FRONTIERS OF PHYSICS

RESEARCH ARTICLE
Volume 18 / Issue 5 / 51304 / 2023

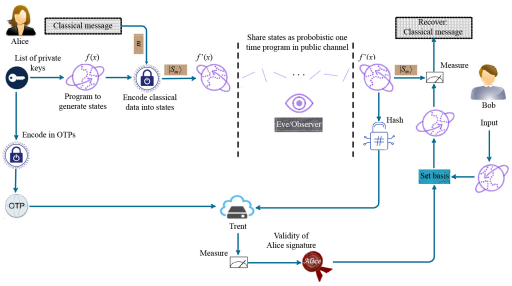
A probabilistic model of quantum states for classical data security

Muhammad Waseem Hafiz[1], Seong Oun Hwang[2,†]

1 Department of IT Convergence Engineering, Gachon University, Seongnam 13120, South Korea
2 Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea
Corresponding author. E-mail: †sohwang@gachon.ac.kr
Received December 12, 2022; accepted April 6, 2023

ABSTRACT

The phenomenal progress of quantum information theory over the last decade has substantially broadened the potential to simulate the superposition of states for exponential speedup of quantum algorithms over their classical peers. Therefore, the conventional and modern cryptographic standards (encryption and authentication) are susceptible to Shor's and Grover's algorithms on quantum computers. The significant improvement in technology permits consummate levels of data protection by encoding classical data into small quantum states that can only be utilized once by leveraging the capabilities of quantum-assisted classical computations. Considering the frequent data breaches and increasingly stringent privacy legislation, we introduce a hybrid quantum-classical model to transform classical data into unclonable states, and we experimentally demonstrate perfect state transfer to exemplify the classical data. To alleviate implementation complexity, we propose an arbitrary quantum signature scheme that does not require the establishment of entangled states to authenticate users in order to transmit and receive arbitrated states to retrieve classical data. The consequences of the probabilistic model indicate that the quantum-assisted classical framework substantially enhances the performance and security of digital data, and paves the way toward real-world applications.



Keywords information security, quantum-classical cryptography, quantum information processing, quantum spin states, spin-$\frac{1}{2}$ algebra, user authentication

1 Introduction

The security of classical cryptosystems is mostly reliant on the complexity of the computations, but quantum computers can efficiently develop quantum states to model multifaceted challenges and to handle computationally complex problems [1–3]. The superposition of states on quantum computers assures the exponential speedup of algorithms and simulations over their classical complements. The probability of each state expresses the particular state's behavior on measurement. Towards the major milestones for the development of quantum computers, Google announced quantum supremacy by producing the Sycamore (54 Qubit) and the Bristlecone (72 Qubit) chips [4]. In contrast, IBM recently announced that they thrived the 100-qubit barrier by producing the 127-qubit Eagle processor [5]. The computational resources of these mainframes can

Higher Education Press

https://doi.org/10.1007/s11467-023-1293-3

effectively handle conventional hard problems like discrete logarithms and integer factorization. These resources also validate the quadratic speedup in tackling unstructured search problems [6, 7], which threatens the complexity of traditional cryptography techniques. An adversary can bout a specific execution, attempting to dispute the operation, regardless of the physical mechanism employed to deactivate the device even after a single use.

The complexity of breaking asymmetric cryptosystems, such as Diffie–Hellman and Elliptic Curve Cryptography (ECC), is reliant on the difficulties in discrete logarithmic problems (DLP) in order to determine integer r, such that $g^r = x \bmod p$, where r is the DLP of x_g. The computation for $r = \log_g x \bmod p$ is quite challenging in the classical environment if the designated parameters are large enough [8]. Furthermore, ECC provides the same level of protection as RSA and DLP methods and is considered secure and efficient [9]. It employs the pair (x, y) in the equation $y^2 = x^3 + ax + b \bmod p$, where $a, b \in Z_p$, along with imaginary point θ at infinity. Factorization of large numbers and reckonings of discrete logarithms can be violated on quantum computers via Shor's algorithm [10]. The smaller key space of ECC compared to RSA makes breaches easier with a modified Shor's algorithm on data encrypted with ECC [11, 12]. Proos and Zalka [13] described the use of Shor's algorithm to break ECC over $GF(p)$, while Boudot *et al.* [14] highlighted the factorization of RSA-240 and cracking a DLP of the same size with Shor's method. It has also been demonstrated that a 1000-qubit processor is required to break a 160-bit elliptic curve, and a 2000-qubit processor is required to factorize 1024-bit RSA [13].

Lov Grover, on the other hand, developed an algorithm to search unsorted databases using quantum resources that deliver a square root speedup over classical brute force [7]. This algorithm can find a specific entry in an unsorted database of N entries from N searches, operates on $2^{n/2}$ for an n-bit cipher, which poses a threat to symmetric cryptographic schemes. In this case, a symmetric cipher with a 128-bit key size, such as AES-128, would offer a security level of 64 bits. Bone and Castro [15] commented on the impact of Grover's algorithm on DES-56, which required just 185 searches to find the key. Recently, Joshi and Gupta [16] implemented Grover's algorithm in a 4-qubit search space using IBM's QISKit. To secure information in the post-quantum era, NIST [17] and NSA [18] recommended the AES cipher with key sizes of 192 and 256 bits. Furthermore, the hash function's security is reliant on a fixed-length output, and Grover's method can be employed to detect a collision by searching an unsorted database, which suffers from the same problem as symmetric ciphers. It has also been proven that this method, when combined with the birthday paradox, may effectively execute a collision attack [19]. As a result, most existing hash algorithms are inadequate for utilization in the quantum era.

Public key algorithms such as DSA, ECDSA, ElGamal, and others are extensively used for digital signatures, and their security is reliant on the aforementioned discrete logarithmic problems, rendering them equally frail to Shor's algorithm on quantum resources. Despite being slower than Shor's method, Grover's algorithm has several applications in symmetric cryptosystems, and the research community is refining Grover's algorithm as well as developing comparable category classifications, which poses a severe threat to classical ciphers [20]. Therefore, cryptographic algorithms that are robust to quantum processes are required.

In the era of quantum information technologies, quantum computation [21], cryptography [22], and metrology [23] enable efficient processing, secure communications, and precise measurements. Quantum cryptography is one of the emergent quantum technologies, and experimental analysis of quantum key distribution (QKD) has already been conducted [24–27]. Although these approaches are favorable, they are far from being enacted with existing technologies. The traditional information exchange techniques can be enhanced by introducing the gain of quantumness [28, 29]. Recently, hybrid systems for probabilistic one-time programs were proposed [30, 31], but they face several theoretical and technological requirements and challenges that limit their implementation. Post-quantum cryptography (PQC) can also be used for authentication and encryption, and is believed to be useful for short-term security, such as authentication [32]. Except for Shor's algorithm, this technique is not yet theoretically secure and raises concerns about security against alternative conventional and quantum algorithms.

The ability to transfer quantum states to carry classical information is an important feature of a quantum information processing system [33]. These states can either contain a message or be utilized to establish entanglement between the two sites [34, 35]. The limitation and the challenge of quantum states are to store and manipulate the reconstruction on a classical computer, and various techniques have been devised that require partial information to inspect the generated states [36–38]. To overcome limitations, we developed a model similar to blind quantum computation (BQC) [39–42] in which the classical client can delegate quantum states for classical data, and the server or a malicious user will not be able to learn any information about the input, output, or algorithm. The proposed method addresses the following concerns.

- A quantum-assisted classical computation model that transforms classical data into unclonable quantum states and predicts classical information based on retrieved quantum states.
- An arbitrary quantum signature (AQS) scheme to authenticates users with classical key and plaintext spaces, making the model feasible for existing technolo-

gies.

We experimentally validated the proposed algorithm's efficiency, feasibility, and stability in authenticating users and transferring quantum states in order to represent classical data for quantum-safe communication.

