Received: 29 July 2024 | Revised: 9 September 2024 | Accepted: 6 October 2024

IET Quantum Communication

DOI: 10.1049/qtc2.12116

ORIGINAL RESEARCH

Advancing quantum communication security: Metamaterial based quantum key distribution with enhanced protocols

Sujit Biswas[1] | Rajat S. Goswami[1] | K. Hemant Kumar Reddy[2] | Sachi Nandan Mohanty[2] | Mohammed Altaf Ahmed[3]

[1]Department of Computer Science and Engineering, National Institute of Technology Arunachal Pradesh, Jote, Arunachal Pradesh, India

[2]Department of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh, India

[3]Department of Computer Engineering, College of Computer Engineering Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia

Correspondence
Rajat S. Goswami.
Email: rajat@nitap.ac.in

Abstract

Quantum Key Distribution (QKD) is increasingly pivotal in securing communication channels against the looming threats posed by quantum computing. However, existing QKD protocols encounter challenges related to efficiency and transmission capabilities. In response, this research investigates the integration of metamaterials into QKD systems, aiming to fortify security and enhance practicality. In the current landscape of quantum communication, where the vulnerability of classical encryption methods is magnified by rapid advancements in quantum computing, finding innovative solutions is imperative. This study is motivated by the need to strengthen the security and viability of QKD protocols to meet the demands of evolving cryptographic threats. By integrating metamaterials, the authors optimise quantum state control, improve signal-to-noise ratio (SNR), and enable longer transmission distances. Through mathematical modelling and simulations, the authors demonstrate how metamaterials reduce errors and enhance the robustness of QKD systems. Our findings show significant improvements in transmission efficiency and security, making Metamaterial-Based Quantum Key Distribution (MQKD) a promising approach for future quantum communication networks. The study not only advances the understanding of the theoretical foundations, but also presents simulated results illustrating the practical effectiveness of MQKD. The exploration of these innovative techniques contributes to the ongoing efforts to secure quantum communication channels.

KEYWORDS

quantum communication, quantum computing, quantum computing techniques

1 | INTRODUCTION

The development of quantum computing opened a new era in information processing by using the principles of quantum physics. Quantum computers, unlike conventional computers, use qubits instead of bits as the fundamental unit of information. Qubits can exist in a superposition of states, allowing quantum computers to do intricate computations at a much-accelerated pace compared to classical computers. Additionally, quantum entanglement allows qubits to be correlated in ways that classical bits cannot, facilitating novel approaches to solving problems Preskill [1]. One of the most prominent algorithms in quantum computing is Shor's algorithm, introduced by Peter Shor in 1994 Shor [2]. This algorithm has the potential to efficiently factorise large numbers, a task considered extremely difficult for classical computers and a cornerstone of modern encryption techniques. This has raised both excitement and concerns in the field of cryptography, as it could potentially render current encryption methods obsolete. Furthermore, quantum computing holds promise in various fields Purohit et al. [3], such as optimisation, drug discovery, and materials science. For instance, the quantum approximate

Rajat S. Goswami, K. Hemant Kumar Reddy and Sachi Nandan Mohanty have contributed equally to this work.

optimisation algorithm aims to solve complex optimisation problems more efficiently than classical algorithms. This has implications for logistical challenges Akleylek et al. [4], from supply chain management to financial modelling. Nonetheless, building and maintaining stable quantum computers is a formidable challenge due to issues such as decoherence, where qubits lose their quantum properties due to environmental interactions. Quantum error correction techniques are being developed to address these challenges, but quantum computers with a substantial quantity of qubits that are operational and error-correction capabilities are still in the experimental stage Arute et al. [5]. Multiple sectors may be profoundly transformed by quantum computing's ability to resolve issues that are virtually impossible for traditional computers.

The growing demand for secure communication has led to the exploration of quantum technologies, with Quantum Key Distribution (QKD) emerging as a promising solution to address the challenges posed by classical cryptographic methods Szikora and Lazányi [6]. Despite its inherent security, QKD protocols face limitations in terms of efficiency and transmission performance Kong [7]. This research is motivated by the pursuit of improving the security and practicality of QKD through the integration of metamaterials, engineered materials designed to manipulate electromagnetic waves at the sub-wavelength scale Oudich and Li [8]. Metamaterial-based Quantum Key Distribution (MQKD) stands at the forefront of quantum technologies, representing a paradigm shift in secure communication protocols. Unlike classical cryptographic methods, by using the basic principles of quantum physics, MQKD provides an unbreakable exchange of key information between communicating participants. The integration of metamaterials into QKD offers several unique advantages:

1. **Enhanced Control Over Quantum States:** Metamaterials allow for precise manipulation of the polarisation, phase, and other properties of photons. This leads to higher fidelity of quantum states, making the key generation process more robust against environmental noise.
2. **Improved Error Correction and Reduced Noise:** The unique interaction between metamaterials and quantum states enables more refined error correction mechanisms, reducing error rates and enhancing the efficiency of the key generation process.
3. **Increased Transmission Efficiency:** Metamaterials can optimise the propagation of quantum signals, enabling secure communication over greater distances without significant signal degradation.
4. **Heightened Security Against Eavesdropping:** The altered quantum states resulting from metamaterial interactions are more complex and less predictable, providing an additional layer of security that complicates potential eavesdropping efforts.

Quantum computing, a revolutionary field harnessing quantum mechanics, has spurred the development of innovative protocols such as MQKD. In classical computing, information is processed using bits, while quantum computers operate with qubits capable of existing in superpositions of states. Moreover, quantum entanglement allows qubits to exhibit correlations beyond the limitations of classical bits, opening avenues for novel problem-solving approaches. By integrating metamaterials into QKD, this study aims to advance the security and practicality of quantum communication systems, pushing the boundaries of what is achievable with traditional quantum cryptographic methods.

1.1 | Quantum communication

A relatively new area of study, quantum communication makes use of the laws of quantum mechanics to facilitate the safe and effective transfer of data. Compared to more traditional forms of communication, in contrast to classical bits that are used to represent information, quantum communication utilises quantum bits, or qubits. These qubits can exist in different quantum states, including superpositions and entanglements, offering innovative methods for encoding and transmitting data securely [9]. A major application of quantum communication is QKD, which uses the properties of qubits to create a secure key between two parties. Notable protocols, such as BB84, exemplify this technique. The security of QKD is grounded in quantum mechanics, making it fundamentally impossible for an eavesdropper to intercept the communication without disturbing the qubits and alerting the parties involved [10]. Furthermore, quantum entanglement in quantum communication enables long-distance interactions. This phenomenon allows for immediate connections between qubits, no matter how far apart they are. Experiments such as quantum teleportation illustrate this effect, where the quantum state of one particle is instantaneously transmitted to another particle located far away, highlighting the non-local characteristics of quantum communication [11]. Quantum communication signifies a transformative approach to secure information exchange. By leveraging qubits and quantum features such as entanglement, it has the potential to transform cryptography and facilitate long-distance communication, offering unmatched levels of security and efficiency Liu et al. [12].

1.2 | Securing quantum communication

To take full advantage of the promise of quantum technologies for secure and private data sharing, quantum communication security is of the greatest significance. Quantum key distribution (QKD) can be seen as an outstanding example of a protocol designed to achieve this objective. Quantum Key Distribution (QKD) employs the fundamental laws of quantum physics to create a mutually agreed secret key between communicating entities. This key may then be used to encrypt and decrypt confidential data. The security of QKD is based on the underlying quantum properties of qubits, including the uncertainty principle and the no-cloning theorem. These properties guarantee that any attempts to eavesdrop on the communication would disturb the fragile quantum states, thereby notifying the authorised parties of a potential attacker [10]. Moreover, the use of quantum entanglement in the context of secure communication serves as an improvement to the existing cryptographic framework. Quantum entanglement, a phenomenon wherein qubits become correlated in a non-local manner, enables the creation of cryptographic primitives, such as QKD and quantum teleportation. These mechanisms, deeply rooted in the non-classical nature of entanglement, bolster the security of quantum communication protocols, rendering them resistant to classical eavesdropping strategies [13]. In conclusion, securing quantum communication is pivotal for realising the full potential of quantum technologies in maintaining privacy and security during data transmission. By leveraging the unique properties of qubits and quantum entanglement, protocols like QKD offer a revolutionary approach to encryption that safeguards against both current and future cryptographic threats.

In this manuscript, an enhanced version of the QKD protocol proposed with metamaterial-based Photon Generation, increased error correction, and privacy amplification on IBM Quantum Computer. To summarise, this study made the following contributions:

(i) Alice produces a series of photons, with each one being produced in a polarisation state that is randomly selected.
(ii) Bob conducts measurements on randomly selected bases (vertical/horizontal or diagonal/anti-diagonal) with predetermined probabilities on incoming photons.
(iii) A cascade code error coding mechanism was incorporated to reduce the error rate of the generated key. Syndrome Vector Comparison and Matrix Construction and Solution have been implemented to generate the error-free key.
(iv) Privacy amplification (Metamaterial hash function) technique employed to modify the generated key which leads to an increase in security. The proposed MQKD protocol reduced error rates, enabled faster key generation, and improved performance over longer distances.

The rest of the paper is organised as follows; Section 2 provides comprehensive details of Quantum Key generation and distribution. Section 3 provides the state-of-the-art attempts in the field of quantum computing security and its analysis. Section 3 presents the proposed protocol design specification and security analysis. The experiment's specifics and the analysis of its results are provided in Ssection 4. Ultimately, the suggested work is summarised in Section 5.

