*Malaysian Journal of Computing*, 6 (2): 812-822, 2021

eISSN: 2600-8238 online

# IMPLEMENTATION OF BLOM'S KEY PREDISTRIBUTION SCHEME BY USING ELLIPTIC CURVE CRYPTOGRAPHY

**Md Nizam Udin[1*], Farah Azaliney Mohd Amin[2], Aminah Abdul Malek[3], Nur Annisa Zulkifili[4], Nur Atiqah Ghazali[5] and Siti Aisyah Mohd Ridzuwan[6]**

[1*,2,3,4,5,6]*Faculty of Computer and Mathematical Sciences*
*Universiti Teknologi MARA Cawangan Negeri Sembilan, Kampus Seremban*
*70300 Seremban, Negeri Sembilan, Malaysia*
[1*]nizam1558@uitm.edu.my, [2]farah525@uitm.edu.my, [3]aminah6869@uitm.edu.my,
[4]nurannisa.btzulkifili@gmail.com, [5]nuratiqahbintighazali@gmail.com,
[6]siti.aishahridzuwan97@gmail.com

## ABSTRACT

*Cryptography, along with its various methods is used to serve the security communication purpose. Cryptography is said to be secure if the encryption key is hard to break by the attacker. Initially, Blom's Key pre-distribution uses an integer finite field which makes this scheme easy to be intervened by attackers and criminal activists. Hence, this study suggests implementing the Elliptic Curve Cryptography to better enhance the security of the original Blom's. In this proposed scheme, points generated from the elliptic curve will be appointed as public identifiers to be used in the original scheme. The private key and session key of each user are generated using the addition law mathematical operation with public identifiers assigned. Two users who intend to communicate with each other will obtain a common session key. Overall, the modification of Blom's Key pre-distribution scheme will be presented in this study.*

**Keywords***: Asymmetric Cryptography, Blom's Key pre-distribution scheme, Elliptic Curve Cryptography.*

Received for review: 17-12-2020; Accepted: 26-02-2021; Published: 12-05-2021

## 1. Introduction

Cryptography is a mathematical technique that provides authentication, identification to user data, confidentiality and also provides security to the data stored (Pitchaiah & Daniel, 2012). Maqsood *et al*. (2017) defined cryptography as the art of secret writing that allows only the sender and intended recipient of a message to view its contents. In daily life, cryptography is applied to a wide range of security-based systems such as ATM cards with a PIN, e-mails or any online transactions, authenticity using digital signage or biometrics, and currently in the most popular mobile messaging application, WhatsApp.

Encryption and decryption are two main processes in cryptography to keep the secret message from being viewed by unauthorised parties. In the encryption process, a message (plaintext) is transformed by algorithms into indecipherable form (ciphertext) while the process of converting ciphertext to plaintext is decryption. Besides, senders and recipients need to have "keys" to encrypt and decrypt messages. Keys are generated to be used with a given suite of

algorithms, called a cipher. Abualghanam *et al*. (2019) state that the key size, which is the number of digits that represents the key, affects the time needed for encrypting and decrypting the message. Note that the larger the key size, the more difficult will it be to crack the algorithm.

Generally, there are three types of key agreement protocol: trusted-server scheme, self-enforcing scheme and key pre-distribution scheme. Blom's Key pre-distribution scheme introduced by Blom (1984) enables privileged users to generate private keys when a trusted authority gives out a set of keys of which he can calculate the public key with any other user using open information (Belim & Belim, 2019). However, this scheme is said to be vulnerable and will be disrupted when an attacker compromises the keys of at least several users (Chan, 2004). This occurs because Blom's Key pre-distribution scheme uses an integer finite field which lowers the computation required for the attacker to regenerate every common shared key previously.

Elliptic Curve Cryptography (ECC) is an approach for security communication by utilising the mathematics behind elliptic curves and it involves a more complicated computation than the factoring integers problem, such as the elliptic curve discrete log problem to generate security between key pairs (Kavyashree *et* al., 2016). The security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. Thus, the main objective of this study is to modify Blom's Key pre-distribution using the functions and characteristics of the elliptic curve and discrete logarithm problem for a more efficient and enhanced security scheme. Then the modified method will show mathematically to prove that the process to generate key session is successful between two parties.

