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 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, Saudy 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 +
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 $Q = dG$), 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 $d_AQ_B = d_A d_B G = d_B d_A G = d_B Q_A$.

### ECDH key generator algorithm

The elliptic curve parameter domain above $E_p$ 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 $n$.

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

![Diagram of public parameters $E/F_q$](image)

**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 curve $E/F_q$ is nonsingular curve 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

<table>
<thead>
<tr>
<th>Method</th>
<th>secp224r1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$ (The field)</td>
<td>269599466671506397946670150870196630673557916260026308143510066298881</td>
</tr>
<tr>
<td>$a$ from $y^2 = x^3 + ax + b$</td>
<td>269599466671506397946670150870196630673557916260026308143510066298878</td>
</tr>
<tr>
<td>$b$ from $y^2 = x^3 + ax + b$</td>
<td>189582862856666080000408668544493926415504680968679321075787234672564</td>
</tr>
<tr>
<td>$G_x, G_y$-Base point which is an $(x, y)$ point on the elliptic curve</td>
<td>1927792911356629307111030803469488026831934219452440156649784352033</td>
</tr>
<tr>
<td>(creates finite field 0 to $N^{-1}$). All operations done (mod $N$).</td>
<td>1992680875803447097019797437088749184205991990603949537637343198772</td>
</tr>
</tbody>
</table>

**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 ($a$):
Stage 2. The public key is represented by a point $Q$ (where $Q = dG$), 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 $(d_B, Q_B) = (X, Y)$

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

Step 3. The counting step, Alice counts points $d_AQ_B$ as well as Bob counts points $d_BQ_A$ 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 $S = d_AQ_B = d_A d_B G (X, Y)$:
18474773625673473791445348971163019521097744517429899874482934101078
8826979367147201391965964039599479557500313953390936744515708764603

Bob's secret key $S = d_BQ_A = d_B d_A G (X, Y)$:
18474773625673473791445348971163019521097744517429899874482934101078
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


© IEOM Society International
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.