Two-Qubit Quantum Secret Sharing Scheme based on Symmetric Bivariate Polynomial

Manoj Kumar, Hardeep and Pratik Gupta, *Member, IAENG*

***Abstract*— This study presents a novel quantum secret sharing scheme that uses a double 2-level $(t,n)-$threshold approach, employing both two-qubit and symmetric bivariate polynomial techniques. In the key distribution step, the dealer employs a symmetric bivariate polynomial to produce shares for each participant. In contrast to prevailing methodologies, our proposed methodology yields a $t-1$ degree polynomial for each participant, hence enhancing its adaptability, feasibility, and ease of execution. Moreover, as a result of the augmented quantity of qubits, our technique has the capability to send a greater amount of information simultaneously. This scheme utilizes pairs of qubits, the fundamental units of quantum information, to encode and share the secret information. By employing symmetric bivariate polynomials, the scheme ensures both security and reliability in the sharing process. The security of the scheme relies on the principles of quantum mechanics, such as the no-cloning theorem and the inherent uncertainty principle, making it highly resistant to eavesdropping or unauthorized access. The utilization of symmetric bivariate polynomials enhances the efficiency and robustness of the secret sharing process, making it a promising approach in quantum cryptography for secure multi-party communication and data sharing.**

***Index Terms*— Quantum Secret Sharing, Symmetric Bivariate Polynomial, Shamir Secret Sharing Scheme, Unitary Operation.**

I. Introduction

Shamir [1] and Blakely [2] independently introduced the $(t,n)-$secret sharing schemes (SSS) for the first time in 1979. In an $(t,n)-$SS, Alice, acting as the dealer, divides the secret into many pieces and allocates them among a number of participants. This allocation ensures that each individual share possesses the ability to reconstruct the original secret, but any subset of shares less than a certain threshold is unable to do so. The SSS has emerged as a crucial element in many applications, such as cloud computing [3] and group communications [4]. polynomials, scheme [2] draws upon principles from geometry, and scheme [5] is founded on the chinese remainder theorem(CRT) methodology. The issue of data security and privacy has garnered considerable attention, leading to a heightened interest in the field of cryptography.

Manuscript received May 18, 2023; revised July 13, 2024.

Manoj Kumar is an Associate Professor at Department of Mathematics and Statistics, Gurukula Kangri (Deemed to be University), Haridwar-249404, Uttarakhand, India. (E-mail: sdmkg1@gmail.com)

Hardeep is a Ph.D. candidate at Department of Mathematics and Statistics, Gurukula Kangri (Deemed to be University), Haridwar-249404, Uttarakhand, India. (Corresponding author to provide phone: +919718928006; E-mail: hardeeppawariya1994@gmail.com).

Pratik Gupta is an Assistant Professor at Department of Applied Mathematics, School of Vocational Studies and Applied Science, Gautam Buddha University, Greater Noida, India. (E-mail: pratikgupta1810@gmail.com)

Significant advancement have been achieved in the field of quantum cryptography, which integrates principles from quantum theory with conventional cryptographic techniques. The primary goal of this discipline is to use quantum phenomena exclusively for the purpose of facilitating information transfer that is unconditionally secure. Quantum encryption has attracted considerable attention in recent years because of its inherent secrecy.

Quantum cryptography approaches, which are rooted in the fundamental laws of quantum physics, have the potential to provide unconditional security. In contrast, traditional cryptographic methods often depend on computational security, which is reliant on the efficiency of computer systems. Therefore, the use of quantum-information-assisted approaches for exchanging secrets among users is both more safe and attractive. Due to the fast progression of quantum technology, conventional classical SSSs have become inadequate in ensuring sufficient security measures. Consequently, the field has witnessed the emergence of quantum secret sharing (QSS) as an alternative solution.

Quantum cryptography encompasses several areas, including fibre network design [6] and quantum secure transportation networks [7]. These fields extensively rely on QSS techniques, which have gained significant attention from researchers. The quantum state storage and computation system is identified as one of the dependable and robust solutions for QSS. Some findings indicate that the QSS system, presented by Hillery et al. in 1999 [8], used the GHZ state. Subsequently, Cleve et al. [9] put up a threshold QSS that incorporated a quantum error-correcting system.

