Front. Phys. 13(2), 130306 (2018)

https://doi.org/10.1007/s11467-017-0717-3

RESERCH ARTICLE

Robust general N user authentication scheme in a centralized quantum communication network via generalized GHZ states

Ahmed Farouk, J. Batle, M. Elhoseny, Mosayeb Naseri, Muzaffar Lone,
Alex Fedorov, Majid Alkhambashi, Syed Hassan Ahmed, M. Abedl-Aty

Supplementary Information

1 Authentication Process between Quantum Authentication Server and One User

The proposed Scheme based on EPR and $CNOT$ Gate

With the objective for protection versus man-in-the-middle, Masquerade as Dishonest and Exchange Fake attacks, the quantum authentication server (QAS) have to verify and authenticate the identity of communicated disjoint users, so they can transmit quantum messages in a secured manner. The authentication process between (QAS) and u_A is achieved by EPR entangled state and $CNOT$ gate. At the time of user enrollment, (QAS) and u_A share a series of joint binary authentication key J_k. QAS generates a EPR state, $|\Psi_{SA}>$ where S and A photons are corresponding to QAS and u_A respectively. QAS reserves its particle locally and transfers the other particles to u_A .

The required steps for authentication between QAS and u_A are shown below and illustrated by (Eq. (1−6))

1. QAS and u_A have a joint binary authentication key J_K as shown in Eq. (1). This information is distributed to u_A at registration time and has to be kept confidently between QAS and u_A.

$$J_k = \{J_1, J_2, \ldots J_{2N}\} \tag{1}$$

2. If u_A would like to send a secret message over the network , u_A informs this information to QAS. When QAS receives the request, it generates EPR pair states $|\Psi_i> = \{\Psi_1, \Psi_2, \Psi_3, \ldots, \Psi_N\}$. For ease the following EPR pair states is assumed to be generated as shown in Eq. (2)

$$|\Psi> = \frac{1}{\sqrt{2}}(|0_S 0_A> + |1_S 1_A> \tag{2}$$

Then, the quantum authentication server reserves S at his location and transfers A particle to u_A

3. Once u_A obtain his A particle, he prepares his own new state n as in Eq. (3). The new state resulted from encrypting the secret identity information as per the particular user operation.

$$|\Phi_{n_{(A)}}> = |J_{2i-1} \otimes J_{2i}>, \quad (3)$$

Where $1 \leq i \leq N$ and $\otimes$ denotes the specified user operation.

4. u_A performs $\not{C}_{NOT}$ operation on both the transmitted particle and n (new state particle) together. The produced particle p will be a three entanglement particles state as in Eq. (4)

$$|\phi_{p_{(A)}}> = \not{C}_{NOT}(|\Phi_{n_{(A)}}> \otimes |\Psi>), \quad (4)$$

Where $\not{C}_{NOT} = \not{C}_0$ at $J_{2i-1} = 0$ and $\not{C}_{NOT} = \not{C}_1$ at $J_{2i-1} = 1$. $\not{C}_0$ and $\not{C}_1$ are described as in Eq. (5):

$$\not{C}_0 = |0_S> |0_A> \otimes I_n + |1_S> |1_A> \otimes \sigma_{x_n},$$
$$\not{C}_1 = |+_S> |+_A> \otimes I_n + |-_S> |-_A> \otimes \sigma_{x_n} \quad (5)$$

5. Afterward, u_A preserves his own particle at his location and transmits the produced particles $|\phi_{p_{(A)}}>$ to QAS

6. When QAS receives $|\phi_{p_{(A)}}>$, it starts decrypting them by performing $\not{C}_{NOT}$ operation on both his particle S and n as showing in Eq. (6)

$$|\phi'_{p_{(A)}}> = \not{C}_{NOT}(|\phi_{p_{(A)}}>) \quad (6)$$

7. QAS starts identity verification of u_A by measuring $|\Phi_{n_{(A)}}>$ according to σ_z . The resulted state have to be in either 0 or 1. If the measurement result is identical to $|J_{2i-1}, J_{2i}>$ so u_A is authenticated and verified. Therefore, they can go ahead for communication process. But, if the resulted measurement is invalid then the authentication process will be aborted and u_A is not authenticated.

2 Authentication Process between Quantum Authentication Server and Two Users

2.1 The proposed Scheme based on GHZ and $CNOT$ Gate

The authentication process among QAS, u_A and u_B is achieved by GHZ entangled state and $CNOT$ gate. At the time of user enrollment,QAS, u_A and u_B share a series of joint binary authentication key J_k. QAS generates a GHZ state, $|\Psi_{ASB}>$ where A , S and B photons are corresponding to u_A , QAS and u_B respectively. QAS reserves its particle locally and transfers the other two particles to each user.

The required steps for authentication between QAS and two users u_A and u_B respectively are shown below and illustrated by (Eq. $(7-12)$).

1. QAS, u_A and u_B have a joint binary authentication key J_K as shown in Eq. (7). This information is distributed to u_A and u_B at registration time and has to be kept confidently among u_A ,u_B and QAS.

$$J_k = \{J_1, J_2, \ldots J_{2N}\} \tag{7}$$

2. If u_A would like to send a secret message to u_B , u_A informs this information to both u_B and QAS. When QAS receives the request, it generates GHZ tripartite states $|\Psi_i> = \{\Psi_1, \Psi_2, \Psi_3, \ldots, \Psi_N\}$. For ease the following GHZ tripartite states is assumed to be generated as shown in Eq. (8)

$$|\Psi> = \frac{1}{\sqrt{2}}(|0_A 0_S 0_B> + |1_A 1_S 1_B> \tag{8}$$

Then, QAS reserves S at his location and transfers A and B particles to u_A and u_B respectively.

3. Once u_A and u_B obtain their A and B particles, each of them prepare his own new state n as in Eq. (9). The new state resulted from encrypting the secret identity information as per the particular user operation.

$$\begin{aligned} |\Phi_{n_{(A)}}> &= |J_{2i-1} \otimes J_{2i}>, \\ |\Phi_{n_{(B)}}> &= |J_{2i+1} \otimes J_{2i}> \end{aligned} \tag{9}$$

Where $1 \leq i \leq N$ and $\otimes$ denotes the specified user operation.

4. u_A and u_B perform $\not{C}_{NOT}$ operation on both the transmitted particle and n (new state particle) together. The produced particle p will be a four entanglement particles state as in Eq. (10)

$$\begin{aligned} |\phi_{p_{(A)}}> &= \not{C}_{NOT}(|\Phi_{n_{(A)}}> \otimes |\Psi>), \\ |\phi_{p_{(B)}}> &= \not{C}_{NOT}(|\Phi_{n_{(B)}}> \otimes |\Psi>) \end{aligned} \tag{10}$$

Where $\not{C}_{NOT} = \not{C}_0$ at $J_{2i} = 0$ and $\not{C}_{NOT} = \not{C}_1$ at $J_{2i} = 1$. $\not{C}_0$ and $\not{C}_1$ are described as in Eq. (11):

$$\begin{aligned} \not{C}_0 &= |0_A> |0_S> |0_B> \otimes I_n + |1_A> |1_S> |1_B> \otimes \sigma_{x_n}, \\ \not{C}_1 &= |+_A> |+_S> |+_B> \otimes I_n + |-_A> |-_S> |-_B> \otimes \sigma_{x_n} \end{aligned} \tag{11}$$

5. Afterward, u_A and u_B preserve their own particles which mean u_A keeps A and u_B keeps B at their locations and transmit the produced particles $|\phi_{p_{(A)}}>$ and $|\phi_{p_{(B)}}>$ respectively to QAS

6. when QAS receives both $|\phi_{p_{(A)}}>$ and $|\phi_{p_{(B)}}>$, it starts decrypting them by performing $\not{C}_{NOT}$ operation on both his particle S and n as showing in Eq. (12)

$$\begin{aligned} |\phi'_{p_{(A)}}> &= \not{C}_{OP}(|\phi_{p_{(A)}}>) \ , \\ |\phi'_{p_{(B)}}> &= \not{C}_{OP}(|\phi_{p_{(B)}}>) \end{aligned} \tag{12}$$

7. QAS starts identity verification of u_A and u_B by measuring $|\Phi_{n_{(A)}}>$ and $|\Phi_{n_{(B)}}>$ according to σ_z . The resulted state have to be in either 0 or 1. If the measurement result is identical to $|J_{2i-1}, J_{2i}>$ and $|J_{2i+1}, J_{2i}>$ so u_A and u_B are authenticated and verified respectively. Therefore, they can go ahead for communication process. But, if the resulted measurement is invalid then the authentication process will be aborted and u_A and u_B are not authenticated.

3 Authentication Process between Quantum Authentication Server and Three Users

3.1 The proposed Scheme based on GHZ and $CNOT$ Gate

The authentication process among QAS, u_A , u_B and u_C is achieved by GHZ entangled state and $CNOT$ gate. At the time of user enrollment, QAS, u_A , u_B and u_C share a series of joint binary authentication key J_k. QAS generates a four photons GHZ state, $|\Psi_{ASBC}>$ where A , S , B and C photons are corresponding to u_A , QAS , u_B and u_C respectively. QAS reserves its particle locally and transfers the other three particles to each user.

The required steps for authentication between QAS and three users u_A , u_B and u_C respectively are shown below and illustrated by (Eq. (13−19)) and Figure S1.

1. QAS, u_A and u_B have a joint binary authentication key J_K as shown in Eq. (13). This information is distributed to u_A , u_B and u_C at registration time and has to be kept confidently among u_A ,u_B , u_C and QAS.

$$J_k = \{J_1, J_2, \dots J_{2N}\} \tag{13}$$

2. If u_A would like to send a secret message to u_B and u_C ; u_A informs this information to u_B , u_C and QAS. When QAS receives the request, it generates GHZ four states $|\Psi_i> = \{\Psi_1, \Psi_2, \Psi_3, \dots, \Psi_N\}$. For ease the following GHZ four states is assumed to be generated as shown in Eq. (14)

$$|\Psi> = \frac{1}{\sqrt{2}}(|0_A 0_S 0_B 0_C> + |1_A 1_S 1_B 1_C> \tag{14}$$

   Then, QAS reserves S at his location and transfers A , B and C particles to u_A , u_B and u_C respectively.

3. Once u_A , u_B and u_C obtain their A , B and C particles, each of them prepare his own new state n as in Eq.(15). The new state resulted from encrypting the secret identity information as per the particular user operation.

$$\begin{aligned} |\Phi_{n_{(A)}}> &= |J_{2i-1} \otimes J_{2i}>, \\ |\Phi_{n_{(B)}}> &= |J_{2i+1} \otimes J_{2i}>, \\ |\Phi_{n_{(C)}}> &= |J_{2i+2} \otimes J_{2i}> \end{aligned} \tag{16}$$

   Where $1 \le i \le N$ and $\otimes$ denotes the specified user operation.

4. u_A , u_B and u_C perform $\not{C}_{NOT}$ operation on both the transmitted particle and n (new state particle) together. The produced particle p will be a five entanglement particles state as in Eq. (17)

$$\begin{aligned} |\phi_{p_{(A)}}> &= \not{C}_{NOT}(|\Phi_{n_{(A)}}> \otimes |\Psi>), \\ |\phi_{p_{(B)}}> &= \not{C}_{NOT}(|\Phi_{n_{(B)}}> \otimes |\Psi>), \\ |\phi_{p_{(C)}}> &= \not{C}_{NOT}(|\Phi_{n_{(C)}}> \otimes |\Psi>) \end{aligned} \tag{17}$$

   Where $\not{C}_{NOT} = \not{C}_0$ at $J_{2i} = 0$ and $\not{C}_{NOT} = \not{C}_1$ at $J_{2i} = 1$. $\not{C}_0$ and $\not{C}_1$ are described as in Eq. (18):

$$\mathbb{C}_0 = |0_A> |0_S> |0_B> |0_C> \otimes I_n + |1_A> |1_S> |1_B> |1_C> \otimes \sigma_{x_n} ,$$
$$\mathbb{C}_1 = |+_A> |+_S> |+_B> |+_C> \otimes I_n + |-_A> |-_S> |-_B> |-_C> \otimes \sigma_{x_n} \quad (18)$$

5. Afterward, u_A , u_B and u_C preserve their own particles which mean u_A keeps A , u_B keeps B and u_C keeps C at their locations and transmit the produced particles $|\phi_{p_{(A)}}>$, $|\phi_{p_{(B)}}>$ and $|\phi_{p_{(C)}}>$ respectively to QAS

6. when QAS receives $|\phi_{p_{(A)}}>$, $|\phi_{p_{(B)}}>$ and $|\phi_{p_{(C)}}>$, it starts decrypting them by performing $\mathbb{C}_{NOT}$ operation on both his particle S and n as showing in Eq. (19)

$$|\phi'_{p_{(A)}}> = \mathbb{C}_{OP}(|\phi_{p_{(A)}}>) ,$$
$$|\phi'_{p_{(B)}}> = \mathbb{C}_{OP}(|\phi_{p_{(B)}}>) ,$$
$$|\phi'_{p_{(C)}}> = \mathbb{C}_{OP}(|\phi_{p_{(C)}}>) \quad (19)$$

7. QAS starts identity verification of u_A , u_B and u_C by measuring $|\Phi_{n_{(A)}}>$, $|\Phi_{n_{(B)}}>$ and $|\Phi_{n_{(C)}}>$ according to σ_z . The resulted state have to be in either 0 or 1. If the measurement result is identical to $|J_{2i-1}$, $J_{2i}>$, $|J_{2i+1}$, $J_{2i}>$ and $|J_{2i+2}$, $J_{2i}>$ so u_A , u_B and u_C are authenticated and verified respectively. Therefore, they can go ahead for communication process. But, if the resulted measurement is invalid then u_A , u_B and u_C are not authenticated. Therefore, the authentication process will be aborted.

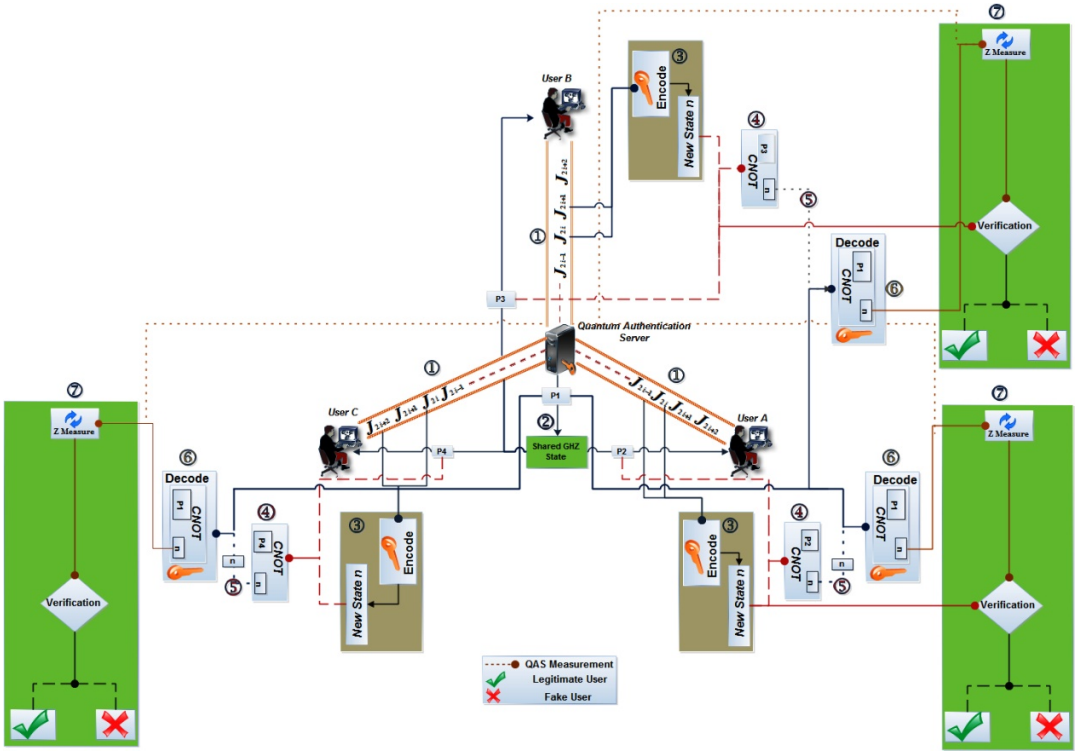


Fig. S1 Authentication Process between Quantum Authentication Server and Three Users.

4 Masquerade as Dishonest Multicast User

If an eavesdropper would like to impersonate as a fraudulent user, then the eavesdropper will take control on the transferring particle , B or C from QAS to u_A , u_B and u_C respectively. By supposing that the eavesdropper performing a universal operation $\mathbb{R}$ on A , B and C *as* shown in Eq. $(20-26)$

$$|0_A\mathbb{R}>\rightarrow \alpha_0|0_A0_E> +\beta_0|0_A1_E> +\gamma_0|1_A0_E> +\delta_0|1_A1_E> \quad (20)$$
$$|1_A\mathbb{R}>\rightarrow \alpha_1|0_A0_E> +\beta_1|0_A1_E> +\gamma_1|1_A0_E> +\delta_1|1_A1_E> \quad (21)$$
$$|0_B\mathbb{R}>\rightarrow \alpha_2|0_B0_E> +\beta_2|0_B1_E> +\gamma_2|1_B0_E> +\delta_2|1_B1_E> \quad (22)$$
$$|1_B\mathbb{R}>\rightarrow \alpha_3|0_B0_E> +\beta_3|0_B1_E> +\gamma_3|1_B0_E> +\delta_3|1_B1_E> \quad (23)$$
$$|0_C\mathbb{R}>\rightarrow \alpha_4|0_C0_E> +\beta_4|0_C1_E> +\gamma_4|1_C0_E> +\delta_4|1_C1_E> \quad (24)$$
$$|1_C\mathbb{R}>\rightarrow \alpha_5|0_C0_E> +\beta_5|0_C1_E> +\gamma_5|1_C0_E> +\delta_5|1_C1_E> \quad (25)$$

Where $|\mathbb{R}>$ denotes a superfluous state which is generated by the eavesdropper, E represents the eavesdropper particle and,

$$|\alpha_0^2|+|\beta_0^2|+|\gamma_0^2|+|\delta_0^2|=|\alpha_1^2|+|\beta_1^2|+|\gamma_1^2|+|\delta_1^2|,$$
$$|\alpha_2^2|+|\beta_2^2|+|\gamma_2^2|+|\delta_2^2|=|\alpha_3^2|+|\beta_3^2|+|\gamma_3^2|+|\delta_3^2|=1 \quad (26)$$

Masquerade as Dishonest Multicast User *A*

By assuming that the eavesdropper will work only on particle A which means particles B *and* C are not included and we excluded it from the transmitted state, so the eavesdropper performing its operation $|0_A\mathbb{R}>$ and $|1_A\mathbb{R}>$, a new transmitted state will be generated as showing in Eq. (27,28)

$$|\Psi_{(SA)}>\rightarrow |\Psi_{(SA)}{}'> \quad (27)$$

$$|\Psi_{(SA)}{}'>=\frac{1}{\sqrt{2}}(\alpha_0|0_S0_A0_E>+\beta_0|0_S0_A1_E>+\gamma_0|0_S1_A0_E>+\delta_0|0_S1_A1_E>+\alpha_1|1_S0_A0_E>+\beta_1|1_S0_A1_E>+\gamma_1|1_S1_A0_E>+\delta_1|1_S1_A1_E>) \quad (28)$$

The eavesdropper transfers the new prepared state $|\Psi_{(SA)}{}'>$ to QAS. Subsequently, QAS applies $\not{C}_{NOT}$ on the received state as outcome one of four states $|\Psi_{(SA)}^{00}>$,$|\Psi_{(SA)}^{01}>$,$|\Psi_{(SA)}^{10}>$,$|\Psi_{(SA)}^{11}>$ which corresponding to the paired bits 00, 01, 10 and 11. By assuming when the paired bits are equivalent to 00 and 01 then QAS operation is equivalent as in Eq. $(29-31)$.

$$|\Psi_{(SA)}^{00}> = \not{C}_0\,|\Psi_{(SA)}{}'> \quad (29)$$

By performing $\not{C}_0$ the result is obtained in Eq. (30,31)

$$|\Psi_{(SA)}^{00}> =\frac{1}{\sqrt{2}}(\alpha_0|0_S0_A0_E>+\beta_0|0_S0_A1_E>+\gamma_0|0_S1_A0_E>+\delta_0|0_S1_A1_E>+\alpha_1|1_S0_A1_E>+\beta_1|1_S0_A0_E>+\gamma_1|1_S1_A1_E>+\delta_1|1_S1_A0_E>) \quad (30)$$

$$|\Psi_{(SA)}^{01}> =\frac{1}{\sqrt{2}}(\alpha_0|0_S0_A1_E>+\beta_0|0_S0_A0_E>+\gamma_0|0_S1_A1_E>+\delta_0|0_S1_A0_E>+\alpha_1|1_S0_A0_E>+\beta_1|1_S0_A1_E>+\gamma_1|1_S1_A0_E>+\delta_1|1_S1_A1_E>) \quad (31)$$

So the possibility for detecting the eavesdropper for $|\Psi_{(SA)}^{00}>$ is $\mathbb{P}_{00_{(A)}}$ can be computed from Eq. (30) as shown in Eq. (32).

$$\mathbb{P}_{00_{(A)}} = \frac{1}{2}\left(|\alpha_1^2|+|\gamma_1^2|+|\beta_0^2|+|\delta_0^2|\right) \tag{32}$$

As well when the paired bits are equivalent to 01, so the chance for discovering the eavesdropper for $|\Psi_{(SA)}^{01}>$ is $\mathbb{P}_{01_{(A)}}$ can be computed from Eq. (31) as shown in Eq. (33)

$$\mathbb{P}_{01_{(A)}} = \frac{1}{2}\left(|\alpha_0^2|+|\gamma_0^2|+|\beta_1^2|+|\delta_1^2|\right) \tag{33}$$

Additionally, the probability for detecting the eavesdropper $\mathbb{P}_{10_{(A)}}$ and $\mathbb{P}_{11_{(A)}}$ is equivalent to $\mathbb{P}_{00_{(A)}}$ and $\mathbb{P}_{01_{(A)}}$respectively. Therefore, the sum of probability for detecting the eavesdropper $\mathbb{P}_{Sum_{(A)}}$ for u_A is equal to ½ as shown in Eq. (34 , 35)

$$\mathbb{P}_{Sum_{(A)}} = \frac{1}{4}\left(\mathbb{P}_{00_{(A)}} + \mathbb{P}_{01_{(A)}} + \mathbb{P}_{10_{(A)}} + \mathbb{P}_{11_{(A)}}\right) \tag{34}$$

$$\mathbb{P}_{Sum_{(A)}} = \frac{1}{2} \tag{35}$$

According to Simmons theory, the consequence of Eq. (35) verified that the proposed scheme is unconditionally secured under this kind of attack.

