

# Implementations of Secure Reconfigurable Cryptoprocessor a Survey

Rajitha Natti and Sridevi Rangu

**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

## 1 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

---

R. Natti (✉) · S. Rangu  
Department of Computer Science & Engineering, Jawaharlal Nehru  
Technological University, Hyderabad, India  
e-mail: rajitha2k2@yahoo.co.in

S. Rangu  
e-mail: sridevirangu@jntuh.ac.in

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. We present the different forms of attacks possible on cryptoprocessors in Sect. 2. The implementation of cryptoprocessors on reconfigurable platform is considered in Sect. 3.

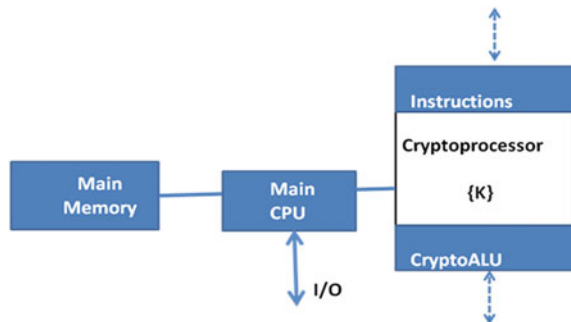
The following are the different architectures of cryptographic computing [1].

- 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. [2, 3] focus on instruction set extensions for cryptographic applications and embedded systems respectively.
- Cryptographic processor (cryptoprocessor): It is a programmable device with a dedicated instruction set to implement the cryptographic algorithm efficiently. [4–6] are examples of cryptoprocessor implementations.
- 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 (Fig. 1).

## 1.1 Motivation

A number of reconfigurable systems have been developed since the 1990s, as they offer strong protection of IP, better protection of key data against vulnerabilities, by integrating functions in software layers into hardware i.e., to System on Chip

**Fig. 1** Architecture of cryptoprocessor [1]



(SoC) or field programmable gate array (FPGA) or application specific integrated circuit (ASIC) depending on functionality. Reconfigurable systems have the ability to hardwire the keys i.e., they can be ‘zeroized’ and can be unseen by world. They are tamper resistant and offer trust.

Reconfigurable systems are more adaptable to applications at low production cost. Video games and all microprocessor unit embedded systems like home appliances and those found in vehicles are examples. They have their use in telecom applications to handle high speed data stream, in rapid prototyping and emulation, in image and signal processing and many more.

## ***1.2 Novelty and Significance to State of the Art***

As software security cannot prevent against hardware attacks, secure processor architectures have been proposed. We identify problems ignored by the current cryptoprocessors like security of interconnects; secure booting, secure key management with focus on lightweight cryptography and post quantum code based cryptography.

The state of art reveals that cryptoprocessor have been implemented with respect to applications [3] or to address specific issue for instance to overcome DPA attack [7] or Cryptoprocessor for SDR etc. or cryptoprocessor for a particular algorithm [8, 9].

## ***1.3 Applications of Cryptoprocessors***

Numerous applications of cryptoprocessor exist. Cryptoprocessors 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.

## ***1.4 Importance of Security in Hardware Processes***

The secure development of software processes has led to the need for inclusion of security as an aspect to software development lifecycle. This is done as a part of the training phase at the beginning of the SDLC as per Microsoft Security Development Lifecycle.

Similarly, there is a need to incorporate security activities into all phases of development lifecycle for hardware processes. Cryptographic hardware is

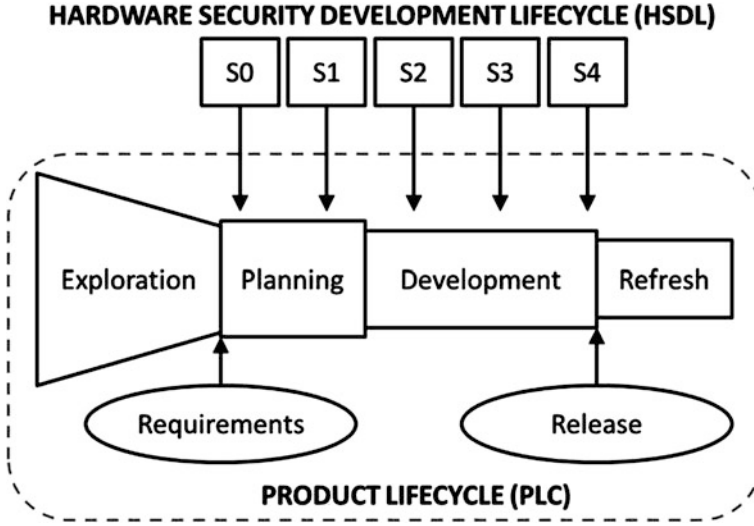


Fig. 2 Incorporating hardware SDL checkpoints into the PLC [10]

vulnerable to both software and hardware attacks and hence security needs to be considered as an integral part of product lifecycle.

