Comparative Analysis of Flexible Cryptographic Implementations

Muhammad Rashid
Computer Engineering Department,
Umm Al-Qura University,
Makkah, Saudi Arabia.
mfelahi@uqu.edu.sa

Malik Imran
National Science, Technology,
and Innovation Plan
Makkah, Saudi Arabia.
mlk. imran88@gmail.com

Atif Raza Jafri
Electrical Engineering Department,
Bahria University,
Islamabad, Pakistan.
atif.raza@bui.edu.pk

Abstract—**Flexible hardware implementations of cryptographic algorithms in the real time applications have been frequently proposed. This paper classifies the state-of-the-art research practices through a Systematic Literature Review (SLR) process. The selected researches have been classified into three design categories: crypto processor, crypto coprocessor and multicore crypto processor. Subsequently, comparative analysis in terms of flexibility, throughput and area is presented. It facilitates the researchers and designers of the domain to select an appropriate design approach for a particular algorithm and/or application.**

Keywords— Crypto processors; coprocessors; multicore processors; symmetric; asymmetric; cryptography; flexibility; throughput; FPGA; CMOS

1. Introduction

Efficient flexible hardware architectures/engines are frequently used to implement the cryptographic algorithms [1 – 51]. For example, a crypto processor [1 – 29] is a programmable hardware, with a dedicated instruction set. In crypto coprocessors [30 – 41], a hardware module is attached with the host processor, such that the attached hardware module can be controlled by using the host processor. Similarly, multiple cores are coupled in a multi core processors design to perform cryptographic operations efficiently [42 – 51]. The objective of this Systematic Literature Review (SLR) is to identify the latest research practices where flexible architectures have been used for cryptographic algorithms. Consequently, the following research questions (RQs) have been developed for this SLR:

RQ 1: What important cryptographic algorithms have been reported recently for flexible implementation?

RQ2: What are the implementation details of selected algorithms in RQ 1?

RQ 3: What are the challenges and consequently the emerging trends for the flexible crypto engines?

The researchers are selected through a systematic methodology, described in Section 2. The selected researches are categorized into three types: symmetric algorithms, asymmetric algorithms and combined (symmetric as well as asymmetric) algorithms A comprehensive analysis of the selected researches is performed and the results are described in Section 3 and Section 4. The answers of all research questions are provided in Section 5. Finally, Section 6 concludes this paper.

2. Methodology

Systematic Literature Review (SLR) [62] is used to carry out this research. This section integrates the two major stages of SLR: 1) classification of selected researches and 2) development of review protocol.

A. Classification of Selected Researches

We have defined three categories in order to organize and classify the selected researches.

- ***Crypto processor*** is a programmable hardware, with a dedicated instruction set, and consists of main memory, arithmetic logical unit and a control unit.
- ***Crypto coprocessor*** is a technique where a hardware module is attached with the host processor such that the attached hardware module cannot be programmed, but can be controlled by using the host processor.
- ***Multicore crypto processor*** considers the parallel architecture for cryptographic computations using several cores. The benefits of multi core systems are parallel speedup and programmability.

B. Research Protocol

The developed review protocol for this SLR consists of: selection and rejection criterion, search process and data extraction/synthesis. The details are given in the following:

- ***Selection and rejection criteria*** defines the rules/parameters for the selection and rejection of the research works. The key elements of the criterion is given below:
  - ➢ Select the research work provided that it must be published in IEEE [58], ACM [59], SPRINGER [60] and ELSEVIER [61], during 2008-2015.

978-1-5090-2520-6/16/$31.00 ©2016 IEEE

- ➢ Select the research work provided that a flexible hardware solution is proposed for cryptographic algorithm.
- ➢ Select the research work only if the target implementation platform is either FPGA or CMOS.

- ***Search process*** selects the research works as per given criterion. To conduct the search process, we have used multiple search terms. The details of these search terms as well as their corresponding results in different selected scientific data bases [58 – 61] are provided at [63].
- ***Data extraction and synthesis*** is required to extract and synthesize the relevant data, required to get the answers of research questions, described in Section 1 of this paper. It allows to fist classify the results in different categories. Based on the classification, a performance comparison is made between different alternatives.

