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; asep.denih@unpak.ac.id

Sukono
Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Padjadjaran, Indonesia
sukono@unpad.ac.id

Abdul Talib Bon
Department of Production and Operations, University Tun Hussein Onn Malaysia, Malaysia
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 at.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 at.al (2020) implementation of elliptic curve diffie-hellman (ECDH) for encoding messeges becomes a point on the GF(p), Bisson at.al (2011) computing the endomorphism ring of an ordinary elliptic curve over a finite field, Saudy at.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 eilptic 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 $y^2 = x^3 +$

$ax + b$ mod p with p is the finite plane and the elements in the galois field are $\{0, 1, 2, \ldots, p - 1\}$ 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

$$E: y^2 = x^3 + ax + b \tag{1}$$

with a, b are constants with the restriction that $4a3 + 27b^2 \neq 0$ which fulfills the non-singular nature of the pair $(x, y) \in R \times R$ along with a special point 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 at.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

$$x_3 = \lambda^2 - x_1 - x_2 \tag{2}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \tag{3}$$

with $\lambda = (3{x_2}^2 + a)/2y_1$. 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 $P + Q + P + (-P) = O$.

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 at.al (2009), Nagaraj at.al (2015), Weng at.al (2017), Kafa (2006), Lopez at.at 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 $Q = d.Q$), 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 $(x_k, y_k) = d_A.Q_B$ and Bob counts points $(x_k, y_k) = d_B.Q_A$ 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 $d_AQ_B = d_A.d_B.G = d_B.d_A.G = d_BQ_A$.

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
Input:	Domain parameter (p, a, b, G, n, h)
Output:	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 $Q_A = d_A.G$ send to User B
3.	User B computes $Q_B = d_B.G$ send to User A

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

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

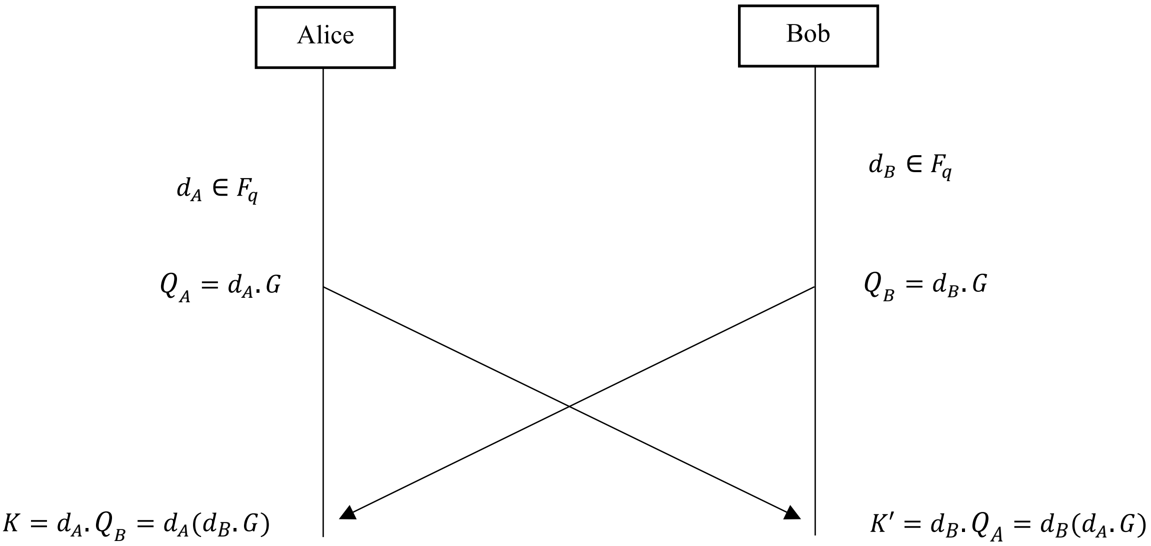

Figure 1. Public parameters E/F_q Elliptic-Curve Diffie-Hellman

3. Discussion result

For crypto, we work in in F_q with $q = p^n$ is a prime power $p \neq 2,3$ and elliptic curver E/F_q is nonsingular curver satisfying the cubic equation $y^2 = x^3 + ax + b$. According to Gamalto (2012), Levi at.al (2003), Gupta at.al (2002), and Ahmad at.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):

1055547654471895219219636310503477701885993314647074015099412719248

- Bob's private value (b):
  2242153487412331267880667974078415913804401790435521765209627471171 7

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

- Alice's public point $(Q = d.G)$ (X, Y)
  89872042299867064722270502270281115492240157558178847035087696145 88
  128961322595254246168676250867286314115802440560630556479782111887 28
- Bob's public point $(Q = d.G)$ (X, Y)
  75289038513996654542262915874803833731527183498733356288137968153 50
  189794981848367835476541566845325493642122156692036283658944081525 97

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 $S = d_A Q_B = d_A.d_B.G$ (X, Y):
  184747736256737437914453489711630195210977445174298998744829341010 78
  88269793671472013919659640395994795557500313953390936744515708764603
- Bob's secret key $S = d_B Q_A = d_B.d_A.G$ (X, Y):
  184747736256737437914453489711630195210977445174298998744829341010 78
  88269793671472013919659640395994795557500313953390936744515708764603.

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 messeges 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 authetication 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. (204),"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 Articial 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 Arti_cial 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

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 whomthe 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.