QSS relies on the fundamental tenets of quantum physics since the secret is communicated, distributed, and recovered via quantum processes. Threshold QSS, as discussed in references [10] and [11], is a crucial approach within the field. Threshold SSSs have the capability to safeguard confidential information against unauthorized access in real-time instances. Furthermore, the task of sharing a quantum state presents greater difficulties compared to sharing a classical state, leading to a very limited amount of study on QSS in comparison to the sharing of classical state information. In our proposed methodology, Alice employs a symmetric bivariate polynomial to produce n shares. This process yields univariate polynomials to a certain degree $t-1$. Subsequently, Alice distributes each share to the relevant participants, following a similar approach as outlined in reference [1]. The subsequent sections of the paper are structured in the following manner: Section 2 presents an overview of the essential background and preliminary notions pertaining to our strategy. In Section 3, we elucidate the conceptualization of our suggested methodology. In Section 4, we present a demonstration of the validity of our approach

and provide proof of the accurate reconstruction of the original secret using the shares. In Section 5, we present specific instances and visual representations to facilitate comprehension of the pragmatic execution of our strategy. In Section 6, we analyze the security aspects of our scheme, ensuring that it is resilient against potential attacks. Section 7 compares our scheme with existing QSS approaches, highlighting its advantages and strengths. In the final Section 8, we summarize our work's key findings and contributions and offer concluding remarks.

II. PRELIMINARIES

This section comprises fundamental results and definitions concerning qubits and their mathematical foundations. These concepts are essential for comprehending the proposed scheme effectively.

A. Qubit Quantum State

A qubit $|\Phi\rangle$ is defined as

$$|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{... (1)}$$

where α and β are scalars (real or complex) and holds the following identity

$$|\alpha|^2 + |\beta|^2 = 1.$$

B. Two qubit quantum state

A two qubit quantum state is defined by

$$|\Phi\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle \quad \text{...(2)}$$

where α_i for $i = 1,2,3,4$ are scalars and they satisfy the following identity

$$\sum_{i=1}^{4} |\alpha_i|^2 = 1.$$

C. Sequence of two qubits

A two qubit sequence $\{|T_s\rangle : s = 1,2,...,m\}$ is defined as

$$|T_s\rangle = \alpha_{1s}|00\rangle + \alpha_{2s}|01\rangle + \alpha_{3s}|10\rangle + \alpha_{4s}|11\rangle \quad \text{...(3)}$$

where α_{is} for $i = 1,2,3,4$ are scalars and they satisfy the following identity

$$\sum_{i=1}^{4} |\alpha_{is}|^2 = 1 \text{ for } s = 1,2,3,...,m.$$

D. Unitary operator

A unitary operator for two-qubit quantum state is defined as

$$\begin{aligned} A(\phi) = {} & \cos(2\phi)|00\rangle\langle 00| - \sin(2\phi)|00\rangle\langle 11| \\ & + |10\rangle\langle 01| + |01\rangle\langle 10| \\ & + \sin(2\phi)|11\rangle\langle 00| + \cos(2\phi)|11\rangle\langle 11|. \end{aligned}$$

E. Symmetric bivariate polynomial (SBP)

A SBP of degree $t-1$ is defined as

$$\begin{aligned} g(x,y) = {} & c_{0,0} + c_{1,0}x + c_{0,1}y + c_{2,0}x^2 \\ & + c_{1,1}xy + c_{0,2}y^2 + ... + c_{t-1,0}x^{t-1} \\ & + c_{t-2,1}x^{t-2}y + ... + c_{0,t-1}y^{t-1} \end{aligned}$$

where $c_{i,j} = c_{j,i}; \forall i, j \in \{0,1,2,...,t-1\}$.

III. PROPOSED SCHEME

In this section, we propose a QSSS that utilizes an SBP $g(x,y)$ of degree $t-1$, where t is the threshold value. The scheme is divided into the following three phases:

A. Key Distribution Phase: In this phase, Alice (the dealer) generates private keys for herself and each participant using the following steps:

(1) Firstly, Alice chooses a random SBP $g(x,y)$ of the degree $t-1$ over finite field F_q such that

$$\begin{aligned} g(x,y) = {} & c_{0,0} + c_{1,0}x + c_{0,1}y \\ & + c_{2,0}x^2 + c_{1,1}xy + c_{0,2}y^2 + \\ & ... + c_{t-1,0}x^{t-1} + c_{t-2,1}x^{t-2}y \\ & + ... + c_{0,t-1}y^{t-1} \pmod q \end{aligned}$$

where $c_{i,j} \in F_q$ and $c_{i,j} = c_{j,i}; \forall i, j \in \{0,1,2,...,t-1\}$, and private value satisfies

$$S = [g(0,0) + b\, g(1,1)] \bmod q,\ b \in F_q.$$

(2) Alice calculates private shares $S_i(y) = g(x_i, y)$ polynomials of degree $t-1$, for participants $N_i,\ i = 1,2,3,...,n,\ (x_i \notin \{0,1\})$, where x_i is the public information associated with each participant N_i.