2 | BACKGROUND AND RELATED WORK

Applying the ideas of quantum physics to enable efficient and secure data transfer, quantum communication is at the cutting edge of groundbreaking developments in secure information sharing. It includes a variety of methods and tools that make use of quantum features such as superposition and entanglement to guarantee communication security and privacy at never-before-seen levels [9, 10]. Quantum key distribution (QKD), demonstrated as the well-known BB84 protocol, is an important idea in quantum communication. QKD exploits the quantum properties of qubits to establish a secret key between parties, rendering the key exchange fundamentally secure against eavesdropping attempts [9]. Quantum entanglement, a phenomenon where particles become intrinsically correlated, forms the basis for many of these protocols Stavdas et al. [14]. Quantum teleportation and quantum repeaters, which use entanglement to transfer qubits safely across great distances, have the potential to change worldwide communication [11, 15, 16] discussed a self-adjusting quantum key renewal management scheme for classical network symmetric cryptography. Practical implementations of quantum communication are challenged by the fragile nature of quantum states due to decoherence. Quantum error correction codes mitigate these issues, paving the way for fault-tolerant quantum communication systems [17]. The creation of quantum networks, which combine quantum communication with traditional infrastructure and enable hybrid communication systems with improved capabilities, has also been facilitated by recent advancements in quantum technology [18, 19]. The potential for quantum communication to transform safe information sharing is quite promising. Its foundations in quantum mechanics, as well as its potential uses in quantum networks, quantum teleportation, and QKD, promise to change the face of secure communication in an environment where connectivity is accelerating. A secure cryptographic key can be established between two parties through QKD, even when there is a potential eavesdropper present. The security of QKD relies on the principles of quantum physics, ensuring its robustness. Bennett and Brassard introduced a secure QKD framework in 1984 Bennett and Brassard [10], commonly referred to as the BB84 QKD system. Quantum communication has witnessed significant advancements in recent years, with a focus on enhancing security, efficiency, and practical implementation Biswas et al. [20, 21]. Notably, research has explored various protocols and technologies to address the challenges and opportunities in the field Chandrashekhar Meshram et al. [22]. Hatakeyama et al. [23] proposed a novel differential-phase-shift quantum-key-distribution (QKD) protocol, aiming to enhance the efficiency of QKD systems by minimising random delays and optimising timing parameters. The implementation of this effort significantly enhanced the overall efficacy of secure key development. Kravtsov et al. [24] introduced a novel concept in the field of safe communication by proposing a relativistic QKD system that employs one-way quantum communication. This study demonstrates creative strategies for ensuring secure communication within a relativistic framework. Bouchard et al. [25] conducted a study that showcased the use of twisted photons inside a round-robin differential-phase-shift QKD system. The integration of twisted photons in QKD systems enhanced their capabilities, resulting in improved resilience against prospective assaults. Wang et al. [26] conducted a study to expand the use of twisted photons in QKD. They introduced a unique method that incorporates a fibre interferometer to improve the resilience of secure communication systems. The field of continuous-variable QKD has seen significant progress via the research conducted by Usenko and Grosshans [27] and Li and Cvijetic [28]. They respectively explored unidimensional continuous-variable QKD and continuous-variable QKD with self-reference detection and discrete modulation, contributing to the expansion of continuous-variable quantum communication capabilities. Notably, recent work by Pavicic et al. [29] presented a mixed basis QKD protocol leveraging linear optics, introducing innovative techniques to enhance the efficiency of quantum communication systems based on continuous variables. Furthermore, measurement-device-independent (MDI) QKD received attention, addressing potential vulnerabilities arising from imperfect devices. Chen et al. [30] investigated MDI QKD with q-plates, while Hwang et al. [31] improved MDI-QKD with uncharacterised qubits. Reflecting contemporary concerns, Coles et al. [32] introduced a numerical approach for unstructured QKD, contributing insights into the practical implementation of secure communication protocols.

Recent advancements in quantum communication have been fuelled by innovative protocols, advanced techniques, and the resolution of practical challenges Rozenman et al. [33]. These developments have collectively propelled the evolution of secure and efficient quantum communication systems.

Despite the availability of various configurations for QKD systems, the BB84 protocol remains a prevalent choice, owing to its enduring utility amidst technological progress. In BB84, Alice, as the sender, chooses between two bases—Horizontal or Vertical—to transmit particles represented by $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, where $|+\rangle$ and $|-\rangle$ are defined as $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ respectively. Subsequently, Bob, the receiver, determines the particle's basis and measures it accordingly. However, the presence of Eve, a potential eavesdropper, introduces the risk of information theft. To ensure comprehensive security, any defects in the original key are presumed to stem from Eve's surveillance. Following post-processing, which involves error correction and privacy amplification, Alice and Bob can derive the secret key based on the error rate of the initial key. Notably, the BB84 protocol encounters interception in approximately one out of every four communications. Consequently, if the error rate of the initial key rises, it is inferred that Eve has compromised 50% of the key. Fuchs et al. Fuchs et al. [34] introduced the concept of optimal eavesdropping in quantum cryptography, providing insights into the information bound and optimal strategies for secure communication. In 2002, Macchiavello Bruss and Macchiavello [35] further explored optimal eavesdropping in quantum cryptography, specifically with six states. Macchiavello's work contributed to enhancing the understanding of security aspects in QKD systems. Scarani et al. Scarani et al. [36] conducted a comprehensive study on the security of practical QKD systems. Their work evaluated the effectiveness and vulnerabilities of various QKD protocols, providing valuable insights into designing secure communication channels based on quantum principles.

In addition to BB84, QKD has evolved to incorporate entangled states, as shown by the ping-pong technique that relies on Bell state measurements. This protocol, introduced by Bostrom and Felbinger in 2002 [37] and further refined in 2008 [38], alternates between message and control modes, enhancing security. The proposed protocol aligns with the fundamentals of the polarisation-based BB84 protocol, a prevalent technique for establishing secure cryptographic keys between parties over unreliable channels. Here, Alice transmits a series of photons with randomly assigned polarisation states to Bob via an unsecured channel. Subsequently, Bob selects a basis randomly for measuring the polarisation of each photon and communicates his selection to Alice. Both parties then perform measurements and compare results to generate a shared secret key.

The protocol incorporates error correction and privacy amplification methods to ensure the security of the shared key. Error correction involves carefully reviewing a section of the key to identify and correct problems, while privacy amplification compresses the key into a concise but strong random sequence, guaranteeing the safe delivery of messages. Although the suggested protocol is vulnerable to future threats such as intercept-resend and photon-number-splitting attacks, it offers a dependable method for generating cryptographic keys specifically designed for safe communication across unprotected channels.

Besides, recent advancements in the field, such as the study conducted by Yuan Cao et al. Cao et al. [39], have contributed to the ongoing progress in quantum communication and its applications.

3 | PROPOSED MODEL

Our suggested approach focuses on three fundamental components. Firstly, secret keys for communication are created using metamaterials. Furthermore, the subsequent step involves error correction, followed by the last step, Privacy Amplification. Therefore, this suggested approach can provide a more resistant key to unauthorised access. Figure 1 presents the step-wise procedure of the Metamaterial-based QKD protocol. This research investigates how metamaterials improve the security of QKD systems. The study employs mathematical modelling and numerical simulations to analyse how metamaterials enhance the control of quantum states, such as polarisation and phase, to reduce noise and errors. The research demonstrates that metamaterials optimise signal transmission and improve resistance to eavesdropping by increasing the complexity of quantum states, making unauthorised interception more detectable. These findings show how the integration of metamaterials fortifies the overall security of QKD systems. Before going to discuss this unique idea, first we demonstrate Metamaterials and their modifications. Then, we discuss QKD and how Metamaterials can affect the QKD protocol for our future communications.

3.1 | Metamaterials

Metamaterials, synthetic materials deliberately crafted to possess unconventional characteristics, are a product of engineering rather than natural occurrence. Engineered to manipulate electromagnetic waves, particularly light, in manners unattainable by conventional materials, they hold the ability to govern light propagation at scales smaller than the wavelength, resulting in distinctive optical behaviours.

Here, we will delve into the mathematical description of metamaterials and their interaction with electromagnetic waves using Maxwell's equations and provide a simplified presentation.

• **Permittivity and Permeability Tensors:** Metamaterials are often characterised by their permittivity (ϵ) and permeability (μ) tensors. These tensors describe how the material responds to electric and magnetic fields, respectively. In the case of anisotropic metamaterials, these tensors become matrices.

$$D = \varepsilon E \tag{1}$$

$$B = \mu H \tag{2}$$

Within the context of these equations, the symbols D represent the electric displacement field, the symbols E stand for the electric field, the signs B stand for the magnetic induction field, and the signs H stand for the magnetic field.

• **Maxwell's Equations with Metamaterials:**
Electricity and Gauss's Law:

$$\nabla \cdot \mathbf{D} = \rho \tag{3}$$

The Law of Gauss for Magnetism:

$$\nabla \cdot \mathbf{B} = 0 \tag{4}$$

The Principle of Faraday's Induction:

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \tag{5}$$

Maxwell's Addition to Ampere's Law:

$$\nabla \times \mathbf{H} = \mathbf{J} + \frac{\partial \mathbf{D}}{\partial t} \tag{6}$$

In these equations, ρ refers to the charge density, **J** corresponds to the current density, **D** signifies the electric displacement field, **B** symbolises the magnetic induction field, **E** represents the electric field, and **H** symbolises the magnetic field. These equations have been adapted to incorporate the effects of metamaterials on electromagnetic fields.

• **Modifications with Metamaterials:** To incorporate metamaterial properties, we should replace the standard permittivity and permeability with the tensors/matrices representing the anisotropic properties of the metamaterial.

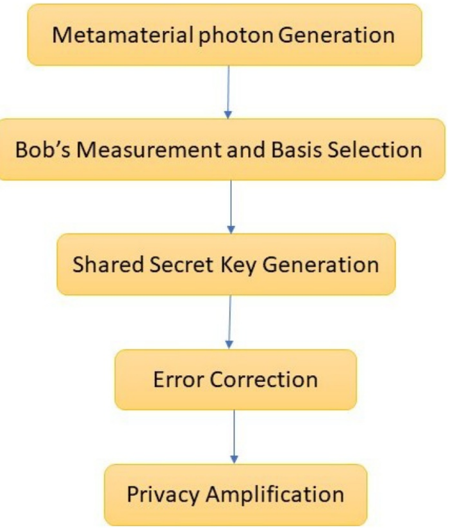

Metamaterial photon Generation
Bob's Measurement and Basis Selection
Shared Secret Key Generation
Error Correction
Privacy Amplification

FIGURE 1 Proposed MQKD model. MQKD, metamaterial-based quantum key distribution.