This article is organized into six sections. Section 2 explains the procedure for generating unclonable quantum states, the signature scheme for user authentication, and the proposed model for securely sharing classical information in the form of quantum states. Experimental results of the proposed methodology when employing surveillance imagery are presented in Section 3. Section 4 contains performance analyses of the proposed model. Section 5 highlights a few real-world applications, and Section 6 comprises concluding remarks as well as information on supplementary documents.

2 Methodology

The establishment of quantum states to model a system, and the arbitrary quantum signature scheme are developed in this section. The proposed AQS scheme, which comprises initialization, signing, and verification, was developed by combining quantum theory with classical cryptography. This section also illustrates a proposed model for secure data sharing between two entities using arbitrary states.

2.1 Generation of quantum spin states

For a spin system, S, vectors are usually signified in terms of a Hermitian Cartesian component such as $\hat{S} = \begin{pmatrix} \hat{S}_x \\ \hat{S}_y \\ \hat{S}_z \end{pmatrix}$, and are represented in the Zeeman basis with the states $|S, m\rangle$ for $m = -S, -S+1, \cdots, S-1, S$ [43, 44]. The Cartesian operators for non-Hermitian components $S_x = \frac{1}{2}(S_+ + S_-)$ and $S_y = \frac{1}{2\mathrm{i}}(S_+ - S_-)$ satisfy the basis of states $\langle m'|\hat{S}_x|m\rangle = \frac{1}{2}\sqrt{S(S+1) - m'm}\,(\delta_{m',m+1} + \delta_{m'+1,m})$, $\langle m'|\hat{S}_y|m\rangle = \frac{1}{2\mathrm{i}}\sqrt{S(S+1) - m'm}\,(\delta_{m',m+1} - \delta_{m'+1,m})$, and $\langle m'|\hat{S}_z|m\rangle = \delta_{m',m}\,m$, where $S_+ = S_x + S_y$ and $S_- = (S_x - \mathrm{i}S_y)$. Hence, $\langle m'|\hat{S}_+|m\rangle = \sqrt{S(S+1) - m'm}\,\delta_{m',m+1}$ and $\langle m'|\hat{S}_-|m\rangle = \sqrt{S(S+1) - m'm}\;\delta_{m'+1,m}$.

For a spin $\frac{1}{2}$ system, the possible states with the z components for the angular momentum are $+\frac{\hbar}{2}$ for spin up, $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and $-\frac{\hbar}{2}$ for spin down, $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Hence, $S_z|+\rangle = +\frac{\hbar}{2}|+\rangle$ and $S_z|-\rangle = -\frac{\hbar}{2}|-\rangle$.

Let us consider $S_z = \begin{pmatrix} i & j \\ k & l \end{pmatrix}$ as a 2×2 matrix that represents the spin $\frac{1}{2}$ system as $\begin{pmatrix} i & j \\ k & l \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = +\frac{\hbar}{2}|+\rangle$ and $\begin{pmatrix} i & j \\ k & l \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\frac{\hbar}{2}|-\rangle$. To solve these equivalences, we received $i = +\frac{\hbar}{2}$, $j = 0$, $k = 0$, and $l = -\frac{\hbar}{2}$. Hence,

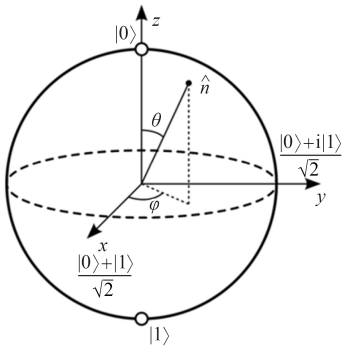
- $S_z = \frac{\hbar}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ with $|+\rangle_z = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|-\rangle_z = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Similarly, the spin operators in x and y directions are

- $S_x = \frac{\hbar}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with $|+\rangle_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $|-\rangle_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$, and
- $S_y = \frac{\hbar}{2}\begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$ with $|+\rangle_y = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \mathrm{i} \end{pmatrix}$ and $|-\rangle_y = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -\mathrm{i} \end{pmatrix}$.

Pauli's matrices σ_i can be extracted from the above equations as $S_i = \frac{\hbar}{2}\sigma_i$.

The spin constituent in the direction along the unit vector as $\hat{n} = \hat{i}\sin\theta\cos\phi + \hat{j}\sin\theta\sin\phi + \hat{k}\cos\theta$,



Spherical coordinates of spin system

therefore, spin vector S can be represented as a unit vector, $S_n = S\,\hat{n}$. Hence, $S_n = S_x\sin\theta\cos\phi + S_y\sin\theta\sin\phi + S_z\cos\theta$, which implies $S_n = \frac{\hbar}{2}\begin{pmatrix} \cos\theta & \sin\theta e^{-\mathrm{i}\phi} \\ \sin\theta e^{-\mathrm{i}\phi} & -\cos\theta \end{pmatrix}$ with eigenvectors $|+\rangle_n = \cos\frac{\theta}{2}|+\rangle + \sin\frac{\theta}{2}e^{\mathrm{i}\phi}|-\rangle$ and $|-\rangle_n = \sin\frac{\theta}{2}|+\rangle - \cos\frac{\theta}{2}e^{\mathrm{i}\phi}|-\rangle$.

The passive operators [39, 45, 46] to spin the states in the coordinate system can be computed as $S_i(\theta_i) = e^{\mathrm{i}S_i\theta_i/\hbar}$. Hence,

- $S_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \mathrm{i}\sin\frac{\theta}{2} \\ \mathrm{i}\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$,
- $S_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$, and
- $S_z(\theta) = \begin{pmatrix} e^{\mathrm{i}\frac{\theta}{2}} & 0 \\ 0 & e^{-\mathrm{i}\frac{\theta}{2}} \end{pmatrix}$.

The superposition of states for a qubit system on the Bloch sphere for diverse phase domains using IBM quantum composer and fetch the states for a classical system as shown in Fig. 1. Quantum mainframes can efficiently simulate the states for many-body systems [47, 48], and these complex states can be used to authenticate users and simulate data over classical as well as quantum computers. For a single qubit system, in Fig. 1, there are several superposition states. Each state has distinct symmetrical characteristics, and the interconnection of these states allows information to be propagated from one state to the next.

Each state comprises binary information 0 and 1, and the probability of each state expresses the particular behavior on measurement. The ability to transfer these

