International Conference on Information Engineering, Management and Security
2015 [ICIEMS 2015]

ISBN	978-81-929742-7-9	**VOL**	01
Website	www.iciems.in	**eMail**	iciems@asdf.res.in
Received	10 - July - 2015	**Accepted**	31- July - 2015
Article ID	ICIEMS016	**eAID**	ICIEMS.2015.016

Implementations of Reconfigurable Cryptoprocessor A Survey

N Rajitha[1], R Sridevi[2]
[1]Research Scholar, JNTUH, Hyderabad
[2]Professor in CSE JNTUH, Hyderabad

ABSTRACT: *One among the several challenges in the area of applied cryptography is not just devising a secure cryptographic algorithm but also to manage with its secure and efficient implementation in the hardware and software platforms. Cryptographic algorithms have widespread use for every conceivable purpose. Hence, secure implementation of the algorithm is essential in order to thwart the side channel attacks. Also, most of the cryptographic algorithms rely on modular arithmetic, algebraic operations and mathematical functions and hence are computation intensive. Consequently, these algorithms may be isolated to be implemented on a secure and separate cryptographic unit.*

Keywords: Trust, FPGA security, Cryptographic processor, reconfigurable cryptosystems.

I. INTRODUCTION

There is an alarming need for securing wide area of applications of cryptography that we use in our daily life besides military, defense, banking, finance sectors and many more. To cater to this need innumerable products/services have been developed which are predominantly based on encryption. Encryption in turn relies on the security of the algorithm and the key used. The different encryption algorithms proposed so far have been subjected to various forms of attacks. While it is not possible to devise an algorithm that works perfectly well and sustains all forms of attacks, cryptographers strive to develop one that is resistant to attacks and that performs well. The task is not just to propose a new algorithm but to create an environment that improves the performance of the algorithm and that protects the keys from attacks. A cryptoprocessor is a specialized processor that executes cryptographic algorithms within the hardware to accelerate encryption algorithms, to offer better data, key protection. Commercial examples of cryptoprocessors include IBM 4758, SafeNet security processor, Atmel Crypto Authentication devices. The following are the different architectures of cryptographic computing[1].

A.Cryptoprocessor Types

· Customized General Purpose Processor: The processor is extended or customized to implement the cryptographic algorithms efficiently. Typical commercially available solutions are CryptoBlaze from Xilinx or the AES New Instructions (AES-NI) incorporated in the new Intel processors.
· Cryptographic processor (cryptoprocessor): It is a programmable device with a dedicated instruction set to implement the cryptographic algorithm efficiently.
· Cryptographic coprocessor (crypto coprocessor): It is a logic device dedicated to the execution of cryptographic functions. Unlike the cryptoprocessor it cannot be programmed, but can be configured, controlled and parameterized.
· Cryptographic array (crypto-array): It is a coarse grained reconfigurable architecture for cryptographic computing.

Cite this article as: N Rajitha, R Sridevi. "Implementations of Reconfigurable Cryptoprocessor A Survey." *International Conference on Information Engineering, Management and Security (2015)*: 98-103. Print.

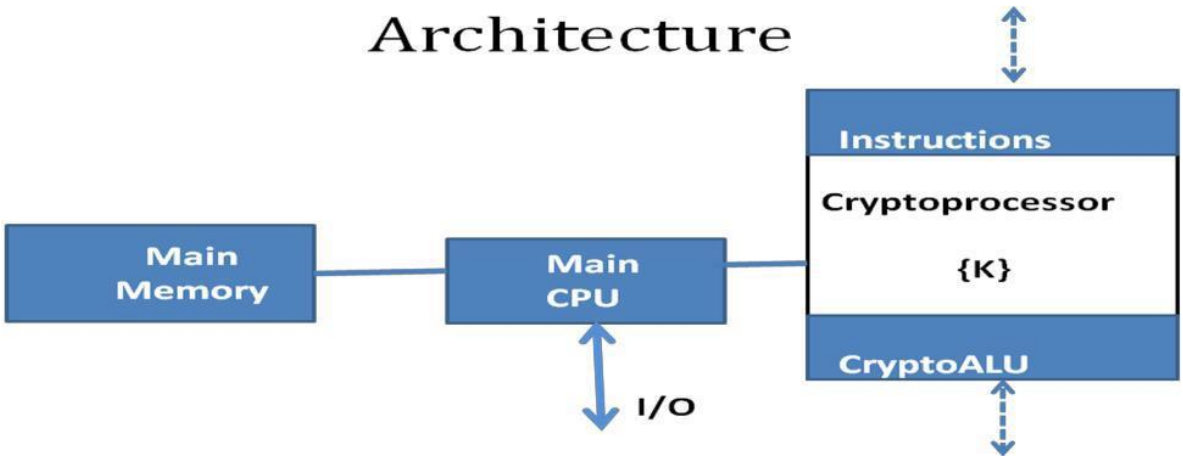

Fig 1 Architecture of Cryptoprocessor [1]