## 2. Literature Review

There are many cryptography algorithms used to secure information such as DES, 3DES, Blowfish, AES, RSA, ElGamal and Paillier (Al Hasib & Haque, 2008). It can be noted that each of these algorithms is unique. However, the main problem is to produce algorithms that can provide a high level of security while only requiring a short time in key generation, encryption and decryption of information.

Elliptic Curve Cryptography (ECC) is an example of asymmetric cryptography which was established independently by Miller (1985) and Koblitz (1987). Unlike symmetric key algorithms that rely on a single private key to both encrypt and decrypt, asymmetric key algorithms use a pair of keys whereby each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt.

Eschenauer & Gligor (2002) suggested a probabilistic key distribution scheme to demonstrate neighboring nodes between pair-wise keys. The proposed scheme suggests that each of the nodes which are already loaded with a key subset from a global key pool where any two neighboring nodes can share at least one common key with a certain probability. The disadvantages of low accessibility without any support for cluster performance and also low in authentication; whereas the advantages are it requires less storage and it is strong against attacks. Later, Dai *et al.* (2006) have proposed a combination of two schemes which are the Lower-Upper (LU) Decomposition Scheme and Modified Blom's Symmetric Key Generation to improve the security and resource-efficiency in wireless sensor networks.

Moreover, Wang *et al*. (2008) prove that the public-key scheme can preferably be better regarding memory usage, message complexity and security resilience. The study uses Elliptic Curve Cryptography based scheme which is ECC-Cert and ECC-PreComp. Although symmetric-key such as Blom's Key pre-distribution Scheme is very efficient in processing time for sensor networks they require complex key management, which may result in large memory and communication overhead. On the other hand, the advances of this new public key like Elliptic Curve Cryptography (ECC) has simpler and cleaner key management but requires more

computational time. Similarly, Du *et al.* (2005) also proved that Blom's Key pre-distribution has much poorer security resilience as compared to the ECC-based pairwise key schemes.

Due to the rapid development of technology to break encrypted keys, thus the size of the encrypted key must continue to grow to remain secure. As a result, it can be a burden for certain devices such as mobile phones that do not have high computing power. Recently, Elliptic Curve Cryptography has become increasingly popular due to its ability to provide the same level of security as RSA with much smaller key sizes.

This has been shown in Malik (2010) who concludes that ECC uses less power to function, strong enough to assure the same or even better level of security and it also works systematically in terms of memory storage as compared to RSA. Hence, this makes ECC an ultimate choice to be a security algorithm implemented for mobile, portable devices and other lower power applications. Therefore, Elliptic Curve Cryptography has been proved to offer practical and efficient solutions to key management since this scheme offer an alternative to the future generation of public-key cryptosystems besides using post-quantum algorithms.

## 3. Methodology

### 3.1 Elliptic Curve over $\mathbb{Z}_p$

Elliptic curve over prime numbers, $p$ are central of public key cryptography. Let $p > 3$ be a prime number, then the equation of elliptic curve over prime number is defined as:

$$E_p(a,b): y^2 = x^3 + ax + b \text{ over } \mathbb{Z}_p \tag{1}$$

where $(a,b) \in \mathbb{Z}_p$ are constant such that $4a^3 + 27b^2 \neq 0 \pmod p$ is the set of solution of $(x,y) \in \mathbb{Z}_p \text{ x } \mathbb{Z}_p$ together with a point at infinity, $O$.

