README

Ling Sun[1,2,3], Wei Wang[1,3], and Meiqin Wang(✉)[1,3]

[1] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, Jinan, China
[2] State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, China
[3] School of Cyber Science and Technology, Shandong University, Qingdao, China
{lingsun, weiwangsdu, mqwang}@sdu.edu.cn

This folder contains the Supplementary Material for the paper titled 'Key-Recovery Attacks on CRAFT and WARP'.

- ▷ 1.16-RK-Differential-Patterns-CRAFT.pdf contains the sixteen related-key differential patterns of CRAFT.
- ▷ 2.28-RTK-Differential-Patterns-CRAFT.pdf contains the 28 related-tweakey differential patterns of CRAFT.
- ▷ 3.CRAFT-Source-Code contains the source code for CRAFT.
- ▷ 4.16-RK-Differential-Patterns-WARP.pdf contains the sixteen related-key differential patterns of WARP.
- ▷ 5.WARP-Source-Code contains the source code for WARP.
- ▷ 6.2-ZC-Linear-Approximations-WARP.pdf illustrates the two groups of zero-correlation linear approximations for WARP.