Standardization Robustness

Distinguishers/Key recovery for FFX-3.1 and FEA

Orr Dunkelman[1], Abhishek Kumar[2], **Eran Lambooij**[1] and Somitra Kumar Sanadhya[2]

[1]University of Haifa, Israel

[2]IIT Ropar, India

Standards Robustness

- ISO 3103
- ISO 3591
- FIPS 46-3
- FIPS 197
- NIST SP-800-38G
- TTAK.KO-12.0275

Standards Robustness

- ISO 3103
- ISO 3591
- ~~FIPS 46-3~~
- FIPS 197
- ~~NIST SP-800-38G~~
- ~~TTAK.KO-12.0275~~

The 2-round Iterated differential

$$(0|\Delta) \xrightarrow{1} (\Delta|0) \xrightarrow{2^{-n/2}} (0|\Delta)$$

Resulting Distinguishers

Algorithm	Rounds	Block size	Keysize	Time complexity	Data complexity[1]
FEA-1[2]	12	8	128	2^{36}	2^{32}
FEA-1	14	8	192	2^{44}	2^{40}
FEA-1	16	8	256	2^{52}	2^{48}
FEA-2	18	8	128	2^{60}	2^{56}
FEA-2	21	8	192	2^{72}	2^{68}
FEA-2	24	8	256	2^{84}	2^{80}
FF1	10	20	128	2^{70}	2^{60}
FF3-1	8	40	128	2^{100}	2^{80}

[1] The 'high' data complexity is possible due to tweaks increasing the domain.

[2] We can use the distinguishers for FEA to mount key recovery attacks against the full construction for all keysizes.