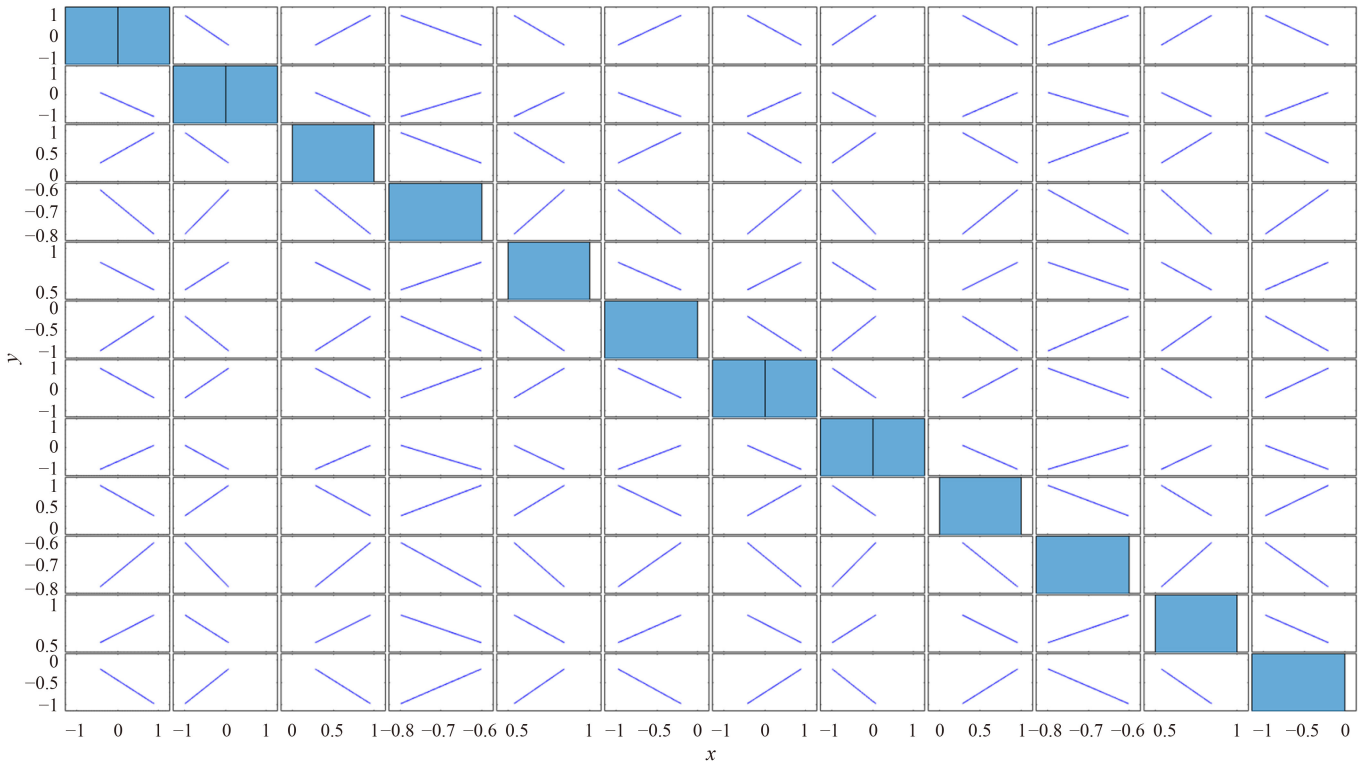


Fig. 1 Demonstration of a six-point spin state system (domain of –21.104 to 9.328 with a step size of 5.558) for a solo qubit.

states to carry classical information is an important feature of a quantum information processing system, and the information obtained via this approach can be conceived as a hash function of q-states on classical systems. These can either contain a message or be employed to establish entanglement between the two sites by utilizing a spin lock mechanism to detect the phase transition between sites and pair generations.

The demonstrated states in Fig. 1 are generated at six points [–21.1040, –15.5460, –9.9880, –4.4300, 1.1280, 6.6860], and each point value indicates 24 distinct states to represent data. For a spin $\frac{1}{2}$ system, we can model complex structures and many-point systems in the phase domain $-720°$ and $720°$ with minimum step sizes. In the supplemental file, Figs. 1 and 2 elaborate on the demonstration of 15 and 25 point systems for various domains of phases.

2.2 AQS scheme

The proposed AQS scheme consists of initializing, signing, and verifying through a combination of quantum theory and classical cryptography.

Assume $\{Q_\alpha^1\}_\alpha$ and $\left\{Q_\beta^2\right\}_\beta$ are two distinct sets of one-way functions with uniform output distribution, where $\alpha, \beta \in \{0,1\}^n$ and Q_α^1, $Q_\beta^2 : \{0,1\}^* \to \{0,1\}^n$. All one-way functions will be independent of each other for different α and $\beta \in \{0,1\}^n$.

Initializing

Let Alice and Bob would like to share a few private credentials with a trustworthy arbitrator, Trent, using QKD or the protocol developed by Marie *et al.* [30, 31].

- Conferring Alice's private key, $P_{k_{AT}} = (P_{k1}^{AT}, P_{k2}^{AT}, \cdots, P_{k\,n}^{AT}) \in \{0,1\}^n$, she secretly chooses one-way function $Q_{P_{k(AT)}}^1$, $Q_{P_{k(AT)}}^2 : \{0,1\}^* \to \{0,1\}^n$ from the sets $\{Q_\alpha^1\}_\alpha$ and $\left\{Q_\beta^2\right\}_\beta$.
- Similarly, conferring Bob's private key, $P_{k_{BT}} = (P_{k1}^{BT}, P_{k2}^{BT}, \cdots, P_{k\,n}^{BT}) \in \{0,1\}^n$, he secretly chooses one-way function $Q_{P_{k(BT)}}^1$, $Q_{P_{k(BT)}}^2 : \{0,1\}^* \to \{0,1\}^n$ from the sets $\{Q_\alpha^1\}_\alpha$ and $\left\{Q_\beta^2\right\}_\beta$.

Let us define $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, \cdots, y_n) \in \{0,1\}^n$, Hadamard $H = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and unit operator I, where $x \oplus y = (x_1 \oplus y_1, x_2 \oplus y_2, \cdots, x_3 \oplus y_3)$ and $H^0 = 1$.

Signing

Let the message $m = (m_1, m_2, \cdots, m_n) \in \{0,1\}^n$ needs to be signed.

- Alice calculates the hash of the message as $h_A = Q_{P_{k(AT)}}^1(m) \oplus Q_{P_{k(AT)}}^2(m)$ and $r_A = h_A \oplus m$, where $h_A = (h_1, h_2, \cdots, h_n)$ and $r_A = (r_1, r_2, \cdots, r_n)$ for each $1 \le i \le n$ and $r_i = h_i \oplus m_i$.
- She generates a signature from her private key for Trent, $|S_{m,p_k,\lambda T}\rangle := \otimes_{i=1}^n |S_i\rangle$,

where $|S_i\rangle = H^{r_i}|m_i\rangle = \begin{cases} |0\rangle & \text{for } r_i = 0 \text{ and } m_i = 0, \\ |1\rangle & \text{for } r_i = 0 \text{ and } m_i = 1, \\ |+\rangle & \text{for } r_i = 1 \text{ and } m_i = 0, \\ |-\rangle & \text{for } r_i = 1 \text{ and } m_i = 1. \end{cases}$

- She sends r_A and $|S_{m,\, P_{k(AT)}}\rangle$ to Bob using the classical and the quantum channel.

Verification

Bob will make an appropriate measurement after receiving r_A and $|S_{m,\, P_{k(AT)}}\rangle$ on each state according to r_i and $|S_i\rangle$ by choosing basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ to measure $|S_i\rangle$ for $r_i = 0$. By using the consequences of $|S_i\rangle$ and the measurement, he is able to set $m_i := \begin{cases} 0 & \text{for } |S_i\rangle = |0\rangle \text{ or } |+\rangle \\ 1 & \text{for } |S_i\rangle = |1\rangle \text{ or } |-\rangle \end{cases}$.

- Bob will use his private key, $P_{k_{BT}}$, and one-way functions, $Q^1_{P_{k(BT)}}$ and $Q^2_{P_{k(BT)}}$, to derive h_B and announce the pair (m, h_B) for Trent to download, where $h_B = Q^1_{P_{k(BT)}}(h_A \parallel r_A \parallel m) \oplus Q^2_{P_{k(BT)}}(h_A \parallel r_A \parallel m)$.
- Trent will compute h'_A and h'_B using the one-way functions of Alice and Bob as:
  - $h'_A = Q^1_{P_{k(AT)}}(m) \oplus Q^2_{P_{k(AT)}}(m)$, and
  - $h'_B = Q^1_{P_{k(BT)}}(h'_A \parallel r'_A \parallel m) \oplus Q^2_{P_{k(BT)}}(h'_A \parallel r'_A \parallel m)$,

  where $r_A = h'_A \oplus m$.
- Trent announces the validity of (m, h_B) publicly if $h'_B = h_B$, and Bob will accept $(m, h_A\, |S_{m,\, P_{k(AT)}}\rangle)$ as a valid signature.

Bob will set the basis accordingly to measure the states, which allows him to fetch the message, $m = (m_1, m_2, \cdots, m_n)$.