Masquerade as Dishonest Multicast User B

By assuming that the eavesdropper will work only on particle *B* which means particles *A and C* are not included and we excluded it from the transmitted state, so the eavesdropper performing its operation $|0_B\mathbb{R}>$ and $|1_B\mathbb{R}>$, a new transmitted state will be generated as showing in Eq. (36,37)

$$|\Psi_{(SB)}> \rightarrow |\Psi_{(SB)}{}'> \tag{36}$$

$$|\Psi_{(SB)}{}'> = \frac{1}{\sqrt{2}}(\alpha_2|0_S0_B0_E> + \beta_2|0_S0_B1_E> + \gamma_2|0_S1_B0_E> + \delta_2|0_S1_B1_E> + \alpha_3|1_S0_B0_E> + \beta_3|1_S0_B1_E> + \gamma_3|1_S1_B0_E> + \delta_3|1_S1_B1_E>) \tag{37}$$

The eavesdropper transfers the new prepared state $|\Psi_{(SB)}{}'>$ to QAS. Subsequently, QAS applies $\not{\mathbb{C}}_{NOT}$ on the received state as outcome one of four states $|\Psi_{(SB)}^{00}>$,$|\Psi_{(SB)}^{01}>$,$|\Psi_{(SB)}^{10}>$,$|\Psi_{(SB)}^{11}>$ which corresponding to the paired bits 00, 01, 10 and 11. By assuming when the paired bits are equivalent to 00 and 01 then QAS operation is equivalent as in Eq. $(38-40)$.

$$|\Psi_{(SB)}^{00}> = \not{\mathbb{C}}_0\,|\Psi_{(SB)}{}'> \tag{38}$$

By performing $\not{\mathbb{C}}_0$ the result is obtained in Eq. (39,40)

$$|\Psi_{(SB)}^{00}> = \frac{1}{\sqrt{2}}(\alpha_2|0_S0_B0_E> + \beta_2|0_S0_B1_E> + \gamma_2|0_S1_B0_E> + \delta_2|0_S1_B1_E> + \alpha_3|1_S0_B1_E> + \beta_3|1_S0_B0_E> + \gamma_3|1_S1_B1_E> + \delta_3|1_S1_B0_E>) \quad (39)$$

$$|\Psi_{(SB)}^{01}> = \frac{1}{\sqrt{2}}(\alpha_2|0_S0_B1_E> + \beta_2|0_S0_B0_E> + \gamma_2|0_S1_B1_E> + \delta_2|0_S1_B0_E> + \alpha_3|1_S0_B0_E> + \beta_3|1_S0_B1_E> + \gamma_3|1_S1_B0_E> + \delta_3|1_S1_B1_E>) \quad (40)$$

So the possibility for detecting the eavesdropper for $|\Psi_{(SB)}^{00}>$ and is $\mathbb{P}_{00_{(B)}}$ can be computed from Eq. (39) as shown in Eq. (41).

$$\mathbb{P}_{00_{(B)}} = \frac{1}{2}(|\alpha_3^2|+|\gamma_3^2|+|\beta_2^2|+|\delta_2^2|) \quad (41)$$

As well when the dual bits are equivalent to 01, so the chance for discovering the eavesdropper for $|\Psi_{(SB)}^{01}>$ is $\mathbb{P}_{01_{(B)}}$ can be computed from Eq. (40) as shown in Eq. (42)

$$\mathbb{P}_{01_{(B)}} = \frac{1}{2}(|\alpha_2^2|+|\gamma_2^2|+|\beta_3^2|+|\delta_3^2|) \quad (42)$$

Additionally, the probability for detecting the eavesdropper $\mathbb{P}_{10_{(B)}}$ and $\mathbb{P}_{11_{(B)}}$ is equivalent to $\mathbb{P}_{00_{(B)}}$ and $\mathbb{P}_{01_{(B)}}$respectively. Therefore, the sum of probability for detecting the eavesdropper $\mathbb{P}_{Sum_{(B)}}$ for u_B is equal to ½ as shown in Eq. (43 , 44)

$$\mathbb{P}_{Sum_{(B)}} = \frac{1}{4}(\mathbb{P}_{00_{(B)}} + \mathbb{P}_{01_{(B)}} + \mathbb{P}_{10_{(B)}} + \mathbb{P}_{11_{(B)}}) \quad (43)$$

$$\mathbb{P}_{Sum_{(B)}} = \frac{1}{2} \quad (44)$$

According to Simmons theory, the consequence of Eq. (44) verified that the proposed scheme is unconditionally secured under this kind of attack.

Masquerade as Dishonest Multicast User C

By assuming that the eavesdropper will work only on particle C which means particles *A and C* are not included and we excluded it from the transmitted state, so the eavesdropper performing its operation $|0_C\mathbb{R}>$ and $|1_C\mathbb{R}>$, a new transmitted state will be generated as showing in Eq. (45,46)

$$|\Psi_{(SC)}> \rightarrow |\Psi_{(SC)}{}'> \quad (45)$$

$$|\Psi_{(SC)}{}'> = \frac{1}{\sqrt{2}}(\alpha_4|0_S0_C0_E> + \beta_4|0_S0_C1_E> + \gamma_4|0_S1_C0_E> + \delta_4|0_S1_C1_E> + \alpha_5|1_S0_C0_E> + \beta_5|1_S0_C1_E> + \gamma_5|1_S1_C0_E> + \delta_5|1_S1_C1_E>) \quad (46)$$

The eavesdropper transfers the new prepared state $|\Psi_{(SC)}{}'>$ to QAS. Subsequently, QAS applies $\not{\mathbb{C}}_{NOT}$ on the received state as outcome one of four states $|\Psi_{(SC)}^{00}>$,$|\Psi_{(SC)}^{01}>$,$|\Psi_{(SC)}^{10}>$,$|\Psi_{(SC)}^{11}>$ which corresponding to the paired bits 00, 01, 10 and 11. By assuming when the paired bits are equivalent to 00 and 01 then QAS operation is equivalent as in Eq. $(47-49)$.

$$|\Psi_{(SC)}^{00}> = \not{\mathbb{C}}_0\ |\Psi_{(SC)}{}'> \tag{47}$$

By performing $\not{\mathbb{C}}_0$ the result is obtained in Eq. (48,49)

$$|\Psi_{(SC)}^{00}> = \frac{1}{\sqrt{2}}(\alpha_4|0_S0_C0_E> + \beta_4|0_S0_C1_E> + \gamma_4|0_S1_C0_E> + \delta_4|0_S1_C1_E> + \alpha_5|1_S0_C1_E> + \beta_5|1_S0_C0_E> + \gamma_5|1_S1_C1_E> + \delta_5|1_S1_C0_E>) \tag{48}$$

$$|\Psi_{(SC)}^{01}> = \frac{1}{\sqrt{2}}(\alpha_4|0_S0_C1_E> + \beta_4|0_S0_C0_E> + \gamma_4|0_S1_C1_E> + \delta_4|0_S1_C0_E> + \alpha_5|1_S0_C0_E> + \beta_5|1_S0_C1_E> + \gamma_5|1_S1_C0_E> + \delta_5|1_S1_C1_E>) \tag{49}$$

So the possibility for detecting the eavesdropper for $|\Psi_{(SC)}^{00}>$ is $\mathbb{P}_{00_{(C)}}$ can be computed from Eq. (48) as shown in Eq. (50).

$$\mathbb{P}_{00_{(A)}} = \frac{1}{2}\ (|\alpha_5^2|+|\gamma_5^2|+|\beta_4^2|+|\delta_4^2|\ ) \tag{50}$$

As well when the paired bits are equivalent to 01, so the chance for discovering the eavesdropper for $|\Psi_{(SA)}^{01}>$ is $\mathbb{P}_{01_{(A)}}$ can be computed from Eq. (49) as shown in Eq. (51)

$$\mathbb{P}_{01_{(A)}} = \frac{1}{2}\ (|\alpha_4^2|+|\gamma_4^2|+|\beta_5^2|+|\delta_5^2|\ ) \tag{51}$$

Additionally, the probability for detecting the eavesdropper $\mathbb{P}_{10_{(C)}}$ and $\mathbb{P}_{11_{(C)}}$ is equivalent to $\mathbb{P}_{00_{(C)}}$ and $\mathbb{P}_{01_{(C)}}$ respectively. Therefore, the sum of probability for detecting the eavesdropper $\mathbb{P}_{Sum_{(C)}}$ for u_C is equal to ½ as shown in Eq. (52 , 53)

$$\mathbb{P}_{Sum_{(C)}} = \frac{1}{4}\ (\mathbb{P}_{00_{(C)}} + \mathbb{P}_{01_{(C)}} + \mathbb{P}_{10_{(C)}} + \mathbb{P}_{11_{(C)}}) \tag{52}$$

$$\mathbb{P}_{Sum_{(C)}} = \frac{1}{2} \tag{53}$$

According to Simmons theory, the consequence of Eq. (53) verified that the proposed scheme is unconditionally secured under this kind of attack.

Masquerade as Dishonest Multicast User A and B

By assuming that the eavesdropper will work on two particles A and B at same time. So the eavesdropper performing its four operations $|0_A\mathbb{R}>$,$|1_A\mathbb{R}>$, $|0_B\mathbb{R}>$ and $|1_B\mathbb{R}>$, a new transmitted state will be generated as showing in Eq. (54,55)

$$|\Psi_{(SAB)}> \rightarrow\ |\Psi_{(SAB)}{}'> \tag{54}$$

$$|\Psi_{(SAB)}{}' > = \frac{1}{\sqrt{2}}(\alpha_0\alpha_2|0_S0_A0_B0_E > + \beta_0\beta_2|0_S0_A0_B1_E > + \alpha_0\gamma_2|0_S0_A1_B0_E > + \beta_0\delta_2|0_S0_A1_B1_E > + \gamma_0\alpha_2|0_S1_A0_B0_E > + \delta_0\beta_2|0_S1_A0_B1_E > + \gamma_0\gamma_2|0_S1_A1_B0_E > + \delta_0\delta_2|0_S1_A1_B1_E > + \alpha_1\alpha_3|1_S0_A0_B0_E > + \beta_1\beta_3|1_S0_A0_B1_E > + \alpha_1\gamma_3|1_S0_A1_B0_E > + \beta_1\delta_3|1_S0_A1_B1_E > + \gamma_1\alpha_3|1_S1_A0_B0_E > + \delta_1\beta_3|1_S1_A0_B1_E > + \gamma_1\gamma_3|1_S1_A1_B0_E > + \delta_1\delta_3|1_S1_A1_B1_E >) \quad (55)$$

The eavesdropper transfers the new prepared state $|\Psi_{(SAB)}{}' >$ to QAS. Subsequently, QAS applies $\not{C}_{NOT}$ on the received state as outcome one of eight states $|\Psi_{(SAB)}^{000} >$, $|\Psi_{(SAB)}^{001} >$, $|\Psi_{(SAB)}^{010} >$, $|\Psi_{(SAB)}^{011} >$, $|\Psi_{(SAB)}^{100} >$, $|\Psi_{(SAB)}^{101} >$,$|\Psi_{(SAB)}^{110} >$ and $|\Psi_{(SAB)}^{111} >$ which corresponding to the tri−bits 000, 001, 010, 011, 100, 101, 110 and 111. By assuming when the tri−bits are equivalent to 000 and 001 then QAS operation is equivalent as in Eq. (56).

$$|\Psi_{(SAB)}^{000} > = \frac{1}{\sqrt{2}}(\alpha_0\alpha_2|0_S0_A0_B0_E > + \beta_0\beta_2|0_S0_A0_B1_E > + \alpha_0\gamma_2|0_S0_A1_B0_E > + \beta_0\delta_2|0_S0_A1_B1_E > + \gamma_0\alpha_2|0_S1_A0_B0_E > + \delta_0\beta_2|0_S1_A0_B1_E > + \gamma_0\gamma_2|0_S1_A1_B0_E > + \delta_0\delta_2|0_S1_A1_B1_E > + \alpha_1\alpha_3|1_S0_A0_B1_E > + \beta_1\beta_3|1_S0_A0_B0_E > + \alpha_1\gamma_3|1_S0_A1_B1_E > + \beta_1\delta_3|1_S0_A1_B0_E > + \gamma_1\alpha_3|1_S1_A0_B1_E > + \delta_1\beta_3|1_S1_A0_B0_E > + \gamma_1\gamma_3|1_S1_A1_B1_E > + \delta_1\delta_3|1_S1_A1_B0_E >) \quad (56)$$

So the possibility for detecting the eavesdropper for $|\Psi_{(SAB)}^{000} >$ is $₱_{000_{(SAB)}}$ can be computed from Eq. (56) as shown in Eq. (57).

$$₱_{000_{(SAB)}} = \frac{1}{2} (|\alpha_1\alpha_3{}^2| + |\gamma_1\alpha_3{}^2| + |\beta_0\beta_2{}^2| + |\delta_0\beta_2{}^2| + |\alpha_1\gamma_3{}^2| + |\gamma_1\gamma_3{}^2| + |\beta_0\delta_2{}^2| + |\delta_0\delta_2{}^2|) \quad (57)$$

As well when the tri−bits are equivalent to 001, so the chance for discovering the eavesdropper for $|\Psi_{(SAB)}^{001} >$ is $₱_{001_{(SAB)}}$ can be computed from Eq. (56) as shown in Eq. (58)

$$₱_{001_{(SAB)}} = \frac{1}{2} (|\alpha_0\alpha_2{}^2| + |\gamma_0\alpha_2{}^2| + |\beta_1\beta_3{}^2| + |\delta_1\beta_3{}^2| + |\alpha_0\gamma_2{}^2| + |\gamma_0\gamma_2{}^2| + |\beta_1\delta_3{}^2| + |\delta_1\delta_3{}^2|) \quad (56)$$

Additionally, the probability for detecting the eavesdropper $₱_{011_{(SAB)}}$, $₱_{101_{(SAB)}}$ and $₱_{110_{(SAB)}}$ is equivalent to $₱_{000_{(SAB)}}$. As well $₱_{010_{(SAB)}}$, $₱_{100_{(SAB)}}$ and $₱_{111_{(SAB)}}$ is equivalent to $₱_{001_{(SAB)}}$. Therefore, the sum of probability for detecting the eavesdropper $₱_{Sum_{(SAB)}}$ for u_A and u_B is equal to ½ as shown in Eq. (57 , 58)

$$₱_{Sum_{(SAB)}} = \frac{1}{8} (₱_{000_{(SAB)}} + ₱_{001_{(SAB)}} + ₱_{010_{(SAB)}} + ₱_{011_{(SAB)}} + ₱_{100_{(SAB)}} + ₱_{101_{(SAB)}} + ₱_{110_{(SAB)}} + ₱_{111_{(SAB)}}) \quad (57)$$

$$₱_{Sum_{(SAB)}} = \frac{1}{2} \quad (58)$$

According to Simmons theory, the consequence of Eq. (58) verified that the proposed scheme is unconditionally secured under this kind of attack.

Masquerade as Dishonest Multicast User A and C

By assuming that the eavesdropper will work on two particles A and C at same time; which means particle B is not included and we excluded it from the transmitted state. So the eavesdropper performing its four operations $|0_A\mathbb{R}>$,$|1_A\mathbb{R}>$, $|0_C\mathbb{R}>$ and $|1_C\mathbb{R}>$, a new transmitted state will be generated as showing in Eq. (59,60)

$$|\Psi_{(SAC)}> \rightarrow |\Psi_{(SAC)}{}'> \tag{59}$$

$$\begin{aligned}|\Psi_{(SAC)}{}'> = \tfrac{1}{\sqrt{2}}(\,&\alpha_0\alpha_4|0_S0_A0_C0_E> + \beta_0\beta_4|0_S0_A0_C1_E> + \alpha_0\gamma_4|0_S0_A1_C0_E> + \beta_0\delta_4|0_S0_A1_C1_E> \\ &+ \gamma_0\alpha_4|0_S1_A0_C0_E> + \delta_0\beta_4|0_S1_A0_C1_E> + \gamma_0\gamma_4|0_S1_A1_C0_E> + \delta_0\delta_4|0_S1_A1_C1_E> \\ &+ \alpha_1\alpha_5|1_S0_A0_C0_E> + \beta_1\beta_5|1_S0_A0_C1_E> + \alpha_1\gamma_5|1_S0_A1_C0_E> + \beta_1\delta_5|1_S0_A1_C1_E> \\ &+ \gamma_1\alpha_5|1_S1_A0_C0_E> + \delta_1\beta_5|1_S1_A0_C1_E> + \gamma_1\gamma_5|1_S1_A1_C0_E> + \delta_1\delta_5|1_S1_A1_C1_E>)\end{aligned} \tag{60}$$

The eavesdropper transfers the new prepared state $|\Psi_{(SAC)}{}'>$ to QAS. Subsequently, QAS applies $\not\subset_{NOT}$ on the received state as outcome one of eight states $|\Psi^{000}_{(SAC)}>$, $|\Psi^{001}_{(SAC)}>$, $|\Psi^{010}_{(SAC)}>$, $|\Psi^{011}_{(SAC)}>$, $|\Psi^{100}_{(SAC)}>$, $|\Psi^{101}_{(SAC)}>$,$|\Psi^{110}_{(SAC)}>$ and $|\Psi^{111}_{(SAC)}>$ which corresponding to the tri−bits 000, 001, 010, 011, 100, 101, 110 and 111. By assuming when the tri−bits are equivalent to 000 and 001 then QAS operation is equivalent as in Eq. (61).

$$\begin{aligned}|\Psi^{000}_{(SAC)}> = \tfrac{1}{\sqrt{2}}(\,&\alpha_0\alpha_4|0_S0_A0_C0_E> + \beta_0\beta_4|0_S0_A0_C1_E> + \alpha_0\gamma_4|0_S0_A1_C0_E> + \\ &\beta_0\delta_4|0_S0_A1_C1_E> + \gamma_0\alpha_4|0_S1_A0_C0_E> + \delta_0\beta_4|0_S1_A0_C1_E> + \gamma_0\gamma_4|0_S1_A1_C0_E> + \\ &\delta_0\delta_4|0_S1_A1_C1_E> + \alpha_1\alpha_5|1_S0_A0_C1_E> + \beta_1\beta_5|1_S0_A0_C0_E> + \alpha_1\gamma_5|1_S0_A1_C1_E> + \\ &\beta_1\delta_5|1_S0_A1_C0_E> + \gamma_1\alpha_5|1_S1_A0_C1_E> + \delta_1\beta_5|1_S1_A0_C0_E> + \gamma_1\gamma_5|1_S1_A1_C1_E> + \\ &\delta_1\delta_5|1_S1_A1_C0_E>)\end{aligned} \tag{61}$$

So the possibility for detecting the eavesdropper for $|\Psi^{000}_{(SAC)}>$ is $\mathbb{P}_{000_{(SAC)}}$ can be computed from Eq. (61) as shown in Eq. (62).

$$\mathbb{P}_{000_{(SAC)}} = \tfrac{1}{2}\,(|\alpha_1\alpha_5{}^2| + |\gamma_1\alpha_5{}^2| + |\beta_0\beta_4{}^2| + |\delta_0\beta_4{}^2| + |\alpha_1\gamma_5{}^2| + |\gamma_1\gamma_5{}^2| + |\beta_0\delta_4{}^2| + |\delta_0\delta_4{}^2|\,) \tag{62}$$

As well when the tri−bits are equivalent to 001, so the chance for discovering the eavesdropper for $|\Psi^{001}_{(SAC)}>$ is $\mathbb{P}_{001_{(SAC)}}$ can be computed from Eq. (61) as shown in Eq. (63)

$$\mathbb{P}_{001_{(SAC)}} = \tfrac{1}{2}\,(|\alpha_0\alpha_4{}^2| + |\gamma_0\alpha_4{}^2| + |\beta_1\beta_5{}^2| + |\delta_1\beta_5{}^2| + |\alpha_0\gamma_4{}^2| + |\gamma_0\gamma_4{}^2| + |\beta_1\delta_5{}^2| + |\delta_1\delta_5{}^2|) \tag{63}$$

Additionally, the probability for detecting the eavesdropper $\mathbb{P}_{011_{(SAC)}}$, $\mathbb{P}_{101_{(SAC)}}$ and $\mathbb{P}_{110_{(SAC)}}$ is equivalent to $\mathbb{P}_{000_{(SAC)}}$. As well $\mathbb{P}_{010_{(SAC)}}$, $\mathbb{P}_{100_{(SAC)}}$ and $\mathbb{P}_{111_{(SAC)}}$ is equivalent to $\mathbb{P}_{001_{(SAC)}}$. Therefore, the sum of probability for detecting the eavesdropper $\mathbb{P}_{Sum_{(SAC)}}$ for u_A and u_C is equal to ½ as shown in Eq. (64 , 65)

$$\mathbb{P}_{Sum_{(SAC)}} = \tfrac{1}{8}\,(\mathbb{P}_{000_{(SAC)}} + \mathbb{P}_{001_{(SAC)}} + \mathbb{P}_{010_{(SAC)}} + \mathbb{P}_{011_{(SAC)}} + \mathbb{P}_{100_{(SAC)}} + \mathbb{P}_{101_{(SAC)}} + \mathbb{P}_{110_{(SAC)}} + \mathbb{P}_{111_{(SAC)}}) \tag{64}$$

$$\mathbb{P}_{Sum_{(SAC)}} = \tfrac{1}{2} \tag{65}$$

According to Simmons theory, the consequence of Eq. (65) verified that the proposed scheme is unconditionally secured under this kind of attack.

