# AN EFFICIENT SECRET SHARING SCHEME FOR QUANTUM KEY DISTRIBUTION

**Manoj Kumar**

*Department of Mathematics and Statistics,*
*Gurukul Kangri Vishwavidyalaya, Haridwar, UK, (India)*

**ABSTRACT**

*Secret sharing schemes have been suggested for sensor networks where the links are liable to be tapped by sending the data in shares which makes the task of the eavesdropper harder. The security in such environments can be made greater by continuous changing of the way the shares are constructed. In the present paper we proposed a verifiable quantum* $(t, n)$ *-threshold secret sharing scheme using Lagrange interpolation and two qudit Bell state in* $p$ *-dimensional Hilbert space. The proposed scheme is enough secure against the fraud in secret share distribution phase as well as secret reconstruction phase.*

***Keywords- Quantum cryptography, Conventional quantum secret sharing, Verifiable quantum secret sharing, Bell state, Pauli operators, Finite fields.***

## I. INTRODUCTION

With the improvement of computing ability and algorithms, especially the presentation of quantum algorithms [9, 11], the security of classical cryptography encounters serious challenges. Under this background, more and more attention is paid to the theory of quantum information. However, the design and cryptanalysis of quantum cryptography is far from satisfactory, especially in quantum secret sharing. Obviously, quantum secret sharing may play an important role in protecting secret information so that the works about quantum secret sharing have attracted a lot of attention in theoretical and experimental ways. The concept of secret sharing was first introduced by independently by Shamir [10] and Blakley[2]. In a conventional $(t, n)$ - threshold secret sharing scheme a trusted dealer divides a secret $S$ into $n$ -shares and distributes them among $n$ -agents such that any coalition of $t$ or more agents can together reconstruct the original secret $S$ but no coalition of fewer than $t$ -agents can. Verifiable secret sharing schemes are important in cloud computing environments. Thus a key can be distributed over many servers by threshold secret sharing mechanism. The key is then reconstructed when needed. The concept of quantum secret sharing was first introduced by Hillery et al. [5], who showed how to implement a conventional threshold scheme using Greenberger-Horne-Zeilinger (GHZ) states in the presence of the outside and inside eavesdroppers. They also showed how to share an unknown qubit between two agents such that only the collaboration of two agents could reconstruct the original qubit. Subsequently a lot of quantum secret sharing schemes have been proposed [6, 7, 8, 12, 13] but they all have lack of verification characteristic which is assumed very crucial property of any cryptographic scheme in realistic applications. The first verifiable quantum secret sharing scheme was proposed by Yang et al. [15]. The verifiable quantum secret sharing scheme proposed by Yang et al. [15] was based upon Li's scheme [15] and it has a drawback that it

requires too much quantum authentication information for its implementation. Later on, Yang et al. [14] proposed another modification of verifiable quantum secret sharing scheme in which a quantum tag is connected to the quantum secret through a unitary operation, so that the quantum tag can be used as a signature to verify the reconstructed quantum secret. A drawback of Yang et al. [14] scheme is that classical secret cannot be shared in it. In the present paper we proposed a verifiable quantum $(t,n)$-threshold secret sharing scheme using Lagrange interpolation and two qudit Bell state in $p$-dimensional Hilbert space.

## II. PRELIMINARIES

In this section we will discuss some auxiliary results and definitions which will be helpful in interpreting the proposed scheme.

**Definition 2.1:** The generalized two qudit Bell state in $p$-dimensional Hilbert space is defined as

$$\left|B_{u,v}\right\rangle = \frac{1}{\sqrt{p}}\sum_{k=0}^{p-1}\exp\left(\frac{2\pi i u}{p}k\right)\left|k, k\oplus v\right\rangle$$

where $k\oplus v=(k+v)\bmod p$ and $u,v\in\{0,1,2,\ldots,p-1\}$.

**Definition 2.2:** The generalized Pauli unitary operator in $p$-dimensional Hilbert space is defined as

$$U_{\alpha,\beta}=\sum_{k=0}^{p-1}\exp\left(\frac{2\pi i\alpha}{p}k\right)\left|k\right\rangle\left\langle k\oplus\beta\right|$$

where $k\oplus\beta=(k+\beta)\bmod p$ and $\alpha,\beta\in\{0,1,2,\ldots,p-1\}$.

**Lemma 2.3 [9]:** In a $p$-dimensional Hilbert space, we have

**(a).** $\langle m|k\rangle=\delta_{mk}$

**(b).** $\left(\left|m\right\rangle\left\langle k\right|\right)\left|n\right\rangle=\left|m\right\rangle\left(\left\langle k|n\right\rangle\right)=\left(\left\langle k|n\right\rangle\right)\left|m\right\rangle$

where $\delta_{mk}$ is a Dirac function and $m,k,n\in\{0,1,2,\ldots,p-1\}$.

