Revenge of the Boomerang

Alex Biryukov and Dmitry Khovratovich

University of Luxembourg

EUROCRYPT 2010
Monaco
1 June 2010

Fall 2009: Sean Murphy's “Return of the Boomerang”;

Boomerang may have returned for the last time...

Fall 2009: Sean Murphy's
"Return of the Boomerang";

Boomerang may have returned for the last time...

Winter 2010: Orr and Adi's Sandwich counterattacks!

We still believe in the Boomerang!

Current results on AES-256:

Attack	Rounds	Time	Source
Related-key boomerang	14	$2^{99.5}$	2009

Current results on AES-256:

Attack	Rounds	Time	Source
Related-key differential	9	2^{26}	Today
Related-key differential	10	2^{45}	Today
Related-key differential	11	2^{70}	Today
Related-key boomerang	14	$2^{99.5}$	2009

Current results on AES-256:

Attack	Rounds	Time	Source
Related-key differential	9	2^{26}	Today
Related-key differential	10	2^{45}	Today
Related-key differential	11	2^{70}	Today
???	12	???	???
???	13	???	???
Related-key boomerang	14	$2^{99.5}$	2009

What is the best for AES?

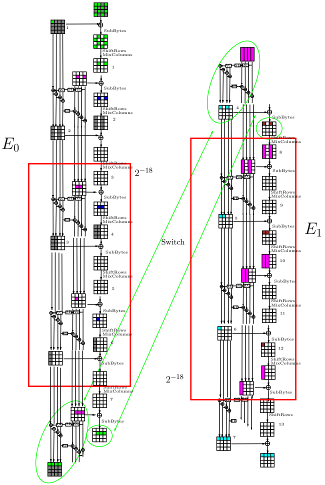
What is the best weapon against AES?

What is the best for AES?

What is the best weapon against AES?

Certainly, the Boomerang-man!

Not just simple boomerang



Tons of tricks:

- S-box switch;
- Feistel switch;
- Ladder switch.

Finally,

Attack	**Rounds**	**Time**	**Source**
Related-key differential	9	2^{26}	Today
Related-key differential	10	2^{45}	Today
Related-key differential	11	2^{70}	Today
Related-key boomerang	13	2^{76}	**Now**
Related-key boomerang	14	$2^{99.5}$	2009