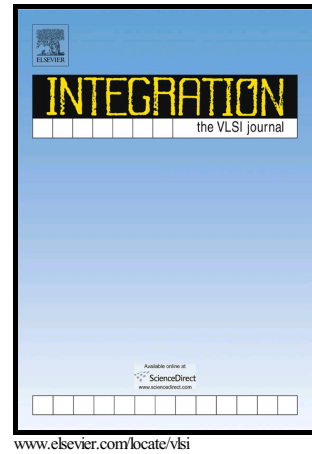


Author's Accepted Manuscript

High-Performance Ternary Operators for Scrambling

Mahya Sam Daliri, Reza Faghieh Mirzaee, Keivan Navi, Nader Bagherzadeh



PII: S0167-9260(17)30179-7
DOI: <http://dx.doi.org/10.1016/j.vlsi.2017.03.010>
Reference: VLSI1322

To appear in: *Integration, the VLSI Journal*

Received date: 20 August 2016
Revised date: 9 February 2017
Accepted date: 21 March 2017

Cite this article as: Mahya Sam Daliri, Reza Faghieh Mirzaee, Keivan Navi and Nader Bagherzadeh, High-Performance Ternary Operators for Scrambling *Integration, the VLSI Journal*, <http://dx.doi.org/10.1016/j.vlsi.2017.03.010>

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 a review of the resulting galley proof before it is published in its final citable 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.

High-Performance Ternary Operators for Scrambling

Mahya Sam Daliri¹, Reza Faghieh Mirzaee², Keivan Navi^{1*}, Nader Bagherzadeh³

¹Faculty of Computer Science and Engineering, Shahid Beheshti University, G.C., Tehran, Iran

²Department of Computer Engineering, Shahr-e-Qods Branch, Islamic Azad University, Tehran, Iran

³Department of Electrical Engineering and Computer Science, University of California, Irvine, USA

*Corresponding Author's. E-Mail: navi@sbu.ac.ir

Abstract

This paper presents two new ternary operators which can be used in different scrambling crypto algorithms. The employment of the proposed operators (ScramOp1 and ScramOp2) leads to reduction in the number of decoding steps, equivalent to only one operation per digit for the receiver side. These operators are presented for the first time in ternary logic. There are some other ternary operators such as SUM, which are specifically suitable for computer arithmetic but they lack desirable efficiency for cryptographic applications. The transistor-level designs of the operators are simulated by using Synopsys HSPICE with 32nm bulk-CMOS technology. Simulation results demonstrate that ScramOp1 and ScramOp2 achieve significant saving in energy consumption (2.11% and 12.14%) in comparison with SUM. Additionally, ScramOp2

Download English Version:

<https://daneshyari.com/en/article/4970681>

Download Persian Version:

<https://daneshyari.com/article/4970681>

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