For example, if ϵ and μ were 3 × 3 matrices for anisotropic metamaterials:

$$D = \varepsilon \cdot E \tag{7}$$

where:

$$\varepsilon = \begin{bmatrix} \varepsilon_{xx} & \varepsilon_{yx} & \varepsilon_{zx} \\ \varepsilon_{xy} & \varepsilon_{yy} & \varepsilon_{zy} \\ \varepsilon_{xz} & \varepsilon_{yz} & \varepsilon_{zz} \end{bmatrix}$$

3.2 | Quantum states and density matrix

Now, we go through the mathematical framework for describing quantum states using the density matrix formalism and then introduce the basic mathematical foundations of QKD, these concepts include quantum superposition, entanglement, and quantisation.

• **Quantum States:** Quantum systems are described by state vectors, denoted as $|\psi\rangle$, which reside in a mathematical space known as Hilbert space. These state vectors evolve according to the Schrödinger equation, a fundamental equation in quantum mechanics:

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle \tag{8}$$

Here, $\hat{H}$ represents the Hamiltonian operator, and $\hbar$ denotes the reduced Planck constant. This equation captures the time evolution of quantum states under the influence of the system's Hamiltonian operator Griffiths and Schroeter [40].

• **Density Matrix Formalism:** The density matrix (ρ) provides a broader description, particularly valuable for characterising mixed states. For a pure state $|\psi\rangle$, the density matrix can be expressed as follows:

$$\rho = |\psi\rangle\langle\psi| \tag{9}$$

For a mixed state consisting of a statistical ensemble of pure states $|\psi_i\rangle$ with corresponding probabilities p_i, the density matrix takes the form:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{10}$$

These concepts are elucidated in detail by Nielsen and Chuang in their renowned textbook Nielsen and Chuang [41].

3.3 | Quantum key distribution (QKD)

- **Principles of Quantum Superposition:** Quantum superposition allows a quantum system to exist in multiple states simultaneously. Mathematically, if $|\psi_1\rangle$ and $|\psi_2\rangle$ are valid states, their superposition is given by the following:

$$|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle \tag{11}$$

Here, α and β represent complex probability amplitudes, subject to the normalisation condition $|\alpha|^2 + |\beta|^2 = 1$.

- **Entanglement:** When several quantum systems' states are sufficiently entangled so that determining the state of one system requires knowledge of the states of the others, this phenomenon is called entanglement. A possible mathematical representation of an entangled state with two particles is as follows:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \tag{12}$$

where, $|0\rangle$ and $|1\rangle$ are basis states.

- **Measurement in Quantum Key Distribution (QKD):** In QKD, quantum information is commonly encoded in photon properties such as polarisation. Polarisers or similar devices are employed for measurements, with outcomes being probabilistic. Notably, the act of measurement disrupts the quantum system's state. The probability of observing a specific outcome m given a quantum state $|\psi\rangle$ is defined as follows:

$$P(m) = \langle\psi|\hat{M}_m^{\dagger}\hat{M}_m|\psi\rangle \tag{13}$$

Here, $\hat{M}_m$ represents the measurement operator associated with outcome m.

These fundamental principles underlie QKD protocols, leveraging the unique properties of quantum mechanics and the impossibility of perfectly copying an unknown quantum state (no-cloning theorem). Protocols such as BB84 and E91 exploit these principles to ensure secure key distribution.

3.4 | Integration of metamaterials into QKD

Integrating metamaterials into QKD involves describing how these artificial materials interact with the quantum states of light used in the QKD process. The MQKD protocol merges the principles of quantum physics, such as superposition and entanglement, with the advanced properties of metamaterials to enhance secure communication. Metamaterials allow precise control over photon quantum states, improving signal-to-noise ratio (SNR) and extending transmission distances. By manipulating polarisation and phase more effectively, metamaterials reduce errors and noise in photon transmission. This integration adds a complex layer of security, making it difficult for eavesdroppers to intercept or alter quantum keys without detection, thus reinforcing the protocol's robustness. The specifics can depend on the design and properties of the metamaterial, but let us outline a general approach:

- **Modified Maxwell's Equations:** As we already discussed earlier, metamaterials modify how electromagnetic waves propagate. These modifications are encapsulated in the permittivity (ε) and permeability (μ) tensors of the metamaterial. In the context of QKD, where quantum states are encoded in the polarisation or other properties of light, these tensors influence the quantum states of light.

For simplicity, let us consider the effect on polarisation states. The interaction between a metamaterial and the quantum state $|\psi\rangle$ can be represented as follows:

$$\hat{U}_{meta}|\psi\rangle \tag{14}$$

Here, $\hat{U}_{meta}$ is the unitary operator representing the interaction with the metamaterial.

- **Signal-to-Noise Ratio (SNR):** The interaction of the quantum states with the metamaterial can influence the SNR. The SNR (SNR) is often related to the fidelity of the quantum states, which can be influenced by the metamaterial's impact. The fidelity (F) can be expressed as follows:

$$F = |\langle\psi_{out}|\psi_{in}\rangle|^2 \tag{15}$$

where, $|\psi_{in}\rangle$ is the input quantum state and $|\psi_{out}\rangle$ is the state after interaction with the metamaterial.

- **Transmission Efficiency:** Transmission efficiency can be influenced by the metamaterial's impact on the quantum states. If $|\psi_{in}\rangle$ is the input state, and $|\psi_{out}\rangle$ is the state after interaction with the metamaterial, the transmission efficiency (η) can be expressed as follows:

$$\eta = \frac{\langle\psi_{out}|\text{Transmission Operator}|\psi_{in}\rangle}{\langle\psi_{in}|\psi_{in}\rangle} \tag{16}$$

- **Manipulation of Quantum States:** Metamaterials can be designed to manipulate the quantum states intentionally. This manipulation can be represented by a unitary operator $\hat{U}_{control}$:

$$\hat{U}_{control}|\psi\rangle \tag{17}$$

3.5 | Proposed algorithm

We divided and discussed our algorithm into three main parts. Firstly Key Generation, secondly Error Correction, and lastly Privacy Amplification.

3.5.1 | Algorithm 01: Metamaterial-enhanced quantum key distribution

Step 1: Metamaterial-based Photon Generation:

- Alice generates N photons with randomly chosen polarisation states, leveraging metamaterial-infused structures.
- The photons are prepared in a state $|\psi\rangle$, where A_1, B_1, C_1, and D_1 are complex amplitudes satisfying Maxwell's Equation for magnetic induction (Equation 2).
- Alice uses an unsecured path to send Bob these photons that have been enhanced by metamaterials.

Step 2: Bob's Measurement and Basis Selection:

- Bob selects a random basis to measure each photon's polarisation, with options including the vertical/horizontal basis with probability p, and the diagonal/anti-diagonal basis with probability $1 - p$.
- Bob conducts measurements on each photon using the chosen basis, resulting in an outcome $|\phi\rangle$ with amplitudes A_2, B_2, C_2 and D_2 satisfying Faraday's Law of Induction $\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$ (Equation 5).
- Bob communicates the basis choice to Alice.

Step 3: Shared Secret Key Generation:

- A few of the bases used for photon measurements are publicly reviewed by Alice and Bob, excluding measurements conducted with different bases.
- Matching basis measurement pairs are utilised to establish a shared secret key.
- After Alice and Bob use the measured polarisation state to assign bit values (0 or 1) to each qubit, they send this sequence of bits across a secure channel.

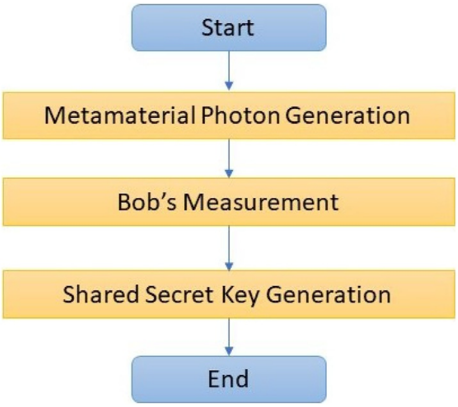


FIGURE 2 Flowchart for metamaterial-enhanced QKD. QKD, quantum key distribution.

The Metamaterial-enhanced QKD (MQKD) process involves several crucial steps to ensure secure communication. The overall procedure is visually summarised in Figure 2, which presents a flowchart outlining the stages from metamaterial photon generation to the generation of a shared secret key. Algorithm 1 provides a detailed, step-by-step description of the MQKD process. It begins with the procedure for generating photons with metamaterial-enhanced properties, followed by Bob's measurement strategy using randomly chosen bases. The final step involves generating the shared secret key based on the matching measurement pairs. By referring to both Figure 1 and Algorithm 1, readers can gain a comprehensive understanding of the MQKD protocol's workflow and the specific operations performed at each stage.

Algorithm 1. Metamaterial-enhanced Quantum Key Distribution (MQKD)

```
procedure MetamaterialPhotonGeneration $N$
    for $i = 1$ to $N$ do
        Alice generates $N$ photons with randomly chosen polarisation states leveraging metamaterial-infused structures.
        The photons are prepared in a state $|\psi\rangle$ with complex amplitudes $A_1$, $B_1$, $C_1$, and $D_1$ satisfying Maxwell's Equation for magnetic induction ($\mathbf{B} = \mu\mathbf{H}$).
        Alice transmits these metamaterial-enhanced photons to Bob over an insecure channel.
    end for
end procedure
procedure BobMeasurement $p$
    for each received photon do
        Bob randomly chooses a basis: whatever one chooses, the probabilities are $p$ for the vertical/horizontal basis and $1 - p$ for the diagonal/anti-diagonal basis.
        With his selected basis, Bob evaluates each photon, resulting in an outcome represented by $|\phi\rangle$ with amplitudes
```

```
            $A_2$, $B_2$, $C_2$, and $D_2$ satisfying Faraday's Law of Induction $\left(\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}\right)$.
            Bob communicates the basis choice to Alice.
    end for
end procedure
procedure SharedSecretKeyGeneration
    for each matching basis measurement pair do
        if measured polarisation matches then
                Assign bit value 0
        else
                Assign bit value 1
        end if
        Store bit in the shared secret key.
    end for
end procedure
```

3.5.2 | Algorithm 02: Error correction for MQKD metamaterial-enhanced quantum key distribution

Step 1: Error Comparison:

- In order to detect irregularities in the bits, Alice and Bob publicly scrutinise certain parts of the shared key.
- M bits are compared, and K of them are found to be different.

