A brief comparison of Simon and Simeck

SIMECK is a new lightweight block cipher design based on combining the design principles of the SIMON and Speck block cipher. While the design allows a smaller and more efficient hardware implementation, its security margins are not well understood. The lack of design rationals of its predecessors further leaves some uncertainty on the security of SIMECK. In this work we give a short analysis of the impact of the design changes by comparing the upper bounds on the probability of differential and linear trails with SIMON. We also give a comparison of the effort of finding those bounds, which surprisingly is significantly lower for SIMECK while covering a larger number of rounds at the same time. Furthermore, we provide new differentials for SIMECK which can cover more rounds compared to previous results on SIMON and study how to choose good differentials for attacks and show that one can find better differentials by building them from a larger set of trail with initially lower probability. We also provide experimental results for the differentials for SIMON32 and SIMECK32 which show that there exist keys for which the probability of the differential is significantly higher than expected. Based on this we mount key recovery attacks on 19/26/33 rounds of SIMECK32/48/64, which also give insights on the reduced key guessing effort due to the different set of rotation constants.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Contributors: Kölbl, S., Roy, A.
Pages: 69-88
Publication date: 2017
Peer-reviewed: Yes

Publication information
Journal: Lecture Notes in Computer Science
Volume: 10098
ISSN (Print): 0302-9743
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Scopus rating (2017): CiteScore 0.9 SJR 0.295 SNIP 0.655
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 0.67 SJR 0.339 SNIP 0.642
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): CiteScore 0.37 SJR 0.369 SNIP 0.684
BFI (2014): BFI-level 1
Scopus rating (2014): CiteScore 0.42 SJR 0.354 SNIP 0.743
BFI (2013): BFI-level 1
Scopus rating (2013): CiteScore 0.49 SJR 0.36 SNIP 0.761
ISI indexed (2013): ISI indexed no
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): CiteScore 0.49 SJR 0.346 SNIP 0.762
ISI indexed (2012): ISI indexed no
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 1
Scopus rating (2011): CiteScore 0.49 SJR 0.338 SNIP 0.765
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.322 SNIP 0.663
Web of Science (2010): Indexed yes
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.302 SNIP 0.576
Web of Science (2009): Indexed yes
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.277 SNIP 0.465
Scopus rating (2007): SJR 0.293 SNIP 0.513
Web of Science (2007): Indexed yes
Scopus rating (2006): SJR 0.317 SNIP 0.661
Web of Science (2006): Indexed yes
Scopus rating (2005): SJR 0.334 SNIP 0.766
Web of Science (2005): Indexed yes
Scopus rating (2004): SJR 0.347 SNIP 0.821
Web of Science (2004): Indexed yes
Scopus rating (2003): SJR 0.41 SNIP 0.859
Web of Science (2003): Indexed yes
Scopus rating (2002): SJR 0.387 SNIP 0.781
Scopus rating (2001): SJR 0.399 SNIP 0.754
Scopus rating (2000): SJR 0.271 SNIP 0.704
Scopus rating (1999): SJR 0.299 SNIP 0.696
Original language: English
Keywords: SIMON, SIMECK, Differential cryptanalysis, Block cipher
Electronic versions:
A_Brief_Comparison_of_Simon_and_Simeck.pdf
DOIs:
10.1007/978-3-319-55714-4_6
Source: FindIt
Source-ID: 2356875604
Research output: Research - peer-review > Conference article – Annual report year: 2017