International Journal of Advanced Technology and Engineering Exploration, Vol 7(62)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2019.650070

Research Article

Smart home IoT use case with elliptic curve based digital signature: an evaluation on security and performance analysis

Azrin Zahan[1], Md. Selim Hossain[2*], Ziaur Rahman[3] and SK. A. Shezan[4]
Department of Information and Communication Technology (ICT) at Mawlana Bhashani Science and Technology University (MBSTU) Santosh, Tangail, Bangladesh[1]
Lecturer, Department of Computer Science and Engineering at Khwaja Yunus Ali University, Enayetpur, Sirajganj, Bangladesh[2]
Assistant Professor, Department of Information and Communication Technology (ICT) at Mawlana Bhashani Science and Technology University (MBSTU) Santosh, Tangail, Bangladesh[3]
Department of Electrical and Electronic Engineering, School of Engineering, RMIT University, Melbourne, Australia[4]

Received: 28-November-2019; Revised: 15-Januray-2020; Accepted: 17-January-2020

Abstract
This paper concerns the lightweight cryptography, elliptic curve cryptography on the Internet of Thing (IoT). Most of the system depends on the internet, so it is IoT that is an excellent evolution of technology. Smart home, city, university are some familiar examples of the Internet of Things. It is a great challenge to modernize our world into the smart world from the security perspective. For instance, at the smart home door system, an unauthorized person can easily break the security that means opening the door after trying the password several times. Some security schemes have been proposed to enhance IoT security issues after adopting the public key infrastructure (PKI) system that is either not secure or has complexity. The lightweight nature of the IoT devices often demands different security approaches apart from existing web security that motivates us to enhance IoT security upon different primitive such as elliptic curve cryptography (ECC). Here, we propose sample IoT scenarios to incorporate ECC instead of an existing technique as it has the thin nature in key size, and at the same size of the key ECC show more strength than RSA-driven technique. We evaluate our proposed system based on a smart-door IoT system using a simulation tool, namely Cryptool 2. The contribution of this work is to show how ECC performs better than the Rivest–Shamir–Adleman (RSA) based approach in the considered IoT use-case.

Keywords
Internet of thing, Elliptic curve cryptography, Security, Smart home.

1.Introduction
The Internet of Things (IoT) is being evolved through four-dimensional or pillars such as individuals, procedures, information and possessions named the Internet of Everything (IoE). It seems IoT has only one component, which is things. We partake to explain in IoE, about the connection of the things and people, collection of the technique. However, the harmless data and intelligent connection of objects and constitutional items work on the internet for the decision as shown in *Figure 1*. All components are discussed in the later section. The IoT now has a more significant opportunity for a career, business, and economy.

Security, network completion, and energy costs are essential thoughts on the internet of everything [1].

It provides a secure scheme to support many devices of context-awareness. Machine to machine (M2M) infrastructures, machine to people (M2P) system, and people to people (P2P) connections comprise IoE technology, which will be used wireless communication and networking [2,3]. A collaborating platform that assimilates evidence as of exposed government agendas, local businesses and citizens to deliver evocative and authoritative knowledge anytime, anywhere on any expedient. It also includes user-generated and global communications.

*Author for correspondence

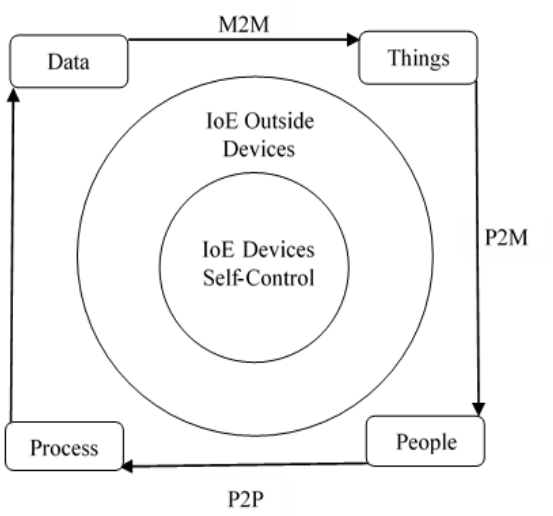

Figure 1 Components of internet of everything with four pillars as IoT evolved as per the technological advancement

The objective of this work is outlined as below-

- Proposing ECC digital signature with IoT based for increasing the security of IoT system.
- Applying the IoT scenarios to integrate ECC instead of an existing technique as it has the thin nature in key size, and at the same size of key ECC shows more strength than RSA-driven technique.
- Evaluating the proposed system in comparison of that ECC performs better than the RSA based approach in the considered IoT use-case.

