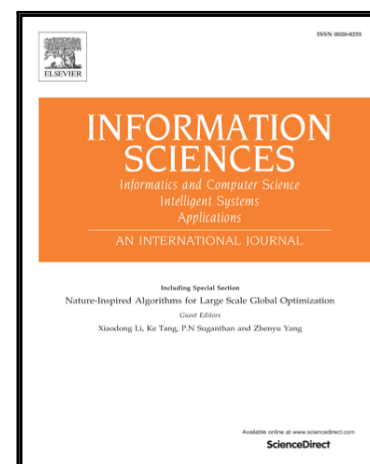


# Accepted Manuscript

Improved known-plaintext attack to permutation-only multimedia ciphers

Leo Yu Zhang, Yuansheng Liu, Cong Wang, Jiantao Zhou, Yushu Zhang, Guanrong Chen

PII: S0020-0255(17)30059-2  
DOI: [10.1016/j.ins.2017.11.021](https://doi.org/10.1016/j.ins.2017.11.021)  
Reference: INS 13249



To appear in: *Information Sciences*

Received date: 4 January 2017  
Revised date: 1 November 2017  
Accepted date: 14 November 2017

Please cite this article as: Leo Yu Zhang, Yuansheng Liu, Cong Wang, Jiantao Zhou, Yushu Zhang, Guanrong Chen, Improved known-plaintext attack to permutation-only multimedia ciphers, *Information Sciences* (2017), doi: [10.1016/j.ins.2017.11.021](https://doi.org/10.1016/j.ins.2017.11.021)

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**

- Based on a rigorous theoretical analysis, we propose an improved known-plaintext attack (KPA) on permutation-only multimedia encryption algorithms.
- The theoretical study results in some novel KPA algorithms, one of which runs at least two orders of magnitude than that of the state-of-the-art methods.

ACCEPTED MANUSCRIPT

Download English Version:

<https://daneshyari.com/en/article/6856849>

Download Persian Version:

<https://daneshyari.com/article/6856849>

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