Journal of Korea Multimedia Society Vol. 22, No. 4, April 2019(pp. 463-471)
https://doi.org/10.9717/kmms.2019.22.4.463

Shuffling of Elliptic Curve Cryptography Key on Device Payment

Chinyere Grace Kennedy[†], Dongsub Cho[††]

ABSTRACT

The growth of mobile technology particularly smartphone applications such as ticketing, access control, and making payments are on the increase. Elliptic Curve Cryptography (ECC)-based systems have also become widely available in the market offering various convenient services by bringing smartphones in proximity to ECC-enabled objects. When a system user attempts to establish a connection, the AIK sends hashes to a server that then verifies the values. ECC can be used with various operating systems in conjunction with other technologies such as biometric verification systems, smart cards, anti-virus programs, and firewalls. The use of Elliptic-curve cryptography ensures efficient verification and signing of security status verification reports which allows the system to take advantage of Trusted Computing Technologies. This paper proposes a device payment method based on ECC and Shuffling based on distributed key exchange. Our study focuses on the secure and efficient implementation of ECC in payment device. This novel approach is well secure against intruders and will prevent the unauthorized extraction of information from communication. It converts plaintext into ASCII value that leads to the point of curve, then after, it performs shuffling to encrypt and decrypt the data to generate secret shared key used by both sender and receiver.

Key words: Elliptic Curve Cryptography, Device Payment, Shuffling Key Process

1. INTRODUCTION

Ubiquitous usage of mobile phones devices has triggered the development of applications targeted at mobile platforms. Consequently, the mobile devices have been established as the major platforms for users to transfer and exchange diverse data over the wireless networks [1]. This strong demand for mobile applications and services raise increasing concerns about the security for their access, user privacy, and the applications. As such, security for mobile accesses turns out to be very significant and critical to guarantee secure mobile transactions, data integrity, and confidentiality [2]. Additionally, this security is critical in protecting mobile users and mobile-based application systems from unauthorized accesses and various attacks [3]. One such application that utilizes the mobile platform is the device payment also known as mobile money or m-commerce. M-commerce entails the use of mobile phones for various online transactions through high-speed internet [1, 4]. The platform is viewed as an attractive substitute for cash, cheque, or credit modes of payment. With such high-end business transactions, provision of security is paramount [5]. Subsequently, financial payment through mobile phones being one of the latest technologies has come across numerous

※ Corresponding Author: Dongsub Cho, Address: Computer Architecture and System Design Lab. Asan Engineering Building, Ewha Womans University 52 Ewhayeodae-Gil, Seodaemun-Gu, Seoul 03760, Korea , TEL: +82-3277-2314, FAX: +82-3277-2306, E-mail: dscho@ewha.ac.kr

Receipt date: Mar. 21, 2018, Revision date: Feb. 27, 2019
Approval date: Mar. 26, 2019

[†] Dept. of Computer Science and Engineering Ewha Womans University, Seoul, South Korea
(E-mail: gkennedy@ewhain.net)
[††] Dept. of Computer Science and Engineering Ewha Womans University, Seoul, South Korea

challenges concerning security because of the public dispersion of mobile phone and devices [5, 14].

Consequently, m-commerce poses a potential risk because it is extremely tedious to provide security to the tasks and transactions done through mobile devices [4]. Device payment was defined [5] as a way of payment where payment transaction is delivered by a wireless network to the mobile device. M-payment transaction is done over varied radio communication protocols (SMS and NFC) with encrypted level of security. A secure device payment system must be attributed to user authentication, data integrity, confidentiality, service availability, mobile service authorization, and non-repudiation [5]. Achieving such security requirements on the system involve the use of a cryptography technique to protect data from hackers while providing for the privacy of encrypted data.