Step 2: Cascade Code Error Correction:

- The shared key is divided into blocks of size n.
- For the primary objective of error correction, a parity check matrix H is used, which has parameters $(n-K) \times n$ and produces several linearly independent rows.
- The Cascade code is used to repair the previously identified incorrect blocks.

Step 3: Syndrome Vector Comparison:

- The syndrome vectors for the error-corrected blocks are compared over a secure channel.
- L blocks with different syndrome vectors are identified.

Step 4: Matrix Construction and Solution:

- Alice and Bob construct matrices S and T using the linearly independent rows of H and the corresponding rows of the key, respectively.
- They solve the equation $HS = T$ for the matrix S, resulting in an $L \times n$ matrix E that represents error patterns.

Step 5: Error Correction Iteration:

- Errors in the key are corrected by flipping corresponding bits based on the error patterns in matrix E.
- The process is repeated until all errors are corrected, yielding a secure and error-free key.

Error correction is a vital component of the Metamaterial-enhanced QKD (MQKD) protocol, ensuring the reliability and security of the shared key. The detailed steps of the error correction process are outlined in Algorithm 2. This algorithm starts with the public comparison of a portion of the shared key between Alice and Bob to identify discrepancies. It then proceeds with the Cascade Code Error Correction, where the key is divided into blocks, and a parity check matrix is employed to correct errors in the identified blocks. The process continues with the comparison of syndrome vectors, the construction and solution of matrices to identify error patterns, and iterative correction until all errors are rectified, resulting in a secure and error-free key. Figure 3 complements this detailed description by providing a flowchart that visually represents the error correction process in MQKD. By following the flowchart, one can easily understand the sequence of operations, from error comparison to the final iteration of error correction. This combination of detailed algorithmic steps and visual representation ensures a comprehensive understanding of the error correction mechanism in MQKD.

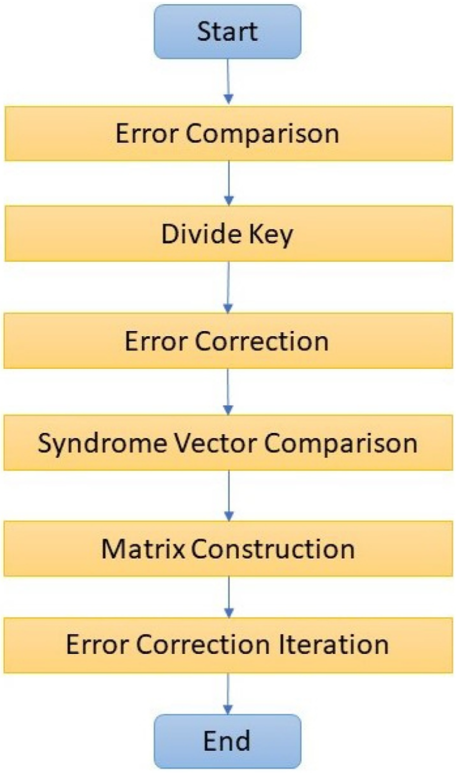


FIGURE 3 Flowchart for error correction in MQKD. MQKD, metamaterial-based quantum key distribution.

Algorithm 2. Error correction for MQKD

```
procedure ErrorCorrection
    Error Comparison:
        Alice and Bob publicly compare a portion of their shared key to identify any discrepancies in the bits.
        $M$ bits are compared, and $K$ of them are found to be different.
    Cascade Code Error Correction:
        The shared key is divided into blocks of size $n$.
        A parity check matrix $\mathbf{H}$ with $(n-K) \times n$ dimensions, consisting of rows that are linearly independent, is employed for error correction.
        Error correction is performed on the identified erroneous blocks using the Cascade code.
    Syndrome Vector Comparison:
        The syndrome vectors for the error-corrected blocks are compared over a secure channel.
        $L$ blocks with different syndrome vectors are identified.
    Matrix Construction and Solution:
        Alice and Bob construct matrices $\mathbf{S}$ and $\mathbf{T}$ using the linearly independent rows of $\mathbf{H}$ and the corresponding rows of the key, respectively.
        They solve the equation $\mathbf{HS} = \mathbf{T}$ for the matrix $\mathbf{S}$, resulting in an $L \times n$ matrix $\mathbf{E}$ that represents error patterns.
    Error Correction Iteration:
        Errors in the key are corrected by flipping corresponding bits based on the error patterns in matrix $\mathbf{E}$.
        The process is repeated until all errors are corrected, yielding a secure and error-free key.
end procedure
```

3.5.3 | Algorithm 03: Privacy amplification for MQKD

Step 1: Metamaterial-based Hash Function:

- Alice and Bob jointly decide on a randomly generated Toeplitz matrix H with dimensions $N \times M$, integrating principles from metamaterials.
- The multiplication of matrices $K \times H$ is executed to derive the hashed key K'.

Step 2: Error Detection and Correction:

- A subset of K' is publicly compared to detect errors.
- If errors are identified, the error correction algorithm is employed to rectify them.

Step 3: Iterative Refinement:

- Steps 1 and 2 are repeated until the error rate is sufficiently low, ensuring a reliable and secure hashed key K'.

Step 4: Final Hashed Key:

- The resulting K' serves as the output of the privacy amplification step, providing a shortened, random, and secure key for subsequent communication.

Privacy amplification is a crucial step in the Metamaterial-enhanced QKD (MQKD) protocol, designed to distill a secure key from the partially secure shared key. The detailed procedure for privacy amplification is outlined in Algorithm 3. This algorithm begins with the joint decision by Alice and Bob on a random Toeplitz matrix, $\mathbf{H}$, with dimensions $N \times M$, integrating principles from metamaterials. They then perform matrix multiplication to compute the hashed key, $\mathbf{K}'$. Subsequent steps involve error detection and correction, where a subset of $\mathbf{K}'$ is publicly compared to identify and rectify errors. The process includes iterative refinement, repeating the steps until the error rate is sufficiently low, and ensuring a reliable and secure hashed key. The final step produces $\mathbf{K}'$ as the output, serving as the shortened, random, and secure key for subsequent communication. Figure 4 complements this detailed description by providing a flowchart that visually represents the privacy amplification process. This flowchart illustrates the sequence of operations from the initial matrix selection and multiplication to error correction and iterative refinement, culminating in the generation of the final hashed key. By referring to both Algorithm 3 and Figure 4, readers can gain a comprehensive understanding of the privacy amplification mechanism in MQKD.

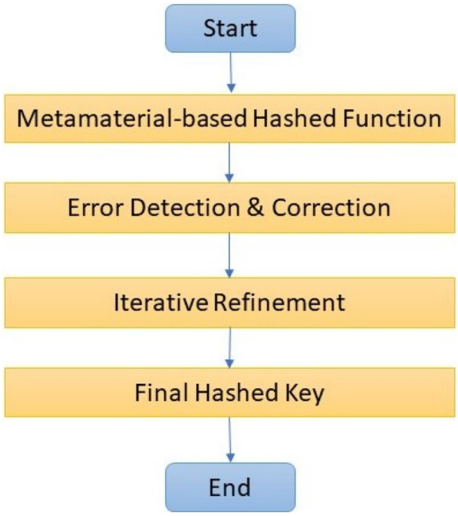

Start
Metamaterial-based Hashed Function
Error Detection & Correction
Iterative Refinement
Final Hashed Key
End

FIGURE 4 Flowchart for privacy amplification.

Algorithm 3. Privacy Amplification for MQKD

```
1: procedure MetamaterialHashFunction $N, M$
2:     Alice and Bob jointly decide on a random Toeplitz matrix $\mathbf{H}$ with dimensions $N \times M$, integrating principles from metamaterials.
3:     Matrix multiplication $\mathbf{K}' = \mathbf{K} \times \mathbf{H}$ is carried out to compute the hashed key $\mathbf{K}'$.
4: end procedure
5: procedure ErrorDetectionAndCorrection
6:     A subset of $\mathbf{K}'$ is publicly compared to detect errors.
7:     If errors are identified, the error correction algorithm is employed to rectify them.
8: end procedure
9: procedure IterativeRefinement
10:     Steps 1 and 2 are repeated until the error rate is sufficiently low, ensuring a reliable and secure hashed key $\mathbf{K}'$.
11: end procedure
12: procedure FinalHashedKey
13:     The resulting $\mathbf{K}'$ serves as the output of the privacy amplification step, providing a shortened, random, and secure key for subsequent communication.
14: end procedure
```

Here, we outline the traditional components of QKD and compare them with the proposed Metamaterial-based QKD (MQKD) protocol. The integration of metamaterials into QKD introduces significant enhancements across various aspects, including photon generation, quantum state control, transmission efficiency, error correction, and privacy amplification. These enhancements are critical in addressing the limitations of traditional QKD, such as vulnerability to noise, limited transmission distances, and susceptibility to advanced eavesdropping techniques. Table 1 provides a comprehensive comparison between traditional QKD and MQKD, highlighting how each component is improved by the incorporation of metamaterials. This comparison underscores the transformative potential of MQKD in achieving more secure, efficient, and robust quantum communication.

3.6 | Security analysis and challenges of the MQKD protocol

The following table provides an overview of the security features of the Metamaterial-based QKD (MQKD) protocol,

TABLE 1 Comparison of traditional QKD and metamaterial-based QKD (MQKD).

