(10) Publication No: **IN202641033375 A1**
(43) Publication Date: 27-03-2026
(22) Date of Filing: 19-03-2026
Journal No: 13/2026

(19) Intellectual Property Office, India

(12) INDIAN PATENT APPLICATION

(54) Title: **A quantum key distribution-based system for secure legal privileged communications**

(51) International Classification:
H04L 9/08, H04L 9/32, H04L 29/06, H04L 9/06 H04L 9/40

(21) Application No: **202641033375**

(31) Priority Document No: --

(32) Priority Date: --

(86) International Application No: --
Filing Date: --

(87) International Publication No: --

(61) Patent of Addition to Application No: --
Filing Date: --

(62) Divisional to Application No: --
Filing Date: --

(71) Name of Applicant(s):
Vels Institute Of Science, Technology And Advanced Studies (vistas),

(72) Name of Inventor(s):
1. Venkateswarlu Ch
2. Ratheeshkumar V V
3. Azizunisaa Begum Sm
4. Sincy Wilson
5. Sree Lekshmi B
6. Mohamed Ali S
7. Athira. V
8. Seena B Nair
9. Aswathi Sukumaran
10. Anna John
11. Ajay Krishna S P
12. Varsha P
13. Shaik Mohammed Ayub

(57) Abstract:

ABSTRACT Disclosed herein is a quantum key distribution-based system for secure legal privileged communications (100), the system (100) comprises a computing unit (102) comprising a processor and a non-transitory memory. The system also includes a communication interface module (104) configured to establish a secure communication channel. A quantum key distribution module (106) configured to generate and distribute cryptographic keys. A key management module (108) configured to store, manage, and periodically update the distributed cryptographic keys. An encryption and decryption module (110) configured to encrypt outgoing legal communication data and decrypt received legal communication data. An authentication and access control module (112) configured to verify the identity of authorized legal participants. A communication monitoring module (114) configured to detect potential security breaches, eavesdropping attempts, or anomalies in the quantum key exchange process. A secure communication interface module (116) configured to facilitate transmission and reception of encrypted legal documents, messages, and data.

FORM 2

THE PATENT ACT 1970

(39 of 1970)

&

THE PATENTS RULES, 2003

COMPLETE SPECIFICATION

(See Section 10, and rule 13)

TITLE OF THE INVENTION

A QUANTUM KEY DISTRIBUTION-BASED SYSTEM FOR SECURE LEGAL PRIVILEGED COMMUNICATIONS

APPLICANT(S)

NAME: VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCED STUDIES (VISTAS)

NATIONALITY: INDIAN

ADDRESS: PALLAVARAM, CHENNAI, TAMIL NADU – 600117, INDIA

The following specification particularly describes the invention and the manner in which it is to be performed

A QUANTUM KEY DISTRIBUTION-BASED SYSTEM FOR SECURE LEGAL PRIVILEGED COMMUNICATIONS

FIELD OF DISCLOSURE

[0001] The present disclosure relates generally relates to the field of secure communication systems and cryptographic technologies. More specifically, it pertains to a quantum key distribution-based system for secure legal privileged communications.

BACKGROUND OF THE DISCLOSURE

[0002] The rapid expansion of digital communication technologies has fundamentally transformed the way legal professionals exchange, store, and manage confidential information. Modern legal practice increasingly relies on electronic communication platforms such as email systems, cloud storage environments, virtual meeting services, and digital document management systems for the transmission and storage of sensitive legal information. Attorneys, legal advisors, corporate counsel, courts, and clients frequently communicate through electronic channels to share privileged documents, case strategies, contractual agreements, financial records, and litigation-related evidence. While such digital platforms have greatly improved efficiency, accessibility, and global collaboration in the legal profession, they have simultaneously introduced significant concerns regarding the confidentiality and security of legally privileged communications.

[0003] Attorney–client privilege is widely recognized as a fundamental principle within many legal systems around the world. This doctrine protects confidential communications between legal professionals and their clients, ensuring that such information cannot be disclosed without the consent of the client. The preservation of this privilege is essential to maintaining trust between clients and their legal representatives, enabling clients to provide full and honest disclosure necessary for effective legal representation.

However, the migration of legal communications to digital networks has introduced vulnerabilities that can threaten the confidentiality of privileged communications. Unauthorized access, cyber espionage, data interception, and information leakage may compromise sensitive legal data and undermine the protections traditionally associated with attorney–client privilege.

