

Accepted Manuscript

Birthday type attacks to the Naccache-Stern Knapsack cryptosystem

M. Anastasiadis, N. Chatzis, K.A. Draziotis

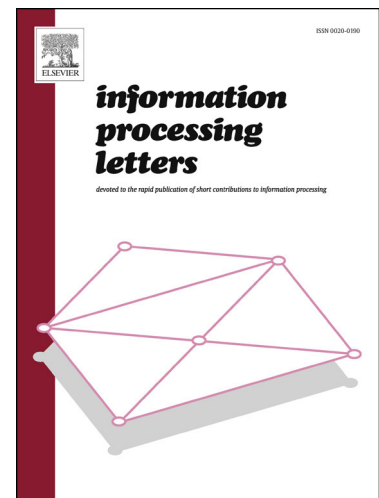
PII: S0020-0190(18)30127-3
DOI: <https://doi.org/10.1016/j.ipl.2018.06.002>
Reference: IPL 5704

To appear in: *Information Processing Letters*

Received date: 22 November 2017
Revised date: 3 June 2018
Accepted date: 3 June 2018

Please cite this article in press as: M. Anastasiadis et al., Birthday type attacks to the Naccache-Stern Knapsack cryptosystem, *Inf. Process. Lett.* (2018), <https://doi.org/10.1016/j.ipl.2018.06.002>

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

- We present an attack to Naccache-Stern knapsack cryptosystem.
- The attack is probabilistic and relies on the birthday paradox.
- Is practical on messages of small or large Hamming weights.
- Performance of time complexity, space complexity and success probability of the attack.

Download English Version:

<https://daneshyari.com/en/article/6874129>

Download Persian Version:

<https://daneshyari.com/article/6874129>

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