Journal of
Sensor and Actuator Networks

MDPI

Article

Implementation of Elliptic Curves in the Polynomial Blom Key Pre-Distribution Scheme for Wireless Sensor Networks and Distributed Ledger Technology

Siti Noor Farwina Mohamad Anwar Antony and Muhammad Fatihin Afiq Bahari *

School of Mathematical Sciences, Universiti Sains Malaysia, George Town 11800, Malaysia
* Correspondence: muhammadfatihinafiq96@gmail.com

Abstract: One of the challenges in securing wireless sensor networks (WSNs) is the key distribution; that is, a single shared key must first be known to a pair of communicating nodes before they can proceed with the secure encryption and decryption of the data. In 1984, Blom proposed a scheme called the symmetric key generation system as one method to solve this problem. Blom's scheme has proven to be $\lambda-$secure, which means that a coalition of $\lambda+1$ nodes can break the scheme. In 2021, a novel and intriguing scheme based on Blom's scheme was proposed. In this scheme, elliptic curves over a finite field are implemented in Blom's scheme for the case when $\lambda=1$. However, the security of this scheme was not discussed. In this paper, we point out a mistake in the algorithm of this novel scheme and propose a way to fix it. The new fixed scheme is shown to be applicable for arbitrary λ. The security of the proposed scheme is also discussed. It is proven that the proposed scheme is also $\lambda-$secure with a certain condition. In addition, we also discuss the application of this proposed scheme in distributed ledger technology (DLT).

Keywords: wireless sensor network (WSN); distributed ledger technology; key distribution scheme; Blom's scheme; elliptic curve; security

Citation: Antony, S.N.F.M.A.; Bahari, M.F.A. Implementation of Elliptic Curves in the Polynomial Blom Key Pre-Distribution Scheme for Wireless Sensor Networks and Distributed Ledger Technology. *J. Sens. Actuator Netw.* **2023**, *12*, 15. https://doi.org/10.3390/jsan12010015

Academic Editor: Jordi Mongay Batalla

Received: 14 November 2022
Revised: 8 December 2022
Accepted: 8 December 2022
Published: 9 February 2023

1. Introduction

A wireless sensor network (WSN) is a network that consists of sensors as nodes, and these sensors are connected to each other wirelessly. Privacy and security are humongous challenges in WSNs. It is no doubt important to create security mechanisms that are customized for WSNs [1].

Cryptography is one security mechanism. However, Gaubatz et al. in [2] mentioned that public-key cryptography is much more complex, requiring more memory and storage, and being both slower and a greater drainer of energy. These characteristics make public-key cryptography unsuitable to be used in most energy-constrained environments, such as WSNs.

In contrast, symmetric key cryptography methods are said to be more resource-efficient, and this makes them preferred for use in WSNs [1]. On the other hand, there are special cases where developers implement the public-key cryptography as a security mechanism, such as RSA [3] and elliptic curve cryptography [4] in resource-constrained sensors.

However, symmetric cryptography has a major disadvantage, which is the problem of key distribution; that is, the shared single key must first be known to the pair of communicating nodes before they can proceed with the secure encryption and decryption of the data [1].

The security of WSNs depends on the effective key distribution, which should be resistant to attacks [5]. Designing an effective key distribution scheme for a WSN is a challenging task due to the constraints on sensors such as energy, computation capability,

and memory [6]. If the key distribution scheme is not able to distribute the keys among sensor nodes in a WSN, then the entire WSN communication may be prone to attacks [7].

Key pre-distribution schemes are suitable to be implemented in WSNs to solve the key distribution problem [5,8]. In a key pre-distribution scheme, an offline trusted third-party installs a set of secret information in each node before the deployment of the nodes to their fields. After the deployment, the sensor nodes use the installed information to compute their common keys [5,8].

Consistent with this, in 1984, a famous key pre-distribution scheme, known as Blom's scheme, was developed [9]. Let λ be any positive integer. Blom's scheme is shown in [6] to be λ-secure, i.e., if at most λ nodes are compromised, then the whole network cannot be compromised and if $\lambda + 1$ nodes are compromised, then the whole network can be compromised. In 2021, Udin et al. [10] developed a novel key pre-distribution scheme, which implements elliptic curves over a finite field in Blom's scheme. However, Udin et al. [10] only presented the algorithm of the case where $\lambda = 1$ did not present the security of this developed scheme.

In addition to being used in WSNs, the concept of key distribution has also been implemented in the distributed ledger technology (DLT). In general, a DLT is based on three technologies, which are public key cryptography, distributed peer-to-peer networks, and consensus mechanisms [11]. Since public key cryptography is involved in DLT, key management for DLT is also important to securely distribute the keys among the nodes. Therefore, a novel key pre-distribution scheme is introduced in this paper that can be implemented in both WSN and DLT.

The objectives: This paper is based on the key pre-distribution scheme proposed in [10]. The objectives of this paper are listed below:

1. We propose a modified scheme that can be used for any arbitrary λ;
2. We discuss and prove the security of the proposed scheme against the coalition of the sensor nodes.

Our contribution: In this paper, we propose a novel key pre-distribution scheme. Specifically, we successfully implement elliptic curves over a prime field by fixing the proposed scheme in [10], and we show that the fixed scheme is applicable for arbitrary λ. We also prove that the proposed scheme is λ-secure. Our proposed scheme has full connectivity, supports the mobility of nodes in the network, has high scalability, and uses the elliptic curves group law and scalar multiplication in the calculation instead of just adding and multiplying integers. The comparison of our proposed scheme and other existing key distribution schemes that are based on Blom's scheme is discussed in Section 6.3. The proposed scheme is designed to be implemented in WSNs. In addition, this scheme can also be implemented in DLT.

The flow of the paper: The remainder of the paper is organized as follows: The literature review related to the proposed scheme is presented in Section 2. In Section 3, the preliminaries are covered. The proposed scheme is introduced in Section 4. The security of the proposed scheme is explained in Section 5. Lastly, Sections 6 and 7 provide the discussion and conclusion, respectively.

2. Literature Review

In this section, several related works will be described.

2.1. Application of Blom's Scheme in WSN

Blom [9] developed a famous symmetric matrix–base key pre-distribution scheme, which is often referred to as Blom's scheme. In Blom's scheme, any pair of nodes in a WSN is able to derive a pairwise secret key. In Blom's scheme, there are two important matrices involved, which are $(\lambda + 1) \times N$ matrix C and the $(\lambda + 1) \times (\lambda + 1)$ symmetric matrix D, where N is the total number of nodes and λ is a positive integer. Both matrices are defined to be over a finite field $\mathbb{F}_q$ of order q, where q is a prime power and $q > N$. Blom's scheme is briefly shown in Section 4.1.

Menezes et al. in [12] defined a key distribution scheme as λ-secure if, given a specified pair of users, any coalition of λ or fewer users (disjoint from the two), pooling their pieces, can do no better at computing the key shared by the two than a party that guesses the key without any pieces whatsoever.

By this logic, Blom's scheme becomes a λ-secure scheme. In other words, in Blom's scheme, if λ or less than λ nodes are compromised, then the system cannot be broken. Otherwise, if more than λ nodes are compromised, any adversaries can compute any keys of any pairs of other non-compromised nodes in the network. However, in order for Blom's scheme to achieve the λ-secure property, every $\lambda + 1$ column of matrix C must be linearly independent [13], where $\lambda + 1 \leq N$. It also makes sense to say that choosing a larger λ will imply higher security in Blom's scheme, but a larger λ requires more memory and computation.

Let N be the total number of nodes. Let U_s be the s node where $1 \leq s \leq N$. Lazos in [14] explained that the original Blom's scheme can be translated into polynomial form. Blom's scheme was originally proposed by Blom in matrix form, as discussed earlier. However, the translation of Blom's scheme into polynomial form is possible. If the polynomial form of Blom's scheme described in [14] is translated back into the original matrix form, it can be seen that matrix C is designed to be a Vandermonde matrix, as shown below.