Masquerade as Dishonest Multicast User B and C

By assuming that the eavesdropper will work on two particles B and C at same time; which means particle A is not included and we excluded it from the transmitted state. So the eavesdropper performing its four operations $|0_B\mathbb{R}>$,$|1_B\mathbb{R}>$, $|0_C\mathbb{R}>$ and $|1_C\mathbb{R}>$, a new transmitted state will be generated as showing in Eq. (66,67)

$$|\Psi_{(SBC)}> \rightarrow |\Psi_{(SBC)}{}'> \tag{66}$$

$$\begin{aligned}|\Psi_{(SBC)}{}'> = \tfrac{1}{\sqrt{2}}(\,&\alpha_2\alpha_4|0_S0_B0_C0_E> + \beta_2\beta_4|0_S0_B0_C1_E> + \alpha_2\gamma_4|0_S0_B1_C0_E> + \beta_2\delta_4|0_S0_B1_C1_E> \\ &+ \gamma_2\alpha_4|0_S1_B0_C0_E> + \delta_2\beta_4|0_S1_B0_C1_E> + \gamma_2\gamma_4|0_S1_B1_C0_E> + \delta_2\delta_4|0_S1_B1_C1_E> \\ &+ \alpha_3\alpha_5|1_S0_B0_C0_E> + \beta_3\beta_5|1_S0_B0_C1_E> + \alpha_3\gamma_5|1_S0_B1_C0_E> + \beta_3\delta_5|1_S0_B1_C1_E> \\ &+ \gamma_3\alpha_5|1_S1_B0_C0_E> + \delta_3\beta_5|1_S1_B0_C1_E> + \gamma_3\gamma_5|1_S1_B1_C0_E> + \delta_5|1_S1_B1_C1_E>)\end{aligned} \tag{67}$$

The eavesdropper transfers the new prepared state $|\Psi_{(SBC)}{}'>$ to QAS. Subsequently, QAS applies $\not\subset_{NOT}$ on the received state as outcome one of eight states $|\Psi^{000}_{(SBC)}>$, $|\Psi^{001}_{(SBC)}>$, $|\Psi^{010}_{(SBC)}>$, $|\Psi^{011}_{(SBC)}>$, $|\Psi^{100}_{(SBC)}>$, $|\Psi^{101}_{(SBC)}>$,$|\Psi^{110}_{(SBC)}>$ and $|\Psi^{111}_{(SBC)}>$ which corresponding to the tri−bits 000, 001, 010, 011, 100, 101, 110 and 111. By assuming when the tri−bits are equivalent to 000 and 001 then QAS operation is equivalent as in Eq. (68).

$$\begin{aligned}|\Psi^{000}_{(SBC)}> = \tfrac{1}{\sqrt{2}}(\,&\alpha_2\alpha_4|0_S0_B0_C0_E> + \beta_2\beta_4|0_S0_B0_C1_E> + \alpha_2\gamma_4|0_S0_B1_C0_E> + \beta_2\delta_4|0_S0_B1_C1_E> \\ &+ \gamma_2\alpha_4|0_S1_B0_C0_E> + \delta_2\beta_4|0_S1_B0_C1_E> + \gamma_2\gamma_4|0_S1_B1_C0_E> + \delta_2\delta_4|0_S1_B1_C1_E> \\ &+ \alpha_3\alpha_5|1_S0_B0_C1_E> + \beta_3\beta_5|1_S0_B0_C0_E> + \alpha_3\gamma_5|1_S0_B1_C1_E> + \beta_3\delta_5|1_S0_B1_C0_E> \\ &+ \gamma_3\alpha_5|1_S1_B0_C1_E> + \delta_3\beta_5|1_S1_B0_C0_E> + \gamma_3\gamma_5|1_S1_B1_C1_E> + \delta_3\delta_5|1_S1_B1_C0_E>)\end{aligned} \tag{68}$$

So the possibility for detecting the eavesdropper for $|\Psi^{000}_{(SBC)}>$ is $₱_{000_{(SBC)}}$ can be computed from Eq. (68) as shown in Eq. (69).

$$₱_{000_{(SBC)}} = \tfrac{1}{2}\,(|\alpha_3\alpha_5{}^2| + |\gamma_3\alpha_5{}^2| + |\beta_2\beta_4{}^2| + |\delta_2\beta_4{}^2| + |\alpha_3\gamma_5{}^2| + |\gamma_3\gamma_5{}^2| + |\beta_2\delta_4{}^2| + |\delta_2\delta_4{}^2|\,) \tag{69}$$

As well when the tri−bits are equivalent to 001, so the chance for discovering the eavesdropper for $|\Psi^{001}_{(SBC)}>$ is $₱_{001_{(SBC)}}$ can be computed from Eq. (68) as shown in Eq. (70)

$$₱_{001_{(SBC)}} = \tfrac{1}{2}\,(|\alpha_2\alpha_4{}^2| + |\gamma_2\alpha_4{}^2| + |\beta_3\beta_5{}^2| + |\delta_3\beta_5{}^2| + |\alpha_2\gamma_4{}^2| + |\gamma_2\gamma_4{}^2| + |\beta_3\delta_5{}^2| + |\delta_3\delta_5{}^2|) \tag{70}$$

Additionally, the probability for detecting the eavesdropper $₱_{011_{(SBC)}}$, $₱_{101_{(SBC)}}$ and $₱_{110_{(SBC)}}$ is equivalent to $₱_{000_{(SBC)}}$. As well $₱_{010_{(SBC)}}$, $₱_{100_{(SBC)}}$ and $₱_{111_{(SBC)}}$ is equivalent to $₱_{001_{(SBC)}}$. Therefore, the sum of probability for detecting the eavesdropper $₱_{Sum_{(SBC)}}$ for u_B and u_C is equal to ½ as shown in Eq. (71 , 72)

$$₱_{Sum_{(SBC)}} = \tfrac{1}{8}\,(₱_{000_{(SBC)}} + ₱_{001_{(SBC)}} + ₱_{010_{(SBC)}} + ₱_{011_{(SBC)}} + ₱_{100_{(SBC)}} + ₱_{101_{(SBC)}} + ₱_{110_{(SBC)}} + ₱_{111_{(SBC)}}) \tag{71}$$

$$₱_{Sum_{(SBC)}} = \tfrac{1}{2} \tag{72}$$

According to Simmons theory, the consequence of Eq. (72) verified that the proposed scheme is unconditionally secured under this kind of attack.

Masquerade as Dishonest Multicast User A, B and C

By assuming that the eavesdropper will work on three particles , B and C at the same , a new transmitted state will be generated as showing in Eq. (73,74)

$$|\Psi_{(SABC)}> \rightarrow |\Psi_{(SABC)}{}'> \tag{73}$$

$$\begin{aligned}|\Psi_{(SABC)}{}'> = \tfrac{1}{\sqrt{2}}(\,&\alpha_0\alpha_2\alpha_4|0_S0_A0_B0_C0_E> + \beta_0\beta_2\beta_4|0_S0_A0_B0_C1_E> + \alpha_0\alpha_2\gamma_4|0_S0_A0_B1_C0_E> + \\ &\beta_0\beta_2\delta_4|0_S0_A0_B1_C1_E> + \alpha_0\gamma_2\alpha_4|0_S0_A1_B0_C0_E> + \beta_0\delta_2\beta_4|0_S0_A1_B0_C1_E> + \alpha_0\gamma_2\gamma_4|0_S0_A1_B1_C0_E> + \\ &\beta_0\delta_2\delta_4|0_S0_A1_B1_C1_E> + \gamma_0\alpha_2\alpha_4|0_S1_A0_B0_C0_E> + \delta_0\beta_2\beta_4|0_S1_A0_B0_C1_E> + \gamma_0\alpha_2\gamma_4|0_S1_A0_B1_C0_E> + \\ &\delta_0\beta_2\delta_4|0_S1_A0_B1_C1_E> + \gamma_0\gamma_2\alpha_4|0_S1_A1_B0_C0_E> + \delta_0\delta_2\beta_4|0_S1_A1_B0_C1_E> + \gamma_0\gamma_2\gamma_4|0_S1_A1_B1_C0_E> + \\ &\delta_0\delta_2\delta_4|0_S1_A1_B1_C1_E> + \alpha_1\alpha_3\alpha_5|1_S0_A0_B0_C0_E> + \beta_1\beta_3\beta_5|1_S0_A0_B0_C1_E> + \alpha_1\alpha_3\gamma_5|1_S0_A0_B1_C0_E> + \\ &\beta_1\beta_3\delta_5|1_S0_A0_B1_C1_E> + \alpha_1\gamma_3\alpha_5|1_S0_A1_B0_C0_E> + \beta_1\delta_3\beta_5|1_S0_A1_B0_C1_E> + \alpha_1\gamma_3\gamma_5|1_S0_A1_B1_C0_E> + \\ &\beta_1\delta_3\delta_5|1_S0_A1_B1_C1_E> + \gamma_1\alpha_3\alpha_5|1_S1_A0_B0_C0_E> + \delta_1\beta_3\beta_5|1_S1_A0_B0_C1_E> + \gamma_1\alpha_3\gamma_5|1_S1_A0_B1_C0_E> + \\ &\delta_1\beta_3\delta_5|1_S1_A0_B1_C1_E> + \gamma_1\gamma_3\alpha_5|1_S1_A1_B0_C0_E> + \delta_1\delta_3\beta_5|1_S1_A1_B0_C1_E> + \gamma_1\gamma_3\gamma_5|1_S1_A1_B1_C0_E> + \\ &\delta_1\delta_3\delta_5|1_S1_A1_B1_C1_E>)\end{aligned} \tag{74}$$

The eavesdropper transfers the new prepared state $|\Psi_{(SABC)}{}'>$ to QAS. Subsequently, QAS applies $\not{C}_{NOT}$ on the received state as outcome one of sixteen states $|\Psi^{0000}_{(SABC)}>$, $|\Psi^{0001}_{(SABC)}>$, $|\Psi^{0010}_{(SABC)}>$, $|\Psi^{0011}_{(SABC)}>$, $|\Psi^{0100}_{(SABC)}>$, $|\Psi^{0101}_{(SABC)}>$, $|\Psi^{0110}_{(SABC)}>$ $|\Psi^{0111}_{(SABC)}>$, $|\Psi^{1000}_{(SABC)}>$, $|\Psi^{1001}_{(SABC)}>$, $|\Psi^{1010}_{(SABC)}>$, $|\Psi^{1011}_{(SABC)}>$, $|\Psi^{1100}_{(SABC)}>$, $|\Psi^{1101}_{(SABC)}>$, $|\Psi^{1110}_{(SABC)}>$ and $|\Psi^{1111}_{(SABC)}>$ which corresponding to the four−bits $0000, \ldots\ldots, 1111$. By assuming when the four−bits are equivalent to 0000 then QAS operation is equivalent as in Eq. (75 , 76).

$$\begin{aligned}|\Psi^{000}_{(SABC)}> = \tfrac{1}{\sqrt{2}}(\,&\alpha_0\alpha_2\alpha_4|0_S0_A0_B0_C0_E> + \beta_0\beta_2\beta_4|0_S0_A0_B0_C1_E> + \alpha_0\alpha_2\gamma_4|0_S0_A0_B1_C0_E> + \\ &\beta_0\beta_2\delta_4|0_S0_A0_B1_C1_E> + \alpha_0\gamma_2\alpha_4|0_S0_A1_B0_C0_E> + \beta_0\delta_2\beta_4|0_S0_A1_B0_C1_E> + \alpha_0\gamma_2\gamma_4|0_S0_A1_B1_C0_E> + \\ &\beta_0\delta_2\delta_4|0_S0_A1_B1_C1_E> + \gamma_0\alpha_2\alpha_4|0_S1_A0_B0_C0_E> + \delta_0\beta_2\beta_4|0_S1_A0_B0_C1_E> + \gamma_0\alpha_2\gamma_4|0_S1_A0_B1_C0_E> + \\ &\delta_0\beta_2\delta_4|0_S1_A0_B1_C1_E> + \gamma_0\gamma_2\alpha_4|0_S1_A1_B0_C0_E> + \delta_0\delta_2\beta_4|0_S1_A1_B0_C1_E> + \gamma_0\gamma_2\gamma_4|0_S1_A1_B1_C0_E> + \\ &\delta_0\delta_2\delta_4|0_S1_A1_B1_C1_E> + \alpha_1\alpha_3\alpha_5|1_S0_A0_B0_C0_E> + \beta_1\beta_3\beta_5|1_S0_A0_B0_C1_E> + \alpha_1\alpha_3\gamma_5|1_S0_A0_B1_C0_E> + \\ &\beta_1\beta_3\delta_5|1_S0_A0_B1_C1_E> + \alpha_1\gamma_3\alpha_5|1_S0_A1_B0_C0_E> + \beta_1\delta_3\beta_5|1_S0_A1_B0_C1_E> + \alpha_1\gamma_3\gamma_5|1_S0_A1_B1_C0_E> + \\ &\beta_1\delta_3\delta_5|1_S0_A1_B1_C1_E> + \gamma_1\alpha_3\alpha_5|1_S1_A0_B0_C0_E> + \delta_1\beta_3\beta_5|1_S1_A0_B0_C1_E> + \gamma_1\alpha_3\gamma_5|1_S1_A0_B1_C0_E> + \\ &\delta_1\beta_3\delta_5|1_S1_A0_B1_C1_E> + \gamma_1\gamma_3\alpha_5|1_S1_A1_B0_C0_E> + \delta_1\delta_3\beta_5|1_S1_A1_B0_C1_E> + \gamma_1\gamma_3\gamma_5|1_S1_A1_B1_C0_E> + \\ &\delta_1\delta_3\delta_5|1_S1_A1_B1_C1_E>)\end{aligned} \tag{75}$$

So the possibility for detecting the eavesdropper for $|\Psi^{0000}_{(SABC)}>$ is $\text{₱}_{0000_{(SABC)}}$ can be computed from Eq. (75) as shown in Eq. (76).

$$\begin{aligned}\text{₱}_{0000_{(SABC)}} = \tfrac{1}{2}\,(&|\beta_0\,\beta_2\beta_4{}^2| + |\beta_0\beta_2\delta_4{}^2| + |\beta_0\delta_2\delta_4{}^2| + |\delta_0\beta_2\delta_4{}^2| + |\delta_0\delta_2\delta_4{}^2| + |\alpha_1\alpha_3\alpha_5{}^2| + |\alpha_1\gamma_3\alpha_5{}^2| + \\ &|\gamma_1\gamma_3\alpha_5{}^2| + (|\gamma_1\alpha_3\alpha_5{}^2| + |\beta_0\delta_2\beta_4{}^2| + |\delta_0\beta_2\beta_4{}^2| + |\delta_0\delta_2\beta_4{}^2| + |\alpha_1\alpha_3\gamma_5{}^2| + |\alpha_1\gamma_3\gamma_5{}^2| + \\ &|\gamma_1\alpha_3\gamma_5{}^2| + |\gamma_1\gamma_3\gamma_5{}^2|\,)\end{aligned} \tag{76}$$

As well when the four−bits are equivalent to 0001, so the chance for discovering the eavesdropper for $|\Psi^{0001}_{(SABC)}>$ is $\text{₱}_{0001_{(SABC)}}$ can be computed from Eq. (75) as shown in Eq. (77)

$$\text{₱}_{0001_{(SABC)}} = \frac{1}{2}\left(|\alpha_0\alpha_2\alpha_4{}^2| + |\alpha_0\alpha_2\gamma_4{}^2| + |\alpha_0\gamma_2\alpha_4{}^2| + |\alpha_0\gamma_2\gamma_4{}^2| + |\gamma_0\alpha_2\alpha_4{}^2| + |\gamma_0\alpha_2\gamma_4{}^2| + |\gamma_0\gamma_2\alpha_4{}^2| + |\gamma_0\gamma_2\gamma_4{}^2| + \left(\left|\beta_1\beta_3\beta_5{}^2\right| + \left|\beta_1\beta_3\delta_5{}^2\right| + \left|\beta_1\delta_3\delta_5{}^2\right| + \left|\delta_1\beta_3\delta_5{}^2\right| + \left|\beta_1\delta_3\beta_5{}^2\right| + \left|\delta_1\beta_3\beta_5{}^2\right| + \left|\delta_1\delta_3\beta_5{}^2\right| + \left|\delta_1\delta_3\delta_5{}^2\right|\right) \quad (77)$$

Additionally, the probability for detecting the eavesdropper $\text{₱}_{0011_{(SABC)}}$, $\text{₱}_{0101_{(SABC)}}$, $\text{₱}_{0110_{(SABC)}}$, $\text{₱}_{1001_{(SABC)}}$, $\text{₱}_{1010_{(SABC)}}$, $\text{₱}_{1100_{(SABC)}}$, $\text{₱}_{1111_{(SABC)}}$ is equivalent to $\text{₱}_{0000_{(SABC)}}$. As well $\text{₱}_{0010_{(SABC)}}$, $\text{₱}_{0100_{(SABC)}}$, $\text{₱}_{0111_{(SABC)}}$, $\text{₱}_{1000_{(SABC)}}$, $\text{₱}_{1011_{(SABC)}}$, $\text{₱}_{1101_{(SABC)}}$, $\text{₱}_{1110_{(SABC)}}$ is equivalent to $\text{₱}_{0001_{(SABC)}}$. Therefore, the sum of probability for detecting the eavesdropper $\text{₱}_{Sum_{(SABC)}}$ for u_A , u_B and u_C is equal to ½ as shown in Eq. (78 , 79)

$$\text{₱}_{Sum_{(SABC)}} = \frac{1}{16}\left(\text{₱}_{0000_{(SABC)}} + \text{₱}_{0001_{(SABC)}} + \text{₱}_{0010_{(SABC)}} + \text{₱}_{0011_{(SABC)}} + \text{₱}_{0100_{(SABC)}} + \text{₱}_{0101_{(SABC)}} + \text{₱}_{0110_{(SABC)}} + \text{₱}_{0111_{(SABC)}} + \text{₱}_{1000_{(SABC)}} + \text{₱}_{1001_{(SABC)}} + \text{₱}_{1010_{(SABC)}} + \text{₱}_{1011_{(SABC)}} + \text{₱}_{1100_{(SABC)}} + \text{₱}_{1101_{(SABC)}} + \text{₱}_{1110_{(SABC)}} + \text{₱}_{1111_{(SABC)}}\right) \quad (78)$$

$$\text{₱}_{Sum_{(SABC)}} = \frac{1}{2} \quad (79)$$

According to Simmons theory, the consequence of Eq. (79) verified that the proposed scheme is unconditionally secured under this kind of attack.