B Cryptoprocessor Implementations

i) Cryptoprocessor implemented in (field programmable gate array) FPGA are fast in terms of cryptographic processing. The complex mathematical operations can be run **quickly and efficiently**. IP blocks can be **modified** if desired as the name suggests. FPGA based cryptoprocessors are used in ATMs, automobiles, robotics etc.

ii) **ASIC based cryptoprocessors** have small footprint and offer high speed. They cannot be changed once produced. They use less power and are used in applications such as RFID, network routers, cameras, cell phones etc.

iii) **Hardware Security Module** (HSM) contains one or more secure cryptoprocessor chips to prevent tampering and bus probing. They come in the form of a plug-in card or an external device that attaches directly to a computer of some sort. HSM can be made to provide backup to computer to which it is attached, NAS, cloud server and can be used as external security token.

iv) **Trusted Platform Module** (TPM) is a cryptoprocessor integrated in software microkernel. The kernel generates and stores keys, passwords and certificates. They can be found in Digital Rights Management to ensure that audio/video file is original and not a copy.

ii) CRYPTOPROCESSOR ATTACKS

The different forms of hardware attacks on algorithmic implementations on cryptographic devices in literature have been identified as given below

i) **Side Channel Attack**: A study of the literature reveals that a major amount of research has been expended during the last decade on side channel attacks and countermeasures. Side channel attacks and can happen in one of the following ways:

a) **Timing Analysis**: Time required by the device to perform encryption/decryption can be used to get additional data to perform an attack.

b) **Electromagnetic analysis**: It is based on the electromagnetic radiation from the circuit that executes the encryption/ decryption algorithm

c) **Power Analysis**: Power consumed by the device implementing the algorithms can be used to perform the attack. It can be of the form Simple Power Analysis or Differential Power Analysis. Side channel attacks and countermeasures can be found in [25], [42],[43], [44]. Pawel Swierczynki et al[25] discuss side channel attack on bitstream encryption of Altera Stratix II and Stratix III FPGA family in the form of black box attack. To combat IP theft and physical cloning bitstream encryption is used.

ii) Fault Injection Attacks: involves inserting fault deliberately into the device and to observe erroneous output.

iii) Counterfeiting: to your name illegally on a clone.

iv) Steal bitstreams

v) Insert Trojan Horse: a common method used to capture passwords.

vi) Overbuilding

vii) Cold boot attack: is a technique to extract disk encryption keys [12].

viii) Cloning: in which your design is copied without knowing how it works

ix) Reverse Engineering: Finding out how the design works

x) Steal IP: IP is stolen either with the intention to sell it to others or to reverse engineer. Another classification of attacks on cryptoprocessor as mentioned in [26] is as follows:

A. *Invasive: Invasive attack give direct access to internal components of the cryptographic device. The attack can be performed by manual micro probing, glitch, laser cutting, ion beam manipulation etc.*

B. *Local Non Invasive: This form of attack involves close observation to operation on the device. The side channel attacks listed above may be considered as an example of such an attack.*

C. *Remote Attacks: Remote attacks involve manipulation of device interfaces. Unlike the previous attacks these attacks do not need physical access. API analysis, protocol analysis, cryptanalysis are examples of such an attack. While API analysis is concerned with cryptographic processor cryptanalysis involves finding out the flaws in the algorithms primitives.*

III. IMPLEMENTATIONS OF

Cite this article as: N Rajitha, R Sridevi. "Implementations of Reconfigurable Cryptoprocessor A Survey." *International Conference on Information Engineering, Management and Security (2015)*: 98-103. Print.

CRYPTOGRAPHIC ALGORITHMS

Security in the digital world is primarily fulfilled by using cryptography. Numerous optimizations have been proposed and implemented for enhancing the performance and efficiency of the cryptographic algorithms that serve the innumerable applications in various fields. We present few such algorithms which have been implemented on FPGA. The significant consideration of most of them is time area product, besides analysis related to side channel resistance, amount of hardware resources utilized etc.