Cryptography is science of securing an information or message mathematically. The cryptography technique is classified under three categories including [4] [13]: Symmetric Key Cryptography (SKC), Asymmetric Key Cryptography (AKC), and Hash Function (HF). To deliver the characteristics of such systems, public key infrastructure (PKI), where reliable certificate establishments endorse ownership of key pairs and certificate is implemented. One such system is ECC crypto-system, an AKC, which is divided into key generation, encryption, and decryption providing for two separate keys; secret and public keys [6]. Distributed ECC provides for spreading of the crypto-system among the service providers and the clients that is the users of device payment systems based on secret sharing. The ECC crypto-system is founded upon the hypothesis that factoring big numbers is computationally hard. ECC keys are characteristically 160 or 224-bits long [7]. ECC provides the same level of security as RSA but with smaller key size which create less heat generation and less power consumption [7]. Distributed ECC generates digital signatures that offer a guarantee of indication to origin, identity and status of an electronic transaction, as well as acknowledging informed agreement by the signer. To create a digital signature, the signing software generates a one-way hash of the electronic data [6].

The user's private key is then used to encrypt the hash, resulting in a unique value to the hashed data. The encrypted hash together with hashing algorithm and other information, form the digital signature. Any modification to the data, results in a different hash value [7]. This characteristic enables others to authenticate the integrity of the data by using the signer's public key to decrypt the hash. In addition, a digital signature makes it hard for the signing party to deny having participated in any validation. This is the non-repudiation attribute [6]. This is the non-repudiation attribute [6]. If a signing party repudiates a valid digital signature, then their private key either stands compromised, or they are being dishonest. ECC's key size provides a greater security as demonstrated in this paper. It is suitable for machine with low bandwidth, less memory and low computing power. Elliptic curve cryptography public key is used in the encryption and verification of messages while secret shared key is used in the decryption and generation of messages [7]. ECC defines the authority level and parameter for both sender and receiver respectively. The system will respond with dual authorized shared key where necessary. The main advantages of ECC over others in cryptosystems are encryption, decryption and signature verification speed up.

Table 1 above shows the main primary uniqueness of ECC key is its relatively small key size with the same level of security as standard. It is observed that the key size and memory intensity of ECC are noticeably smaller in comparison with other asymmetric systems, which has created a lot of interest especially in the mobile electronics field. For instance, the same level of security expected from 1024-bit of RSA key can be handled by ECC 160-bit key [6]. RSA normally requires 1024-bits for corporate use and it also requires 2048-bits for highly valuable keys. ECC and AES has a better advantage to RSA since their key lengths are relatively smaller, for this reason this study will be centred on ECC key. This has created a lot of interest especially from the mobile electronics field. Fig. 1 shows the various workflow in a bank-centric device payment. The bank prepares the account data which includes identification of authorized consumer, it makes the consumer to accept contactless card payments or transport cards. On the process payments are made current financial network which is the NFC.

The mobile network is used during the personalization of the device. This paper proposes a device payment method based on ECC and Shuffling based on distributed key.

2. RELATED WORKS

The key strength of the ECC is in its ability to achieve high standard of security using small key size. Brown D. et al [8] shows the expected future security of the encryption as a random number generator. They opined that ECC may be a more efficient encryption system than the more traditional methods.

Branovic [9] used the method called Simple Scaler hardware emulator to try to get the hardware use of various cryptosystems. In their [9] work they found that memory latency can cause inexpensive commodity systems some difficulty.

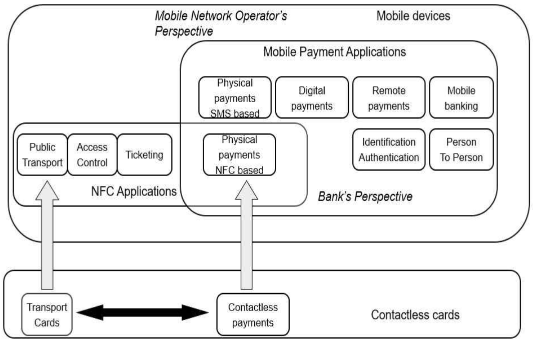


Fig. 1. Retail M-Payment Ecosystem [Eelco de Jong].