**Theorem 2.4:** If an unitary operator $U_{\alpha,\beta}=\sum_{k=0}^{p-1}\exp\left(\frac{2\pi i\alpha}{p}k\right)\left|k\right\rangle\left\langle k\oplus\beta\right|$ is operated on one particle of a two qudit Bell state $\left|B_{u,v}\right\rangle=\frac{1}{\sqrt{p}}\sum_{k=0}^{p-1}\exp\left(\frac{2\pi i u}{p}k\right)\left|k,k\oplus v\right\rangle$, then Bell state $\left|B_{u,v}\right\rangle$ changes to a new state, say $\left|B_{u\oplus\alpha,v\oplus\beta}\right\rangle$ i.e. $U_{\alpha,\beta}\left|B_{u,v}\right\rangle=\left|B_{u\oplus\alpha,v\oplus\beta}\right\rangle$, where $k\oplus\beta=(k+\beta)\bmod p$ and $\alpha,\beta,u,v\in\{0,1,2,\ldots,p-1\}$.

**Proof.** We have

$$U_{\alpha,\beta}=\sum_{k=0}^{p-1}\exp\left(\frac{2\pi i\alpha}{p}k\right)\left|k\right\rangle\left\langle k\oplus\beta\right|$$

$$=\left[\exp\left(\frac{2\pi i\alpha}{p}\cdot 0\right)\left|0\right\rangle\left\langle 0\oplus\beta\right|+\exp\left(\frac{2\pi i\alpha}{p}\cdot 1\right)\left|1\right\rangle\left\langle 1\oplus\beta\right|+\right.$$

$$\ldots+\exp\left(\frac{2\pi i\alpha}{p}\cdot(p-1)\right)\left|p-1\right\rangle\left\langle(p-1)\oplus\beta\right|\Big] \qquad (2.1)$$

and

$$\left|B_{u,v}\right\rangle=\frac{1}{\sqrt{p}}\sum_{k=0}^{p-1}\exp\left(\frac{2\pi i u}{p}k\right)\left|k,k\oplus v\right\rangle$$

$$=\frac{1}{\sqrt{p}}\Big[\exp\left(\frac{2\pi i u}{p}\cdot 0\right)\left|0,0\oplus v\right\rangle+\exp\left(\frac{2\pi i u}{p}\cdot 1\right)\left|1,1\oplus v\right\rangle+$$

$$\ldots+\exp\left(\frac{2\pi i u}{p}\cdot(p-1)\right)\left|(p-1),(p-1)\oplus v\right\rangle\Big] \qquad (2.2)$$

Operating $U_{\alpha,\beta}$ on $\left|B_{u,v}\right\rangle$ using relations (2.1), (2.2) and lemma 2.3, we obtain

$$U_{\alpha,\beta}\left|B_{u,v}\right\rangle=\frac{1}{\sqrt{p}}\Big[\exp\left(\frac{2\pi i(\alpha\oplus u)}{p}\cdot 0\right)\left|0,0\oplus(\beta\oplus v)\right\rangle+$$

$$\exp\left(\frac{2\pi i(\alpha\oplus u)}{p}\cdot 1\right)\left|1,1\oplus(\beta\oplus v)\right\rangle+$$

$$\ldots+\exp\left(\frac{2\pi i(\alpha\oplus u)}{p}\cdot(p-1)\right)\left|(p-1),(p-1)\oplus(\beta\oplus v)\right\rangle\Big]$$

$$=\frac{1}{\sqrt{p}}\sum_{k=0}^{p-1}\exp\left(\frac{2\pi i(\alpha\oplus u)}{p}\cdot k\right)\left|k,k\oplus(\beta\oplus v)\right\rangle\Big]$$

$$=\left|B_{u\oplus\alpha,v\oplus\beta}\right\rangle.$$

Thus we get

$$U_{\alpha,\beta}\left|B_{u,v}\right\rangle=\left|B_{u\oplus\alpha,v\oplus\beta}\right\rangle.$$

This completes the proof of the theorem.

## III. CONSTRUCTION OF THE PROPOSED SECRET SHARING SCHEME

Suppose a dealer $D$ wants to share his secret $S$ among $n$-agents, say $A_1$, $A_2$, …, $A_n$. According to the theory of conventional secret sharing scheme it is assumed that any coalition of $t$ or more agents can together reconstruct the original secret $S$ but no coalition of fever than $t$ agents can. The construction of the proposed verifiable $(t,n)$-threshold quantum secret sharing scheme consists of the following phases:

**Phase-I: Secret Share Distribution Phase.**

To distribute the secret $S$, dealer goes through the following steps:

1. For given $t$ and $n$, dealer uses the Bertnard's principle [1] to find an appropriate prime number $p$ such that $n\le p\le 2n$.