5 Two Way Channel Substitution Fraudulent Attack between Quantum Authentication Server and One User

The operation of the eavesdropper Θ_1 and ε on the transferred particle A is given by (Eq. (80) − (83))

$$|0_A\mathcal{E}> \rightarrow \alpha_\varepsilon|0_A\mathcal{E}_{00}> + \beta_\varepsilon|1_A\mathcal{E}_{01}> \quad (80)$$

$$|1_A\mathcal{E}> \rightarrow \beta_\varepsilon|0_A\mathcal{E}_{10}> + \alpha_\varepsilon|1_A\mathcal{E}_{11}> \quad (81)$$

$$|+_A\mathcal{E}> \rightarrow \frac{1}{2}|+_A>\left(\alpha_\varepsilon|\mathcal{E}_{00}> + \alpha_\varepsilon|\mathcal{E}_{11}> + \beta_\varepsilon|\mathcal{E}_{01}> + \beta_\varepsilon|\mathcal{E}_{10}>\right) + \frac{1}{2}|-_A>\left(\alpha_\varepsilon|\mathcal{E}_{00}> - \alpha_\varepsilon|\mathcal{E}_{11}> - \beta_\varepsilon|\mathcal{E}_{01}> + \beta_\varepsilon|\mathcal{E}_{10}>\right) \quad (82)$$

$$|-_A\mathcal{E}> \rightarrow \frac{1}{2}|+_A>\left(\alpha_\varepsilon|\mathcal{E}_{00}> - \alpha_\varepsilon|\mathcal{E}_{11}> + \beta_\varepsilon|\mathcal{E}_{01}> - \beta_\varepsilon|\mathcal{E}_{10}>\right) + \frac{1}{2}|-_A>\left(\alpha_\varepsilon|\mathcal{E}_{00}> + \alpha_\varepsilon|\mathcal{E}_{11}> - \beta_\varepsilon|\mathcal{E}_{01}> - \beta_\varepsilon|\mathcal{E}_{10}>\right) \quad (83)$$

The operation of the eavesdropper Θ_2 and μ on the transferred information particle $|\Phi_{n_{(A)}}>$ is given by (Eq. (84) −(87))

$$|0_{n_{(A)}}\mu> \rightarrow \alpha_\mu|0_{n_{(A)}}\mu_{00}> + \beta_\mu|1_{n_{(A)}}\mu_{01}> \quad (84)$$

$$|1_{n_{(A)}}\mu> \rightarrow \beta_\mu|0_{n_{(A)}}\mu_{10}> + \alpha_\mu|1_{n_{(A)}}\mu_{11}> \quad (85)$$

$$|+_{n_{(A)}}\mu> \rightarrow \frac{1}{2}|+_{n_{(A)}}>(\alpha_\mu|\mu_{00}> + \alpha_\mu|\mu_{11}> + \beta_\mu|\mu_{01}> + \beta_\mu|\mu_{10}>) + \frac{1}{2}|-_{n_{(A)}}>(\alpha_\mu|\mu_{00}> - \alpha_\mu|\mu_{11}> - \beta_\mu|\mu_{01}> + \beta_\mu|\mu_{10}>) \quad (86)$$

$$|-_{n_{(A)}}\mu> \rightarrow \frac{1}{2}|+_{n_{(A)}}>(\alpha_\mu|\mu_{00}> - \alpha_\mu|\mu_{11}> + \beta_\mu|\mu_{01}> - \beta_\mu|\mu_{10}>) + \frac{1}{2}|-_{n_{(A)}}>(\alpha_\mu|\mu_{00}> + \alpha_\mu|\mu_{11}> - \beta_\mu|\mu_{01}> - \beta_\mu|\mu_{10}>) \quad (87)$$

Correspondingly, performing the unitary operation involves the following prerequisites see (Eq. (88) to (90))

$$|\alpha_\varepsilon^2|+|\beta_\varepsilon^2| = 1,\ |\alpha_\mu^2|+|\beta_\mu^2| = 1 \quad (88)$$

$$<\varepsilon_{00}\,|\,\varepsilon_{10}> + <\varepsilon_{01}\,|\,\varepsilon_{11}> = 0 \quad (89)$$

$$<\mu_{00}\,|\,\mu_{10}> + <\mu_{01}\,|\,\mu_{11}> = 0 \quad (90)$$

Additionally, for simplifying the discussion, assumes that equations for orthogonal conditions and equations for non-orthogonal conditions are given by (Eq. $(91-92)$) and (Eq. $(93-94)$) respectively.

$$<\varepsilon_{00}\,|\,\varepsilon_{01}> = <\varepsilon_{10}\,|\,\varepsilon_{11}> = <\varepsilon_{00}\,|\,\varepsilon_{10}> = <\varepsilon_{01}\,|\,\varepsilon_{11}> = 0 \quad (91)$$

$$<\mu_{00}\,|\,\mu_{01}> = <\mu_{10}\,|\,\mu_{11}> = <\mu_{00}\,|\,\mu_{10}> = <\mu_{01}\,|\,\mu_{11}> = 0 \quad (92)$$

$$<\varepsilon_{00}\,|\,\varepsilon_{11}> = \cos\theta_\varepsilon\,,\ <\varepsilon_{01}\,|\,\varepsilon_{10}> = \cos\varphi_\varepsilon \quad (93)$$

$$<\mu_{00}\,|\,\mu_{11}> = \cos\theta_\mu\,,\ <\mu_{01}\,|\,\mu_{10}> = \cos\varphi_\mu \quad (94)$$

When the two-bit key $J_i J_{i+1}$ = 00, so the subsequent encrypted state by QAS is given by (Eq. (95,96))

$$|\Psi_{(SA)}^{00}> = \not{\mathbb{C}}_0\,\Theta_2\ \{\ \not{\mathbb{C}}_0\ [\ \Theta_1\ (\ \Psi_{(SA)}^{00}\ |\ \varepsilon\ >)\ |\ |\Phi_{n_{(A)}}>\ ]\ \ |\ \mu\ >\ \} \quad (95)$$

$$|\Psi_{(SA)}^{00}> = \frac{1}{\sqrt{2}}\Big[(\alpha_\varepsilon\,\alpha_\mu\,|0_S0_A0_{n_{(A)}}\,\varepsilon_{00}\,\mu_{00}> + \alpha_\varepsilon\,\beta_\mu\,|0_S0_A1_{n_{(A)}}\,\varepsilon_{00}\,\mu_{01}> + \beta_\varepsilon\,\beta_\mu|0_S1_A0_{n_{(A)}}\,\varepsilon_{01}\,\mu_{10}> + \beta_\varepsilon\,\alpha_\mu|0_S1_A1_{n_{(A)}}\,\varepsilon_{01}\,\mu_{11}> + \beta_\varepsilon\,\alpha_\mu\,\Big|1_S0_A1_{n_{(A)}}\,\varepsilon_{10}\,\mu_{00}> + \beta_\varepsilon\,\beta_\mu\Big|\,1_S0_A0_{n_{(A)}}\,\varepsilon_{01}\,\mu_{01}> + \alpha_\varepsilon\,\beta_\mu\,|1_S1_A1_{n_{(A)}}\,\varepsilon_{11}\,\mu_{10}\ >\ + \alpha_\varepsilon\,\alpha_\mu\,|1_S1_A0_{n_{(A)}}\,\varepsilon_{11}\,\mu_{11}>)\ \Big] \quad (96)$$

The eavesdropper will be detected if the transferred particle state is not $|0_{n_{(A)}}>$, in such condition, the Probability of detecting the eavesdropper when $J_i\,J_{i+1}\ =\ 00$ is given by (Eq. (97))

$$\mathrm{P}_{\mathrm{Sum}}(J_i\,J_{i+1}\ =\ 00\ ) = (\alpha_\varepsilon\,\beta_\mu)^2 + (\beta_\varepsilon\,\alpha_\mu)^2 \quad (97)$$

By performing the comparable sequences from (Eq.$(95)\ -\ (97)$) for $J_i\ J_{i+1}\ =\ 01$ indicating that the Probability of detecting the eavesdropper is equivalent to $\mathrm{P}_{\mathrm{Sum}}(J_i\ J_{i+1} = 00\ )$. The Probability of detecting the eavesdropper when $J_i\ J_{i+1} = 10$ is given by (Eq. (98))

$$\mathbb{P}_{\mathrm{Sum}}(J_i\ J_{i+1} = 10\ ) = \frac{1}{2}\left[\left[\begin{array}{c}[\,(\alpha_\varepsilon\,\beta_\mu)^2(\,1+\cos\theta_\varepsilon) + (\beta_\varepsilon\,\beta_\mu)^2(\,1+\cos\varphi_\varepsilon) + (\alpha_\varepsilon\,\alpha_\mu)^2(\,1-\cos\theta_\varepsilon) \\ + (\beta_\varepsilon\,\alpha_\mu)^2(\,1-\cos\varphi_\varepsilon)]\end{array}\right]\right] \quad (98)$$

By performing the comparable sequences from (Eq.(95) − (97)) for $J_i\ J_{i+1} = 11$ indicating that the Probability of detecting the eavesdropper is equivalent to $\mathbb{P}_{\mathrm{Sum}}(J_i\ J_{i+1} = 10\ )$. From above equations we can realize that when $J_i = 0$ the Probability of detecting the eavesdropper is equivalent to $(\alpha_\varepsilon\,\beta_\mu)^2 + (\beta_\varepsilon\,\alpha_\mu)^2$and when $J_i = 1$ is equivalent to $\frac{1}{2}\left[\left[\,[\,(\alpha_\varepsilon\,\beta_\mu)^2(\,1+\cos\theta_\varepsilon) + (\beta_\varepsilon\,\beta_\mu)^2(\,1+\cos\varphi_\varepsilon) + (\alpha_\varepsilon\,\alpha_\mu)^2(\,1-\cos\theta_\varepsilon) + (\beta_\varepsilon\,\alpha_\mu)^2(\,1-\cos\varphi_\varepsilon)]\,\right]\right]$.

By combining Eq. (97) and Eq. (98), we can compute the total Probability of detecting the eavesdropper in the authentication process is given by (Eq. (99))

$$\mathbb{P}_{\mathrm{Sum}} = ½\,[\,\mathbb{P}_{\mathrm{Sum}}(J_i\ = 0\,) + \mathbb{P}_{\mathrm{Sum}}(J_i\ = 1\,)] \quad (99)$$

If the eavesdropper would like to reduce his detecting possibility then the eavesdropper has to adapt $\mathbb{P}_{\mathrm{Sum}}$ as minimum detecting possibility see (Eq. (100)). Eq. (100) computed under the assumption of $\alpha_\varepsilon = \alpha_\mu = 1$

$$Sum = Min(\mathbb{P}_{\mathrm{Sum}}) = \frac{1}{4}\,(1 - cos\ \theta_\varepsilon) \quad (100)$$

From Eq. (100) it's shown that $Min(\mathbb{P}_{\mathrm{Sum}})$ is correlated on $cos\ \theta_\varepsilon$ but uncorrelated to θ_μ. Therefore, the eavesdropper's unconditional information amount on the transferred key bits among QAS and u_A can be approximated by (Eq. (101)).

$$\mathfrak{T}(J_K\ , \Theta_{Total}\,) = \sum_{x,y} \mathcal{P}\big(J_K\ , \Theta_{Total}\,\big) \log_2 \frac{\mathcal{P}(J_K\ , \Theta_{Total}\,)}{\mathcal{P}(J_K)\,\mathcal{P}(\,\Theta_{Total})} \quad (101)$$

Where Θ_{Total} denotes the total operation applied by the eavesdropper Θ_1 and Θ_2, x denotes the key values (00, 01, 10, 11) with probability $\mathcal{P}(x) = \frac{1}{4}$, J_K specifies the chosen random values from variable x , $y = \varepsilon_{ij}\mu_{\upsilon\tau}$ with i, j, $\upsilon\,, \tau \in \{\,0\,, 1\}$ which denotes 16 probabilities of the joint measurement result of the eavesdropper at positions Θ_1 and Θ_2. For restoring the value of eavesdropper's unconditional information amount from Eq. (101). We should only realize the $\mathcal{P}(J_K)$ and $\mathcal{P}(\,\Theta_{Total}\,|\,J_K\,)$ by (Eq. (102))

$$\mathcal{P}(J_K\ , \Theta_{Total}\,) = \mathcal{P}(\,J_K\,)\mathcal{P}(\,\Theta_{Total}\,|\,J_K\,) \quad (102)$$

Supposing a particular case 'P($\varepsilon_{00}\,\mu_{00}$ | 00) by substituting in Eq. (96), the reduced detecting possibility of the eavesdropper's unconditional operation Θ_{Total} is either $\varepsilon_{00}\,\mu_{00}$ or $\varepsilon_{11}\,\mu_{11}$ with equal probability of ½ when J_{2i-1} $J_{2i} = 00$ see (Eq. (103))

$$|\Psi_{Sum_{SA}}^{00}> = \frac{1}{\sqrt{2}}(\ |0_S 0_A 0_{n_{(A)}}\varepsilon_{00}\,\mu_{00}> + |1_S 1_A 0_{n_{(A)}}\varepsilon_{11}\,\mu_{11}> \quad (103)$$

Since $<\varepsilon_{00}\,|\,\varepsilon_{11}> = cos\ \theta_\varepsilon$ from Eq. (93) so,

$$\mathcal{P}(\,\mathcal{E}_{00}\,\mu_{00}\mid 00\,) = (1\,+\,sin\,\theta_{\mathcal{E}})\,/\,2 \tag{104}$$

As $(x) = \frac{1}{4}$, so $\mathcal{P}(00\,) = \frac{1}{4}$ and from (Eq. (104)) $\mathcal{P}(\,\mathcal{E}_{00}\,\mu_{00}\mid 00\,)$ = $(1\,+\,sin\,\theta_{\mathcal{E}})$ / 2. Accordingly by substitution in Eq. (102), the eavesdropper's unconditional information amount on the transferred key bits J_{2i-1} $J_{2i} = 00$ is given by (Eq. (105))

$$\mathcal{P}(\;00\,,\,\mathcal{E}_{00}\,\mu_{00}\;) = \mathcal{P}(00\,)\mathcal{P}(\,\mathcal{E}_{00}\,\mu_{00}\mid 00\,) = \frac{1+sin\,\theta_{\mathcal{E}}}{8} \tag{105}$$

Therefore, the mutual obtained information by eavesdropper's total operation Θ_{Total} is given by (Eq. (106))

$$\mathfrak{T} = \frac{1}{4}\,[\,(\,1 + sin\,\theta_{\mathcal{E}}\,)\log_2(\,1 + sin\,\theta_{\mathcal{E}}\,) + (\,1 - sin\,\theta_{\mathcal{E}}\,)\log_2(\,1 - sin\,\theta_{\mathcal{E}}\,)\,] \tag{106}$$

Since $\sin\theta_{\mathcal{E}} = \sqrt{8 \times Sum - 16 \times\ Sum^2}$ (see Supplementary Information (7) for Proving Relation between $\sin\theta_{\mathcal{E}}$ and Sum), by substitution in Eq. (106)

$$\begin{aligned}\mathfrak{T} = \frac{1}{4}\,[\,(\,1 + \sqrt{8 \times Sum - 16 \times\ Sum^2})\log_2(\,1 + \sqrt{8 \times Sum - 16 \times\ Sum^2}\,) \\ + (\,1 - \sqrt{8 \times Sum - 16 \times\ Sum^2})\log_2(\,1 - \sqrt{8 \times Sum - 16 \times\ Sum^2}\,)\end{aligned} \tag{107}$$

The correlation between the mutual information $\mathfrak{T}$ and the minimum detecting possibility Sum for the eavesdropper is shown in Table S1 and Figure S2

Table S1. Correlation between Mutual Information $\mathfrak{T}$ and the Minimum Detecting Possibility Sum for One User

Sum	0%	5%	10%	12.5%	25%	35%	45%	50%
$\mathfrak{T}$ (Bits) One User	0	0.139	0.2655	0.3227	0.5	0.37717	0.139	0

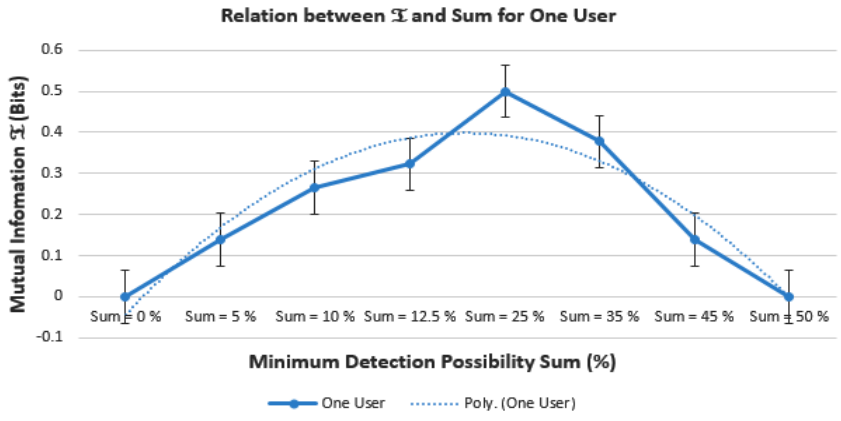


Fig. S2 The Correlation between the Mutual Information $\mathfrak{T}$ and the Minimum Detecting Possibility Sum for One User.

If the eavesdropper would like for unconditionally obtaining the transferred authentication key J_K between QAS and u_A ,so for every transferred key, the eavesdropper must conclude which $two-bits$ are utilized for the authentication process. In accordance with the eavesdropper's measurement output $y = \mathcal{E}_{ij}\mu_{\upsilon\tau}$ with $i,j,\upsilon,\tau \in \{0,1\}$, and the key values $(00,01,10,11)$. Therefore, the eavesdropper can conclude the probability of the transmitted key bits.

For example if $y = \mathcal{E}_{00}\mu_{11}$ then the eavesdropper can conclude that the transferred authentication key bits either 00, 10 or 11 with probability equal to 0.5, 0.25 and 0.25 respectively. By supposing that the eavesdropper selects the likelihood for identifying the transmitted key values 00 or 01 is $\mathcal{P}$ and for identifying 10 or 11 is $1-\mathcal{P}$ and take into consideration the unsuccessful measurement result as in Eq. (105). Consequently, the unconditional detection possibility $\mathcal{P}_e$ of J_K is given by (Eq. (108))

$$\mathcal{P}_e = \frac{(1+\sin\theta_\mathcal{E})}{2}\left[\frac{1}{2}\mathcal{P} + \frac{1}{4}(1-\mathcal{P})\right] + \frac{(1-\sin\theta_\mathcal{E})}{2}\left[\frac{1}{4}(1-\mathcal{P})\right] \tag{108}$$

By simplification of Eq. (108) $\mathcal{P}_e$ of J_K is given by (Eq. (109)) (see Supplementary Information (8) for Proving Relation between $\mathcal{P}_e$, $\mathcal{P}$ and $\sin\theta_\mathcal{E}$)

$$\mathcal{P}_e = \frac{1}{8}[\,(\sin\theta_\mathcal{E}(3\times\mathcal{P}-1)+4] \tag{109}$$

If $\mathcal{P}=1$ implies that the detection possibility $\mathcal{P}_e$ is maximized see (Eq. (110)) (see Supplementary Information (9) for Proving Relation between $\mathcal{P}_e$, ${\mathcal{P}_e}^m$ and Sum)

$${\mathcal{P}_e}^m = \frac{1}{4}\left(\sqrt{16\times Sum - 16\times Sum^2}+1\right) \tag{110}$$

Table S2 and Figure S3 show the correlation between maximized unconditional detection Possibility ${\mathcal{P}_e}^m$ and the minimum detection possibility Sum

Table S2 Correlation between Maximized Unconditional Detection Possibility ${\mathcal{P}_e}^m$ and Sum for One User

Sum	0%	5%	10%	12.5%	25%	35%	45%	50%
${\mathcal{P}_e}^m$	0.25	0.40	0.45	0.47	0.50	0.47	0.4	0.25

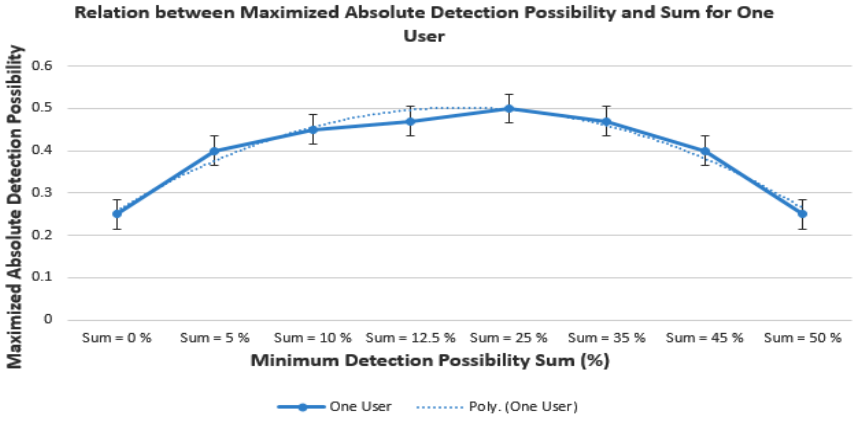


Fig. S3 Correlation between Maximized Unconditional Detection Possibility $\mathcal{P}_e{}^m$ and Sum for One User.

Therefore, the possibility of the eavesdropper for positively retrieving the transferred keys $\mathcal{P}_e{}^r \; for \, J_k = \{J_1, J_2, J_3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots J_{2N}\}$ see (Eq. (111))

$$\mathcal{P}_e{}^r = [\mathcal{P}_e{}^m(1 - Sum)]^{N/2} \tag{111}$$

By substituting (Eq. (110)) in equation (Eq. (111), so

$$\mathcal{P}_e{}^r = \left[\tfrac{1}{4}\left(\sqrt{8 \times Sum - 16 \times Sum^2} + 1\right)(1 - Sum)\right]^{N/2} \tag{112}$$

6 Two Way Channel Substitution Fraudulent Attack between Quantum Authentication Server and Two Users.

Firstly, the eavesdropper listens to the communication channel and intercept the transmitting particle from QAS to u_A and u_B . The eavesdropper applies operations Θ_1 and Θ_2 along with supportive particles $\mathcal{E}, \gamma$ at his side on the transmitted particles A and B respectively. Subsequently, the eavesdropper transfers the produced particle to u_A and u_B. Once u_A and u_B obtain the resulted transferred particle, they doesn't know there is an eavesdropper and he executed an operation. Both u_A and u_B apply their ordinary operations and transfer the resulted particle to QAS. The eavesdropper interrupts the new state particle sent by u_A and u_B. The eavesdropper performs operations Θ_3 and Θ_4 along with supportive particles μ, η at his side on the new particles $|\Phi_{n_{(A)}}>$ and $|\Phi_{n_{(B)}}>$ respectively. Successively, the eavesdropper transfers the resulted particle to QAS. The eavesdropper attempts to obtain a confident amount of information about the key by utilizing two supportive particles ε, μ on particle A and other two γ, η on particle B.

