

Download file | iLovePDF x Detroit 2020 x +

ieomsociety.org/detroit2020/



Home Authors Program Registration Committee Competitions Keynote Global Engineering Education GBME Industry4.0 Panels Sponsors



Home Authors Program Registration Committee Competitions Keynote Global Engineering Education GBME Industry4.0 Panels Sponsors

» Committee

## Committee

### Conference Committee

#### Conference Chairs

- Dr. Muhammad Sohail Ahmed, Professor, Engineering Management, School of Engineering, Eastern Michigan University, Ypsilanti, MI, USA
- Dr. Ahad Ali, Associate Professor and Director of Industrial Engineering Program, Lawrence Technological University, Southfield, Michigan, USA
- Dr. Leslie Monplaisir, Professor and Chair, Department of Industrial and Manufacturing Engineering, Wayne State University, Detroit, MI, USA
- Dr. Wilkistar Otieno, Associate Professor and Chair, Industrial & Manufacturing Engineering, University of Wisconsin-Milwaukee, USA

#### Program Chairs

- Dr. Daw Alwerfalli, Professor and Director of Engineering Management Program, A. Leon Linton Department of Mechanical, Robotics and Industrial Engineering, Lawrence Technological University, Southfield, Michigan, USA
- Dr. Jihong Yan, Professor in Industrial Engineering and Deputy Dean of School of Mechatronics Engineering, Head of intelligent Manufacturing Scientific Research Team, Harbin Institute of Technology, Harbin, China

#### Industry Chairs

- Steven Sibrel, Sr. Supplier Quality Manager, Harman International, Novi, Michigan, USA and Professional Development Chair & Past Chair-ASQ Greater Detroit
- Dr. Saso Krstovski, Lean Manufacturing Coach/Six Sigma Master Black Belt, Van Dyke Transmission Plant, Ford Motor Company, Michigan, USA

### Diversity and Inclusion Chairs / Women in Industry and Academia Chairs

- **Shannon Dare**, Global Technology Planning & Strategy, Body & Chassis, Ford Motor Company
  - **Cheryl Thompson**, Founder and CEO of CADIA, Center for Automotive Diversity, Inclusion & Advancement, Detroit, Michigan
- 

### Organizing Committee

- Dr. George Pappas, Assistant Professor, Electrical and Computer Engineering, Lawrence Technological University
  - Dr. Hayder Zghair, Adjunct Professor, Lawrence Technological University
  - Dr. Saso Krstovski, Adjunct Professor, Lawrence Technological University
  - Dr. Andy Pandian, Associate Professor, Saginaw Valley State University, Michigan
  - Dr. CJ Chung, Professor of Computer Science and Director of Robofest, Lawrence Technological University
  - Dr. Sibrina N. Collins, Executive Director, The Marburger STEM Center, Lawrence Technological University
- 

### Global Engineering Education Chairs

- Dr. Abu Masud, Boeing Global Engineering Professor, Industrial and Manufacturing Engineering Department, Wichita State University, Kansas, USA
- Dr. Hamid Parsaei, Professor of Industrial and Systems Engineering, Texas A&M University (College Station)

### IEOM Global Business Management Education Chairs

- **Prof. Jose Arturo Garza-Reyes**, Professor of Operations Management and Head of the Centre for Supply Chain Improvement, College of Business, Law and Social Sciences, The University of Derby, UK
- **Prof. Vikas Kumar**, Director of Research and Scholarship and Professor of Operations and Supply Chain Management, Bristol Business School, University of the West of England, UK

### Industry 4.0 Chairs

- Dr. Abdul Talib Bon, UTHM, Malaysia
- Dr. Mehran Doulat, Xiamen University Malaysia

### Industry Solutions Chair

- Dr. Joseph Ogundu, President at Emerald Global Consulting Inc., Detroit, Michigan

### Technical Chairs

- Dr. Hayder Zghair, Adjunct Professor, Lawrence Technological University, Michigan, USA
- Dr. Andy Pandian, Saginaw Valley State University, Michigan, USA

### Publication Chair

Dr. Mohammed Rahman, Central Connecticut State University, USA

### Sponsors and Exhibitors Chair

Professor Don Reimer, Lawrence Technological University, Southfield, Michigan, USA

### 6th NA Conference Chairs (2021 Monterrey)

- Dr. Bernaro Villarreal Celstino, University of Monterrey, México
- Ing. Luz María Valdez de la Rosa, University of Monterrey, México
- Ing. Jacobo Tijerina Aguilera, University of Monterrey, México

