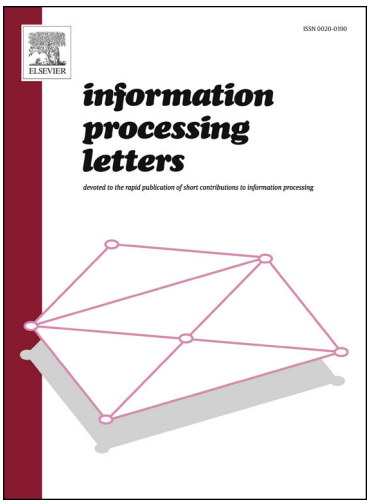
Accepted Manuscript



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

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.