Gupta and Stebila [10] also did a study on the communication relationship between ECC and RSA. Their result shows the encryption feasibility on the PDA which decryption and signing can carry out, but the research is only based on the web security.

Obaidur Rahaman [11] proposed a new technique where he uses classic technique of mapping to characterize affine points in the elliptic curve that has been displaced. ASCII values of plain text were paired up and it served as input for the Elliptic curve cryptography. In their new proposed approach, they were able to implement text encryption and decryption using card shuffling logic. However, with all the above method or approach to security of devices lack depth which our approach will display.

Our approach considered randomly shuffling shared secret to cause the attacker not to be able to predicate the secret keys. The main key factor in this approach is the strength of the key which will prevent the brute force on the plaintext and ciphertext. Though there are many secure algorithms, but this project implemented ECDH algorithm.

Encryption process otherwise known as ElGamal Cryptosystem as Fig. 2. The first step involves obtaining the random public key from a trusted key server. Then, an arbitrary shuffling process of selected points follows. This is as good as using a

Table 1. Comparison of Key Size (Cryptography)

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

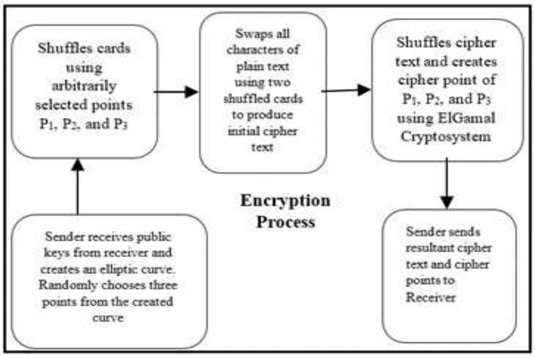

Shuffles cards using arbitrarily selected points P1, P2, and P3
Swaps all characters of plain text using two shuffled cards to produce initial cipher text
Shuffles cipher text and creates cipher point of P1, P2, and P3 using ElGamal Cryptosystem
Encryption Process
Sender receives public keys from receiver and creates an elliptic curve. Randomly chooses three points from the created curve
Sender sends resultant cipher text and cipher points to Receiver

Fig. 2. Encryption Process (ElGamal Cryptosystem).

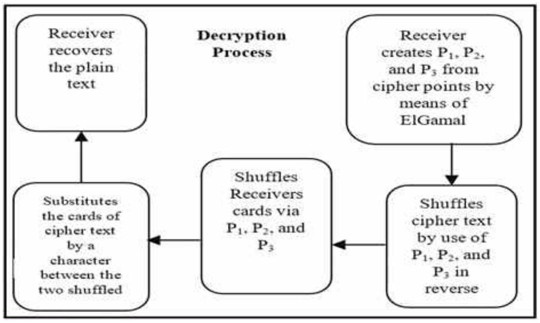

Receiver recovers the plain text
Decryption Process
Receiver creates P1, P2, and P3 from cipher points by means of ElGamal
Substitutes the cards of cipher text by a character between the two shuffled
Shuffles Receivers cards via P1, P2, and P3
Shuffles cipher text by use of P1, P2, and P3 in reverse

Fig. 3. Decryption Process (ElGamal Cryptosystem).

guessing method. The acquired public key enhances the swap of all characters of text using shuffling [11]. The shuffling uses ElGamal cryptosystem, finally the sender sends result ciphertext to cipher points to the receiver.

Decryption process as Fig. 3 shows received text message which is randomly generated, the receiver uses encryption algorithm to access the text - observe that the shuffle is on reverse order. Then the shuffle received card substitutes the ciphertext. Finally, the receiver retrieves or recovers the plain text [11]. In this logic, the receiver chooses Ep (a, b) with an elliptic curve over GF (p), e1 is a point on elliptic curve, e1= (x1, y1) e2=d*e1, where d is the private key. Shuffling process entails the sender receiving public keys Ep (a, b), e1 and e2 as broadcasted by the receiver, and choosing three points P1, P2, and P3 over the elliptic curve [11].

