

Accepted Manuscript

Revisiting AES related-key differential attacks with constraint programming

David Gérardt, Pascal Lafourcade, Marine Minier, Christine Solnon

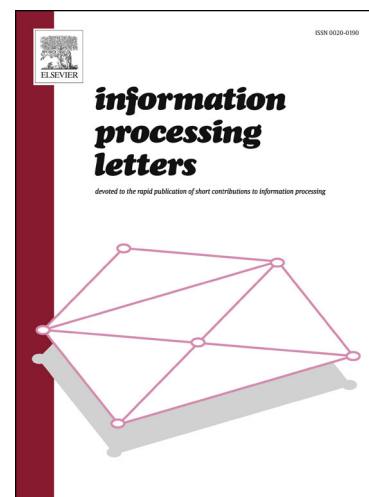
PII: S0020-0190(18)30139-X
DOI: <https://doi.org/10.1016/j.ipl.2018.07.001>
Reference: IPL 5716

To appear in: *Information Processing Letters*

Received date: 2 October 2017
Revised date: 2 July 2018
Accepted date: 2 July 2018

Please cite this article in press as: D. Gérardt et al., Revisiting AES related-key differential attacks with constraint programming, *Inf. Process. Lett.* (2018), <https://doi.org/10.1016/j.ipl.2018.07.001>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



Highlights

- New results on the best related-key differential on 10 rounds of AES-192.
- New results on the best related-key differential for the whole AES-256.
- Using CP models.

Download English Version:

<https://daneshyari.com/en/article/6874111>

Download Persian Version:

<https://daneshyari.com/article/6874111>

[Daneshyari.com](https://daneshyari.com)