2. Using $p$ (chosen as above), dealer construct a finite field $F = Z_p$.

3. Choosing the numbers $a_1, a_2, \ldots, a_{t-1}$ in the field $F$, the dealer construct a polynomial as under

$$P(x) = S \oplus a_1 x \oplus a_2 x^2 \oplus \ldots \oplus a_{t-1} x^{t-1}$$

where $S$ is the secret to be shared among the agents.

4. Dealer again picks the numbers $x_1, x_2, \ldots, x_n$ in the field $F$ such that

$L_k = \prod_{\substack{1 \le m \le n \\ m \ne k}} \left( \frac{x_m}{x_m - x_k} \right)$ is an integer, where $x_m \ne x_k$ for all $m \ne k$.

5. Dealer publicly announces all $x_1, x_2, \ldots, x_n$.

In fact $x_1, x_2, \ldots, x_n$ are used as the ID of the agents $A_1, A_2, \ldots, A_n$ respectively.

6. Dealer calculates $P(x_1), P(x_2), \ldots, P(x_n)$.

7. Using the quantum secure direct communication techniques [3, 4], dealer sends $P(x_1), P(x_2), \ldots, P(x_n)$ to the agents $A_1, A_2, \ldots, A_n$ respectively.

In fact $P(x_1), P(x_2), \ldots, P(x_n)$ are the private shares of the agents $A_1, A_2, \ldots, A_n$ respectively.

**Phase II: Reconstruction of the original secret $S$.**

According to the $(t, n)$-threshold secret sharing hypothesis, any coalition of $t$ or more agents can together reconstruct the original secret $S$ and no coalition of fever than $t$ agents can. If $t$-agents $A_1, A_2, \ldots, A_t$ want to reconstruct the secret $S$, then this phase consists of the following steps:

1. Dealer randomly yields a two qudit Bell state in a $p$-dimensional Hilbert space, as under

$$\left| B_{u,v} \right\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \exp\left( \frac{2\pi i u}{p} k \right) \left| k, k \oplus v \right\rangle$$

where $k \oplus v = (k + v) \bmod p$ and $u, v \in \{0, 1, 2, \ldots, p-1\}$.

2. Dealer randomly constructs some decoy particles in the $Z$-basis and $X$-basis,

where $Z$-basis $= \left\{ \left| m \right\rangle, m = 0, 1, 2, \ldots, p-1 \right\}$, $X$-basis $= \left\{ \left| M_m \right\rangle, m = 0, 1, 2, \ldots, p-1 \right\}$

and $\left| M_m \right\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \exp\left( \frac{2\pi i m}{p} k \right) \left| k \right\rangle$.

3. Dealer inserts the second particle of $\left| B_{u,v} \right\rangle$ into the decoy particles.

4. Keeping in mind the record of insertion position of the second particle of $\left| B_{u,v} \right\rangle$ and initial states of the decoy particles, dealer sends these particles to the agent $A_1$.

5. After ensuring that agent $A_1$ has received these particles, dealer publishes the position and basis of the decoy particles and tells agent $A_1$ to measure these particles in an appropriate $Z$-basis or $X$-basis according to his basis.
6. After measuring the decoy particles, agent $A_1$ publicly announces his measurement results.
7. Dealer matches the measurement results of agent $A_1$ with his record and if these results do not match with the initial states, he tells the agent $A_1$ to abort the process and start a new process; otherwise they carry on the scheme.
8. After performing an unitary operation $U_{(L_1\ P(x_1) \bmod p),0} = \sum_{k=0}^{p-1} \exp\left(\frac{2\pi i (L_1\ P(x_1) \bmod p)}{p} k\right) |k\rangle\langle k|$ on the second particle of $|B_{u,v}\rangle$, agent $A_1$ constructs some decoy particles in the $Z$-basis and $X$-basis.
9. After inserting the second particle of $|B_{u,v}\rangle$ into the decoy particles (constructed by him), agent $A_1$ sends these particles to the agent $A_2$.

The above step numbers 2 to 8 are repeated to verify the security of the quantum channel between agent $A_1$ and agent $A_2$ through the decoy particles. Similarly agent $A_2$ performs an unitary operation $U_{(L_2\ P(x_2) \bmod p),0}$ on the second particle of $|B_{u,v}\rangle$ and constructs some decoy particles in the $Z$-basis and $X$-basis.

The above process is uninterrupted until the last agent $A_t$.