### Conference Secretariat

- Dr. Taufiqul Islam, Operations Manager, IEOM Society International
- 

## Track Chairs

### Artificial Intelligence

- Dr. Samira A. Rahimi, McGill University, Canada
- Ehsan Teymourian, Rutgers University, USA

### Automation and Agility

- Dr. Alok K. Verma, Old Dominion University, Norfolk



5<sup>th</sup> NA International Conference on  
**Industrial Engineering and  
 Operations Management**  
 August 10-14, 2020, Detroit, MI, USA  
**Virtual Conference**



🏠 > Authors

## Authors

### Call for Papers and Presentations (Flyer)

Due to many requests, submission deadline is extended to July 10, 2020

IEOM Society is organizing the 5th North American International Conference on Industrial Engineering and Operations Management in Detroit, Michigan, USA during August 10-14, 2020. The conference aims to provide a forum for academics, researchers and practitioners to exchange ideas and recent developments in the field of Industrial Engineering and Operations Management. The conference is also expected to foster networking, collaboration and joint effort among the conference participants to advance the theory and practice as well as to identify major trends in Industrial Engineering and Operations Management.

Submission Site: <https://www.xcdsystem.com/IEOM/abstract/index.cfm?ID=M6q7kay>

Authors can submit full paper(s) or abstract(s) only. Authors MUST use the conference template to prepare papers or abstracts. IEOM Society encourages to submit full paper(s). All full papers will be subjected to double peer review. Accepted papers will be published in the proceedings and indexed by Scopus. PREVIOUS IEOM PAPERS ARE IN SCOPUS ALREADY. Any submission implies that an author will present the paper or abstract virtually or orally.

[Paper Template WORD \(\\*.docx\)](#)

[Abstract Template WORD \(\\*.docx\)](#)

Sample IEOM Papers can be followed to prepare a quality paper:

[Paper 1](#), [Paper 2](#), [Paper 3](#), [Paper 4](#), [Paper 5](#), [Paper 6](#), [Paper 7](#), [Paper 8](#), [Paper 9](#) and [Paper 10](#).

ACCEPTED PAPERS WILL BE PUBLISHED IN IEOM # 1 (2020) AND # 2 (2020) VOLUMES. THE CONFERENCE PROCEEDINGS WILL BE PUBLISHED IN IEOM # 3 (2020) VOLUME.



## Competitions

### Student Competitions – IEOM 2020 Detroit

- [Undergraduate Student Paper Competition Sponsored by SIEMENS](#)
- [Graduate Student Paper Competition Sponsored by EATON Corporation](#)
- [Master Thesis Competition](#)
- [Doctoral Dissertation Competition](#)
- [Senior Capstone Design Project Competition sponsored by Tooling Tech Group](#)
- [Undergraduate Research Competition](#)
- [High School and Middle School STEM Competition](#)
- [Lean Six Sigma Competition sponsored by Tooling Tech Group](#)
- [Simulation Competition](#)
- [Supply Chain and Logistics Competition](#)
- [Undergraduate and Graduate Poster Competition](#)

#### **Undergraduate Student Paper Competition Sponsored by SIEMENS**

The IEOM UNDERGRADUATE Student Paper Competition Sponsored by SIEMENS will recognize outstanding papers in the field of industrial engineering, manufacturing engineering, systems engineering, operations research, engineering management and operations management written by student(s). Selected papers will be considered for the competition and must be presented at the 2020 Detroit Conference . The paper will be judged based on the technical content and presentation. A group of academics / professionals will serve as judges. Scoring rubrics will be used for both parts of the judging. Winners will receive award certificates. These awards are presented at the 2020 Detroit Conference.

Submit your paper online:



5<sup>th</sup> NA International Conference on  
**Industrial Engineering and  
Operations Management**  
August 10-14, 2020, Detroit, MI, USA  
**Virtual Conference**



[Home](#) [Authors](#) [Program](#) [Registration](#) [Committee](#) [Competitions](#) [Keynote](#) [Global Engineering Education](#) [GBME](#) [Industry4.0](#) [Panels](#) [Sponsors](#)

🏠 > [Global Engineering Education](#)

## Global Engineering Education

### 18th IEOM Global Engineering Education

Detroit, Michigan, USA, August 10-14, 2020

IEOM Society International addresses the issues of Global Engineering Education. There are various levels of readiness of engineering graduates from various parts of the world. One of the main themes is how to reduce the readiness gap of engineering graduates around the world. The special focus is given to Industrial Engineering and Manufacturing Engineering including Engineering Management. Are the engineering graduates ready to take on the challenges of the current global economy? With the great success of Global Engineering Education Series of last IEOM conferences, IEOM Detroit Conference will have a dedicated session for the 18th Global Engineering Education where distinguished speakers will discuss the readiness of engineering graduates for workforce around the world. Thirty six featured speakers will be from various part of the world to address engineering education challenges and opportunities.

