Security Analysis of Authentication Protocol for Mobile Devices Using Hyperelliptic Curve Cryptography

Turki Kordy[†] , Prof.Fazal Noor[2††] and Dr.Oussama Benrhouma[3†††]

Islamic University, Computer Science College, Madinah , KSA

Summary
Nowadays, most e-commerce applications are facing issues to secure a proper authentication level. Mobile devices are related to attack the problems in cloud computing, considering that the present authentication. In view of their computational power constraints, key size and memory capacity, RSA public-key cryptography is not suited for these systems. On the contrary, we find Hyperelliptic Curve Cryptosystem (HECC) is considered more suitable for securing communications in mobile and IoT transaction resources like storage, time, or power. This protocol uses Hyperelliptic curve asymmetric cryptography, and the findings show that it exceeds RSA in terms of performance. The experimental work will indicates that the suggested system performance is equivalent with that of RSA. For secure access in limited devices, the security analysis will use a mutual two-factor authentication mechanism for mobile devices based on a hyperelliptic curve digital signature method. Overall, this search tries to suggest a protocol that enables to achieve a considerable level of security.

Key words:
Authentication, ECC, HECC, Privacy, RSA, Security

1. Introduction

Cryptography is a scientific art used for mathematically encrypting and decrypting information for secret communication. It enables the user to safely pass data without damaging the system's stability. Key to the public Cryptography is one of the cryptographic methods consisting of the private and public-key pair of keys. Public key is used for data encryption and private data decryption. The quickest public key cryptography technique with high efficiency and safety is a hyperelliptic curve cryptography [1,2]. The higher genus curve for encryption known as Hyperelliptic Curve Cryptosystem was proposed by Neal Koblitz in 1988. Because HECC has huge security and high-performance features for the applications. Many researchers have been developing to build create the hyperelliptic Curve Cryptosystem and protocol. This function makes HECC among the many encryption systems very common [3]. The major difference in group activities between ECC and HECC is that they consist of separate operating sequences. In addition, the hyperelliptic curve points do not form a group in comparison to the elliptic curve. The divisor class group is the additive group on which cryptographic components are introduced. The reduced divisor is each element of this group. In comparison with ECC's point operation in order to achieve fundamental cryptography, HECC divisor group operations are more complex. It is also difficult to enforce HECC in a constrained environment. A comparatively short encryption key is implemented by Hyperelliptic, making it less processed, which makes it easier for mobile devices. The Hyperelliptic encryption key with 80-bit has the same security as the 256-bit elliptical encryption curve. The lower key sizes and computing needs allow elliptic curve encryption suitable for computer resource and lower processing requirements, such as mobile devices and IoT [4]. In the Internet of Things (IoT) model more objects are connected to the internet every day. This latest connectivity includes IoT technologies in many areas such as healthcare, intelligent housing, transport and agriculture. The low power wide area network (LPWAN) model is currently a specific architecture for IoT networks in order to get ideas of these networks and to deal with other network requirements [5]. Such an IoT devices with lower power wide area called LoRa Wan technology. This technique ensures that the IoT object is fully compatible and can be linked with mobile devices which has no complex implementations necessary .It is a radio frequency layer, has a long range of bands and has special modulation dependent on Chirp spread spectrum (CSS) modulation [5].

LoRaWAN is a low-power network protocol for Internet of Things that enables different LoRa items to be connected to state, national, or international networks by means of batteries. Thanks to the concept of operationality of this system, battery life of sensors can be increased to ten years and in a brief period of time it has become very common in the world. This technology doesn't require a SIM card. The LoRaWAN network coverage enables the development of 868 MHz technology in difficult areas and operating frequencies. Although there is no permitted range, a private network can be deployed without problems. [6] It is not only

Manuscript received October 5, 2021
Manuscript revised October 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.10.12

a matter of selecting the correct protocol for the Internet of Things (IoT), but also of applying good practices and guidelines to the market, and of ensuring it remains safe and stable. Furthermore, in this search, the data are transmitted and retrieved via the LoRaWAN network by using additional encryption layer that would be implemented using hyperelliptic curve cryptosystem to avoid the dealing of data by such an attack. There is a single portal gateway connecting to a central database and mobile device representing the LoRa end node in combination with a computer.

2. Tables, Figures and Equations

2.1 Tables and Figures

Process
Private key :KA ∈ RN ; Random prime number kA is chosen in order of N. **Public key:** PA =KA * D; PA is represented as pair of polynomials as [(u(x), v(x))] and D is Divisor **Shared or agreed key**: QA = KA * PB ; PB is represented as receivers public key. **Ciphertext:** CM ={ QA , Em+PA}; Cm is represented as [(u(x), v(x))].

Table 1: Key generation using Hyperelliptic curve algorithm [27].

