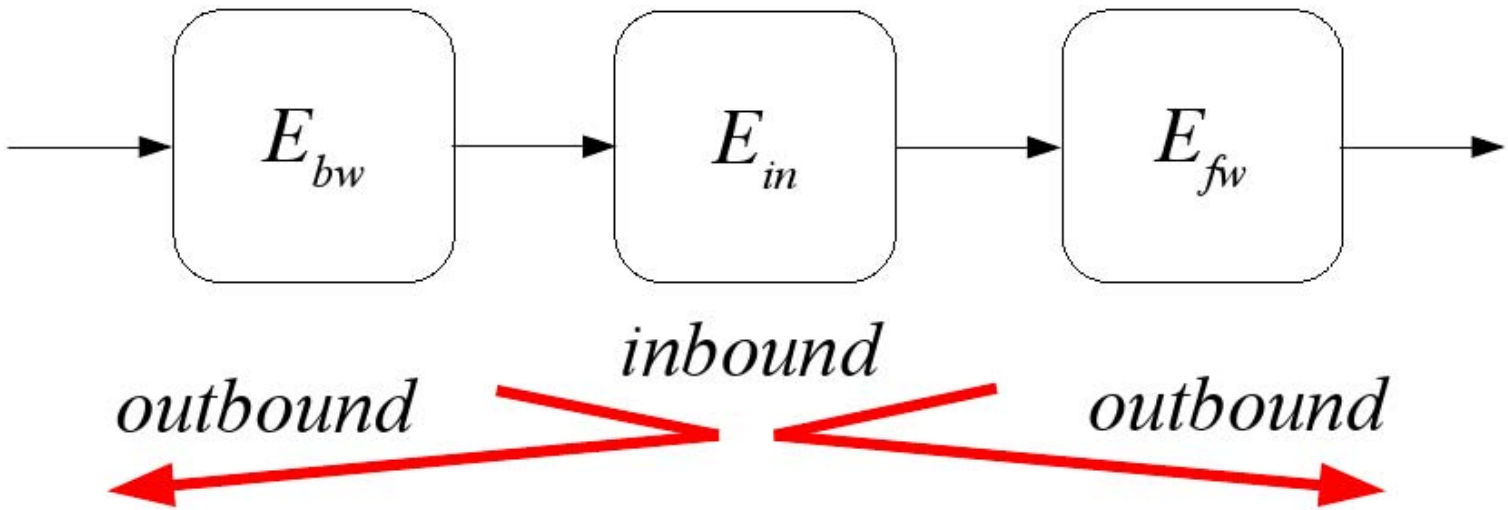
Rotational attacks

Several mention in the last 15+ years by
Bernstein, Biham, Dunkelman et al.,
Kelsey et al., Leander, Standaert et al, ...

Most recently generalized to ARX constructions and applied to reduced Threefish by
Khovratovich and Nikolić, FSE 2010

Rebound approach

A new variant of differential cryptanalysis:



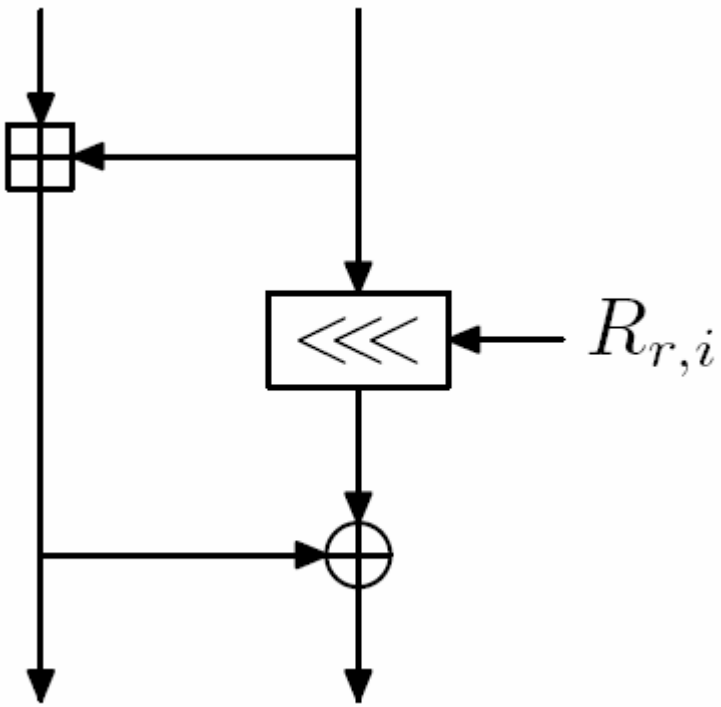
Developed during the design of Grøstl [MRST09]