The operation of the eavesdropper Θ_1 and ε on the transferred particle A is given by (Eq. (113) − (116))

$$|0_A\mathcal{E}> \rightarrow \alpha_\varepsilon|0_A\mathcal{E}_{00}> + \beta_\varepsilon|1_A\mathcal{E}_{01}> \tag{113}$$

$$|1_A\mathcal{E}> \rightarrow \beta_\varepsilon|0_A\mathcal{E}_{10}> + \alpha_\varepsilon|1_A\mathcal{E}_{11}> \tag{114}$$

$$\begin{aligned} |+_A\,\mathcal{E}> \rightarrow\; & \tfrac{1}{2}|+_A>(\alpha_\varepsilon|\mathcal{E}_{00}> + \alpha_\varepsilon|\mathcal{E}_{11}> + \beta_\varepsilon|\mathcal{E}_{01}> + \beta_\varepsilon|\mathcal{E}_{10}>) \\ & + \tfrac{1}{2}|-_A>(\alpha_\varepsilon|\mathcal{E}_{00}> - \alpha_\varepsilon|\mathcal{E}_{11}> - \beta_\varepsilon|\mathcal{E}_{01}> + \beta_\varepsilon|\mathcal{E}_{10}>) \end{aligned} \tag{115}$$

$$\begin{aligned} |-_A\,\mathcal{E}> \rightarrow\; & \tfrac{1}{2}|+_A>(\alpha_\varepsilon|\mathcal{E}_{00}> - \alpha_\varepsilon|\mathcal{E}_{11}> + \beta_\varepsilon|\mathcal{E}_{01}> - \beta_\varepsilon|\mathcal{E}_{10}>) \\ & + \tfrac{1}{2}|-_A>(\alpha_\varepsilon|\mathcal{E}_{00}> + \alpha_\varepsilon|\mathcal{E}_{11}> - \beta_\varepsilon|\mathcal{E}_{01}> - \beta_\varepsilon|\mathcal{E}_{10}>) \end{aligned} \tag{116}$$

Correspondingly, the operation of the eavesdropper Θ_2 and γ on the transferred particle B *is* given by (Eq. (117) − (120))

$$|0_{\mathrm{B}}\gamma> \rightarrow \alpha_{\gamma}|0_{\mathrm{B}}\gamma_{00}> + \beta_{\gamma}|1_{\mathrm{B}}\gamma_{01}> \quad (117)$$

$$|1_{\mathrm{B}}\gamma> \rightarrow \beta_{\gamma}|0_{\mathrm{B}}\gamma_{10}> + \alpha_{\gamma}|1_{\mathrm{B}}\gamma_{11}> \quad (118)$$

$$|+_{\mathrm{B}}\gamma> \rightarrow \frac{1}{2}|+_{\mathrm{B}}>(\alpha_{\gamma}|\gamma_{00}> + \alpha_{\gamma}|\gamma_{11}> + \beta_{\gamma}|\gamma_{01}> + \beta_{\gamma}|\gamma_{10}>) + \frac{1}{2}|-_{\mathrm{B}}>(\alpha_{\gamma}|\gamma_{00}> - \alpha_{\gamma}|\gamma_{11}> - \beta_{\gamma}|\gamma_{01}> + \beta_{\gamma}|\gamma_{10}>) \quad (119)$$

$$|-_{\mathrm{B}}\gamma> \rightarrow \frac{1}{2}|+_{\mathrm{B}}>(\alpha_{\gamma}|\gamma_{00}> - \alpha_{\gamma}|\gamma_{11}> + \beta_{\gamma}|\gamma_{01}> - \beta_{\gamma}|\gamma_{10}>) + \frac{1}{2}|-_{\mathrm{B}}>(\alpha_{\gamma}|\gamma_{00}> + \alpha_{\gamma}|\gamma_{11}> - \beta_{\gamma}|\gamma_{01}> - \beta_{\gamma}|\gamma_{10}>) \quad (120)$$

The operation of the eavesdropper Θ_3 and μ on the transferred information particle $|\Phi_{n_{(A)}}>$ is given by (Eq. (121) $-$(124))

$$|0_{\mathrm{n}_{(A)}}\mu> \rightarrow \alpha_{\mu}|0_{\mathrm{n}_{(A)}}\mu_{00}> + \beta_{\mu}|1_{\mathrm{n}_{(A)}}\mu_{01}> \quad (121)$$

$$|1_{\mathrm{n}_{(A)}}\mu> \rightarrow \beta_{\mu}|0_{\mathrm{n}_{(A)}}\mu_{10}> + \alpha_{\mu}|1_{\mathrm{n}_{(A)}}\mu_{11}> \quad (122)$$

$$|0_{\mathrm{n}_{(A)}}\mu> \rightarrow \frac{1}{2}|+_{\mathrm{n}_{(A)}}>(\alpha_{\mu}|\mu_{00}> + \alpha_{\mu}|\mu_{11}> + \beta_{\mu}|\mu_{01}> + \beta_{\mu}|\mu_{10}>) + \frac{1}{2}|-_{\mathrm{n}_{(A)}}>(\alpha_{\mu}|\mu_{00}> - \alpha_{\mu}|\mu_{11}> - \beta_{\mu}|\mu_{01}> + \beta_{\mu}|\mu_{10}>) \quad (123)$$

$$|-_{\mathrm{n}_{(A)}}\mu> \rightarrow \frac{1}{2}|+_{\mathrm{n}_{(A)}}>(\alpha_{\mu}|\mu_{00}> - \alpha_{\mu}|\mu_{11}> + \beta_{\mu}|\mu_{01}> - \beta_{\mu}|\mu_{10}>) + \frac{1}{2}|-_{\mathrm{n}_{(A)}}>(\alpha_{\mu}|\mu_{00}> + \alpha_{\mu}|\mu_{11}> - \beta_{\mu}|\mu_{01}> - \beta_{\mu}|\mu_{10}>) \quad (124)$$

Correspondingly, the operation of the eavesdropper Θ_4 and η on the transferred information particle $|\Phi_{n_{(B)}}>$ is given by (Eq. (125) $-$ (128))

$$|0_{\mathrm{n}_{(B)}}\eta> \rightarrow \alpha_{\eta}|0_{\mathrm{n}_{(B)}}\eta_{00}> + \beta_{\eta}|1_{\mathrm{n}_{(B)}}\eta_{01}> \quad (125)$$

$$|1_{\mathrm{n}_{(B)}}\eta> \rightarrow \beta_{\eta}|0_{\mathrm{n}_{(B)}}\eta_{10}> + \alpha_{\eta}|1_{\mathrm{n}_{(B)}}\eta_{11}> \quad (126)$$

$$|+_{\mathrm{n}_{(B)}}\eta> \rightarrow \frac{1}{2}|+_{\mathrm{n}_{(B)}}>(\alpha_{\eta}|\eta_{00}> + \alpha_{\eta}|\eta_{11}> + \beta_{\eta}|\eta_{01}> + \beta_{\eta}|\eta_{10}>) + \frac{1}{2}|-_{\mathrm{n}_{(B)}}>(\alpha_{\eta}|\eta_{00}> - \alpha_{\eta}|\eta_{11}> - \beta_{\eta}|\eta_{01}> + \beta_{\eta}|\eta_{10}>) \quad (127)$$

$$|-_{\mathrm{n}_{(B)}}\eta> \rightarrow \frac{1}{2}|+_{\mathrm{n}_{(B)}}>(\alpha_{\eta}|\eta_{00}> - \alpha_{\eta}|\eta_{11}> + \beta_{\eta}|\eta_{01}> - \beta_{\eta}|\eta_{10}>) + \frac{1}{2}|-_{\mathrm{n}_{(B)}}>(\alpha_{\eta}|\eta_{00}> + \alpha_{\eta}|\eta_{11}> - \beta_{\eta}|\eta_{01}> - \beta_{\eta}|\eta_{10}>) \quad (128)$$

Correspondingly, performing the unitary operation involves the following prerequisites see (Eq. (129) to (133))

$$|\alpha_{\varepsilon}^2|+|\beta_{\varepsilon}^2| = 1,\ |\alpha_{\eta}^2|+|\beta_{\eta}^2|,\ |\alpha_{\mu}^2|+|\beta_{\mu}^2| = 1,\ |\alpha_{\gamma}^2|+|\beta_{\gamma}^2| = 1 \quad (129)$$

$$<\varepsilon_{00}\,|\,\varepsilon_{10}> + <\varepsilon_{01}\,|\,\varepsilon_{11}> = 0 \quad (130)$$

$$<\eta_{00}\,|\,\eta_{10}> + <\eta_{01}\,|\,\eta_{11}> = 0 \quad (131)$$

$$<\mu_{00}\,|\,\mu_{10}> + <\mu_{01}\,|\,\mu_{11}> = 0 \quad (132)$$

$$<\gamma_{00}\,|\,\gamma_{10}> + <\gamma_{01}\,|\,\gamma_{11}> = 0 \quad (133)$$

Additionally, for simplifying the discussion, assumes that equations for orthogonal conditions and equations for non-orthogonal conditions are given by (Eq. $(134-137)$) and (Eq. $(138-141)$) respectively.

$$< \mathcal{E}_{00} \mid \mathcal{E}_{01} > = < \mathcal{E}_{10} \mid \mathcal{E}_{11} > = < \mathcal{E}_{00} \mid \mathcal{E}_{10} > = < \mathcal{E}_{01} \mid \mathcal{E}_{11} > \; = \; 0 \tag{134}$$

$$< \eta_{00} \mid \eta_{01} > = < \eta_{10} \mid \eta_{11} > = < \eta_{00} \mid \eta_{10} > = < \eta_{01} \mid \eta_{11} > \; = \; 0 \tag{135}$$

$$< \mu_{00} \mid \mu_{01} > = < \mu_{10} \mid \mu_{11} > = < \mu_{00} \mid \mu_{10} > = < \mu_{01} \mid \mu_{11} > \; = \; 0 \tag{136}$$

$$< \gamma_{00} \mid \gamma_{01} > = < \gamma_{10} \mid \gamma_{11} > = < \gamma_{00} \mid \gamma_{10} > = < \gamma_{01} \mid \gamma_{11} > \; = 0 \tag{137}$$

$$< \mathcal{E}_{00} \mid \mathcal{E}_{11} > = \cos \theta_{\mathcal{E}} \, , < \mathcal{E}_{01} \mid \mathcal{E}_{10} > = \cos \varphi_{\mathcal{E}} \tag{138}$$

$$< \eta_{00} \mid \eta_{11} > = \cos \theta_{\eta} \, , < \eta_{01} \mid \eta_{10} > = \cos \varphi_{\eta} \tag{139}$$

$$< \mu_{00} \mid \mu_{11} > = \cos \theta_{\mu} \, , < \mu_{01} \mid \mu_{10} > = \cos \varphi_{\mu} \tag{140}$$

$$< \gamma_{00} \mid \gamma_{11} > = \cos \theta_{\gamma} \, , < \gamma_{01} \mid \gamma_{10} > = \cos \varphi_{\gamma} \tag{141}$$

When the three-bit key $J_{i-1} J_i \; J_{i+1} \; = 000$, so the subsequent encrypted state by QAS is given by (Eq. (142, 143))

$$|\Psi^{000}_{(SAB)} > = \not{\mathbb{C}}_0 \, \Theta_3 \Theta_4 \; \{ \not{\mathbb{C}}_0 \; [\Theta_1 \; (\Psi^{000}_{(SAB)} \mid \mathcal{E} >) \mid |\Phi_{\mathrm{n}_{(A)}} >] \; [\Theta_2 \; (\Psi^{000}_{i\,(SAB)} \mid \gamma >) \mid |\Phi_{\mathrm{n}_{(B)}} >] \mid \mu > \mid \eta > \; \} \tag{142}$$

$$\begin{aligned} |\Psi^{000}_{(SAB)} > = \tfrac{1}{\sqrt{2}} \Big[(\alpha_{\mathcal{E}} \, \alpha_{\mu} \, |0_{\mathrm{S}} 0_{\mathrm{A}} 0_{\mathrm{n}_{(A)}} \, \mathcal{E}_{00} \, \mu_{00} > \; + \alpha_{\mathcal{E}} \, \beta_{\mu} \, |0_{\mathrm{S}} 0_{\mathrm{A}} 1_{\mathrm{n}_{(A)}} \, \mathcal{E}_{00} \, \mu_{01} > \; + \beta_{\mathcal{E}} \, \beta_{\mu} |0_{\mathrm{S}} 1_{\mathrm{A}} 0_{\mathrm{n}_{(A)}} \, \mathcal{E}_{01} \, \mu_{10} > \\ + \beta_{\mathcal{E}} \, \alpha_{\mu} |0_{\mathrm{S}} 1_{\mathrm{A}} 1_{\mathrm{n}_{(A)}} \, \mathcal{E}_{01} \, \mu_{11} > + \beta_{\mathcal{E}} \, \alpha_{\mu} \, \big| 1_{\mathrm{S}} 0_{\mathrm{A}} 1_{\mathrm{n}_{(A)}} \, \mathcal{E}_{10} \, \mu_{00} > \; + \beta_{\mathcal{E}} \, \beta_{\mu} \big| \, 1_{\mathrm{S}} 0_{\mathrm{A}} 0_{\mathrm{n}_{(A)}} \, \mathcal{E}_{01} \, \mu_{01} > \\ + \alpha_{\mathcal{E}} \, \beta_{\mu} \, |1_{\mathrm{S}} 1_{\mathrm{A}} 1_{\mathrm{n}_{(A)}} \, \mathcal{E}_{11} \, \mu_{10} \; > \; + \alpha_{\mathcal{E}} \, \alpha_{\mu} \, |1_{\mathrm{S}} 1_{\mathrm{A}} 0_{\mathrm{n}_{(A)}} \, \mathcal{E}_{11} \, \mu_{11} >) \; \Big] + \Big[(\alpha_{\gamma} \, \alpha_{\eta} \, |0_{\mathrm{S}} 0_{\mathrm{B}} 0_{\mathrm{n}_{(B)}} \, \gamma_{00} \, \eta_{00} > \\ + \alpha_{\gamma} \, \beta_{\eta} \, |0_{\mathrm{S}} 0_{\mathrm{B}} 1_{\mathrm{n}_{(B)}} \, \gamma_{00} \, \eta_{01} > \; + \beta_{\gamma} \, \beta_{\eta} |0_{\mathrm{S}} 1_{\mathrm{B}} 0_{\mathrm{n}_{(B)}} \, \gamma_{01} \, \eta_{10} > \; + \beta_{\gamma} \, \alpha_{\eta} |0_{\mathrm{S}} 1_{\mathrm{B}} 1_{\mathrm{n}_{(B)}} \, \gamma_{01} \, \eta_{11} > \\ + \beta_{\gamma} \, \alpha_{\eta} \, \big| 1_{\mathrm{S}} 0_{\mathrm{B}} 1_{\mathrm{n}_{(B)}} \, \gamma_{10} \, \eta_{00} > \; + \beta_{\gamma} \, \beta_{\eta} \big| \, 1_{\mathrm{S}} 0_{\mathrm{B}} 0_{\mathrm{n}_{(B)}} \, \gamma_{01} \, \eta_{01} > \; + \alpha_{\gamma} \, \beta_{\eta} \, |1_{\mathrm{S}} 1_{\mathbf{B}} 1_{\mathrm{n}_{(B)}} \, \gamma_{11} \, \eta_{10} \; > \\ + \alpha_{\gamma} \, \alpha_{\eta} \, |1_{\mathrm{S}} 1_{\mathrm{B}} 0_{\mathrm{n}_{(B)}} \, \gamma_{11} \, \eta_{11} >) \; \Big] \end{aligned} \tag{143}$$

The eavesdropper will be detected if the transferred particle state is not $|0_{\mathrm{n}_{(A)}} >$ or $|0_{\mathrm{n}_{(B)}} >$, in such condition, the Probability of detecting the eavesdropper when $J_{i-1} J_i \; J_{i+1} = \; 000$ is given by (Eq. (144))

$$\mathbb{P}_{\mathrm{Sum}}(J_{i-1} J_i \; J_{i+1} \; = \; 000 \;) = (\alpha_{\mathcal{E}} \, \beta_{\mu})^2 + \; (\beta_{\mathcal{E}} \, \alpha_{\mu})^2 + (\alpha_{\gamma} \, \beta_{\eta})^2 + \; (\beta_{\gamma} \, \alpha_{\eta})^2 \tag{144}$$

By performing the comparable sequences from (Eq. $(142) - (144)$) for $J_{i-1} J_i \; J_{i+1} \; = \; 001 \, , 010$ and 011 indicating that the Probability of detecting the eavesdropper is equivalent to $\mathbb{P}_{\mathrm{Sum}}(J_{i-1} J_i \; J_{i+1} = \; 000 \;)$.

The Probability of detecting the eavesdropper when $J_{i-1} J_i \; J_{i+1} = \; 100$ is given by (Eq. (145))

$$\mathbb{P}_{\mathrm{Sum}}(J_{i-1}\,J_i\;J_{i+1}=\;100\;\;)=\frac{1}{2}\Big[\Big[\,[\,(\alpha_\varepsilon\,\beta_\mu)^2(\,1+\cos\theta_\varepsilon)+\,\big(\beta_\varepsilon\,\beta_\mu\big)^2(\,1+\cos\varphi_\varepsilon)+\,\big(\alpha_\varepsilon\,\alpha_\mu\big)^2(\,1-\cos\theta_\varepsilon)+\big(\beta_\varepsilon\,\alpha_\mu\big)^2(\,1-\cos\varphi_\varepsilon)]\,\Big]+\Big[\,[\,(\alpha_\gamma\,\beta_\eta)^2\big(\,1+\cos\theta_\gamma\big)+\,\big(\beta_\gamma\,\beta_\eta\big)^2\big(\,1+\cos\varphi_\gamma\big)+\,\big(\alpha_\gamma\,\alpha_\eta\big)^2\big(\,1-\cos\theta_\gamma\big)+\big(\beta_\gamma\,\alpha_\eta\big)^2(\,1-\cos\varphi_\gamma)]\,\Big]\Big] \tag{145}$$

By performing the comparable sequences from (Eq. (142) − (144)) for $J_{i-1}J_i\;\;J_{i+1}\;=101\,,110$ and 111 indicating that the Probability of detecting the eavesdropper is equivalent to $\mathbb{P}_{\mathrm{Sum}}(J_{i-1}\,J_i\;J_{i+1}=100\;)$. From above equations we can realize that when $J_{i-1}\;=\;0$ the Probability of detecting the eavesdropper is equivalent to $(\alpha_\varepsilon\,\beta_\mu)^2+\;(\beta_\varepsilon\,\alpha_\mu)^2+(\alpha_\gamma\,\beta_\eta)^2+\;(\beta_\gamma\,\alpha_\eta)^2$ and when $J_{i-1}\;=\;1$ is equivalent to $\frac{1}{2}\Big[\Big[\,[\,(\alpha_\varepsilon\,\beta_\mu)^2(\,1+\cos\theta_\varepsilon)+(\beta_\varepsilon\,\beta_\mu)^2(\,1+\cos\varphi_\varepsilon)+\,\big(\alpha_\varepsilon\,\alpha_\mu\big)^2(\,1-\cos\theta_\varepsilon)\;+\,\big(\beta_\varepsilon\,\alpha_\mu\big)^2(\,1-\cos\varphi_\varepsilon)]\,\Big]+\Big[\,[\,(\alpha_\gamma\,\beta_\eta)^2(\,1+\cos\theta_\gamma)+(\beta_\gamma\,\beta_\eta)^2(\,1+\cos\varphi_\gamma)+\,\big(\alpha_\gamma\,\alpha_\eta\big)^2(\,1-\cos\theta_\gamma)\;+\,\big(\beta_\gamma\,\alpha_\eta\big)^2(\,1-\cos\varphi_\gamma)]\,\Big]\Big]$.