So far, the article is prepared with the following structures-including background, proposed method and materials, evaluation, result discussion, imitations that concluded with a conclusion and future scope section.

2.Background

We proposed a secured smart door system using Elliptic ECC. Following a similar way, it is demanded to implement a complete smart-home system further to keep the system safe against hackers. So, the opponent hackers cannot access our personal information or cannot get the password to access the house where the proposed door works. Through the background study, we have learned that RSA keys are large (e.g., 1024 or 2048 bits long). Therefore, applying RSA digital signature (RSADSA) for small IoT use-case brings higher complexity and costs. At the same time, processing requires excessive power. Elliptic curve cryptography-based signature (ECCDSA) is a decisive communal cryptosystem [4] for example RSA, Rabin, and El Gamal [5]. Still, unlike its counterparts, it could be an efficient technique for its key-size and light-weight nature and processing. For lower-key length, it requires lower computation and saves memory space. ECC needs 160 bits key while RSA demands 1024-bit key aimed at the similar security [6]. Apart from IoT, it has the potentials to be applied trendy the field of wireless system, less amount of power needed strategies like as mobile communication, etc.

It is given by a NIST ECC specification that shows ECC's special characteristics. For example, near defend 128-bit AES key, RSA key size: 3072 bits and Size of ECC key: 256 bits [7]. Numerous announcement safeties structures, whichever ECC-based or non ECC-based, have been wished-for in works to explain safety and confidentiality matters in RFID structures. In this segment, it has been planned some of the current ECC-based safekeeping systems for RFID structures since the authentication scheme also depends on ECC. ECC-based shared authentication structure that gratifies the security necessities in an RFID transplant arrangement. ECC is a scalar growing which includes point addition and replication process [8]. ECC has been presented as a substitute to the selected approaches like the DSA to eradicate the difficulties of key size, redundancy, and low speed. ECC as the algebraic-curve-based arrangement usages elliptical curve points over a restricted arena [9]. It also has been resolute that ECC is quicker than RSA in making a digital signature, but sluggish in digital signature confirmation. Consequently, RSA can be the finest choice for requests challenging confirmation of messages more regularly than the signature cohort [8]. The usage of ECC delivers substantial development in terms of calculating power and key proportions. This fact confirms the applicability of the scheme in handheld devices such as smart cards, personal digital support, IoT devices. ECC [10] brand practice elliptic curves in which variables and coefficients are constrained. There are two families of elliptic curve (prime field Fp and Galois field $2m$.) used widely in cryptography. ECC usages the curve equation.

$$y3 = x2 + ax + b$$

Where a and b are the constants with discriminant function and Elliptic curves are measured by cubic equations alike to those cast-offs for calculating the boundary of an ellipse [11].

From *Table 1* it has been seen that ECC with lesser key size Centrals to obvious cost investments. ECC with lesser key size also eases the design of quicker cryptographic operations that route on small chips with tiny memory [9]. This is suitable for resource-constrained schemes since it decreases the power consumption and heat production. As a result, ECC is well appropriate for smart devices that function in reserve constraint situations. ECC develops a more real-world system of practice. And as security requirements become more demanding, and processors become more powerful, significantly more modest increases in key length are essential and saves ECC applications lesser and more well-organized than other implementations. ECC can use a significantly shorter key and bid the same level of safety as other asymmetric algorithms using much greater ones [12].

Table 2 describes that ECC-160-point development is additional well-organized than the RSA-1024 private-key process [13] measure the danger of practice of a key on the foundation of the key distance of RSA and ECC. They accomplished that cashbox 2014, use of 1024-bit RSA delivers some small danger though 160-bit ECC over the main field. It may securely be rummage-sale for a much lengthier dated decided RSA is quicker than ECC. But safety, intelligent ECC outstrips RSA [14] associate the procedures of digital signatures in RSA and ECC. Then proposed, RSA may be a respectable excellent for the requests, where confirmation of communication is obligatory more than a generation of the signature [15]. It is recommended that presently, RSA is tougher than ECC even though they also designated ECC outclasses than RSA in future [16] that ECC outdoes concerning working efficiency and security over RSA.