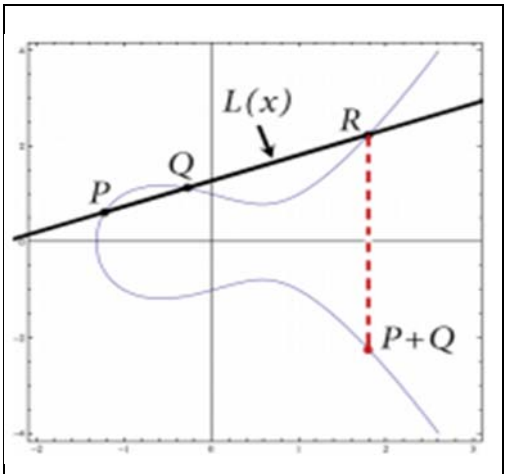

Figure 1: Point Addition on an Elliptic Curve over R [25].

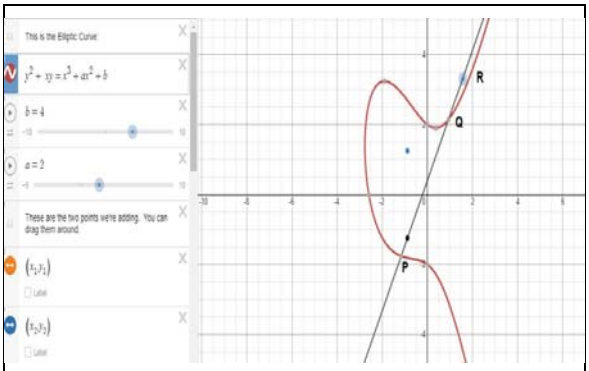

Figure 2: Elliptic Curve points using Demo-online [26].

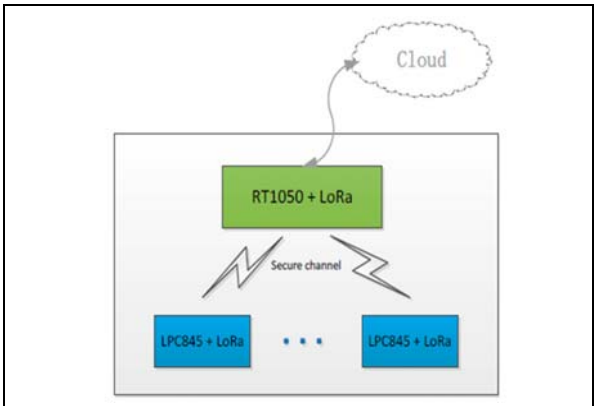

Figure 3: System block diagram. LPC845/i.MXRT1050 is as LoRa controller via SPI interface. [28]

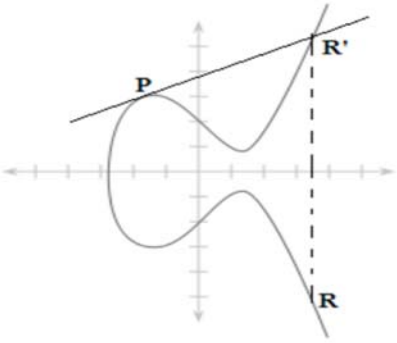

Figure 4.: Point doubling on an Elliptic Curve over R [25].

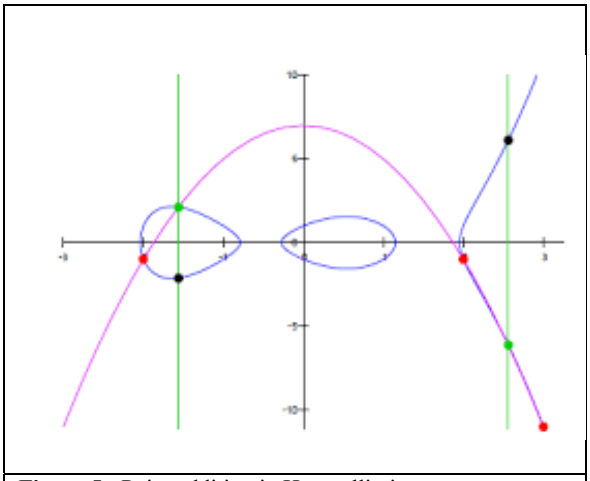

Figure 5.: Point addition in Hyperelliptic curve

2.2 Equations

Given: An elliptic curve $\boldsymbol{E}$: $\boldsymbol{y}2 = \boldsymbol{x}3 + a\boldsymbol{x} + b$.
Input: P, Q ϵ E, where P = $(x1, y1)$ Q = $(x2, y2)$.
Output: P + Q = $(x3, y3)$.
If $\boldsymbol{x}1 \neq \boldsymbol{x}2$ then // we can compute the slope m directly

$$\boldsymbol{m} = \frac{\boldsymbol{y2} - \boldsymbol{y1}}{\boldsymbol{x2} - \boldsymbol{x1}}$$