3. CLASSIFICATION RESULTS

We have selected 51 researches [1 – 51] and classified them into three categories: symmetric, asymmetric and combined. The brief description of the identified algorithms in the selected researches can be viewed at [63].

A. Symmetric Algorithms

The selected researches for symmetric algorithms are further classified according to the design type and a particular symmetric algorithm.

- For crypto processor design type, high speed implementations of AES (Advanced Encryption Standard) algorithm are proposed in [1], [4] and [5]. The performance analysis of stream ciphers, used in several telecommunication protocols, is presented in [2]. Furthermore, a highly flexible solution is obtained in [3] by combining multiple symmetric block ciphers, stream ciphers and hash functions.
- For crypto coprocessor design type, AES algorithm is implemented in [32], [33] and [35]. The parameterized approach of [32] allows to perform a tradeoff between throughput and area. The use of parallel AES pipelines at low frequency reduces the power consumption in [33] and [35]. A highly flexible solution, providing a common implementation for supporting different cryptographic operations, is presented in [31].
- For multicore crypto processor design type, the implementation of AES has been observed for modern application like software defined radios [42] and high speed network applications [43].

B. Asymmetric Algorithms

It has been observed that most of the selected researches in the category of asymmetric algorithms target Elliptic Curve Point Multiplication (ECPM) layer of the ECC (Elliptic curve cryptography) with different algorithms: Double and Add [8], [13], [14], [19], [24], [36], [45], [47], Montgomery[10], [11], [18], [21], Lopez Dahab [17], [20], [23], [38], [46], Non Adjacent Form (NAF) [6], Addition and Subtraction [9] and Montgomery ladder [37]. Furthermore, there are some researches where more than one asymmetric algorithm has been targeted. For example, Double and Add algorithm is combined with RSA (Rivest Shamir Adleman) algorithm in [12], [25] and [44].

C. Combined Algorithms

AES symmetric algorithm is frequently combined with asymmetric algorithms and hash functions for multiple objectives according to the requirements of the target application. The examples are:

- RFID (Radio Frequency Identification) application in [26] requires encryption/decryption, key establishment and message authentication. Consequently, AES, ECDSA (Elliptic Curve Digital Signature Algorithm) and SHA-1 (hash function) are used.
- In order to provide a high throughput-to-area ratio, combined algorithms have been targeted in [27 – 29].
- For multicore architectures, the work in [48] implements AES and RSA on an ultra-low powered multi-core processor with 144 tiny cores. Similarly, a configurable IPSec (Internet Protocol Security) processor is proposed in [49], [50] and [51] for high performance network security applications. The IPSec protocol processing (AH and ESP) and crypto algorithms (AES and HMAC-SHA-1) are integrated such that the number of the protocol processing cores and cryptographic algorithms cores can be configured for different performance applications.

4. COMPARATIVE ANALYSIS

The main objective of this section is to provide enough details to compare performance in the most objective way possible. The comparison will be made in all those situation where a common hardware platform is used for the same algorithm and same key length.

A. Symmetric Algorithms

The implementation details for symmetric algorithms are provided according to the design type.

- For crypto processor implementations, a comparison can be made among [1], [4] and [5] for their FPGA implementation results. The area used in [1] is minimum as compared to [4] and [5]. On the other hand, all the three solutions [1], [4] and [5] provide the same results for the ratio of throughput and frequency. Furthermore, the better frequency in [1] entails to a shorter critical path through the use of 2-slow retiming technique in as compared to the parallel sub-pipeline architecture proposed in [4].