[0004] Traditional information security systems used in digital communications typically rely on classical cryptographic techniques. These methods include encryption algorithms such as symmetric key encryption and public key cryptography, which are designed to protect information by transforming readable data into encoded formats that can only be decrypted by authorized recipients. Such encryption mechanisms are widely implemented in secure email systems, virtual private networks, secure messaging platforms, and document encryption solutions used by legal organizations. While these technologies have provided a significant level of protection for digital communications, they rely heavily on mathematical complexity as the basis of their security. The strength of classical cryptographic systems is therefore dependent on the computational difficulty of solving certain mathematical problems.

[0005] In recent years, however, advances in computational capabilities have raised concerns regarding the long-term security of conventional cryptographic techniques. Increasing processing power, the development of high-performance computing infrastructures, and the emergence of advanced cryptanalytic methods have made it possible to perform increasingly sophisticated attacks on encryption systems. More significantly, the theoretical development and experimental progress in quantum computing technologies have introduced new challenges to classical cryptographic security. Quantum computers have the potential to perform certain types of calculations at speeds that significantly exceed those of traditional computing systems, which may enable them to solve

complex mathematical problems that are currently used as the foundation of many widely deployed cryptographic algorithms.

[0006] For example, several widely used public key encryption methods rely on mathematical problems such as integer factorization and discrete logarithms, which are considered computationally difficult for classical computers to solve. However, quantum algorithms have been proposed that could potentially solve these problems much more efficiently if sufficiently powerful quantum computers become available. This potential capability has raised concerns among cyber security researchers, governments, and industry stakeholders regarding the vulnerability of existing cryptographic infrastructures. If large-scale quantum computing systems become practical, many current encryption schemes used in secure communications could become vulnerable to decryption attacks.

[0007] The legal sector is particularly sensitive to such security vulnerabilities because legal communications often contain highly confidential information related to litigation strategies, intellectual property, financial transactions, corporate negotiations, and personal client matters. Unauthorized access to such information could have severe consequences, including loss of legal privilege, reputational damage, financial harm, and compromise of legal proceedings. Additionally, legal communications often involve long-term confidentiality requirements, meaning that sensitive information must remain secure for extended periods of time. Even if encrypted communications cannot be decrypted immediately, adversaries may store encrypted data with the intention of decrypting it in the future once more advanced computational capabilities become available.

[0008] Beyond the threat posed by evolving computational technologies, digital legal communications also face a wide range of cyber security risks arising from network vulnerabilities, malicious actors, and insider threats. Cyber-attacks targeting law firms, corporate legal departments, and government legal institutions have become increasingly common in recent years. Attackers may attempt to intercept communications, gain

unauthorized access to document repositories, or exploit weaknesses in authentication systems to obtain confidential information. Phishing attacks, ransomware campaigns, and targeted data breaches have affected numerous legal organizations around the world, highlighting the critical importance of robust security mechanisms for protecting privileged communications.

[0009] Another challenge associated with protecting legal communications arises from the increasing complexity of modern communication infrastructures. Legal professionals often interact with clients and collaborators across multiple jurisdictions using a variety of digital platforms. Communications may pass through multiple servers, network nodes, and service providers before reaching their intended destination. Each component within this communication chain introduces potential vulnerabilities that could be exploited by attackers seeking to intercept or manipulate confidential information. Ensuring end-to-end security across such distributed communication environments presents a significant technical challenge.

[0010] Furthermore, the adoption of cloud-based services within the legal industry has introduced additional concerns regarding data confidentiality and control. Many legal organizations now store sensitive documents in cloud storage platforms and use cloud-based collaboration tools to facilitate document sharing and case management. While cloud computing offers advantages such as scalability, remote accessibility, and cost efficiency, it also raises questions regarding data sovereignty, third-party access, and the potential for unauthorized disclosure of confidential information. Legal professionals must therefore ensure that any technology used to store or transmit privileged communications provides a high level of security and trustworthiness.

[0011] Regulatory and compliance requirements also play a critical role in shaping the security practices of legal organizations. Many jurisdictions impose strict rules governing the protection of confidential client information,

professional ethics, and data privacy. Legal professionals may be required to implement appropriate technical safeguards to protect client communications from unauthorized access or disclosure. Failure to maintain adequate security measures could result in legal liability, disciplinary actions, or loss of professional accreditation. As digital technologies continue to evolve, legal practitioners must therefore adopt increasingly sophisticated methods to ensure compliance with these regulatory obligations.