Component	Traditional QKD	Metamaterial-based QKD (MQKD)
Photon generation	Standard photon generation techniques using typical quantum optics devices.	Photon generation enhanced by metamaterials, providing precise control over polarisation, phase, and propagation direction. This results in higher fidelity and robustness against environmental noise.
Quantum state control	Limited control over quantum states, primarily using conventional optical elements.	Enhanced quantum state control through metamaterials, allowing for tailored manipulation of quantum properties like polarisation and phase.
Transmission efficiency	Transmission is often limited by distance and environmental factors, leading to signal degradation	Metamaterials optimise signal propagation, increasing transmission efficiency and enabling secure communication over longer distances.
Error correction	Classical error correction methods, such as cascade codes, that do not account for material-specific quantum state alterations.	Error correction tailored to the unique quantum state alterations induced by metamaterials, resulting in lower error rates and a more reliable key generation process.
Noise reduction	Relies on standard techniques to mitigate noise, often less effective in highly noisy environments.	Metamaterials inherently reduce noise by controlling the interaction of photons with the environment, improving signal-to-noise ratio (SNR).
Privacy amplification	Classical hash functions are used to compress and secure the key.	Metamaterial-based hash function that leverages quantum state modifications, adding complexity and enhancing security against eavesdropping.
Resistance to eavesdropping	Security is strong but relies on the basic principles of quantum mechanics and standard optical devices.	Enhanced resistance to eavesdropping due to the complex and less predictable quantum states created by metamaterial interactions, making it harder for an adversary to intercept and measure the key without detection.
Customisation and adaptability	Limited by the properties of naturally occurring materials and conventional optical elements.	High level of customisation and adaptability through the design of specific metamaterials, allowing for tailored QKD systems based on the communication channel or environment.

comparing its resistance to various potential attacks with that of traditional QKD. The integration of metamaterials introduces significant improvements in the protocol's ability to withstand these attacks.

- **Impact of Metamaterials on Quantum States**
  Metamaterials are engineered to manipulate electromagnetic waves at sub-wavelength scales, which allows for precise control over the properties of photons, such as polarisation and phase. This control is critical in QKD, where the security of the protocol relies on the quantum states of the photons.
  The quantum state of a photon can be represented by a state vector $|\psi\rangle$ in a Hilbert space. In the MQKD protocol, the interaction between a photon and a metamaterial can be modelled by a unitary operator U_{meta} that describes the transformation of the photon's quantum state:

$$|\psi_{out}\rangle = U_{meta}|\psi_{in}\rangle$$

Where:

- $|\psi_{in}\rangle$ is the initial quantum state of the photon before interaction with the metamaterial.
- U_{meta} is the unitary operator representing the metamaterial's effect on the photon's quantum state.
- $|\psi_{out}\rangle$ is the quantum state after the photon has interacted with the metamaterial.
  The unitary operator U_{meta} is designed to enhance certain properties of the quantum state, such as its robustness against noise and external perturbations. This transformation can reduce the likelihood of errors during transmission and increase the difficulty for an eavesdropper to gain useful information.

- **Increased Resistance to Eavesdropping**
  Eavesdropping attacks, such as the intercept-resend attack, rely on the ability to measure the quantum state of the photons without being detected. The security of QKD protocols is based on the principle that any measurement of a quantum state by an eavesdropper will disturb the state, introducing errors that can be detected by the legitimate parties.
  The fidelity F between the original quantum state $|\psi_{in}\rangle$ and the state after a potential eavesdropping attempt $|\psi_{eaves}\rangle$ can be used to quantify the security of the protocol:

$$F = |\langle\psi_{in}|\psi_{eaves}\rangle|^2$$

For a secure QKD protocol, the fidelity should be low when eavesdropping occurs, indicating a significant disturbance to the quantum state. The use of metamaterials increases the complexity of the quantum states, making it more difficult for an eavesdropper to perform measurements that closely match the original state. As a result, the fidelity F is reduced, making eavesdropping attempts more detectable.

- **Mitigating Man-in-the-Middle Attacks**
  In a man-in-the-middle (MITM) attack, an adversary intercepts and possibly alters the communication between two parties. The enhanced security provided by metamaterials can be modelled by examining the changes in the quantum state's density matrix ρ.
  The density matrix ρ represents the state of a quantum system, and any interaction with an adversary will typically alter this matrix. The metamaterial-enhanced quantum state can be described by a modified density matrix ρ_{meta}:

$$\rho_{meta} = U_{meta}\rho_{in}U_{meta}^{\dagger}$$

Where:

- ρ_{in} is the initial density matrix of the quantum state.
- $U_{meta}^{\dagger}$ is the conjugate transpose of the unitary operator representing the metamaterial's effect.
  This modified density matrix can be compared to the density matrix of the state after a potential MITM attack ρ_{MITM}:

$$\text{Trace}\left(\rho_{meta}\rho_{MITM}\right) < 1$$

This inequality indicates that the quantum state has been altered due to the MITM attack, which can be detected by the legitimate parties.

This Table 2 illustrates how the MQKD protocol enhances security across several dimensions, making it more resilient to common quantum and classical attacks compared to traditional QKD. By integrating metamaterials, the MQKD protocol not only maintains the fundamental security properties of QKD but also introduces additional layers of defence, thereby improving the overall robustness of the system.

While the integration of metamaterials into QKD offers significant benefits, it also introduces several technical and practical challenges. Table 3 summarises the key challenges and their potential impacts on the development and implementation of the Metamaterial-based QKD (MQKD) protocol.

The table above highlights the major challenges associated with integrating metamaterials into QKD. Addressing these challenges is essential to realising the full potential of the MQKD protocol and ensuring its successful implementation in practical quantum communication systems.

4 | RESULT DISCUSSION AND SIMULATION

Let N represent the quantity of photons generated by Alice. For each photon i, Alice generates a photon in a state $|\psi_i\rangle$ with complex amplitudes α_{iA}, α_{iB}, α_{iC}, and α_{iD} satisfying Maxwell's Equation $B = \mu H$.

TABLE 2 Security analysis of traditional QKD versus metamaterial-based QKD (MQKD).

Type of attack	Traditional QKD defence	MQKD enhanced defence
Eavesdropping (e.g., intercept-resend, photon number splitting)	Relies on detecting disturbances in quantum states due to measurement, leading to increased error rates.	Enhanced detection of eavesdropping due to metamaterial-induced quantum state alterations, which introduce additional complexities that make undetected interception difficult.
Man-in-the-middle attack	Security is primarily ensured through quantum state disturbance detection.	Increased robustness due to the complex and precise quantum states generated by metamaterials, making it harder for an attacker to replicate or alter without detection.
Cloning attack	Protected by the no-cloning theorem, which prevents exact copying of unknown quantum states.	Further resistance to cloning due to the unique quantum state modifications by metamaterials, making states even more complex and harder to duplicate without error.
Side-channel attack	Limited defences; relies on secure implementation to prevent leakage.	Additional protection through metamaterial modifications that reduce the susceptibility of quantum states to side-channel information leakage.
Privacy amplification vulnerability	Uses classical hash functions to remove partial information from the key.	Enhanced privacy amplification using metamaterial-based hash functions, which introduce further security by leveraging the modified quantum states, making it even harder for eavesdroppers to extract useful information.

TABLE 3 Challenges of integrating metamaterials into QKD and their impacts.

Challenge	Description	Impact
Fabrication and material quality	The precise fabrication of metamaterials is complex, and any imperfections can compromise the quantum states.	High-quality fabrication is essential for reliable MQKD performance, requiring advanced techniques and rigorous quality control.
Scalability	Scaling the use of metamaterials for widespread deployment poses challenges in maintaining precision and consistency.	Scalability is crucial for practical adoption, necessitating cost-effective manufacturing processes and scalable designs.
Integration with existing infrastructure	Compatibility with current quantum communication systems and protocols may require modifications to QKD hardware and software.	Seamless integration is necessary to avoid overhauls of existing systems, requiring interdisciplinary collaboration.
Environmental sensitivity	Metamaterials can be sensitive to environmental factors such as temperature and electromagnetic interference.	Robust metamaterials and protective measures are needed to ensure stability and reliability in varied conditions.
Complexity in theoretical modelling and simulation	Accurate modelling of interactions between metamaterials and quantum states is complex and resource-intensive.	Improved theoretical models and simulation tools are required for better design and optimisation of MQKD systems.
Cost considerations	The complexity of materials and fabrication processes may result in higher costs for MQKD systems.	Balancing enhanced security with cost-effectiveness is crucial for the commercial viability of MQKD.

Suppose Alice generates $N = 3$ photons, and the states are represented as follows:

$$
\begin{aligned}
|\psi_1\rangle &= \alpha_{1A} + \alpha_{1B} + \alpha_{1C} + \alpha_{1D} \\
|\psi_2\rangle &= \alpha_{2A} + \alpha_{2B} + \alpha_{2C} + \alpha_{2D} \\
|\psi_3\rangle &= \alpha_{3A} + \alpha_{3B} + \alpha_{3C} + \alpha_{3D}
\end{aligned}
$$

Let p be the probability of choosing the vertical or horizontal basis. For each received photon i, Bob randomly selects a basis: vertical or horizontal with probability p, diagonal or anti-diagonal with probability $1-p$. Bob measures each photon in the chosen basis, obtaining a result $|\phi_i\rangle$ with amplitudes β_{iA}, β_{iB}, β_{iC} and β_{iD} satisfying Faraday's Law of Induction. $\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$

Here, for each photon, Bob measures the polarisation in one of the two bases, and let us assume the measured states are:

$$
\begin{aligned}
|\phi_1\rangle &= \beta_{1A} + \beta_{1B} + \beta_{1C} + \beta_{1D} \\
|\phi_2\rangle &= \beta_{2A} + \beta_{2B} + \beta_{2C} + \beta_{2D} \\
|\phi_3\rangle &= \beta_{3A} + \beta_{3B} + \beta_{3C} + \beta_{3D}
\end{aligned}
$$

For each matching basis measurement pair i, if the measured polarisation matches, assign bit value 0; otherwise, assign bit value 1. Store the bit in the shared secret key (K). The shared secret key (K) will be generated based on the matching basis measurements. For example, if the measured polarisations match for the first and third photons but not for the second, the corresponding bits in the shared secret key would be 001.

Now, a subset of the shared key is publicly compared by Alice and Bob to identify differing bits. Suppose, $M = 4$ bits are compared, and $K = 2$ of them are found to be different. The shared key is divided into blocks of size $n = 2$. A parity check matrix H of size $(n - K) \times n$ is used for error correction. Error correction is performed on the identified erroneous blocks using the Cascade code. Let's say the corrected key is:

$$\text{SharedKey}_{\text{Corrected}} = [0, 1, 1, 1, 0, 0, 0, 1]$$

The syndrome vectors for the error-corrected blocks are compared over a secure channel. Suppose $L = 2$ blocks with different syndrome vectors are identified. Now, Alice and Bob construct matrices S and T using the linearly independent rows of H and the corresponding rows of the key, respectively. They solve the equation $HS = T$ for the matrix S, obtaining an $L \times n$ matrix E representing error patterns. Errors in the key are corrected by flipping corresponding bits based on the error patterns in matrix E. The process is repeated until all errors are corrected, yielding a secure and error-free key. Let us say the final error-corrected key is:

$$\text{SharedKey}_{\text{ErrorCorrected}} = [0, 1, 0, 1, 1, 0, 0, 1].$$

After that, Alice and Bob agree on a random Toeplitz matrix H of size $N \times M$. Matrix multiplication $K' = K \times H$ is performed to obtain the hashed key K'.