- For crypto coprocessor implementations, block cipher algorithms are implemented in [32], [33] and [35]. Work in [33] and [35] can be compared as they have used AES with 128 bit key length over FPGA. By applying a 5-stage pipelined technique, the throughout achieved in [33] is higher as compared to [35]. As far as the area is concerned, we have observed the same throughput per unit slice for both the cases. However, the frequency used in [33] is better which may be due to the implementation on Virtex-6 device as compared to the work in [35] where a relatively slower Virtex-5 device is used. The work in [32] provides the variable key lengths (128, 192 and 564). The overhead of this flexibility for 128 bit key solution, as compared to the work in [33], in terms of area is almost 4 times whereas the throughput is almost half even at the doubled frequency.
- For multi core crypto processor implementations, the work in [42] and [43] implements the AES algorithm with multiple key lengths. It has been observed that the area in [42] is 3 times less as compared to [43]. Moreover, the work in [42], also reported higher throughput and frequency when uses Virtex-4 as compared to [43] where Virtex-2 is used.

B. *Asymmetric Algorithms*

In order to perform a comparative analysis for asymmetric algorithms, we have to organize the selected researches on the basis of targeted algorithms.

- For example, Double and Add is published in [8], [12], [13], [14], [19], [24], [25], [36], [44], [45], and [47]. Among these, [12], [25] and [44] also implement RSA along with Double and Add.
- Similarly, Lopez and Dahab implementations are available in [17], [20], [23], [38] and [46].
- Montgomery algorithm implementations are published in [10], [11], [18], [21] and [37] whereas Montgomery with NAF is described in [22].
- Remaining papers i.e. [6], [9], [15], [16], [7] and [39] are focused on other individual algorithms.

Once the researches are segregated on the basis of algorithms, it is required to compare the researches with the same key length and similar hardware implementation platform, as given in the following.

- In double and add algorithm category, [14], [19] and [36] are comparable, first of all, due to the same key length of 163 bits. Secondly, Startix-II and Viretex-4 FPGAs are used for implementation whose respective ALMs and slices have the same hardware complexity. When comparing throughputs, [14] takes minimum time. However, if we take the product of time and area as a metric of comparison, the work in [19] outperforms [14] by 25% less area-time product. Whereas the solution in [36] has 5 times more area-time product as compared to [19] in order to achieve the additional flexibility in terms of key length. Another comparison can be made for flexibility aspect between [13] and [36] which provide the flexibility through programmability and dynamic reconfiguration respectively. For 163 bit key length, solution in [13] outperforms [36] by achieving less processing time at less hardware cost. Individual result comparison for 192 and 224 bit key lengths can be made for [8] and [24] where 0.13 μm technology is used. The area-time product of both of these implementations are very close to each other for both 192 and 224 bit key lengths. Rest of the papers in this category cannot be directly compared due to the difference in key sizes and/or use of implementation technology i.e. FPGA and CMOS implementation e.g. algorithms to be implemented are same in [12], [22], [25] and [44] are same but supported key lengths and implementation technologies are different.
- Among different Lopez and Dahab implementations, [23], [38] and [46] can be compared because of the similar key length and the same target FPGA device. The area used in [46] is in the middle of the three whereas it achieves highest frequency. Consequently, in terms of the area-time product of [23], [38] and [46], the solution in [46] outperforms the rest.
- For Montgomery algorithm implementations, it is difficult to find the candidates for a balanced comparison due to the use of different FPGA devices.
- Finally, it is also not possible to compare architectures presented in [6], [9], [15], [16], [7] and [39] due to difference in algorithms under consideration and key lengths.

C. *Combined Algorithms*

The unified implementation of symmetric as well asymmetric algorithms are presented in [26 – 29], [40 - 41] and [48 – 51] for crypto processor, coprocessor and multi core crypto processors design types respectively. As different unified architecture target different algorithms, it is not possible to compare the performance of different unified architectures. However, it is important to highlight the motivation behind each unified implementation.

- For the crypto processor category, area comparison can be made between [27] and [29]. The work in [27] uses almost the same resources as that of [29] but provides more algorithmic support and variations in key length. Achieved frequency is almost same in both the cases.
- For crypto coprocessor design type, the work in [40] targets separate cores for each algorithm such that the required algorithm can be mapped on FPGA as per requirements.