(3) Alice sends each share $S_i(y)$ to participants N_i secretly through quantum secure direct communication presented in [14]-[16].

B. Sharing of quantum states phase: In this phase, Alice wishes to distribute secret information $\{|T_s\rangle\}$ among n participants using the following steps:

(1) First, Alice generates a random sequence of two-qubits $\{|T_s\rangle\}$.

(2) Now, Alice embeds private value into $\{|T_s\rangle\}$ by performing a phase shift operation $A(\phi_0)$ on each quantum state of $\{|T_s\rangle\}$, where $\phi_0 = \dfrac{-\pi S}{q}$ and S is the private key for Alice. Then, each quantum state in $\{|T_s\rangle\}$ will be of the form $\{|T_s^0\rangle : |T_s^0\rangle = A(\phi_0)|T_s\rangle,\ p = 1,2,3,...,m\}$.

(3) For distributing $\{|T_s^0\rangle\}$, Alice chooses some decoy particles for eavesdropping detection from the following bell bases.

$$\alpha = \left\{ \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \right.$$

$$\left\{\frac{|01\rangle+|10\rangle}{\sqrt{2}}, \frac{|01\rangle-|10\rangle}{\sqrt{2}}\right\}.$$

(4) Next, Alice inserts some random decoy particles into the sequence of two qubits to get an expanded sequence, say $\left\{\left|T_s^{\,0}\right\rangle'\right\}$, then he observes each decoy particle's position and state $\left\{\left|T_s^{\,0}\right\rangle'\right\}$.

(5) After observing each decoy particle's position and state, Alice publicly announces the results and then sends $\left\{\left|T_s^{\,0}\right\rangle'\right\}$ to any participant N_i, $i=1,2,3,...,n,$ through quantum communication [14-16].

(6) Alice transfers the position and state of each decoy particle to N_i through [14-16]. Then N_i measures each decoy particle according to their bases in α and analyses each measurement result against publicly available states and positions.

(7) If the rate of error goes higher than the value of t, then the sequence $\left\{\left|T_s^{\,0}\right\rangle'\right\}$ is eliminated, and Alice begins a new procedure. Otherwise, process will continue.

With the help of the above steps, the dealer distributes the initial information $\left\{\left|T_s\right\rangle\right\}$ into n parts.

C. Recovery Phase: Suppose participants $\{N_1, N_2, N_3, ..., N_t\}$ wish to recreate the original information $\left\{\left|T_s\right\rangle\right\}$. For the recreation of $\left\{\left|T_s\right\rangle\right\}$, the following steps need to be done.

(1) As N_1 knows every decoy particle's position and state, so he deletes the decoy particles from $\left\{\left|T_s^{\,0}\right\rangle'\right\}$ to extract the sequence $\left\{\left|T_s^{\,0}\right\rangle\right\}$. Now, N_1 performs phase shift operator $A(\phi_1)$, $\phi_1=\frac{\pi C_1}{q}$ on each qutrit of sequen $\left\{\left|T_s^{\,0}\right\rangle\right\}$, to give a new sequence $\left\{\left|T_s^{\,1}\right\rangle\right\}$, where $\left|T_s^{\,1}\right\rangle = A(\phi_1)\left|T_s\right\rangle$. Then N_1 sends $\left\{\left|T_s^{\,1}\right\rangle\right\}$ to N_2.

(2) Now N_2 does the same as N_1 does in step (1). N_2 performs phase shift operator $A(\phi_2)$, $\phi_2=\frac{\pi C_2}{q}$ on $\left\{\left|T_s^{\,1}\right\rangle\right\}$ to obtain a new sequence $\left\{\left|T_s^{\,2}\right\rangle\right\}$, where $\left|T_s^{\,2}\right\rangle = A(\phi_2)\left|T_s^{\,1}\right\rangle$. Then N_2 sends $\left\{\left|T_s^{\,2}\right\rangle\right\}$ to N_3.

(3) Each remaining member, $N_s; s=3,4,...,t,$ now repeats the process as N_2 does in step (2). After the last participant N_t completes his phase shift operation $A(\phi_t)$, $\phi_t=\frac{\pi C_t}{q}$, where

$$C_t = S_t(0)\prod_{j=1,\,j\neq t}^{t}\frac{x_j}{x_j-x_t} + b\,S_t(1)\prod_{j=1,\,j\neq t}^{t}\frac{1-x_j}{x_t-x_j},$$

then we obtain $\left\{\left|T_s^{\,t}\right\rangle\right\}$, where

$$\begin{aligned}\left|T_s^{\,t}\right\rangle &= A(\phi_t)A(\phi_{t-1})...A(\phi_1)\left|T_s^{\,0}\right\rangle\\ &= A(\phi_t)A(\phi_{t-1})...A(\phi_1)A(\phi_0)\left|T_s^{\,0}\right\rangle\\ &= A(\phi_t+\phi_{t-1}+...+\phi_1+\phi_0)\left|T_s\right\rangle\\ &= \left|T_s\right\rangle.\end{aligned}$$

Hence, each t out of n participant can recover the original information successfully. The graphical representation of proposed method is drawn in Fig 1.