A subset of K' is publicly compared to detect errors. If errors are identified, the error correction algorithm is employed to rectify them. These Steps are repeated until the error rate is sufficiently low, ensuring a reliable and secure hashed key K'. The resulting K' serves as the output of the privacy amplification step, providing a shortened, random, and secure key for subsequent communication. Finally, we can say the final hashed key is:

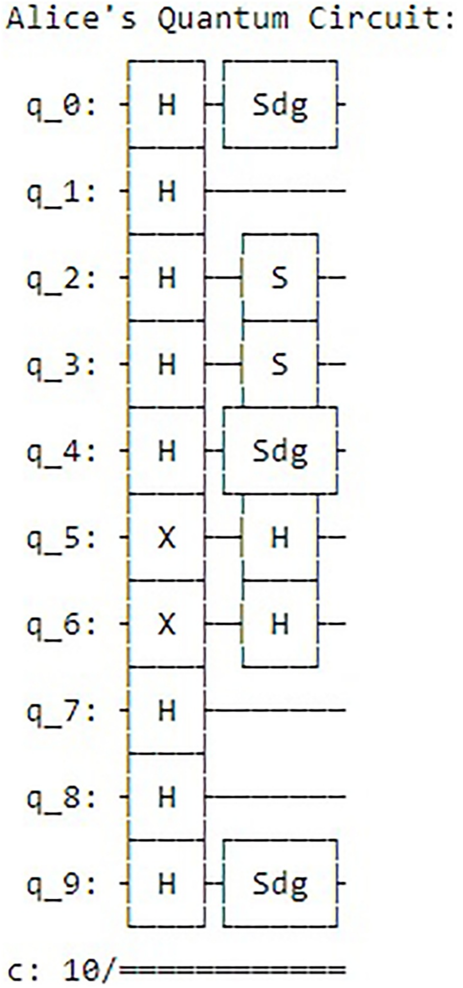
$\text{FinalHashedKey} = [1, 0, 1, 0, 1, 0, 1, 1]$

The final result is the FinalHashedKey, which is a secure and reliable key obtained after MQKD, error correction, and privacy amplification. This key can now be used for secure communication between Alice and Bob.

4.1 | Simulation

To validate the effectiveness of our proposed QKD (MQKD) protocol leveraging metamaterial-infused structures, we conducted simulations using Qiskit, an open-source quantum computing framework. The simulation of the first algorithm consists of three main procedures: Metamaterial Photon Generation, Bob's Measurement, and Shared Secret Key Generation.

- **Metamaterial Photon Generation:** In this step, Alice generates a sequence of photons, each prepared in a randomly chosen polarisation state. Qubits representing these photons are initialised based on the chosen polarisation states, leveraging metamaterial principles to simulate their behaviour according to Maxwell's Equation for magnetic induction $(B = \mu H)$. These metamaterial-enhanced photons are then transmitted to Bob over an insecure channel. This process is visually represented in Figure 5, which shows the quantum circuit used by Alice for preparing and transmitting the photons.
- **Bob's Measurement:** Upon receiving the photons, Bob performs measurements in randomly chosen bases (vertical/horizontal or diagonal/anti-diagonal) with specified probabilities. The measurement outcomes, denoted as $|\phi\rangle$, are obtained, and the chosen basis information is communicated back to Alice. Upon receiving the photons, Bob performs measurements in randomly chosen bases (vertical/horizontal or diagonal/anti-diagonal) with specified probabilities. The measurement outcomes, denoted as $|\phi\rangle$, are obtained, and the chosen basis information is communicated back to Alice. This process is visually represented in Figure 6, which shows the quantum circuit used by Bob for measuring the photons and determining their polarisation states.



```
Alice's Quantum Circuit:
     ┌───┐┌─────┐
q_0: ┤ H ├┤ Sdg ├
     ├───┤└─────┘
q_1: ┤ H ├───────
     ├───┤ ┌───┐
q_2: ┤ H ├─┤ S ├─
     ├───┤ ├───┤
q_3: ┤ H ├─┤ S ├─
     ├───┤┌┴───┴┐
q_4: ┤ H ├┤ Sdg ├
     ├───┤└┬───┬┘
q_5: ┤ X ├─┤ H ├─
     ├───┤ ├───┤
q_6: ┤ X ├─┤ H ├─
     ├───┤ └───┘
q_7: ┤ H ├───────
     ├───┤
q_8: ┤ H ├───────
     ├───┤┌─────┐
q_9: ┤ H ├┤ Sdg ├
     └───┘└─────┘
c: 10/═══════════
```

FIGURE 5 Quantum circuit for Alice.

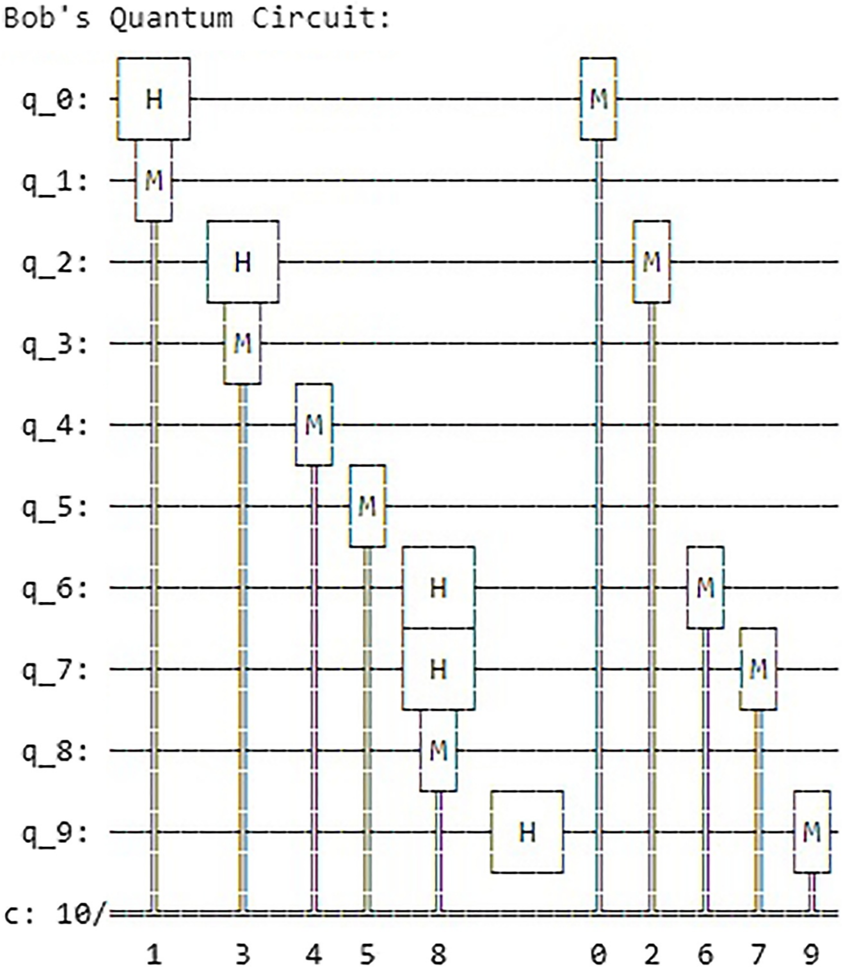
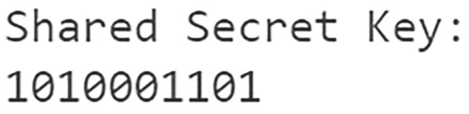


FIGURE 6 Quantum circuit for bob.

- **Shared Secret Key Generation:** Matching basis measurement pairs are used to generate a shared secret key. If the measured polarisation matches, a bit value of '0' is assigned; otherwise, '1' is assigned. The resulting bit sequence forms the shared secret key between Alice and Bob. Matching basis measurement pairs are used to generate a shared secret key. If the measured polarisation matches, a bit value of '0' is assigned; otherwise, '1' is assigned. The resulting bit sequence forms the shared secret key between Alice and Bob. This process is visually represented in Figure 7, which illustrates the formation of the shared secret key based on the matching basis measurements.

To evaluate the robustness of our QKD protocol, we implemented a simulated error correction algorithm using Qiskit. The error correction procedure involves several key steps, as described below:

- **Error Comparison:** A subset of the shared secret key, generated through the QKD protocol, is publicly compared by Alice and Bob to identify differing bits. This initial error analysis allows them to quantify the extent of errors present in the shared key.



```
Shared Secret Key:
1010001101
```

FIGURE 7 Shared secret key.

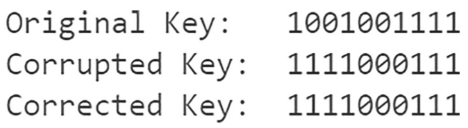
- **Cascade Code Error Correction:** The shared key is divided into blocks of size n, and a parity check matrix H is employed for error correction using the Cascade code. The matrix H, with linearly independent rows, facilitates the identification and correction of errors within the key.
- **Syndrome Vector Comparison:** The syndrome vectors for the error-corrected blocks are compared over a secure channel. This step enables the identification of blocks with different syndrome vectors, indicating potential errors.
- **Matrix Construction and Solution:** Matrices S and T are constructed using the linearly independent rows of H and the corresponding rows of the key, respectively. Solving the equation HS = T yields an L × n matrix E, representing error patterns within the key.
- **Error Correction Iteration:** Errors in the key are corrected by iteratively flipping corresponding bits based on the error patterns in matrix E. The process continues

until all errors are corrected, resulting in a secure and error-free key.

