Reconfigurable hardware architecture of public key crypto processor for VANET and wireless sensor nodes

G. Leelavathi* and K. Shaila

VTU-Research Centre,
Vivekananda Institute of Technology,
Visvesvaraya Technological University,
Belgaum, Karnataka, India
Email: nisargamodini@gmail.com
Email: shailak17@gmail.com
*Corresponding author

K.R. Venugopal

Bangalore University,
Bengaluru, Karnataka, India
Email: venugopalkr@gmail.com

Abstract: This work proposes encryption of text and image data, embedding as elliptic curve point. Finite field arithmetic is utilised efficiently in this reconfigurable crypto system. Pre-computations for text data and image input conversion is done using MATLAB. This architecture is tailored for cryptographic applications and VANET using Xilinx Spartan-xc3s100e-4-fg320 FPGA with Verilog coding. Total encryption and decryption time results around 10.09021 microseconds for 100×100 images, 22.091 microseconds for 256×256 images and 0.029 microseconds for a message. The message size is varied with different stream size and dynamic mapping of input data and a cipher image with high randomness indicates good security i.e., less vulnerable to attacks. An entropy statistical analysis is performed on plain and encrypted images to assess the strength of the proposed method. An encryption throughput rate is 450 Mbps and area throughput 3.63, which is a good improvement over previous implementations.

Keywords: elliptic curve cryptography; entropy; ElGamal; FPGA; mapping; public key cryptography; VANET.

Reference to this paper should be made as follows: Leelavathi, G., Shaila, K. and Venugopal, K.R. (2020) 'Reconfigurable hardware architecture of public key crypto processor for VANET and wireless sensor nodes', *Int. J. Vehicle Information and Communication Systems*, Vol. 5, No. 1, pp.11–25.

Biographical notes: G. Leelavathi is an Assistant Professor in the Department of Electronics and Communication Engineering at Govt. SKSJTI, Bangalore, India. She received her BE and ME degrees in Electronics and Communication Engineering from Bangalore University and Visvesvaraya Technological University, respectively. Her research areas are wireless sensor networks and reconfigurable embedded systems. She has published around 10 papers in national and international conferences.

K. Shaila is a Professor and Head of the Department, Vivekananda Institute of Technology. She obtained her PhD degree in Computer Science and Engineering from Bangalore University, ME degree in Electronics and Communication from University Visvesvaraya College of Engineering, Bangalore University and BE degree from PES Institute of Technology, Bangalore University, Bangalore. She has over 20 years of teaching experience. She has authored *Digital Circuits and Systems* published by Tata McGraw Hill, New Delhi and *Secure Data Communication Techniques* by LAP LAMBERT publishers, Germany. She has published papers in refereed International Journals and International Conferences. She has received Best Teacher and Best Researcher Award. Her name appears in Marquis Who's Who in the World Science and Engineering. She is the Life Member of ISTE, iMAPs, Member of ACM, IEANG and Reviewer for conference and journals. Her research areas include wireless sensor networks, ad-hoc networks and image processing.

K.R. Venugopal is a Vice Chancellor, Bangalore University. He has 11 degrees with PhD in Computer Science Engineering from IIT-Madras, Chennai and another PhD in Economics from Bangalore University. He has degrees in Law, Mass Communication, Electronics, Economics, Business Finance, Computer Science, Public Relations and Industrial Relations. He has authored and edited 64 books and published more than 700 papers in refereed International Journals and International Conferences. He has supervised 630 ME Dissertations, 25 PhDs and filed 101 Patents. He was a Post-Doctoral Research Scholar and a visiting Professor at University of Southern California, USA. He has been conferred Fellow of IEEE, USA and ACM Distinguished Educator for contributions to Computer Science Engineering and Electrical Engineering Education.

This paper is a revised and expanded version of a paper entitled 'Message and Image Encryption Embedding Data to GF(2^m) Elliptic Curve Point for Nodes in Wireless Sensor Networks' presented at the 'BDCC-2018 EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing', Coimbatore, Tamilnadu, India, 12–13 December 2018.

1 Introduction

Wireless Sensor Networks (WSNs) form an ad hoc network, comprising multi-functional sensor nodes. Security procedures are generally the tasks consuming most of the overall processing capacity in network devices of WSNs (Akylidiz et al., 2002). Security techniques demand a certain amount of resources for the implementation which are limited in tiny wireless sensor nodes. Elliptic Curve Cryptography (ECC) is selected to satisfy the constraints of WSNs due to its high security for smaller key bit length (Shaila et al., 2011; Leelavathi et al., 2017).

Either cryptography or steganography can be used to provide security. Cryptography uses mathematics in which the data are converted into some other form using to encrypt and decrypt data; then the encrypted data are transmitted over the channel. Steganography is the method of shield writing encoding/embedding hidden material in cover media. Image encryption is given much attention for information security and many image encryption algorithms presented. Due to some inherent structures of images like high data redundancy and bulk data capacity, the encryption of image is different from that of text. This makes them difficult to handle by conventional encryption

methods. The purpose of this work is to provide security through a three-step process, i.e., pre-computations using MATLAB, mapping to elliptic curve point and encryption by ElGamal process.