[0012] In addition to confidentiality concerns, ensuring the authenticity and integrity of legal communications is equally important. Legal documents and communications must remain accurate and unaltered to preserve their evidentiary value in legal proceedings. Any unauthorized modification or tampering with legal records could have significant implications for litigation outcomes, contractual enforcement, and dispute resolution processes. Consequently, secure communication systems used within the legal domain must provide mechanisms not only for protecting confidentiality but also for ensuring that transmitted information remains authentic and verifiable.

[0013] The need for highly secure communication systems is further amplified by the globalization of legal services. Law firms and legal departments frequently collaborate across international boundaries, exchanging sensitive information through cross-border digital communication networks. Such interactions may involve multiple legal frameworks, regulatory standards, and cyber security environments. The complexity of managing secure communications across these diverse contexts increases the risk of data exposure and requires advanced technological solutions capable of maintaining consistent security protections across geographically distributed networks.

[0014] Researchers and technology developers have therefore been exploring alternative cryptographic approaches that could provide stronger security guarantees than traditional methods. One area of significant interest involves the application of quantum mechanics principles to

information security. Quantum information science has introduced new concepts for secure communication that leverage the fundamental properties of quantum particles such as photons. These approaches are fundamentally different from classical cryptographic techniques because their security is derived from the laws of physics rather than computational complexity.

[0015] Quantum communication technologies have the potential to offer new methods for establishing secure cryptographic keys between communicating parties. In particular, quantum-based communication mechanisms can allow two parties to detect the presence of any third party attempting to intercept their communication channel. This capability arises from fundamental quantum properties such as measurement disturbance and the no-cloning principle, which prevent quantum states from being observed or copied without altering their original condition. As a result, quantum communication systems can provide unique mechanisms for detecting eavesdropping attempts during the process of key exchange.

[0016] Despite the promising capabilities of quantum communication technologies, their integration into practical communication infrastructures presents numerous technical and operational challenges. The implementation of quantum communication systems typically requires specialized hardware components such as photon sources, quantum detectors, and optical transmission channels capable of preserving delicate quantum states. Environmental noise, signal attenuation, and physical limitations of transmission media can affect the reliability of quantum communication processes. Additionally, integrating quantum-based security mechanisms with existing digital communication systems requires careful design to ensure compatibility and scalability.

[0017] The legal domain presents a particularly compelling use case for advanced secure communication technologies due to the critical importance of maintaining confidentiality and trust. Legal professionals must ensure that sensitive communications remain protected from unauthorized access while

also maintaining compliance with legal and ethical obligations related to client confidentiality. As digital communication infrastructures continue to evolve and cyber security threats become increasingly sophisticated, there is a growing need for security solutions capable of providing stronger and more resilient protections for legally privileged communications.

[0018] At the same time, the legal sector must also consider practical factors such as usability, accessibility, and interoperability when adopting new communication technologies. Legal professionals require communication systems that integrate seamlessly with their existing workflows, document management platforms, and collaboration tools. Security solutions must therefore balance advanced protection mechanisms with operational efficiency to ensure that legal practitioners can continue to communicate effectively with clients, colleagues, and judicial institutions.

[0019] Thus, in light of the above-stated discussion, there exists a need for a quantum key distribution-based system for secure legal privileged communications.

SUMMARY OF THE DISCLOSURE

[0020] The following is a summary description of illustrative embodiments of the invention. It is provided as a preface to assist those skilled in the art to more rapidly assimilate the detailed design discussion which ensues and is not intended in any way to limit the scope of the claims which are appended hereto in order to particularly point out the invention.

[0021] According to illustrative embodiments, the present disclosure focuses on a quantum key distribution-based system for secure legal privileged communications which overcomes the above-mentioned disadvantages or provide the users with a useful or commercial choice.

[0022] An objective of the present disclosure is to establish a communication framework that utilizes quantum cryptographic techniques to protect attorney–client privileged data from unauthorized access, interception, or tampering.

[0023] Another objective of the present disclosure is to provide a quantum key distribution-based system for secure legal privileged communications that ensures highly secure transmission of confidential information exchanged between authorized legal entities.

[0024] Another objective of the present disclosure is to enable secure key generation and distribution using quantum key distribution mechanisms, thereby ensuring that encryption keys used for legal communications remain confidential and resistant to cyber threats.

[0025] Another objective of the present disclosure is to detect potential eavesdropping or interception attempts during data transmission through inherent properties of quantum communication protocols.