$x3 = m2 \_ (x1 + x2)$
$y3 = m (x1 - x2) - y1$
Return $(x3, y3)$
else if $x1 = x2$ then
if $y1 \neq y2$ then // the line through P and Q is vertical
return ∞
else if $y1 = y2$ then // P: Q
if $\boldsymbol{y}1 \neq 0$ then // we compute the line tangent at P

$$m = \frac{3x\ 1/2 + a}{2y1}$$

X3 = m2 _ 2x1
y3 = m (x1 – x3)- y1
return (x3, y3)
else if $\mathbf{y}1 = 0$ then // the line tangent to P is vertical
return ∞

An algorithm to compute the group law for elliptic curves (24)

Algorithm 1: Common Case for Group Addition (g=2)	
Require:	Include two divisor, where D_1= div (u_1, v_1) , D_2= div (u_2, v_2)
Ensure:	D_3= div (u_3, v_3) = D_1 + D_2
	1: k = f - v_1h-v^2_1 / u_1 **(exact division)**
	2. S ≡ $\frac{v2-v1}{u1}$ mode u_2
	3. z = su_1
	4. u '= $\frac{k-s\,(z+\,h+2v1)}{u2}$ **(exact division)**
	5. u_3 = u ' made monic
	6.v_3 ≡ - (h + z + v_1) mod u_3

Algorithm 1 all stages when two divisors are added [29].

Algorithm 2: other known Case for Group Doubling (g=2)	
Require:	D_1= div (u_1, v_1)
Ensure:	D_2= div (u_2, v_2) = 2D_1
	1: k = v^2_1-v_1 h – f / u_1 **(exact division)**
	2. S ≡ $\frac{k}{h+2v1}$
	3. u ' = s + $\frac{k-s\,(h+2v1)}{u1}$ **(exact division)**
	4. u_2 = u ' made monic
	5. v_2 ≡ - (h + su_1 + v_1) mod u_2

Algorithm 2 all stages when two divisors are doubled [29].

3.1 Problem Definition.

Now is the era of Internet of Things IoT, and it is believed that one in four devices will be connected to the internet by the year 2025. With billions of devices connected to the internet, security is often overlooked by the manufacturers and designers of these devices. One of the promising technologies is the LoRaWan. The figure below shows the general layout, of the LPWAN sensors, gateways, network servers, and the application servers. What is necessary is to have an end to end secured communications [7].

The current offerings of LORA devices security are based on several encryption algorithms such as RSA, AES, and ECC. This thesis main contribution is the proposal of usage of security based on hyperelliptic curve cryptography. The study looks at the current ECC cryptography and the proposal of HECC. There are several contributions offered by the HECC proposal. One is the shorter key size compared to ECC and the legacy methods. We study the feasibility of HECC in such applications. We also propose the hybrid cryptosystem based on HECC. It is not only a matter of selecting the correct protocol to ensure Internet of Things (IoT) rollout and to keep this stable and secure, but also of using the application mechanism and best practices and guidelines for industry. In reality, authentication and encryption are mandatory—but networks and computers can be compromised if security keys are not safe, randomized between devices, or if once used cryptographic numbers (nonces), as seen in several blog posts, LoRaWAN is designed quite securely. Therefore, it is important to search for LoRaWAN Certified CM instruments to ensure that the equipment is validated and operates according to the specification [7].

3.2 Contributions

The main significance of secure connection is realized by serval users, but the main purpose based on the security of gateway or IP devices to Internet. However, the gap analysis is to secure the interfaces between gateway and end devices. It has been implemented of security in such devices like wireless protocols and Bluetooth or ZigBee, but it is quite difficult to repeat to other platforms. This application demonstrates how to establish IoT secure channel to LoRa WAN between gateway and end devices using hyperelliptic curve cryptosystem. Moreover, it has been developed MatLab software for two implemented algorithms include ECC and HECC. It has been illustrated the study performance analysis of finding time of file size and time taken before and after encryption or decryption between the two mentioned algorithms.

3.3 Significance of the Study

Due to the use of network connectivity in daily life, our privacy is apparent. Therefore, the protection of communication through IoT devices is one field of great need for study. IoT devices such as e-commerce and multiple sectors can be used in many ways. The real issue is figuring out how to secure these high-tech devices efficiently. For example, cryptography was used only for military purposes. But now it is used more to ensure transactions online, ATM, and card safe status, depending on encryption.

The importance of this study lies in the fact that the proposed model based on IoT Device secure connection with LoRa from tampering with the data that is between gateway and end devices. The data used in communication is highly sensitive and must be secured from intruders. The technique of the study presents secure transmission of a message through sensor nodes and complete basic security criteria of secrecy using a hyperelliptic curve cryptosystem that can be suitable for almost any IoT deceived in the constrained environment.