In the proposed work, a new image encryption algorithm based on embedding of image data to elliptic curve point is being applied. To begin with, the plain-image is converted into ASCII values matrix by MATLAB and then the ASCII value is embedded to EC point for encryption. Further, the parameters of elliptic curve selected randomly by the user for encryption and decryption process of the algorithm play a vital role for security. Subsequently the image is being encrypted with ElGamal public key cryptography algorithm.

2 Literature survey

A sensor based FPGA and application domains of FPGAs are discussed in De la Piedra et al. (2012) and Rodriguez-Andina et al. (2007). Their survey explores the possible usage of FPGAs in sensor node architecture and applications aiming on the proper optimisation of resources of modern FPGAs. The inadequacies in the research nodes and the commercial nodes in terms of extended processing capabilities are emphasised. A block oriented key and data is considered in the design with binary field (Leelavathi et al., 2017). Mapping of text data to an elliptic curve over the Galois field is described in King (2009). George Amalarethinam and Geetha (2015) adds 32×48, magic rectangle to enhance randomness of the cipher text with RSA cryptosystem using Java. Soleymani (2013) introduced a map table technique to transform an image pixel value to a point on a predefined elliptic curve over finite field GF (p). The design was implemented and analysed by MATLAB with Intel Microprocessor.

Gupta and Silakari (2011) developed diffusion template with 3D standard map and a Cat map. Astya et al. (2014) implemented a technique for BMP images of different sizes using ECC in C language. Singh and Singh (2015) includes digital signature with cipher image to afford authenticity and integrity by grouping the pixels according to the ECC parameters. Instead of mapping of values pairing of the grouped pixels is mapped to elliptic curve coordinate. Nagaraj et al. (2015) proposed magic matrix operations for protecting images and design is implemented using Dot Net software. They apply the encryption methods only on gray scale images. Zhu et al. (2010) scrambles the image pixels, with watermark thus increasing the difficulty in decoding. Woolinger et al. (2003) concentrate on symmetric key (AES, DES) and asymmetric key (RSA, ECC) algorithm implementation on FPGAs on Xilinx and Altera FPGAs with several types of attacks. Many parameters are used in related area (hardware) results in literature survey include CLBs, LUTs, FFs, number of CLB slices and equivalent logic gates.

Problem definition: From the literature survey it is observed that most of the designs are software implementation with different programming languages like Java, C, C++, and DOT-NET. The works discussed from literature are majorly focused on the encryption and decryption of images with software implementation, using different programming languages on processors. This necessitates the hardware design of proposed cryptosystem. In case of public key algorithms general purpose CPUs are not enhanced for fast execution particularly. As the input characters i.e., input data size increases the matrix size increases and leads to computational complexity thereby using

more area (Leelavathi et al., 2018). Scalar point multiplication which includes point addition and point doubling consumes maximum computational time.

Crypto-accelerators are proficient and characteristically accomplish better power efficiency and performance over software implementation with a general purpose processor. This proposed work is concentrated on the design of efficient hardware architecture for ECC over binary Galois field, which is mainly affected by the underlying arithmetic primitives. Scalar multiplication the most critical operation is replaced by message mapping to an elliptic curve point and ElGamal technique is employed with ECC parameters set. Primary field is considered with mapping of message in some implementations. It is required to design a crypto processor with low computational complexity to match the requirements of WSN nodes. In the previous decade, the method of hardware employment of an ECC algorithm drew much attentive competition with security, speed and area constraints.

Contribution: Amiri and Elkeelany (2013) proposed a reconfigurable architecture using ECC for mapping and encrypting a message. The message considered is 163-bit static data with sequential and parallel architecture. The basic idea is modified in our approach to reduce the computational complexity in ECC. The data considered is 9 bit hex value with a continuous message and also an image is encrypted to provide security of the data.

The proposed work considers both data and image, aims to design crypto processor with hardware implementations. The binary field GF (2^m) is chosen for design and embedding a message on an elliptic curve points. The variable text length is considered as input data and also different size images for image inputs. It is a stream oriented approach than static size data input. The proposed work targets to design arithmetic architectures for public key cryptosystem considering stream of input data and the work is also extended to encryption of images with different sizes.

Remaining parts of this paper are organised as follows. The proposed model with ECC basics and computational details are provided in Section 2. Section 3 describes the implementation details of the proposed approach. In Section 4 the simulation set up and results with discussion of performance and entropy analysis are presented. Section 5 concludes the paper.

3 Model and computational details

The cryptosystem designed is dedicated to encrypt the text message and an image at hardware level. The ECC algorithm's performance depends competently on the arithmetic in the underlying Galois Field (GF). The GFs are binary fields GF (2^m) and prime fields GF (p). The representation considered in this work is a normal base that is most appropriate for hardware implementation.