In quantum communication systems, error correction is crucial for maintaining the integrity of the secret key. The process involves identifying and correcting errors through iterative methods. Specifically, errors in the key are corrected by flipping the corresponding bits based on the error patterns identified in the matrix E. This iterative process continues until all errors are resolved, resulting in a secure and error-free key. Figure 8 illustrates the process of error correction applied to the secret key. This diagram shows how errors are systematically corrected to ensure that the final key is both secure and accurate. Additionally, Figure 9 provides a quantum representation of the error correction process. This visual representation highlights the quantum mechanisms involved in error correction, demonstrating the complexity and precision required to maintain key security in quantum systems.

The final hashed key generation procedure involves several key steps, as described below:

- **Metamaterial Hash Function:** Alice and Bob agree on a random Toeplitz matrix H, incorporating metamaterial principles. Matrix multiplication $K' = K \times H$ is performed to obtain the hashed key K'. This process ensures that the resulting hashed key reflects the metamaterial-infused characteristics, enhancing security.
- **Error Detection and Correction:** A subset of the hashed key K' is publicly compared to detect errors. If errors are identified, the error correction algorithm is employed to rectify them. This step contributes to the overall reliability and accuracy of the generated hashed key.
- **Iterative Refinement:** The process of agreeing on the Toeplitz matrix and matrix multiplication is repeated iteratively until the error rate is sufficiently low. This iterative refinement ensures the convergence of the system to a reliable and secure hashed key, contributing to the robustness of the privacy amplification step.
- **Final Hashed Key Generation:** The resulting corrected hashed key K' serves as the output of the privacy amplification step, providing a shortened, random, and secure key for subsequent communication. This final key is essential for ensuring the security and confidentiality of quantum communication channels.



```
Original Key:   1001001111
Corrupted Key:  1111000111
Corrected Key:  1111000111
```

FIGURE 8 Error correction on secret key.

Figure 10 illustrates the process of final hashed key generation. This diagram shows how the corrected key is hashed to produce the final secure key, which is essential for maintaining the security and confidentiality of quantum communication channels.

The circuit (Figure 11) illustrates the steps involved in initialising metamaterial-enhanced photons by Alice, followed by Bob's measurements in randomly selected bases. The protocol culminates in shared secret key generation, error simulation and correction, and privacy amplification through matrix hashing. Each component highlights the quantum mechanics

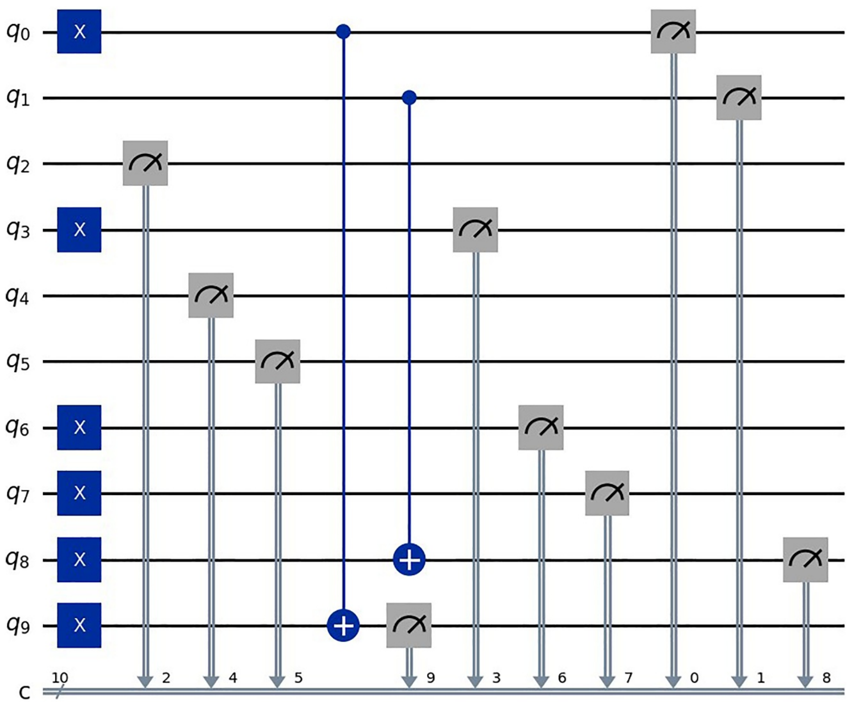


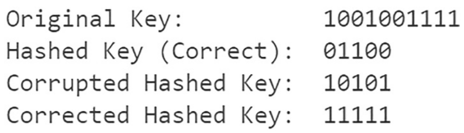
FIGURE 9 Quantum representation: Error correction.

principles that facilitate secure communication between Alice and Bob.

The simulation results presented in this section provide a detailed comparison of the performance between the traditional QKD protocol and the proposed Metamaterial-based QKD (MQKD) protocol. The simulations were conducted using the Qiskit quantum computing framework, focussing on key performance metrics such as transmission efficiency, error rates, noise reduction, and overall security.

The results clearly demonstrate the advantages of the MQKD protocol:

1. **Improved Transmission Efficiency:** The simulations show that the MQKD protocol significantly enhances transmission efficiency. By utilising metamaterials, the quantum states of photons are better preserved during transmission, reducing the impact of environmental factors and allowing for secure communication over longer distances compared to traditional QKD.
2. **Reduced Error Rates:** One of the most significant findings from the simulations is the reduction in error rates achieved by the MQKD protocol. The metamaterial-enhanced error correction mechanism proves to be more effective in detecting and correcting errors, which directly translates to a more reliable key generation process. This improvement is critical in maintaining the integrity of the quantum key, especially in noisy environments.
3. **Enhanced Noise Reduction:** The MQKD protocol's inherent noise reduction capabilities, attributed to the interaction of photons with metamaterials, were evident in the simulations. The results show a higher signal-to-noise ratio (SNR) in MQKD, which contributes to the robustness of the quantum communication channel and reduces the likelihood of key compromise due to noise interference.
4. **Increased Security Against Eavesdropping:** The simulations also highlight the enhanced security features of the MQKD protocol. The complexity and unpredictability of the quantum states altered by metamaterials make it significantly more challenging for potential eavesdroppers to intercept and measure the quantum key without detection. This increased resistance to eavesdropping is a crucial advantage of the MQKD protocol over traditional QKD.



```
Original Key:           1001001111
Hashed Key (Correct):   01100
Corrupted Hashed Key:   10101
Corrected Hashed Key:   11111
```

FIGURE 10 Final hashed key.

Overall, the simulation results validate the theoretical benefits of integrating metamaterials into the QKD framework. The MQKD protocol not only outperforms traditional QKD in terms of efficiency and reliability but also offers a higher level of security, making it a promising solution for future quantum communication systems. The proposed MQKD protocol not only advances the theoretical understanding of quantum communication, but also paves the way for practical, real-world applications. Its integration of metamaterials for enhanced quantum state control provides opportunities for developing next-generation quantum networks

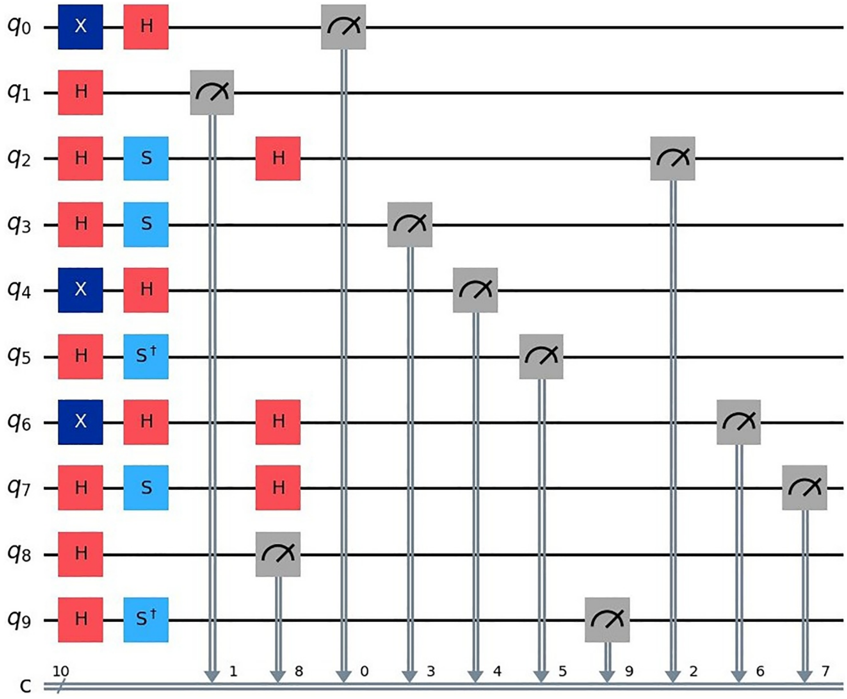


FIGURE 11 Quantum circuit representation of the MQKD protocol. MQKD, metamaterial-based quantum key distribution.

TABLE 4 Comparison of future research and real-time implementation potential.

Aspect	Future research scope	Real-time implementation
Material exploration	New types of metamaterials for better quantum state control	Adaptation of available metamaterials for secure communication
Quantum network expansion	Large-scale quantum network protocols and hybrid systems	Integration with current networks, extending communication distance
Error correction	Development of new metamaterial-based error correction models	Improved error rates and noise reduction in real-world systems
Scalability	Protocol adaptability to different quantum systems	Ease of deployment in commercial and governmental sectors
Security enhancements	Research into new attack-resistant quantum key mechanisms	Real-time resistance against eavesdropping and hacking attempts

with improved security and efficiency. The following Table 4 makes the study suitable for both future research and real-time implementation.

5 | CONCLUSION

This paper presents the MQKD protocol, which combines the concepts of quantum physics with metamaterial technology to provide secure communication. The protocol includes the creation, transfer, and modification of quantum states using metamaterial-based photon generation, measurement, error correction, and privacy amplification techniques. The framework of MQKD is the gpurposeson of photons by Alice, who employs intricate amplitudes that follow Maxwell's Equation to encode quantum information. Afterwards, Bob performs polarisation measurements on the incoming photons using random basis selection and measurement. This process allows him to construct a shared secret key by matching the basis measurements. The protocol utilises error correction via the implementation of the Cascade code and matrix operations, guaranteeing the dependability and confidentiality of the produced key. The recurrent enhancing and privacy amplification phases significantly improve the security of the shared key by identifying and rectifying mistakes, resulting in a compressed, randomised, and highly secure final hashed key. Metamaterials enhance the durability and effectiveness of the QKD process, demonstrating the promise of advanced materials in the realm of quantum communication.