Global Engineering Education Topics can be related on:

- Accreditation
- Learning Assessment
- Problem based learning
- Project based learning
- Active collaborative learning
- Student learning assessment
- Teaching and learning
- Pedagogy
- Curriculum improvement



» - Panels

## Panels

### Panels

#### Panel on Lean Six Sigma

4:00 – 5:00 pm, Monday, August 10, Room 1

Panel Chair



**Steven Sibrel**  
Senior Supplier Quality Manager  
Harman International  
Novi, Michigan, USA  
Professional Development Chair and Past Chair – ASQ Greater Detroit

Steve Sibrel is a business process improvement trainer, coach and auditor with over 35 years of experience in the business and manufacturing world. He is currently working as Senior Supplier Quality Manager at Harman International, a manufacturer of audio and infotainment systems for consumer, professional, and automotive industries, with well-known brands such as JBL, Lexicon, Crown, Infinity, Mark Levinson, Becker and Harman-Kardon. Previously he held a number of engineering and management positions in diverse industries at Applied Materials (Semiconductor), NEC (Telecommunications) and Texas Instruments (Military). He has conducted over 200 supplier audits in North America, Europe, and Asia and is a Lead Auditor for ISO/TS16949, ISO9001, ISO13485, ISO17025, and 21CFR820. He has been the Chair for Professional Development for the ASQ Detroit section since 2008. He received the Distinguished Service Award in 2008 and the Leadership Award in 2013 from ASQ. Current ASQ Certifications



5<sup>th</sup> NA International Conference on  
**Industrial Engineering and  
Operations Management**  
August 10-14, 2020, Detroit, MI, USA  
**Virtual Conference**



[Home](#) [Authors](#) [Program](#) [Registration](#) [Committee](#) [Competitions](#) [Keynote](#) [Global Engineering Education](#) [GBME](#) [Industry4.0](#) [Panels](#) [Sponsors](#)

» [Sponsors](#)

## Sponsors

### Sponsors and Partners

Three levels of sponsorship are available with \$2,000, \$1,000 and \$500. Scroll down to see details.

#### Sponsors / Corporate Partners



TOOLINGTECH GROUP



#### University Partners / Affiliate Universities



# **Elliptic Curve Diffie-Hellman Cryptosystem for Public Exchange Process**

**Asep Saepulrohman, Asep Denih**

Department of Computer Science, Faculty of Mathematics and Natural Sciences, Pakuan University, Indonesia  
[asepspl@unpak.ac.id](mailto:asepspl@unpak.ac.id); [asep.denih@unpak.ac.id](mailto:asep.denih@unpak.ac.id)

**Sukono**

Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Padjadjaran, Indonesia  
[sukono@unpad.ac.id](mailto:sukono@unpad.ac.id)

**Abdul Talib Bon**

Department of Production and Operations, University Tun Hussein Onn Malaysia, Malaysia  
[talibon@gmail.com](mailto:talibon@gmail.com)

## **Abstract**

This paper announces data security cryptosystems using Elliptic Curve Diffie-Hellman (ECDH) with elliptic curve type parameter `secp224r1`. It discusses key exchanges such as, for example, the process of calculating symmetric keys chosen from elliptic groups by binary (+) operations, encryption processes, and decryption processes, etc. The proposed cryptosystem that belongs to this site contains a number of materials relating to security, digital forensics, networks, and many other things. Such systems are known to show hidden appeal. We also show that the new cryptosystem has multi-stability and attractiveness that coexist. This implementation uses Elliptic Curve Cryptography (ECC) with JavaScript.

## **Keywords:**

Cryptography, elliptic curve Diffie-Hellman, ECC, cryptosystems, data security.