A. **Symmetric key algorithm implementations** We now discuss few implementations of symmetric key cryptographic algorithms on FPGA. Cryptoraptor [45] considers high performance implementation of set of symmetric key algorithm. The architecture comprises of processing elements(PE) linked by connection row (CR). The PE have independent functional units for arithmetic, shift, logical, table look permutation and operations. Multiplication is limitation due to the limited addressing structure of TLU. It also lacks support for varying modulo in modular arithmetic operations. Rajesh Kannan et al in [46] implement AES, RC5 and RC6 block cipher algorithms in which they discuss on area analysis and power consumptions.

B. Implementations of asymmetric cryptographic algorithms

Many implementations of the asymmetric cryptographic algorithms exist with optimizations to address the needs of embedded system applications. Few of the implementations are as described below.

Base Ext. A→B B→A	Throughput (1024 bits) [Enc/s] (rel.)	Throughput (2048 bits) [Enc/s] (rel.)
M M	194 (46%)	28 (50%)
B M	267 (63%)	38 (67%)
B K	408 (97%)	55 (98%)
B S	419 (100%)	56 (100%)

Table 1 Asymmetric Cryptography with Graphic cards Base Extension Techniques RNS Method [33].

Tim Erhan Guneysu in [33] investigates High Performance Computing implementation of symmetric AES block cipher, ECC and RSA on FPGA.

Feature	ECC(146bits)	RSA(1024bits)
Frequency (MHz)	50	28
Logic size (Slices)	3,036	4,595
Execution time	7.28msec (scalar multiplication)	58.9msec (decryption with 1024-bit sized key)

Table 2 Characteristics of ECC and RSA Crypto Blocks [39]

C. Implementations of hash functions

Hash functions are used for authentication, for providing data integrity and along with public key algorithms as digital signatures. MD5, SHA1, SHA-512 are prominent hash digest algoritms. BLAKE is one of the candidate of SHA3 and Keccak is SHA3 finalist which are based on sponge structure.

Cite this article as: N Rajitha, R Sridevi. "Implementations of Reconfigurable Cryptoprocessor A Survey." *International Conference on Information Engineering, Management and Security (2015)*: 98-103. Print.

Algorithm	Technology	Area	Frequency	Through-put (Gbps)
Blake-512 [36]	FPGA Virtex 5	108 slices	358 MHz	0.3
Keccak-1600 [34]	FPGA Stratix III	4684 LUT	206 MHz	8.5

Table 3 Comparison of hardware implementation of Hash functions [38]

D. Implementations of lightweight cryptography

For the fast growing applications of ubiquitous computing, new lightweight cryptographic design approaches are emerging which are investigated in [40]. The implementation of PRESENT-128 lightweight cryptographic algorithm on Spartan III XCS400-5 with a frequency of 254MHz achieves a throughput of 508Mbps

Algorithm	key size	block size	datapath width	cycles / block	T'put [Kbps]	Tech. [μm]	Area [GE]	Eff. [bps/GE]	Cur. [μA]
Serialized Architecture									
DES	56	64	4	144	44.44	0.18	2,309	19.25	1.19
DESL	56	64	4	144	44.44	0.18	1,848	24.05	0.89
DESX	184	64	4	144	44.44	0.18	2,629	16.9	–
DESXL	184	64	4	144	44.44	0.18	2,168	20.5	–

Table 4 Hardware implementation results of DES, DESX, DESL and DESXL. All figures are obtained at or calculated for a frequency of100KHz. [40]

FPGA implementation on low cost Spartan III of ultra light weight cryptographic algorithm Hummingbird is considered in [31]. Hummingbird has its application in RFID tags, wireless control and communication devices and resource constraint devices.

E. A glance on code based cryptography and its implementations

Encryption with Coding Theory by Claude Shannon as basis is used in McEliece and Niederreiter which are considered as candidates for post quantum cryptosystems. McEliece is based on binary Goppa Codes which are fast to decode. McEliece and Niederreiter differ in the description of the codes. While the former cannot be used to generate signatures the later can be used for digital signatures.