IV. Correctness

Theorem-1: In Shamir's SS, assume that every participant N_j has the information (x_j, y) which is public and shares $g(x_j, y)$, $j=1,2,3,...,k$, $n\geq k\geq t$. By summing each component $C_j=\left[S_j(0)\prod_{i=1,i\neq j}^{t}\frac{x_i}{x_i-x_j} + b\,S_j(1)\prod_{i=1,i\neq j}^{t}\frac{1-x_i}{x_j-x_i}\right]\bmod q$ any t participants can reconstruct the value

$$S=[g(0,0)+b\,g(1,1)]\bmod q.$$

That is,

$$\begin{aligned}S&=[g(0,0)+b\,g(1,1)]\bmod q\\ &=\sum_{j=1}^{t}C_j\,(\bmod q)=\sum_{j=1}^{t}\left[S_j(0)\prod_{i=1,i\neq j}^{t}\frac{x_i}{x_i-x_j} + b\,S_j(1)\prod_{i=1,i\neq j}^{t}\frac{1-x_i}{x_j-x_i}\right]\bmod q\end{aligned}$$

where $g(x_j, y)$ is SBP of degree $t-1$ over F_q, q is prime.

Proof- By Lagrange Interpolation,

$$g(x,y)=\sum_{j=1}^{t}g(x_j,y)\prod_{i=1,i\neq j}^{t}\frac{x-x_i}{x_j-x_i}.$$

We have,

$$g(0,0)=\sum_{j=1}^{t} g(x_j,0)\prod_{i=1,i\neq j}^{t}\frac{x_i}{x_i-x_j}$$

and

$$g(1,1)=\sum_{j=1}^{t} g(x_j,1)\prod_{i=1,i\neq j}^{t}\frac{1-x_i}{x_j-x_i}.$$

So,

$$\begin{aligned}&\sum_{j=1}^{t} C_j \pmod q\\ &=\sum_{j=1}^{t}\Bigg[S_j(0)\prod_{i=1,i\neq j}^{t}\frac{x_i}{x_i-x_j}\\ &\qquad +b\,S_j(1)\prod_{i=1,i\neq j}^{t}\frac{1-x_i}{x_j-x_i}\Bigg]\bmod q\\ &=\left[g(0,0)+b\,g(1,1)\right]\bmod q=S\,.\end{aligned}$$

This proves our theorem-1.

Theorem-2[13] The unitary operator applied on two-qubit quantum state satisfies the following relation

$$A(\phi_1+\phi_2)|T_s\rangle=A(\phi_1)A(\phi_2)|T_s\rangle.$$

Correctness of our scheme: Suppose each qubit's initial state in the sequence is $\{|T_s\rangle : s=1,2,3,...,m\}$. When dealer and any t out of n participants have completed their corresponding operations $A(\phi_k), k=0,1,...,t$, on $\{|T_s\rangle : s=1,2,...,m\}$, then the initial state $\{|T_s\rangle : s=1,2,...,m\}$ will be recovered, because of the equation below

$$\begin{aligned}&A\left(\phi_0+\sum_{k=1}^{t}\phi_k\right)|T_s\rangle\\ &=A\left(\frac{\pi}{q}\left(\sum_{k=1}^{t}C_k-S\right)\right)|T_s\rangle.\\ &=A(\mathbb{N}\pi)|T_s\rangle\\ &=|T_s\rangle\end{aligned}$$

V. Concrete Illustration of The Proposed Method

The following example, which is a $(3,5)-$threshold QSS scheme over a finite field F_7, will be used to justify our proposed schemes.