3. ANALYSIS OF ELLIPTIC CURVES CRYPTOGRAPHY

Cell phones are one of the driving tools of the modern age, especially as mobile devices have been integrated into workplace, banking, and entertainment system. Smartphones have almost everything once only had by desktop computers. The simplicity and convenience that comes with mobile banking has encouraged the users to transfer money online between accounts using mobile phones [17]. This essentially means that the movement of sensitive information now takes place in a platform that is smaller and more exposed to external threats as compared to the relatively stable and secure desktop platform that was in frequent use before now. The relative efficiency of transfer comes with a compromise on the key-size and reduced security. Power limitations and computational limitations are among the most important limitations faced on mobile devices. The surge to take lead in innovation in the mobile technology industry has pushed the makers to introduce robust encryption schemes as well as acquaint the ability to use brute force to crack the powerful encryptions [18].

ECC was introduced by Neal Koblitz and Victor Miller in 1985 [19] as a unique way of using encryption of public key. The encryption of public key provides a way to exchange the keys among different entities in a secure manner. There are several standards in place for ECC including Standards for Efficient Cryptography Group (SECG), National Institute of Standards and Technology (NIST), and American National Standard Institute (ANSI) [20]. Elliptic curve cryptography is different from the conventional schemes in that it uses discrete algorithm which cannot be easily used when the key size is the same [21]. The key bytes of elliptic curve encryption are less compared to the RSA scheme. RSA key-size cannot be less than 1024-bits for financial institutions, so that the users can see the drop-in battery life as they wait [22]. The speed of encryption through elliptic curve is much more than what is seen in RSA schemes. ECC has been observed to run more than a hundred times faster RSA with same security [23].

Many cryptographic algorithms are publicly obtainable, though certain organizations may keep it a secret. Elliptic curves contain adding and doubling operations that are defined in fields either even or odd. A field is defined through a concept of rings and groups. Ring is a set that has two operations, whose properties are similar to those of groups. Groups are closed sets wherein two elements' operation leads to another element. Both rings and groups contain identity elements as well as inverses for the elements contained in the field. While in a ring, a group is formed by elements and the operator of multiplication, it is called as a field. Elliptic curves exist in as well as off fields. The algorithms of encryption are similar except the operations of doubling and adding.

Mobile platform offers increased security for payment not only because of a small key size, but also because of the optimization of the operations of doubling and adding in it [24]. "At the focus of modern device payment systems' security is the concept of payment tokenization. The actual credit card number and expiration date are replaced with a payment token that is compatible with existing merchant systems" [25]. However, certain factors must be considered while selecting the public key cryptosystem for use in a mobile environment. These factors include mobile battery life, memory, and bandwidth. These factors are highly limited in such constrained environments like wireless pagers or mobile phones. Therefore, the suitability of a public key scheme relies on the efficiency in terms of key sizes and computing costs. The obvious choice for device payment because its strength-per-bit is the highest in comparison to the other public key cryptosystems [25].

4. IMPLEMENTATION OF SHUFFLE ALGORITHM

With regards to the expected outcome, C programming language presents procedural way of coding and not object-oriented. Therefore, each code that facilitates the exchange of secret keys from the transmitter side to the receiver is already preset and simply requires the programmer to input the codes. A complier will be used to execute the outcome of the programming. The C program will be run on Arduino, which will take the typed source program and convert it into an object file, that can be executed by the program. Arduino is an open source tool developed based on hardware and software platform that can control and sense objects than the desktop computer [26]. According to Arduino in 2011, Arduino development board is designed as a wiring board just as a physical computing platform, which is based on multimedia programming environment. It has a computing platform that are based on a microcontroller board, it has also a development environment for sending a set of instructions for implementation.