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ r_{U_1} & r_{U_2} & \dots & r_{U_N} \\ (r_{U_1})^2 & (r_{U_2})^2 & \dots & (r_{U_N})^2 \\ \vdots & \vdots & \ddots & \vdots \\ (r_{U_1})^\lambda & (r_{U_2})^\lambda & \dots & (r_{U_N})^\lambda \end{bmatrix}$$

where $r_{U_1}, r_{U_2}, r_{U_3}, \cdots, r_{U_N} \in \mathbb{Z}_p$ (p is a prime).

Reddy [15] used Blom's scheme and proposed a method to generate matrix C. An $N \times N$ non-binary Hadamard matrix over $\mathbb{F}_p$, where p is a prime, is constructed first, where the entries of this matrix are only 1 and $p - 1$. The first $\lambda + 1$ rows and N columns of this matrix are selected as the rows and columns of matrix C. Using this type of Hadamard matrix to generate matrix C is proven to reduce the computation overhead and storage usage to store the columns of C in sensor nodes.

Khan et al. [16] mentioned that in the original Blom's scheme, $(\lambda + 1) \times N$ matrix C is a generator matrix of maximum distance separable (MDS) codes, where N is the total number of nodes. A modified scheme was proposed in [16], where they used maximum rank distance (MRD) codes instead of MDS codes. Khan et al. also mentioned that in MDS codes, the $(\lambda + 1) \times N$ matrix C has $\lambda + 1$ linearly independent columns where $\lambda + 1 \leq N$. In contrast, in MRD codes, $(\lambda + 1) \times N$ matrix C has N linearly independent columns. Khan et al. stated that this affects the security of the system, since if MDS codes are used, then an adversary needs to only compromise $\lambda + 1$ nodes in order to compromise the whole network. However, if MRD codes are used, then an adversary needs to capture nodes equal to the number of linearly independent columns of matrix C. Hence, using MRD codes instead of MDS increases the security parameter from $\lambda + 1$ to N.

Wang et al. [17] proposed a key pre-distribution scheme based on multiple key spaces, which combines balanced incomplete block designs (BIBD) and Blom's scheme. In [17], Wang et al. let $(\lambda + 1) \times N$ matrix C be a Vandermonde matrix generated by using the primitive element $s \in \mathbb{F}_q$, where $q > N$, as shown below.

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ s & s^2 & \dots & s^N \\ (s)^2 & (s^2)^2 & \dots & (s^N)^2 \\ \vdots & \vdots & \ddots & \vdots \\ (s)^\lambda & (s^2)^\lambda & \dots & (s^N)^\lambda \end{bmatrix}.$$

Wang et al. also mentioned that the base station randomly generates $n^2 + n + 1$ symmetric matrix D of size $(\lambda + 1) \times (\lambda + 1)$, where all of these symmetric matrices are called key spaces. Next, these key spaces are distributed to N nodes using hybrid BIBD designs. By using all of this information, two nodes establish the pairwise key in the key agreement algorithm. Wang et al. stated that this proposed scheme is also λ-secure, which is the same as the original Blom's scheme.

Hussain and Ibrahem in [18] proposed an efficient pairwise key management scheme for WSNs based on Blom's scheme. The alteration made in [18] was in the matrix C. Matrix C is generated using the circular matrix technique instead of the usual Vandermonde matrix or Hadamard matrix, as proposed in [15]. In [18], matrix C was designed using a circular matrix, and it was also proven that this method ensures that every $\lambda + 1$ column of matrix C is linearly independent where $\lambda + 1 \leq N$. In the circular matrix technique, let the columns be denoted by i and the rows by j, where $0 \leq i \leq N - 1$ and $0 \leq j \leq \lambda$. Let $C(j, i)$ be the j row and i column entry in matrix C. Hussain and Ibrahem let $C(j, i) = (i - j) \pmod N$. Hence, by obtaining matrix C and developing the secret symmetric matrix D as defined in the original Blom's scheme, the same Blom's scheme algorithm is used to calculate the pairwise keys of any two nodes in the network. It was also shown that this proposed scheme consumes lower energy as compared with Blom's scheme.

Belim and Belim [19] implemented simplex channels in Blom's key pre-distribution scheme. By referring to the polynomial form of Blom's scheme, as shown in [14], Belim and Belim used the function of three variables $f(x, y, s)$ instead of the function with two variables $f(x, y)$. Here, the variable s can accept two values (1 or -1), and these two values define the direction of the information stream between two communicating nodes. In the polynomial Blom scheme, the function $f(x, y)$ must be symmetric, i.e., $f(x, y) = f(y, x)$. However, for the function $f(x, y, s)$ in this proposed scheme, there are three requirements imposed, which are $f(x, y, 1) \neq f(y, x, 1), f(x, y, -1) \neq f(y, x, -1)$, and $f(x, y, 1) = f(y, x, -1)$. Belim and Belim [19] also proposed $f(x, y, s)$ as a possible function to be used. This proposed scheme actually refuses the idea of symmetric polynomials in the original Blom's scheme. In this scheme, the exchange of information becomes asymmetrical.

Udin et al. [10] proposed a modification of Blom's scheme, which applied elliptic curves over a finite field. Instead of using the matrix representation of Blom's scheme, Udin et al. used the polynomial representation of Blom's scheme, as shown in [14]. However, Udin et al. only applied the proposed scheme for the case where $\lambda = 1$, and the security of this proposed scheme was not discussed.

2.2. Application of Blom's Scheme in DLT

DLT can be classified into two main categories: permissionless DLT and permissioned DLT [20]. In permissionless DLT, the nodes can participate without a specific identity and in contrast, only a set of known or identified nodes can participate in permissioned DLT [20]. Hyperledger [21] and its variation, hyperledger fabric [22] (usually called fabric), are two examples of permissioned DLT, as mentioned in [20].

In the fabric, there are generally three types of nodes involved, which are the clients, the endorsing peers, and the orderers [20,23]. A membership service provider (MSP) is in charge in the fabric for associating the nodes with cryptography identities [20]. For example, if a node desires to join a network in the fabric, then MSP will give an identity to the node and allow the node to join the network. In other words, MSP maintains the permissioned nature of the fabric.

Since the use of cryptography is crucial in maintaining the security of the communication in the fabric, the keys of the nodes in the fabric have to be properly managed. Androulaki et al. [20] stated that the tools for key management in the fabric are also part of the MSP and by default, MSP in the fabric handles standard public key infrastructure (PKI) methods [20]. Albakri et al. [23] explained that all existing key establishment schemes or key distribution schemes in DLT networks are based on PKI, which is an interactive method that requires information to be exchanged and verified between nodes in order to

establish a key for secure communication. This unfortunately results in a long processing time for key establishment [23].

Therefore, Albakri et al. [23] proposed a novel key pre-distribution scheme that can be implemented specifically in the fabric. The proposed scheme in [23] uses Blom's scheme to establish the shared keys among the nodes in the fabric. Instead of using the matrix form of Blom's scheme, Albakri et al. used the polynomial form of Blom's scheme, which is the same as the form that was explained by Lazos in [14].

Since the proposed scheme in [23] is based on Blom's scheme, the data required by the nodes for key establishment are preloaded into the nodes by an offline third-party trusted authority (TA). Hence, if two nodes desire to establish a shared key to secure the communication between them, the nodes do not have to exchange or verify any information needed for key establishment, since the information was preloaded into the nodes before deployment. In other words, the pre-distribution method enables the nodes in the fabric to non-interactively establish keys with other nodes in the network. As a result, this reduces the processing time for the keys' establishment.

In [23], Albakri et al. used three symmetric polynomials, which are $f_i(x, y)$ where $i = 1, 2, 3$ for key establishment. These polynomials are the same as the polynomial in Blom's scheme, as described by Lazos in [14]. $f_1(x, y)$ is used for the establishment of the shared keys between the clients and the endorsing peers, $f_2(x, y)$ is used for the establishment of the shared keys between the clients and the orderers, and $f_3(x, y)$ is used for the establishment of the shared keys between the orderers and the endorsing peers. Albakri et al. also mentioned that their proposed scheme is the first polynomial-based key management scheme in DLT since the key management schemes of other DLTs are based on PKI. As a result, Albakri et al. proved that their proposed scheme is faster in processing compared with other DLT key management schemes, such as public-key schemes.