3.4 LoRa WAN

LoRa (long range short) is modulation to get information form air through large range using very little power. LoRa packet on the small device to the could or server, the device could be forwarded as listening to the packet and send them to the could. It is a revolutionary mechanism for the modulation of spectrum from current technologies Chirp Spread Spectrum (CSS). It has an It Sensitivity offset versus data rate by using either 125Khz or 500Khz bandwidth channels for uplink and 500Khz bandwidth downlink channels. Operating in a fixed channel of 125Khz or 500Khz, it provides a compensation of sensitivity versus data rates when working on uplink channels and 500Khz on downlink channels. Low data rate, low capacity, low-cost and long-range sensor applications in various vertical markets, LoRaWAN is an excellent internet of objects protocol (IoT) for various applications. Today, millions of LoRaWAN terminal nodes are linked with thousands of gateways worldwide [8].

3.4.1 Network Architecture

The modulation of LoRa is carried out by commercial and medical radio (ISM) team. LoRaWAN has three significant components include network servers, end devices and gateways. It is used as a star topology and as a gateway for transmitting messages between network servers and end devices. Both Gateways linked by normal IP technology to the central network server while the LoRa single-hop connectivity is used for one or more

gateway end-devices. The connectivity between terminals and gateways can be modulated by Frequency-shit keying (FSK) or LoRa through different data rates and channels [8].
The most important management roles in network server NS (LoRa Alliance, 2018) are:
• NS controls and manages all communication requests from sensors, NS advises any sensor on which channel it operates and which SF factor it uses and which power level for transmission is needed.
• The most optimal base station for the sensor connection and messages is described by the network server.
• The network server has general administration tasks, the reporting of base stations and the control of sensors. [8]

3.5 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is an advanced, publicly available cryptography scheme that focuses on the algebraic structure of elliptical curves through endless fields and complexities of a discrete elliptical curve problem (ECDLP). ECC integrates all the potentials of the key asymmetric cryptosystems such as cryptography, key Exchange and signatures. ECC cryptography, as it utilizes smaller key and signature than that of RSA for the same level of security, is recognized as a natural contemporary alternative to the RSA cryptography system. For instance, the ECC key 256-bit is the same as the RSA key 3072-bit. [9].

3.6 Literature Reviews

Mukhopadhyay et al proposed a plan for securing the data clouds by implementing the key agreement, encryption, and signature verification with HECC. This provides less storage, less power, and bandwidth than other alternative cryptosystems because it creates very small key sizes for encryption and decryption compare with ECC. However, the HECC has not been implemented much in IoT devices. The research shows that the existing authentication protocols using RSA public key cryptography are not suitable for such devices regarding with their limitation of its key sizes, memory capacity and computing power [10].
Chou & Washington performed and observed the aim of the mobile devices requirements to board the restriction on power and bandwidth and to comprehend an appropriate level of security. The ECC security resulting from the elliptic curve logarithm which is that the Discrete logarithm problem in group labelled by points on an elliptic curve over a limited filed. The results during a rapid reduce in key size needed to produce the identical level of security. It also states that the current authentication protocols, supported RSA asymmetric cryptography do not seem to be appropriate for such devices because of their boundaries in computing power, memory capacity, key sizes and cryptographic support. For that reason, a useful protocol for resource-controlled platforms that achieve grade of security the same as the one accomplished by the protocols in use today is meant and applied. Elliptic curve asymmetric cryptography and therefore the results show that the presentation achieved is wonderful in contrast to RSA. There are more advantages of ECC compared to RSA for reducing processing that it can be offered a smaller key size with the same level of security based on mutual authenticated key agreement protocol. This enhances the security of user authentication and key exchange. However, for the curve HECC work over a finite field on 40 bits to 80 bits in order to compute the group operations. Thus, using hyperelliptic curve would increase the security level over ECC [11].
Arthur M [12] has proved that in comparison with Elliptic Curve, HECC on prime field is adequate enough, particularly when large groups of points are required. Fan and Gong [13] also proved that HECC delivers greater performance, in terms of numerical overheads and key sizes than either integer factorization systems or distinct logarithm systems. And bandwidth Deng Jian—zhi [14] illustrate that HECC based Digital Signature architecture that solves the issue by verifying the file integrity and signature ID and it particularly suitable for internet operations that require identification validation. It also provides the HEC-DSA Hardware Module and validates it with the Quartus II 6.0 simulator. S.Baktir [15] launches implementation of the HECC region on an embedded processor with the odd feature field and proves to be a movement of about 57 % compared to other cryptographic algorithms the implementation of genus 2 HECC over GF (281) on 32-bit ARM7DMI processors Furthermore, the application implemented for compilation and debugging of field multiplication fields reversals and community additions and doubling is supported by the use of Microsoft's VisualC++ compilers 6.0 and Developer Studio 6. Prasanna Ganesan highlights Hyperelliptic Curve Cryptography is used by mobile devices with a limited capacity. For both RSA and HECC accuracy measurements are made using the 2.5.1 wireless toolkit PALMIII and J2ME. It is also recommended to reach the high level of security using Hyper Elliptic Cryptography based on ElGamal and MD5 authentication algorithm [16]. Michael Jacobson [17] observes that Jacobian hyperelliptic curve defines discrete cryptographic logarithm protocols over a finite field. It proposed the Weil Descent technique for solving discrete logarithmic hyperelliptic curve problems (HCDLP). The index calculus attacks on HCDLP and the descent attack on the ECDLP are both

