

Accepted Manuscript

Comments on “Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation”

Hu Xiong, Qiang Wang, Jianfei Sun

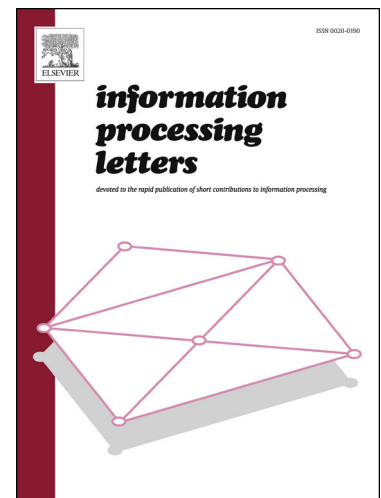
PII: S0020-0190(17)30130-8
DOI: <http://dx.doi.org/10.1016/j.ipl.2017.07.008>
Reference: IPL 5564

To appear in: *Information Processing Letters*

Received date: 24 September 2016
Revised date: 21 June 2017
Accepted date: 8 July 2017

Please cite this article in press as: H. Xiong et al., Comments on “Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation”, *Inf. Process. Lett.* (2017), <http://dx.doi.org/10.1016/j.ipl.2017.07.008>

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

- Attribute-based encryption (ABE) allows fine-grained and versatile sharing of encrypted data.
- Xu et al. proposed a novel ABE scheme with verifiable outsourced decryption recently.
- We show that anyone can forge a valid ciphertext to replace the original ciphertext.

Download English Version:

<https://daneshyari.com/en/article/4950873>

Download Persian Version:

<https://daneshyari.com/article/4950873>

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