Table 1 Public key size for ECC and RSA and respective ratio according to NIST

Key Size of ECC (Bits)	Key Size of RSA (Bits)	Ratio of Key Size
160	1024	1:6
224	2048	1:12
256	3072	1:20
512	15360	1:30

Table 2 Comparison amid ECC and RSA with reverence toward different key issues

Key point	ECC	RSA
Key sizes	Shorter pair of keys for the ECC	Larger pair of keys for the RSA
Bandwidth	The bandwidth of ECC is significant.	The bandwidth of RSA is considerably less than ECC.
Key Generation	Quicker	Comparable slower
Encryption	Quicker	It is Slower
Decryption	Slower than RSA	It is Faster than ECC
Efficiency	It is more competent for insignificant devices.	It is less competent than ECC

3.Internet of things

The IoT that remains a subset of the IoE. It controls devices directly that are outside the organizations. It is useful for presenting data of the organization, and stop them from passing data across the administration's network where difficulty exists. There are four apparatus of IoT which is people, process, data, and thing. It is discussed in the IoE. The uncertainty we imprecate at, respectively, of these dimensions, and their working procedure, the value of your which tends to transform will be seen that there are some special purposes for connecting the flows of information from one entity to another. People, Equipment, submissions, and network entities can be P2P, M2P or M2M [17]. The next one is that the main business variables are charged car driver consist of invention, operative production; asset consumption, client knowledge, and amount restraint that determine the ability to gain the benefit for an IOE based investment and M2M networks. IoT/Sensors (e.g. Remote monitoring). Another important thing is P2P that means people to people contacts. Association (e.g. Video/TP) with M2P networks.

People: To cooperate with separately other people need devices, like mobiles, for social networking, such as Facebook and LinkedIn, Tablets and PCs are used. IoT will remain in the communication of the characters on the Internet. For instance, for receiving and sending data, sensors may be used happening our skin or clothes to healthcare-providers [18].

Process: Developing expertise, marketing, administrative, and supplementary methods that resolve to maintain and trendy no small amount, systematize the critical mass in connections and the consequent collection, investigation, and dissemination of data that resolve unavoidable in the IoT. Processes also play an essential part how each of these objects such as people, data, as well as things interconnect through each added within the smart system toward social reimbursements and financial cost.

Things: Things are numerous mechanical devices such as sensors or meters etc. It is linked to any object and capable of distributing information. The things drive additional information, which helps make decisions for characters and parties. In IoT it helps to adapt traffic conditions by intelligent shipping systems. They are delivering energy consumption, automating factory floor operations by robots.

Data: Generating data from any sources such as smart camera where sensors are developing day by day. Novel categories of plans create more data that not ever occurred before. For illustration, sensors are used in everyday life in developed countries like temperature sensors, motion sensors. It is helped by analysing big data to sense of this slide of information, recognizing and merging appropriate information features popular conducts that divulge new understandings and permit better choice creation.

4.Proposed method: considered smart home IoT use case

We simulate a sample IoT use-case scenario-based Packet-tracer and Crypto-tool. Its second version is one of the latest successors of CrypTool 1, which has a popular e-learning program for cryptography and cryptanalysis. The modern technique presents a graphical user interface for coding. So, the working process canister be envisioned as well as managed to permit automatic operation and contact of cryptographic methods. CrypTool 2 supports Microsoft office operator boundary design standard, as long as reliable and rich manipulator knowledge. However, at first, we implement of the considered smart home use-case scenario. For this implementation, we need some requirements such as ceiling fan, window, gateway, smart home, etc. in our living room. We are a success to control the speed of ceiling fan and window by Smartphone, as shown in *Figure 2*.

In *Figure 2*, the fan is in off mode, and the window is closed. After configuring devices, when we click the large button to monitor the speed of the ceiling, fan will be increased. When we click off switch, it turns on static mode. We can also open or close the window by click. This process is exposed in *Figure 3*, and the outcome of this process is revealed in *Figure 4*. In *Figure 3*, we see the IoE monitor for changing state. We experience clicking high mode in Ceiling fan status bar and on the mode in window status bar. Then the fan starts to move fast, and the window turns to open state. In *Figure 4*, we see that the fan is running, and the window is open. It is possible by the IoE technique. Here we use the Cisco simulation tool for our purpose.