[0026] Another objective of the present disclosure is to facilitate end-to-end encrypted communication channels between legal professionals, clients, and associated entities while maintaining the integrity and confidentiality of privileged legal information.

[0027] Another objective of the present disclosure is to provide a secure data exchange platform for legal documentation, including contracts, case files, legal opinions, and confidential advisory communications.

[0028] Another objective of the present disclosure is to integrate the quantum key distribution system with existing digital legal communication infrastructures, thereby enhancing security without significantly altering conventional communication workflows.

[0029] Another objective of the present disclosure is to enable real-time monitoring and verification of secure communication sessions, ensuring that only authorized parties can participate in privileged legal exchanges.

[0030] Another objective of the present disclosure is to enhance data integrity and authentication mechanisms in legal communications by utilizing quantum-generated cryptographic keys.

[0031] Yet another objective of the present disclosure is to provide a robust and scalable secure communication architecture that can be deployed

across law firms, judicial institutions, and corporate legal departments for safeguarding sensitive legal information.

[0032] In light of the above, a quantum key distribution-based system for secure legal privileged communications, the system comprises a computing unit comprising a processor and a non-transitory memory storing machine-readable instructions executable by the processor. The system also includes a communication interface module configured to establish a secure communication channel between a pluralities of authorized legal participants. The system also includes a quantum key distribution module configured to generate and distribute cryptographic keys between the authorized legal participants using quantum communication principles to ensure secure key exchange and detection of unauthorized interception. The system also includes a key management module configured to store, manage, and periodically update the distributed cryptographic keys for encrypting and decrypting privileged legal communication data. The system also includes an encryption and decryption module configured to encrypt outgoing legal communication data and decrypt received legal communication data using the cryptographic keys provided by the key management module. The system also includes an authentication and access control module configured to verify the identity of authorized legal participants and restrict access to privileged legal communications based on predefined authorization credentials. The system also includes a communication monitoring module configured to detect potential security breaches, eavesdropping attempts, or anomalies in the quantum key exchange process and generate security alerts in response thereto. The system also includes a secure communication interface module configured to facilitate transmission and reception of encrypted legal documents, messages, and data between the authorized legal participants while maintaining confidentiality and integrity of attorney–client privileged communications.

[0033] In one embodiment, the communication interface module is further configured to establish the secure communication channel through at least one of a wired communication network, a wireless communication network, or an internet-based communication infrastructure to enable remote interaction between the authorized legal participants.

[0034] In one embodiment, the quantum key distribution module is configured to generate and distribute cryptographic keys using at least one quantum key distribution protocol including a quantum photon transmission mechanism configured to detect interception attempts during the key exchange process.

[0035] In one embodiment, the key management module is configured to periodically refresh, revoke, and regenerate cryptographic keys based on predefined security policies or detected communication anomalies.

[0036] In one embodiment, the encryption and decryption module is further configured to apply symmetric or hybrid encryption techniques in combination with the distributed quantum keys to secure privileged legal communication data.

[0037] In one embodiment, the authentication and access control module is configured to authenticate the authorized legal participants using multi-factor authentication including at least one of biometric verification, digital certificates, secure login credentials, or hardware authentication tokens.

[0038] In one embodiment, the communication monitoring module is configured to continuously monitor the quantum key exchange process and identify anomalies including signal disturbances, interception attempts, or unauthorized access attempts within the communication channel.

[0039] In one embodiment, the communication monitoring module is further configured to generate automated security alerts and initiate protective actions including key revocation, communication suspension, or notification to authorized administrators upon detection of a potential security breach.

[0040] In one embodiment, the secure communication interface module is configured to provide a user interface enabling authorized legal participants

to securely transmit, receive, and store encrypted legal documents, messages, and confidential case-related information.

[0041] In one embodiment, the secure communication interface module further maintains an immutable communication log including timestamps, transaction identifiers, and participant authentication records for auditing and compliance verification purposes.

[0042] These and other advantages will be apparent from the present application of the embodiments described herein.

[0043] The preceding is a simplified summary to provide an understanding of some embodiments of the present invention. This summary is neither an extensive nor exhaustive overview of the present invention and its various embodiments. The summary presents selected concepts of the embodiments of the present invention in a simplified form as an introduction to the more detailed description presented below. As will be appreciated, other embodiments of the present invention are possible utilizing, alone or in combination, one or more of the features set forth above or described in detail below.