## **1. Introduction**

Elliptic-Curve Diffie-Hellman (ECDH) builds a shared secret (used as a key) between two parties by making an elliptic curve public-private key agreement protocol on an insecure channel. The key can then be used to encrypt the communication which then uses a symmetric-key password. This is a variant of the Diffie-Hellman protocol using elliptic curve cryptography. ECDH has many applications in cryptography and data security, such as recent research working on cryptographic applications in various fields of science and information security development such as Susantio et.al (2016) with the implementation of elliptic curve cryptography in binary field research, Kumar (2015) analysis of Diffie-Hellman key exchange algorithm with proposed key exchange algorithm, Saepulrohman et.al (2020) implementation of elliptic curve diffie-hellman (ECDH) for encoding messages becomes a point on the  $GF(p)$ , Bisson et.al (2011) computing the endomorphism ring of an ordinary elliptic curve over a finite field, Saady et.al (2019) secure communication, etc.

Modeling related to public key encryption schemes will be explained in terms of encryption operations, decryption and settings related to key deployment procedures. This work reports the special nature of elliptic curves that attracts cryptographers, one of which is closed to the sum of two points in the elliptic curve according to Myasnikov A. G. and Roman Kov V. (2014). Detailed analysis has been carried out on ECDH with the help of phase plots, point sum tables. Then Subramanian, E. K., & Tamilselvan, L. (2020) in his research with the title elliptic curve Diffie-Hellman cryptosystem in big data cloud security and Verma, S. K., Ojha, D. B. (2012) a discussion on Elliptic Curve cryptography and its applications.

Since the new elliptic curve cryptography offers the same level of security as conventional public-key cryptographic algorithms, but with a shorter key size and it shows hidden appeal. According to Ahirwal, R. R., & Ahke, M. (2013) comparison of elliptic curve cryptography (ECC) with RSA, the ECC key length is shorter than RSA, for example 160-bit ECC keys provide the same security as 1024-bit RSA keys. Arithmetic operations on cryptographic cryptography based on elliptic curves do not use real numbers, but cryptography operates in the realm of integers. In plaintext cryptography, ciphertext, and keys are expressed as integers. Therefore, for elliptic curves to be used in data security systems, elliptic curves are defined in finite fields or Galois Field  $GF(p)$  and  $GF(2^m)$ . The general shape of the elliptic curve in  $GF(p)$  or  $GF(2^m)$  is  $y^2 = x^3 +$

$ax + b \pmod p$  with  $p$  is the finite plane and the elements in the galois field are  $\{0, 1, 2, \dots, p - 1\}$  where the addition and multiplication operations are carried out with the modulus of  $p$ . In the cryptography, Washington, L. C. (2008) show elliptic curve  $E$  have been modelled into mathematical equations in the graph of an equation of the form

$$E: y^2 = x^3 + ax + b \quad (1)$$

with  $a, b$  are constants with the restriction that  $4a^3 + 27b^2 \neq 0$  which fulfills the non-singular nature of the pair  $(x, y) \in R \times R$  along with a special point  $\mathcal{O}$  called the infinity point called the Weierstrass equation for elliptical curves. Since each elliptic curve is determined by a cubic equation, Bezout's theorem explains that each line intersects the curve exactly at three points, taken with multiplicity. Valenta et.al (2018) define group law by requiring that the three co-linear points add up to zero. Adding operations on elliptic curves on  $GF(p)$  have the same rules as real numbers. First case if  $x_1 \neq x_2$  then the sum operation  $P + Q = R$ . Addition  $R = (x_3, y_3)$  is sought by determining lines  $l$  through  $P$  and  $Q$  that intersect at  $-R$ , where  $R$  is the result of reflection  $-R$  on the  $x$ -axis. The coordinates of the point  $R$  can be determined by the following equation

$$x_3 = \lambda^2 - x_1 - x_2 \quad (2)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (3)$$

with  $\lambda = (3x_2^2 + a)/2y_1$ . The second case, point  $P$  and  $Q$  the same point  $x_1 = x_2$  can then be written  $P + P = R$ .  $R$  is found by determining the line  $l$  which is tangent to the elliptic curve at point  $P$ , then the intersection of line  $l$  with the elliptic curve is  $-R$  which is a reflection of the  $x$ -axis. The last case if  $x_1 = x_2$  and  $y_1 = -y_2$ , in this case  $Q = -P$  where the lines  $l$  through  $P$  and  $Q$  do not intersect the elliptic curve so that they are said to have an infinity point, written  $P + Q = P + (-P) = \mathcal{O}$ .