The compiler works in two phases: phase 1 scans the source programs and generates an intermediate code that simplifies the grammar for subsequent processing. This converts the intermediate code into an object code. The second phase is the

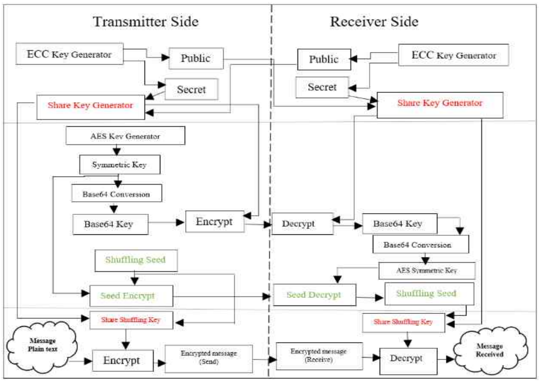
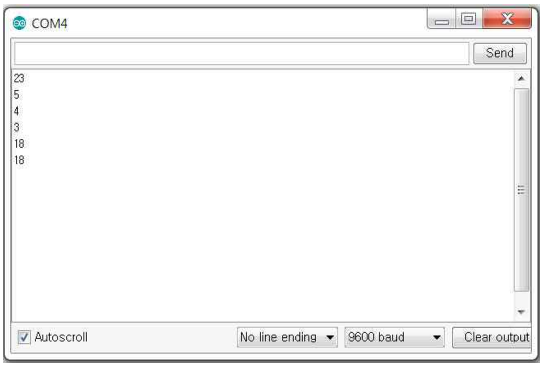


Fig. 4. Encryption and Decryption Process of the Proposed Method.

linker. It appends a standard library code to the object file in order to complete the code. This results in to an executable embedded systems program.

Fig. 4 shows three categories the encrypted and decrypted process, namely; ECC key generator part, AES key generator part and Shared Shuffling Key Part which is our proposed algorithm framework. The dotted line is the separation of the physical hardware with serial cable. Shuffling seed is a random seed that are generated from encrypted and decrypted seed. It also shows the Diffie-Hellman key exchange, it allows two users client A and client B, who might have never met before, or even work together but can communicate with an established secret key. The process entails that one of the first pubic key cryptographic protocols uses secret key between two communication channels. The protocol has a constrain, then shared key by itself can never be transmitted over the channel. This algorithm is designed in a way that it can be used to interpret any decrypted messages. We implemented the secret key exchange using C programming language. The advantage of this project over other existing cryptographic key algorithm is the key strength which is built up on the shuffle key. It also provides a better security and faster to implement to compare to other algorithm.

Defining Basic procedure used in this our proposed ECDH algorithm as shown in Fig. 5 and below shows the detailed explanation of the giving algorithm:



```
23
5
4
3
18
18
```

Fig. 5. Result Secret shared key.

Client A and Client B need to agree on a prime number, p and base g before initiating communication:

p=23 and g=5

Client A selects Private key a whose value is 7 and computes:

Client A=ga mod p= 4

Client B selects Private key b whose value is 9 and computes:

Client B=gb mod p= 3

Client A sends A to Client B and Client B sends to Client A

To get the shared secret key, Client A computes: secret = Client Ba mod p, 7^4 mod 23

Shared Secret = 18

To get the shared secret key, Client A computes: secret = Client Ab mod p, 9^3 mod 23