Property	Spartan-3an	Virtex-5
Slices	2979	1385
BRAMs	5	5
Clock Frequency	92 MHz	190 MHz
Clock cycles	94,249	94,249
Decryption Latency	1.02 ms	0.50 ms
Security	80 bits	80 bits

Table 5 Mceliece Decryption Implementations [37]

Cite this article as: N Rajitha, R Sridevi. "Implementations of Reconfigurable Cryptoprocessor A Survey." *International Conference on Information Engineering, Management and Security (2015)*: 98-103. Print.

IV. OBSERVATIONS & OPEN QUESTIONS

A. Applications of Cryptoprocessors Numerous applications of cryptoprocessor exist. They can be used in Automated Teller Machine Security, E-commerce applications, smart cards, wireless communication devices, resource constrained devices such as sensors, RFID tags, smart phones, smart cameras, digital rights management, trusted computing, prepayment metering systems, pay per use, banking, military and defense applications.

B. Open Problems

One of the open problems is the remote attacks (in the form of API attack) on cryptoprocessor which may be passive or active and which unlike the physical or invasive attacks doesn't need any contact with the implementation unit. Wollinger et al [47] discuss on the architectures of programmable routing in FPGA in the form of hierarchical and island style. FPGA security resistance to invasive and non-invasive attacks is still under experimentation as new attacks are devised before existing attacks are solved. Much of the work on cryptoprocessors is specific to the application domain or to address a particular form of attack and is not generic to cater to many applications unless customized. Key management in general is not considered as part of th cyrptoprocessor implementation. Several designs of cryptoprocessors are proposed and implemented but still fully functional cryptoprocessor designs addressing integrity, key generation, key management, privacy of both symmetric and asymmetric cryptosystems is still a challenge.

V. ACKNOWLEDGEMENT

The first author would like to express gratitude to TEQIP II. This work has been carried out as a part of Ph D under TEQIP II.

VI. REFERENCES

[1] 1. LILIAN BOSSUET et al Architectures of Flexible Symmetric Key CryptoEngines—A Survey: From Hardware Coprocessor to Multi- Crypto-Processor System on Chip ACM Computing Surveys, Vol. 45,No. 4, Article 41, August 2013.
[2] Crypto-processor - architecture, programming and evaluation of the security Lubos Gaspar Ph D Thesis, November 2012.
[3] Sandro Bartolini, Instruction Set Extensions for Cryptographic Applications, Springer Cryptographic Engineering, 2009.
[4] N. Sklavos , On the Hardware Implementation Cost of Crypto- Processors Architectures, Information Security Journal: A Global Perspective, Taylor& Francis, Vol 19 2010.
[5] Santosh Ghosh et al, BLAKE-512-Based 128-Bit CCA2 Secure Timing Attack Resistant McEliece Cryptoprocessor, IEEE Transactions on Computers 2014.
[6] Siddhartha Chhabra et al An Analysis of Secure Processor Architectures,Springer LNCS 2010.
[7] Sujoy Sinha Roy et al, Compact Ring-LWE Cryptoprocessor, Springer LNCS Vol 8731, 2014
[8] Hans Eberle et al, A Public-key Cryptographic Processor for RSA and ECC, IEEE proceeding 2004
[9] Trimberger and Moore: FPGA Security: Motivations,Features,and Applications, Invited Paper IEEE Proceedings Aug 2014
[10] Stepahnie Kerchof et al, Towards Green Cryptography: A Comparison of Lightweight Ciphers from the Energy Viewpoint, Springer LNCS Vol 7428, 2012
[11] Kotaro Okamoto et al , A Hierarchical Formal Approach to Verifying Side-channel Resistant Cryptographic Processors in Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium.
[12] J.Alex Halderman et al Lest We Remember: ColdBoot Attacks on Encryption Keys, Proc.2008 USENIX Security Symposium
[13] Stefan Tillich, Instruction set extensions for support of cryptography on Embedded Systems, Ph D thesis, Graz University of Technology Nov 2008
[14] Michael Grand et al, Design and Implementation of a Multi-Core Crypto-Processor for Software Defined Radios, Springer LNCS Vol 6578 2011
[15] Joel Reardon et al, On secure data deletion, IEEE S&P Symposium, May 2014.
[16] Masoud Rostami et al, A Primer on Hardware Security , Models, Metrics, Vol 102, Proceeedings of IEEE, August 2014.
[17] Hao Zhang et al, In-Memory Big Data Management & Processiing: A Survey, 2014
[18] Peter A. H. Peterson, Cryptkeeper: Improving Security With Encrypted RAM, IEEE 2010.
[19] J.Alex Halderman et al, Lest We remember Cold boot attacks on encryption keys, Usenix 2008.
[20] S Subha, An algorithm for deletion in Flash Memories, IEEE 2009.
[21] Peter Gutmann, Data Remanance in Semiconductor Devices, 2000.
[22] Peter Gutmann, Secure Deletion of Data from Magnetic & Solid-State Memory, Sixth USENIX security Symposium , 1996
[23] Siddhartha Chhabra et al, An analysis of Secure Processor Architecture, AES Key Wrap Specification 2001. Lubos Gaspar et al, Secure extension for soft general purpose processor **Property Spartan-3an Virtex-5** Slices 2979 1385 BRAMs 5 5 Clock Frequency 92 MHz 190 MHz Clock cycles 94,249 94,249 Decryption Latency 1.02 ms 0.50 ms Security 80 bits 80 bits
[24] Lubos Gaspar et al, Secure extension for soft general purpose processor with secure key management, IEEE 2011.
[25] PAWEL SWIERCZYNSKI et al, Physical Security Evaluation of the Bitstream Encryption Mechanism of Altera Stratix II and Stratix III FPGAs, ACM Transactions on Reconfigurable Technology and Systems, Vol. 7, No.4, Article 7,Publication date: December 2014.
[26] MoezBen MBarka Cryptoprocessor application & attacks survey, May 2008
[27] Mehran Mozaffaci kenani et al, Fault Resilient lightweight cryptographic block cipher for secure embedded system, IEEE Embedded Systems letter, Vol 16, Dec 2014.

