Implementations of Reconfigurable Cryptoprocessor A Survey

N Rajitha¹, R Sridevi²
¹Research Scholar, JNTUH, Hyderabad
²Professor 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 algorithms 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.
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 attacks 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 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.”

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.

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

Table 1: Asymmetric Cryptography with Graphic cards Base Extension

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>ECC (146bits)</th>
<th>RSA (1024bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency (MHz)</td>
<td>50</td>
<td>28</td>
</tr>
<tr>
<td>Logic size (Slices)</td>
<td>3,036</td>
<td>4,595</td>
</tr>
<tr>
<td>Execution time</td>
<td>7.28msec (scalar multiplication)</td>
<td>58.9msec (decryption with 1024-bit sized key)</td>
</tr>
</tbody>
</table>

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 algorithms. BLAKE is one of the candidate of SHA3 and Keccak is SHA3 finalist which are based on sponge structure.

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.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Technology</th>
<th>Area</th>
<th>Frequency</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blake-512</td>
<td>FPGA</td>
<td>108</td>
<td>389 MHz</td>
<td>0.3</td>
</tr>
<tr>
<td>Kecckak-1600</td>
<td>FPGA</td>
<td>4684</td>
<td>206 MHz</td>
<td>8.5</td>
</tr>
</tbody>
</table>

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

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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Spartan-3an</th>
<th>Virtex-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slices</td>
<td>2979</td>
<td>1385</td>
</tr>
<tr>
<td>BRAMs</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Clock Frequency</td>
<td>92 MHz</td>
<td>190 MHz</td>
</tr>
<tr>
<td>Clock cycles</td>
<td>94,249</td>
<td>94,249</td>
</tr>
<tr>
<td>Decryption Latency</td>
<td>1.02 ms</td>
<td>0.50 ms</td>
</tr>
<tr>
<td>Security</td>
<td>80 bits</td>
<td>80 bits</td>
</tr>
</tbody>
</table>

Table 4 Hardware implementation results of DES, DESX, DESL and DESXL. All figures are obtained at or calculated for a frequency of 100KHz. [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.
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 crypto-processors 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 cryptographic processor implementation. Several designs of crypto-processors are proposed and implemented but still fully functional crypto-processor 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

[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-III Vortex-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

[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
[34] Beuchat et al, Compact Implementation of BLAKE on FPGA, 2010
[38] Zhije Shi et al, Hardware Implementation of Hash Function, Springer LLC 2012
[39] Ho-Won Kim et al, Design and Implementation of public key cryptoprocessor and its application to a security system
[43] Amir Moradi, Side-Channel Leakage through Static Power Should we care in practice