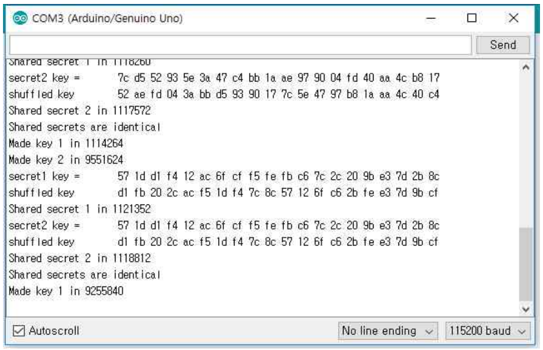
Shared Secret = 18

Client A which is Alice and Client B which is Bob agreed on two numbers as can be seen above p(Prime number 23) and g(Generator of P 5). Then Alice and Bob has their private keys, They send each other the computed value Ba = gb and Ab = ga. Both Alice and Bob obtained the same value of the secret shared key as 18. They are the ones that are authorized to perform this activity because their private keys have constants a and b that prevent anyone from intruding. It means in between 23, 3, 4, 5 will be difficult to combine the numbers to obtain the shares secret key which is 18. Fig. 5 above shows that the algorithm is well secure since the a and b cannot be transmitted across the wire.

5. ECC KEY GENERATION AND RESULT

On the Transmitter side ECC key generator uses public and secret keys to share key generator.

The shared secret key identical is generated from ECC which implies that the key can be decrypted and used by the receiver. Symmetric key generator uses Base64 Conversion to convert



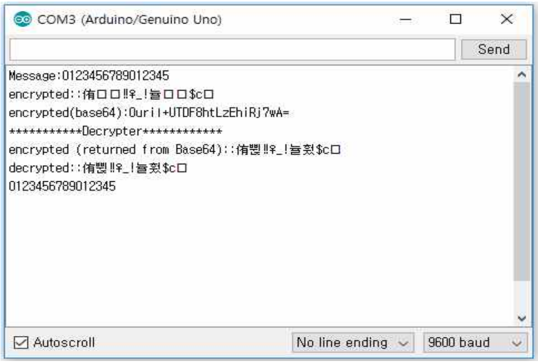
```
Shared secret 1 in 1118260
secret2 key =      7c d5 52 93 5e 3a 47 c4 bb 1a ae 97 90 04 fd 40 aa 4c b8 17
shuffled key       52 ae fd 04 3a bb d5 93 90 17 7c 5e 47 97 b8 1a aa 4c 40 c4
Shared secret 2 in 1117572
Shared secrets are identical
Made key 1 in 1114264
Made key 2 in 9551624
secret1 key =      57 1d d1 f4 12 ac 6f cf f5 fe fb c6 7c 2c 20 9b e3 7d 2b 8c
shuffled key       d1 fb 20 2c ac f5 1d f4 7c 8c 57 12 6f c6 2b fe e3 7d 9b cf
Shared secret 1 in 1121352
secret2 key =      57 1d d1 f4 12 ac 6f cf f5 fe fb c6 7c 2c 20 9b e3 7d 2b 8c
shuffled key       d1 fb 20 2c ac f5 1d f4 7c 8c 57 12 6f c6 2b fe e3 7d 9b cf
Shared secret 2 in 1118812
Shared secrets are identical
Made key 1 in 9255840
```

☑ Autoscroll No line ending 115200 baud

Fig. 6. Generated Shared key.

base64 key which was encrypted to be decrypted. The decrypted seed receives encrypted seed that is shuffled and sent to Share shuffling key. In Fig. 6, the encrypted message with base64 key returned from base64 with decrypted key. The shuffled key was not first identical because the secret key 1 and secret key 2 are not the same. Then as the simulation repeats it tasked with the same secret key 1 and secret key 2, it shows the shuffled key identical which was the expected result.

Applications of this project to device payment will make use of the user selected share key randomly for data unlock in the secure element. Strength of application protection in device payment is not entirely dependent on the strength of the user selected key; “secure elements built into the Base64 key or device benefit from additional protections provided by the device OS which prohibits applications to access the secure element as shown in Fig. 7. Research has been done on the application of elliptic curves over the logic of card shuffling for text encryption and traditional key exchange. They observed many positive aspects in their proposed algorithm, thus suggesting ECC as very appropriate for use in device payment. This type of cryptosystem uses the same key for both encryption and decryption. Some of the advantages of this proposed method is that it is very fast relative to public key cryptography and considered system secure, if the key is strong. The limitation could be complication of exchange and administration of the key.



```
Message:0123456789012345
encrypted::侑□□‼♀_!늘□□$c□
encrypted(base64):OuriI+UTDF8htLzEhiRj7wA=
***********Decrypter************
encrypted (returned from Base64)::侑뾇‼♀_!늘췄$c□
decrypted::侑뾇‼♀_!늘췄$c□
0123456789012345
```

☑ Autoscroll No line ending 9600 baud

Fig. 7. Shuffle key result.