The implementation of Blom's scheme in the fabric or another permissioned DLT is a good idea since this can reduce and simplify the shared key establishment process, as proven in [23]. Another reason is that in the permissioned DLT, each node is known and given an identity before it joins the network. Therefore, the identities of the nodes can also be defined as pre-distributed information before deployment that can be used for the establishment process of the shared keys, after deployment using Blom's scheme.

3. Preliminaries

In this section, the preliminaries are discussed in order to allow us to understand and derive the next section.

3.1. Greatest Common Divisor

One important property of the greatest common divisor, as described in [24], is

Proposition 1. *If* $\gcd(a, b) = 1$ *and* $\gcd(a, c) = 1$, *then* $\gcd(a, bc) = 1$.

Proposition 1 will later be used in the proofs of Theorems 4 and 5.

3.2. Elliptic Curves

In this section, we define an elliptic curve and describe a few other basic studies related to elliptic curves, as explained in [25].

Definition 1. *Let K be a field with a characteristic other than 2 and 3. An elliptic curve, E, defined over K, is the graph of an equation of the form*

$$E : y^2 = x^3 + Ax + B$$

where $A, B \in K$. *The set of points with coordinates in field L, where* $K \subseteq L$ *on E, is denoted as* $E(L)$ *such that*

$$E(L) = \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}_\infty\}$$

where $\mathcal{O}_\infty$ is a point at infinity to the elliptic curve.

The point at infinity, $\mathcal{O}_\infty$, is a point sitting at the top or the bottom of the $y-$axis, and this point is the identity element in $E(L)$. In this paper, we work with E over a prime field, $\mathbb{F}_p$, where p is a prime and $p > 3$ (to avoid characteristics 2 and 3). We also do not allow E to have multiple roots, i.e., we want to make sure E has three distinct roots. The discriminant of E is $-4A^3 - 27B^2$, and this can be shown easily since E is cubic. Therefore, it is compulsory to make sure that $4A^3 + 27B^2 \not\equiv 0 \pmod{p}$ if E is defined over $\mathbb{F}_p$.

Another important idea for elliptic curves over a finite field, $E(\mathbb{F}_p)$, is that they form additive abelian finite groups with $\mathcal{O}_\infty$ as the identity element, since this satisfies the group axioms [25]. Therefore, the order of $E(\mathbb{F}_p)$ is the number of points on E denoted as $|E(\mathbb{F}_p)|$, and the order of point P, such that $P \in E(\mathbb{F}_p)$ is the smallest integer $k > 0$ such that $kP = \mathcal{O}_\infty$.

In Section 4.2, we explore the scalar multiplication on elliptic curves over a finite field. Theorem 1 below was described in [26] and is essential in proving Theorem 3.

Theorem 1. *Let G be a finite group.*

1. *Let H be any subgroup of G. The order of H divides the order of G;*
2. *Let $g \in G$. The order of g divides the order of G.*

3.3. Lagrange Interpolation Polynomial

In the proof of Theorem 4, we will use the bivariate Lagrange interpolation. Before that, let us take a look at the Lagrange interpolation polynomial, as explained in [27], in Theorem 2.

Theorem 2. *Let*

$$(x_1, f(x_1)), (x_2, f(x_2)), \cdots, (x_{n+1}, f(x_{n+1}))$$

be points, such that x_i is distinct for $1 \leq i \leq n+1$ and $f(x_i)$ is a value corresponding to x_i. A unique polynomial $P(x)$ of degree at most n exists with

$$P(x_i) = f(x_i), \quad \text{for each } i \in \{1, 2, \cdots, n+1\}.$$

This polynomial is given by

$$P(x) = \sum_{i=1}^{n+1} \left(f(x_i) \prod_{h=1, h\neq i}^{n+1} \frac{x - x_h}{x_i - x_h} \right).$$

4. Materials and Methods

In this section, we first briefly present the original Blom scheme and the alteration of Blom's scheme made in [10] in Section 4.1. We also present Theorem 3 in Section 4.2, which plays a crucial role in proving the security of the proposed scheme. The proposed scheme and an example are shown in Sections 4.3 and 4.4, respectively.

4.1. Blom's Key Pre-Distribution Scheme

As explained in [9,12,13], Blom's original scheme is described here. Let N be the total number of sensor nodes in the WSN. Let λ be a positive integer. λ is also an indicator such that as long as not more than λ nodes are compromised, the network is perfectly secure (we call this the λ-secure property).

1. Before the deployment of the sensor nodes, an offline key distribution center will first construct a $(\lambda + 1) \times N$ matrix C over a finite field $\mathbb{F}_q$ of order q, where q is a prime power and $q > N$. Matrix C is publicly known, which means any sensors and adversaries are allowed to know C. Let c_i be the ith column of matrix C, where $1 \leq i \leq N$. Note that c_i is a $(\lambda + 1)$-tuple over $\mathbb{F}_q$. Column c_i is assigned to node U_i.

2. Then, the key distribution center will create a random $(\lambda+1)\times(\lambda+1)$ symmetric matrix D over $\mathbb{F}_q$. Matrix D must be kept secret, which means any sensors and adversaries are not allowed to know D.
3. The key distribution center will compute an $N\times(\lambda+1)$ matrix M such that $M=(D\cdot C)^T$, where $(D\cdot C)^T$ is the transpose of $(D\cdot C)$.
4. Let m_i be the i row of matrix M, where $1\leq i\leq N$. Note that m_i is a $(\lambda+1)$-tuple over $\mathbb{F}_q$. The key distribution center will then give m_i to node U_i over a secure channel.
5. Let us say node U_i wants to communicate with node U_j. Both will compute the same key, as follows:
   - Node U_i will compute $m_i\cdot c_j$, which we call $k_{i,j}$. Note that $k_{i,j}$ is a single element in $\mathbb{F}_q$.
   - Node U_j will compute $m_j\cdot c_i$, which we call $k_{j,i}$. Note that $k_{j,i}$ is a single element in $\mathbb{F}_q$.

Note that $k_{i,j}$ is the (i,j) entry of $N\times N$ matrix K where $K=M\cdot C$ and $k_{j,i}$ is the (j,i) entry of matrix K. Note that K is a symmetric matrix, since

$$K=M\cdot C=(D\cdot C)^T\cdot C=C^T\cdot D^T\cdot C=C^T\cdot D\cdot C=C^T\cdot M^T=(M\cdot C)^T=K^T.$$

Since K is symmetric, it is clear that $k_{i,j}=k_{j,i}$. Therefore, node U_i and node U_j have computed the same key.