A. Key Distribution Phase

In this phase, Alice (dealer) produces private keys for himself and each participant with the help of the following steps:

(1) Dealer chooses a random SBP $g(x,y)=3+x+y+xy+x^2+y^2 \pmod 7$ of degree two over F_7, with the secret information

$$S=\left[g(0,0)+3g(1,1)\right]\bmod 7=6\,.$$

(2) Dealer chooses the public key $x_k=k+1$ for participant $N_k, k=1,2,3,4,5$. Then, dealer calculates $g_k=g(x_k,y)$ using the polynomial

$$g(x,y)=3+x+y+xy+x^2+y^2 \pmod 7$$

with the relation $g_k=g(x_k,y)$, as follows:

$$\begin{aligned}S_1&=g(x_1,y)=g(2,y)=2+3y+y^2\\ S_2&=g(x_2,y)=g(3,y)=1+4y+y^2\\ S_3&=g(x_3,y)=g(4,y)=2+5y+y^2\\ S_4&=g(x_4,y)=g(5,y)=5+6y+y^2\\ S_5&=g(x_5,y)=g(6,y)=3+y^2\,.\end{aligned}$$

(3) Now, dealer sends the shares $g_1=2+3y+y^2$, $g_2=1+4y+y^2$, $g_3=2+5y+y^2$, $g_4=5+6y+y^2$ and $g_5=3+y^2$ to the participants N_1, N_2, N_3, N_4 and N_5 respectively through [14-16].

B. Sharing of Quantum State Phase

In this phase, firstly dealer performs his unitary operation P, $\phi_0=\frac{-\pi S}{q}=\frac{-6\pi}{7}$ on the sequence of two-qubits $\{|T_s\rangle : s=1,2,...,m\}$. Then, he distributes the sequence into n members as we did in *Sharing of quantum states phase* of section III.

C. Recovery Phase

Suppose N_1, N_3 and N_5 wish to recover the secret information $\{|T_s\rangle : s=1,2,...,m\}$. For this, participants N_1, N_3 and N_5 respectively calculate C_1, C_2 and C_5 using interpolation method as follow:

$$\begin{aligned}C_1&=\Bigg[S_1(0)\prod_{i=3}^{t}\frac{x_i}{x_i-x_1}\\ &\qquad +b\,S_1(1)\prod_{i=3}^{t}\frac{1-x_i}{x_1-x_i}\Bigg]\bmod 7\\ &=\Bigg[2\frac{x_3}{x_3-x_1}\frac{x_5}{x_5-x_1}\\ &\qquad +18\frac{1-x_3}{x_3-x_1}\frac{1-x_5}{x_5-x_1}\Bigg]\bmod 7\\ &=3.\end{aligned}$$

$$C_3 = \left[S_3(0) \prod_{i=1, i\neq 3}^{t} \frac{x_i}{x_i - x_3} + b\, S_3(1) \prod_{i=1, i\neq 3}^{t} \frac{1-x_i}{x_3 - x_i} \right] \bmod 7$$
$$= \left[2 \frac{x_1}{x_1 - x_3} \frac{x_5}{x_5 - x_3} + 3 \frac{1-x_1}{x_3 - x_1} \frac{1-x_5}{x_3 - x_1} \right] \bmod 7$$
$$= 6.$$

$$C_5 = \left[S_5(0) \prod_{i=1, i\neq 5}^{t} \frac{x_i}{x_i - x_5} + b\, S_5(1) \prod_{i=1, i\neq 5}^{t} \frac{1-x_i}{x_5 - x_i} \right] \bmod 7$$
$$= \left[3 \frac{x_1}{x_1 - x_5} \frac{x_3}{x_3 - x_5} + 12 \frac{1-x_1}{x_5 - x_1} \frac{1-x_3}{x_5 - x_3} \right] \bmod 7$$
$$= 4.$$

Using these above values, we get

$$\phi_1 = \frac{\pi C_1}{q} = \frac{3\pi}{7},\ \phi_3 = \frac{\pi C_3}{q} = \frac{6\pi}{7},\ \phi_5 = \frac{\pi C_5}{q} = \frac{4\pi}{7}.$$

Now, N_1, N_3 and N_5 performs their corresponding unitary operations on encoded sequence $\left\{ \left| T_s^{\,0} \right\rangle : s = 1, 2, ..., m \right\}$..

Then, we get

$$\left| T_s^{\,3} \right\rangle = A(\phi_5) A(\phi_3) A(\phi_1) \left| T_s^{\,0} \right\rangle$$
$$= A(\phi_5) A(\phi_3) A(\phi_1) A(\phi_0) \left| T_s \right\rangle$$
$$= A(\phi_5 + \phi_3 + \phi_1 + \phi_0) \left| T_s \right\rangle$$
$$= A\left(\frac{4\pi}{7} + \frac{6\pi}{7} + \frac{3\pi}{7} - \frac{6\pi}{7} \right) \left| T_s \right\rangle$$
$$= \left| T_s \right\rangle.$$

Hence, 3 out of 5 participants can recover the initial information.

VI. Security

This study uses the Lagrange interpolation method and phase shift operation to construct a symmetric bivariate polynomial-based QSS scheme. Attacks are classified as either internal or external, depending on how a message is retrieved. This research focuses on external threats and investigates how an eavesdropper can acquire secret or large data without being caught. For internal attacks, the scheme investigates whether a single participant can rebuild the initial information on their own or whether a group of participants can do so when the number of participants is fewer than t.