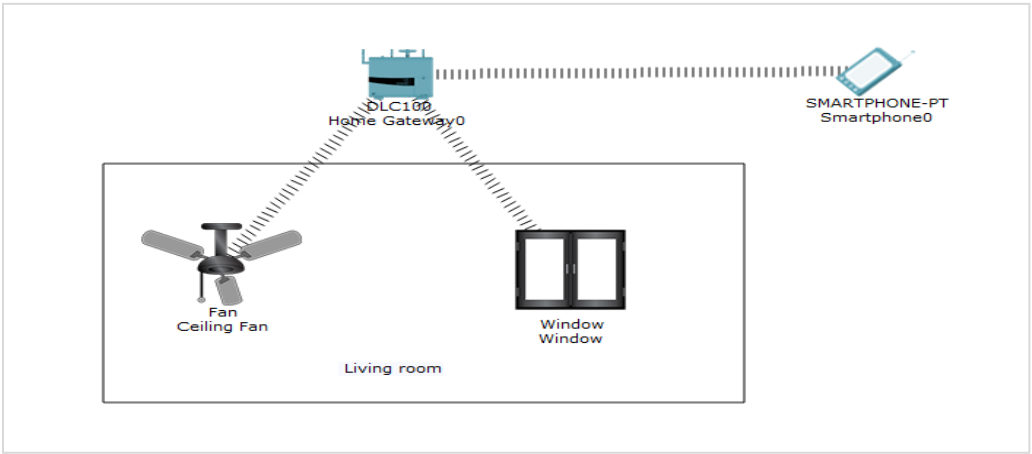

Figure 2 Considered smart home (SH) IoT use-case visual implementation on packet-tracer to apply with ECC based signature

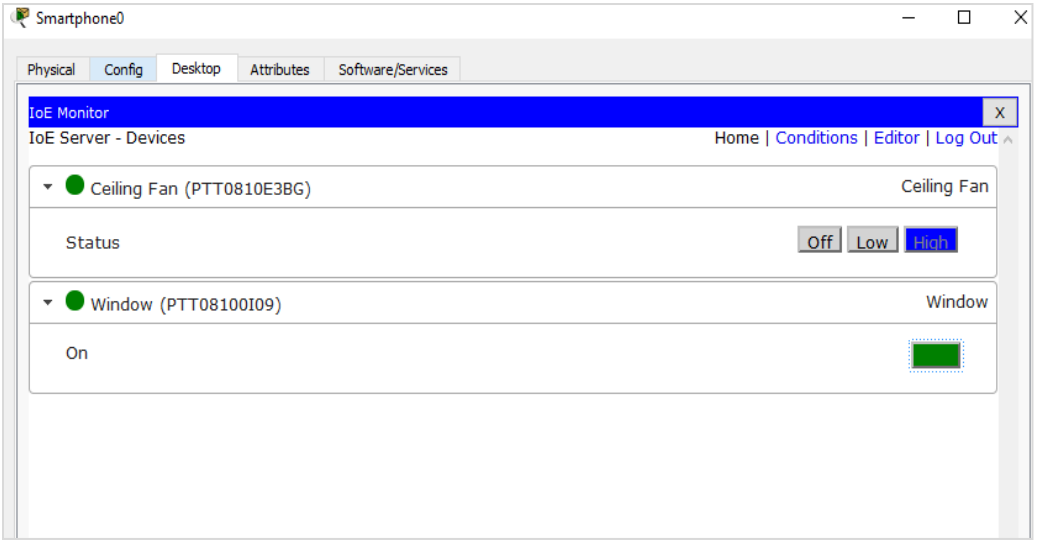

Figure 3 Secure smart home dashboard interface to control manage different devices