### 3.1.1 Determine Points on Elliptic Curve over $\mathbb{Z}_p$

We can determine all points on the elliptic curve over $\mathbb{Z}_p$ by first looking at each possible $x \in \mathbb{Z}_p$, computing $x^3 + ax + b \bmod p$, then we try to solve equation (1) for $y$. For a given $x$ we test if $z \equiv x^3 + ax + b \pmod p$ is a quadratic residue by applying Euler's criterion (Stinson & Paterson, 2018). There is an explicit formula to compute square roots of quadratic residue modulo $p$ for $p \equiv 3 (\text{mod } 4)$ which is

$$y \equiv \pm z^{(p+1)/4} \pmod p \tag{2}$$

Table 1 shows all points on the elliptic curve, $E_{11}(1,6)$.

Table 1. Points on the elliptic curve, $E_{11}(1,6)$

| | |
|---|---|
| $(2,4)$ | $(2,7)$ |
| $(3,5)$ | $(3,6)$ |
| $(5,2)$ | $(5,9)$ |
| $(7,2)$ | $(7,9)$ |
| $(8,3)$ | $(8,8)$ |
| $(10,2)$ | $(10,9)$ |
| $(\infty,\infty)$ | |

### 3.1.2 Addition Law of Elliptic Curve over $\mathbb{Z}_p$

All arithmetic operations are performed in $\mathbb{Z}_p$, then the addition law on $E_p(a,b)$ as follows: Suppose we have two points on $E_p(a,b)$, $P=(x_1,y_1)$ and $Q=(x_2,y_2)$.

If $P \neq Q$, then $P+Q=(x_3,y_3)$, where

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1,$$

and

$$m = (y_2 - y_1)(x_2 - x_1)^{-1}$$

If $P=Q$, then $P+Q == 2P=(x_3,y_3)$ called point doubling, where

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1,$$

and

$$m = (3x_1 + a)(2y_1)^{-1}$$

If $P=(x_1,y_1)$ and $Q=(x_1,-y_1)$, then $P+Q=O$. Finally, define $P+O=O+P=P$ for all $P \in E_p(a,b)$.

### 3.1.3 Point Multiplication

$E_p(a,b)$ is isomorphic to $\mathbb{Z}_p$ since any group of prime order is cyclic, and any point other than the point at infinity is a generator of $E_p(a,b)$. Let the generator $\alpha=(x_0,y_0)$. To compute the "power" of $\alpha$ (since the group operation is additive, then we will write as multiple of $\alpha$). To compute $2\alpha=(x_0,y_0)+(x_0,y_0)$, we need to compute

$$m \equiv (3x_0 + a)(2y_0)^{-1} \pmod{p}$$

then we have

$$x_1 \equiv m^2 - x_0 - x_0 \pmod{p}$$
$$y_1 \equiv m(x_0 - x_1) - y_0 \pmod{p},$$

so $2\alpha=(x_1,y_1)$.

To compute $3\alpha = 2\alpha + \alpha = (x_1,y_1)+(x_0,y_0)$. We start again computing

$$m \equiv (y_1 - y_0)(x_1 - x_0)^{-1} \pmod{p}$$

then we have

$$x_2 \equiv m^2 - x_1 - x_0 \pmod{p}$$
$$y_2 \equiv m(x_1 - x_2) - y_1 \pmod{p},$$

so $3\alpha=(x_2,y_2)$. The process is continuing to find $k\alpha$ ($k$ is multiple of $\alpha$).

### 3.2 Blom's Key Pre Distribution Scheme

Let a network has *n* users, then choose *p* be a prime. All users know the prime *p*. The network also assigned trusted authority (TA). TA will compile verification algorithms and made them public. TA also certifies that $ver_U$ is a verification of $U$ and not for the attacker. Then, Blom's Key pre-distribution scheme is shown in the following Figure 1 below (Trappe, 2006).