Udin et al. [10] proposed a scheme based on Blom's scheme for the case $\lambda=1$. Let N be the total number of nodes. Let U_s be the s node where $1\leq s\leq N$. If the scheme proposed in [10] is translated back into matrix form, it can be seen that the points of the elliptic curve over a finite field $\mathbb{F}_p$ (or $\mathbb{Z}_p$) can be defined as the entries in the symmetric matrix D, and matrix C was defined as a Vandermonde matrix, as shown below

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ r_{U_1} & r_{U_2} & r_{U_3} & \dots & r_{U_N} \\ (r_{U_1})^2 & (r_{U_2})^2 & (r_{U_3})^2 & \dots & (r_{U_N})^2 \\ (r_{U_1})^3 & (r_{U_2})^3 & (r_{U_3})^3 & \dots & (r_{U_N})^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (r_{U_1})^\lambda & (r_{U_2})^\lambda & (r_{U_3})^\lambda & \dots & (r_{U_N})^\lambda \end{bmatrix}$$

where $r_{U_1}, r_{U_2}, r_{U_3}, \cdots, r_{U_N}\in\mathbb{Z}_p$ and is distinct where p is the prime used in the prime field $\mathbb{F}_p$, in which the elliptic curve has been defined. $r_{U_1}, r_{U_2}, r_{U_3}, \cdots, r_{U_N}$ represent the public key of node $U_1, U_2, U_3, \cdots, U_N$, respectively. In this paper, we studied Blom's scheme and the scheme proposed in [10]. We proposed a modified scheme that can be applied to all positive integers λ, and the security of the scheme for arbitrary λ was also discussed. We modified the second-row entries in the Vandermonde matrix to be over modulo $|E(\mathbb{F}_p)|$, which is the number of points in $E(\mathbb{F}_p)$ or the order of $E(\mathbb{F}_p)$ instead of the integers modulo p, $\mathbb{Z}_p$. This is because in order to prove the security of this proposed scheme, the calculation over modulo $|E(\mathbb{F}_p)|$ has to be made instead of modulo p. The modified scheme was proposed in polynomial form as shown in [14] instead of in matrix form. In proving the security of the modified scheme, we used the bivariate Lagrange interpolation polynomial to calculate the secret polynomial to show that the coalition of $\lambda+1$ nodes can break the scheme. The univariate Lagrange interpolation polynomial is shown in Theorem 2. Based on this univariate Lagrange interpolation, we managed to derive the bivariate Lagrange interpolation that was used in proving Theorem 4.

4.2. Scalar Multiplication on Elliptic Curves over Finite Field

When discussing the security of the proposed scheme, the scalars of points on E can be reduced to modulo $|E(\mathbb{F})|$, i.e., the order of $E(\mathbb{F})$. This result comes from Theorem 3.

Theorem 3. *Let E be an elliptic curve over a finite field, F_q, and the order of $E(\mathbb{F}_q)$ be n, where n can be prime or composite. Let $P \in E(\mathbb{F}_q)$. If $a \equiv b \pmod{n}$ for integers a and b, then $aP = bP$.*

Proof of Theorem 3. Let m be the order of P. We also know from Theorem 1 that $m \mid n$, and this implies $n = km$ for some integer k. Since $a \equiv b \pmod{n}$, $a \equiv b \pmod{km}$, and this implies $a = hkm + b$ for some integer h. Hence,

$$aP = (hkm + b)P = hkmP + bP = hk\mathcal{O}_\infty + bP = bP.$$

□

4.3. Proposed Algorithm for Arbitrary λ

The proposed algorithm for arbitrary λ is shown in this section. The notations used for this scheme are listed in Table 1 below.

Table 1. Notations used in the proposed scheme.

Notation	Description
p	A prime
$\mathbb{F}_p$	Finite field with p elements
N	The total number of nodes
λ	A positive integer
$\gcd(a, b)$	The greatest common divisor of integers a and b
E	An elliptic curve defined over field K of form E: $y^2 = x^3 + Ax + B$ where $A, B \in K$
$E(L)$	The set of points with coordinates in some field L on E, i.e., $E(L) = \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}_\infty\}$ where $K \subseteq L$, and K is the field in which E is defined over
$\lvert E(\mathbb{F}_p)\rvert$	The number of points on E
$\mathbb{Z}_{\lvert E(\mathbb{F}_p)\rvert}$	Integers modulo $\lvert E(\mathbb{F}_p)\rvert$
P	A point on E
$\mathcal{O}_\infty$	Point at infinity on E
$f(x, y)$	A secret symmetric bivariate polynomial known only by the trusted authority
U_s	The sth node where $1 \leq s \leq N$
r_{U_s}	The public key of node U_s used in the proposed scheme where $1 \leq s \leq N$
$g_{U_s}(x)$	$f(x, r_{U_s})$, i.e., secret information given to node U_s where $1 \leq s \leq N$
$K_{U_sU_t}$	$f(r_{U_s}, r_{U_t})$, i.e., the shared key between node U_s and node U_t where $1 \leq s \leq N$, $1 \leq t \leq N$ and $s \neq t$

The algorithm of the proposed scheme for arbitrary λ is shown below:

1. Let p be a prime greater than 3, and p is publicly known to all. Let N be the total number of nodes. Let U_s be the s node where $1 \leq s \leq N$. The trusted authority (TA) chooses an elliptic curve E over prime field $\mathbb{F}_p$ such that

$$E : y^2 = x^3 + Ax + B$$

where $A, B \in \mathbb{F}_p$ and $4A^3 + 27B^2 \not\equiv 0 \pmod{p}$. The elliptic curve is known publicly. Let $E(\mathbb{F}_p)$ be the set of points on E such that

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}_\infty\}$$

where $\mathcal{O}_\infty$ is a point at infinity to the elliptic curve. Let $|E(\mathbb{F}_p)|$ be the number of elements in $E(\mathbb{F}_p)$, and note that $|E(\mathbb{F}_p)|$ can be either a prime or a composite. It is compulsory to make sure that $|E(\mathbb{F}_p)| > N$, because each node must be given a distinct public key, where these public keys are elements in the integer modulo $|E(\mathbb{F}_p)|$.

2. $\mathbb{Z}_{|E(\mathbb{F}_p)|}$ is the set of integers modulo $|E(\mathbb{F}_p)|$. TA selects an element $r_{U_s} \in \mathbb{Z}_{|E(\mathbb{F}_p)|}$ for node U_s, which is also made public such that $r_{U_s} \neq r_{U_t}$ for $s \neq t$.
3. Let $\lambda \in \{1, 2, 3, ...\}$. For $0 \leq i, j \leq \lambda$, the TA chooses random points $P_{ij} \in E(\mathbb{F}_p)$ where $P_{ij} = (x_{ij}, y_{ij})$ such that $P_{ij} = P_{ji}$ and forms the polynomial

$$f(x, y) = \sum_{i=0}^{\lambda} \sum_{j=0}^{\lambda} P_{ij} x^i y^j.$$

The chosen P_{ij} and the polynomial f above are privately known only by the TA. The polynomial f is symmetric, i.e., $f(x, y) = f(y, x)$. The number of points P_{ij} to be chosen by the TA depends on the value of λ, where

$$\text{The number of points } P_{ij} = \frac{(\lambda + 1)(\lambda + 2)}{2}.$$

4. For each node U_s, the TA computes

$$g_{U_s}(x) = f(x, r_{U_s}).$$

The TA then privately sends $g_{U_s}(x)$ to node U_s over a secure channel. Note that node U_s only knows $g_{U_s}(x)$ and does not know the coefficients P_{ij}. $g_{U_s}(x)$ is privately known only by the TA and node U_s. Note that the scalar of each point can be reduced to modulo $|E(\mathbb{F}_p)|$ based on Theorem 3.
5. If two nodes, U_1 and U_2, want to communicate with each other, they individually compute the common key (shared key), $K_{U_1U_2}$ (the same as $K_{U_2U_1}$), where node U_1 computes

$$K_{U_1U_2} = g_{U_1}(r_{U_2})$$

and node U_2 computes

$$K_{U_2U_1} = g_{U_2}(r_{U_1}).$$

Note that $K_{U_1U_2} = K_{U_2U_1} = f(r_{U_1}, r_{U_2})$.

4.4. Example for $\lambda = 2$

Let N be the total number of nodes. Let U_s be the s node where $1 \leq s \leq N$. Let us say that there are three nodes, namely U_1, U_2, and U_3.