defined in detail. Alexander Klimm designed the Crypto Processor to authenticate access regulation for automobiles. It also develops the automobiles access control system's hardware and software interface [18]. Kahlil Chatterjee [19] examines aspects of major operations such as scalar multiplication. Group Operations of Jacobian and Finite Field Operations has an impact on effective ECC/HECC implementation. It also contrasts the timescale of operations such as scalar multiplication for ECC and HECC Cryptosystem. The results on the Intel Core 2DUO CPU PC were tested by HECC T6400@2.00GHz with 4GB RAM and by the Windows View Operating System using jdk1.6.

The performance has been provided in comparison of ECC and HECC. indeed, both cryptosystem software has implemented for restricted devices, such as smart card and mobile devices. Analytics of Wollinger Explicit Formula for the addition and doubling operations for hyperelliptic curve cryptosystems, conducted using the Cantor algorithm and Harley [20]. Xuanwn Zhou proves that ring signature solves efficiently and significantly increases the performance of signature generation and verification in group Cryptosystems. It also demonstrates improvement of the ring signatures, thereby improving the safety, stability and performance of the Software Engineering [21].

3.7 Experimental result and discussion

The proposed protocol has implemented HEC (genus 2) on different prime fields. It demonstrates that two ECC and HECC logarithms on different prime filed using MatLab. The components of sectional operation have been measured on a PC with Intel Core AMD Ryzen 7 with 2.90 GHz with installed RAM 16.0 GB and Windows 10 Home operating system.

The tables and diagrams below shows the comparison between RSA and ECC in terms of Security performance during the encryption and decryption process. Finally, it sum up with new implementation method using hyperelliptic curve and how this cryptography has more efficiency impact on security.

This table shows a difference in file text size between the original file (plain text file) called the test file and the encrypted text in bytes. It shows that the file size has increased after encrypting the plaintext. Other elements are related to the time taken during the encryption and decryption process. The diagrams show below will illustrate this in more detail.

Input value	1st	2nd	3rd	4th	5th	6th
Test Character	128	192	256	512	740	868
Plain text size in bytes	802	1185	1656	3150	4561	5394
Encrypted text size in byte	23259	34366	47909	91235	132154	156311
Time Encryption in milli second	302.162 7	398.8987	555.5376	1148.2	1529.3	1923.6
Time Decryption in milli second	0.2707	0.3264	0.227	0.0885	0.13	0.0826

Table 2: The comparison of files based on file size and consumption time applied by ECC.

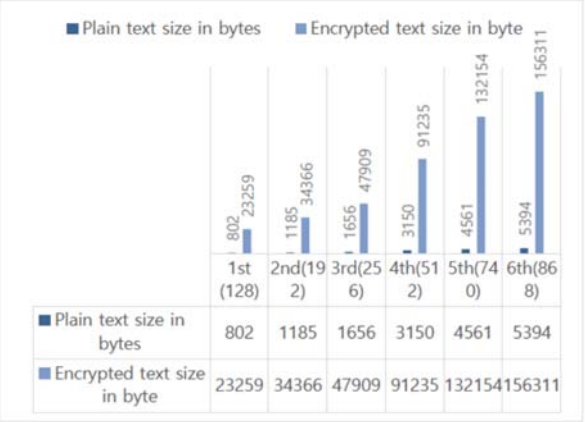

Figure 6: Comparative analysis of file size before and after Encryption process.

This diagram shows that the first input value 1 of 128 characters has 802 bytes before encryption in the original plaintext. By applying ECC's encryption process, this file has expanded to 23259 bytes, that a file size of 23,259 Kb after the encryption process. So, as the number of characters in the file increases, more file size is required for encryption.

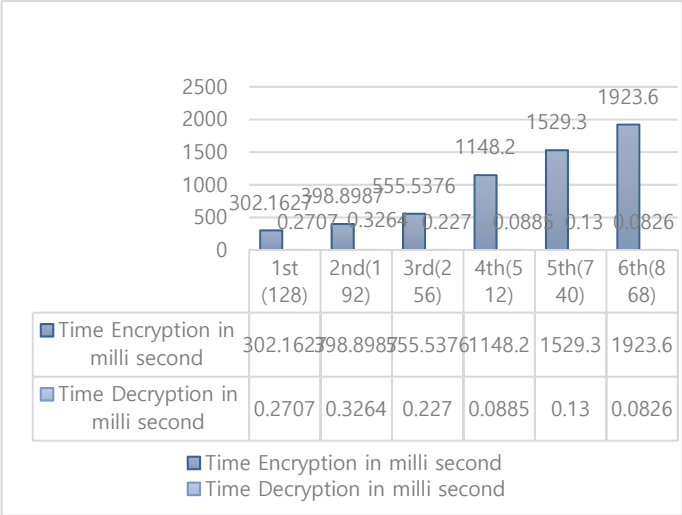

Figure 7: A Comparative analysis of execution time of Encryption and Decryption.