An elliptic curve over GF (2^m) is defined as the cubic equation ($E_{a,\ b}$). The *Points of* the *Elliptic Curve* (E) are a set of solutions obtained with equation (1), where, $a, b, x, y \in$ GF (2^m) and $b \neq 0$. The elliptic curve $E_{a,b}$ considered in this work for cryptographic application is represented in equation (2).

$$(x, y) \mid y^2 + x * y = x^3 + ax^2 + b \tag{1}$$

$$y^2 + x * y = x^3 + x^2 + 1 \tag{2}$$

The additive Abelian group elliptic curve $E_{a,b}$ contains points $(x, y) \in$ GF (2^m), are in affine coordinate system, where a and b are equal to 1.

The core challenge is to map the characters of message and an image to (x, y) point i.e., $P(x, y)$ on the $E_{a,b}$ elliptic curve defined by equation (2). As described in King (2009) and Amiri and Elkeelany (2013), it is unlikely that any character of message or an image (hexadecimal value) belong to an Elliptic curve field. Therefore to perform any mathematical operation on data (message or an image) it would have to be within $E_{a,b}$ i.e., additive Abelian group. It is proved in King (2009) that any message M can be mapped to a valid elliptic curve point with a deterministic algorithm as described in Algorithm (1).

Finite multiplication and finite addition are used to encrypt the data to be transmitted using ElGamal method. The computation of γ, with chosen values of x_1 and M is given by equation (3).

$$\gamma = \left(M^2 / x_1^2\right) + \left(M / x_1\right) + x_1 + a + \left(b^2 / x_1^2\right) \tag{3}$$

where $M,\ x_1 \in GF\left(2^m\right),\ M$ is the message or image data in hexadecimal value. The point $(x_1,\ M)\ \in E_{a+\gamma,b}$ where $E_{a+\gamma,b}$ denotes the whole points $(x, y) \in$ GF (2^m) and fulfil equation (4).

$$y^2 + x * y = x^3 + (1+\gamma)\ x^2 + 1 \tag{4}$$

where $a = 1 + \gamma,\ b = 1 \in GF(2^m)$. For any $\gamma \in GF(2^m)$, the equation $\lambda^2 + \lambda = \gamma$ has a solution when, $Tr\ (\gamma) = 0$, the details are originally found in King (2009) and Amiri and Elkeelany (2013) where mapping a message M to an elliptic curve point is explained mathematically in detail. With solution of λ, the isomorphism can be implemented, which is represented as $E_{a,b} \to E_{a+\gamma,b}$ and $E_{a+\gamma,b} \to E_{a,b}$. The λ is defined by the equation (5).

$$\lambda = \sum_{i=0}^{(n-1)/2} \left(\gamma^2\right)^{2i} \tag{5}$$

The computation of λ with γ input is performed by an exponential module, where the 8 bit exponent 2 is carried out by squaring and XOR operations for $0 \le i \le 4$, 8 bit system.

4 Implementation details

4.1 Encryption architecture

In this architecture Alice and Bob are considered as the sender and receiver. The ElGamal public key encryption includes scheming Bob's public key via finite multiplication procedure under $E_{a,b}$. Bobs public key $qax = db*x$, in which the first coordinate of the point $P(x, y)$ is multiplied by Bob's private key db. The public key is expected to be conveyed to Alice through a secured exchange protocol. Alice's encryption key is computed $(ka*db*x)=(ka*qax)$, where ka is Alice's private key. The encryption process with elliptic curve is shown in Figure 1. The complete process of encryption is given in Figure 2. The procedure for mapping of input data to EC point is given in Algorithm 1.

Figure 1 Process of message mapping

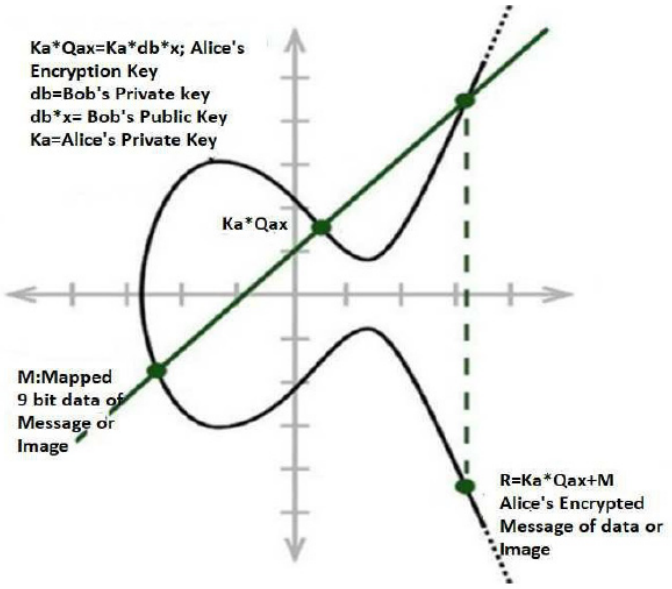
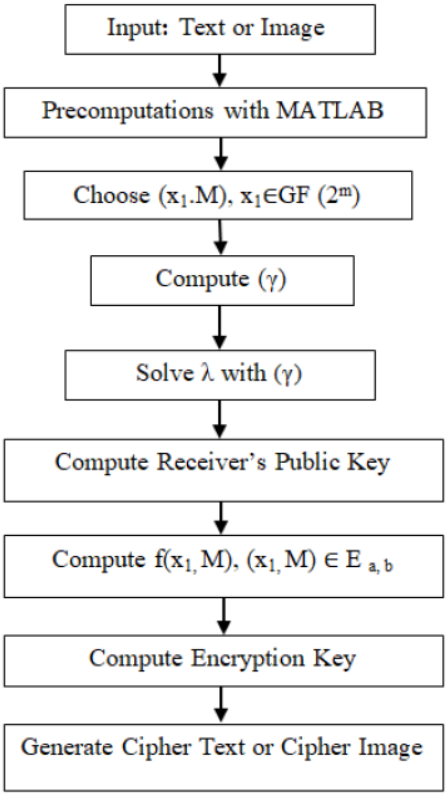