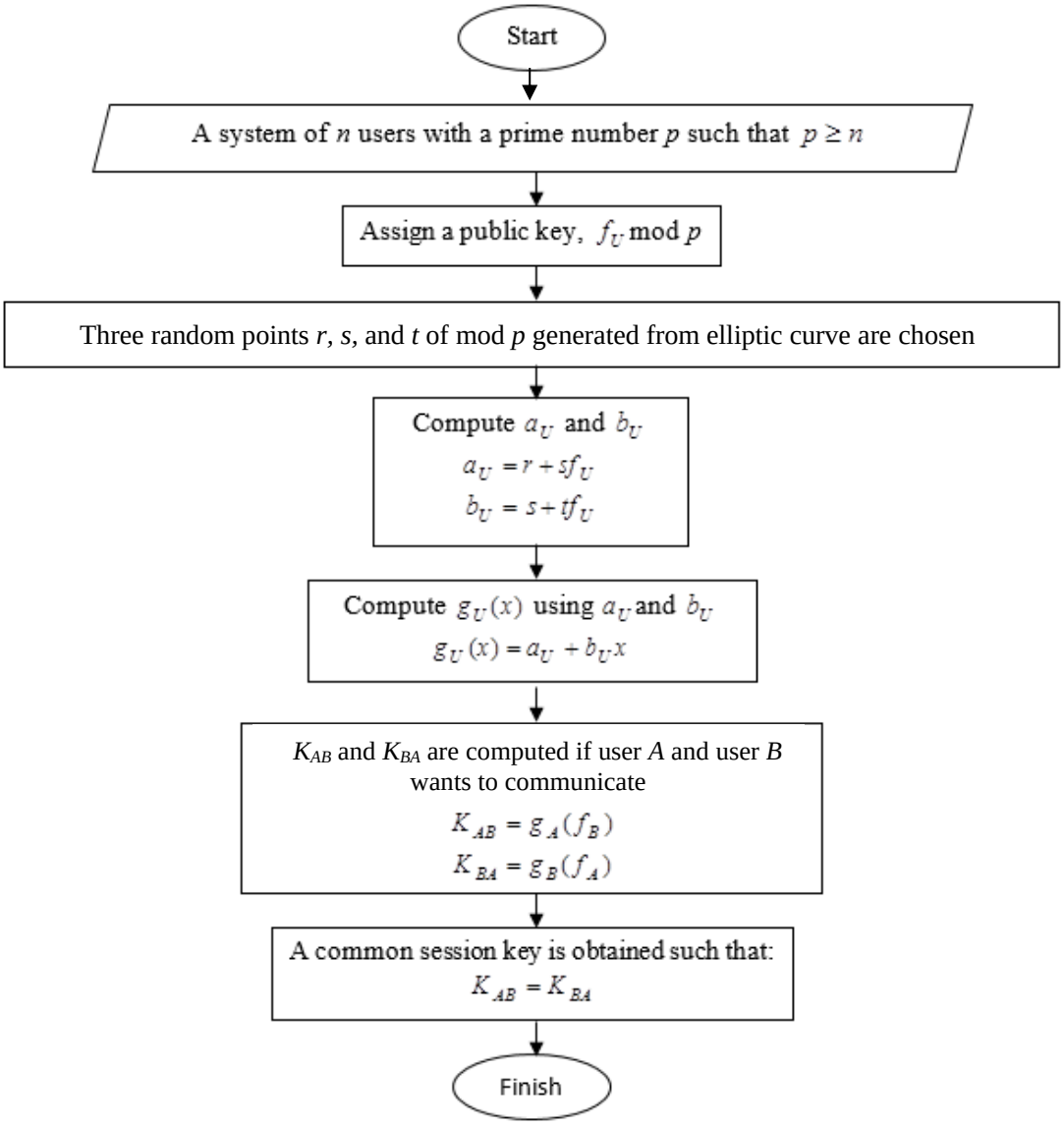


Figure 1. Blom's Key pre-distribution

1. Every user, $U$ is assigned a distinct public key $z_U \pmod p$.
2. TA chooses three random numbers $a$, $b$, $c \pmod p$ keep it unrevealed.
3. For every user $U$, TA calculates the numbers

$$r_U \equiv a + b(z_U) \pmod p \tag{3}$$

$$s_U \equiv b + c(z_U) \pmod p \tag{4}$$

4. TA forms a linear polynomial for every user

$$f_U(x) \equiv r_U + s_U x \pmod p \tag{5}$$

and sends them via his secure channel to $U$.