Section 2 is an introduction to theories related to elliptic curve cryptography, dynamics and phase plots. Section 3 states the results of the discussion accompanied by examples, and section 4 concludes this work with a summary of the main results.

## 2. Research Methodology

The objects and data analyzed and used in this study were taken from <https://asecuritysite.com/encryption/js08>. The method used in the Diffie-Hellman shared joint key exchange for elliptic curve cryptography has been done by many researchers before Fujdiak et.al (2009), Nagaraj et.al (2015), Weng et.al (2017), Kafa (2006), Lopez et.al (1999), and King (2001). Such as before explaining further, suppose Alice wants to make a shared key with Bob on an insecure channel then steps as follows:

### System parameters

Choose cryptographically strong domain parameters (that is,  $(p, a, b, G, n, h)$  in the main case  $(m, f(x), a, b, G, n, h)$  in binary cases) must be agreed upon. The system parameters must be exchanged authentically between the parties involved in the communication.

### Key agreement

Key agreements must also be secured with strong authentication. with the following procedure:

1. Each party must have a key pair suitable for elliptic curve cryptography, which consists of private key  $d$  (integers randomly selected in intervals  $[1, n - 1]$  and public keys represented by a point  $Q$  (where  $Q = d \cdot G$ ), that is, the result of adding  $G$  to itself time).
2. Allow the Alice key pair  $(d_A, Q_A)$  Bob key pair to be  $(d_B, Q_B)$  where each party must know the other party's public key before executing the protocol.
3. Alice counts points  $(x_k, y_k) = d_A \cdot Q_B$  and Bob counts points  $(x_k, y_k) = d_B \cdot Q_A$  where the shared secret is  $x_k$  (coordinate  $x$  point). Most standard protocols based on ECDH come from the  $x_k$  symmetric key using several hash-based key derivation functions.
4. The shared secrets calculated by both parties are the same, because  $d_A Q_B = d_A \cdot d_B \cdot G = d_B \cdot d_A \cdot G = d_B Q_A$ .

### ECDH key generator algorithm

The elliptic curve parameter domain above  $F_p$  is defined as the equation  $T(p, a, b, G, n, h)$ , where  $p$  is field that the curve is defined over,  $a, b$  he elliptic curve equation coefficient,  $G$  the generator point is the group building elements,  $n$  is prime order of  $G$  i.e. positive integers smallest is  $nG = 0$ , and  $h$  cofactor, number of points in the group elliptic  $E_p(a, b)$  divided by  $n$ ,

Algorithm	ECDH key generator algorithm
<b>Input:</b>	Domain parameter $(p, a, b, G, n, h)$
<b>Output:</b>	Private key: $d_A, d_B$ and Public key: $Q_A, Q_B$
	1. Choose an integer $d_A, d_B \in [1, n - 1]$
	2. User A computes $Q_A = d_A \cdot G$ send to User B
	3. User B computes $Q_B = d_B \cdot G$ send to User A

- 
4. User A calculate  $K = d_A \cdot Q_B = d_A(d_B \cdot G)$
  5. User B calculate  $K' = d_B \cdot Q_A = d_B(d_A \cdot G)$
- 

The public parameters  $E/F_q$  procedure between Alice and Bob uses this public secret to encrypt and decrypt their data sent and received if represented in Figure 1