1. Let $p = 11$ and p be publicly known to all. TA chooses an elliptic curve E over prime field $\mathbb{F}_{11}$ such that

$$E : y^2 = x^3 + x + 6$$

where $4(1)^3 + 27(6)^2 \not\equiv 0 \pmod{11}$. The elliptic curve is known publicly. Let $E(\mathbb{F}_{11})$ be the set of points on E.
2. Note that $|E(\mathbb{F}_{11})| = 13$, which is a prime. TA selects an element $r_{U_s} \in \mathbb{Z}_{|E(\mathbb{F}_p)|}$ for node U_s, which is also made public such that $r_{U_s} \neq r_{U_t}$ for $s \neq t$, as shown below.

$$r_{U_1} = 10,$$
$$r_{U_2} = 7,$$
$$r_{U_3} = 1.$$

3. Let $\lambda = 2$. For $0 \leq i, j \leq 2$, the TA chooses random points $P_{ij} \in E(\mathbb{F}_{11})$ where $P_{ij} = (x_{ij}, y_{ij})$ such that $P_{ij} = P_{ji}$, as shown below.

$$P_{00} = (2, 4), P_{10} = P_{01} = (5, 9),$$
$$P_{11} = (8, 3), P_{12} = P_{21} = (3, 5),$$
$$P_{22} = (7, 2), P_{02} = P_{20} = (10, 9).$$

The TA then forms the secret polynomial $f(x, y)$, as shown below.

$$\begin{aligned} f(x,y) &= \sum_{i=0}^{2}\sum_{j=0}^{2} P_{ij}x^i y^j \\ &= P_{00}x^0y^0 + P_{01}x^0y^1 + P_{02}x^0y^2 + P_{10}x^1y^0 + P_{11}x^1y^1 + P_{12}x^1y^2 + P_{20}x^2y^0 + P_{21}x^2y^1 + P_{22}x^2y^2 \\ &= (2,4) + (5,9)y + (10,9)y^2 + (5,9)x + (8,3)xy + (3,5)xy^2 + (10,9)x^2 + (3,5)x^2y + (7,2)x^2y^2. \end{aligned}$$

4. For node U_1, the TA computes

$$\begin{aligned} g_{U_1}(x) &= f(x, r_{U_1} = 10) \\ &= P_{00} + P_{01}(r_{U_1}) + P_{02}(r_{U_1})^2 + P_{10}x + P_{11}(r_{U_1})x + P_{12}(r_{U_1})^2x + P_{20}x^2 + P_{21}(r_{U_1})x^2 + P_{22}(r_{U_1})^2x^2 \\ &= (3,5) + (10,9)x + (10,9)x^2. \end{aligned}$$

For node U_2, the TA computes

$$\begin{aligned} g_{U_2}(x) &= f(x, r_{U_2} = 7) \\ &= P_{00} + P_{01}(r_{U_2}) + P_{02}(r_{U_2})^2 + P_{10}x + P_{11}(r_{U_2})x + P_{12}(r_{U_2})^2x + P_{20}x^2 + P_{21}(r_{U_2})x^2 + P_{22}(r_{U_2})^2x^2 \\ &= (8,8) + (3,5)x + (3,6)x^2. \end{aligned}$$

For node U_3, the TA computes

$$\begin{aligned} g_{U_3}(x) &= f(x, r_{U_3} = 1) \\ &= P_{00} + P_{01}(r_{U_3}) + P_{02}(r_{U_3})^2 + P_{10}x + P_{11}(r_{U_3})x + P_{12}(r_{U_3})^2x + P_{20}x^2 + P_{21}(r_{U_3})x^2 + P_{22}(r_{U_3})^2x^2 \\ &= (7,9) + (10,9)x + (5,9)x^2. \end{aligned}$$

The TA then privately sends $g_{U_1}(x)$, $g_{U_2}(x)$, and $g_{U_3}(x)$ to nodes U_1, U_2, and U_3, respectively, over a secure channel. Note that the scalar of each point can be reduced to modulo $|E(\mathbb{F}_{11})|$ based on Theorem 3.

5. If U_2 and U_3 want to communicate with each other, they individually compute the common key (shared key), $K_{U_2U_3}$ (the same as $K_{U_3U_2}$), where node U_2 computes

$$\begin{aligned} K_{U_2U_3} &= g_{U_2}(r_{U_3}) \\ &= (8,8) + (1)(3,5) + (1^2)(3,6) \\ &= (8,8) \end{aligned}$$

and node U_3 computes

$$\begin{aligned} K_{U_3U_2} &= g_{U_3}(r_{U_2}) \\ &= (7,9) + (7)(10,9) + (7^2)(5,9) \\ &= (8,8). \end{aligned}$$

Note that $K_{U_2U_3} = K_{U_3U_2} = f(r_{U_2}, r_{U_3})$.

Let us say that an adversary wants to attack this scheme. We conjecture that a coalition of $\lambda + 1 = 3$ will break the scheme and the secret polynomial $f(x, y)$ can be obtained by the adversary. Assume that the adversary has compromised node U_1, node U_2, and node U_3. By compromising U_1, U_2, and U_3, the adversary obtains

$$\begin{aligned} r_{U_1} &= 10, \ g_{U_1}(x) = (3,5) + (10,9)x + (10,9)x^2, \\ r_{U_2} &= 7, \quad g_{U_2}(x) = (8,8) + (3,5)x + (3,6)x^2, \\ r_{U_3} &= 1, \quad g_{U_3}(x) = (7,9) + (10,9)x + (5,9)x^2. \end{aligned}$$

The adversary then uses the bivariate Lagrange interpolation polynomial as shown on the next page. Note that the scalars can be reduced to modulo $|E(\mathbb{F}_{11})| = 13$.

$$
\begin{aligned}
f(x,y) &= \sum_{j=1}^{\lambda+1=3} \left(g_{U_j}(x) \prod_{h=1,h\neq j}^{\lambda+1=3} \frac{y - r_{U_h}}{r_{U_j} - r_{U_h}} \right) \\
&= g_{U_1}(x)\frac{(y-7)(y-1)}{(10-7)(10-1)} + g_{U_2}(x)\frac{(y-10)(y-1)}{(7-10)(7-1)} + g_{U_3}(x)\frac{(y-10)(y-7)}{(1-10)(1-7)} \\
&= g_{U_1}(x)\frac{y^2-8y+7}{27} + g_{U_2}(x)\frac{y^2-11y+10}{-18} + g_{U_3}(x)\frac{y^2-17y+70}{54} \\
&= ((3,5)+(10,9)x+(10,9)x^2)(y^2+5y+7) + ((8,8)+(3,5)x+(3,6)x^2)(5y^2+10y+11) \\
&\quad + ((7,9)+(10,9)x+(5,9)x^2)(7y^2+11y+9) \\
&= (10,9)y^2 + (5,9)y + (2,4) + (3,5)xy^2 + (8,3)xy + (5,9)x + (7,2)x^2y^2 + (3,5)x^2y + (10,9)x^2,
\end{aligned}
$$

which is exactly the same as the original $f(x,y)$. Thus, the adversary can compute any keys of any pairs of nodes by using $f(x,y)$.

5. Results

As we have seen from the examples in the previous section, $|E(\mathbb{F}_p)|$ can be either prime or composite, and this depends on the elliptic curve E chosen. We also restrict the public key for each user U_s, which is denoted by r_{U_s}, in that it must be an integers modulo $\mathbb{Z}_{|E(\mathbb{F}_p)|}$, i.e., $r_{U_s} \in \mathbb{Z}_{|E(\mathbb{F}_p)|}$. If an adversary compromises $\lambda+1$ nodes, the adversary can use the bivariate Lagrange interpolation polynomial to derive the secret polynomial $f(x,y)$. In the interpolation calculation, the adversary must reduce the scalars of points to modulo $|E(\mathbb{F}_p)|$ in order to obtain the polynomial $f(x,y)$. As we have seen in the example in Section 4.4, the adversary manages to obtain $f(x,y)$ since $|E(\mathbb{F}_{11})| = 13$ is a prime. However, for the case where $|E(\mathbb{F}_p)|$ is a composite, some inverses of the scalars of the points modulo $|E(\mathbb{F}_p)|$ might not exist, and an adversary might not able to derive $f(x,y)$ in the bivariate Lagrange's interpolation. We provide the theorems in this section to discuss the security of the proposed scheme.

