

Article

IMPLEMENTATION OF EFFICIENT CRYPTOGRAPHIC ARITHMETIC UNITS

June 2020 · International Journal of Security and Its Applications 14(2):1 - 18

DOI:10.33832/ijjsia.2020.14.2.01

Authors:



Kiran KUMAR V.G

A J Institute of Engineering and Technology, Mangaluru



C. Shantharama Rai

A.J.Institute of Engineering and Technology

Request full-text

Download citation

Copy link



To read the full-text of this research, you can request a copy directly from the authors.

Citations (1)

References (17)

Abstract

In the era of Internet of Things (IoT), there has been enormous increase in the implementation of smart devices with constrained resources to implement various cryptographic arithmetic primitives. Most of the conventional cryptographic algorithms like the IDEA, RSA etc. involve simple operations like addition, multiplication and complex operations like addition-modulo, multiplication-modulo etc. such algorithms may not be fit the resource constrained devices. While the current conventional algorithms approved National Institute of Standards and Technology (NIST) - can be implemented to route the resource constrained devices, their performance may not be satisfactory. Over the years, extensive research has been carried out configuring the cryptographic arithmetic structures, the basic arithmetic modules using different design styles, algorithms and aspects. In this paper efficient cryptographic arithmetic modules is implemented by combining the reversible logic and Vedic mathematics. The synthesis and implementation show that the proposed modules have considerable amount of improvement in the Area, power dissipation and delay.

Discover the world's research

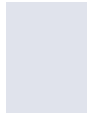
- 25+ million members
- 160+ million publication pages
- 2.3+ | citatic [Join for free](#)

Sponsored videos



No full-text available

Principal
A.J. Institute of Engineering & Technology
Mangaluru - 575 006



To read the full-text of this research,
you can request a copy directly from the authors.

[Request full-text PDF](#)

[Citations \(1\)](#)

[References \(17\)](#)

DESIGN AND IMPLEMENTATION OF AN EFFICIENT FPGA ARCHITECTURE FOR CRYPTOGRAPHIC ALGORITHMS

Thesis

Aug 2021

 Kiran KUMAR V.G ·  C. Shantharama Rai

[View](#) [Show abstract](#)

Recommended publications [Discover more](#)

Article [Full-text available](#)

Why discourse matters only sometimes: Effective arguing beyond the nation-state

January 2010 · Review of International Studies

[...] ·  Diana Panke



Pre- and post-agreement discourses are an integral part of international relations. Yet, they only matter sometimes as an empirical analysis of European judicial discourses shows. State of the art Habermasian and social psychology approaches on effective arguing cannot sufficiently explain variation in the success of discourses. This requires a fine-grained perspective: Only if actors share ... [\[Show full abstract\]](#)

[View full-text](#)

Article [Full-text available](#)

Status, endogenous reference standards, and the growth-inequality relation: A note

October 2008

 Frederic Tournemaine · [...] ·  Christopher Tsoukis

We develop an endogenous growth model with heterogeneous agents who care about their status in society. Following the social psychology literature, we formalise the idea that the reference standard to which people compare themselves is a choice variable. In such a framework, we analyse the determinants of the choice of the reference standard and their effects on growth and distribution. We show ... [\[Show full abstract\]](#)

[View full-text](#)

Article [Full-text available](#)

A French adviser in the time of Choukoutien archaeological excavation: Study based on the recently p...

March 2008 · Chung Yang Yen Chiu Yuan Li Shih Yu Yen Yen Chiu So Chi K'an /Bulletin of the Institute of History and Philology Academia Sinica

[...] ·  Li-Chuan Tai

In the field of the history of European natural sciences, scientific institutions, such as museums, which played a key decision-making role and performed multiple functions, have been largely explored. However, due to the lack of systematic archives, fewer studies have focused on the researchers sent by the museums to collect the specimens in various parts of the world, and the nature of their ... [\[Show full abstract\]](#)

[View full-text](#)

Article

Choosing the Joneses : Endogenous Goals and Reference Standards

May 2004 · Scandinavian Journal of Economics

Markus Knell · [...] · Armin Falk

A growing economic literature stresses the importance of relative comparisons, e.g., for savings and consumption or happiness. In this literature it is usually assumed that reference standards against which people compare themselves are exogenously given. In contrast findings from social psychology suggest that people play an active role in determining their reference standards. We present a ... [\[Show full abstract\]](#)

[Read more](#)



Company

[About us](#)
[News](#)
[Careers](#)

Support

[Help Center](#)

Business solutions

[Advertising](#)
[Recruiting](#)