The experimental distinguishing attacks on a new family of lightweight block ciphers "Simeck"

Сосков Александр Саляхович
Институт вычислительных технологий СО РАН (Новосибирск), Россия
e-mail: sashasasha-1987@mail.ru

В работе была приведена «отличительная атака»на Simeck, который является новым семейством «легковесных»блочных шифров. Было найдено наибольшее число раундов, после которых «отличительная атака»была реализована успешно. Для Simeck 48/96 and Simeck 64/128 это число равно 18 и 19 раундов, что составляет 50% и 43% от общего количества раундов, соответственно.