[0044] These elements, together with the other aspects of the present disclosure and various features are pointed out with particularity in the claims annexed hereto and form a part of the present disclosure. For a better understanding of the present disclosure, its operating advantages, and the specified object attained by its uses, reference should be made to the accompanying drawings and descriptive matter in which there are illustrated exemplary embodiments of the present disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0045] To describe the technical solutions in the embodiments of the present disclosure or in the prior art more clearly, the following briefly describes the accompanying drawings required for describing the embodiments or the prior art. Apparently, the accompanying drawings in the following description merely show some embodiments of the present disclosure, and a person of ordinary skill in the art can derive other

implementations from these accompanying drawings without creative efforts. All of the embodiments or the implementations shall fall within the protection scope of the present disclosure.

[0046] The advantages and features of the present disclosure will become better understood with reference to the following detailed description taken in conjunction with the accompanying drawing, in which:

[0047] FIG. 1 illustrates a flowchart outlining sequential step involved in a quantum key distribution-based system for secure legal privileged communications, in accordance with an exemplary embodiment of the present disclosure;

[0048] Like reference, numerals refer to like parts throughout the description of several views of the drawing;

[0049] The quantum key distribution-based system for secure legal privileged communications, which like reference letters indicate corresponding parts in the various figures. It should be noted that the accompanying figure is intended to present illustrations of exemplary embodiments of the present disclosure. This figure is not intended to limit the scope of the present disclosure. It should also be noted that the accompanying figure is not necessarily drawn to scale.

DETAILED DESCRIPTION OF THE DISCLOSURE

[0050] The following is a detailed description of embodiments of the disclosure depicted in the accompanying drawings. The embodiments are in such detail as to communicate the disclosure. However, the amount of detail offered is not intended to limit the anticipated variations of embodiments; on the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the present disclosure.

[0051] In the following description, numerous specific details are set forth in order to provide a thorough understanding of the embodiments of the

present disclosure. It may be apparent to one skilled in the art that embodiments of the present disclosure may be practiced without some of these specific details.

[0052] Various terms as used herein are shown below. To the extent a term is used, it should be given the broadest definition persons in the pertinent art have given that term as reflected in printed publications and issued patents at the time of filing.

[0053] The terms “a” and “an” herein do not denote a limitation of quantity, but rather denote the presence of at least one of the referenced items.

[0054] The terms “having”, “comprising”, “including”, and variations thereof signify the presence of a component.

[0055] Referring now to FIG. 1 to describe various exemplary embodiments of the present disclosure. FIG. 1 illustrates a flowchart outlining sequential step involved in a quantum key distribution-based system for secure legal privileged communications, in accordance with an exemplary embodiment of the present disclosure.

[0056] A quantum key distribution-based system for secure legal privileged communications 100, the system 100 comprises a computing unit 102 comprising a processor and a non-transitory memory storing machine-readable instructions executable by the processor.

[0057] The system also includes a communication interface module 104 configured to establish a secure communication channel between a plurality of authorized legal participants. The communication interface module 104 is further configured to establish the secure communication channel through at least one of a wired communication network, a wireless communication network, or an internet-based communication infrastructure to enable remote interaction between the authorized legal participants.

[0058] The system also includes a quantum key distribution module 106 configured to generate and distribute cryptographic keys between the

authorized legal participants using quantum communication principles to ensure secure key exchange and detection of unauthorized interception. The quantum key distribution module 106 is configured to generate and distribute cryptographic keys using at least one quantum key distribution protocol including a quantum photon transmission mechanism configured to detect interception attempts during the key exchange process.

[0059] The system also includes a key management module 108 configured to store, manage, and periodically update the distributed cryptographic keys for encrypting and decrypting privileged legal communication data. The key management module 108 is configured to periodically refresh, revoke, and regenerate cryptographic keys based on predefined security policies or detected communication anomalies.

[0060] The system also includes an encryption and decryption module 110 configured to encrypt outgoing legal communication data and decrypt received legal communication data using the cryptographic keys provided by the key management module. The encryption and decryption module 110 is further configured to apply symmetric or hybrid encryption techniques in combination with the distributed quantum keys to secure privileged legal communication data.

[0061] The system also includes an authentication and access control module 112 configured to verify the identity of authorized legal participants and restrict access to privileged legal communications based on predefined authorization credentials. The authentication and access control module 112 is configured to authenticate the authorized legal participants using multi-factor authentication including at least one of biometric verification, digital certificates, secure login credentials, or hardware authentication tokens.

