

Accepted Manuscript

Energy efficient modular exponentiation for public-key cryptography based on bit forwarding techniques

Satyanarayana Vollala, N. Ramasubramanian

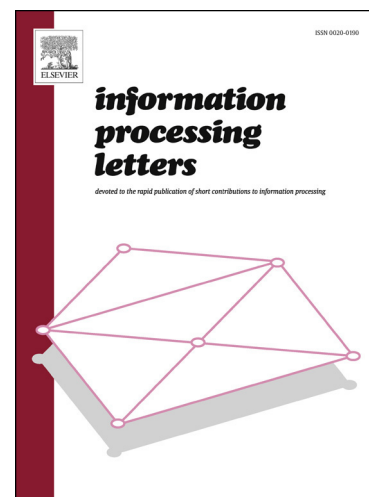
PII: S0020-0190(16)30171-5
DOI: <http://dx.doi.org/10.1016/j.ipl.2016.11.007>
Reference: IPL 5486

To appear in: *Information Processing Letters*

Received date: 31 July 2015
Revised date: 19 April 2016
Accepted date: 23 November 2016

Please cite this article in press as: S. Vollala, N. Ramasubramanian, Energy efficient modular exponentiation for public-key cryptography based on bit forwarding techniques, *Inf. Process. Lett.* (2017), <http://dx.doi.org/10.1016/j.ipl.2016.11.007>

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

- Bit Forwarding algorithms have been designed to reduce the frequency of modular multiplications in PKC.
- Montgomery multiplication method has been tuned according to the needs of proposed Techniques.
- All the proposed algorithms are implemented in hardware.
- Hardware realizations have been proved to be energy efficient.

Download English Version:

<https://daneshyari.com/en/article/4950948>

Download Persian Version:

<https://daneshyari.com/article/4950948>

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