10. After ensuring that the above process has been completed, dealer performs an unitary operation $U_{(p-u),(p-v)\oplus H(S)}$ on the first particle of $|B_{u,v}\rangle$ where $H(S) \in F$ is a hash function which is publicly announced by the dealer.
11. Dealer sends the first particle of $|B_{u,v}\rangle$ to the agent $A_t$.
12. After receiving the first particle of $|B_{u,v}\rangle$, the agent $A_t$ performs a Bell state measurement on the state $|B_{u',v'}\rangle$ where $|B_{u',v'}\rangle$ is a new state of $|B_{u,v}\rangle$ and is obtained by operating the unitary operations of the $t$-agents together with the dealer.
13. After performing Bell state measurement on the state $|B_{u',v'}\rangle$, the agent $A_t$ obtains a secret $S = u'$ and verification information $H(S) = v'$.
14. Agent $A_t$ computes $H(u')$. If $H(u') = v'$ then the agent $A_t$ can confide that the reconstructed secret $S$ is correct and the proposed quantum $(t,n)$-threshold secret sharing scheme is stopped otherwise the proposed quantum $(t,n)$-threshold secret sharing scheme is aborted and restarted.

## IV. SECURITY ANALYSIS

We know that a quantum secret sharing scheme is secure against any outside attacker if it is secure against a dishonest participant. Also we know that a dishonest participant can intercept other participant's particles and resends forged particles or entangle aider particles on the intercepted particles and pilfer the secret information through measuring the aider particles. As discussed above, it is evident from the intercept and resend attack, and entangle and measure attack that neither outside eavesdropper nor dishonest participant can filch the secret information from the transmitted particles because the transmitted particles in our proposed quantum secret sharing scheme are conserved by the decoy particles which are randomly yield in the computational $Z$ -basis or $X$ -basis. This shows that our proposed quantum secret sharing scheme is more secure against dishonest participants i.e. it is more secure against any outside eavesdropper.

## V. CONCLUSION

Verifiable secret sharing schemes are ideal for storing information that is highly sensitive and highly important. These schemes are important in cloud computing environments. Thus a key can be distributed over many servers by threshold secret sharing mechanism. The key is then reconstructed when needed. Secret sharing has also been suggested for sensor networks where the links are liable to be tapped by sending the data in shares which makes the task of the eavesdropper harder. The security in such environments can be made greater by continuous changing of the way the shares are constructed.

## REFERENCES

[1] Aigner M. and Ziegler G. M., Proofs from the Book, Springer, Berlin, 7-10, 2006.

[2] Blakley G. R., Safeguarding cryptographic keys, In Proc. of AFIPS National Computer Conference, New York, 48:313-317, 1979.

[3] Cai Q. Y. and Li W. B., Deterministic secure communication without using entanglement, Chin. Phys. Lett. 21 (2004) 601-603.

[4] Deng F. G. and Long G. L., Secure direct communication with a quantum one-time pad, Phys. Rev. A 69 (2004) 052319.

[5] Hillery M., Buzek V. and Berthiaume A., Quantum secret sharing, Phys. Rev. A 59 (1999) 1829-1834.

[6] Hsu J. L., Chong S. K., Hwang T. and Tsai C. W., Dynamic quantum secret sharing, Quantum Inf. Process. 12 (2013), 331-344.

[7] Li Q., Long D. Y., Chan W. H. and Qiu D. W., Sharing a quantum secret without a trusted party, Quantum Inf. Process. 10 (2011) 97-106.

[8] Liu L. L., Tsai C. W. and Hwang T., Quantum secret sharing using symmetric state, Int. J. Theor. Phys. 51 (2012) 2291-2306.

[9] Nielsen M. and Chuang I., Quantum Computation and Quantum Information, pp. 28-43. Cambridge University Press, Cambridge (2000).

[10] Shamir A., How to share a secret ?, Communications of the ACM, 22(11): 612-613, 1979.

[11] Shor P. W., Algorithms for quantum computation: discrete logarithms and factoring, In: Proceedings of the 35th Annual Symposium of Foundation of Computer Science (1994).

[12] Sun Y., Xu S. W., Chen X. B., Niu X. X. and Yang Y. X., Expansible quantum secret sharing network, Quantum Inf. Process. 12 (2013) 2877-2888.

[13] Tseng H.Y., Tsai C. W., Hwang T. and Li C. M., Quantum secret sharing based on quantum search algorithm, Int. J. Theor. Phys. 51 (2012), 3101-3108.

[14] Yang Y. G., Jia X., Wang H. Y. and Zhang H., Verifiable quantum (k, n)-threshold secret sharing, Quantum Inf. Process. 11 (2012), 1619-1625.

[15] Yang Y. G., Teng Y. W., Chai H. P. and Wen Q. Y., Verifiable quantum (k, n)-threshold secret key sharing, Int. J. Theor. Phys. 50 (2011), 792-798.