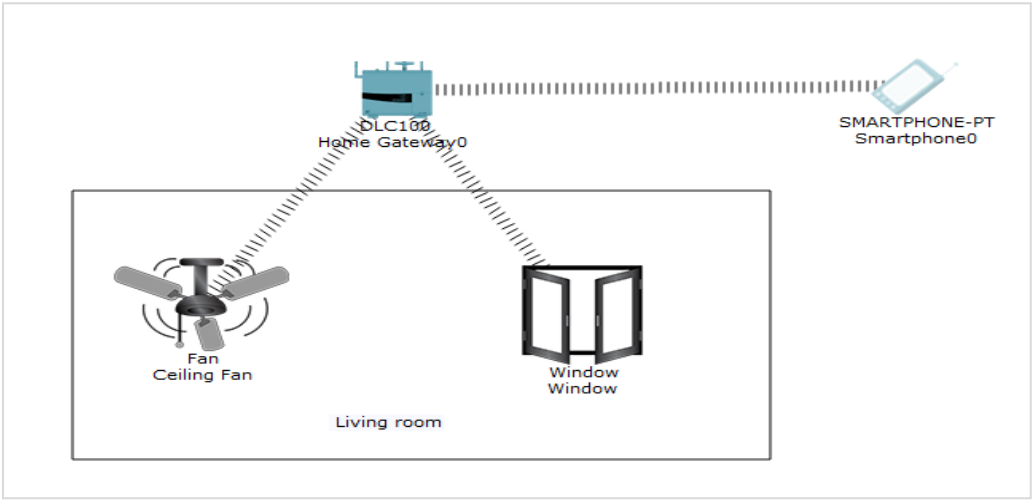

Figure 4 A running SH IoT case controlled from the dashboard

5.Performance analysis

An elliptic arc that is not a singular cubic curve [19]. Over a field K, two variables such as, f(x, y) =0 with a rational fact. The arena K is typically occupied to be the composite figures, real, rational, algebraic postponements of rational, p-adic facts, or a finite ground. For cryptography, Elliptic bends are examined with Fp (underlying fields). Here are leading and p>3. F2m is a binary illustration with 2m fundamentals [20].

Components:

1. Public_Key, P_K
2. Private_Key, S_k
3. Set of Operators that work on these Keys
4. Predefined Constraints (required by some algorithms)

An Elliptic curve can be shown as E_P (a, b). P is the prime numeral where a, b modulo to mod P. The following equation is called ECC equation. *Figure 5* shows the Curve.

$$y^2 = x^3 + ax + b$$

Unlike ellipse it is described by calculation of the circumference. Let's explain a complete example of between Alice and Bob as shown by *Figure 6.*