The simulation results, performed using Qiskit, demonstrate the efficacy of the MQKD protocol in generating a safe and dependable shared key. Incorporating metamaterials into the QKD process not only propels the area of quantum communication forward but also creates opportunities to investigate the potential collaborations between quantum technologies and advanced materials.

In conclusion, this study presents a MQKD protocol that enhances the security and efficiency of traditional QKD systems. By leveraging metamaterials, the proposed protocol improves photon generation, reduces error rates, and extends transmission distances. Our simulations validate these enhancements, showing increased resistance to eavesdropping and noise interference. The results suggest that MQKD offers a viable solution for secure communication in real-world quantum networks, with potential for future research into advanced metamaterials and quantum systems. The MQKD protocol also represents a significant step forward in QKD, leveraging the unique properties of metamaterials to achieve heightened security and reliability. As quantum technologies continue to evolve, MQKD stands out as a promising approach for establishing secure communication channels in future quantum networks.

AUTHOR CONTRIBUTIONS

Sujit Biswas: Conceptualization; investigation; methodology; resources; software; writing—original draft. **Rajat S. Goswami**: Conceptualization; methodology; resources. **K. Hemant Kumar Reddy**: Conceptualization; methodology; writing—review and editing. **Sachi Nandan Mohanty**: Conceptualization; methodology; writing—review and editing. **Mohammed Altaf Ahmed**: Conceptualization; methodology; writing—review and editing.

ACKNOWLEDGEMENTS

The work is original and unpublished and has not been submitted for publication elsewhere. No Funding is available.

CONFLICT OF INTEREST STATEMENT

Not applicable. There is no competing interest with any financial or personal nature.

DATA AVAILABILITY STATEMENT

The dataset is available and provided on demand.

ORCID

Rajat S. Goswami https://orcid.org/0000-0002-1592-5765
K. Hemant Kumar Reddy https://orcid.org/0000-0003-2492-3312
Mohammed Altaf Ahmed https://orcid.org/0000-0003-0355-7835

REFERENCES

1. Preskill, J.: Quantum computing in the nisq era and beyond. Quantum 2, 79 (2018). https://doi.org/10.22331/q-2018-08-06-79
2. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. Ieee (1994)
3. Purohit, A., et al.: Building a quantum-ready ecosystem. IET Quan. Commun. 5(1), 1–18 (2024). https://doi.org/10.1049/qtc2.12072
4. Akleylek, S., et al.: An efficient lattice-based signature scheme with provably secure instantiation. In: Progress in Cryptology–

AFRICACRYPT 2016: 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings 8, pp. 44–60. Springer (2016)

5. Arute, F., et al.: Quantum supremacy using a programmable superconducting processor. Nature 574(7779), 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5
6. Szikora, P., Lazányi, K.: The end of encryption? the era of quantum computers. In: Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach, pp. 61–72. Springer (2022). https://doi.org/10.1007/978-94-024-2174-3_5
7. Kong, P.-Y.: A review of quantum key distribution protocols in the perspective of smart grid communication security. IEEE Syst. J. 16(1), 41–54 (2020). https://doi.org/10.1109/jsyst.2020.3024956
8. Oudich, M., Li, Y.: Tunable sub-wavelength acoustic energy harvesting with a metamaterial plate. J. Phys. Appl. Phys. 50(31), 315104 (2017). https://doi.org/10.1088/1361-6463/aa779d
9. Gisin, N., Thew, R.: Quantum communication. Nat. Photonics 1(3), 165–171 (2007). https://doi.org/10.1038/nphoton.2007.22
10. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. arXiv preprint arXiv:2003.06557 (2020)
11. Bouwmeester, D., et al.: Experimental quantum teleportation. Nature 390(6660), 575–579 (1997). https://doi.org/10.1038/37539
12. Liu, R., et al.: Towards the industrialisation of quantum key distribution in communication networks: a short survey. IET Quan. Commun. 3(3), 151–163 (2022). https://doi.org/10.1049/qtc2.12044
13. Ekert, A.K.: Quantum cryptography based on bell's theorem. Phys. Rev. Lett. 67(6), 661–663 (1991). https://doi.org/10.1103/physrevlett.67.661
14. Stavdas, A., et al.: Quantum key distribution for v2i communications with software-defined networking. IET Quan. Commun. 5(1), 38–45 (2024). https://doi.org/10.1049/qtc2.12070
15. Briegel, H.-J., et al.: Quantum repeaters: the role of imperfect local operations in quantum communication. Phys. Rev. Lett. 81(26), 5932–5935 (1998). https://doi.org/10.1103/physrevlett.81.5932
16. Han, J., et al.: A self-adjusting quantum key renewal management scheme in classical network symmetric cryptography. J. Supercomput. 76(6), 4212–4230 (2020). https://doi.org/10.1007/s11227-018-2276-y
17. Preskill, J.: Reliable quantum computers. Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci. 454(1969), 385–410 (1998). https://doi.org/10.1098/rspa.1998.0167
18. Kimble, H.J.: The quantum internet. Nature 453(7198), 1023–1030 (2008). https://doi.org/10.1038/nature07127
19. Wehner, S., Elkouss, D., Hanson, R.: Quantum internet: a vision for the road ahead. Science 362(6412), 9288 (2018). https://doi.org/10.1126/science.aam9288
20. Biswas, S., Goswami, R.S., Reddy, K.H.K.: Advancing Quantum Steganography: A Secure Iot Communication with Reversible Decoding and Customized Encryption Technique for Smart Cities, vol. 1–20. Cluster Computing (2024)
21. Biswas, S., et al.: Exploring the fusion of lattice-based quantum key distribution for secure internet of things communications. IET Quan. Commun. (2024). https://doi.org/10.1049/qtc2.12105
22. Meshram, C., et al.: An efficient certificateless group signcryption scheme using quantum Chebyshev chaotic maps in hc-iot environments. J. Supercomput. 79(15), 1–26 (2023). https://doi.org/10.1007/s11227-023-05303-2
23. Hatakeyama, Y., et al.: Differential-phase-shift quantum-key-distribution protocol with a small number of random delays. Phys. Rev. a 95(4), 042301 (2017). https://doi.org/10.1103/physreva.95.042301
24. Kravtsov, K., et al.: Relativistic quantum key distribution system with one-way quantum communication. Sci. Rep. 8(1), 6102 (2018). https://doi.org/10.1038/s41598-018-24533-6
25. Bouchard, F., et al.: Round-robin differential-phase-shift quantum key distribution with twisted photons. Phys. Rev. 98(1), 010301 (2018). https://doi.org/10.1103/physreva.98.010301
26. Wang, S., et al.: The a satellite-to-ground quantum key distribution protocol based on orbital angular momentum of light. In: Journal of Physics: Conference Series, vol. 1757(1), p. 012173 (2021). https://doi.org/10.1088/1742-6596/1757/1/012173. IOP Publishing
27. Usenko, V.C., Grosshans, F.: Unidimensional continuous-variable quantum key distribution. Phys. Rev. 92(6), 062337 (2015). https://doi.org/10.1103/physreva.92.062337
28. Li, M., Cvijetic, M.: Continuous-variable quantum key distribution with self-reference detection and discrete modulation. IEEE J. Quant. Electron. 54(5), 1–8 (2018). https://doi.org/10.1109/jqe.2018.2867651
29. Pavičić, M., et al.: Mixed basis quantum key distribution with linear optics. Opt Express 25(20), 23545–23555 (2017). https://doi.org/10.1364/oe.25.023545
30. Chen, D., Shang-Hong, Z., Ying, S.: Measurement-device-independent quantum key distribution with q-plate. Quant. Inf. Process. 14(12), 4575–4584 (2015). https://doi.org/10.1007/s11128-015-1147-1
31. Hwang, W.-Y., Su, H.-Y., Bae, J.: Improved measurement-device-independent quantum key distribution with uncharacterized qubits. Phys. Rev. 95(6), 062313 (2017). https://doi.org/10.1103/physreva.95.062313
32. Coles, P.J., Metodiev, E.M., Lütkenhaus, N.: Numerical approach for unstructured quantum key distribution. Nat. Commun. 7(1), 11712 (2016). https://doi.org/10.1038/ncomms11712
33. Rozenman, G.G., et al.: The quantum internet: a synergy of quantum information technologies and 6g networks. IET Quan. Commun. 4(4), 147–166 (2023). https://doi.org/10.1049/qtc2.12069
34. Fuchs, C.A., et al.: Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy. Phys. Rev. 56(2), 1163–1172 (1997). https://doi.org/10.1103/physreva.56.1163
35. Bruss, D., Macchiavello, C.: Optimal eavesdropping in cryptography with three-dimensional quantum states. Phys. Rev. Lett. 88(12), 127901 (2002). https://doi.org/10.1103/physrevlett.88.127901
36. Scarani, V., et al.: The security of practical quantum key distribution. Rev. Mod. Phys. 81(3), 1301–1350 (2009). https://doi.org/10.1103/revmodphys.81.1301
37. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. 89(18), 187902 (2002). https://doi.org/10.1103/physrevlett.89.187902
38. Boström, K., Felbinger, T.: On the security of the ping-pong protocol. Phys. Lett. 372(22), 3953–3956 (2008). https://doi.org/10.1016/j.physleta.2008.03.048
39. Cao, Y., et al.: The evolution of quantum key distribution networks: on the road to the qinternet. IEEE Commun. Surv. Tutorials 24(2), 839–894 (2022). https://doi.org/10.1109/COMST.2022.3144219
40. Griffiths, D.J., Schroeter, D.F.: Introduction to Quantum Mechanics. Cambridge University Press, 2018 (2018). ISBN 978-1-107-18963-8
41. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information. Phys. Today 54(2), 60–62 (2001). https://doi.org/10.1063/1.1428442

How to cite this article: Biswas, S., et al.: Advancing quantum communication security: metamaterial based quantum key distribution with enhanced protocols. IET Quant. Comm. 5(4), 399–416 (2024). https://doi.org/10.1049/qtc2.12116