# 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<sup>9</sup>
- ▶ 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<sup>6</sup> (459-bit)
- ▶ 17 rounds: near collisions in 2<sup>24</sup> (434-bit)
- ▶ 21 rounds: distinguisher in 2<sup>4</sup>
- ▶ 21 rounds: impossible differential
- ▶ 23 rounds: key recovery in 2<sup>274</sup>
- ▶ 24 rounds: key recovery in 2<sup>431</sup>
- ▶ 25 rounds: key recovery in 2<sup>441</sup>