Rethinking IDEA

Orr Dunkelman

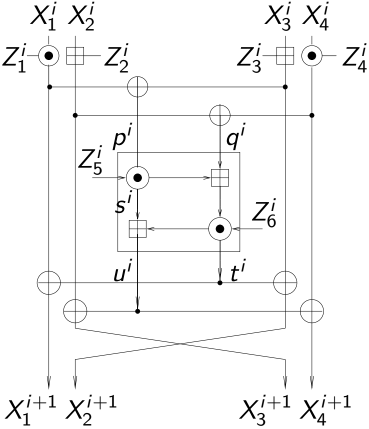
Department of Computer Science, University of Haifa
Faculty of Mathematics and Computer Science
Weizmann Institute of Science

16 August, 2011

Joint work with Eli Biham, Nathan Keller, and Adi Shamir

IDEA

- 64-bit block, 128-bit key block cipher
- Presented by Lai and Massey in 1991
- Widely used in many applications
- Has 8.5 rounds
- A “red cape” for cryptanalysts — more than 20 research papers.



Previous Results on IDEA

Rounds	Attack Type	Data	Time	Source
2	Differential	2^{10} CP	2^{40}	[M93]
2.5	Differential	2^{10} CP	$2^{104.7}$	[M93]
3	Differential-Linear	2^{29} CP	2^{44}	[BKR97]
3.5	Differential	2^{56} CP	2^{67}	[BKR97]
3.5	Linear	103 KP	2^{97}	[J05]
4	Impossible Differential	$2^{36.6}$ CP	$2^{66.6}$	[BBS99]
4	Linear	114 KP	2^{114}	[NPV04]
4.5	Impossible Differential	2^{64} KP	$2^{110.4}$	[BBS99]
5	Demirci-Selçuk-Türe	2^{24} CP	2^{126}	[DST03]
5	Demirci-Selçuk-Türe	$2^{24.6}$ CP	2^{124}	[AS06]
5.5	Key-dependent Linear	2^{21} CP	$2^{112.1}$	[SL09]
6	Key-dependent Linear	2^{49} CP	$2^{112.1}$	[SL09]

Previous Results on IDEA

Rounds	Attack Type	Data	Time	Source
2	Differential	2^{10} CP	2^{40}	[M93]
2.5	Differential	2^{10} CP	$2^{104.7}$	[M93]
3	Differential-Linear	2^{29} CP	2^{44}	[BKR97]
3.5	Differential	2^{56} CP	2^{67}	[BKR97]
4	Impossible Differential	$2^{36.6}$ CP	$2^{66.6}$	[BBS99]
4.5	Impossible Differential	2^{64} KP	$2^{110.4}$	[BBS99]
5	Demirci-Selçuk-Türe	$2^{24.6}$ CP	2^{124}	[AS06]
5.5	Key-dependent Linear	2^{21} CP	$2^{112.1}$	[SL09]
6	Key-dependent Linear	2^{49} CP	$2^{112.1}$	[SL09]
4.5	Meet-in-the-Middle	2 KP	2^{103}	**New!**

Previous Results on IDEA

Rounds	Attack Type	Data	Time	Source
2	Differential	2^{10} CP	2^{40}	[M93]
2.5	Differential	2^{10} CP	$2^{104.7}$	[M93]
3	Differential-Linear	2^{29} CP	2^{44}	[BKR97]
3.5	Differential	2^{56} CP	2^{67}	[BKR97]
4	Impossible Differential	$2^{36.6}$ CP	$2^{66.6}$	[BBS99]
4.5	Impossible Differential	2^{64} KP	$2^{110.4}$	[BBS99]
5	Demirci-Selçuk-Türe	$2^{24.6}$ CP	2^{124}	[AS06]
5.5	Key-dependent Linear	2^{21} CP	$2^{112.1}$	[SL09]
6	Key-dependent Linear	2^{49} CP	$2^{112.1}$	[SL09]
4.5	Meet-in-the-Middle	2 KP	2^{103}	**New!**
6	Meet-in-the-Middle BD-relation	2 KP	$2^{123.4}$	**New!**
6	Meet-in-the-Middle BD-relation	16 KP	$2^{111.8}$	**New!**

Questions?

Available online at
http://eprint.iacr.org/2011/417

Thank you for you attention!