- For multi crypto processor category, the work in [50] have proposed implementation of two protocol processing schemes i.e. AH (Authentication Header) and ESP (Encapsulating Security Payload) along with support for AES and HMAC-SHA-1. Similar to [50], the work in [51] targets the same application and the results show the suitability of the proposed architecture for gate way applications

5. Answers of Research questions

This section provides the answers to the research questions based on the results described in the previous sections of this paper (Section 3 and Section 4).

RQ 1: What important cryptographic algorithms have been reported recently for flexible implementation?

Answer: It can be concluded that:

- AES is the most commonly used symmetric algorithm over the last few years for high speed applications. However, new applications, such as wireless communications and network security, require to support multiple algorithms on one chip.
- In case of asymmetric cryptography, elliptic curve point multiplication (ECPM) is frequently implemented. Consequently, we have identified 6 algorithms for ECPM. Furthermore, 3 algorithms have been identified for the protocol layer of ECC. It has been observed that ECC has been used for area efficient high throughput design. However, the use of ECC in the resource constrained (low area as well as low power) applications is emerging.

RQ2: What are the implementation details of selected algorithms in RQ 1?

Answer: The implementation details for symmetric, asymmetric and combined categories are Section 4. The emphasis is to provide enough details so that a fair comparison can be made in different design categories (crypto processor, crypto coprocessor and multi core crypto processor).

RQ 3: What are the challenges and consequently the emerging trends for the flexible crypto engines?

Answer: Selected researches in this paper highlight a number of challenges. Consequently, the solutions proposed in the selected researches have led to the emergence of new trends. Here we summarize our observations:

- For symmetric algorithms, flexible hardware development of AES algorithm has been a high priority and several techniques have been proposed for its implementation [1], [4], [5].
- For asymmetric algorithms, ECC is the leading technique in this category. The most time consuming operation in ECC protocols is the ECPM. Thus, it can be observed that much of the research in the current literature optimizes the ECPM operation [13], [19].
- In many applications, the high-speed performance is required to be achieved within a restricted area performance. The work presented in [14], [18] and [32] are the typical examples of this trend.
- In addition to higher throughput and lower area optimizations, another trend is the development of reconfigurable crypto chips providing side channel attacks (SCA) resistance [11], [12], [16], [17], [24], [30], [37]. The side channel attacks can extract the secret key by sampling the execution time or power consumption or electromagnetic radiation during the encryption process and then performing statistical analysis, without destroying the device.
- It has been observed that all the selected researches providing security features [11], [12], [16], [17], [24], [30], [37] are related to the side channel attack countermeasures. However, in [57] it has been argued that the security threats must be considered at all levels of abstraction such as algorithmic level, software level, microarchitecture level, logic level, and physical level. Architectural robustness can be significantly improved if security aspects are taken into account at all steps in the design process.
- While the area optimized designs have been proposed without countermeasures as well as with counter measures, power optimization is equally important for symmetric [33] as well as symmetric algorithms [21] cryptography.
- The need of supporting multiple cryptographic algorithms on a single chip is increasing. Therefore, the development of a unified architecture, capable of executing multiple algorithms at the same time, is emerging day by day. It allows to optimize the area resources while slightly compromising on speed and throughput.
- It is critical to increase the performance of a cryptographic platform/engine in many challenging and emerging applications like Software Defined Radio (SDR), cloud computing, network servers and cellular sites. Therefore, the inherit benefits of multicore architectures (such as parallel speedup, programmability, and low power density) have been exploited rather than to increase the complexity of a single core. .

6. Conclusions

The objective of this paper is to provide a comparative analysis of flexible cryptographic implementations. The selected researches, obtained through a systematic literature review process, have been classified into three design categories: crypto processors, crypto coprocessors and multicore crypto processors. In addition to the flexibility and higher throughput, the selected researches are classified according to three additional design constraints: area, power and security. Implementation parameters have been presented and analyzed to compare performance in the most objective way possible. Finally, the selected researches in this paper highlight a number of challenges leading to the emergence of new trends.