2.3 Proposed model for state transfer

We consider data sharing between Alice and Bob where Alice provides data in the form of arbitrary states, and Bob retrieves data from the received states. She encodes classical data in the form of states, which grow linearly in the number of q-sequences required to execute function f, and then sends the states to Bob. He will assess the received states sequentially to extract the plaintext data. These evaluations are primarily irreversible, and Bob must evaluate function $f(x)$, whereas (in unison for some input) it prevents him from learning about $f(x')$ such that $x' \neq x$. The overview of quantum-assisted classical computation is given in Fig. 2.

The interconnection of states allows Alice to propagate information from one state to the next, and each state contains binary information 0 and 1 at the same time. For the classical 8-bit data stream illustrated in Fig. 2, the transitions to spin states are as follows.

- If the first bit is 0, the transferred state would be

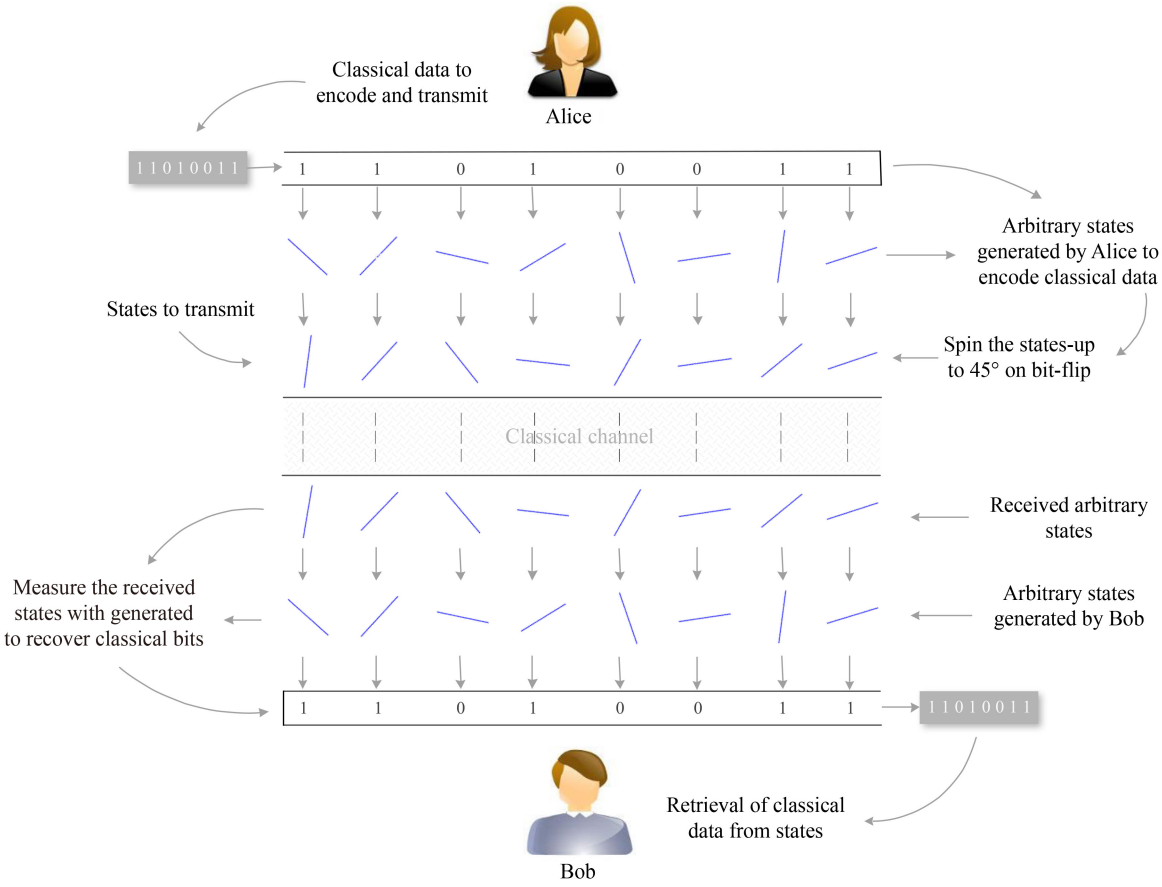


Fig. 2 Mechanism for classical data sharing upon the transition of unclonable quantum states.

the same as the generated one.

- If the first bit is 1, it spins the state at the designated phase (up-spin of 45°) in Fig. 2.
- The proceeding states spins at the designated phase on the bit flip.
- On reception, the receiver sets the basis with the shared information and a private key to measure the incoming states to retrieve the classical bits.

The probabilistic version of states (pointed out by Roehsner MC *et al.* [30, 31]) for the classical data, encoded using a single qubit, is specified in Fig. 3. The measurement corresponding to input is anti-commute [49], which can be obtained by fixing the basis to be consistent with inputs 0 and 1, σ_z for 0 and σ_x for 1, respectively, to find the state to encode and decode the data.

The encoding is related to Wiesner's conjugate encoding [50] and is equivalent to the quantum random access code addressed in Ref. [51].

To demonstrate the feasibility of the proposed scheme, we consider a program to generate q-states for universal classical computation that transforms classical message m into state $|m\rangle$, in which two entities can share their data without disclosing their credentials to other parties. To accomplish the objective, Alice encodes her classical data stream with the generated q-states and transmits it with the delegation of signature. On the other hand, after authenticating Bob's factual identification, the program returns a classical bit sequence. Figure 4 depicts an overview of the model.

Bob computes a hash of the message to sign, uses it as input to generate states for message retrieval, and Trent verifies the output of the one-way function (see Section 2.2). However, we assume spin locking between Alice and Bob in order to generate q-states on both sides (either with Trent or in a symmetric fashion) to transform classical bits into spin states and then extract the classical data by measuring the generated and received states.

3 Experimental results

We conducted an experiment using surveillance drone imagery to securely transmit specified aerial information to the receiver (Fig. 5). Table 1 analyzes the information loss in the recovered imagery (compared to the original) to confirm the efficacy of classical data recovery from quantum states.

The source was high-resolution aerial surveillance

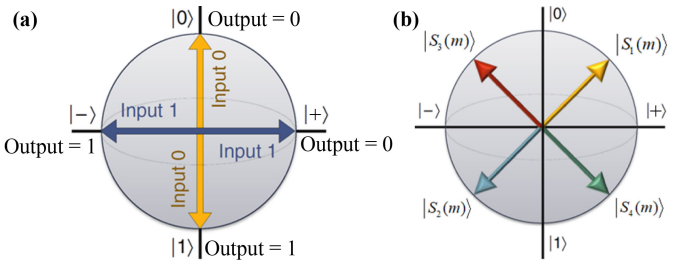


Fig. 3 **(a)** Probabilistic version of states for classical data, and **(b)** measurement of the basis for finding the states.