Figure 2 Processes of message or image mapping and encryption



Algorithm 1 Mapping of message to an elliptic curve point

Input: x_1 co-ordinate of EC point, M Character in input stream

Select $y^2 + x * y = x^3 + x^2 + 1$

Choose $x_1 \in GF(2^m)$

Set $\gamma = \left(M^2 / x_1^2\right) + \left(M / x_1\right) + x_1 + a + \left(b^2 / x_1^2\right)$

Return $x_1 \in E_{1+\lambda,1}$

The data from the text file and image file is extracted and converted to hexadecimal values. These hexadecimal values are treated as a message (M) and using the same values the point $P(x, M + x.\lambda)$ is generated and mapped. The message (M) is used in the equation to calculate (γ). The second point $P(x, M + x.\lambda)$ is calculated through finite multiplication, addition and XOR operations. Computation of $P = (x, y) \in E_{a+\gamma,b}$ and mapping f: $E_{a+\gamma,b} \to E_{a,b}$ is denoted by $f(P) = f(x, y) = (x, M + x.\lambda) = (x^*, y^*) \in E_{a,b}$. Finally, the message ($M$) is being mapped on the elliptic curve defined by equation (2) as shown in Figure 1. Following the ElGamal encryption technique, two coordinates ($C1x$, $C2y$) cipher data are computed and transmitted.

4.2 Decryption method

The decryption is performed with the points received cipher text points ($C1x$, $C2y$). The first coordinated of the received cipher text is Alice's public key $C1x = (ka * x)$, required for decryption process at receiver's side. The second coordinate of the cipher text is $C2y$= M +Ka*Qax. In order to decrypt the message as a first step it is required to perform $(-db * (ka * x))$, in which db is the (Bob's) receiver's private key. The decryption process with [M +Ka*Qax] – [db*(Ka*x)] equation i.e., ($C2y$) – db*($C1x$) is performed by finite multiplication and XOR operation. This is followed by a finite addition under $E_{a,b}$ between the cipher message $M + Ka * Qax$ and the decryption key $-db^* (Kax)$ to get back the original message data.

5 Results and discussion

5.1 Simulation setup and results

The Spartan FPGA device xc3s100e-4cp132 is used in this work for hardware implementation and it is low cost FPGA. The same design on advanced FPGAs works expectedly faster satisfying all requirements of area and speed. The timing waveform for the image and message is shown in Figure 3. The input values x, db, Ka and M, are of 9 bits. The 32 bit count value depends on the input message or image data.

The simulation process with execution details on MATLAB for cipher text of message is shown in Figure 4. The Verilog code files interfaced with MATLAB can be observed on current folder column. An example of text message results is shown in Figure 5. The device utilisation summary of this design is provided in Figure 6 and the

static device utilisation details in Figure 7. The results are obtained with different images considered for executions are shown in Figure 8. The *M* [8:0] is the input plain text data, *y* [8:0] cipher output and outl [8:0] is decrypted output i.e., the original message. The text message of different sizes is considered for simulation as shown in Figure 4 and image of different sizes is reshaped before assigning as input image.