External attack: This section will focus on the intercept-and-resend attack, a scenario where an unauthorized individual intercepts the quantum state transmitted by the dealer and retransmits a modified quantum state without notice. Before Alice transmits the sequence of quantum states to the individuals involved in sharing the quantum state phase, they must randomly introduce decoy particles into the sequence of quantum states.

$$\mu = \left\{ \mu_1 = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \mu_2 = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \right\},$$

$$\upsilon = \left\{ \upsilon_1 = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \upsilon_2 = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \right\}.$$

Alice keeps track of the participants' positions and communicates the sequence to them, instructing them to measure the particles in the bell bases according to the instructions and then checking the measurement results with them. Because an eavesdropper will be unfamiliar with the position and condition of the decoy particles, they may mismeasure them. For each decoy particle, an eavesdropper will be discovered with a probability of $1 - \left(\frac{5}{8}\right)^d$ [17], where the number of decoy particles is represented by d. The likelihood of detecting eavesdroppers will converge to 1 when d is large enough, ensuring 100% eavesdropper detection. Decoy qubits [18] can be used to defend against this attack.

Another attack that an eavesdropper can mount the proposed scheme is entangle-and-measure attack. Suppose, an eavesdropper intercepts the transmitting particle transferred from participant N_{r-1} to participant N_r and applies a phase shift operation A_D on the particle $|D\rangle$. Since, decoy particle is chosen from mutually unbiased bases μ and υ, therefore, if decoy particle belongs to μ-basis, then, after performing phase shift operation A_D on the entangled aider particle, the measurements of eavesdropper are given as

$$A_D |\mu_1\rangle |D\rangle = \alpha_{00} |00\rangle |e_{00}\rangle + \alpha_{01} |01\rangle |e_{01}\rangle + \alpha_{02} |10\rangle |e_{02}\rangle + \alpha_{03} |11\rangle |e_{03}\rangle$$
$$A_D |\mu_2\rangle |D\rangle = \alpha_{10} |00\rangle |e_{10}\rangle + \alpha_{11} |01\rangle |e_{11}\rangle + \alpha_{12} |10\rangle |e_{12}\rangle + \alpha_{13} |11\rangle |e_{13}\rangle$$

where $|e_{ij}\rangle$ are the states determined by A_D with $i, j \in \{0,1,2,3\}$,

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{02}|^2 + |\alpha_{03}|^2 = 1 \text{ and}$$
$$|\alpha_{10}|^2 + |\alpha_{11}|^2 + |\alpha_{12}|^2 + |\alpha_{13}|^2 = 1.$$

If an eavesdropper wants to avoid eavesdropping checking, he/she equates

$$\alpha_{01} = \alpha_{02} = 0 \quad \text{and} \quad \alpha_{10} = \alpha_{13} = 0.$$

Thus, the simplified decoy particle after applying A_D is given as follows

$$A_D|\mu_1\rangle|D\rangle = \alpha_{00}|00\rangle|e_{00}\rangle + \alpha_{03}|11\rangle|e_{03}\rangle$$

and

$$A_D|\mu_2\rangle|D\rangle = \alpha_{11}|01\rangle|e_{11}\rangle + \alpha_{12}|10\rangle|e_{12}\rangle.$$

Further, if decoy particle is taken from υ-basis then after applying A_D on the entangled particle, the measurements of an eavesdropper are given by

$$\begin{aligned} A_D|\upsilon_1\rangle|D\rangle &= \beta_{00}|00\rangle|e_{00}\rangle + \beta_{01}|01\rangle|e_{01}\rangle \\ &\quad + \beta_{02}|10\rangle|e_{02}\rangle + \beta_{03}|11\rangle|e_{03}\rangle \\ A_D|\upsilon_2\rangle|D\rangle &= \beta_{10}|00\rangle|e_{10}\rangle + \beta_{11}|01\rangle|e_{11}\rangle \\ &\quad + \beta_{12}|10\rangle|e_{12}\rangle + \beta_{13}|11\rangle|e_{13}\rangle \end{aligned}$$

where $|e_{ij}\rangle$ are the states determined by A_D with $i, j \in \{0,1,2,3\}$,

$$|\beta_{00}|^2 + |\beta_{01}|^2 + |\beta_{02}|^2 + |\beta_{03}|^2 = 1$$

and

$$|\beta_{10}|^2 + |\beta_{11}|^2 + |\beta_{12}|^2 + |\beta_{13}|^2 = 1.$$

If eavesdropper wants to avoid eavesdropping checking, he/she equates

$$\beta_{01} = \beta_{02} = 0 \quad \text{and} \quad \beta_{10} = \beta_{13} = 0.$$

It is evident from the above computations; the proposed scheme could resist the entangle-and-measure attack.