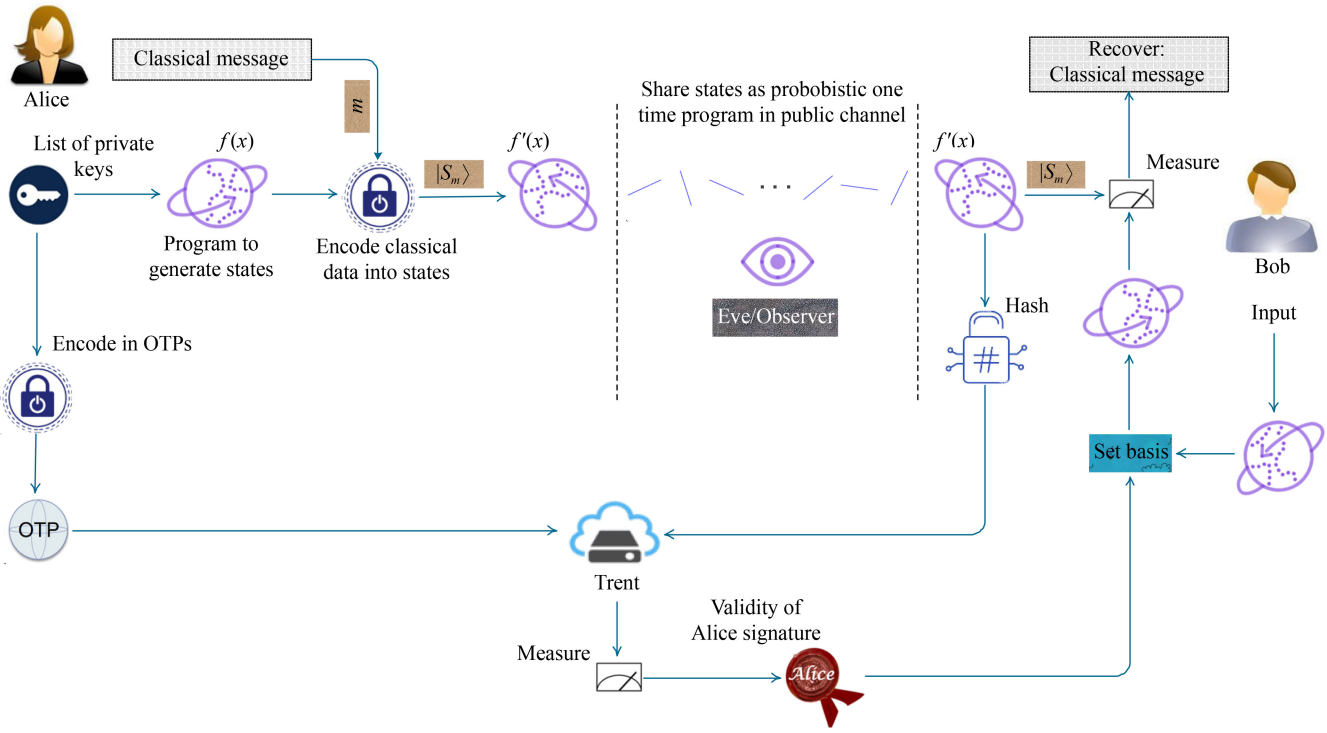


Fig. 4 Proposed methodology for secure data sharing between two entities on the conjunction of quantum states.

imagery (image 1) captured with a high payload capacity WingtraOne mapping drone equipped with a Sony RX1R II camera, accessible from the WingtraOne data sets repository. We assumed the spectator is required to transmit specific information from the construction site (image 2) to another individual to demonstrate the progress in a specific region (image 3). The experiment was carried out under ideal conditions, with no channel loss or state disruption, transforming the imagery into q-states for transmission and recovering it from free states upon reception. We used correlation analysis [52, 53] to compare the transmitted and recovered data and observed a minor loss in the retrieved information. Analyses of the structural similarity index measure (SSIM), the structural content (SC), and normalized absolute error (NAE) [54, 55] for the original and recovered imagery (see Fig. 5) were carried out in Table 1 to validate the feasibility of the proposed methodology in Fig. 4. The supplementary document contains detailed experiments on multispectral, medical, and RGB images, as well as correlation analyses in horizontal, vertical, and diagonal directions.

The correlation error and NAE between the original and recovered images were almost negligible, whereas the recovered content's luminance, divergence, and assembly had more than 98% similarity to the original captured content. The structural details of the recovered imagery in terms of sharpness and noise had more than 99% similarity. These results validate the efficacy of the proposed model with a trivial loss in the recovery of data from q-states.

4 Discussion

Quantum technology permits consummate levels of data protection by encoding classical information into small quantum states for quantum-assisted classical computations. These programs expedite the diversity of applications ranging from data sharing to one-time signature delegation authority [31]. The exponential speedup of quantum computers can unravel multifaceted challenges, but the generated states in this study are unclonable and cannot be copied or replicated by the observer in the channel. An observer needs to compute 1440^n combinations to predict the basis of the states, where n is the number of

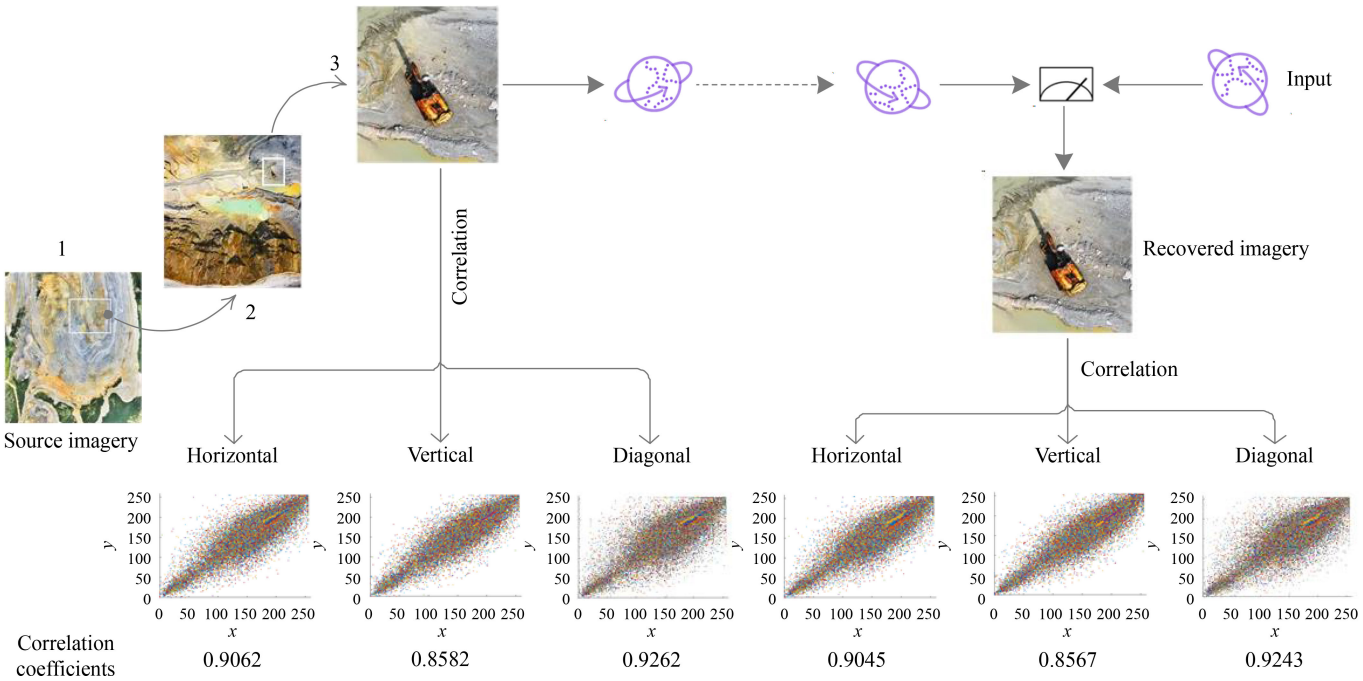


Fig. 5 Experimental analysis of classical drone imagery transition into quantum states and imagery recovery from the states upon reception based on measurement of the spin lock system.

Table 1 Similarity analysis of original and recovered surveillance drone imagery.

Correlation error			NAE	SSIM	SC
Horizontal	Vertical	Diagonal			
0.0019	0.0018	0.0021	0.0074	0.9859	0.9997

points on which the states are generated. To predict the measurement for the correct basis on six-point state generation (see Fig. 1), it is necessary to compute 1440^6 combinations if a step size of 1 was used to generate states.

4.1 Attacks on model

State encoding programs are non-orthogonal and coupled with the no-cloning theorem [56], which implies the impossibility of producing two copies from a single copy. In a single-shot regime of state conversion for a distinct copy of a state, where numerous copies are assumed to be available, one must solve for all pure and mixed states [57–59]. The mixed states prevent dishonest users from learning about the function's coherent query and extracting any information about classified data.