Figure 3 Timing waveform for image input

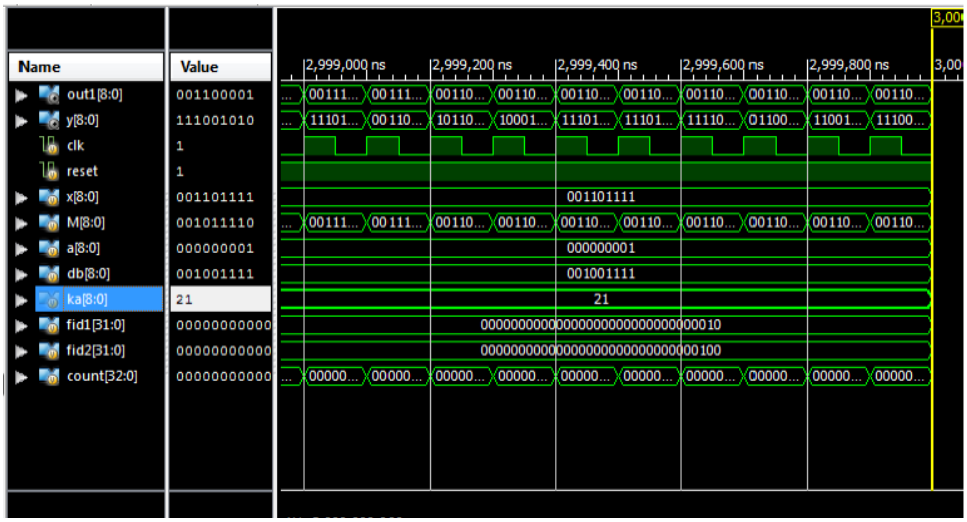


Figure 4 Execution details on MATLAB for cipher text of message

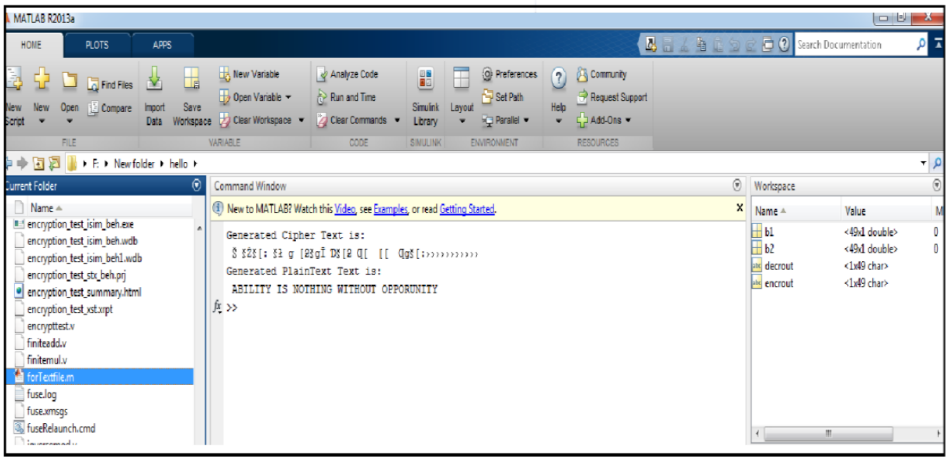


Figure 5 Cipher text of message

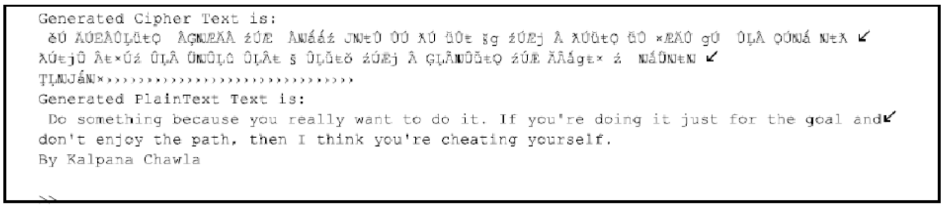


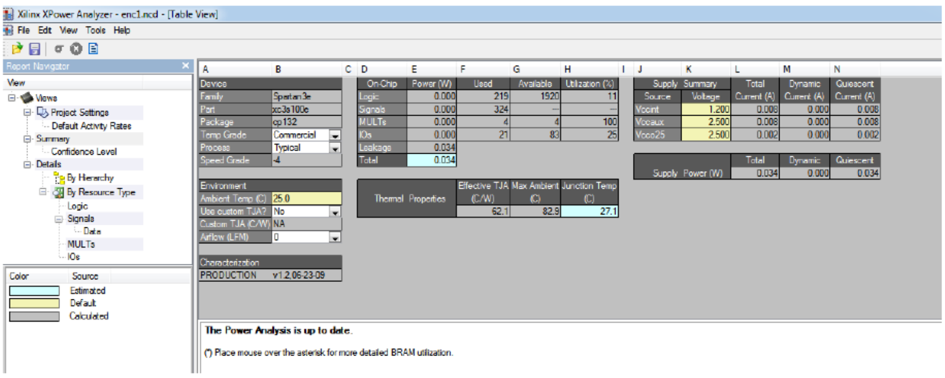
Figure 6 Device utilisation details

Project File:	eccexample.xise	**Parser Errors:**	No Errors
Module Name:	enc1	**Implementation State:**	Programming File Generated
Target Device:	xc3s100e-4cp132	**• Errors:**	
Product Version:	ISE 14.7	**• Warnings:**	
Design Goal:	Balanced	**• Routing Results:**	All Signals Completely Routed
Design Strategy:	Xilinx Default (unlocked)	**• Timing Constraints:**	
Environment:	System Settings	**• Final Timing Score:**	0 (Timing Report)