This diagram shows the time required by the two cryptosystems. The encryption process takes more time than the decryption process. For example, 128 characters take 302.1627 milliseconds, which is 0.3021627 seconds during encryption. However, less time is required during decryption, 0.2707 milliseconds, which is equivalent to 0.0002707 seconds.

Key length (bit)		Computational time	
ECC	RSA	ECC	RSA
163	1024	1.147	0.063
233	2240	1.265	0.031
283	3072	1.395	0.031
409	7680	1.375	0.031
571	15360	1.265	0.015

Table 3: 1 Running time for Encryption [22].

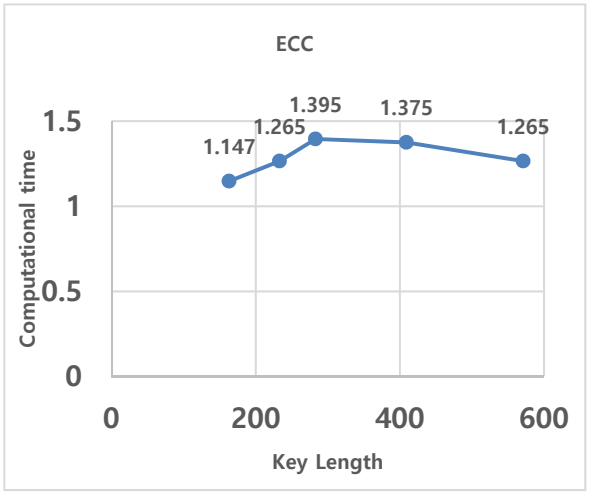

Figure 8: The key length and computational time of ECC after Encryption [22].

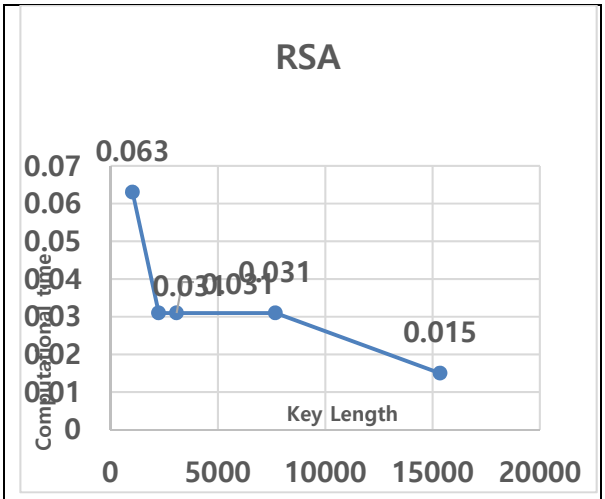

Figure 9: The key length and computational time of RSA after Encryption [22].

The table shows that RSA encryption is faster than ECC encryption. But there's not such a huge disparity between the two computational timings. From the point of view of encryption, we may thus assume that the two

methods are performing the same, but the RSA algorithm is superior.

We must obtain finite groups from their Jacobians for the usage of the hyperelliptic curve g ≥2 in cryptography applications. For an elliptic curve which was specified by a finite Fq, the curve may be limited to a collection of points with Fq coords.

The crypto-system of the hyperelliptic curve is the crypto-system of the elliptical curve. The ECC technique includes the definition of the defined members of the group. An operation on two elements in the set will lead to the group itself being an element. The time needed to encrypt, and decrypt is increased in the ECC as the timestamp (t) is increased whereas in the HECC the timestamp is lowered by encrypting and decrypting

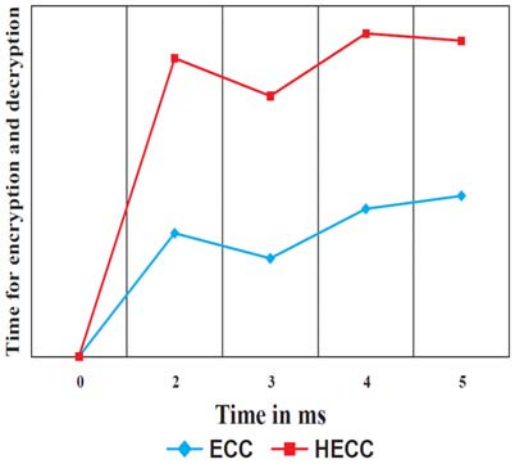

Figure 1 : Comparison of HECC and ECC in terms of Encryption and Decryption time [23].