Birthday attack

The birthday paradox contemplates the probability of randomly chosen states from a set of n states, and substantiates similar features with the selected states. This attack exploits the reckonings behind the state conversion problem in probability theory and depends on a fixed degree of permutation, such as $S = \{S_i \in S_{4\times4}(I, S_x(\theta), S_y(\theta), S_z(\theta)),\ i = 1, 2, \cdots, 24\}$. On measurement, each state clicks the 50% probability of diverging into a definite state. To launch this attack on the states generated in Fig. 1 in order to find a collision in random attempts, the probability is $\frac{1}{(2\times m\times n)-d}$ for measuring an accurate basis to retrieve a classical solo bit, where m, n, and d correspond to row, column, and diagonal entries of states. Each state spins on a different point; thus, finding a collision between the axis of rotation for the states is not possible by an observer in the channel.

Secret state recovery attack

An adversary needs to estimate function $f''(x)$ for $f'(x)$ to recover the secret states.

- Let $b \in \{0, 1\}$, $x \in \{0, 1\}^n$, and α_1, α_2 are two arbitrary numbers in $\{0, 1\}^n$ fixed by an adversary.
- To measure the states in the channel, $|S_m\rangle$, an adversary needs to produce arbitrary states $|\alpha\rangle$ to estimate an arbitrary function:

$$\varepsilon(f) = \begin{cases} |0\rangle \ \text{ for } & \{|S_{m_1}\rangle, |\alpha_1\rangle\}, \\ & \{|S_{m_2}\rangle, |\alpha_1\rangle\}, \\ |1\rangle \ \text{ for } & \{|S_{m_1}\rangle, |\alpha_2\rangle\}, \\ & \{|S_{m_2}\rangle, |\alpha_2\rangle\}. \end{cases}$$

- By using function $\varepsilon(f)$ and the states over the channel, an adversary can try to estimate $f''(x) = ((|S_{m_1}, \alpha_1\rangle, |S_{m_1}, \alpha_2\rangle) \approx (|S_{m_2}, \alpha_1\rangle, |S_{m_2}, \alpha_2\rangle))$ to forge a message by measuring the states on a channel using $f''(x)$.

The generated states in the algorithm shown in Fig. 4 withstand this attack by means of Trent to validate the factual identity and unique states for the message. The states $|S_i\rangle$ for message m_i are inimitable and have no collisions or correlations. Table 2 summarizes the characteristics of the proposed model in comparison to existing methodologies.

The most frequent approaches employ quantum channels for a perfect state transfer to carry classical data. For perfect state transfer on the quantum channel, existing methodologies assume entanglement, which is far from being addressed with the existing technology. Our proposed model is compatible with today's technology because it shares data in the form of perfect states over a classical channel, rather than establishing a secure path using entanglement.

4.2 Attacks on AQS

The novelty of existing AQS schemes depends on QKD, BQC, and the distribution of quantum particles among partners using entangled states, whereas the proposed technique leverages the classical channel to interact with the verifier through a trusted arbitrator. Furthermore, a quantum swap test [61] is not required to validate the quantum message for the devised technique in this work. In this section, a few key analyses are carried out to assess the resilience of the developed scheme counter to certain attacks.

Security of the private key

A malicious user can forge the signature on any message in AQS schemes if the private key is revealed. In the proposed scheme, Alice and Trent share private key $P_{k(AT)}$ using QKD or the technique developed in [31], which constrains a malicious user from breaking or

Table 2 Comparison of the proposed probabilistic model with existing methodologies.

Methodology	State transfer	Entanglement	Forgery attack	Birthday attack	Channel
Proposed	Perfect	No	No	No	Classical/Quantum
Ref. [60]	No	No	–	Yes	Classical/Quantum
Ref. [30]	Perfect	Yes	No	No	Quantum
Ref. [31]	Perfect	No	No	No	Quantum
Ref. [39]	–	Yes	No	–	Quantum
Ref. [57]	Perfect	Yes	No	–	Quantum

bypassing the private key in the initializing phase.

- An adversary needs to fetch the information, m, r_A, h_B, and $|S_{m,P_{K(AT)}}\rangle$, interpreted through the public channel to break the private key.
- He can try to impersonate Bob to verify the signature with $P_{k(BT)}$ to derive h_A.
- r_A, h_B, and $|S_{m,P_{K(AT)}}\rangle$ are redundant parameters derived from m, h_A, and $P_{K(BT)}$, and an adversary needs to predict the output of $Q^1_{P_{k(AT)}}$ and $Q^2_{P_{k(AT)}}$ with an insignificant probability of $1/2^{2n}$.
- After predicting the output, he needs to estimate m from the transformed unclonable states with a probability of $1/2^{2\times 3n}$ to predict h_A.

Arbitrary states enable distinct sequences for the same input data while preventing information leakage that may compromise the key. As a result, the probability of estimating m to break the key is negligible.

Forgery attack

There are two possibilities to forge the signature by a malicious user.

1. Forge a legitimate signature with an arbitrarily generated signature on the same message: Given the unique states for message m and private key $P_{K(AT)}$, the accompanying signature, $|S_{m,P_{K(AT)}}\rangle = \otimes_{i=1}^{n} H^{r_i}|m_i\rangle$, will be unique. Therefore, it is impossible to replace a valid signature with a fake signature $\left(|m\rangle, h^*_A, \left|S^*_{m,P_{K(AT)}}\right\rangle\right)$ on the same message.

2. Forge with arbitrarily produced signature on a new message: A malicious user needs to set pair (m^*, h^*_B) and share it with Trent to announce its validity publicly. Although he expects to receive $h^*_B = h'_B$, without knowledge of $Q^1_{P_{k(BT)}}$, $Q^2_{P_{k(BT)}}$, h'_A, and r'_A, he will try to guess $h^*_B = h'_B$ with an insignificant probability of $1/2^n$. Hence, this forgery is also not viable for adversary.

Disavowal attack

In the proposed scheme, Alice and Trent will not share h_A with Bob. He has to derive it from signature $|S_{m,P_{K(AT)}}\rangle$ by measuring the received states. He can confirm the validity of the signature $(m, h_A, |S_{m,P_{K(AT)}}\rangle)$ with the assistance of Trent by sharing the derived h_A. As a result, neither Alice nor Bob can deny the authenticity of a particular signature $(m, h_A, |S_{m,P_{K(AT)}}\rangle)$.

4.3 Characteristics comparison

In modern signature schemes, both the signer and the verifier need to perform QKD [62, 63] or BQC [40] to share an n-bit secret key before signing a message. The distribution of quantum particles among companions, before establishing a signature by the signer or arbitrator, can reduce the efficiency of signature schemes [64, 65]. Furthermore, entangled-state-based signature schemes are promising, but the effectiveness of their implementation is too complex with the existing technology. Table 3 contains a few analyses of the proposed approach in contrast to existing methodologies.

Most existing authentication methods, irrespective of plaintext, key, or signature space, need entanglement or the quantum channel, which are not compatible with today's technology. The schemes proposed in Refs. [36] and [39] employ BQC to establish entangled states between end users under perfect security constraints, but an adversary can disrupt the states during formation of a secure connection using BQC, rendering the path unavailable for communication. As a result, end users would be unable to establish a secure connection. The signature space between Alice-Bob and Alice-Trent in the proposed model is quantum, to prevent forgery and manipulation, whereas the key and plaintext are classical, making it feasible with existing technology.

5 Applications

The developed probabilistic model has a wide range of potential applications, including satellite and drone imagery, conventional, medical, and RGB content, quan-

Table 3 Comparison of the proposed scheme with existing methodologies.