Security Assurance is one of the important parameters for many embedded applications which are lightweight and resource constrained. The emergence of system on chip, network on chip applications has further fuelled the need for security assurance. Hence the software development lifecycle has been adapted to hardware in [10] as depicted in Fig. 2.

## 2 Attacks on Cryptoprocessor

The different forms of hardware attacks of 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 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 [11–14]. Side channel attack on bit stream encryption of Altera Stratix II and Stratix III FPGA family in the form of black box attack can be found in [11]. To combat IP theft and physical cloning bit stream encryption is used.
- (ii) *Fault Injection Attacks*: involves inserting fault deliberately into the device and to observe erroneous output.
- (iii) *Counterfeiting*: is to use your name illegally on a clone.
- (iv) *Insert Trojan Horse*: is a common method used to capture passwords.
- (v) *Cold boot attack*: is a technique to extract disk encryption keys [15].
- (vi) *Cloning*: in which your design is copied without knowing how it works.
- (vii) *Reverse Engineering*: is finding out how the design works.
- (viii) *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 [16] is as follows:

## 2.1 *Invasive*

Invasive attack gives 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.

## 2.2 *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.

## 2.3 *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.

### 3 Implementations of Cryptosystems

There is a growing interest in devising cryptographic hardware that is resistant to the attacks mentioned in Sect. 2, side channel attacks in particular. 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 and also on ASIC in certain cases. The significant consideration of most of them is time area product, besides analysis related to side channel resistance, amount of hardware resources utilized etc.

#### 3.1 Symmetric Key Algorithm Implementations

We now discuss few implementations of symmetric key cryptographic algorithms on FPGA. Cryptoraptor [17] considers high performance implementation of set of symmetric key algorithm. The architecture comprises of processing elements (PE) linked by connection row (CR). The PE has independent functional units for arithmetic, shift, logical, table look permutation and operations. Multiplication is limitation due to the limited addressing structure of table look-up unit (TLU). It also lacks support for varying modulo in modular arithmetic operations.

Implementation of AES, RC5 and RC6 block cipher algorithms is considered in [18] in which they discuss area analysis and power consumptions.

#### 3.2 Implementations of Asymmetric Cryptographic Algorithms

Many implementations of the asymmetric cryptographic algorithms exist with optimizations to address the needs of embedded system applications. Tim Erhan Guneyasu in [19] investigates High Performance Computing implementation of symmetric AES block cipher, ECC and RSA on FPGA (Table 1).

**Table 1** Characteristic of ECC and RSA crypto blocks [23]

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

### 3.3 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 algorithms. BLAKE is one of the candidates of SHA3 and Keccak is SHA3 finalist which is based on sponge structure (Table 2).

### 3.4 Implementations of Lightweight Cryptography

For the fast growing applications of ubiquitous computing, new lightweight cryptographic design approaches are emerging which are investigated in [20].

FPGA implementation on low cost Spartan III of ultra light weight cryptographic algorithm Hummingbird is considered in [21]. Hummingbird has its application in RFID tags, wireless control and communication devices and resource constraint devices (Table 3).

### 3.5 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 (Table 4).

**Table 3** Implementation results of PRESENT-128 [20]

Cipher	Block size	FPGA device	Maximum frequency (MHz)	Throughput (Mbps)	Total equiv. slices	Efficiency (Mbps/slice)
PRESENT-128	64	Spartan-III XCS400-5	254	508	202	2.51

**Table 2** Comparison of hardware implementation of Hash functions [24]

Algorithm	Technology	Area	Frequency (MHz)	Throughput (giga bits per second)
Blake-512 [25]	FPGA Virtex 5	108 slices	358	0.3
Keccak-1600 [26]	FPGA Stratix III	4684 LUT	206	8.5

**Table 4** McEliece decryption implementations [27]

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

## 4 Conclusion and Open Problems

A study on existing approaches to software engineering for hardware processes is considered in this paper besides investigating the general characteristics, implementations and uses of reconfigurable cryptoprocessors.