References

[1] Reza Rezaeian Farashahi, Bahram Rashidi and Sayed Masoud Sayedi, "FPGA based fast and high-throughput 2-slow retiming 128-bit AES encryption Algorithm", Microelectronics Journal, vol. 45, no. 8, pp 1014-1025, August 2014.

[2] Paris Kitsos, Nicolas Sklavos, George Provelengios and Athanassios N. Skodras, "FPGA-based performance analysis of stream ciphers ZUC, Snow3g, Grain V1, Mickey V2, Trivium and E0", Microprocessors and Microsystems, vol. 37, no. 2, pp. 235-245, March 2013.

[3] Gokhan Sayilar and Derek Chiou, "Cryptoraptor: High throughput reconfigurable cryptographic processor", IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, 2014, pp. 155-161.

[4] K. Rahimunnisa, P. Karthigaikumar, N. Anitha Christy, S. Suresh Kumar and J. Jayakumar, "PSP: Parallel sub-pipelined architecture for high throughput AES on FPGA and ASIC", Central European Journal of Computer Science, vol. 3, no. 4, pp. 173-186, December 2013.

[5] Liakot Ali, Ishak Aris, Fakir Sharif Hossain and Niranjan Roy, "Design of an ultra high speed AES processor for next generation IT security", Computers and Electrical Engineering, vol. 37, no. 6, pp. 1160-1170, November 2011.

[6] Reza Azarderakhsh, Kimmo U. Jarvinen, and Mehran Mozaffari-Kermani, "Efficient Algorithm and Architecture for Elliptic Curve Cryptography for Extremely Constrained Secure Applications", IEEE Transactions on Circuits and Systems, vol. 61, no. 4, pp. 1144 - 1155, April 2014.

[7] Jyu-Yuan Lai and Chih-Tsun Huang, "Energy-Adaptive Dual-Field Processor for High-Performance Elliptic Curve Cryptographic Applications", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 19, no. 8, pp. 1512 - 1517, August 2011.

[8] Hamid Reza Ahmadi and Ali Afzali-Kusha, "A low-power and low-energy flexible GF(p) elliptic-curve cryptography processor", Journal of Zhejiang University-SCIENCE C (Computers & Electronics), vol. 11, no. 9, pp. 724-736, September 2010.

[9] Jyu-Yuan Lai and Chih-Tsun Huang, "A Highly Efficient Cipher Processor for Dual-Field Elliptic Curve Cryptography", IEEE Transactions on Circuits and Systems , vol. 56, no. 5, pp. 394-398, May 2009.

[10] Zia-Uddin-Ahamed Khan and Mohammed Benaissa, "Throughput/Area-efficient ECC Processor Using Montgomery Point Multiplication on FPGA", IEEE Transactions on Circuits and Systems , vol. 62, no. 11, pp. 1078 - 1082 , November 2015.

[11] Hamad Alrimeih and Daler Rakhmatov, "Fast and Flexible Hardware Support for ECC Over Multiple Standard Prime Fields", IEEE Transactions onVery Large Scale Integration (VLSI) Systems, vol. 22, no. 12, pp. 2661 - 2674 , December 2014.

[12] Christopher Popper, Oliver Mischke, and Tim Guneysu, "MicroACP - A Fast and Secure Reconfigurable Asymmetric Crypto-Processor – Overhead Evaluation of Side-Channel Countermeasures," 10th International Symposium on Reconfigurable Computing: Architectures, Tools, and Applications, Vilamoura, 2014, pp. 240-247.

[13] K.C. Cinnati Loi and Seok-Bum Ko, "High performance scalable elliptic curve cryptosystem processor for Koblitz curves", Microprocessors and Microsystems, vol. 37, no. 4-5, pp. 394–406, April 2013.

[14] Reza Azarderakhsh and Arash Reyhani-Masoleh, "High-Performance Implementation of Point Multiplication on Koblitz Curves", IEEE Transactions on Circuits and Systems, vol. 60, no. 1, pp. 41-45, January 2013.

[15] Reza Azarderakhsh and Arash Reyhani-Masoleh, "Efficient FPGA Implementations of Point Multiplication on Binary Edwards and Generalized Hessian Curves Using Gaussian Normal Basis", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 20, no. 8, pp. 1453 - 1466, August 2012.