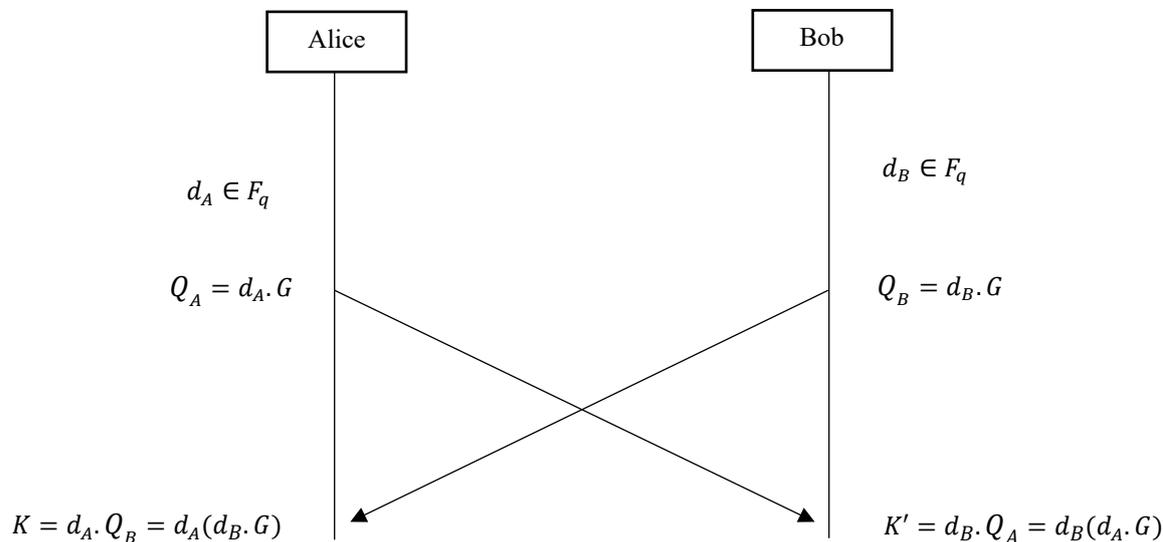


Figure 1. Public parameters  $E/F_q$  Elliptic-Curve Diffie-Hellman

### 3. Discussion result

For crypto, we work in  $F_q$  with  $q = p^n$  is a prime power  $p \neq 2, 3$  and elliptic curve  $E/F_q$  is nonsingular curve satisfying the cubic equation  $y^2 = x^3 + ax + b$ . According to Gamalto (2012), Levi et al (2003), Gupta et al (2002), and Ahmad et al (2016) the set of point on  $E$  lying in  $F_q$  plus the point infinity turns into a group, denoted  $E(F_q)$ . In this paper, Elliptic Curve Diffie Hellman (ECDH) is used to generate a shared key. This implementation uses Elliptic Curve Cryptography (ECC) with JavaScript given by the following dynamics: In this example we use secp224r1 to generate points on the curve. Its format is: We tested for curve validation in secp224r1 by using a on the curve  $y^2 = x^3 + ax + b$ . The coordinates of our generator were

Method	secp224r1
$p$ (The field)	26959946667150639794667015087019630673557916260026308143510066298881
$a$ from $y^2 = x^3 + ax + b$	26959946667150639794667015087019630673557916260026308143510066298878
$b$ from $y^2 = x^3 + ax + b$	18958286285566608000408668544493926415504680968679321075787234672564
$G_x, G_y$ -Base point which is an $(x, y)$ point on the elliptic curve	19277929113566293071110308034699488026831934219452440156649784352033 19926808758034470970197974370888749184205991990603949537637343198772
(creates finite field 0 to $N-1$ ). All operations done (mod $N$ ).	26959946667150639794667015087019625940457807714424391721682722368061

**Stage 1.** Secure encrypted communication between two parties requires that they first exchange keys in a secure physical manner, such as a list of paper keys carried by trusted couriers. The Diffie-Hellman key exchange method allows two parties who have no prior knowledge of each other to jointly build a shared secret key through insecure channels.

- Alice's private value ( $a$ ):

10555476544718952192196363105034777018859933146470740150994127192483

- Bob's private value ( $b$ ):  
22421534874123312678806679740784159138044017904355217652096274711717

**Stage 2.** The public key is represented by a point  $Q$  (where  $Q = d \cdot G$ ), that is, the result of adding  $G$  to itself  $d$  time with the Alice key pair  $(d_A, Q_A) = (X, Y)$  and Bob key pair  $(d_B, Q_B) = (X, Y)$

- Alice's public point ( $Q = d \cdot G$ ) ( $X, Y$ )  
8987204229986706472227050227028111549224015755817884703508769614588  
12896132259525424616867625086728631411580244056063055647978211188728
- Bob's public point ( $Q = d \cdot G$ ) ( $X, Y$ )  
7528903851399665454226291587480383373152718349873335628813796815350  
18979498184836783547654156684532549364212215669203628365894408152597

**Step 3.** The counting step, Alice counts points  $d_A Q_B$  as well as Bob counts points  $d_B Q_A$  where the shared secret is  $xk$  (coordinates  $x$  points) and most standard protocols are based on ECDH derived from  $xk$  symmetric keys using several hash-based key derivation functions

- Alice's secret key  $S = d_A Q_B = d_A \cdot d_B \cdot G$  ( $X, Y$ ):  
18474773625673743791445348971163019521097744517429899874482934101078  
8826979367147201391965964039599479557500313953390936744515708764603
- Bob's secret key  $S = d_B Q_A = d_B \cdot d_A \cdot G$  ( $X, Y$ ):  
18474773625673743791445348971163019521097744517429899874482934101078  
8826979367147201391965964039599479557500313953390936744515708764603.