Theorem 4. *Let E be an elliptic curve over a prime field, $\mathbb{F}_p$, chosen for the proposed scheme, where $E(\mathbb{F}_p)$ is the set of all points on the elliptic curve E. Let N be the total number of nodes. Let U_s be the s node where $1 \leq s \leq N$. Let r_{U_s} be the public key of node U_s such that no two public keys are the same. If $\lambda+1$ users, namely $U_1, U_2, \cdots, U_{\lambda+1}$, are compromised, and*

$$\gcd\left((r_{U_s} - r_{U_t})(mod\ |E(\mathbb{F}_p)|), |E(\mathbb{F}_p)|\right) = 1$$

where $s \neq t$, then the adversary can derive the secret polynomial $f(x,y)$, and can thus calculate any pairwise keys of any non-compromised nodes.

Proof of Theorem 4. Assume that $\lambda+1$ users, namely $U_1, U_2, \cdots, U_{\lambda+1}$, are compromised. Let $r_{U_1}, r_{U_2}, \cdots, r_{U_{\lambda+1}}$ be distinct elements in $\mathbb{Z}_{|E(\mathbb{F}_p)|}$ and $g_{U_1}(x), g_{U_2}(x), \cdots, g_{U_{\lambda+1}}(x)$ be polynomials in $E(\mathbb{F}_p)[x]$. These polynomials are of degree at most λ, and not necessarily distinct. Now, we have a set of $\lambda+1$ data points

$$(g_{U_1}(x), r_{U_1}), (g_{U_2}(x), r_{U_2}), (g_{U_3}(x), r_{U_3}), \cdots, (g_{U_{\lambda+1}}(x), r_{U_{\lambda+1}}).$$

We find a polynomial that satisfies the data points above by using the bivariate Lagrange interpolation polynomial. Let

$$f(x,y) = \sum_{j=1}^{\lambda+1} \left(g_{U_j}(x)\ell_j(y) \right)$$

where

$$\ell_j(y) = \prod_{h=1, h\neq j}^{\lambda+1} \frac{y - r_{U_h}}{r_{U_j} - r_{U_h}}$$

for $1 \leq j \leq \lambda + 1$.

Note that, given the initial assumption that no two r_{U_s} are the same, $r_{U_j} - r_{U_h} \neq 0$ when $h \neq j$ and also

$$\gcd\left((r_{U_s} - r_{U_t}) (\mathrm{mod}\ |E(\mathbb{F}_p)|), |E(\mathbb{F}_p)|\right) = 1,$$

where $s \neq t$. By Proposition 1, we know that

$$\gcd\left(\prod_{h=1, h\neq j}^{\lambda+1} (r_{U_j} - r_{U_h}) (\mathrm{mod}\ |E(\mathbb{F}_p)|), |E(\mathbb{F}_p)|\right) = 1$$

for all $1 \leq j \leq \lambda + 1$. Hence, the inverse of

$$\prod_{h=1, h\neq j}^{\lambda+1} (r_{U_j} - r_{U_h}) \pmod{|E(\mathbb{F}_p)|}$$

always exists. Therefore, the proposed expression $f(x, y)$ is always well-defined.

In $\ell_j(y)$, there are λ factors in the product, and each factor contains one y. $g_{Uj}(x)$ is a polynomial of degree at most λ in x for all j. Therefore, $f(x, y)$, which is a sum of these λ-degree polynomials in both x and y, must be a polynomial of degree at most λ in both x and y.

Now, we want to show that $f(x, r_{U_i}) = g_{U_i}(x)$ for $1 \leq i \leq \lambda + 1$. Substituting r_{U_i} into $\ell_j(x)$, we obtain

$$\ell_j(r_{U_i}) = \prod_{h=1, h\neq j}^{\lambda+1} \frac{r_{U_i} - r_{U_h}}{r_{U_j} - r_{U_h}}.$$

Since the product omits the term where $h = j$, if $i = j$, then all terms that appear are

$$\frac{r_{U_j} - r_{U_h}}{r_{U_j} - r_{U_h}} = 1.$$

Furthermore, if $i \neq j$, then one of the terms (where $h = i$) in the product will be

$$\frac{r_{U_i} - r_{U_i}}{r_{U_j} - r_{U_i}} = 0.$$

This causes the entire product to become zero. Therefore,

$$\ell_j(r_{U_i}) = \delta_{ji} = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases},$$

where δ_{ji} is the Kronecker delta. Hence, we may conclude that

$$f(x, r_{U_i}) = \sum_{j=1}^{\lambda+1} \left(g_{U_j}(x)\ell_j(r_{U_i})\right) = \sum_{j=1}^{\lambda+1} \left(g_{U_j}(x)\delta_{ji}\right) = g_{U_i}(x).$$

By now, we know that $f(x, y)$ is a polynomial of degree at most λ in both x and y, where $f(x, r_{U_i}) = g_{U_i}(x)$ for $1 \leq i \leq \lambda + 1$.

Now, we show that $f(x, y)$ is unique. Note that x is a free variable. Therefore, x can be any constant. Let x be a constant c. Let there be another interpolating polynomial $g(c, y)$

of the degree, at most λ in y, where $g(c, r_{U_i}) = g_{U_i}(c)$. Assume that $g(c,y) \neq f(c,y)$. Note that $g(c, r_{U_i}) = f(c, r_{U_i})$ for $1 \leq i \leq \lambda + 1$.

Let $h(c,y) = g(c,y) - f(c,y)$. It follows that $h(c,y) = 0$ when $y = r_{U_i}$ for $1 \leq i \leq \lambda + 1$. This implies that $h(c,y)$ has $\lambda + 1$ zeros. However, $g(c,y) - f(c,y)$ is of the degree, at most, λ in y, and by the fundamental theorem of algebra, it can have at most λ zeros. We arrive at a contradiction. Therefore, $g(c,y) = f(c,y)$. The polynomial $f(c,y)$ is unique. Hence, the polynomial $f(x,y)$ is unique.

In the proposed scheme, the TA constructs a polynomial $f(x,y)$ of degree at most λ in both x and y and $f(x, r_{U_i}) = g_{U_i}(x)$ for $1 \leq i \leq \lambda + 1$. By the uniqueness of the bivariate Lagrange interpolating polynomial, the interpolating polynomial must be the same as the polynomial $f(x,y)$ constructed by the TA. □

Theorem 5. *Let E be an elliptic curve over a prime field, $\mathbb{F}_p$, chosen for the proposed scheme, where $E(\mathbb{F}_p)$ is the set of all points on the elliptic curve E. Let N be the total number of nodes. Let U_s be the s node where $1 \leq s \leq N$. Let r_{U_s} be the public key of node U_s such that no two public keys are the same. If at most λ users, namely $U_1, U_2, \cdots, U_k$, are compromised, where $k \leq \lambda$ and*

$$\gcd\left((r_{U_s} - r_{U_t})(mod\ \left|E(\mathbb{F}_p)\right|), \left|E(\mathbb{F}_p)\right|\right) = 1$$

where $s \neq t$, then the adversary cannot derive the secret polynomial $f(x,y)$ and, hence, any pairwise keys of any non-compromised nodes cannot be calculated by the adversary.

Proof of Theorem 5. Let k be the number of compromised nodes, where $k \leq \lambda$. Let an adversary compromise a set of k nodes, namely $U_1, U_2, \cdots, U_k$. Therefore the adversary has a set of k points

$$(g_{U_1}(x), r_{U_1}), (g_{U_2}(x), r_{U_2}), \cdots, (g_{U_k}(x), r_{U_k})$$

such that

$$g_{U_i}(x) = f(x, r_{U_i})$$

for $1 \leq i \leq k$.

Let $K_{U_{k+1}U_{k+2}}$ be the real shared key of non-compromised nodes U_{k+1} and U_{k+2}, and the adversary wants to calculate this key. Let $K^*_{U_{k+1}U_{k+2}}$ be the key conjectured by the adversary.