[16] Ayantika Chatterjee and Indranil Sengupta, "Design of a high performance Binary Edwards Curve based processor secured against side channel analysis", Integration the VLSI Journal, vol. 45, no. 3, pp. 331-340, June 2012.

[17] Vladimir Trujillo-Olaya, Timothy Sherwood and Cetin Kaya Koc, "Analysis of performance versus security in hardware realizations of small elliptic curves for lightweight applications", Journal of Cryptographic Engineering, vol. 2, no. 3, pp. 179-188, October 2012.

[18] Michal Varchola, Tim Guneysu and Oliver Mischke, "MicroECC: A Lightweight Reconfigurable Elliptic Curve Crypto-Processor", International Conference on Reconfigurable Computing and FPGAs (ReConFig) , Cancun, 2011, pp. 204-210.

[19] Kimmo Jarvinen, "Optimized FPGA-based elliptic curve cryptography processor for high-speed applications", Integration the VLSI Journal, vol. 44, no. 4, pp. 270-279, September 2011.

[20] DAN Yong-ping, ZOU Xue-cheng, LIU Zheng-lin, HAN Yu and YI Li-hua, "Design of highly efficient elliptic curve crypto-processor with two multiplications over GF(2163)", The Journal of China Universities of Posts and Telecommunications, vol. 16, no. 2, pp. 72-79, April 2009.

[21] Maurice Keller, Andrew Byrne and William P. Marnane, "Elliptic Curve Cryptography on FPGA for Low-Power Applications", ACM Transactions on Reconfigurable Technology and Systems (TRETS), vol. 2, no. 1, pp. 1-20, March 2009.

[22] Kimmo Jarvinen and Jorma Skytta, "On Parallelization of High-Speed Processors for Elliptic Curve Cryptography", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 16, no. 9, pp. 1162 - 1175 , August 2008.

[23] William N. Chelton and Mohammed Benaissa, "Fast Elliptic Curve Cryptography on FPGA", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 16, no. 2, pp. 198-205, Feburary 2008.

[24] Santosh Ghosh, Monjur Alam, Dipanwita Roy Chowdhury and Indranil Sen Gupta, "Parallel crypto-devices for GF(p) elliptic curve multiplication resistant against side channel attacks", Computers and Electrical Engineering, vol. 35, no. 2, pp. 329-338, March 2009.

[25] Yi Wang, Douglas L. Maskell and Jussipekka Leiwo, "A unified architecture for a public key cryptographic coprocessor," Journal of Systems Architecture, vol. 54, no. 10, pp. 1004-1016, October 2008.

[26] Thomas Plos, Michael Hutter, Martin Feldhofer, Maksimiljan Stiglic, and Francesco Cavaliere, "Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 21, no. 11, pp. 1965-1974, November 2013.

[27] Yi Wang and Renfa Li, "FPGA based unified architecture for public key and private key cryptosystems", Frontiers of Computer Science, vol. 7, no. 3, pp. 307-316, June 2013.

[28] Shylashree Nagaraja and Venugopalachar Sridhar, "A Unified Architecture for a Dual Field ECC Processor Applicable to AES,"5th International Conference on Computational Intelligence, Modelling and Simulation (CIMSim), Seoul, 2013, pp. 321-326.

[29] Yi Wang and Renfa Li, "A Unified Architecture for Supporting Operations of AES and ECC," 4th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Tianjin, 2011, pp. 185-189.

[30] Weiwei Shan, Xing Yuan Fu, and Zhipeng Xu, "A Secure Reconfigurable Crypto IC With Countermeasures Against SPA, DPA, and EMA", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 7, pp. 1201-1205, July 2015.

[31] Khawar Shahzad, Ayesha Khalid, Zoltan Endre Rakossy, Goutam Paul and Anupam Chattopadhyay, "CoARX: A Coprocessor for ARX-based Cryptographic Algorithms", 50th ACM/EDAC/IEEE Design Automation Conference (DAC), Austin, 2013, pp. 1-10.