5. If Ali (A) wants to communicate with Bob (B), then Ali computes

$$K_{AB} \equiv f_A(z_B) = r_A + s_A(z_B) \pmod p \tag{6}$$

while Bob computes

$$K_{BA} \equiv f_B(z_A) \equiv r_B + s_B(z_A) \pmod p \tag{7}$$

$K_{AB} \equiv K_{BA}$ is shown below.

$$\begin{aligned} K_{AB} \equiv f_A(z_B) &\equiv r_A + s_A(z_B) \pmod p \\ &\equiv a + b(z_A) + \big(b + c(z_A)\big)(z_B) \pmod p \\ &\equiv a + b(z_A) + b(z_B) + c(z_A)(z_B) \pmod p \\ &\equiv a + b(z_B) + b(z_A) + c(z_A)(z_B) \pmod p \\ &\equiv a + b(z_B) + \big(b + c(z_B)\big)(z_A) \pmod p \\ &\equiv r_B + s_B(z_A) \pmod p \\ &\equiv f_B(z_A) \\ &\equiv K_{BA} \end{aligned}$$

## 4. Result and Discussion

### 4.1 Modification of Blom's Key Pre-distribution Scheme

The original Blom's Key pre-distribution scheme is modified and improvised by implementing the elliptic curve cryptography. Let a network has $n$ users, then choose $p$ be a prime such that $p \geq n$. All users know the prime $p$. The network also assigned trusted authority (TA). TA will compile verification algorithms and made them public. TA also certifies that $ver_U$ is the verification of $U$ and not for the attacker. The new scheme is as shown in Figure 1.