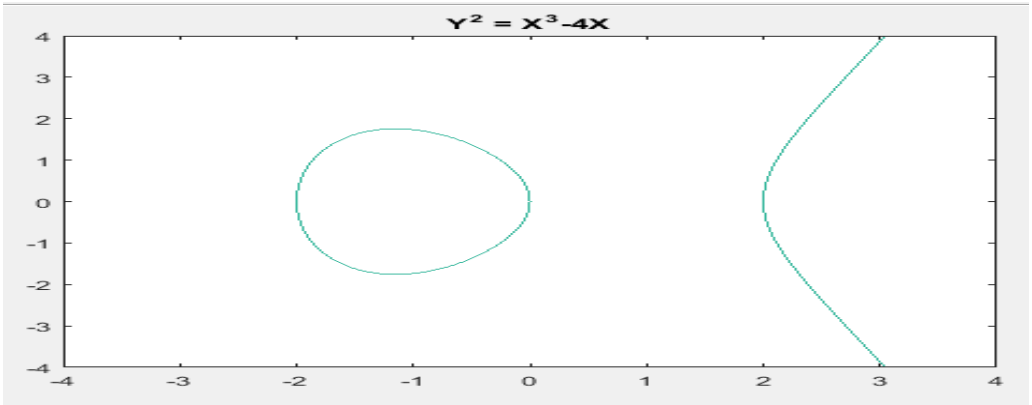

Figure 5 ECC plotting on MATLAB for y2=x^3 – 4x

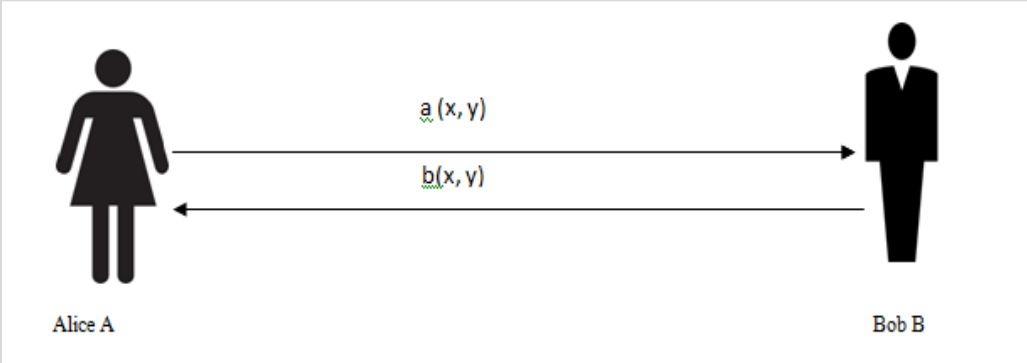

Figure 6 Key conversation between Alice and Bob

Alice calculates a (b (x, y)) where Bob finds b(a(x, y)). subsequently $ab = ba$ as per the ECC rules.
Where Alice and Bob famine to decide arranged a communal key and it is computed by Alice and Bob their pubkey and prikey.

Alice: $prikey, Sk = a$
$pubkey, Pk = a * B$
Bob: $prikey = b$
$pubkey = PB = b * B$
Alice and Bob exchange respectively extra pubkey. Mutually yield the creation of prikey, Sk, since added user's pubkey, Pk where,

$$Alice \rightarrow KAB = a(bB)$$
$$Bob \rightarrow KAB = b(aB)$$
$$Shared\ Secret\ Key = KAB = abB$$

A (Y_A, X_A) – PubPriKey pair
B (Y_B, X_B) – PubPriKey pair
1. The end Alice computes:

$$K = (xK, yK) = XA * YB$$

2. The end Bob can compute:

$$L = (xL, yL) = XB * Y$$

3.Since
$YXB = XAdBG = dBdAG = XBY.$
Consequently $K = L$ then $xK = xL$

4. Hereafter the communal undisclosed remains xK
a) Generation of Signature:
For validation a sample text m by Alice, by means of private key dA and public key QA = dA * G
1. Compute, e = H (m), where H is a cryptographic hash function, SHA-II
2. Get a haphazard numeral k from the matrix [1, n − 1] defined
3. Calculate r = x1 (mod n), wherever (x1, y1) = k * G.If r = 0, go to step 2
4. Compute s = k^(-1) (e + dAr)(mod n). If s = 0, verve to phase 2
5. The desired signature is the couple (r,s)
b) Signature Verification:
Aimed at B to verify A's name, B must have A's pubkey Y
1. Authenticate that r and s remain numbers in [1, n − 1]. If not, the sign is illegal
2. Firstly compute e = H (m),
3. then, w = s -1 (mod n)
4. where u1 = ew (mod n) and u2 = rw (mod n)
5. find (x1, y1) = u1G + u2Y
6. The sign is lawful if x1 = r (mod n), wrong else

6.Result analysis and comparison

With Cryptool 2, we can visualize the key exchange system by Diffie and Hellmann. The process is shown in the following *Figure 7* where different Attacks and its respective level can be computed. *Figure 8* shows the security level comparison. *Table 3* demonstrations the results for different attack use cases. We test the efficiency of RSA and ECC by five Attacks in 5 cases. In case 1, we test by ROBOT attack, and see the efficiency of ECC is well than RSA. Similarly, we test by DROWN, BEAST, Lucky 13 and Logjam Attack for getting the desired output. In the figure, we see that the security level of ECC is additionally well-organized than RSA.

For the same level of security, meaningfully lesser parameters can be second-hand in ECC than RSA. For example, to accomplish 112 bits of safety level, RSA algorithm requirements a key size of 2048 bits, while ECC desires a key size of 224 bits [15] as shown in *Table 4*. A proportional investigation of RSA and ECC is accessible on the foundation encryption and decryption times for the data of 8 bits, 64 bits, and 256 bits.