6. CONCLUSION

Data encryption using shuffle key, which is an elliptic curve cryptography points was implemented. By the understanding of the shuffle key related with data, the points corresponding to data over shared key, shows that encryption can be used to shuffle key to generate shared key for more reliable security. This project demonstrated random selection of keys that can improve the performance of security against several cryptographic attacks and prevent brute force on the plaintext and ciphertext.

Our approach will be very effective on the payment devices that requires low power and storage use. The drawback of this paper could be the incorrect of precision.

REFERENCE

[1] L. Antovski and M. Gusev, “M-Payments,” *Proceedings of the 25th International Conference Information Technology Interfaces,* pp. 95-100, 2003.

[2] M. Jakobsson and D. Pointcheval, “Mutual Authentication for Low-power Mobile Devices,” *Lecture Notes in Computer Science,* Vol. 2339, pp. 178-195, 2002.

[3] P. Dadhich, K. Dutta, and M.C. Govil, “Secur-

ity Issues in Mobile Agents," *International Journal of Computer Applications,* Vol. 11, No. 4, pp. 1-7, 2010.

[4] J.M. Lee, S.W. Kim, O.J. Kwon, "Implementation of a Flexible Architecture for a Mobile Cart Applying Design Patterns," *Journal of Korea Multimedia Society*, Vol. 19, No. 4, pp. 747-755, 2016.

[5] X. Zheng and D. Chen, "Study of mobile payments systems," *IEEE International Conference on E-Commerce*, pp. 24-27, 2003.

[6] Ayushi, "A Symmetric Key Cryptographic Algorithm," *International Journal of Computer Applications,* Vol. 1, No. 15, pp. 1-4, 2010.

[7] P.K. Sahoo, G. Jena, R.K. Chhotray, and S. Patnaik, "An Implementation of Elliptic Curve Cryptography" *International Journal of Engineering Research and Technology*, Vol. 2, Issue 1, pp. 1-8, 2013.

[8] D.R.L. Brown and R.P. Gallant, *The Static Diffie-Hellman Problem*, ePrint 2004/306, International Association for Cryptologic Research, 2004.

[9] Branovic, R. Giorgi, and E. Martinelli, "Memory Performance of PublicKey Cryptography Methods in Mobile Environments," *Proceeding of ACM SIGARCH Workshop on Memory Performance: Dealing with Applications, Systems and Architecture*, pp. 24-31, 2003.

[10] V. Gupta, D. Stebila, and S.C. Shantz, "Integrating Elliptic Curve Cryptography into the Web's Security Infrastructure," *Proceedings of the 13th International World Wide Web conference,* pp. 402-403, 2004.

[11] O. Rahaman, "Data and Information Security in Modern World by Using Elliptic Curve Cryptography," *Computer Science and Engineering,* Vol. 7, No. 2, pp. 29-44, 2017.

[12] R.V.R. Deij, K. Hageman, A. Sperotto, and A. Pras, "The Performance Impact of Elliptic Curve Cryptography on DNSSEC Validation," *IEEE/ACM Transactions on Networking* Vol. 25, Issue 2, pp. 738-750, 2017.

[13] S.A.M. Ilyas, *RFID Handbook Applications Technology Security and Privacy,*Publ. CRC press, USA, 2008.

[14] D. Eisenreich and B. DeMuth, "*Designing Embedded Internet Devices", Publ. Newnes, pp. 582, USA, Book,* 2002.