The performance study between ECC and HECC reveals that the HECC system performs more efficiently. Figure 4.11 illustrates the time required for the x axis to be encrypted and decrypted, and the key size of the y-axis cryptosystem. The 160-bit ECC system takes time to encrypt and decrypt compared to the HECC cryptography. For cryptographic processing, the HECC cryptography simply requires 80-bit size. Here, when the key size is reduced, the necessary encrypting and decryption time is less than ECC. It is therefore obvious that the key size is directly related to the time required for encryption and decryption and the lower-key size HECC cryptography provide secure cloud resource processing. The HECC method also costs less since the key size is small. This algorithm is robust to several kinds of attackers. It takes less time at operating stages and is ideal for an efficient and scalable cloud environment. It specifies a minimum key size for the security offered by the ECC system.

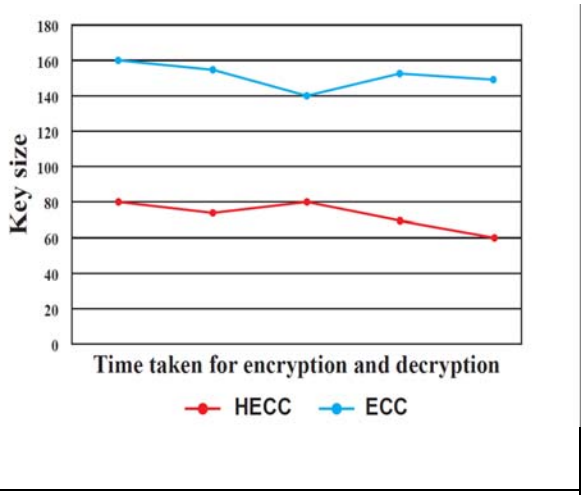

Figure 2: Comparison of HECC and ECC in terms of Key size [23].

3.6 Conclusion

To sum up everything that has been stated so far, could computing is jeopardizing many challenges related with the efficient security.

Technology via gateway networks for the end-node covering all areas. This application LoRaWAN defines how secure connections between devices should be established. NXP MCU clients have access to an IoT secure library. For this item, it should be utilized a comparable safe connection using a proposed hyperelliptic curve scheme. This research also advised that the data provided across the network should be processed more reliably. It happens by adding an efficient encryption using hyperelliptic curves that offered more dependability and secure that network.

During this investigation, it was discovered that ECC outperformed the RSA algorithm based on execution time, speed, scalability, flexibility, reliability, security and limitation, all of which are important for secure communication. Although the RSA algorithms were competent, they took longer than ECC and had a trade-off between memory use and encryption speed. In contrast, the hyperelliptic curve has the best performance in terms of security and efficient compare with others that has been shown in the proposed result to reduce the complexity for securing the LoRa Wan linked with mobile device.

3.7 Future Work

It has been applied a highly performance such as encryption and decryption time and key generation. Such LoRa WAN device that has been implemented by using hyperelliptic curve to secure the communication to mobile device. This work has contributed on the expansion and widespread approval of such other IoT devices.
We may work on the hardware implementation of Hyper Elliptic Curve Cryptosystems in the future, including key exchange and digital signature. This thesis is entirely based on Affine Space calculations. We may subsequently build an explicit formula in projective space that eliminates the inversion step. Radio Frequency and Bluetooth devices are examples of IoT devices that would be deployed using the same suggested architecture.

Acknowledgments

I would like to thank My Faculty Computer Science and Information Systems Islamic University for providing the resources to help carry out my research work.
Without the advice of my committee members, the assistance of friends, and the support of my family, I would not have been able to complete my dissertation. I would like to thank my adviser from the bottom of my heart to my advisor, Professor Dr. Fazal Noor, for his excellent guidance, caring, patience, and providing me with an excellent atmosphere for doing research, his guidance helped me in all the time of research and writing of this thesis.

References

[1] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions onInformationTheory*, *22*(6),644-654.

[2] Stallings, W. (2006). *Cryptography and network security, 4/E*. Pearson Education India.

[3] Koblitz, N. (1988, August). A family of jacobians suitable for discrete log cryptosystems. In *Conference on the Theory and Application of Cryptography* (pp. 94-99). Springer, New York, NY.

[4] Mukhopadhyay, D., Thakur, A., Chaudhari, N., & Nanekar, S. (2015). Architecture to Implement Secure Cloud Computing with Elliptic Curve Cryptography. *SmartCR*, *5*(3), 201-208.

[5] Petajajarvi, J., Mikhaylov, K., Roivainen, A., Hanninen, T., & Pettissalo, M. (2015, December). On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology. In *2015 14th international conference on its telecommunications (itst)* (pp. 55-59). IEEE.

[6] Workgroup, T. M. (2015). A technical overview of LoRa and LoRaWAN. *no. November*. Retrieved from https://www.tuv.com/content-media-files/master-content/services/products/1555-tuv-rheinland-lora-alliance-certification/tuv-rheinland-lora-alliance-certification-overview-lora-and-lorawan-en.pdf.

[7] Alliance, L. (2015). What Is LoRa. A technical overview of LoRa and LoRaWAN, 5-17.*Retrieved from* https://lora-alliance.org/resource_hub/lorawan-is-secure-but-implementation-matters/.