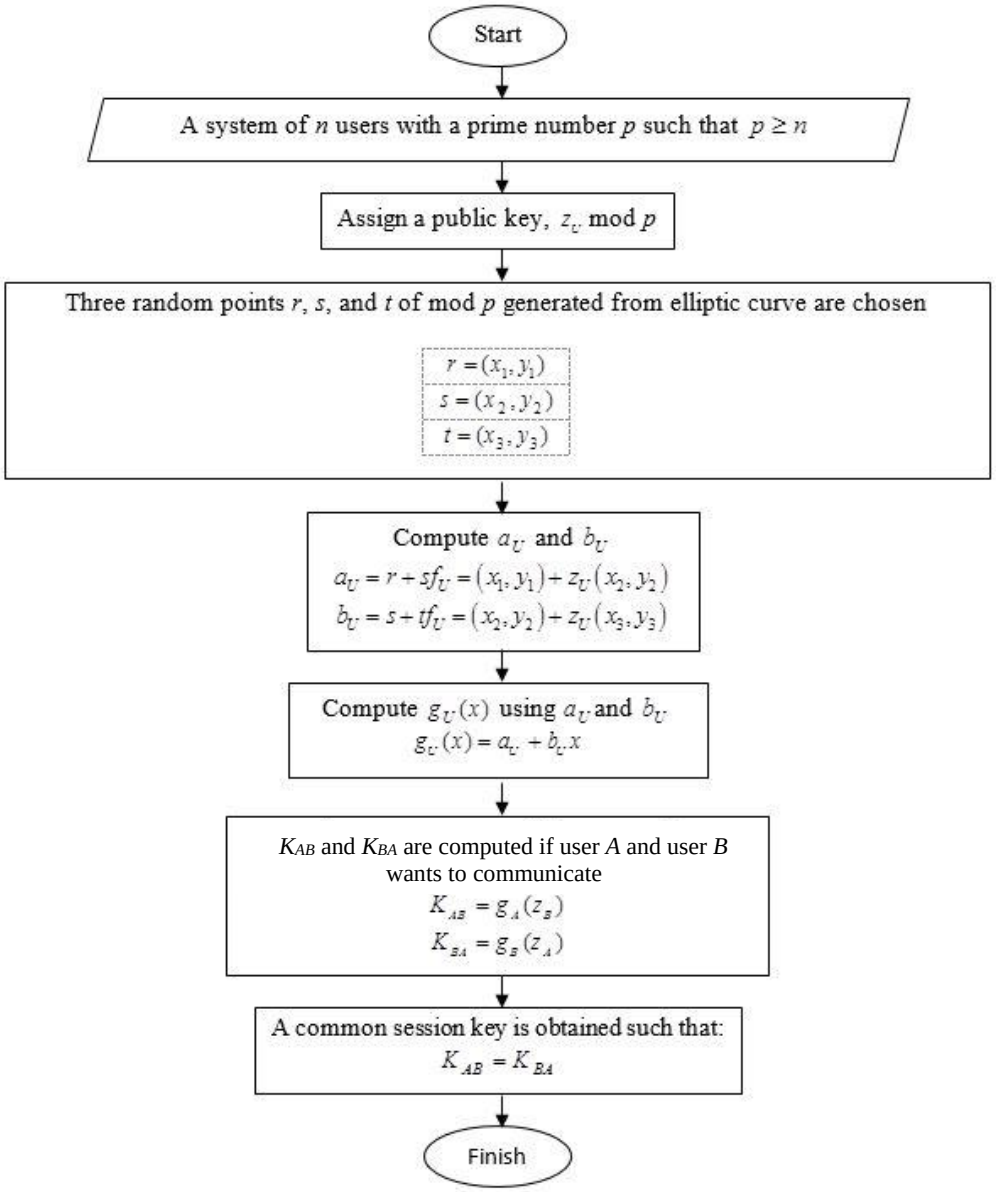


Figure 2. Modification of Blom's Key pre-distribution Scheme Using Elliptic Curve over prime $p$.

1. Every user, $U$ is assigned a distinct public key $z_U \pmod p$.
2. TA chooses three random points from $E_p(a,b)$ which is $(x_1, y_1), (x_2, y_2)$ and $(x_3, y_3)$ and keeps it unrevealed.
3. For every user $U$, TA calculates the numbers

$$(v_x, v_y)_U \equiv (x_1, y_1) + (x_2, y_2)(z_U) \pmod p \tag{8}$$

$$(w_x, w_y)_U \equiv (x_2, y_2) + (x_3, y_3)(z_U) \pmod p \tag{9}$$

4. TA forms a linear polynomial for every user

$$f_U(x) \equiv (v_x, v_y)_U + (w_x, w_y)_U \, x \pmod{p} \tag{10}$$

and sends them in his secure channel to $U$.

5. If Ali (A) wants to communicate with Bob (B), then Ali computes

$$K_{AB} \equiv f_A(z_B) \equiv (v_x, v_y)_A + (w_x, w_y)_A (z_B) \pmod{p} \tag{11}$$

while Bob computes

$$K_{BA} \equiv f_B(z_A) \equiv (v_x, v_y)_B + (w_x, w_y)_B (z_A) \pmod{p} \tag{12}$$

$K_{AB} \equiv K_{BA}$ is shown below.

$$\begin{aligned}
K_{AB} \equiv f_A(z_B) &\equiv (v_x, v_y)_A + (w_x, w_y)_A (z_B) \pmod{p} \\
&\equiv (x_1, y_1) + (x_2, y_2)(z_A) + \big((x_2, y_2) + (x_3, y_3)(z_A)\big)(z_B) \pmod{p} \\
&\equiv (x_1, y_1) + (x_2, y_2)(z_A) + (x_2, y_2)(z_B) + (x_3, y_3)(z_A)(z_B) \pmod{p} \\
&\equiv (x_1, y_1) + (x_2, y_2)(z_B) + (x_2, y_2)(z_A) + (x_3, y_3)(z_A)(z_B) \pmod{p} \\
&\equiv (x_1, y_1) + (x_2, y_2)(z_B) + \big((x_2, y_2) + (x_3, y_3)(z_B)\big)(z_A) \pmod{p} \\
&\equiv (v_x, v_y)_B + (w_x, w_y)_B (z_A) \pmod{p} \\
&\equiv f_B(z_A) \pmod{p} \\
&\equiv K_{BA}
\end{aligned}$$

The modification of Blom's Key Pre-distribution scheme in this study includes the utilization of the chosen elliptic curve equation and its parameter which are:

$$E_{11}(1,6): y^2 \equiv x^3 + x + 6 \pmod{11}$$

where $a = 1$, $b = 6$ and $p = 11$. The detailed calculation of the whole process of modified Blom's Key pre-distribution scheme is demonstrated below.