By combining Eq. (144) and Eq. (145), we can compute the total Probability of detecting the eavesdropper in the authentication process is given by (Eq. (146))

$$\mathbb{P}_{\mathrm{Sum}}=\tfrac{1}{2}\,[\,\mathbb{P}_{\mathrm{Sum}}(J_{i-1}\;=\;0\,)+\;\mathbb{P}_{\mathrm{Sum}}(J_{i-1}\;=\;1\,)] \tag{146}$$

If the eavesdropper would like to reduce his detecting possibility then the eavesdropper has to adapt $\mathbb{P}_{\mathrm{Sum}}$ as minimum detecting possibility see (Eq. (147)). Eq. (147) computed under the assumption of $\alpha_\varepsilon=\;\alpha_\eta=\alpha_\mu=\;\alpha_\gamma=1$

$$Sum=Min(\mathbb{P}_{\mathrm{Sum}})=\frac{1}{4}\,(1-cos\;\theta_\varepsilon+1-cos\;\theta_\gamma) \tag{147}$$

From Eq. (147) it's shown that $Min(\mathbb{P}_{\mathrm{Sum}})$ is correlated on $cos\;\theta_\varepsilon$ and $cos\;\theta_\gamma$ but uncorrelated to θ_η and θ_μ. Therefore, the eavesdropper's unconditional information amount on the transferred key bits among $QAS\;\;$, u_A and u_B can be approximated by (Eq. (148)).

$$\mathfrak{T}(J_K\;,\Theta_{Total}\,)=\sum_{x,y,z}\mathcal{P}\big(J_K\;,\Theta_{Total}\,\big)\log_2\frac{\mathcal{P}\big(J_K\;,\Theta_{Total}\,\big)}{\mathcal{P}(J_K)\,\mathcal{P}(\,\Theta_{Total})} \tag{148}$$

Where Θ_{Total} denotes the total operation applied by the eavesdropper $\Theta_1\;,\;\Theta_2\,,\Theta_3$ and Θ_4, x denotes the key values (000, 001, 010, 011, 100, 101, 110, 111) with probability $\mathcal{P}(x)=\frac{1}{8}$, J_K specifies the chosen random values from variable $x\,,\;y\;=\varepsilon_{ij}\mu_{\upsilon\tau}$ with $i,j,\upsilon\,,\tau\;\in\{\,0\,,1\}$ which denotes 16 probabilities of the joint measurement result of the eavesdropper at positions Θ_1 and $\Theta_3\,,\;z\;=\gamma_{kl}\eta_{\varsigma\varkappa}$ with $k,l,\varsigma\,,\varkappa\;\in\{\,0\,,1\}$ which denotes 16 probabilities of the joint measurement result of the eavesdropper at positions Θ_2 and Θ_4. For restoring the value of eavesdropper's unconditional information amount from Eq. (148). We should only realize the $\mathcal{P}(J_K)$ and $\mathcal{P}(\,\Theta_{Total}\,|\,J_K\,)$ by (Eq. (149))

$$\mathcal{P}(J_K\;,\Theta_{Total}\,)=\mathcal{P}(\,J_K\,)\mathcal{P}(\,\Theta_{Total}\,|\,J_K\,) \tag{149}$$

Supposing a particular case 'P($\mathcal{E}_{00}\,\mu_{00}\,\gamma_{00}\eta_{00}|\ 000$) by substituting in Eq. (143), the reduced detecting possibility of the eavesdropper's unconditional operation Θ_{Total} is either $\mathcal{E}_{00}\,\mu_{00}\,\gamma_{00}\eta_{00}$ or $\mathcal{E}_{11}\,\mu_{11}\,\gamma_{11}\eta_{11}$ with equal probability of ½ when $J_{2i-1}\,J_{2i}\,J_{2i+1} = 000$ see (Eq. (150))

$$|\Psi_{Sum}^{000}{}_{SAB}> = \frac{1}{\sqrt{2}}(\ |0_S 0_A 0_{n_{(A)}}\mathcal{E}_{00}\,\mu_{00}> + |1_S 1_A 0_{n_{(A)}}\mathcal{E}_{11}\,\mu_{11}> + |0_S 0_B 0_{n_{(B)}}\,\gamma_{00}\,\eta_{00}> + |1_S 1_B 0_{n_{(B)}}\,\gamma_{11}\,\eta_{11}> \tag{150}$$

Since $<\mathcal{E}_{00}\mid\mathcal{E}_{11}> = cos\ \theta_{\mathcal{E}}$ and $<\gamma_{00}\mid\gamma_{11}> = \cos\theta_{\gamma}$ from Eq. (138) and (141) respectively so,

$$\mathcal{P}(\ \mathcal{E}_{00}\,\mu_{00}\,\gamma_{00}\eta_{00}|\ 000\ ) = (2\ +\ sin\ \theta_{Sum})\ /\ 2 \tag{151}$$

As $(x) = \frac{1}{8}$, so $\mathcal{P}(000) = \frac{1}{8}$ and from (Eq. (151)) $\mathcal{P}(\ \mathcal{E}_{00}\,\mu_{00}\,\gamma_{00}\eta_{00}|\ 000\ ) = (2\ +\ sin\ \theta_{Sum})\ /\ 2$. Accordingly by substitution in Eq. (149), the eavesdropper's unconditional information amount on the transferred key bits $J_{2i-1}\,J_{2i}\,J_{2i+1} = 000$ is given by (Eq. (152))

$$\mathcal{P}(\ 000\ ,\ \mathcal{E}_{00}\,\mu_{00}\,\gamma_{00}\eta_{00}\ ) = \mathcal{P}(000)\mathcal{P}(\ \mathcal{E}_{00}\,\mu_{00}\,\gamma_{00}\eta_{00}|\ 000\ ) = \frac{2+sin\ \theta_{\mathrm{Sum}}}{16} \tag{152}$$

Therefore, the mutual obtained information by eavesdropper's total operation Θ_{Total} is given by (Eq. (153))

$$\mathfrak{T} = \frac{1}{8}\ [\ (\ 1 + sin\ \theta_{\mathrm{Sum}}\ )\log_2(\ 1 + sin\ \theta_{\mathrm{Sum}}\ ) + (\ 1 - sin\ \theta_{\mathrm{Sum}}\ )\log_2(\ 1 - sin\ \theta_{\mathrm{Sum}}\ )\ ] \tag{153}$$

Since $\sin\theta_{\mathrm{Sum}} = \sqrt{16 \times Sum - 16 \times\ Sum^2 - 3}$ (see Supplementary Information (10) for Proving Relation between $\sin\theta_{\mathrm{Sum}}$ and Sum), by substitution in Eq. (153)

$$\begin{aligned}\mathfrak{T} = \frac{1}{8}\ [\ &(\ 1 + \sqrt{16 \times Sum - 16 \times\ Sum^2 - 3})\log_2(\ 1 + \sqrt{16 \times Sum - 16 \times\ Sum^2 - 3}\ ) \\ &+ (\ 1 - \sqrt{16 \times Sum - 16 \times\ Sum^2 - 3})\log_2(\ 1 - \sqrt{16 \times Sum - 16 \times\ Sum^2 - 3}\ )\end{aligned} \tag{154}$$

The correlation between the mutual information $\mathfrak{T}$ and the minimum detecting possibility Sum for the eavesdropper is shown in Table S3 and Figure S4.

Table S3. Correlation between Mutual Information $\mathfrak{T}$ and the Minimum Detecting Possibility Sum for Two Users

Sum	0%	5%	10%	12.5%	25%	35%	45%	50%
$\mathfrak{T}$ (Bits) Two User	0.5	0.378	0.2655	0.28	0.125	0.13325	0.23	0.25

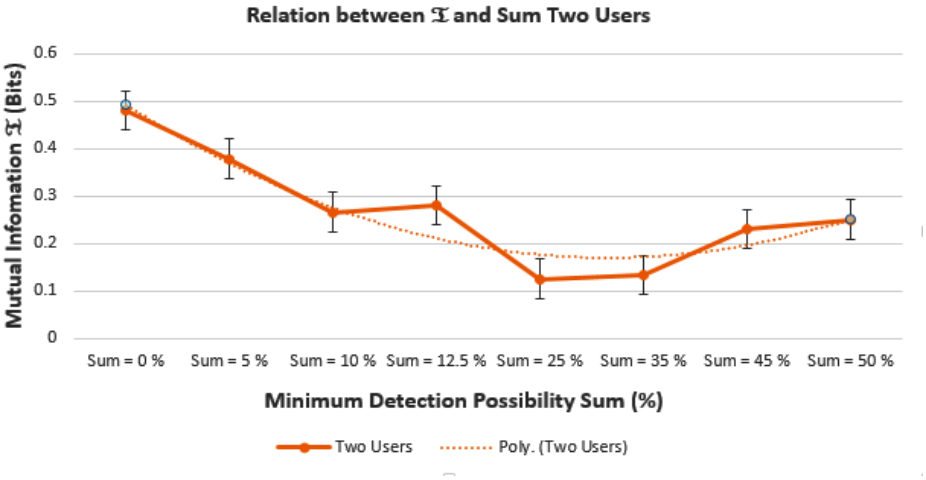


Fig. S4 The Correlation between the Mutual information $\mathfrak{T}$ and the Minimum Detecting Possibility Sum for Two Users.

If the eavesdropper would like for unconditionally obtaining the transferred authentication key J_K among QAS , u_A and u_B , so for every transferred key, the eavesdropper must conclude which $tri-bits$ are utilized for the authentication process. In accordance with the eavesdropper's measurement productivity $y = \mathcal{E}_{ij}\mu_{\upsilon\tau}$ with i,j, $\upsilon,\tau \in \{0,1\}$, $z = \gamma_{kl}\eta_{\varsigma\varkappa}$ with $k,l,\varsigma,\varkappa \in \{0,1\}$ and the key values $(000,001,010,011,100,101,110,111)$. Therefore, the eavesdropper can conclude the probability of the transmitted key bits.

For example if $y = \mathcal{E}_{00}\mu_{11}$ and $z = \gamma_{00}\eta_{11}$then the eavesdropper can conclude that the transported authentication key bits either 000, 101 or 111 with probability equal to 0.5, 0.25 and 0.25 respectively. By supposing that the eavesdropper selects the likelihood for identifying the transmitted key values $000, 001, 010$ or 011 is $\mathcal{P}$ and for identifying $100, 101, 110$ or 111 is $1-\mathcal{P}$ and take into consideration the unsuccessful measurement result as in Eq. (152). Consequently, the unconditional detection possibility $\mathcal{P}_e$ of J_K is given by (Eq. (155))

$$\mathcal{P}_e = \frac{(2+\sin\theta_{\text{Suml}})}{2}\left[\frac{1}{2}\mathcal{P} + \frac{1}{4}(1-\mathcal{P})\right] + \frac{(2-\sin\theta_{\text{Sum}})}{2}\left[\frac{1}{4}(1-\mathcal{P})\right] \tag{155}$$

By simplification of Eq. (126) $\mathcal{P}_e$ of J_K is given by (Eq. (156)) (see Supplementary information (11) for Proving Relation between $\mathcal{P}_e$, $\mathcal{P}$ and $\sin\theta_{\text{Sum}}$)

$$\mathcal{P}_e = \frac{1}{8}[(\sin\theta_{Sum}(3\times \mathcal{P}-1)+4] \tag{156}$$

If $\mathcal{P}=1$ implies that the detection possibility $\mathcal{P}_e$ is maximized see (Eq. (157)) (see Supplementary Information (12) for Proving Relation between $\mathcal{P}_e$,$\mathcal{P}_e{}^m$ and Sum)

$$\mathcal{P}_e{}^m = \frac{1}{4}\left(\sqrt{16\times Sum - 16\times Sum^2 - 3} + 2\right) \tag{157}$$

Table S4 and Figure S5 show the Correlation between Maximized Unconditional Detection Possibility $\mathcal{P}_e{}^m$ and the minimum detection possibility Sum.

Table S4 Correlation between Maximized Unconditional Detection Possibility $\mathcal{P}_e{}^m$ and Sum for Two Users

Sum	0%	5%	10%	12.5%	25%	35%	45%	50%
$\mathcal{P}_e{}^m$	0.07	0.125	0.187	0.22	0.50	0.72	0.74	0.75

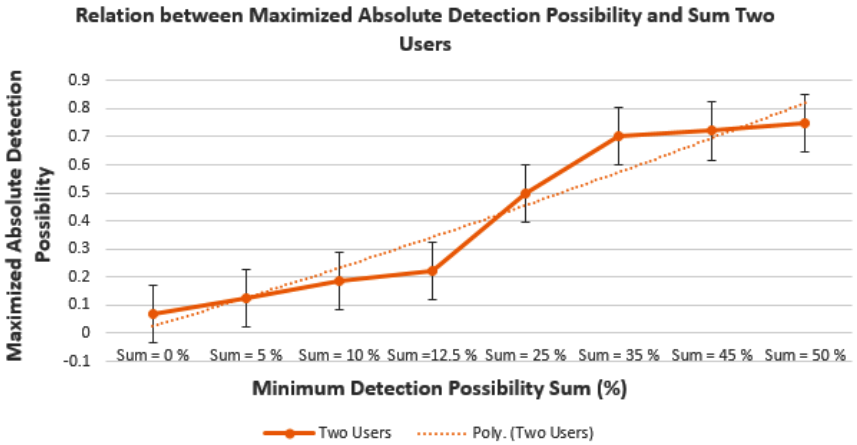


Fig. S5 Correlation between Maximized Unconditional Detection Possibility $\mathcal{P}_e{}^m$ and Sum for Two Users.

Therefore, the possibility of the eavesdropper for positively retrieving the transferred keys $\mathcal{P}_e{}^r \; for \; J_k = \{J_1, J_2, J_3 \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \; J_{2N}\}$ see (Eq. (158))

$$\mathcal{P}_e{}^r = [\mathcal{P}_e{}^m (\, 1 - Sum)]^{3N/4} \tag{158}$$

By substituting (Eq. (157)) in equation (Eq. (158)), so

$$\mathcal{P}_e{}^r = \left[\frac{1}{4}\left(\sqrt{16 \times Sum - 16 \times \; Sum^2 - 3} \; + 2\right)(\, 1 - Sum)\right]^{3N/4} \tag{159}$$

7 Proving Relation between sin θ_ε and Sum

From Eq. (100) $$Sum = Min(P_{Sum}) = \frac{1}{4}\,(1 - cos\;\theta_\varepsilon) \tag{160}$$

$$Sum = \frac{1}{4} - \frac{1}{4} cos\;\theta_\varepsilon \tag{161}$$

$$4 \times Sum = 1 - cos\;\theta_\varepsilon \tag{162}$$

$$cos\;\theta_\varepsilon = \; 1 - 4 \times Sum \tag{163}$$

$$cos\;\theta_\varepsilon{}^2 = \; [1 - \; 4 \times Sum]^2 \tag{164}$$

$$cos\;\theta_\varepsilon{}^2 = \; [1 - 8 \; \times Sum + 16 \times Sum^2] \tag{165}$$

By using the mathematical formulation of

$$cos\;\theta_\varepsilon{}^2 \; + sin\;\theta_\varepsilon{}^2 = 1 \tag{166}$$

Therefore, by substituting from Eq. (165) in Eq. (166)

$$1 - 8 \; \times Sum + 16 \times Sum^2 \; + sin\;\theta_\varepsilon{}^2 = 1 \tag{167}$$

$$sin\;\theta_\varepsilon{}^2 = 1 - 1 + 8 \; \times Sum - 16 \times Sum^2 \tag{168}$$

$$sin\;\theta_\varepsilon{}^2 = 8 \; \times Sum - 16 \times Sum^2 \tag{169}$$

So

$$sin\,\theta_{\mathcal{E}} = \sqrt{8 \times Sum - 16 \times Sum^2} \tag{170}$$

8 Proving Relation between P_e , P and sin $\theta_{\mathcal{E}}$

$$P_e = \frac{(1 + sin\,\theta_{\mathcal{E}})}{2}\left[\frac{1}{2}\,P + \frac{1}{4}\,(1 - P)\right] + \frac{(1 - sin\,\theta_{\mathcal{E}})}{2}\left[\frac{1}{4}\,(1 - P)\right] \tag{170}$$

By dividing Eq. (170) into Eq. (171) and Eq. (172)

$$\frac{(1 + sin\,\theta_{\mathcal{E}})}{2}\left[\frac{1}{2}\,P + \frac{1}{4}\,(1 - P)\right] \tag{171}$$

$$\frac{(1 - sin\,\theta_{\mathcal{E}})}{2}\left[\frac{1}{4}\,(1 - P)\right] \tag{172}$$

By simplify Eq. (171)

$$\frac{(P + P\,sin\,\theta_{\mathcal{E}})}{4} + \frac{(1 + sin\,\theta_{\mathcal{E}})(1 - P)}{8} \tag{173}$$

$$\frac{(P + P\,sin\,\theta_{\mathcal{E}})}{4} + \frac{(1 - P + sin\,\theta_{\mathcal{E}} - P\,sin\,\theta_{\mathcal{E}})}{8} \tag{174}$$

$$\frac{(2 \times P + 2 \times P\,sin\,\theta_{\mathcal{E}} + 1 - P + sin\,\theta_{\mathcal{E}} - P\,sin\,\theta_{\mathcal{E}})}{8} \tag{175}$$

By simplify Eq. (172)

$$\frac{(1 - sin\,\theta_{\mathcal{E}})(1 - P)}{8} \tag{176}$$

$$\frac{(1 - P - sin\,\theta_{\mathcal{E}} + P\,sin\,\theta_{\mathcal{E}})}{8} \tag{177}$$

By adding Eq. (175) and Eq. (177)

$$P_e = \frac{[2 + sin\,\theta_{\mathcal{E}}(2 \times P + P - 1)]}{8} \tag{178}$$

$$P_e = \frac{[2 + sin\,\theta_{\mathcal{E}}(2 \times P + P - 1)]}{8} \tag{179}$$

$$P_e = \frac{1}{8}[\,(\,sin\,\theta_{\mathcal{E}}(3 \times P - 1\,) + 2] \tag{180}$$

So Eq. (180) = Eq. (109)

9 Proving Relation between P_e , $P_e{}^m$ and Sum

From Eq. (180) $P_e = \frac{1}{8}[\,(\,sin\,\theta_{\mathcal{E}}(3 \times P - 1\,) + 2]$

If $P = 1$ indicates that the total estimation probability P_e is maximized to $P_e{}^m$

$$P_e{}^m = \frac{1}{8}[\,(\,sin\,\theta_{\mathcal{E}}((3 \times 1) - 1\,) + 2] \tag{181}$$

$$P_e{}^m = \frac{1}{8}[\,(\,2 \times sin\,\theta_{\mathcal{E}}) + 2] \tag{182}$$

$$P_e{}^m = \frac{2}{8}[\,sin\,\theta_{\mathcal{E}} + 1] \tag{183}$$

$$\mathrm{P}_e{}^m = \frac{1}{4}[\, sin\, \theta_\varepsilon + 1] \tag{184}$$

From Eq. (170), $sin\, \theta_\varepsilon = \sqrt{8 \times Sum - 16 \times\ Sum^2}$, by substitution in Eq. (184)

$$\mathrm{P}_e{}^m = \frac{1}{4}\left[\, \sqrt{8 \times Sum - 16 \times\ Sum^2} + 1\right] \tag{185}$$

So Eq. (185) = Eq. (110)

10 Proving Relation between $\sin \theta_{\mathrm{Sum}}$ and Sum

From Eq. (147) $$Sum = Min(\mathrm{P}_{\mathrm{Sum}}) = \frac{1}{4}\ (1 - cos\ \theta_\varepsilon + 1 - cos\ \theta_\gamma) \tag{186}$$

$$Sum = \frac{2}{4} - \frac{1}{4} cos\ \theta_{Sum} \tag{187}$$

$$4 \times Sum = 2 - cos\ \theta_{Sum} \tag{188}$$

$$cos\ \theta_{Sum} =\ 2 - 4 \times Sum \tag{189}$$

$$cos\ \theta_{\mathrm{Sum}}{}^2 =\ [2 -\ 4 \times Sum]^2 \tag{190}$$

$$cos\ \theta_{\mathrm{Sum}}{}^2 =\ [4 - 16\ \times Sum + 16 \times Sum^2] \tag{191}$$

By using the mathematical formulation of

$$cos\ \theta_{\mathrm{Sum}}{}^2\ + sin\ \theta_{\mathrm{Sum}}{}^2 = 1 \tag{192}$$

Therefore, by substituting from Eq. (191) in Eq. (192)

$$4 - 16\ \times Sum + 16 \times Sum^2\ + sin\ \theta_{\mathrm{Sum}}{}^2 = 1 \tag{193}$$

$$sin\ \theta_{\mathrm{Sum}}{}^2 = 1 - 4 + 16\ \times Sum - 16 \times Sum^2 \tag{194}$$

$$sin\ \theta_{\mathrm{Sum}}{}^2 = 16\ \times Sum - 16 \times Sum^2 - 3 \tag{195}$$

So

$$sin\ \theta_{Sum} =\ \sqrt{16\ \times Sum - 16 \times Sum^2 - 3} \tag{196}$$

11 Proving Relation between $\mathcal{P}_e$, $\mathcal{P}$ and $\sin \theta_{\mathrm{Sum}}$

$$\mathcal{P}_e = \frac{(2 + sin\ \theta_{\mathrm{Sum}})}{2}\left[\frac{1}{2}\ \mathcal{P} + \frac{1}{4}\ (1 - \mathcal{P})\right] + \frac{(2 - sin\ \theta_{\mathrm{Sum}})}{2}\left[\frac{1}{4}\ (1 - \mathcal{P})\right] \tag{197}$$

By dividing Eq. (197) into Eq. (198) and Eq. (199)

$$\frac{(2+\sin\theta_{\text{Sum1}})}{2}\left[\frac{1}{2}\mathcal{P}+\frac{1}{4}(1-\mathcal{P})\right] \quad (198)$$

$$\frac{(2-\sin\theta_{\text{Sum}})}{2}\left[\frac{1}{4}(1-\mathcal{P})\right] \quad (199)$$

By simplify Eq. (198)

$$\frac{(2\times\mathcal{P}+\mathcal{P}\sin\theta_{Sum})}{4}+\frac{(2-2\times\mathcal{P}+\sin\theta_{Sum}-\mathcal{P}\sin\theta_{Sum})}{8} \quad (199)$$

$$\frac{(4\times\mathcal{P}+2\times\mathcal{P}\sin\theta_{Sum}+2-2\times\mathcal{P}+\sin\theta_{Sum}-\mathcal{P}\sin\theta_{Sum})}{8} \quad (200)$$

By simplify Eq. (199)

$$\frac{(2-\sin\theta_{\text{Sum}})(1-\mathcal{P})}{8} \quad (201)$$

$$\frac{(2-2\times\mathcal{P}-\sin\theta_{Sum}+\mathcal{P}\sin\theta_{Sum})}{8} \quad (202)$$

By adding Eq. (200) and Eq. (202)

$$\mathcal{P}_e=\frac{[4+\sin\theta_{Sum}(2\times\mathcal{P}+\mathcal{P}-1)]}{8} \quad (203)$$

$$\mathcal{P}_e=\frac{[2+\sin\theta_{Sum}(2\times\mathcal{P}+\mathcal{P}-1)]}{8} \quad (204)$$

$$\mathcal{P}_e=\frac{1}{8}[\,(\sin\theta_{Sum}(3\times\mathcal{P}-1)+4] \quad (205)$$

So Eq. (205) = Eq. (156)

12 Proving Relation between $\mathcal{P}_e$, ${\mathcal{P}_e}^m$ and Sum

From Eq. (205) $\mathcal{P}_e=\frac{1}{8}[\,(\sin\theta_{Sum}(3\times\mathcal{P}-1)+4]$

If $\mathcal{P}=1$ implies that the detection possibility $\mathcal{P}_e$ is maximized to ${\mathcal{P}_e}^m$

$${\mathcal{P}_e}^m=\frac{1}{8}[\,(\sin\theta_{Sum}((3\times1)-1)+4] \quad (206)$$

$${\mathcal{P}_e}^m=\frac{1}{8}[\,(2\times\sin\theta_{Sum})+4] \quad (207)$$

$${\mathcal{P}_e}^m=\frac{2}{8}[\sin\theta_{Sum}+2] \quad (208)$$

$${\mathcal{P}_e}^m=\frac{1}{4}[\sin\theta_{Sum}+2] \quad (209)$$

From Eq. (196) $\sin\theta_{Sum}=\sqrt{16\times Sum-16\times Sum^2-3}$, by substitution in Eq. (209)

$${\mathcal{P}_e}^m=\frac{1}{4}\left[\sqrt{16\times Sum-16\times Sum^2-3}+2\right] \quad (210)$$

So Eq. (210) = Eq. (157)

13 Detailed Computations for Relation between N, Sum , $\mathcal{P}_e{}^r$

Table S5 (A, B, C, D) Numerical Calculations for Fig. S6 ((A), (B), (C), (D)) .

