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

Publisher: IEEE

M. Priyatharshini ; C. Sharanya **All Authors**

Abstract

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 emphasizetheir importance in data security. The VLSI architecture for the Fast Modular Exponentiation Algorithm (FMEA) and its implementation in the RSA algorithmare 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,asshown 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 fieldalgebraic 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.

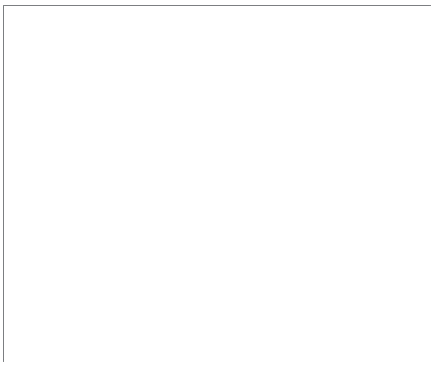
Authors

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