#### 4. Conclusion

In this work, we introduce a data security system in finite fields. The proposed system has rich dynamics as confirmed by a software that implements the ECDH key exchange algorithm and the encryption-decryption algorithm has been successfully built. The software can send sms messages (key or ciphertext) and receive data properly. We also show examples of the process of encryption and decryption with an algorithm that would not be possible without a key generated from the key exchange process using the ECDH algorithm. Further research can be carried out to find potential applications in communication engineering and cryptosystems for post-quantum cryptographic algorithms used to build secret keys between two parties through insecure communication channels.

#### References

- Susantio, D. R., Muchtadi-Alamsyah, I., (2016), "Implementation of Elliptic Curve Cryptography in Binary Field." Journal of Physics: Conference Series, vol.710, no. 1, <https://doi.org/10.1088/1742-6596/710/1/012022>.
- Kumar, R., Ravindranath, C. C., (2015), "Analysis of Diffie-Hellman Key Exchange Algorithm with Proposed Key Exchange Algorithm." International Journal of Emerging Trends Technology in Computer Science (IJETTCS), vol. no. 1, p. 40-43.
- Saepulrohman, A., & Negara, T. P. (2020), "Implementation of elliptic curve diffie-hellman (Ecdh) for encoding messages becomes a point on the  $gf(p)$ ", International Journal of Advanced Science and Technology, Vol. 29 Iss 6 pp. 3264–3273.
- Bisson, G., Sutherland, A. V., (2011), "Computing the endomorphism ring of an ordinary elliptic curve over a finite field." Journal of Number Theory, vol. 131, no.5, p. 815-831. <https://doi.org/10.1016/j.jnt.2009.11.00>.
- Saudy, N. F., Ali, I. A., Barkouky, R. Al., (2019), "Error analysis and detection procedures for elliptic curve cryptography." Ain Shams Engineering Journal, vol. 10, no. 3, p. 587-597. <https://doi.org/10.1016/j.asej.2018.11.007>.
- Myasnikov, A. G., Roman Kov, V., (2014), "Verbally closed subgroups of free groups." Journal of Group Theory vol. 17, no. 1, p. 29-40. <https://doi.org/10.1515/jgt-2013-0034>.
- Subramanian, E. K., & Tamilselvan, L. (2020), "Elliptic curve Diffie–Hellman cryptosystem in big data cloud security", Cluster Computing, 3. <https://doi.org/10.1007/s10586-020-03069-3>.