A

Sum (%)	N ($Bits$)	$P_e{}^r$
0	2	0.25
0	4	6.25×10^{-2}
0	8	3.91×10^{-3}
0	16	1.53×10^{-5}

B

Sum (%)	N ($Bits$)	$P_e{}^r$
12.5	2	4.08×10^{-1}
12.5	4	1.668×10^{-1}
12.5	8	2.782×10^{-2}
12.5	16	7.7×10^{-4}

C

Sum (%)	N ($Bits$)	$P_e{}^r$
25	2	0.375
25	4	1.406×10^{-1}
25	8	1.97×10^{-2}
25	16	3.91×10^{-4}

D

Sum (%)	N ($Bits$)	$P_e{}^r$
50	2	1.25×10^{-1}
50	4	1.56×10^{-2}
50	8	2.5×10^{-4}
50	16	5.96×10^{-8}

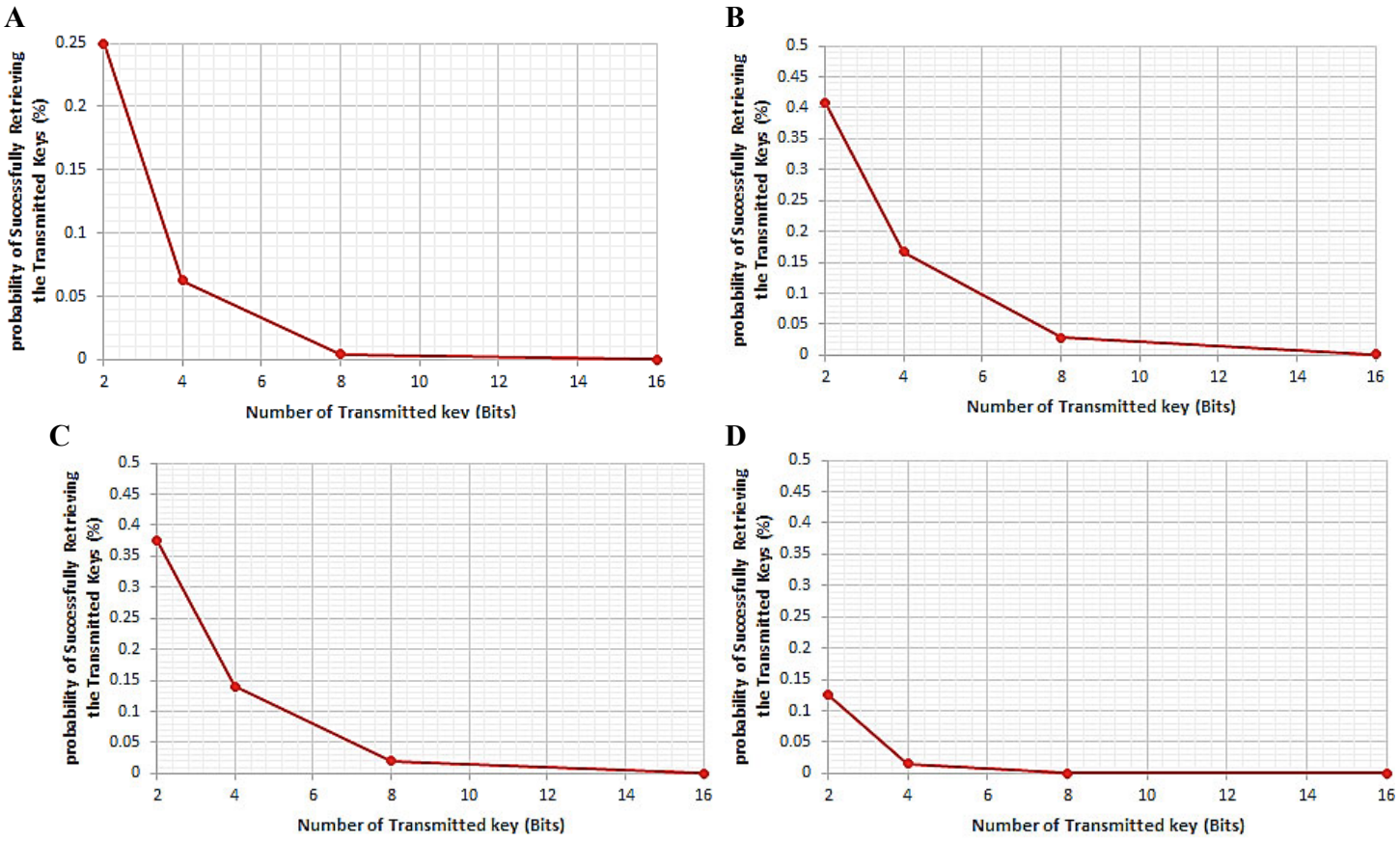


Fig. S6 (A) Relation between $P_e{}^r$, $N =$ [2 ,4 , 8 , 16] and $Sum =$ [0]% ; **(B)** $Sum =$ [12.5]% ; **(C)** $Sum =$ [25]% ; **(D)** $Sum =$ [50]% .

14 Detailed Computations for Relation between $\mathcal{P}_e{}^r$ and N while $\mathcal{P}_e{}^m = [12.5, 25, 37.5, 50]\%$ and $Sum = [0, 12.5, 25, 50]\%$

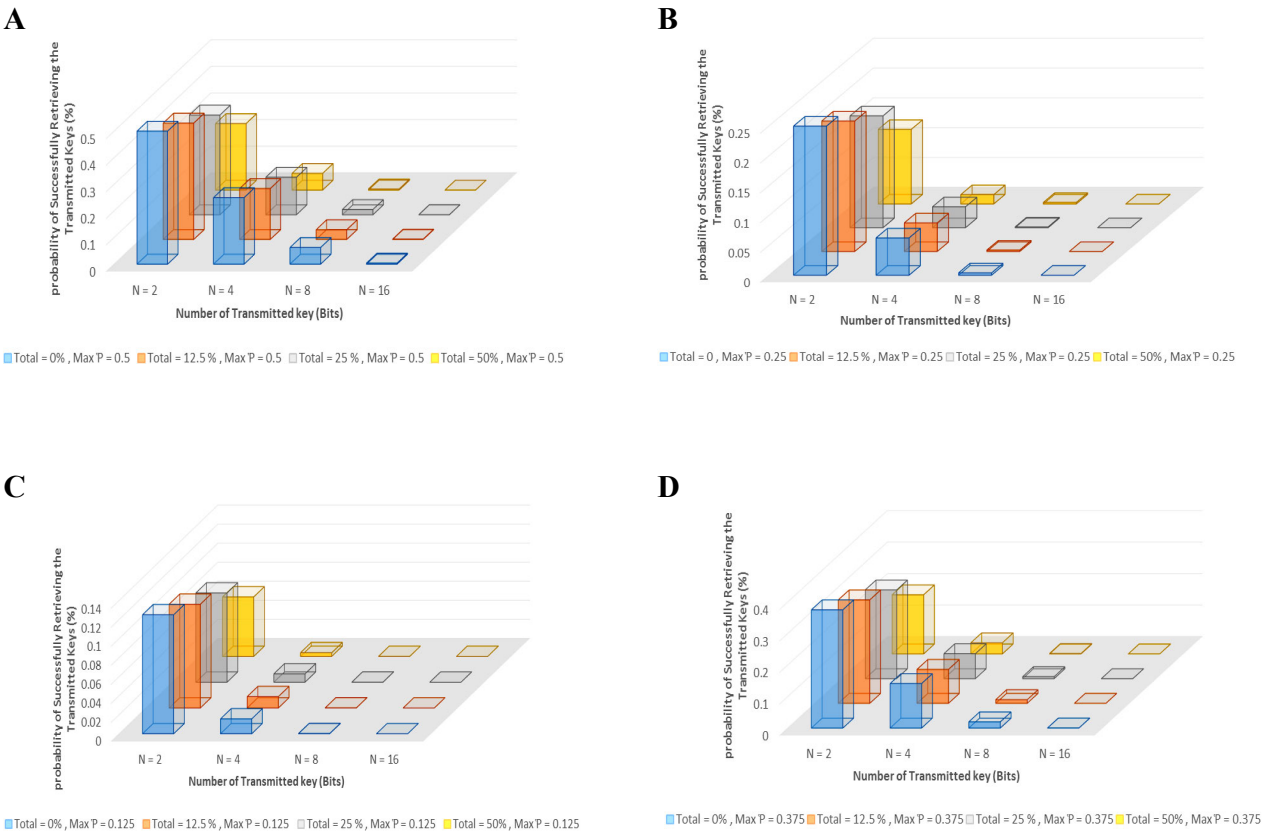


Fig. S7 (A) Relation between $P_e{}^r$, $N = [2, 4, 8, 16]$ while $Sum = [0, 12.5, 25, 50]\%$ and $P_e{}^m = [50]\%$ **(B)** $P_e{}^m = [25]\%$; **(C)** $P_e{}^m = [12.5]\%$; **(D)** $P_e{}^m = [37.5]\%$.

Table S6 (A, B, C, D) Numerical Calculations for Fig. S7 ((B), (A), (C), (D)) respectively.

$P_e{}^m$	Sum (%)	N ($Bits$)	$P_e{}^r$
0.25	0	2	0.25
0.25	0	4	0.0625
0.25	0	8	3.91×10^{-3}
0.25	0	16	1.53×10^{-5}
0.25	12.5	2	0.21875
0.25	12.5	4	0.04785
0.25	12.5	8	2.28×10^{-3}
0.25	12.5	16	5.24×10^{-6}
0.25	25	2	0.1875
0.25	25	4	0.0351
0.25	25	8	1.23×10^{-3}
0.25	25	16	1.53×10^{-6}

$P_e{}^m$	Sum (%)	N ($Bits$)	$P_e{}^r$
0.50	0	2	0.5
0.50	0	4	0.25
0.50	0	8	0.0625
0.50	0	16	3.91×10^{-3}
0.50	12.5	2	0.4375
0.50	12.5	4	0.1914
0.50	12.5	8	0.0366
0.50	12.5	16	1.34×10^{-3}
0.50	25	2	0.375
0.50	25	4	0.1406
0.50	25	8	0.0197
0.50	25	16	3.91×10^{-4}

0.25	50	2	0.125
0.25	50	4	0.015625
0.25	50	8	2.44×10^{-4}
0.25	50	16	5.96×10^{-8}

A

0.50	50	2	0.25
0.50	50	4	0.0625
0.50	50	8	3.91×10^{-3}
0.50	50	16	1.53×10^{-5}

B

C

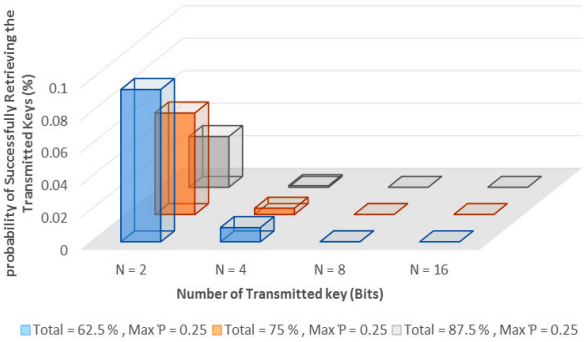
P_e^m	*Sum* (%)	*N* (*Bits*)	P_e^r
0.125	0	2	0.125
0.125	0	4	0.0156
0.125	0	8	2.5×10^{-4}
0.125	0	16	5.96×10^{-8}
0.125	12.5	2	0.109
0.125	12.5	4	0.0119
0.125	12.5	8	1.43×10^{-4}
0.125	12.5	16	2.04×10^{-8}
0.125	25	2	0.09375
0.125	25	4	8.78×10^{-3}
0.125	25	8	7.72×10^{-5}
0.125	25	16	5.96×10^{-9}
0.125	50	2	0.0625
0.125	50	4	3.91×10^{-3}
0.125	50	8	1.53×10^{-5}
0.125	50	16	2.32×10^{-10}

D

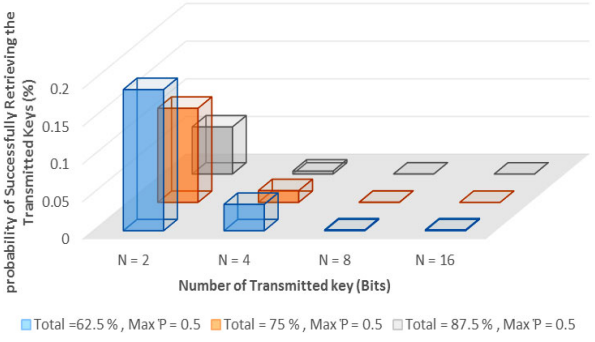
P_e^m	*Sum* (%)	*N* (*Bits*)	P_e^r
0.375	0	2	0.375
0.375	0	4	0.1406
0.375	0	8	0.0197
0.375	0	16	3.91×10^{-4}
0.375	12.5	2	0.3281
0.375	12.5	4	0.10766
0.375	12.5	8	0.01159
0.375	12.5	16	1.34×10^{-3}
0.375	25	2	0.28125
0.375	25	4	0.07910
0.375	25	8	6.25×10^{-3}
0.375	25	16	3.91×10^{-5}
0.375	50	2	0.1875
0.375	50	4	0.03515
0.375	50	8	1.32×10^{-3}
0.375	50	16	1.53×10^{-6}

15 Detailed Computations for Relation between P_e^r and *N* while $P_e^m = [12.5, 25, 37.5, 50]$% and $Sum = [62.5, 75, 87.5]$%

A



B



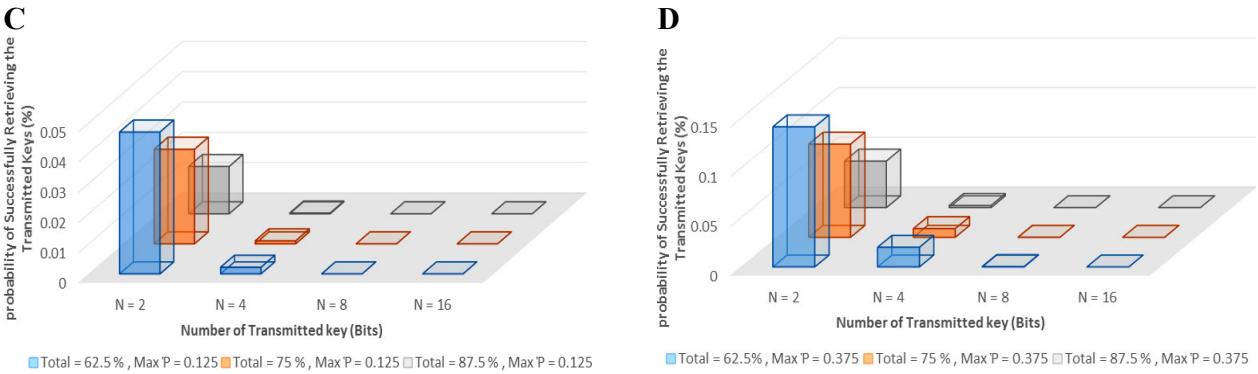


Fig. S8 (A) Relation between $P_e{}^r$, $N = [2, 4, 8, 16]$ while $Sum = [62.5, 75, 87.5]\%$ and $P_e{}^m = [25]\%$ **(B)** $P_e{}^m = [50]\%$; **(C)** $P_e{}^m = [12.5]\%$; **(D)** $P_e{}^m = [37.5]\%$.

Table S7 (A, B, C, D) Numerical Calculations for Fig. S8 ((C), (A), (D), (B)) respectively.

A

$P_e{}^m$	Sum (%)	N ($Bits$)	$P_e{}^r$
0.125	62.5	2	4.68×10^{-2}
0.125	62.5	4	2.19×10^{-3}
0.125	62.5	8	4.82×10^{-6}
0.125	62.5	16	2.33×10^{-11}
0.125	75	2	3.125×10^{-2}
0.125	75	4	9.77×10^{-4}
0.125	75	8	9.54×10^{-7}
0.125	75	16	9.095×10^{-13}
0.125	87.5	2	0.015625
0.125	87.5	4	2.5×10^{-4}
0.125	87.5	8	5.96×10^{-8}
0.125	87.5	16	3.55×10^{-15}

B

$P_e{}^m$	Sum (%)	N ($Bits$)	$P_e{}^r$
0.25	62.5	2	9.37×10^{-2}
0.25	62.5	4	8.79×10^{-3}
0.25	62.5	8	7.7×10^{-5}
0.25	62.5	16	5.96×10^{-9}
0.25	75	2	0.0625
0.25	75	4	3.91×10^{-3}
0.25	75	8	1.53×10^{-5}
0.25	75	16	2.33×10^{-10}
0.25	87.5	2	0.03125
0.25	87.5	4	9.77×10^{-4}
0.25	87.5	8	9.54×10^{-7}
0.25	87.5	16	9.095×10^{-13}

C

$P_e{}^m$	Sum (%)	N ($Bits$)	$P_e{}^r$
0.375	62.5	2	1.41×10^{-1}
0.375	62.5	4	1.97×10^{-2}
0.375	62.5	8	3.91×10^{-4}
0.375	62.5	16	1.53×10^{-7}
0.375	75	2	9.37×10^{-2}
0.375	75	4	8.79×10^{-3}
0.375	75	8	7.7×10^{-5}
0.375	75	16	5.96×10^{-9}
0.375	87.5	2	4.68×10^{-2}
0.375	87.5	4	2.19×10^{-3}
0.375	87.5	8	4.82×10^{-6}
0.375	87.5	16	2.33×10^{-11}

D

$P_e{}^m$	Sum (%)	N ($Bits$)	$P_e{}^r$
0.50	62.5	2	1.87×10^{-1}
0.50	62.5	4	3.51×10^{-2}
0.50	62.5	8	1.23×10^{-3}
0.50	62.5	16	1.53×10^{-6}
0.50	75	2	0.125
0.50	75	4	0.015625
0.50	75	8	2.5×10^{-4}
0.50	75	16	5.96×10^{-8}
0.50	87.5	2	0.0625
0.50	87.5	4	3.91×10^{-3}
0.50	87.5	8	1.53×10^{-5}
0.50	87.5	16	2.33×10^{-10}

16 Detailed Computations for Relation between N, Sum , $\mathcal{P}_e{}^r$ for Two Users

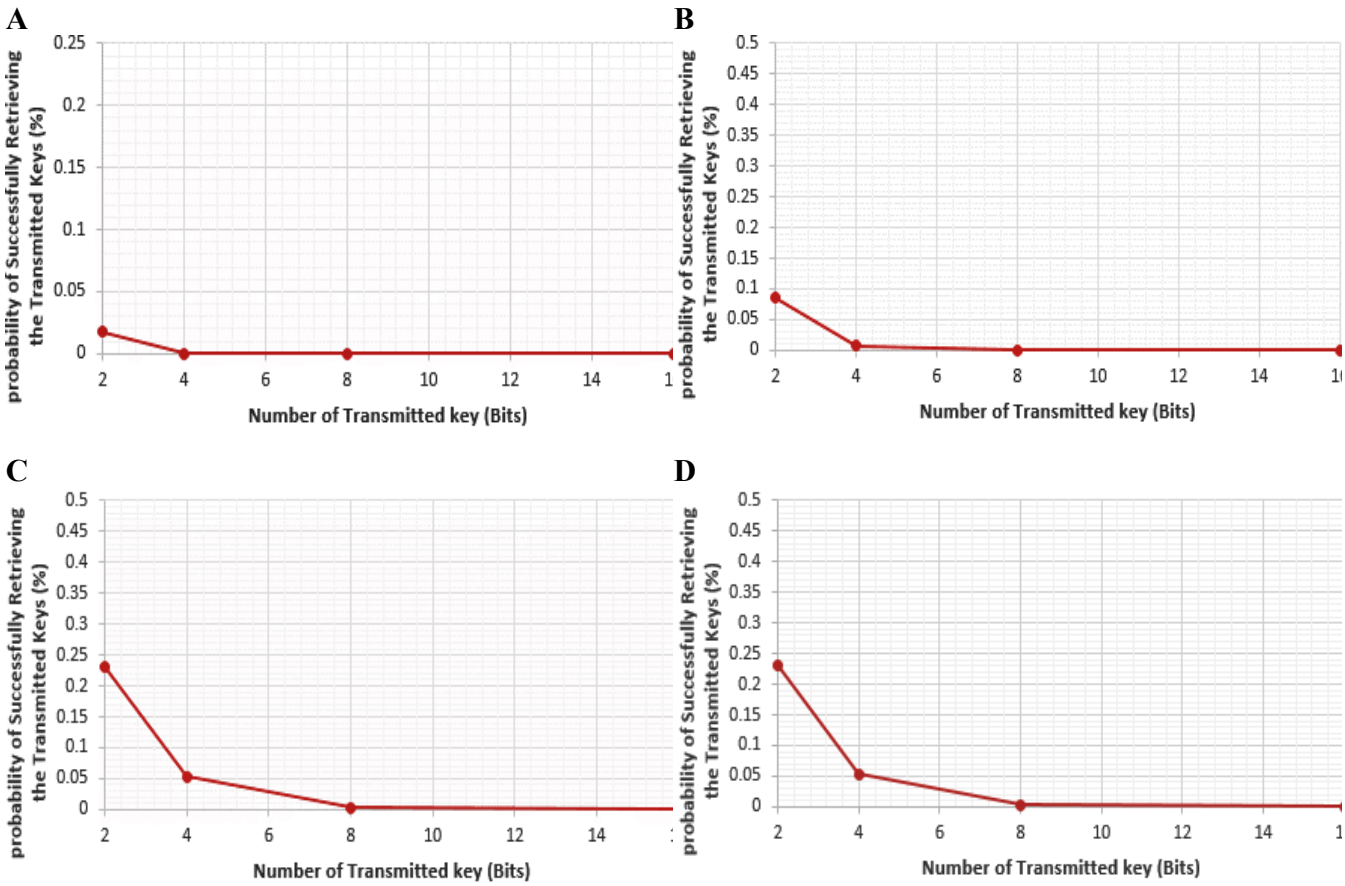


Fig. S9 (A) Relation between $\mathcal{P}_e{}^r$, $N =$ [2 ,4 , 8 , 16] and $Sum =$ [0]% ; **(B)** $Sum =$ [12.5]% ; **(C)** $Sum =$ [25]% ; **(D)** $Sum =$ [50]% .