[32] Hassan Anwar, Masoud Daneshtalab, Masoumeh Ebrahimi, Sergei dytckov, Juha Plosila, Hannu Tenhunen and Giovanni Beltrame, "Parameterized AES-based Crypto Processor for FPGAs", 17th Euromicro Conference on Digital System Design (DSD), Verona, 2014, pp. 465 - 472.

[33] Hassan Anwar, Masoud Daneshtalab, Masoumeh Ebrahimi, Juha Plosila and Hannu Tenhunen, "FPGA Implementation of AES-based Crypto

Processor", 20th International Conference on Electronics, Circuits, and Systems (ICECS), Abu Dhabi, 2013, pp. 369 - 372.

[34] Lubos Gaspar, Viktor Fischer, Lilian Bossuet, and Robert Fouquet, "Secure Extension of FPGA General Purpose Processors for Symmetric Key Cryptography with Partial Reconfiguration Capabilities", ACM Transactions on Reconfigurable Technology and Systems (TRETS), vol. 5, no. 3, pp. 1-13, October 2012.

[35] Mostafa I. Soliman and Ghada Y. Abozaid, "FPGA implementation and performance evaluation of a high throughput crypto coprocessor", Journal of Parallel and Distributed Computing, vol. 71, no. 8, pp. 1075–1084, August 2011.

[36] M. Morales-Sandoval, C. Feregrino-Uribe, R. Cumplido and I. Algredo-Badillo, "A reconfigurable GF(2M) elliptic curve cryptographic coprocessor", 7th Southern Conference on Programmable Logic (SPL), Cordoba, 2011, pp. 209 - 214.

[37] Xu Guo and Patrick Schaumont, "Optimized System-on-Chip Integration of a Programmable ECC Coprocessor", ACM Transactions on Reconfigurable Technology and Systems (TRETS), vol. 4, no. 1, pp. 1-21, December 2010.

[38] Chang Hoon Kim, Soonhak Kwon and Chun Pyo Hong, "FPGA implementation of high performance elliptic curve cryptographic processor over GF(2163)", Journal of Systems Architecture, vol. 54, no. 10, pp. 893-900, April 2008.

[39] Michael Gautschi, Michael Muehlberghuber, Andreas Traber, Sven Stucki, Matthias Baer, Renzo Andri, Luca Benini, Beat Muheim and Hubert Kaeslin, "SIR10US: A Tightly Coupled Elliptic-Curve Cryptography Co-Processor for the OpenRISC", 25th International Conference on Application-specific Systems, Architectures and Processors (ASAP) , Zurich, 2014, pp. 25-29.

[40] Shice Ni, Yong Dou, Kai Chen, and Lin Deng, "A Novel Design of Flexible Crypto Coprocessor and Its Application", 10th Annual Conference on Advanced Computer Architecture (ACA), Shenyang, 2014, pp. 128-139.

[41] Antonio de la Piedra, An Braeken and Abdellah Touhafi, "A Performance Comparison Study of ECC and AES in Commercial and Research Sensor Nodes", 2013 IEEE, EUROCON, Zagreb, 2013, pp. 347-354.

[42] Michael Grand, Lilian Bossuet, Bertrand Le Gal, Guy Gogniat and Dominique Dallet, "Design and Implementation of a Multi-Core Crypto-Processor for Software Defined Radios", 7th International Symposium on Reconfigurable Computing: Architectures, Tools and Applications, Belfast, 2011, pp. 29-40.

[43] Mao-Yin Wang, Chih-Pin Su, Chia-Lung Horng, Cheng-Wen Wu, and Chih-Tsun Huang, "Single- and Multi-core Configurable AES Architectures for Flexible Security", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 18, no. 4, pp. 541-552, April 2010.

[44] Jun Han, Renfeng Dou, Lingyun Zeng, Shuai Wang, Zhiyi Yu, and Xiaoyang Zeng, "A Heterogeneous Multicore Crypto-Processor With Flexible Long-Word-Length Computation", IEEE Transcations on Circuits and Systems, vol. 62, no. 5, pp. 1372-1381, May 2015.