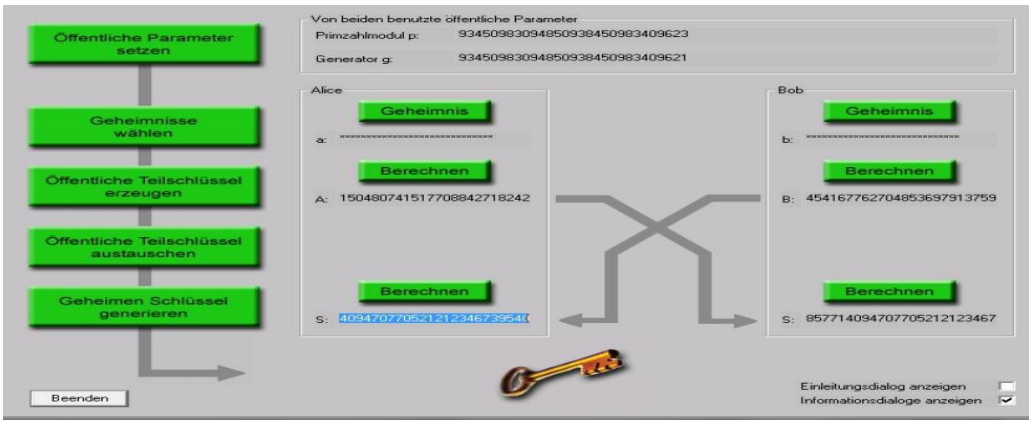

Figure 7 Key exchange system by diffie and hellmann. DROWN, BEAST, lucky thirteen or logjam are well known attack fashionable cryptographic algorithms

Table 3 Security level of ECC vs. RSA for different attack

Case	Attack	RSA level	ECC level
1	ROBOT [20]	122	158
2	DROWN [21]	68	120
3	BEAST [22]	100	140
4	Lucky [23]	270	360
5	Logjam [23]	210	290

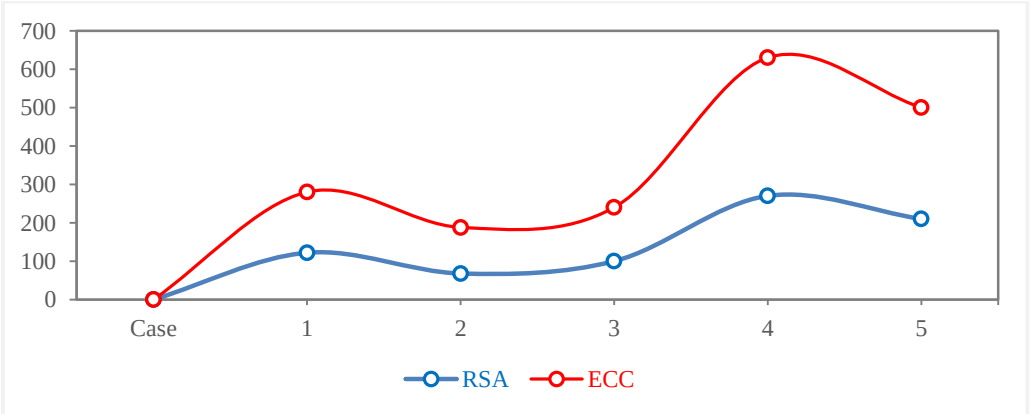

Figure 8 Security level comparison against considered attacks as on table 3 between ECC based technique and RSA based technique plotted on MATLAB