[0062] The system also includes a communication monitoring module 114 configured to detect potential security breaches, eavesdropping attempts, or anomalies in the quantum key exchange process and generate security

alerts in response thereto. The communication monitoring module 114 is configured to continuously monitor the quantum key exchange process and identify anomalies including signal disturbances, interception attempts, or unauthorized access attempts within the communication channel. The communication monitoring module 114 is further configured to generate automated security alerts and initiate protective actions including key revocation, communication suspension, or notification to authorized administrators upon detection of a potential security breach.

[0063] The system also includes a secure communication interface module 116 configured to facilitate transmission and reception of encrypted legal documents, messages, and data between the authorized legal participants while maintaining confidentiality and integrity of attorney–client privileged communications. The secure communication interface module 116 is configured to provide a user interface enabling authorized legal participants to securely transmit, receive, and store encrypted legal documents, messages, and confidential case-related information. The secure communication interface module 116 further maintains an immutable communication log including timestamps, transaction identifiers, and participant authentication records for auditing and compliance verification purposes.

[0064] FIG. 1 illustrates a flowchart outlining sequential step involved in a quantum key distribution-based system for secure legal privileged communications.

[0065] At 102, the process begins with the initialization of a computing unit 102 which functions as the central processing and coordination component of the system. The computing unit 102 comprises a processor and a non-transitory memory storing machine-readable instructions that are executed by the processor to control the overall operational workflow of the system. During system activation, the processor retrieves the stored instructions from the memory and initializes the communication infrastructure,

cryptographic operations, authentication protocols, and monitoring mechanisms necessary for maintaining confidentiality in legal communications. The computing unit 102 further coordinate's interactions between multiple modules of the system, ensuring that communication requests from authorized participants are processed securely while maintaining compliance with legal confidentiality standards such as attorney–client privilege. By managing data flow, cryptographic operations, and system responses, the computing unit 102 establishes a controlled environment in which privileged legal communications can be exchanged securely without risk of unauthorized interception.

[0066] At 104, the flowchart proceeds to the operation of a communication interface module 104 responsible for establishing secure communication channels between a plurality of authorized legal participants. These participants may include attorneys, legal consultants, clients, paralegals, or authorized administrative personnel who require access to privileged legal communication platforms. The communication interface module 104 facilitates the connection of participant devices such as computers, secure mobile devices, or dedicated legal communication terminals through a communication network. During this stage, the module configures communication protocols, verifies network connectivity, and prepares the system environment for encrypted message exchange. The communication interface module 104 ensures that the communication pathway between participants is properly established before any sensitive information is transmitted, thereby providing the foundational infrastructure required for secure legal correspondence. Through this module, legal professionals and clients are able to initiate secure communication sessions while maintaining confidentiality and integrity of the transmitted information.

[0067] At 106, the system activates a quantum key distribution module 106 that performs the generation and distribution of cryptographic keys using quantum communication principles. In this stage of the flowchart, the

module employs quantum key distribution techniques to create encryption keys that are fundamentally secure due to the laws of quantum mechanics. The quantum key distribution module 106 generates quantum states, typically represented by polarized photons or similar quantum signals, which are transmitted between the authorized participants through a quantum communication channel. As the quantum states are exchanged, the participants measure the transmitted signals to derive identical cryptographic keys used for secure communication. Due to the inherent properties of quantum mechanics, any attempt by an unauthorized party to intercept or measure the quantum states will disturb the quantum signals, thereby revealing the presence of an eavesdropping attempt. The system continuously analyzes these signals to confirm that the key distribution process remains uncompromised. In this manner, the quantum key distribution module 106 ensures the secure generation and exchange of encryption keys that form the foundation of the system's communication security.

[0068] At 108, the system proceeds to a key management module 108 responsible for storing, managing, and periodically updating the distributed cryptographic keys. The key management module 108 securely stores the generated keys within protected memory structures associated with the computing unit 102 and manages their lifecycle throughout the communication process. The module maintains synchronization between the keys used by different participants and ensures that the keys are accessible only to authorized system components. Additionally, the key management module 108 periodically refreshes the cryptographic keys by initiating new quantum key distribution sessions, thereby reducing the risk of key compromise and maintaining long-term communication security. Through controlled key rotation and secure storage mechanisms, the module ensures that encryption keys remain protected from unauthorized access while supporting continuous secure communication between legal participants.