[15] T. Izu and T. Takagi, A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks, *Proceeding of PKC 2003, 6th International Workshop on Theory and Practice in Public Key Cryptography*, pp. 280-296, 2002.

[16] H. Ning and Z. Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework," *IEEE Communications Letters,* Vol. 15, No. 4, pp. 461-463, 2011.

[17] S. Mewada, P. Sharma, S.S Gautam "Classification of Efficient Symmetric Key Cryptographic Algorithm," *International Journal of Computer Science and Information Security,* Vol. 14, No. 2, 2016.

[18] B.J. Jang, K.S. Moon, S.H. Lee, "Effective Compression Technique for Secure Transmission and Storage of GIS Digital Map," *Journal of Korea Multimedia Society*, Vol. 14. No 2, pp. 210-218, 2011.

[19] C.G. Kennedy, D.S. Cho, "Design and Simulation of NFC-Based M2M payment Model for Mobile Phone with Trusted Platform Module," *Journal for China-USA Business Review,* Vol. 16, No. 10, pp. 491-503, 2017.

[20] S. Karnouskos and F. Fokus "Mobile Payment:a journey through existing procedures and standardization initiatives, "*IEEE Communications Surveys and Tutorials*, Vol. 6, No. 4, pp. 44-66, 2004

[21] AlShaali and Varshney, "On the usability of mobile commerce", *International Journal of Mo-bile Communications*, Vol. 3, No. 1, pp. 29-37, 2005.

[22] L. Batina, G. B.Muurling, and S. B. Ors, “Flexible Hardware Design for RSA and Elliptic Curve Cryptosystem“, *Proceedings of the Cryptographer's Track at the RSA Conference*, pp. 1250 - 263, 2004.

[23] L. Zhao and K. Chen, “Application of Elliptic Curve Cryptosystem for Security Protocol of Wireless Communication,” *Computer Engineering,* Vol. 28, No. 3, pp. 128-129, 2002.

[24] National Security Agency, Case for Ellipti Curve Cryptography, www.nsa.gov/business/programs/elliptic_curve.shtml, (accessed Jan., 19, 2019).

[25] W. Chou, “Elliptic Curve Cryptography and Its Applications to Mobile Devices“ *Retrieved:* http://honors.cs.umd.edu/reports/ECCpaper.pdf. (accessed April., 20, 2019)

[26] http://www.arduino.org/products/board arduino-uno “Aruino- Introduction“ (accessed Feb., 20, 2019).

Dong Sub Cho

He is currently a Professor in Department of Computer Science and Engineering with Ewha Womans University in Seoul, South Korea. He graduated and had bachelor's Degree and master's degree from Dept. of Electrical Engineering with Seoul National University in 1979 and 1981, respectively. He did his Ph.D. at Dept. of Computer Engineering with the same university in 1986. He had sabbatical leave and worked as Visiting Scholar at University of California, Irvine, in 1996. He is also a member of IEEE. He served as President of Korean Multimedia Society in 2012. His research interest includes: Computer Architecture and Systems Design, AI-based Embedded Systems, Smart Learning for Computer Education, Cryptography for Web-based Service, and Performance Evaluation of Open Software-Hardware Integration.

Chinyere Grace Kennedy

She is currently a PhD student in Computer Science and Engineering with Ewha Womans University located in Seoul, South Korea. She did her master's degree with the same University in Information Technology. She studied in her bachelor's degree in Electrical and Electronics Engineering with Enugu State University of Science and Technology in Enugu (ESUT), Nigeria. She is the current vice president of SWE Lagos chapter, she is also a member of IEEE and COREN respectively. She has done a few publications on Computer Networking area. Her research interest includes, Network Security, Design of Cryptographic Protocols, Information Security, Secret Sharing and Secure Multi-Party Computing Protocols, Public Key Cryptography and ID-Based Cryptography.