Already successfully applied to Whirlpool and several SHA-3 candidates

Skein

- Block-cipher based design
- Add-Rotate-Xor as building blocks
- 72 rounds

Rotational property of basic Skein transformation

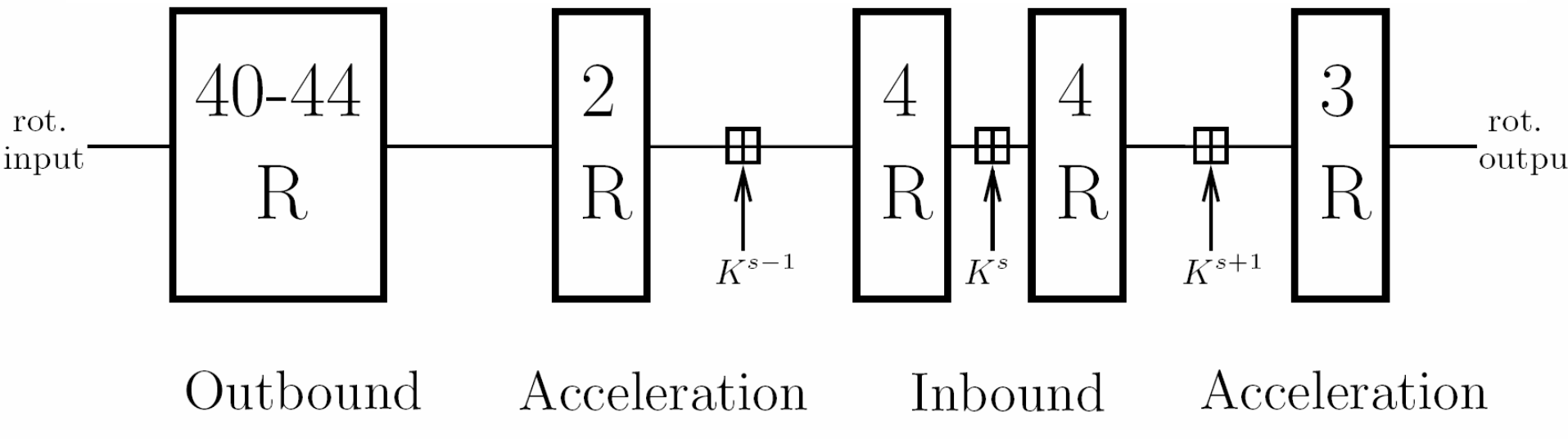


probability is between 0.375 and 0.25

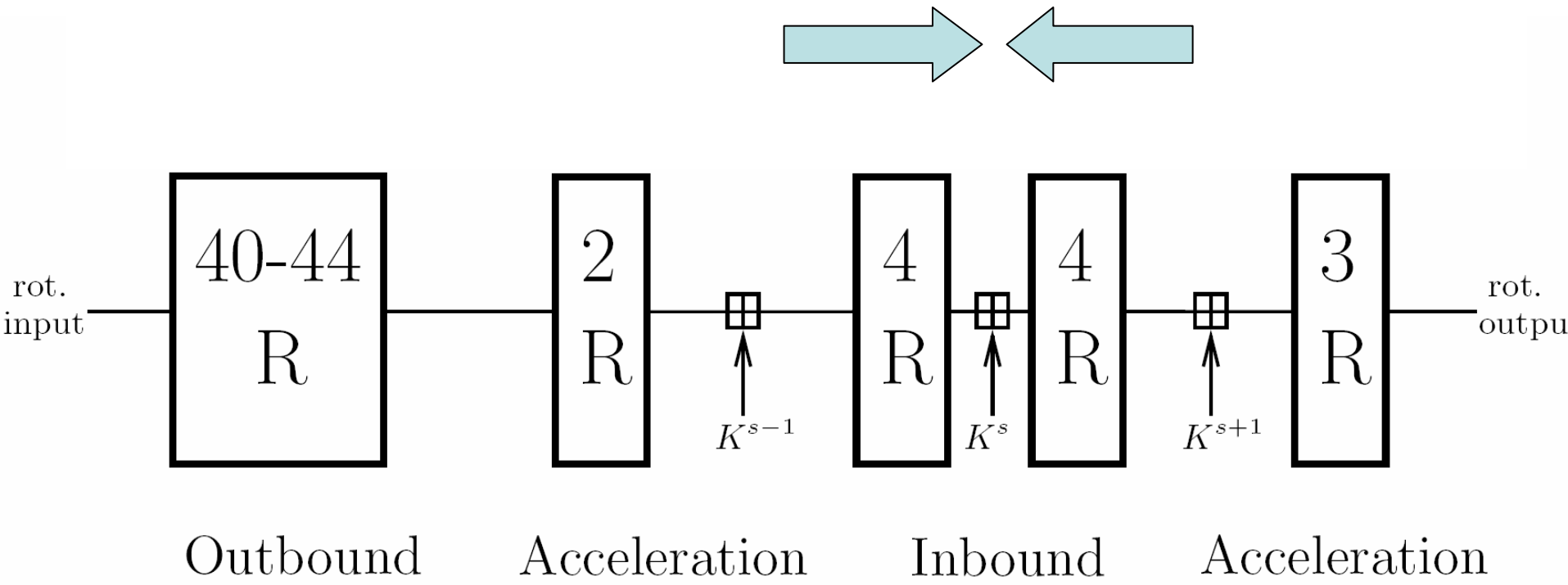
Results

Rounds	Attack	Method
Skein/Threefish-256 (72 rounds)		
24*	Key recovery	Related-key differential
39	Key recovery	Related-key rotational
53	Distinguisher	Rotational rebound
Skein/Threefish-512 (72 rounds)		
25*	Key recovery	Related-key differential
33*	Key recovery	Related-key boomerang
35*	Key recovery	Known-related-key distinguisher
42	Distinguisher	Related-key rotational
57	Distinguisher	Rotational rebound