Device Utilization Summary

Logic Utilization	Used	Available	Utilization	Note(s)
Number of 4 input LUTs	203	1,920	10%	
Number of occupied Slices	124	960	12%	
Number of Slices containing only related logic	124	124	100%	
Number of Slices containing unrelated logic	0	124	0%	
Total Number of 4 input LUTs	222	1,920	11%	
Number used as logic	203			
Number used as a route-thru	19			
Number of bonded IOBs	21	83	25%	
Number of MULT18X18SIOs	4	4	100%	
Average Fanout of Non-Clock Nets	2.26			

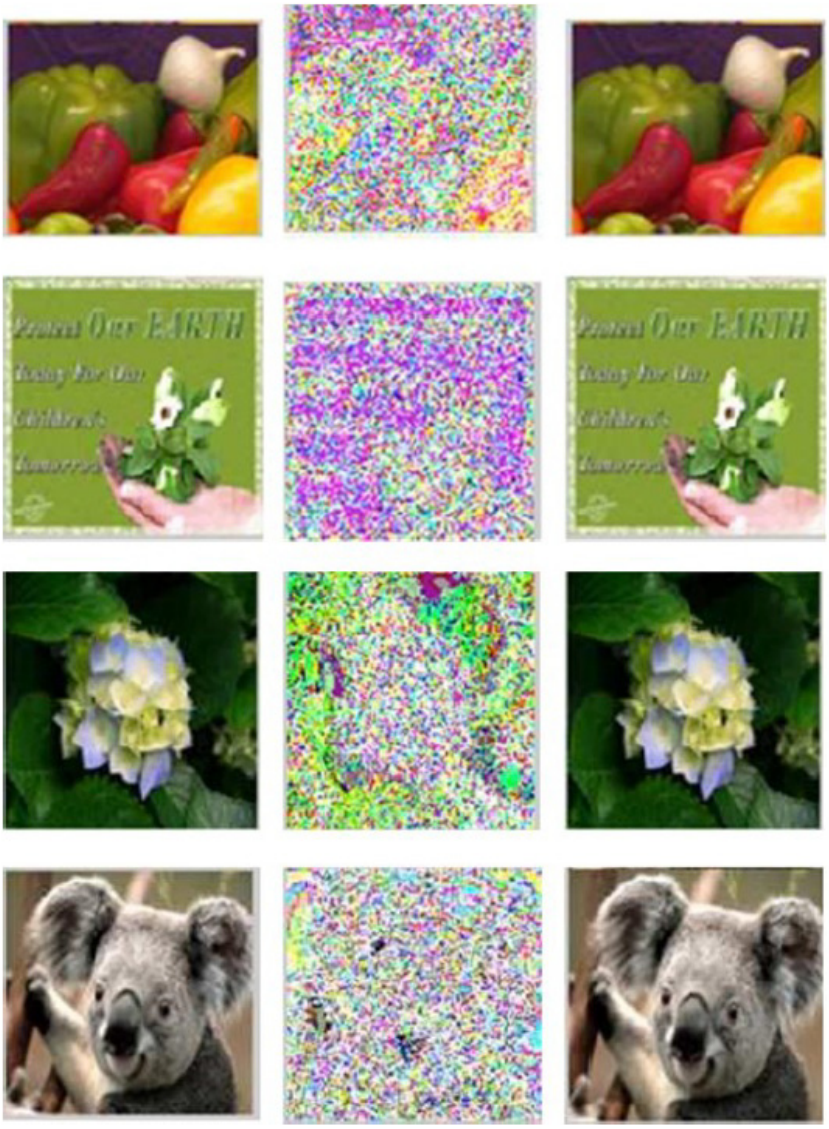
Figure 7 Static power utilisation details



5.2 Performance analysis

Security of the encrypted message is offered by a rapid mapping procedure i.e., mapping data to elliptic curve point. This mapping method shows irregularity in the cipher text with respect to the input data. Encrypt and decrypt operation most effectively takes place on the curve using ElGamal encryption algorithm. This method increases the security by avoiding the brute force attack by developing confusions to the third person. With a given plaintext it produces different cipher text thus, avoiding from identifying intercepted messages by comparing them to a set of known cipher text.

Figure 8 Original, encrypted and decrypted images of pepper, earth, flower and panda



Following the conventions of Woolinger et al. (2003) we have practised to mention CLB Slices and LUTs as hardware costs associated with area and performance to compute throughput, which are considered as important characteristics in cryptographic implementation. Encryption Throughput, Throughput per CLB Slice (TPS) and Throughput per LUTs (TPL) metrics are utilised to evaluate the area performance.

We have tailored this architecture for cryptographic applications specifically consisting of cost-efficient Xilinx Spartan-3 FPGA xc3s500e-4-fg320. The encryption and decryption time depends on the data and image to be processed. The time required is proportional to the count value, with the message length and image size. A new embedding process is presented to transform text data and image pixel hexadecimal value to a random point on a predefined elliptic curve over binary field GF (2^m) with ElGamal encryption. The output for text messages is shown in Figure 5. The Static power utilisation of 0.034 Watts is observed in Figure 7. The encryption process output is shown in Figures 8 and 9 for different images. Total encryption and decryption time results are around 10.09021 microseconds for 100×100 images and 0.029 microseconds for a message.