Table S8 (A, B, C, D) Numerical Calculations for Fig. S9 ((A), (B), (C), (D)) .

A

Sum (%)	N $(Bits)$	$\mathcal{P}_e{}^r$
0	2	1.73×10^{-2}
0	4	3×10^{-4}
0	8	9×10^{-8}
0	16	8.15×10^{-15}

B

Sum (%)	N $(Bits)$	$\mathcal{P}_e{}^r$
12.5	2	8.5×10^{-2}
12.5	4	7.18×10^{-3}
12.5	8	5.2×10^{-5}
12.5	16	2.66×10^{-9}

C

Sum (%)	N $(Bits)$	$\mathcal{P}_e{}^r$
25	2	0.2296
25	4	5.27×10^{-2}
25	8	2.78×10^{-3}
25	16	7.73×10^{-6}

D

Sum (%)	N $(Bits)$	$\mathcal{P}_e{}^r$
50	2	2.3×10^{-1}
50	4	5.27×10^{-2}
50	8	2.78×10^{-3}
50	16	7.73×10^{-6}

17 Detailed Computations for Relation between $\mathcal{P}_e{}^r$ and N while $\mathcal{P}_e{}^m = [12.5, 25, 37.5, 50]$% and $Sum = [0, 12.5, 25, 50]$% for Two Users

Table S9 (A, B, C, D) Numerical Calculations for Fig. S10 ((B), (A), (C), (D)) respectively.

$\mathcal{P}_e{}^m$	$Sum\ (\%)$	$N\ (Bits)$	$\mathcal{P}_e{}^r$
0.25	0	2	1.25×10^{-1}
0.25	0	4	1.56×10^{-2}
0.25	0	8	2.44×10^{-4}
0.25	0	16	5.96×10^{-8}
0.25	12.5	2	0.1023
0.25	12.5	4	0.01047
0.25	12.5	8	1.1×10^{-4}
0.25	12.5	16	1.20×10^{-8}
0.25	25	2	0.08119
0.25	25	4	0.0066
0.25	25	8	4.35×10^{-5}
0.25	25	16	1.9×10^{-9}
0.25	50	2	4.42×10^{-2}
0.25	50	4	1.95×10^{-3}
0.25	50	8	3.8×10^{-6}
0.25	50	16	1.5×10^{-11}

A

$\mathcal{P}_e{}^m$	$Sum\ (\%)$	$N\ (Bits)$	$\mathcal{P}_e{}^r$
0.50	0	2	0.35
0.50	0	4	1.25×10^{-1}
0.50	0	8	1.56×10^{-2}
0.50	0	16	2.44×10^{-4}
0.50	12.5	2	0.29
0.50	12.5	4	0.084
0.50	12.5	8	0.007
0.50	12.5	16	4.9×10^{-5}
0.50	25	2	0.23
0.50	25	4	0.053
0.50	25	8	0.0028
0.50	25	16	7.7×10^{-6}
0.50	50	2	1.25×10^{-1}
0.50	50	4	1.56×10^{-2}
0.50	50	8	2.44×10^{-4}
0.50	50	16	5.96×10^{-8}

B

C

$\mathcal{P}_e{}^m$	$Sum\ (\%)$	$N\ (Bits)$	$\mathcal{P}_e{}^r$
0.125	0	2	0.044
0.125	0	4	1.95×10^{-3}
0.125	0	8	3.8×10^{-6}
0.125	0	16	1.46×10^{-11}
0.125	12.5	2	0.036
0.125	12.5	4	1.3×10^{-3}
0.125	12.5	8	1.7×10^{-6}
0.125	12.5	16	2.8×10^{-12}
0.125	25	2	0.029
0.125	25	4	8.2×10^{-4}
0.125	25	8	6.8×10^{-7}
0.125	25	16	4.61×10^{-13}
0.125	50	2	1.56×10^{-2}
0.125	50	4	2.44×10^{-4}
0.125	50	8	5.96×10^{-8}
0.125	50	16	3.6×10^{-15}

D

$\mathcal{P}_e{}^m$	$Sum\ (\%)$	$N\ (Bits)$	$\mathcal{P}_e{}^r$
0.375	0	2	0.23
0.375	0	4	0.053
0.375	0	8	0.0028
0.375	0	16	7.7×10^{-6}
0.375	12.5	2	0.188
0.375	12.5	4	3.5×10^{-2}
0.375	12.5	8	1.2×10^{-3}
0.375	12.5	16	1.56×10^{-6}
0.375	25	2	0.149
0.375	25	4	0.022
0.375	25	8	4.9×10^{-4}
0.375	25	16	2.45×10^{-7}
0.375	50	2	0.08119
0.375	50	4	0.0066
0.375	50	8	4.35×10^{-5}
0.375	50	16	1.9×10^{-9}

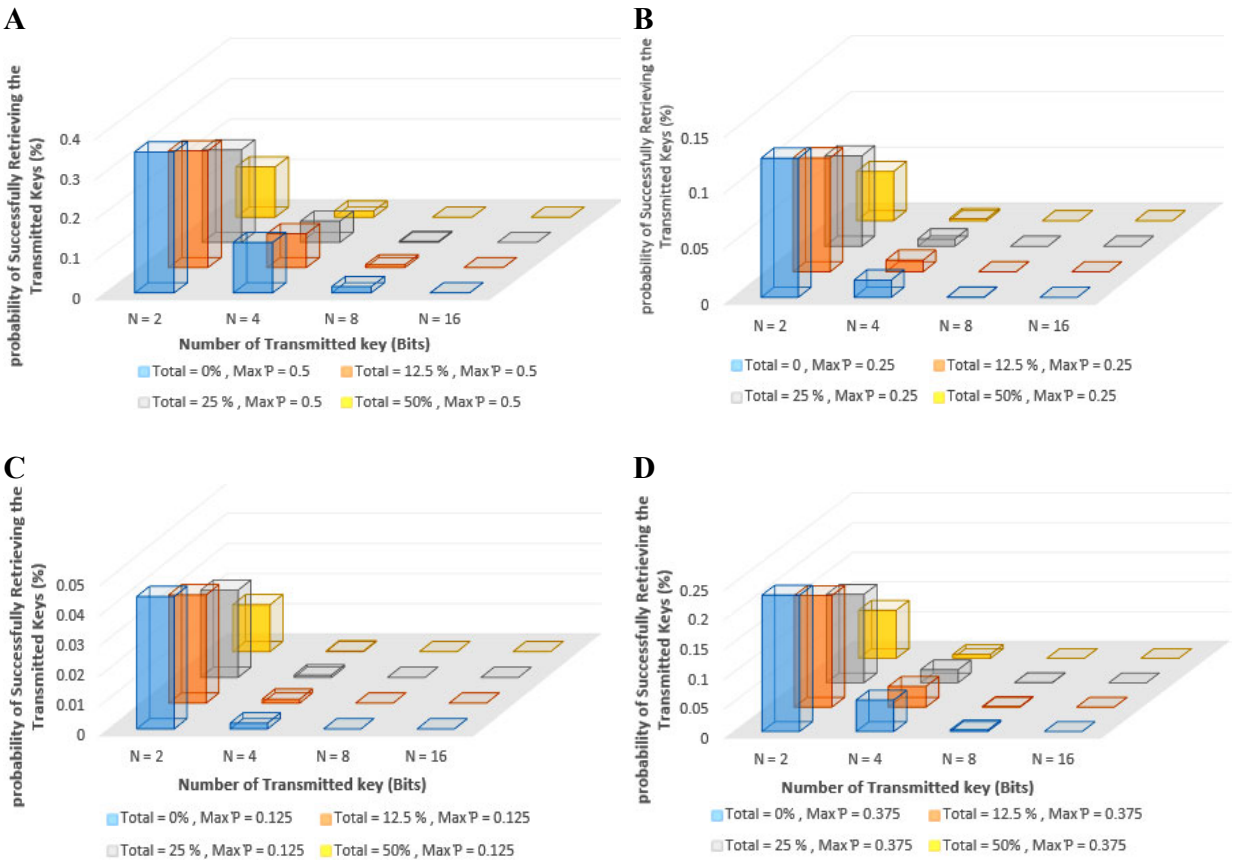


Fig. S10 (A) Relation between $\mathcal{P}_e{}^r$, $N =$ [2 ,4 , 8 , 16] while Sum = [0,12.5,25,50]% and $\mathcal{P}_e{}^m$ = [50]% **(B)** $\mathcal{P}_e{}^m$ = [25]% ; **(C)** $\mathcal{P}_e{}^m$ = [12.5]% ; **(D)** $\mathcal{P}_e{}^m$ = [37.5]% .

18 Detailed Computations for Relation between $\mathcal{P}_e{}^r$ and N while $\mathcal{P}_e{}^m$ = [12.5 , 25, 37.5 , 50]% and Sum = [62.5, 75, 87.5]% for Two Users

Table S10 (A, B, C, D) Numerical Calculations for Fig. S11 ((C), (A), (D), (B)) respectively.

A

$\mathcal{P}_e{}^m$	Sum (%)	N ($Bits$)	$\mathcal{P}_e{}^r$
0.125	62.5	2	1.015×10^{-2}
0.125	62.5	4	1.03×10^{-4}
0.125	62.5	8	1.06×10^{-9}
0.125	62.5	16	1.13×10^{-16}
0.125	75	2	5.5×10^{-3}
0.125	75	4	3.1×10^{-5}
0.125	75	8	9.3×10^{-10}
0.125	75	16	8.7×10^{-19}
0.125	87.5	2	1.95×10^{-3}
0.125	87.5	4	3.8×10^{-6}
0.125	87.5	8	1.5×10^{-11}
0.125	87.5	16	2.12×10^{-22}

B

$\mathcal{P}_e{}^m$	Sum (%)	N ($Bits$)	$\mathcal{P}_e{}^r$
0.25	62.5	2	2.9×10^{-2}
0.25	62.5	4	8.2×10^{-4}
0.25	62.5	8	6.8×10^{-7}
0.25	62.5	16	4.61×10^{-13}
0.25	75	2	1.56×10^{-2}
0.25	75	4	2.44×10^{-4}
0.25	75	8	5.96×10^{-8}
0.25	75	16	3.6×10^{-15}
0.25	87.5	2	0.0055
0.25	87.5	4	3.1×10^{-5}
0.25	87.5	8	9.3×10^{-10}
0.25	87.5	16	8.7×10^{-19}

C

$\mathcal{P}_e{}^m$	Sum (%)	N ($Bits$)	$\mathcal{P}_e{}^r$

D

$\mathcal{P}_e{}^m$	Sum (%)	N ($Bits$)	$\mathcal{P}_e{}^r$

0.375	62.5	2	5.29×10^{-2}
0.375	62.5	4	2.8×10^{-3}
0.375	62.5	8	7.86×10^{-6}
0.375	62.5	16	6.17×10^{-11}
0.375	75	2	2.9×10^{-2}
0.375	75	4	8.2×10^{-4}
0.375	75	8	6.8×10^{-7}
0.375	75	16	4.61×10^{-13}
0.375	87.5	2	1.06×10^{-2}
0.375	87.5	4	1.03×10^{-4}
0.375	87.5	8	1.06×10^{-8}
0.375	87.5	16	1.13×10^{-16}

0.50	62.5	2	8.2×10^{-2}
0.50	62.5	4	6.6×10^{-3}
0.50	62.5	8	4.35×10^{-5}
0.50	62.5	16	1.9×10^{-9}
0.50	75	2	0.044
0.50	75	4	1.95×10^{-3}
0.50	75	8	3.8×10^{-6}
0.50	75	16	1.46×10^{-11}
0.50	87.5	2	1.56×10^{-2}
0.50	87.5	4	2.44×10^{-4}
0.50	87.5	8	5.96×10^{-8}
0.50	87.5	16	3.6×10^{-15}

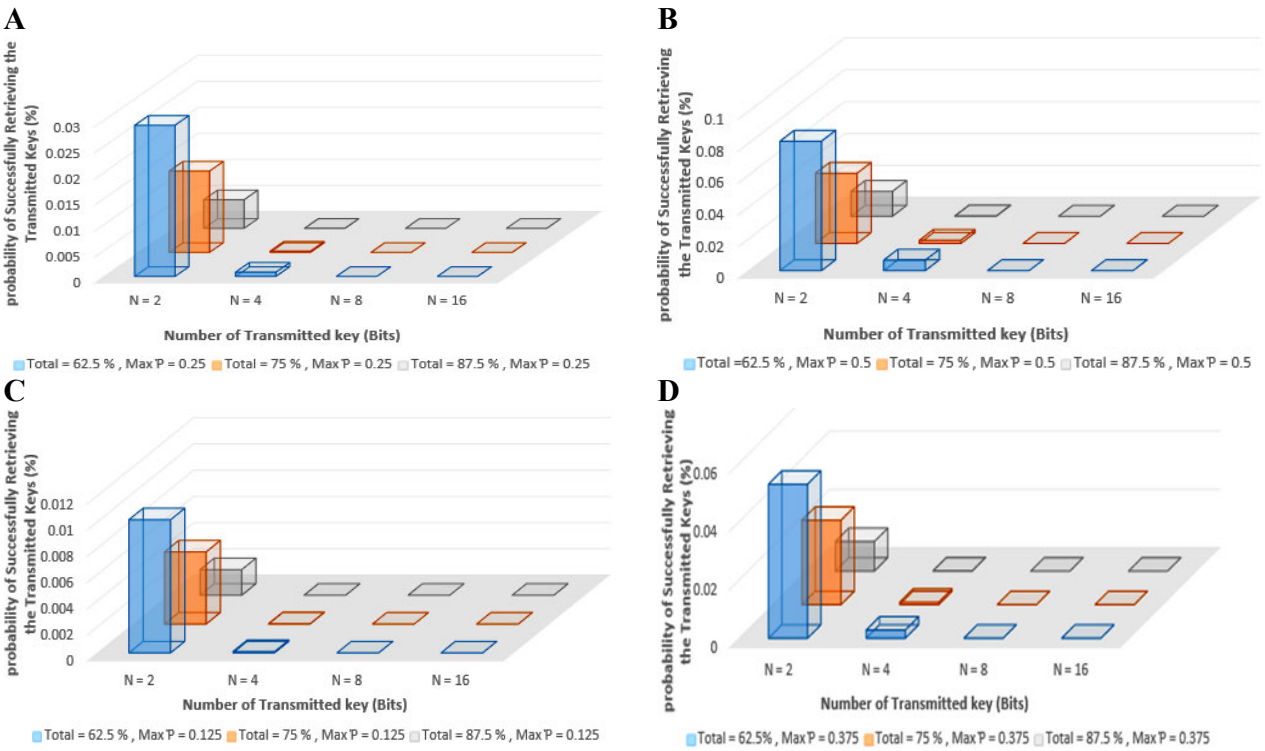


Fig. S11 (A) Relation between $\mathcal{P}_e{}^r$, $N =$ [2 ,4 , 8 , 16] while Sum = [62.5,75,87.5]% and $\mathcal{P}_e{}^m$ = [25]% **(B)** $\mathcal{P}_e{}^m$ = [50]% ; **(C)** $\mathcal{P}_e{}^m$ = [12.5]% ; **(D)** $\mathcal{P}_e{}^m$ = [37.5]% .

19 Analysis of Unconditional Retrieved Mutual Information for One and Two Users by the Attacker

A **B**

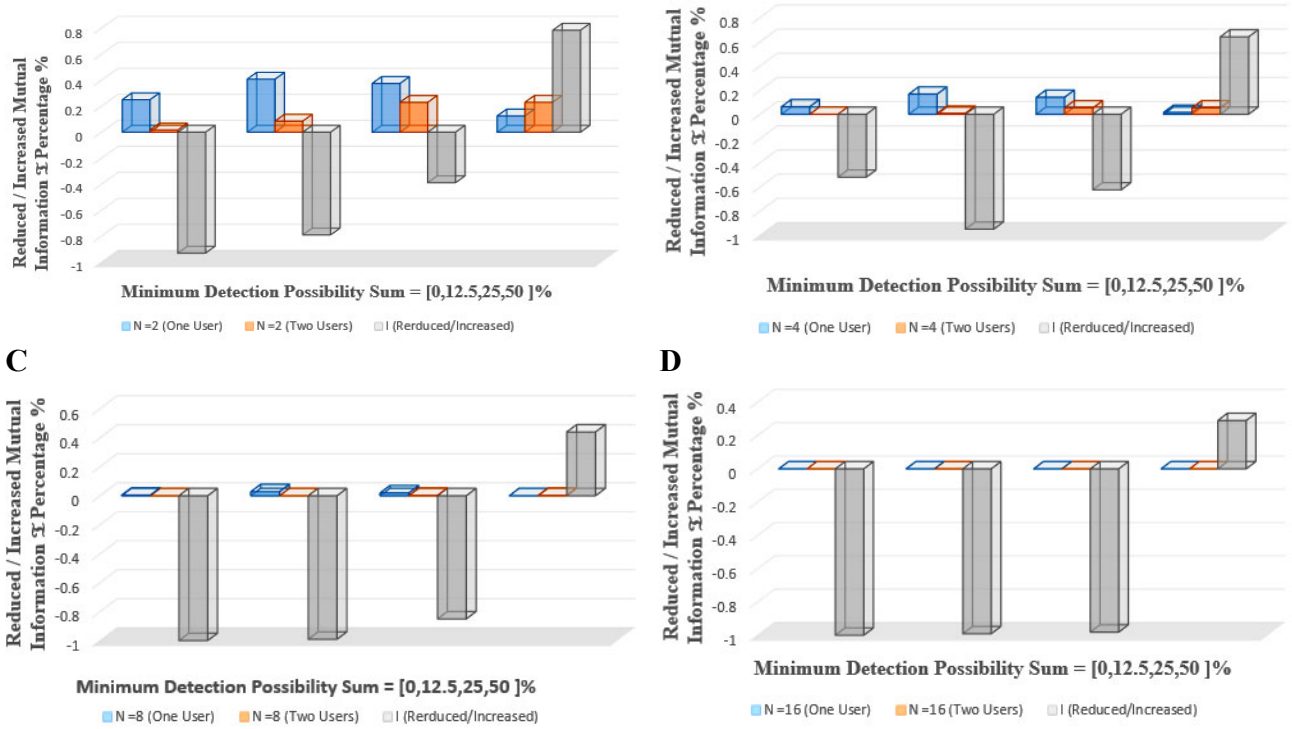


Fig. S12 Relation between Reduced / Increased Mutual Information ℑ Percentage % and Minimum Detection Possibility Sum = [0,12.5,25,50]% for One and Two Users. **(A)** $N =$ [2] **(B)** = [4] ; **(C)** $N =$ [8] ; **(D)** N = [16] .

Table S11 (A, B, C, D) Numerical Calculations for Fig. S12 ((A), (B), (C), (D)).

A

Sum (%)	N (*Bits*)	One User	Two Users	I(Reduced /Increased)
0	2	0.25	0.0173	-93%
12.5	2	0.408	0.085	-79%
25	2	0.375	0.2296	-38.80%
50	2	0.125	0.23	78%

B

Sum (%)	N (*Bits*)	One User	Two Users	I(Reduced /Increased)
0	4	0.0625	0.0003	-52%
12.5	4	0.1668	0.0078	-95%
25	4	0.1406	0.0527	-62.50%
50	4	0.0156	0.0527	64%

C

Sum (%)	N (*Bits*)	One User	Two Users	I(Reduced /Increased)
0	8	0.0039	9×10^{-8}	-100%
12.5	8	0.0278	0.00005	-99%
25	8	0.0197	0.00278	-85.00%
50	8	0.0003	0.00278	44%

D

Sum (%)	N (*Bits*)	One User	Two Users	I(Reduced /Increased)
0	16	1.53×10^{-5}	8.5×10^{-15}	-100%
12.5	16	0.0008	2.66×10^{-9}	-99%
25	16	3.91×10^{-4}	7.73×10^{-6}	-98.00%
50	16	5.96×10^{-8}	7.73×10^{-6}	29%

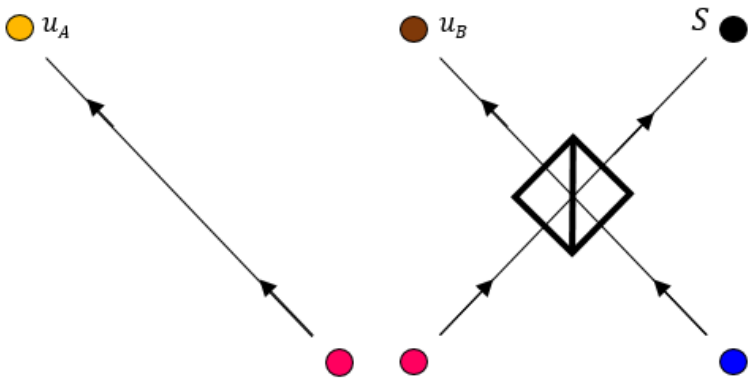


Fig. S13 Generation of *GHZ* States.