[45] Pascal Sasdrich and Tim Guneysu, "Efficient Elliptic-Curve Cryptography Using Curve 25519 on Reconfigurable Devices", 10th International Symposium on Reconfigurable Computing: Architectures, Tools, and Applications, Vilamoura, 2014, pp. 25-36.

[46] Yu Zhang, Dongdong Chen, Younhee Choi, Li Chen and Seok-Bum Ko, "A high performance ECC hardware implementation with instruction-level parallelism over GF(2163)", Microprocessors and Microsystems, vol. 34, no. 6, pp. 228-236, April 2010.

[47] Junfeng Fan, Kazuo Sakiyama and Ingrid Verbauwhede, "Elliptic curve cryptography on embedded multicore systems", Design Automation for Embedded Systems, vol. 12, no. 3, pp. 231-242, Semptember 2008.

[48] Tobias Schneider, Ingo von Maurich, Tim Guneysu and David Oswald, "Cryptographic Algorithms on the GA144 Asynchronous Multi-Core Processor", Journal of Signal Processing Systems, vol. 77, no. 1, pp. 151-167, October 2014.

[49] Yun Niu, Li-ji Wu, Yang Liu, Xiang-min Zhang and Hong-yi Chen, "A 10 Gbps in-line network security processor based on configurable hetero-multi-cores", Journal of Zhejiang University-SCIENCE C (Computers & Electronics), vol. 14, no. 8, pp. 642-651, August 2013.

[50] Yun Niu, Liji Wu, Li Wang, Xiangmin Zhang and Jun Xu, "A Configurable IPSec Processor for High Performance In-Line Security Network Processor", 7th International Conference on Computational Intelligence and Security (CIS), Hainan, 2011, pp. 674 - 678.

[51] Mao-Yin Wang and Cheng-Wen Wu, "A Mesh-Structured Scalable IPsec Processor", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 18, no. 5, pp. 725 - 731, May 2010.

[52] Bruce Schneier, Applied Cryptography: "Protocols, Algorithms and Source Code in C", 20th Anniversary Edition, John Wiley & Sons, 784 pages, ISBN: 978-1-119-09672-6, May 2015.

[53] Federal Information Processing Standards Publication (FIPS PUB) 197, National Institute of Standards and Technology (NIST). Advanced encryption standard (AES).

[54] Technical Guideline TR-03111. (2012, June) Elliptic Curve Cryptography, Available at: http://www.bsi.bund.de.

[55] Hamid Reza Ghasemi, Hossein Mohammadi, Behnam Robatmili, and Nasser Yazdani "Augmenting general purpose processors for network processing", IEEE International Conference on Field-Programmable Technology (FPT), 2003, pp. 416-419.

[56] P. Karthigai Kumar and K. Baskaran, "An ASIC implementation of low power and high throughput blowfish crypto algorithm", Microelectronics Journal, vol. 41, no. 6, pp. 347-355, June 2010.

[57] Lilian Bossuet, Michael Grand, Lubos Gaspar and Guy Gogniat, "Architectures of flexible symmetric key crypto engines—a survey: From hardware coprocessor to multi-crypto-processor system on chip", ACM Computing Surveys (CSUR), vol. 45, no. 4, pp. 1-33, August 2013.

[58] IEEE scientific database. Last Accessed, November 2014. http://ieeexplore.ieee.org/.

[59] ACM. Last Accessed November 2014. http://dl.acm.org/.

[60] Springer. Last Accessed July 2014. http://link.springer.com/.

[61] Elsevier. Last Accessed July 2014. http://www.sciencedirect.com/.

[62] Mathieu Lavallée, Pierre-N. Robillard, and Reza Mirsalari, "Performing Systematic Literature Reviews With Novices: An Iterative Approach", IEEE Transanctions on Education, vol. 57, no. 3, pp. 175-181, August 2015.

[63] IDECAA Project, http://idecaa.com/pro-status.php