The adversary then defines the polynomial $f^*(x,y)$ as follows

$$f^*(x,y) = f(x,y) + (K^*_{U_{k+1}U_{k+2}} - K_{U_{k+1}U_{k+2}}) \prod_{1 \leq i \leq k} \frac{(x - r_{U_i})(y - r_{U_i})}{(r_{U_{k+1}} - r_{U_i})(r_{U_{k+2}} - r_{U_i})}.$$

Since

$$\gcd\left((r_{U_s} - r_{U_t})(\text{mod}\ \left|E(\mathbb{F}_p)\right|), \left|E(\mathbb{F}_p)\right|\right) = 1$$

where $s \neq t$, by Proposition 1, we know that

$$\gcd\left(\prod_{1 \leq i \leq k} (r_{U_{k+1}} - r_{U_i})(r_{U_{k+2}} - r_{U_i})\left|E(\mathbb{F}_p)\right|), \left|E(\mathbb{F}_p)\right|\right) = 1.$$

Therefore, the inverse of

$$\prod_{1 \leq i \leq k} (r_{U_{k+1}} - r_{U_i})(r_{U_{k+2}} - r_{U_i}) \pmod{\left|E(\mathbb{F}_p)\right|}$$

always exists. Hence, the proposed $f^*(x,y)$ is well-defined. Note that $f^*(x,y)$ has the same properties as $f(x,y)$, as shown below:

1. f^* is symmetric, i.e., $f^*(x,y) = f^*(y,x)$;

2. For $1 \leq i \leq k$, it holds that $f^*(x, r_{U_i}) = f(x, r_{U_i}) = g_{U_i}(x)$;
3. f^* has a degree of at most λ in both x and y, since $f(x, y)$ has a degree of at most λ in both x and y and $k \leq \lambda$.

Note also

$$f^*(r_{U_{k+1}}, r_{U_{k+2}}) = f(r_{U_{k+1}}, r_{U_{k+2}}) + K^*_{U_{k+1}U_{k+2}} - K_{U_{k+1}U_{k+2}} = K^*_{U_{k+1}U_{k+2}}.$$

Therefore, any values of $K^*_{U_{k+1}U_{k+2}}$ would eventually be consistent with the information that the adversary holds. For any possible value of the key, $K^*_{U_{k+1}U_{k+2}}$, there is a symmetric polynomial f^* that satisfies all three properties listed above, which are satisfied by the actual polynomial $f(x, y)$. Thus, if the adversary compromises at most λ nodes, the adversary cannot derive the secret polynomial $f(x, y)$. □

Theorem 6. *Let E be an elliptic curve over a prime field, $\mathbb{F}_p$, chosen for the proposed scheme, where $E(\mathbb{F}_p)$ is the set of all points on the elliptic curve E. Let N be the total number of nodes. Let U_s be the s node where $1 \leq s \leq N$. Let r_{U_s} be the public key of user U_s, such that no two public keys are the same. If*

$$\gcd\left((r_{U_s} - r_{U_t})(mod\ \left|E(\mathbb{F}_p)\right|), \left|E(\mathbb{F}_p)\right|\right) = 1$$

where $s \neq t$, then the proposed scheme is λ-secure.

Proof of Theorem 6. Given that

$$\gcd\left((r_{U_s} - r_{U_t})(\text{mod}\ \left|E(\mathbb{F}_p)\right|), \left|E(\mathbb{F}_p)\right|\right) = 1$$

where $s \neq t$, by Theorems 4 and 5, it is clear that the proposed scheme is λ-secure. □

6. Discussion

In this section, we discuss the possibility of applying our proposed scheme in DLT, acknowledging the pros and cons of the proposed scheme, and provide a comparison of the proposed scheme with several other related schemes.

6.1. The Application of the Proposed Scheme in Hyperledger Fabric DLT

In Section 2.2, we reviewed the key pre-distribution scheme proposed by Albakri et al. in [23]. By comparing the scheme proposed in this paper with the scheme proposed by Albakri et al., the obvious difference between these two can be seen from the coefficients of the polynomial $f(x, y)$. The coefficients in the three polynomials in the scheme proposed by Albakri et al. are the usual integers modulo p, where p is a prime, whereas the coefficients in the polynomial in our proposed scheme are basically points on elliptic curves over a prime field. In our scheme, it is also possible for us to generate three polynomials $f(x, y)$ by using a single elliptic curve over a prime field or three different elliptic curves over a prime field. Therefore, our proposed scheme is also possible to be implemented in the fabric. If our proposed scheme can be implemented in the fabric, then there exists the possibility that our scheme can be implemented in other DLT types as well, such as other variations of Hyperledger, i.e., Burrow, Indy, Sawtooth, and many more.

6.2. The Pros and Cons

All key distribution schemes have their own advantages and weaknesses. In this section, we discuss the pros and cons of our proposed scheme.

The advantages:

1. The proposed scheme has high connectivity, which means all nodes in the network are able to compute the shared keys among each other. In other words, the probability of sharing keys between nodes is 1.
2. The proposed scheme has high scalability, which means our proposed scheme can be used in networks with a huge number of nodes.

3. The proposed scheme supports the mobility of a node as long as the identities or the public keys of the new neighboring nodes are already stored in the moving node.
4. The information needed to establish the shared keys are stored in the nodes before deployment by an offline TA. Therefore, an adversary cannot attack the TA to obtain the secret polynomial $f(x, y)$ and the information required to compute the shared keys.
5. Elliptic curves are used in the proposed scheme, which increases the complexity of the calculation. Scalar multiplication and the group law of elliptic curves are implemented, instead of just adding and multiplying integers.
6. This scheme can be implemented in WSNs, and also possibly in DLT technology, as discussed earlier.

The disadvantages:

1. The proposed scheme does not support the flexibility requirement. In other words, if our proposed scheme is implemented in a network, then new joining nodes cannot simply join the network, since the identities or the public keys of the new nodes were not distributed in the existing nodes before deployment.
2. The proposed scheme is not secure against the capture of nodes. However, Albakri et al. [23] mentioned that there are several security mechanisms that can be utilized to eliminate this problem, such as tamper-proof mechanisms to protect the information in the nodes from an attacker, even if the attacker captures the nodes.

6.3. The Comparison of the Proposed Scheme with Other Existing Schemes

Before we proceed to the comparison, let us understand these key management requirements, shown in Table 2, as stated by Kandi et al. in [28].

Table 2. Key management requirements.

Requirement	Description
Resilience	Capturing devices must have a minimal impact on the network security
Connectivity	The probability of sharing keys between nodes must be maximum
Mobility	Moving devices must share keys with their new neighbors
Flexibility	Devices must be able to join or leave the network at any time
Scalability	Increasing the network size must not degrade performance

Next, in Table 3, we compare our proposed scheme with other key distribution schemes that are based on Blom's scheme.

Table 3. Comparison of the proposed scheme with existing work.

Scheme	Resilience	Connectivity	Mobility	Flexibility	Scalability	Use of Elliptic Curves	Value of λ
Blom [9]	λ	1	Yes (within network)	No	High	No	Any positive integer
Lazos [14]	λ	1	Yes (within network)	No	High	No	Any positive integer
Khan et al. [16]	N (total number of nodes)	1	Yes (within network)	Yes	High	No	Any positive integer
Wang et al. [17]	λ	1	Yes (within network)	Yes	High	No	Any positive integer
Udin et al. [10]	Unknown	1	Yes (within network)	No	High	Yes	1
Our scheme	λ	1	Yes (within network)	No	High	Yes	Any positive integer

7. Conclusions

In this paper, a key pre-distribution scheme is proposed that can be used in WSNs. The proposed scheme implements elliptic curves over a prime field in Blom's scheme, and is also based on the scheme that was introduced by Udin et al. in [10]. The proposed scheme is shown to be applicable for an arbitrary positive integer λ and is proven to be $\lambda-$secure (the same as the original Blom scheme), with the condition that

$$\gcd\left((r_{U_s} - r_{U_t})(\mathrm{mod}\ |E(\mathbb{F}_p)|), |E(\mathbb{F}_p)|\right) = 1$$

where $s \neq t$. However, if $|E(\mathbb{F}_p)|$ is a prime, then the condition above is automatically fulfilled.