Methodology		Proposed	Ref. [30]	Ref. [31]	Ref. [36]	Ref. [39]	Ref. [62]	Ref. [63]	Ref. [64]
Space analysis	Plaintext space	Classical	Classical	Classical	–	–	Classical	Quantum	Classical
	Keyspace	Classical	Classical	Classical	–	–	–	Quantum	–
	Signature space	Quantum	Quantum	Classical	–	–	Quantum	Quantum	Quantum
Channel	Alice-Bob	Classical/Quantum	Quantum	Quantum	–	–	Quantum	Quantum	Quantum
	Alice-Trent	Classical/Quantum	–	–	–	–	–	–	Quantum
	Bob-Trent	Classical	–	–	–	–	Quantum	Quantum	Quantum
Supplementary requirements	Shared key	No	Yes	No	–	–	Yes	Yes	No
	QKD	No	Yes	–	–	–	Yes	Yes	No
	BQC	No	No	–	Yes	Yes	–	–	–
	Entangled states	No	Yes	–	Yes	Yes	No	No	No
	Swap test	No	Yes	–	Yes	–	No	Yes	Yes

tum-assisted classical internet, internet of things security, and so on. We summarize a few segments related to real-time applications below.

Satellite imagery: At the time of writing, the Defense Advanced Research Projects Agency (DARPA) was preparing to launch the Blackjack LEO satellite for surveillance imaging, secure data transfer, navigation, and satellite phones [66, 67]. Hancom, on the other hand, recently launched Sejong-1 (South Korea's first private commercial earth observation satellite) for integrated image analysis, with plans to launch five more LEO spacecraft by 2025 [68]. However, satellite data transmission may pose certain threats, such as cyberattacks. Radiometric, spectral, spatial, and temporal resolutions of imagery can benefit from the proposed probabilistic model in real-time secure transmissions for decision-making.

Quantum internet: The objective of the quantum internet is to deliver new technologies by enabling quantum communications among numerous locations around the globe [69]. The proposed model can transform quantum information into classical data, and offers interaction between the quantum internet and current technologies.

Internet of things security: To work effectively, IoT applications collect a large amount of personal data. IoT devices employ conventional hashing algorithms to encrypt passwords to secure user data, but they may be cracked using a rainbow table. In the development of IoT devices, developers must include a digital signature while developing software in order to prevent hackers from replacing it with malicious firmware [70]. The proposed AQS algorithm can be used in IoT devices with slight modifications for device constraints. In general, hackers bypass a secure boot by replicating the authentic signature using a Dyn or Mirai botnet, a baby monitor, and TRENDnet attacks [70, 71]. For the proposed AQS, there is a need to measure perfect states in which digital signatures are generated and placed, with infinite computational resources to bypass the secure boot.

6 Conclusion

In this paper, we demonstrated the arbitrated quantum signature and unclonable spin states, in both theory and experimentation, for secure transmission and reception of classical data. The experiment is comprehended without assumptions of computational hardness and entanglement exertion, and the findings verified that quantum physics countenances improved security tradeoffs for certain computing tasks in classical communications. We observed that the outcomes produced by the proposed methodology are in good accord with the readily available technology, and we believe that the provided work insinuates the rich domain of quantum practices to enhance the security of classical computations. Future advancements would allow for quantum state verification and non-separable measurement on the client side, which might be the intention of, and an improvement to, the anticipated model.

Electronic supplementary materials The online version contains supplementary material available at https://doi.org/10.1007/s11467-023-1293-3 and https://journal.hep.com.cn/fop/EN/10.1007/s11467-023-1293-3. The supplementary material includes a file with experimental details on the generation of spin states for 15- and 25-point systems, as well as hyperspectral, MRI, and standard RGB image analysis. MATLAB,. Fig, files for the generation of distinct states for 6-, 15-, and 25-point static state systems are also attached. For a 6-point system, we provide two files to demonstrate the distinction between the produced states.

Conflict of interest The authors confirm they have no conflicts of interest regarding the publishing of this article.

Acknowledgements This work was supported in part by the National Research Foundation of Korea Grant funded by the Korea Government [Ministry of Science and ICT (MSIT)] under Grant No. 2020R1A2B5B01002145, and in part by the Gachon University Research Fund under Grant No. GCU-202106360001.

References

1. R. S. Bennink, Efficient verification of anticoncentrated quantum states, *npj Quantum Inf.* 7(1), 127 (2021)
2. H. Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, and J. R. McClean, Quantum advantage in learning from experiments, *Science* 376(6598), 1182 (2022)
3. N. N. Zhang, M. J. Tao, W. T. He, X. Y. Chen, X. Y. Kong, F. G. Deng, N. Lambert, and Q. Ai, Efficient quantum simulation of open quantum dynamics at various Hamiltonians and spectral densities, *Front. Phys.* 16(5), 51501 (2021)
4. F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, et al., Quantum supremacy using a programmable superconducting processor, *Nature* 574(7779), 505 (2019)
5. J. Chow, O. Dial, and J. Gambetta, IBM Quantum breaks the 100-qubit processor barrier, IBM Research Blog, 2021
6. P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in: Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994
7. L. K. Grover, A fast quantum mechanical algorithm for database search: in: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, 1996, pp 212–219
8. M. W. Hafiz, W. K. Lee, S. O. Hwang, M. Khan, and A. Latif, Discrete logarithmic factorial problem and Einstein crystal model based public-key cryptosystem for digital content confidentiality, *IEEE Access* 10,