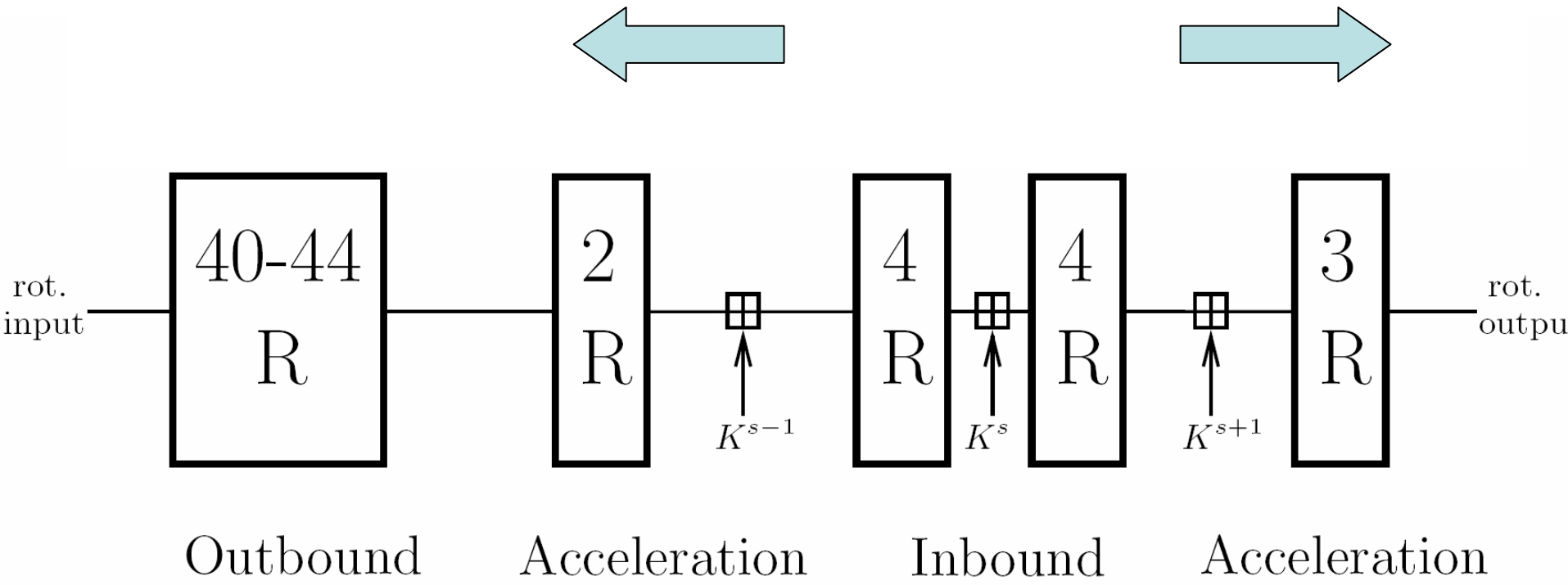
The basic approach



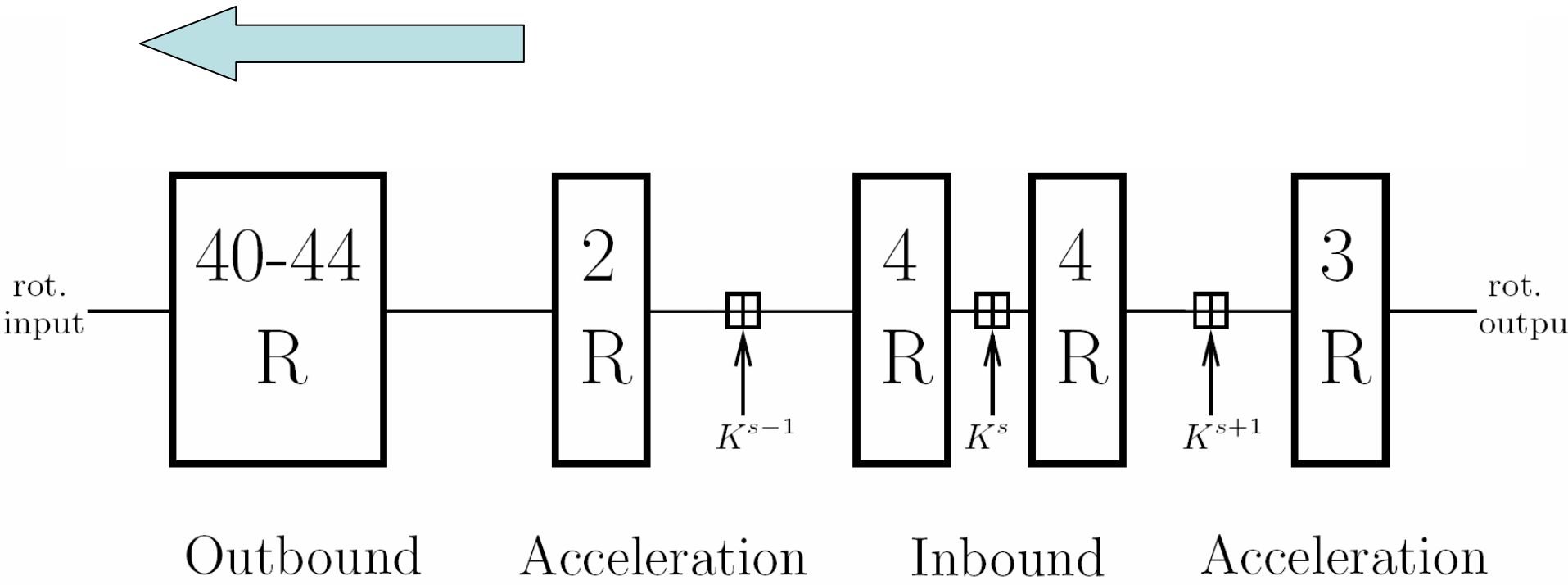
Inbound part



Acceleration part



Outbound part



Some details

- Modular corrections instead of xor corrections
- By putting simple linear constraints on inputs, paths are improved **throughout all** the rounds
  - The same property makes the SHA-1 collision attacks possible in the first place
- Matching is helped using simple neutral bit techniques

What „distingiusher“?

No handwaving, the approach:

1. Define distinguishing property: *rotational collision*
2. Prove lower bound on query complexity of a black box adversary
3. Show that cryptanalytic attack is faster than lower bound

See also

Biryukov et al, Crypto 2009

Lamberger et al, Asiacrypt 2009

Interpretation of results

Results valid for almost 80% of the rounds:

- Rotational collisions of the compression function
- Rotationally colliding input/output pairs for the cipher Threefish in the open-key model

Discussion

Impact of Results on Skein hash

- Results only on cipher and compression functions

- Extensions to hash function?
  - UBI mode facilitates this
  - less degrees of freedom → less rounds

- Easy tweak: change of constant will shorten outbound part
- Differential instead of rotational?

Rebound approach on other ARX primitives?

- Still to be done
- Mostly differential rather than rotational
- Needed:
  - Tools for constructing complex paths
    Since Dobbertin and Wang, we know this can be done
  - Lots of motivation, time, and hard work

Conclusions

- Rotational property + Rebound approach = Attack on reduced Skein (almost 80% of the rounds)
- No direct impact on hash security

- Rebound approach on ARX is a big „todo“, but *very* complicated

Rotational Rebound Attack on Reduced Skein

Dmitry Khovratovich, University of Luxembourg
Ivica Nikolić, University of Luxembourg
Christian Rechberger, KU Leuven