[0069] At 110, the flowchart advances to the operation of an encryption and decryption module 110 that secures the content of legal communications. The encryption and decryption module 110 utilizes the cryptographic keys provided by the key management module 108 to convert outgoing legal communication data into encrypted form prior to transmission. Such communication data may include legal documents, confidential case notes, legal advice, client correspondence, and other sensitive information protected under attorney client privilege. When a participant sends a message or document, the module encrypts the data using the current cryptographic key to ensure that the information cannot be interpreted by unauthorized entities during transmission. When the encrypted data is received by another authorized participant, the module decrypts the information using the corresponding cryptographic key, thereby restoring the original content for legitimate use. By implementing strong encryption and decryption processes, the module ensures that all privileged legal information remains confidential and protected from unauthorized disclosure.

[0070] At 112, the system engages an authentication and access control module 112 that verifies the identity of authorized participants and regulates access to the secure communication platform. During the authentication process, the module validates user credentials such as digital certificates, secure authentication tokens, biometric verification data, or encrypted login credentials. The authentication and access control module 112 further checks the authorization privileges associated with each participant to determine whether the individual has permission to access specific communication sessions or legal documents. If a user fails to meet the authentication requirements or attempts to access restricted data without proper authorization, the module denies access and records the event for security auditing purposes. By implementing strict authentication protocols and access control mechanisms, the system ensures that privileged legal

communications remain accessible only to verified and authorized participants.

[0071] At 114, the system activates a communication monitoring module 114 designed to continuously supervise the security status of the communication network and the quantum key exchange process. The communication monitoring module 114 analyzes communication traffic, key distribution signals, and system activity logs to detect any irregularities or potential security threats. For example, the module may identify anomalies in quantum signal measurements that indicate potential eavesdropping attempts during key exchange. Additionally, the module monitors network communication patterns to detect suspicious activities such as repeated unauthorized access attempts or abnormal data transmission patterns. If the module identifies a potential security breach, it generates security alerts and may trigger protective actions such as terminating the communication session, initiating a new key distribution process, or notifying system administrators of the detected threat. Through continuous monitoring and anomaly detection, the communication monitoring module 114 enhances the overall security and reliability of the system.

[0072] At 116, the system provides secure communication functionality through a secure communication interface module 116 that facilitates the transmission and reception of encrypted legal documents, messages, and data between authorized participants. The secure communication interface module 116 presents an interactive platform through which attorneys and clients can exchange confidential information in a secure and user-friendly manner. The module retrieves encrypted communication data processed by the encryption and decryption module 110 and delivers it to the intended recipients through the secure communication channel established earlier in the process. Additionally, the interface module may provide features such as secure document sharing, encrypted messaging threads, legal file management, and communication history tracking. Because all

communications transmitted through this interface are protected by quantum-generated encryption keys and strict authentication controls, the confidentiality and integrity of attorney–client communications are maintained at all times.

[0073] While the invention has been described in connection with what is presently considered to be the most practical and various embodiments, it will be understood that the invention is not to be limited to the disclosed embodiments, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the scope of the appended claims.

[0074] A person of ordinary skill in the art may be aware that, in combination with the examples described in the embodiments disclosed in this specification, units and algorithm steps may be implemented by electronic hardware, computer software, or a combination thereof.

[0075] The foregoing descriptions of specific embodiments of the present disclosure have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed, and many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described to best explain the principles of the present disclosure and its practical application, and to thereby enable others skilled in the art to best utilize the present disclosure and various embodiments with various modifications as are suited to the particular use contemplated. It is understood that various omissions and substitutions of equivalents are contemplated as circumstances may suggest or render expedient, but such omissions and substitutions are intended to cover the application or implementation without departing from the scope of the present disclosure.

[0076] Disjunctive language such as the phrase “at least one of X, Y, Z,” unless specifically stated otherwise, is otherwise understood with the context as used in general to present that an item, term, etc., may be either

X, Y, or Z, or any combination thereof (e.g., X, Y, and/or Z). Thus, such disjunctive language is not generally intended to, and should not, imply that certain embodiments require at least one of X, at least one of Y, or at least one of Z to each be present.

[0077] In a case that no conflict occurs, the embodiments in the present disclosure and the features in the embodiments may be mutually combined. The foregoing descriptions are merely specific implementations of the present disclosure, but are not intended to limit the protection scope of the present disclosure. Any variation or replacement readily figured out by a person skilled in the art within the technical scope disclosed in the present disclosure shall fall within the protection scope of the present disclosure. Therefore, the protection scope of the present disclosure shall be subject to the protection scope of the claims.

