



Access provided by: Vels Institute of Science Technology & Advanced Studies (VISTAS)

Sign Out

Access provided by: Vels Institute of Science Technology & Advanced Studies (VISTAS)

Sign Out

All



ADVANCED SEARCH

Conferences > 2023 Second International Con... ?

An Analysis of Public-Key Cryptography (PKC) Architecture for Hardware Security

Publisher: IEEE

Cite This



M. Priyatharshini ; C. Sharanya All Authors



65 Full Text Views

Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Download PDF

Document Sections

- I. INTRODUCTION
- II. RSA
- III. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)
- V. Applications of Public-key Cryptography in Hardware Security
- V. Results and Implementation

Show Full Outline

Authors

Figures

References

Keywords

Abstract:

Hardware security recreates an important part of protecting devices and data from stealing. Hardware-based security solutions deliver better security than software securi... **View more**

Metadata

Abstract:

Hardware security recreates an important part of protecting devices and data from stealing. Hardware-based security solutions deliver better security than software security, which is essential in today's handheld devices. However, hardware trustworthiness has become in this work, and the widely used Public Key Cryptography (PKC) algorithms such as RSA and ECC have been studied and implemented to emphasize their importance in data security. The VLSI architecture for the Fast Modular Exponentiation Algorithm (FMEA) and its implementation in the RSA algorithm are presented. Implementation of ECC over GF(p) with underlying mathematical fields is also discussed. The architecture is described using Verilog HDL (Hardware Description Language), synthesized and verified in ZED (Zynq Evaluation and Development) Board (XC7Z020CLG484-1).

Published in: 2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)

Date of Conference: 18-19 August 2023

DOI: 10.1109/SmartTechCon57526.2023.10391654

Date Added to IEEE Xplore: 19 January 2024

Publisher: IEEE



Metrics
More Like This

► ISBN Information:

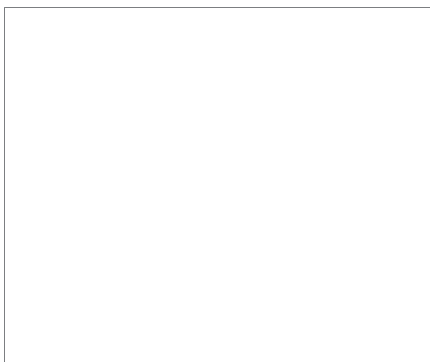
Conference Location: Singapore, Singapore

☰ Contents

I. INTRODUCTION

Public Key Cryptography plays a significant role in hardware security, as shown in fig. 1. In this regard, cryptography plays a vital role in private key network attacks. Encryption requires elevated information protection with minimum power consumption and significant speed performance in a hardware cryptography system. Elliptic Curve Cryptography (ECC) is public-key cryptography founded on elliptic curves' finite field algebraic structure. The Security level of 160 bits key size in ECC is equivalent to 1024 bits key length of RSA. In ECC, primary operations such as key agreement, signature generation, signing, and verification involve point addition and multiplication.

Authors	▼
Figures	▼
References	▼
Keywords	▼
Metrics	▼

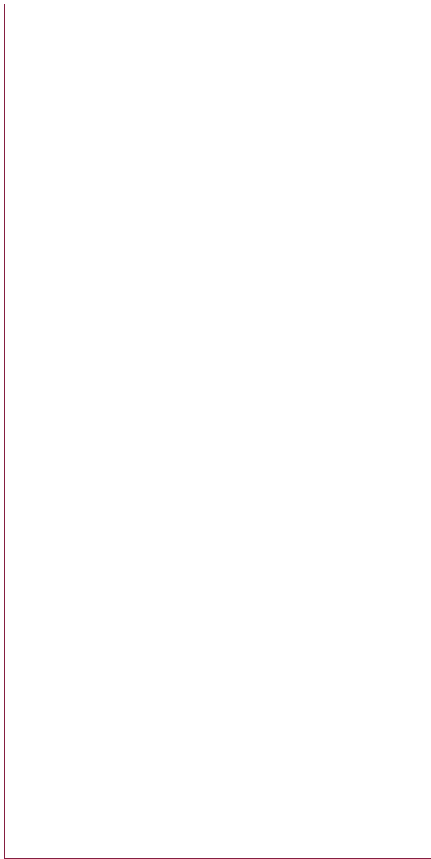


More Like This

Elliptic Curve Cryptography Point Multiplication Core for Hardware Security Module
IEEE Transactions on Computers
Published: 2020

A Low-Cost Very Large Scale Integration Architecture for Multistandard Inverse Transform
IEEE Transactions on Circuits and Systems II: Express Briefs
Published: 2010

Show More



IEEE Personal Account

CHANGE
USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED
DOCUMENTS

Profile Information


COMMUNICATIONS
PREFERENCES
PROFESSION AND
EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800
678 4333
WORLDWIDE: +1 732
981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#)  | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History
- » View Purchased Documents

Profile Information

- » Communications Preferences
- » Profession and Education

» Technical Interests

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.