One of the challenges 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.

We need to focus on the formal tools for verification and validation of hardware design processes. The metrics that can be used for assessing the performance is still limited to throughput which again is platform, algorithm and application dependent and not generic. Hence the comparison of the algorithm performance cannot be judged very easily. There is a lot of scope on the adaptation of the process development lifecycle with respect to hardware or embedded software.

Wollinger et al. [22] 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 the cryptoprocessor 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.

**Acknowledgments** This work has been carried out as a part of Ph D under TEQIP-II.



## References

1. Lilian Bossuet, 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. Sandro Bartolini, Instruction Set Extensions for Cryptographic Applications, Springer Cryptographic Engineering, 2009.
3. Stefan Tillich, Instruction Set extensions for support of Cryptography on Embedded Systems, Ph D thesis, Graz University of Technology Nov 2008.
4. Lubos Gaspar, Cryptoprocessor –Architecture, Programming and Evaluation of the Security, Ph D Thesis, November 2012.
5. Sujoy Sinha Roy et al, Compact Ring-LWE Cryptoprocessor, Springer LNCS Vol 8731, 2014.
6. Michael Grand et al, Design and Implementation of a Multi-Core Crypto-Processor for Software Defined Radios, Springer LNCS Vol 6578 2011.
7. 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.
8. Santosh Ghosh et al, BLAKE-512-Based 128-Bit CCA2 Secure Timing Attack Resistant McEliece Cryptoprocessor, IEEE Transactions on Computers 2014.
9. Hans Eberle et al, A Public-key Cryptographic Processor for RSA and ECC, IEEE proceeding 2004.
10. Hareesh Khattri et al, HSDL: A Security Development Lifecycle for Hardware Technologies 2012 IEEE International Symposium on Hardware-Oriented Security & Trust.
11. 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.
12. Power Kotaro Okamoto, A Hierarchical Formal Approach to Verifying Side-channel Resistant Cryptographic Processors, IEEE, 2014.
13. Amir Moradi, Side-Channel Leakage through Static Power Should We Care In Practice.
14. 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 Systems, Vol. 22, No. 1, January 2014.
15. J. Alex Halderman et al, Lest We Remember: Cold Boot Attacks on Encryption Keys, Proc. 2008 USENIX Security Symposium.
16. MoezBen MBarka, Cryptoprocessor Application & Attacks Survey, May 2008.
17. Gokhan Sayiler, Cryptoraptor: High Throughput Reconfigurable Cryptographic Processor, IEEE 2014.
18. Rajesh Kannan et al, Reconfigurable Cryptoprocessor for Multiple Crypto Algorithm, IEEE Symposium 2011.
19. Tim Erhan Guneyysu, Thesis, Cryptography and Cryptanalysis of Reconfigurable Devices Bochum, 2009.
20. Axer York Poschmann, Ph D Thesis, Lightweight Cryptography Feb 2009.
21. Xin Xin Fan et al, FPGA Implementation of Humming bird cryptographic algorithm, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2010.
22. Thomas Wollinger et al, Security on FPGAs: State of Art Implementations and Attacks, ACM Transactions on Embedded Computing Systems, Vol. 3, No. 3, August 2004.
23. HoWon Kim et al, Design and Implementation of Private and Public Key Cryptoprocessor and its Application to a Security System.
24. Zhije Shi et al, Hardware Implementation of Hash Function, Springer LLC 2012.
25. Bertoni, The Keccak sponge function family: Hardware performance 2010.
26. Beauchat et al, Compact Implementation of BLAKE on FPGA, 2010.
27. Santosh Gosh et al, A speed area optimized embedded Coprocessor for Mc Eliece Cryptosystem, IEEE Conference 2012.

Information Systems Design and Intelligent Applications

Proceedings of Third International Conference INDIA

2016, Volume 1

Satapathy, S.C.; Mandal, J.K.; Udgata, S.K.; Bhateja, V.

(Eds.)

2016, XX, 753 p. 314 illus., Softcover

ISBN: 978-81-322-2753-3