Table 4 Security level according to NIST

Security bit level	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

7.Conclusion and future scope

IoT is used remarkably in all fields as per the advancement of Technology. We have proposed the application of elliptic curve based digital signature (ECDSA) instead of the existing RSA-driven signing technique. The several IoT use-case setup shows it can address better performance and a higher neck and neck of security strength. We encountered difficulties while implementing the scenario incorporating cryptographic tools, that however, may influence the accuracy of our result. Our ongoing work can be improved using a more skillful implementation and evaluation in which we demand to compete as one of our earliest future works.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Hussain F. Internet of things: building blocks and business models. Springer International Publishing; 2017.
[2] Rosing M. Implementing elliptic curve cryptography. Manning Publications Co.; 1999.
[3] P Shruti, R Chandraleka. Elliptic curve cryptography security in the context of internet of things. International Journal of Scientific & Engineering Research. 2017; 8(5):90-3.
[4] Vargheese R, Dahir H. An IoT/IoE enabled architecture framework for precision on shelf availability: enhancing proactive shopper experience. In international conference on Big Data 2014 (pp. 21-6). IEEE.
[5] Clarke RY. Smart cities and the internet of everything: the foundation for delivering next-generation citizen services. Alexandria, VA, Tech. Rep. 2013.
[6] Hankerson D, Menezes AJ, Vanstone S. Guide to elliptic curve cryptography. Computing Reviews. 2005; 46(1).
[7] Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation. 1987; 48(177):203-9.
[8] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security. 2001; 1(1):36-63.
[9] Tange H, Andersen B. Attacks and countermeasures on AES and ECC. In international symposium on wireless personal multimedia communications 2013 (pp. 1-5). IEEE.
[10] Geometry RA. IEEE 13th international conference on wireless and mobile computing, networking and communications. International workshop on smart environments and urban networking-2017.
[11] Forouzan BA. Cryptography & network security. McGraw-Hill, Inc.; 2007.
[12] Gupta V, Stebila D, Fung S, Shantz SC, Gura N, Eberle H. Speeding up secure web transactions using elliptic curve cryptography. In NDSS 2004.
[13] Sinha R, Srivastava HK, Gupta S. Performance based comparison study of RSA and elliptic curve cryptography. International Journal of Scientific & Engineering Research. 2013; 4(5):720-5.
[14] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust threshold DSS signatures. In international conference on the theory and applications of cryptographic techniques 1996 (pp. 354-71). Springer, Berlin, Heidelberg.
[15] Joye M, Tymen C. Protections against differential analysis for elliptic curve cryptography—an algebraic approach. In international workshop on cryptographic hardware and embedded systems 2001 (pp. 377-90). Springer, Berlin, Heidelberg.
[16] Tiwari HD, Kim JH. Novel method for DNA-based elliptic curve cryptography for IoT devices. ETRI Journal. 2018; 40(3):396-409.
[17] Jansma N, Arrendondo B. Performance comparison of elliptic curve and RSA digital signatures. nicj. net/files. 2004.
[18] Rajeshwari PG, Thilagavathi K. An efficient authentication protocol based on elliptic curve cryptography for mobile network. International Journal of Computer Science and Network Security. 2009; 9(2):176-85.
[19] Kumari S, Karuppiah M, Das AK, Li X, Wu F, Kumar N. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. The Journal of Supercomputing. 2018; 74(12):6428-53.
[20] Bos J, Kaihara M, Kleinjung T, Lenstra AK, Montgomery PL. On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography. 2009.
[21] Mahto D, Khan DA, Yadav DK. Security analysis of elliptic curve cryptography and RSA. In proceedings of the world congress on engineering 2016 (pp. 419-22).

[22] Mahto D, Yadav DK. Network security using ECC with biometric. In international conference on heterogeneous networking for quality, reliability, security and robustness 2013 (pp. 842-53). Springer, Berlin, Heidelberg.
[23] Mahto D, Yadav DK. RSA and ECC: a comparative analysis. International Journal of Applied Engineering Research. 2017; 12(19):9053-61.

Azrin Zahan received his Bachelor from the Department of Information and Communication Technology (ICT) of Mawlana Bhashani Science and Technology University (MBSTU). His research interest includes Smart Grid Security, Cybersecurity, Cryptography, Blockchain, and the Internet of Things.
Email: azrinzahanmbstu@gmail.com

Md. Selim Hossain has been working as a Lecturer in Department of Computer Science and Engineering at Khwaja Yunus Ali University, Sirajganj, Bangladesh. He completed his B.Sc. degree on Telecommunication and Electronic Engineering from Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh and M.Sc. (Engg.) on Information and Communication Technology from Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. His main research interest is based on IoT, Blockchain, Cryptography and Network Security, Antenna, Algorithm and Software Engineering.

Ziaur Rahman, is currently a PhD Candidate at RMIT University, Melbourne, and an Assistant Professor (currently in study leave) of the Department of ICT, MBSTU, Bangladesh. He was graduated from Shenyang University of Chemical Technology, China, in 2012 and completed Masters from IUT, OIC in 2015. His articles received the best paper award and nomination in IEEE conferences and published in reputed journals. His research includes Blockchain aligned IoT, Cybersecurity and Software Engineering.

SK. A. Shezan, currently pursuing his PhD degree in Electrical and Electronic Engineering from RMIT University, Melbourne, Australia. He was a lecturer of Electrical and Electronic Engineering Deptartment of Uttara University, Dhaka, Bangladesh. He received his Master of Engineering degree from University of Malaya, in 2016. Moreover, he received his Bachelor of Engineering degree in Electrical Engineering and Automation from Shenyang University of Chemical Technology, China, in 2013. His research interests are Microgrid, HRES, Solar Energy, Wind Energy,etc.