102119 (2022)
9. C. Paar and J. Pelzl, Introduction to public-key cryptography, in: Understanding Cryptography, Berlin, Heidelberg: Springer, 2010
10. P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Rev.* 41(2), 303 (1999)
11. Z. Kirsch and M. Chow, Quantum computing: The risk to existing encryption methods, URL: www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf
12. M. I. Bhat and K. J. Giri, Impact of computational power on cryptography, in: Multimedia Security, Singapore: Springer, 2021 pp 45–88
13. J. Proos and C. Zalka, Shor's discrete logarithm quantum algorithm for elliptic curves. arXiv: quant-ph/0301141 (2003)
14. F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé, and P. Zimmermann, Comparing the difficulty of factorization and discrete logarithm: A 240-digit experiment, in: Annual International Cryptology Conference, 2020, pp 62–91
15. S. Bone and M. Castro, A brief history of quantum computing, Imperial College in London, 1997
16. S. Joshi and D. Gupta, Grover's algorithm in a 4-qubit search space, *Journal of Quantum Computing.* 3(4), 137 (2021)
17. M. E. Smid, Development of the advanced encryption standard, *J. Res. Natl. Inst. Stand. Technol.* 126, 126024 (2021)
18. NSA/CSS, Commercial national security algorithm suite and quantum computing FAQ, Information assurance directorate, 2016
19. G. Brassard, P. Høyer, and A. Tapp, Quantum cryptanalysis of hash and claw-free functions, in: Latin American Symposium on Theoretical Informatics, Berlin, Heidelberg: Springer, 1998, pp 163–169
20. X. Q. Cai, T. Y. Wang, C. Y. Wei, and F. Gao, Cryptanalysis of quantum digital signature for the access control of sensitive data, *Physica A* 593, 126949 (2022)
21. G. Benenti, G. Casati, D. Rossini, and G. Strini, Principles of quantum computation and information: A comprehensive textbook, 2019
22. C. Portmann and R. Renner, Security in quantum cryptography, *Rev. Mod. Phys.* 94(2), 025008 (2022)
23. N. Shettell, E. Kashefi, and D. Markham, Cryptographic approach to quantum metrology, *Phys. Rev. A* 105(1), L010401 (2022)
24. F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* 92(2), 025002 (2020)
25. S. K. Liao, W. Q. Cai, W. Y. Liu, L. Zhang, Y. Li, et al., Satellite-to-ground quantum key distribution, *Nature* 549(7670), 43 (2017)
26. H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite, *Nat. Photonics* 11(8), 502 (2017)
27. Y. F. Yan, L. Zhou, W. Zhong, and Y. B. Sheng, Measurement-device-independent quantum key distribution of multiple degrees of freedom of a single photon, *Front. Phys.* 16(1), 11501 (2021)
28. Z. G. Wang, S. J. Wei, and G. L. Long, A quantum circuit design of AES requiring fewer quantum qubits and gate operations, *Front. Phys.* 17(4), 41501 (2022)
29. H. M. Waseem and S. O. Hwang, Design of highly nonlinear confusion component based on entangled points of quantum spin states, *Sci. Rep.* 13(1), 1099 (2023)
30. M. C. Roehsner, J. A. Kettlewell, J. Fitzsimons, and P. Walther, Probabilistic one-time programs using quantum entanglement, *npj Quantum Inf.* 7, 98 (2021)
31. M. C. Roehsner, J. A. Kettlewell, T. B. Batalhão, J. F. Fitzsimons, and P. Walther, Quantum advantage for probabilistic one-time programs, *Nat. Commun.* 9(1), 5225 (2018)
32. K. Han, A. Raza, and S. O. Hwang, CAPTCHA-based secret-key sharing using quantum communication, *IT Prof.* 23(6), 46 (2021)
33. J. L. Pachuau and A. K. Saha, Generic conversion method for various spatial domain filters in quantum image processing, *Physica A* 596, 127196 (2022)
34. Y. Wei, S. Wang, Y. Zhu, and T. Li, Sender-controlled measurement-device-independent multiparty quantum communication, *Front. Phys.* 17(2), 21503 (2022)
35. Z. Ji, P. Fan, and H. Zhang, Entanglement swapping for Bell states and Greenberger–Horne–Zeilinger states in qubit systems, *Physica A* 585, 126400 (2022)
36. O. M. Sotnikov, I. A. Iakovlev, A. A. Iliasov, M. I. Katsnelson, A. A. Bagrov, and V. V. Mazurenko, Certification of quantum states with hidden structure of their bitstrings, *npj Quantum Inf.* 8, 41 (2022)
37. J. Xiao, J. Wen, S. Wei, and G. Long, Reconstructing unknown quantum states using variational layerwise method, *Front. Phys.* 17(5), 51501 (2022)
38. C. Luo, F. Guo, W. Wan, Y. Fang, P. Wang, and X. Huang, Demonstration of ghost communication with an encrypted speckle, *Opt. Laser Technol.* 149, 107926 (2022)
39. Z. Qu, K. Wang, and M. Zheng, Secure quantum fog computing model based on blind quantum computation, *J. Ambient Intell. Humaniz. Comput.* 13(8), 3807 (2022)
40. Q. Li, Z. Li, W. H. Chan, S. Zhang, and C. Liu, Blind quantum computation with identity authentication, *Phys. Lett. A* 382(14), 938 (2018)
41. S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Demonstration of blind quantum computing, *Science* 335(6066), 303 (2012)
42. Q. Li, C. Liu, Y. Peng, F. Yu, and C. Zhang, Blind quantum computation where a user only performs single-qubit gates, *Opt. Laser Technol.* 142, 107190 (2021)
43. N. Wheeler, Spin matrices for arbitrary spin, Reed College Physics Department, Portland, 2000
44. H. M. Waseem and M. Khan, Information confidentiality using quantum spinning, rotation and finite state machine, *Int. J. Theor. Phys.* 57(11), 3584 (2018)
45. J. Branson, Quantum physics, derive the expression for rotation operator, 2013
46. A. Alghafis, H. M. Waseem, M. Khan, and S. S. Jamal, A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states, *Physica A* 554, 123908 (2020)
47. F. Tacchino, A. Chiesa, S. Carretta, and D. Gerace,

Quantum computers as universal quantum Simulators: State-of-the-art and perspectives, *Adv. Quantum Technol.* 3(3), 1900052 (2020)
48. H. M. Waseem and M. Khan, A new approach to digital content privacy using quantum spin and finite-state machine, *Appl. Phys. B* 125(2), 27 (2019)
49. R. E. Kastner, Unitary-only quantum theory cannot consistently describe the use of itself: On the frauchiger–renner paradox, *Found. Phys.* 50(5), 441 (2020)
50. S. Wiesner, Conjugate coding, *ACM Sigact News.* 15(1), 78 (1983)
51. A. Nayak, Optimal lower bounds for quantum automata and random access codes, in: 40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039), IEEE, 1999, pp 369–376
52. H. M. Waseem, A. Alghafis, and M. Khan, An efficient public key cryptosystem based on dihedral group and quantum spin states, *IEEE Access* 8, 71821 (2020)
53. S. I. Batool, M. Amin, and H. M. Waseem, Public key digital contents confidentiality scheme based on quantum spin and finite state automation, *Physica A* 537, 122677 (2020)
54. A. Alghafis, H. M. Waseem, M. Khan, S. S. Jamal, M. Amin, and S. I. Batool, A novel digital contents privacy scheme based on quantum harmonic oscillator and schrodinger paradox, *Wirel. Netw.*, (2020)
55. A. H. Ismail, H. M. Waseem, M. Ishtiaq, S. S. Jamal, and M. Khan, Quantum spin half algebra and generalized megrelishvili protocol for confidentiality of digital images, *Int. J. Theor. Phys.* 60(5), 1720 (2021)
56. W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* 299(5886), 802 (1982)
57. K. D. Wu, T. Theurer, G. Y. Xiang, C. F. Li, G. C. Guo, M. B. Plenio, and A. Streltsov, Quantum coherence and state conversion: Theory and experiment, *npj Quantum Inf.* 6, 22 (2020)
58. Z. D. Ye, D. Pan, Z. Sun, C. G. Du, L. G. Yin, and G. L. Long, Generic security analysis framework for quantum secure direct communication, *Front. Phys.* 16(2), 21503 (2021)
59. B. Regula, K. Fang, X. Wang, and G. Adesso, One-shot coherence distillation, *Phys. Rev. Lett.* 121(1), 010401 (2018)
60. R. Kuang and M. Barbeau, Quantum permutation pad for universal quantum-safe cryptography, *Quantum Inform. Process.* 21(6), 211 (2022)
61. S. Foulds, V. Kendon, and T. Spiller, The controlled SWAP test for determining quantum entanglement, *Quantum Sci. Technol.* 6(3), 035002 (2021)
62. D. H. Jiang, Y. L. Xu, and G. B. Xu, Arbitrary quantum signature based on local indistinguishability of orthogonal product states, *Int. J. Theor. Phys.* 58(3), 1036 (2019)
63. L. Zhang, H. W. Sun, K. J. Zhang, and H. Y. Jia, An improved arbitrated quantum signature protocol based on the key-controlled chained CNOT encryption, *Quantum Inform. Process.* 16(3), 70 (2017)
64. M. Q. Wang, X. Wang, and T. Zhan, An efficient quantum digital signature for classical messages, *Quantum Inform. Process.* 17(10), 275 (2018)
65. S. Akleylek, M. Soysaldı, W. K. Lee, S. O. Hwang, and D. C. Wong, Novel Postquantum MQ-based signature scheme for Internet of things with parallel implementation, *IEEE Internet Things J.* 8(8), 6983 (2021)
66. S. Erwin, Parsons to Develop Ground Operations Center for DARPA's Blackjack Satellites, Space News, 2021
67. M. Borowitz, The military use of small satellites in orbit, Briefings de l'Ifri, Ifri, 2022
68. Korea-EU Research Centre, Sejong-1, Hancom to launch S. Korea's first private satellite for integrated image analysis service, 2022
69. S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, *Science* 362(6412), eaam9288 (2018)
70. A. P. Bhatt and A. Sharma, Quantum cryptography for internet of things security, *J. Electron. Sci. Technol.* 17(3), 213 (2019)
71. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, *IEEE Internet Things J.* 4(5), 1125 (2017)