In the proposed scheme, the probability of sharing keys between nodes is 1, the mobility of the nodes is supported as long as the nodes are still in the network, and the scheme is also applicable for huge networks. Unfortunately, this scheme does not support the flexibility requirement. In addition, the proposed scheme can also be applied in DLT technology, such as fabric.

In future research, the proposed scheme can be improved further. To satisfy the flexibility requirement, our scheme can be combined with a balanced incomplete block design (BIBD) as implemented by Wang et al. in [17]. Another possibility is that our scheme can apply the maximum rank distance (MRD) codes instead of the maximum distance separable (MDS). Furthermore, to protect the information in the captured nodes from the adversary, we can apply tamper-proof mechanisms in our scheme, as suggested in [23]. Finally, the implementation of our scheme in DLT can be studied further. We showed that our proposed scheme can be implemented in the fabric, and we believe that the proposed scheme can also be implemented in other types of DLT. This research should focus on permissioned DLT instead of permissionless DLT since in our scheme, the identities of the nodes in the network are important to the generation of the shared keys.

Author Contributions: Conceptualization, M.F.A.B. and S.N.F.M.A.A.; methodology, M.F.A.B. and S.N.F.M.A.A.; validation, M.F.A.B. and S.N.F.M.A.A.; writing—original draft preparation, M.F.A.B.; writing—review and editing, S.N.F.M.A.A.; project administration, S.N.F.M.A.A.; funding acquisition, S.N.F.M.A.A.; supervision, S.N.F.M.A.A.; resources, M.F.A.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Universiti Sains Malaysia under the short-term grant 391 scheme, project number 304/PMATHS/6315553.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We are very grateful to Hailiza Kamarulhaili for the insight and to Universiti Sains Malaysia for facilitating access to the resources used in this research.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

WSN	wireless sensor network
TA	trusted authority
DLT	distributed ledger technology
MSP	membership service provider
MRD	maximum rank distance
MDS	maximum distance separable
PKI	public key infrastructure

References

1. Dargie, W.; Poellabauer, C. *Fundamentals of Wireless Sensor Networks: Theory and Practice*, 1st ed.; John Wiley & Sons Ltd.: West Sussex, UK, 2010; ISBN 978-0-470-99765-9.
2. Gaubatz, G.; Kaps, J.-P.; Sunar, B. Public key cryptography in sensor networks–revisited. In Proceedings of the Security in Ad-hoc and Sensor Networks, Heidelberg, Germany, 6 August 2004; pp. 2–18.
3. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public–key cryptosystems. *Commun. ACM* **1983**, *26*, 96–99. [CrossRef]
4. Miller, V.S. Use of Elliptic Curves in Cryptography. In Proceedings of the Advances in Cryptology—CRYPTO '85, Santa Barbara, CA, USA, 18–22 August 1985; Lecture Notes in Computer Science; Williams, H.C., Ed.; Springer: Berlin/Heidelberg, Germany, 1985; Volume 218, pp. 417–426.
5. Ahlawat, P. Key distribution and management in wsn security: A state of the art. *Int. Innov. Technol. Explor. Eng. (IJITEE)* **2019**, *9*, 462–472. [CrossRef]
6. Zhang, J.; Varadharajan, V. Wireless sensor network key management survey and taxonomy. *J. Netw. Comput. Appl.* **2010**, *33*, 63–75. [CrossRef]
7. Premamayudu, B.; Rao, B.T.; Rao, K.V.; Peram, S.R. Key pre- distribution protocol for node to node for wireless sensor networks. *Ann. R. Soc. Cell Biol.* **2021**, *25*, 16769–16779.
8. Dargahi, T.; Javadi, H.H.; Hosseinzadeh, M. Application-specific hybrid symmetric design of key pre–distribution for wireless sensor networks. *Secur. Commun. Netw.* **2015**, *8*, 1561–1574. [CrossRef]
9. Blom, R. An optimal class of symmetric key generation systems. In Proceedings of the Advances in Cryptology EUROCRYPT 1984, Paris, France, 9–11 April 1984; Beth, T., Cot, N., Ingemarsson, I., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1985; Volume 209, pp. 335–338.
10. Udin, M.N.; Mohd Amin, F.A.; Abdul Malek, A.; Zulkifili, N.A.; Ghazali, N.A.; Mohd Ridzuwan, S.A. Implementation of Blom's key pre-distribution scheme by using elliptic curve cryptography. *Malays. J. Comput.* **2021**, *6*, 812–822.
11. El Ioini, N.; Pahl, C. A Review of Distributed Ledger Technologies. In Proceedings of the OTM 2018 Conferences, On the Move to Meaningful Internet Systems, Valletta, Malta, 22–26 October 2018; Panetto, H., Debruyne, C., Proper, H., Ardagna, C., Roman, D., Meersman, R., Eds.; Springer: Cham, Switzerland, 2018; pp. 277–288.
12. Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*, 1st ed.; CRC Press: Boca Raton, FL, USA, 1996; ISBN 0-8493-8523-7.
13. Du, W.; Deng, J.; Han, Y.S.; Varshney, P.K.; Katz, J.; Khalili, A. A pairwise key pre-distribution scheme for wireless sensor networks. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2005**, *8*, 228–258. [CrossRef]
14. Lazos, L. ECE596C: Key Distribution. Available online: https://uweb.engr.arizona.edu/~ece596c/lazos/lectures/lecture15.pdf (accessed on 12 October 2022).
15. Reddy, R.S. Key management in wireless sensor networks using a modified Blom's scheme. *arXiv* **2011**, arXiv:1103.5712. https://doi.org/10.48550/arXiv.1103.5712.
16. Khan, E.; Gabidulin, E.; Honary, B.; Ahmed, H. Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks. *J. IET Wirel. Sens. Syst.* **2012**, *2*, 108–114. [CrossRef]
17. Wang, Y.; Qin, Z.; Zhang, Q.; Wang, H.; Huang, J. A key pre- distribution scheme based on multiple key spaces in wireless sensor networks. In Proceedings of the 2014 Tenth International Conference on Computational Intelligence and Security, Kunming, China, 15–16 November 2014; pp. 652–656.
18. Hussain, A.W.; Ibrahem, M.K. An efficient pairwise and group key management scheme for wireless sensor network. *J. Int. J. Enhanc. Res. Sci. Technol. Eng.* **2015**, *4*, 25–31.
19. Belim, S.V.; Belim, S.Y. Implementation of simplex channels in the Blom's keys pre-distribution scheme. *J. Phys. Conf. Ser.* **2019**, *1210*, 1–5. [CrossRef]
20. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
21. Hyperledger. Available online: http://www.hyperledger.org (accessed on 29 November 2022).
22. Hyperledger Fabric. Available online: http://github.com/hyperledger/fabric (accessed on 29 November 2022).
23. Albakri, A.; Harn, L.; Maddumala, M. Polynomial-Based Lightweight Key Management in a Permissioned Blockchain. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 1–9.
24. Summary for Greatest Common Divisor. Available online: https://www.xiangsun.org/wp-content/uploads/2013/02/gcd.pdf (accessed on 12 October 2022).
25. Washington, L.C. *Elliptic Curves: Number Theory and Cryptography*, 2nd ed.; Chapman & Hall/CRC: Boca Raton, FL, USA, 2008; ISBN 978-1-4200-7146-7.
26. Pinter, C.C. *A Book of Abstract Algebra*, 2nd ed.; Dover Publications, Inc.: Mineola, NY, USA, 1990; ISBN 978-0-486-47417-5.

27. Burden, R.L.; Faires, J.D. *Numerical Analysis*, 9th ed.; Brooks/Cole, Cengage Learning: Boston, MA, USA, 2011; ISBN 978-0-538-73351-9.
28. Kandi, M.A.; Kouicem, D.E.; Doudou, M.; Lakhlef, H.; Bouabdallah, A.; Challal, Y. A decentralized blockchain-based key management protocol for heterogeneous and dynamic IoT devices. *Comput. Commun.* **2022**, *191*, 11–25. [CrossRef]