Internal attack: This section discusses a typical attack that participants can use, called the "participant attack." In this attack, with only one share, the participant N_i cannot recreate the value S that the dealer had previously encoded in qubits because of the perfectness [19] of [1]. In other words, fewer than t participants cannot recover any information in [1].

VII. Comparison

There are numerous QSS schemes, but the majority are two-level [8, 20, 21] and structural [22, 23]. For example, the developers of the scheme [23] have employed a phase operation to implant the information into a qubit, allowing the information to be recovered once all participants have completed their operations. In [24], a specific QSS based on the Grover method was presented. However, compared to 4-level and structure designs, these 2-level schemes are less general and practicable. QSS plans are less flexible than others in that all shareholders must be present to reconstruct the information. Our four-level threshold QSS scheme is more versatile, general, and practical than these schemes. Qin et al. [11, 25] presented two threshold SSSs based on Shamir's Lagrange interpolation method. One significant difference between our proposed QSS and most existing [11, 25] QSSs is that our scheme is based on an SBP, whereas [11, 25] depends on a univariate polynomial. In our scheme, we used a SBP to generate shares for each participant compared to a univariate polynomial. Furthermore, under our proposed framework, the created shares are represented as univariate polynomials of degree $t-1$. In contrast, the existing schemes [11, 12] generate shares that are represented as integer values. In our technique, decoy particles are used to deceive the third party throughout the particle transmission process, preventing it from obtaining beneficial particles without a valid measurement basis. In other words, our system can withstand an eavesdropping examination. In this scheme, every shareholder must store a share, which is a $t-1$ degree univariate polynomial. Before performing unitary operations, each shareholder must compute the Lagrange component. All of these evaluations are substantially faster than typical public-key evaluations because they involve small-modulus multiplications and additions, whereas public-key computations involve large-modulus modular exponentiations

VIII. Conclusion

This study introduces a QSS system based on SBP. In contrast to the majority of current schemes, our proposed method produces a $t-1$ degree polynomial as a share for each participant. In order to guarantee the confidentiality of confidential communication, we employ a decoy particle, namely a two-qubit in a four-dimensional Hilbert space. The permission structure that we suggest exhibits enhanced flexibility, scalability with respect to participant numbers, realism, and ease of implementation. Moreover, it suffices to perform a unitary transformation to securely transmit confidential data.

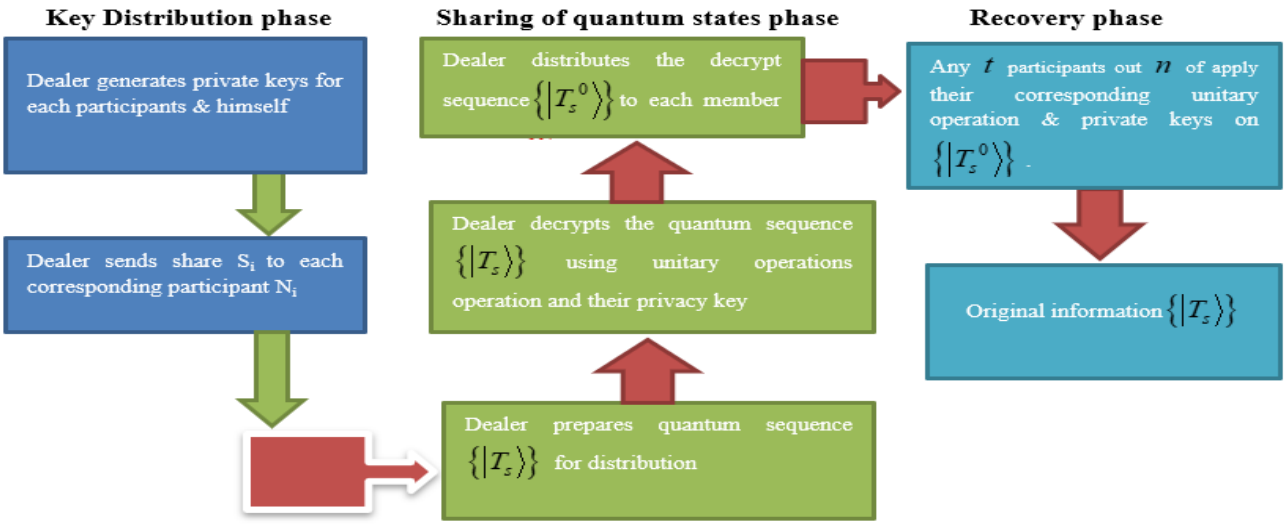

Fig 1. Graphical Representation of the Proposed Scheme

REFERENCES

[1] Shamir, "How to share a secret," Communications of the ACM, 22(11), 612-613, 1979.