[8] *Migrating an Internet of Things (IoT) Sensor Design to LoRaWAN*. (2018). LoRa Alliance. Semtech Corporation, Camarillo, CA. Available at :https://www.semiconductorstore.com/pdf/Migrating-Sensor-Design-LoRaWAN-WhitePaper_FINAL.pdf (Accessed:05/2018).

[9] Nakov, S. (2018). Elliptic Curve Cryptography (ECC). *Practical Cryptography for Developers .Retrieved from* https://cryptobook.nakov.com/asymmetric-key-ciphers/elliptic-curve-cryptography-ecc.

[10] Mukhopadhyay, D., Thakur, A., Chaudhari, N., & Nanekar, S. (2015). Architecture to Implement Secure Cloud Computing with Elliptic Curve Cryptography. *SmartCR*, *5*(3), 201-208.

[11] Chou, W., & Washington, D. L. (2003). Elliptic curve cryptography and its applications to mobile devices. *University of Maryland, College Park, USA*.

[12] Avanzi, R. M. (2004, August). Aspects of hyperelliptic curves over large prime fields in software implementations. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 148-162). Springer, Berlin, Heidelberg.

[13] Fan, X., & Gong, G. (2007, August). Efficient explicit formulae for genus 2 hyperelliptic curves over prime fields and their implementations. In *International Workshop on Selected Areas in Cryptography* (pp. 155-172). Springer, Berlin, Heidelberg.

[14] Jian-zhi, D., Xiao-hui, C., & Qiong, G. (2009, July). Design of hyper elliptic curve digital signature. In *2009 International Conference on Information Technology and Computer Science* (Vol. 2, pp. 45-47). IEEE.

[15] Baktir, S., Pelzl, J., Wollinger, T., Sunar, B., & Paar, C. (2004, November). Optimal tower fields for hyperelliptic curve cryptosystems. In *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.* (Vol. 1, pp. 522-526). IEEE.

[16] Ganesan, S. P. (2010). An authentication protocol for mobile devices using hyperelliptic curve cryptography. *International J. of Recent Trends in Engineering and Technology*, *3*(2), 2-4.

[17] Jacobson Jr, M. J., Menezes, A. J., & Stein, A. (2004). Hyperelliptic curves and cryptography. *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, *41*, 255-282.

[18] Klimm, A., Haas, M., Sander, O., & Becker, J. (2010, September). A flexible integrated cryptoprocessor for authentication protocols based on hyperelliptic curve cryptography. In *2010 International Symposium on System on Chip* (pp. 35-42). IEEE.

[19] Chatterjee, K., De, A., & Gupta, D. (2011). Software Implementation of Curve based Cryptography for Constrained Devices. *International Journal of Computer Applications*, *24*(5), 18-23.

[20] Wollinger, T., Pelzl, J., & Paar, C. (2005). Cantor versus Harley: optimization and analysis of explicit formulae for hyperelliptic curve cryptosystems. *IEEE Transactions on Computers*, *54*(7), 861-872.

[21] Zhou, X. (2009, December). Improved ring signature scheme based on hyper-elliptic curves. In *2009 Second International Conference on Future Information Technology and Management Engineering* (pp. 373-376). IEEE.

[22] Saho, N. J. G., & Ezin, E. C. (2020, October). Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm. In *CARI 2020-Colloque Africain sur la Recherche en Informatique et en Mathématiques Apliquées*.

[23] Nagendran, K., Nadesan, T., Chandrika, P., & Chethana, R. (2018). Hyper Elliptic Curve Cryptography (HECC) to ensure data security in the cloud. *International Journal of Engineering & Technology*, *7*(4.19), 186-188.

[24] Wilcox, N. (2018). *A Computational Introduction to Elliptic and Hyperelliptic Curve Cryptography* (Doctoral dissertation, Oberlin College).

[25] Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., & Vercauteren, F. (Eds.). (2005). *Handbook of elliptic and hyperelliptic curve cryptography*. CRC press.

[26]Graphing calculator. (n.d.) *Elliptic curve point*. Retrieved from https://www.desmos.com/calculator/ialhd71we3.

[27] Vijayakumar, P., Vijayalakshmi, V., & Zayaraz, G. (2014). Comparative study of hyperelliptic curve cryptosystem over prime field and its survey. *International Journal of Hybrid Information Technology*, *7*(1), 137-146.

[28] NXP Semiconductors.(2018). *IoT Device Secure Connection with LoRa,* Application Note, Rev. 0. Available at: https://www.nxp.com/docs/en/nxp/application-notes/AN12257.pdf (Accessed:09/2018).

[29] Pelzl, J., Wollinger, T., & Paar, C. (2004). Special hyperelliptic curve cryptosystems of genus two: Efficient arithmetic and fast implementation. *Embedded Cryptographic Hardware: Design and Security*.