I/We Claim:

1. A quantum key distribution-based system for secure legal privileged communications (100), the system (100) comprising:

a computing unit (102) comprising a processor and a non-transitory memory storing machine-readable instructions executable by the processor;

a communication interface module (104) configured to establish a secure communication channel between a plurality of authorized legal participants;

a quantum key distribution module (106) configured to generate and distribute cryptographic keys between the authorized legal participants using quantum communication principles to ensure secure key exchange and detection of unauthorized interception;

a key management module (108) configured to store, manage, and periodically update the distributed cryptographic keys for encrypting and decrypting privileged legal communication data;

an encryption and decryption module (110) configured to encrypt outgoing legal communication data and decrypt received legal communication data using the cryptographic keys provided by the key management module;

an authentication and access control module (112) configured to verify the identity of authorized legal participants and restrict access to privileged legal communications based on predefined authorization credentials;

a communication monitoring module (114) configured to detect potential security breaches, eavesdropping attempts, or anomalies in the quantum key exchange process and generate security alerts in response thereto; and

a secure communication interface module (116) configured to facilitate transmission and reception of encrypted legal documents, messages, and data between the authorized legal participants while maintaining confidentiality and integrity of attorney–client privileged communications.

2. The system (100) as claimed in claim 1, wherein the communication interface module (104) is further configured to establish the secure communication channel through at least one of a wired communication network, a wireless communication network, or an internet-based communication infrastructure to enable remote interaction between the authorized legal participants.
3. The system (100) as claimed in claim 1, wherein the quantum key distribution module (106) is configured to generate and distribute cryptographic keys using at least one quantum key distribution protocol including a quantum photon transmission mechanism configured to detect interception attempts during the key exchange process.
4. The system (100) as claimed in claim 1, wherein the key management module (108) is configured to periodically refresh, revoke, and regenerate cryptographic keys based on predefined security policies or detected communication anomalies.
5. The system (100) as claimed in claim 1, wherein the encryption and decryption module (110) is further configured to apply symmetric or hybrid encryption techniques in combination with the distributed quantum keys to secure privileged legal communication data.
6. The system (100) as claimed in claim 1, wherein the authentication and access control module (112) is configured to authenticate the authorized legal participants using multi-factor authentication including at least one of biometric verification, digital certificates, secure login credentials, or hardware authentication tokens.
7. The system (100) as claimed in claim 1, wherein the communication monitoring module (114) is configured to continuously monitor the

quantum key exchange process and identify anomalies including signal disturbances, interception attempts, or unauthorized access attempts within the communication channel.

8. The system (100) as claimed in claim 1, wherein the communication monitoring module (114) is further configured to generate automated security alerts and initiate protective actions including key revocation, communication suspension, or notification to authorized administrators upon detection of a potential security breach.

9. The system (100) as claimed in claim 1, wherein the secure communication interface module (116) is configured to provide a user interface enabling authorized legal participants to securely transmit, receive, and store encrypted legal documents, messages, and confidential case-related information.

10. The system (100) as claimed in claim 1, wherein the secure communication interface module (116) further maintains an immutable communication log including timestamps, transaction identifiers, and participant authentication records for auditing and compliance verification purposes.

Dated this 18th day of March 2026.

URVASHI SHARMA
AGENT FOR THE APPLICANTS
IN/PA No. 3830

A QUANTUM KEY DISTRIBUTION-BASED SYSTEM FOR SECURE LEGAL PRIVILEGED COMMUNICATIONS

ABSTRACT

Disclosed herein is a quantum key distribution-based system for secure legal privileged communications (100), the system (100) comprises a computing unit (102) comprising a processor and a non-transitory memory. The system also includes a communication interface module (104) configured to establish a secure communication channel. A quantum key distribution module (106) configured to generate and distribute cryptographic keys. A key management module (108) configured to store, manage, and periodically update the distributed cryptographic keys. An encryption and decryption module (110) configured to encrypt outgoing legal communication data and decrypt received legal communication data. An authentication and access control module (112) configured to verify the identity of authorized legal participants. A communication monitoring module (114) configured to detect potential security breaches, eavesdropping attempts, or anomalies in the quantum key exchange process. A secure communication interface module (116) configured to facilitate transmission and reception of encrypted legal documents, messages, and data.

Claims – 10, FIG. - 1