[2] G.R. Blakley, "December. Safeguarding cryptographic keys," In Managing Requirements Knowledge, International Workshop on IEEE Computer Society, 313-313, 1979.

[3] M. Nojoumian, and D.R. Stinson, "Social secret sharing in cloud computing using a new trust function," In 2012 Tenth Annual International Conference on Privacy, Security and Trust . IEEE, 161-167, 2012.

[4] L. Harn, and C. Lin, "Authenticated group key transfer protocol based on secret sharing," IEEE Transactions on Computers, 59(6), 842-846, 2010.

[5] M. Mignotte, "How to share a secret," In Workshop on Cryptography. Springer, Berlin, Heidelberg, 371-375, 1982.

[6] M. Hai-Qiang, W. Ke-Jin, and Y. Jian-Hui, "Experimental single qubit quantum secret sharing in a fiber network configuration" Optics Letters, 38(21), 4494-4497, 2013.

[7] X. Yang, K. Wei, H. Ma, , H. Liu, Z. Yin, Z. Cao, and L. Wu, "Detector-device-independent quantum secret sharing with source flaws," Scientific Reports, 8(1), 1-6, 2018.

[8] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing," Physical Review A, 59(3), 1829, 1999.

[9] R. Cleve, D. Gottesman, and H. K. Lo, , "How to share a quantum secret," Physical Review Letters, 83(3), 648, 1999.

[10] C. Hao, and M. Wenping, " (t,n) – Threshold quantum state sharing scheme based on linear equations and unitary operation," IEEE Photonics Journal, 9(1), 1-7, 2017.

[11] H. Qin, X. Zhu, and Y. Dai, " (t,n) – Threshold quantum secret sharing using the phase shift operation," Quantum Information Processing, 14(8), 2997-3004, 2015.

[12] C. Lu, F. Miao, K. Meng, and Y. Yu, "Threshold quantum secret sharing based on single qubit" Quantum Information Processing, 17(3), 1-13, 2018.

[13] M. Kumar, M. K. Gupta, S. S. Dubey, and A. Kumar, "(T, N)-Threshold Quantum State Sharing Scheme Of An Arbitrary One-Qutrit Based On Linear Equation," International Journal of Scientific & Technology Research, 8(10), 334-340, 2019.

[14] F.G. Deng, and G.L. Long, "Secure direct communication with a quantum one- time pad," Physical Review A, 69(5), 052319,2004.

[15] D. Costa, N.G. de Almeida, and C. J. Villas-Boas, "Secure quantum communication using classical correlated channel," Quantum Information Processing, 15(10), 4303-4311, 2016.

[16] S. Mi, T. J. Wang, G. S. Jin, and C. Wang, "High-capacity quantum secure direct communication with orbital angular momentum of photons," IEEE Photonics Journal, 7(5), 1-8, 2015.

[17] H. Qin, and Y. Dai, "Dynamic quantum secret sharing by using d – dimensional GHZ state," Quantum information processing, 16(3), 64, 2017.

[18] W. Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Physical Review Letters, 91(5), 057901, 2003.

[19] M. Fuyou, , X. Yan, , W. Xingfu, and M. Badawy, "Randomized Component and Its Application to (t,m,n) -Group Oriented Secret Sharing," IEEE Transactions on Information Forensics and Security, 10(5), 889-899, 2014.

[20] G. P. Guo, and G. C. Guo, "Quantum secret sharing without entanglement," Physics Letters A, 310(4), 247-251, 2003.

[21] D. Markham, and B.C. Sanders, Graph states for quantum secret sharing. Physical Review A, 78(4), 042309, 2008.

[22] A. Tavakoli, I. Herbauts, M. Zukowski, and M. Bourennane, "Secret sharing with a single d-level ˙ quantum system," Physical Review A, 92(3), p.030302, 2015.

[23] W. Yang, L. Huang, R. Shi, and L. He, "Secret sharing based on quantum Fourier transform," Quantum Information Processing, 12(7), 2465-2474, 2013.

[24] L. Y. Hsu, "Quantum secret-sharing protocol based on Grover's algorithm," Physical Review A, 68(2), 022306, 2003.

[25] H. Qin, and Y. Dai, d -Dimensional quantum state sharing with adversary structure. Quantum Information Processing, 15(4), 1689-1701, 2016.