ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 4
2016

М. Э. Т у ж и л и н (Москва, Лаб. ТВП)**. Криптографические свойства шифров SIMON и SPECK.**

В июне 2013 года 6 представителей АНБ опубликовали два семейства блочных шифров для «легкой криптографии» — SIMON и SPECK [1].

Шифры семейства SIMON предназначены для аппаратной реализации и представляют собой сети Фейстеля.

Шифры семейства SPECK предназначены для программной реализации и могут быть описаны как композиции двух сетей Фейстеля.

Шифры обоих семейств могут иметь длину блока 32, 48, 64, 96 или 128 битов и длину ключа 64, 72, 96, 144, 192 или 128 битов.

Вобзоре 2014 года [2] были приведены результаты анализа редуцированных версий шифров SIMON и SPECK по отношению к линейному методу, разностному методу и его модификациям: методу невозможных разностей, методу усеченных разностей, методу «прямоугольника», методу «бумеранга».

В 2015–2016 годах появились новые статьи, посвященные криптоанализу рассматриваемых шифров.

В [3] усовершенствован метод невозможных разностей по отношению к шифру SPECK.

В [4] проведен углубленный анализ шифра SIMON64/128 по отношению к разностному методу.

Совершенствованию линейного метода в применении к шифру SIMON посвящены статьи [5] и [6].

В работах [7] и [8] рассматривается вопрос об автоматическом поиске наилучших линейных и разностных характеристикдля применения к шифру SIMON.

СПИСОК ЛИТЕРАТУРЫ

1. *Beaulieu R.*, *Shors D.*, *Smith J.*, *Treatman-Clark S.*, *Weeks B.*, *Wingers L.* The SIMON and SPECK families of lightweight block ciphers. — Cryptology ePrint Archive 2013/404.
2. *Tuzhilin M.* Block ciphers SIMON and SPECK (invited talk). — CTCRYPT 2014.
3. *Chen Z.*, *Wang N.*, *Wang X.* Impossible Differential Cryptanalysis of Reduced Round SIMON. — Cryptology ePrint Archive 2015/286.
4. *Mourouzis T.*, *Song G.*, *Courtois N.*, *Christofi M.* Advanced Differential Cryptanalysis of Reduced-Round SIMON64/128 Using Large-Round Statistical Distinguishers. — Cryptology ePrint Archive 2015/481.
5. *Chen H.*, *Wang X.* Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-guessing Techniques. — Cryptology ePrint Archive 2015/666.
6. *Abdelraheem M.*, *Alizadeh J.*, *Alkhzaimi H.*, *Aref M.*, *Bagheri N.*, *Gauravaram P.* Improved Linear Cryptanalysis of reduced-round SIMON-32 and SIMON-48. — Cryptology ePrint Archive 2015/988.

7. *Song L.*, *Huang Z.*, *Yang Q.* Automatic Differential Analysis of ARX Block Ciphers with Application to SPECK and LEA. — Cryptology ePrint Archive 2016/209.
8. *Biryukov A.*, *Velichkov V.*, *Corre Y.* Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck. — Cryptology ePrint Archive 2016/409.