Amiri and Elkeelany (2013) take up 163-bit static data input for implementation of different key sizes. For comparison we have considered the 2^5 i.e., 32 bit key size. Table gives this performance analysis in comparison with previous works. Astya et al. (2014) and Nagaraj and Raju (2015) applies encryption methods only on Grey scale images.

Table 1 shows the device utilisation with more number of LUTs utilised and 124 slices. The more number of LUTs indicates that it reduces the computational delay. It is observed the setup and hold time are at 0 time, which indicates no combinational path delay is found in the design. The computational time for different messages is compared with Rami (2009) as shown in Table 2. It is 0.029 microseconds and the computational throughput is 310 Mbps as given in Table 3. The number of registers required for the design is 124 and it is 80 times less than the previous implementation as tabulated in Table 4.

Table 1 Device utilisation

Logic utilisation	*Used*	*Available*	*Percentage of usage*
4 input LUTs	203	1920	10
Slices	124	960	12
Bonded IOBs	21	83	21

Table 2 Computation time comparison for message input on FPGA

Reference	*Tool*	*Encryption time*	*Decryption time*	*Total*
Amiri and Elkeelany (2013)	FPGA Cyclone IV E	3.706 m sec	2.712 m sec	6.418 m sec
Our work	Xilinx Spartan	0.020 μ sec	0.009 μ sec	0.029 μ sec

Table 3 Throughput comparison for message input on FPGA

Reference	*Tool*	*Encryption throughput*	*Decryption throughput*	*Total throughput*
Amiri and Elkeelany (2013)	FPGA cyclone IV E	8.706 Kbps	11.799 Kbps	4.985 Kbps
Our work	Xilinx Spartan	450 Mbps	1000 Mbps	310 Mbps

Table 4 Device utilisation comparison for message input on FPGA

Reference	*Logic elements*	*Registers*
Amiri and Elkeelany (2013)	13%	11059
Our work	10%	124

Area throughput is calculated in terms of TPS (encryption rate/number of slices) and TPL (encryption rate/number of LUTs) as shown in Table 5. In TPS and TPL the encryption rate is directly proportional and the number of slices or LUTs is inversely proportional. With increase in number of slices, the throughput decreases. The throughput (TPS and TPL) increases with increase in encryption rate and it is 3.63 and 2.22 as given in Table 5.

Table 5 Area throughput for message inputs

LUTs	*Slices*	*Encryption throughput*	*TPS*	*TPL*
203	124	450 Mbps	3.63	2.22

To evaluate the strength of this algorithm an entropy statistical analysis is performed on plain and encrypted images and the results are shown in Table 7. The cipher image names are shown in bold.

The Table 6 contains computational time comparison for 256*256 image input with previous implementations on different tools. The encryption and decryption time are in terms of microseconds with this design.

Table 6 Computational time comparison for 256*256 image input

Reference	*Tool*	*Encryption time*	*Decryption time*	*Total time*
Singh and Singh (2015)	Mathematica	0.29sec	0.30sec	0.59sec
Gupta and Silakari (2011)	Mat lab	11.24sec	11.20sec	35.44sec
Astya et al. (2014)	C	421ms	342ms	763ms
Gupta et al. (2009)	C++	0.06sec	NA	NA
Zhu et al. (2010)	C	NA	NA	3.3661sec
Our work	HDL Xilinx Spartan 3	16.0401 μs	8.0520 μs	22.0921 μs

Table 7 Entropy values of images

Images	*Entropy*
EarthResize	7.2322
Earthenc	7.2873
Earthdec	7.2322
FlowerResize	7.2218
Flowerenc	7.6347
Flowerdec	7.2218
PandaResize	7.8074
Pandaenc	7.3050
Pandadec	7.8216
PotResize	6.2264
Potenc	7.0926
Potdec	6.2264

5.3 Entropy analysis

Randomness in cipher image designates the proportion of security. A cipher image with high randomness is less vulnerable to the different attacks. To measure the randomness of an image a statistical scalar parameter entropy is used. To show that cipher image has a random texture [8] maximum value is around 8 and it is calculated by equation (8) and the results are shown in Table 7.

$$Emtropy = \sum_{i=0}^{n} P_i \log_2 P_i \tag{8}$$

When choosing the image, the irregular size of the image is resized and given as input for conversion. Plain images with low entropy values are not suitable for this proposed work, as it is observed with an encrypted image of Figure 9.

Figure 9 Images with low entropy values

The experimental result shows that the proposed algorithm can successfully encrypt/decrypt the images with separate secret keys and the algorithm has good encryption effect. Ciphered text and image developed by this method will be entirely different when compared to the original text and image data and will be suitable for the

secured transmission over WSNs. Thus, this model provides an additional level of security to public key algorithm and efficient utilisation of area and memory with reduced computational time. An entropy analysis a common quality measurement to measure the randomness in ciphered image is carried out. Results showed that the proposed method gives better results than steganographic approaches.

This design due to dynamic mapping resistant against brute force and side channel attacks. To our knowledge till date, recent work on FPGA is concentrated only for the data of some static size of bits. In this work we have considered the stream of input data and the work is also extended to encryption of images of different sizes.