Each user is given a random public key such that $z_U \leq 11$, where user A, $z_A = 7$ and user B, $z_B = 9$. The trusted authority then will assign three points from the elliptic curve as public identifiers randomly,

$$\begin{aligned}
r &\equiv (x_1, y_1) \pmod{p} \equiv (2,4) \pmod{11}, \\
s &\equiv (x_2, y_2) \pmod{p} \equiv (5,9) \pmod{11}, \\
t &\equiv (x_3, y_3) \pmod{p} \equiv (7,2) \pmod{11}
\end{aligned}$$

Then, the trusted authority computes $a_U$ and $b_U$ for each user using the formula stated in Figure 2 where the calculations use the addition law over mod *p*. The calculation $a_A$ and $b_A$ for user A using additive law and multiplicative law is as follows:

$$a_A \equiv (x_1, y_1) + z_A (x_2, y_2) (\text{mod } p) \equiv (2,4) + 7(5,9) (\text{mod} 11)$$
$$b_A \equiv (x_2, y_2) + z_A (x_3, y_3) (\text{mod } p) \equiv (5,9) + 7(7,2) (\text{mod} 11)$$

By using multiplicative law to find $7(5,9)$.

$$\text{Let } P = (5,9)$$
$$2P = (5,9) + (5,9)$$
$$\lambda \equiv \frac{3(5^2)+1}{2(9)} (\text{mod} 11) \equiv 3 (\text{mod} 11)$$
$$x \equiv 3^2 - 2(5) (\text{mod} 11) = 10$$
$$y \equiv 3(5-10) - 9 (\text{mod} 11) = 9$$
$$2P = (10,9)$$
$$3P = 2P + P = (10,9) + (5,9)$$
$$\lambda \equiv \frac{9-9}{5-10} (\text{mod} 11) \equiv 0 (\text{mod} 11)$$
$$x \equiv 0^2 - 10 - 5 (\text{mod} 11) = 7$$
$$y \equiv 0(10-7) - 9 (\text{mod} 11) = 2$$
$$3P = (7,2)$$
$$4P = 3P + P = (7,2) + (5,9) = (3,6)$$
$$5P = 4P + P = (3,6) + (5,9) = (8,3)$$
$$6P = 5P + P = (8,3) + (5,9) = (2,7)$$
$$7P = 6P + P = (2,7) + (5,9) = (2,4)$$

$$a_A \equiv (x_1, y_1) + z_A (x_2, y_2) (\text{mod } p) \equiv (2,4) + (2,4) (\text{mod} 11)$$
$$\equiv (5,9)$$

Using additive law and multiplicative law to find $b_A$.

$$b_A \equiv (x_2, y_2) + z_A (x_3, y_3) (\text{mod } p) \equiv (5,9) + 7(7,2) (\text{mod} 11)$$
$$\equiv (3,5)$$

The same method is applied to find $a_B$ and $b_B$ for user B and the results are:

$$a_B \equiv (7,2)$$
$$b_B \equiv (10,9)$$

The system will compute $g_U(x)$ using $a_U$ and $b_U$ .

$$g_A(x) = a_U + b_U x$$
$$\text{User A: } g_A(x) = (5,9) + (3,5)x$$
$$\text{User B: } g_A(x) = (7,2) + (10,9)x$$

If user A wants to communicate with user B, then the session key of $K_{AB}$ and $K_{BA}$ need to be generated where both of the session keys are similar.

$$\begin{aligned} K_{AB} = g_A(z_B) &= (5,9) + 9(3,5) \\ &= (5,9) + (7,2) \\ &= (3,6) \\ K_{BA} = g_B(z_A) &= (7,2) + 7(10,9) \\ &= (7,2) + (5,9) \\ &= (3,6) \end{aligned}$$

Therefore, it was proven that $K_{AB}$ and $K_{BA}$ are equal. Then, this session key will be used through symmetric encryption system when user A and user B wish to communicate with each other.