- Verma, S. K., Ojha, D. B. (2012), "A Discussion on Elliptic Curve Cryptography and Its Applications." International Journal of Computer Science Issues 2012, vol. 9, no. , p. 74-77.
- Ahirwal, R. R., & Ahke, M. (2013)," Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information on Wide Area Network", International Journal of Computer Science and Information Technologies, 4(2), 363–368.
- Valenta, L., Sullivan, N., Sanso, A., & Heninger, N. (2018)," In Search of CurveSwap: Measuring Elliptic Curve Implementations in the Wild.", Proceedings - 3rd IEEE European Symposium on Security and Privacy, EURO S and P 2018, 384–398. <https://doi.org/10.1109/EuroSP.2018.00034>
- Fujdiak, R., Misurec, J., Mlynek, P., & Janer, L. (2016)," Cryptograph key distribution with elliptic curve Diffie-Hellman algorithm in low-power devices for power grids", Revue Roumaine Des Sciences Techniques Serie Electrotechnique et Energetique, 61(1), 84–88.
- Certicom Research. (2009),"Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography", Standards for Efficient Cryptography, 1(Sec 1), 1–22. <https://doi.org/10.1002/smj>.
- Nagaraj, S., Raju, G. S. V. P., Srinadth, V. (2015) "Data encryption and authentication using public key approach." Procedia Computer Science, vol 48, p.126-132. <https://doi.org/10.1016/j.procs.2015.04.161>.
- Sonnino, A., & Sonnino, G. (2017), "Elliptic-Curves Cryptography on High- Dimensional Surfaces." International Journal of Advanced Engineering Research and Science (IJAERS), vol. 4, no. 2. <https://dx.doi.org/10.22161/ijaers.4.2.28>.
- Weng, J., Dou, Y., Ma, C. (2016), "Research on attacking a special elliptic curve discrete logarithm problem", Mathematica. Problems in Engineering, <https://doi.org/10.1155/2016/5361695>.
- Johnson, D., Menezes, A., & Vanstone, S. (2004),"The Elliptic Curve Digital Signature Algorithm Validation System ( ECDSAVS ). 56. <http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf>.
- Kefa R. (2006), "Elliptic Curve Cryptography over Binary Finite Field  $GF(2^m)$ ." Information Technology Journal, vol. 5, no.1, p. 204-229.
- Lopez, J., Dahab, R. (1999), "Fast multiplication on elliptic curves over  $GF(2^m)$  without precomputation." Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1717(107), p. 316-327. <https://doi.org/10.1007/3-540-48059-527>.
- King, B. (2001), "An improved implementation of elliptic curves over  $GF(2^n)$  when using projective point arithmetic." Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2259(1), p. 134-150. <https://doi.org/10.1007/3-540-45537-x11>.
- Gemalto. (2012). "Benefits of Elliptic Curve Cryptography", March. [http://www.securitydocumentworld.com/creo\\_files/upload/client\\_files/gov\\_wp\\_ecc1.pdf](http://www.securitydocumentworld.com/creo_files/upload/client_files/gov_wp_ecc1.pdf)
- Levi, A., & Savas, E. (2003)," Performance evaluation of public-key cryptosystem operations in WTLS protocol.", Proceedings - IEEE Symposium on Computers and Communications, 1245–1250. <https://doi.org/10.1109/ISCC.2003.1214285>.
- Gupta, V., Gupta, S., Chang, S., & Stebila, D. (2002),"Performance analysis of elliptic curve cryptography for SSL", Proceedings of the Workshop on Wireless Security, 87–94. <https://doi.org/10.1145/570681.570691>
- Ahmad, I., & Waseem, M. (2016),"Implementation of 163-bit Elliptic Curve Diffie Hellman (ECDH) Key Exchange Protocol Using BigDigits Arithmetic", International Journal of Advanced Trends in Computer Science and Engineering, 5(4), 65–70.
- Washington, L. C. (2008),"Elliptic Curves: Number Theory and Cryptography, Second Edition (Discrete Mathematics and Its Applications)".

## **Acknowledgements**

Acknowledgments are conveyed to the Rector, Director of Directorate of Research, Community Involvement and Innovation, and the Dean of Faculty of Mathematics and Natural Sciences, Pakuan University with whom the Internal Grant Program of Universitas Padjadjaran was made possible to fund this research. The grant is a means of enhancing research and publication activities for researchers at Pakuan University.

## **Biographies**

**Asep Saepulrohman** is a lecturer in the Department of Computer Science, Faculty of Mathematics and Natural Sciences, Pakuan University. The field of applied mathematics, with a field of concentration of cryptography and mathematical model.

**Asep Denih** is a lecturer at the Department of Computer Science, Pakuan University. He received his Master of Science in Information Technology for Natural Resources Management (GIS & RS) from IPB University – Indonesia. He then obtain his Ph.D. in Environmental Informatics from University of Miyazaki – Japan. He is currently as the Editor of the Journal *Komputasi* in the Department of Computer Science, Faculty of Mathematics and Natural Sciences, Pakuan University. He is as the Director of Research and Development at Innovation Center for Tropical Sciences. Currently, He is as the Dean of Faculty of Mathematics and Natural Sciences, Pakuan University, Bogor, Indonesia.

**Sukono** is a lecturer in the Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Padjadjaran. Currently as Chair of the Research Collaboration Community (RCC), the field of applied mathematics, with a field of concentration of financial mathematics and actuarial sciences.

**Abdul Talib Bon** is a professor of Production and Operations Management in the Faculty of Technology Management and Business at the Universiti Tun Hussein Onn Malaysia since 1999. He has a PhD in Computer Science, which he obtained from the Universite de La Rochelle, France in the year 2008. His doctoral thesis was on topic Process Quality Improvement on Beltline Moulding Manufacturing. He studied Business Administration in the Universiti Kebangsaan Malaysia for which he was awarded the MBA in the year 1998. He's bachelor degree and diploma in Mechanical Engineering which his obtained from the Universiti Teknologi Malaysia. He received his postgraduate certificate in Mechatronics and Robotics from Carlisle, United Kingdom in 1997. He had published more 150 International Proceedings and International Journals and 8 books. He is a member of MSORSM, IIF, IEOM, IIE, INFORMS, TAM and MIM.