6 Conclusions

The different level of security with different sizes of input data and image can be obtained to check suitability for WSNs. The static power utilisation of 0.034 Watts is observed. To evaluate the strength of this algorithm an entropy statistical analysis is performed on plain and encrypted images whose values are found around 8 to indicate randomness in cipher image. Total encryption and decryption time results are around 10.09021 microsecond for 100×100 image, 22.091 microsecond for 256×256 image and 0.029 microsecond for a message. Computational and combination path delay is not observed in any modules designed for implementation. The design gives good throughput with message and it is in terms of Mbps.

The cryptosystem developed exhibits a shield against brute force attacks and thus the cryptosystem primarily focuses on the increased level of security. The proposed architecture achieves a substantial reduction in the area and time that makes it more appropriate for constrained implementations of cryptographic primitives in ultra-low power devices like WSN nodes. Further, this work can be extended with advanced FPGAs that result in less area utilisation and computational time.

References

Akylidiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002) 'Wireless sensor network: a survey on sensor networks', *IEEE Communication Magazine*, Vol. 48, No. 8, pp.102–114.

Amiri, R. and Elkeelany, O. (2013) 'Concurrent reconfigurable architecture for mapping and encrypting a message in elliptic curve cryptography', *Proceedings of the IEEE South Eastcon*, pp.1–6.

Astya, P.N., Singh, B. and Chauhan, D. (2014) 'Image encryption and decryption using elliptic curve cryptography', *International Journal of Advance Research in Science and Engineering*, Vol. 29, No. 10, pp.198–205.

De la Piedra, A., Braeken, A. and Touhafi, A. (2012) 'Sensor systems based on FPGAs and their applications: a survey', *Journal of Sensors*, Vol. 12, pp.12235–12264.

George Amalarethinam, D.J. and Geetha, J.S. (2015) 'Image encryption and decryption in public key cryptography based on MR', *Proceedings of International Conference on Computing and Communications Technologies*, pp.133–138.

Gupta, K. and Silakari, S. (2011) 'Efficient hybrid image cryptosystem using ECC and chaotic map', *International Journal of Computer Applications*, Vol.9, No.3, pp.1–13.

Gupta, K., Silakari, S., Gupta, R. and Khan, S.A. (2009) 'An ethical way for image encryption using ECC', *Proceedings of 1st International Conference on Computational Intelligence, Communication Systems and Networks*, pp.342–345.

King, B. (2009) 'Mapping an arbitrary message to an elliptic curve when defined over GF (2^n)', *International Journal of Network Security*, Vol. 8, No. 2, pp.169–176.

Leelavathi, G., Shaila, K. and Venugopal, K.R. (2017) 'Implementation of ECC on FPGA using scalable architecture with equal data and key for WSN', *International Journal of Engineering and Technology*, Vol. 9, No. 2, pp.773–796.

Leelavathi, G., Shaila, K. and Venugopal, K.R. (2018) 'Implementation of elliptical curve cryptography on FPGA for nodes in wireless sensor networks', *Proceedings of FEAST*, pp.121–125.

Nagaraj, S. and Raju, G.S.V.P. (2015) 'Image security using ECC approach', *Indian Journal of Science and Technology*, Vol. 8, No. 26, pp.1–5.

Nagaraj, S., Raju, G.S.V.P. and Rao, K.K. (2015) 'Image encryption using elliptic curve cryptograhy and matrix', *Proceedings of Science direct Elsevier International Conference on Computer, Communication and Convergence*, pp.276–281.

Rodriguez-Andina, J.J., Moure, M.J. and Valdes, M.D. (2007) 'Features, design tools, and application domains of FPGAs', *IEEE Transactions on Industrial Electronics*, Vol. 54, No. 4, pp.1810–1823.

Shaila, K., Manjula, S.H., Thriveni, J., Venugopal K.R. and Patnaik L.M. (2011) 'Resilience against node capture attack using asymmetric matrices in key predistribution scheme in wireless sensor networks', *International Journal on Computer Science and Engineering*, Vol. 11, No. 3, pp.31–41.

Singh, L.D. and Singh, K.M. (2015) 'Image encryption using elliptic curve cryptography', *Proceedings of 11th International Multi-Conference on Information Processing*, pp.472–481.

Soleymani, A., Nordin, M.J. and Ali, Z.M. (2013) 'Novel public key image encryption based on elliptic curves over prime group field', *Journal of Image and Graphics*, Vol. 1, No.1, pp.43–49.

Woolinger, T., Gujardo, J. and Paar, C. (2003) 'Cryptography on FPGAs: state of the art implementations and attacks', *ACM Special Issue Security and Embedded Systems*, ACM 0164-0925/99/0100-0111, p.40.

Zhu, G., Wang, W., Zhang, X. and Wang, M. (2010) 'Digital image encryption algorithm based on pixels', *IEEE International Conference on Intelligent Computing and Intelligent Systems,* pp.769–772.