## 5. Conclusion

In the first instance, this study focused on modifying Blom's Key pre-distribution scheme by implementing the elliptic curve to overcome the deficiency and utilizes the complexity of the scheme to become more secured for the users. Since the functions and the elements from the elliptic curves are more complicated and can generate many points, it managed to help increase the security of the session key and any other keys from the attackers. In this study, it was proven that the elliptic curve can be implemented in Blom's Key pre-distribution scheme competently and effectively. Moreover, it has been shown that the modified scheme can generate a common session key share between two users such that $K_{AB} = K_{BA}$ to be used in the encryption and decryption processes. To enhance the modification of Blom's Key pre-distribution scheme, future researchers should apply some of the protocols in Elliptic Curve Cryptography and run a few tests on the scheme to be able to know the performance of the proposed scheme. By implementing a protocol, the scheme may become more secured, efficient and uses less computational power.

**Acknowledgement**

The authors would like to thank Universiti Teknologi MARA (UiTM) Negeri Sembilan, Seremban Campus for the facilities involved in making this research success.

## References

Abualghanam, O., Qatawneh, M., & Almobaideen, W. (2019). A Survey Of Key Distribution In The Context Of Internet Of Things. *Journal of Theoretical and Applied Information Technology, 97*(22), 3217–3241.

Al Hasib, A., & Haque, A. A. M. M. (2008). *A comparative study of the performance and security issues of AES and RSA cryptography.* Paper presented at the 2008 Third International Conference on Convergence and Hybrid Information Technology.

Belim, S. V., & Belim, S. Y. (2019). *Implementation of Simplex Channels in the Blom's Keys Pre-Distribution Scheme.* Paper presented at the Journal of Physics: Conference Series.

Blom, R. (1984). *An optimal class of symmetric key generation systems.* Paper presented at the Workshop on the Theory and Application of of Cryptographic Techniques.

Chan, A.-F. (2004). *Probabilistic distributed key predistribution for mobile ad hoc networks.* Paper presented at the 2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577).

Dai, T. T., Pathan, A.-S. K., & Hong, C. S. (2006). *A resource-optimal key pre-distribution scheme with enhanced security for wireless sensor networks.* Paper presented at the Asia-Pacific Network Operations and Management Symposium.

Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J., & Khalili, A. (2005). A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC), 8*(2), 228–258.

Eschenauer, L., & Gligor, V. D. (2002). *A key-management scheme for distributed sensor networks.* Paper presented at the Proceedings of the 9th ACM conference on Computer and communications security.

Kavyashree, B., Girijamba, D. L., & Kavya, A. P. (2016). Outline of Modified Menezes Vanstone Elliptic Curve

Cryptography Algorithm. *International Research Journal of Engineering and Technology 3*(12), 1044–1048.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203–209.

Malik, M. Y. (2010). *Efficient implementation of elliptic curve cryptography using low-power digital signal processor.* Paper presented at the 2010 The 12th International Conference on Advanced Communication Technology (ICACT).

Maqsood, F., Ahmed, M., Ali, M. M., & Shah, M. A. (2017). Cryptography: A comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications, 8*(6), 442–448.

Miller, V. S. (1985). *Use of elliptic curves in cryptography.* Paper presented at the Conference on the theory and application of cryptographic techniques.

Pitchaiah, M., & Daniel, P. (2012). Implementation of advanced encryption standard algorithm.

Stinson, D. R., & Paterson, M. (2018). *Cryptography: Theory and practice*: CRC press.

Trappe, W. (2006). *Introduction to cryptography with coding theory*: Pearson Education India.

Wang, H., Sheng, B., Tan, C. C., & Li, Q. (2008). *Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control.* Paper presented at the 2008 The 28th International Conference on Distributed Computing Systems.