IMPROVED ANALYSIS OF THREEFISH

Jean-Philippe Aumasson, Willi Meier, Raphael Phan

THREEFISH

Threefish-512: block cipher used in Skein

Skein: SHA-3 submission of Schneier et al.

MMO mode $E_h(t, m) \oplus m$

512-bit key, 512-bit blocks, 128-bit tweak

72 rounds

KNOWN RESULTS

- 8 rounds: near collisions (511-bit)
- 17 rounds: distinguisher in 2^9
- 24 rounds: key recovery
- 25 rounds: key recovery (conjectured)

PROPERTIES TO EXPLOIT

- Simple linear key schedule
- Subkey collisions easy to find
- Round easy to linearize
- Large blocks
- Tweak = additional public input

NEW RESULTS

- 16 rounds: near collisions in 2^6 (459-bit)
- 17 rounds: near collisions in 2^{24} (434-bit)
- 21 rounds: distinguisher in 2^4
- 21 rounds: impossible differential
- 23 rounds: key recovery in 2^{274}
- 24 rounds: key recovery in 2^{431}
- 25 rounds: key recovery in 2^{441}