Cite this article as: N Rajitha, R Sridevi. "Implementations of Reconfigurable Cryptoprocessor A Survey." *International Conference on Information Engineering, Management and Security (2015)*: 98-103. Print.

[28] Gaurav Bansod et al, Implementation of a new light weight encryption design for embedded security, IEEE Transactions on Information Forensics & Security, 2013.
[29] Majzoobi & Koushnfar, Time bounded Authentications of FPGAs, IEEE Transactions on Information Forensics & Security, Sept 2011
[30] Hero Maderis, Theisis , A Scalar Multiplication in Elliptic Curve Cryptography with Binary Polynomial operation in Galois Field Oct 2009
[31] Xin Xin Fan et al, FPGA Implementation of Humming bird cryptographic algorithm, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2010
[32] Lejla Batina et al, Hardware Architectures for Public Key Cryptography, 2002
[33] Tim Erhan Guneysu, Thesis, Cryptography and cryptanalysis of reconfigurable devices Bochum , 2009
[34] Beuchat et al, Compact Implementation of BLAKE on FPGA, 2010
[35] Baldwin B eta al, FPGA Implementation of SHA3 candidates July 2011
[36] Bertoni, The Keccak sponge function family: Hardware performance 2010
[37] Santosh Gosh et al, A speed area optimized embedded Coprocessor for Mc Eliece Cryptosystem, IEEE Conference 2012
[38] Zhije Shi et al, Hardware Implementation of Hash Function, Springer LLC 2012
[39] HoWon Kim et al, Design and Implementation of public key cryptoprocessor and its application to a security system
[40] Axer York Poschmann, Ph D Thesis, Lightweight cryptography Feb 2009
[41] Ricardo Chaves, Ph D Thesis, Secure Computing in reconfigurable devices, 2007
[42] PowerKotaro Okamoto, A Hierarchical Formal Approach to Verifying Side-channel Resistant Cryptographic Processors, IEEE, 2014
[43] Amir Moradi ,Side-Channel Leakage through Static Power Should we care in practice
[44] Jen-Wei Lee, Efficient Power-Analysis-Resistant Dual-Field Elliptic Curve Cryptographic Processor Using Heterogeneous Dual-Processing- Element Architecture, IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 22, NO. 1, JANUARY 2014
[45] Gokhan Sayiler, Cryptoraptor: High Throughput Reconfigurable Cryptographic Processor, IEEE 2014.
[46] Rajesh Kannan et al Recongfigurable Cryptoprocessor for multiple crypto Algorithm, IEEE Symposium 2011.

Cite this article as: N Rajitha, R Sridevi. "Implementations of Reconfigurable Cryptoprocessor A Survey." *International Conference on Information Engineering, Management and Security (2015)*: 98-103. Print.