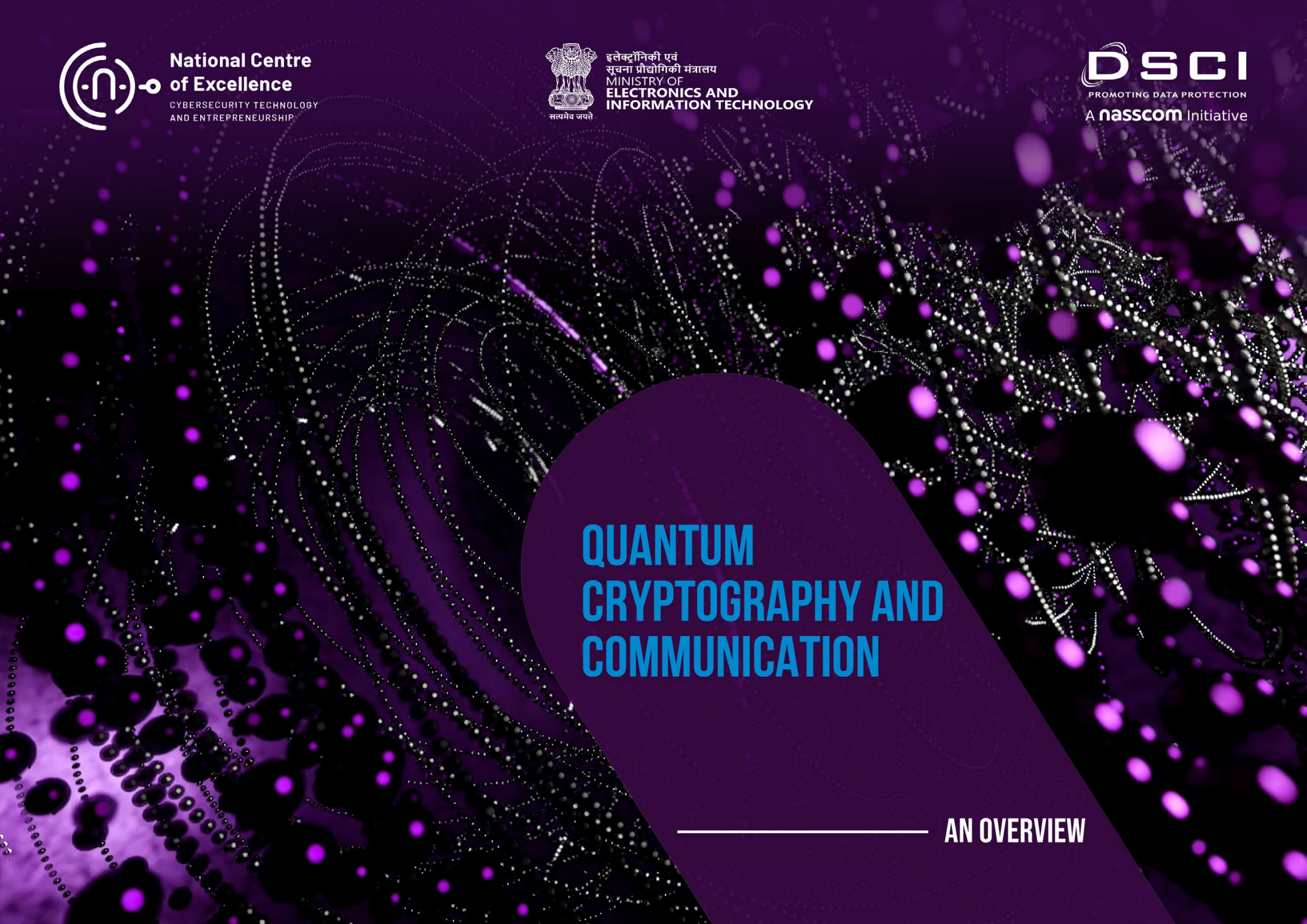
National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative



QUANTUM CRYPTOGRAPHY AND COMMUNICATION

AN OVERVIEW

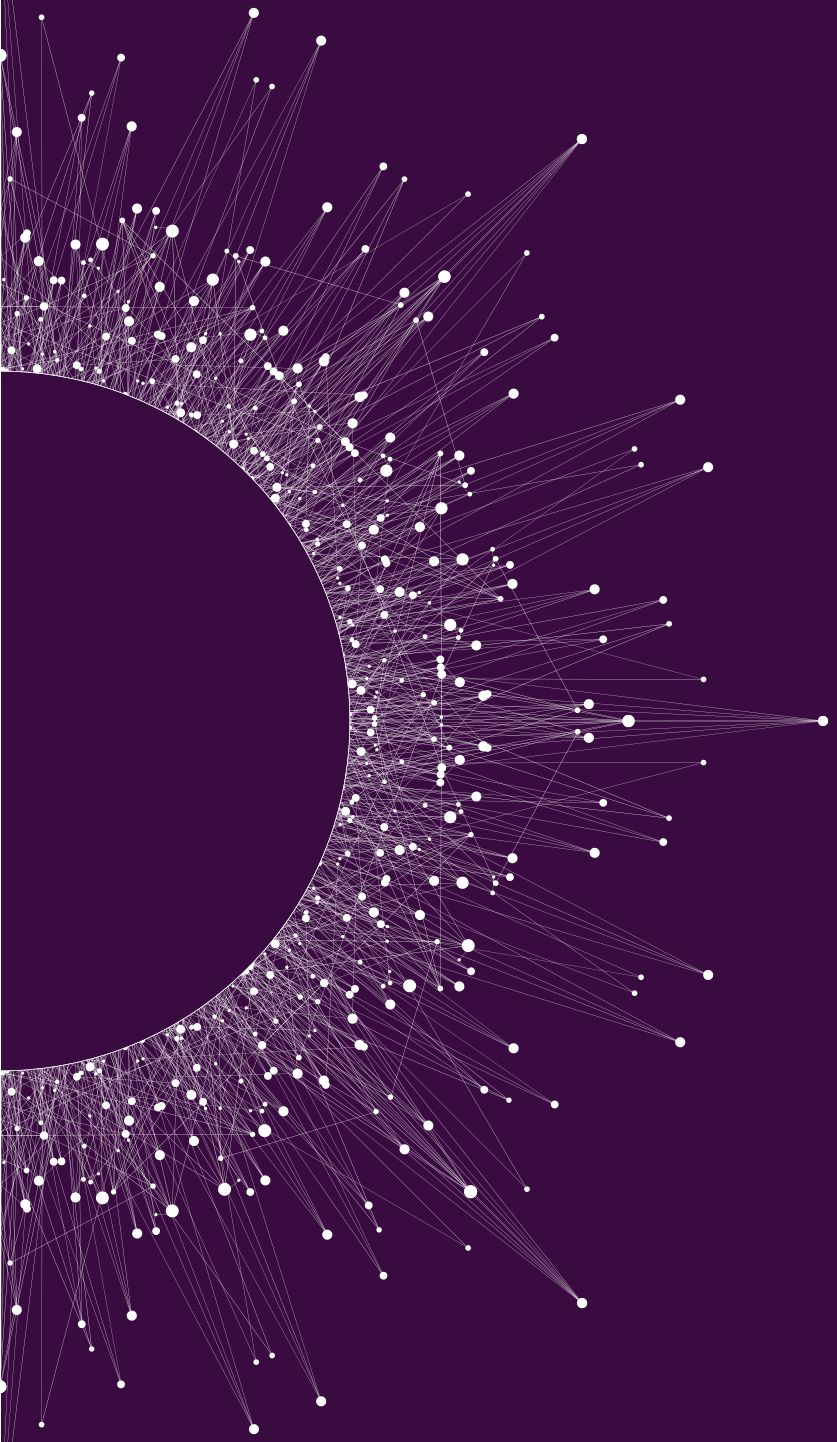
Contributors

Dr Anil Prabhakar, Professor, Dept. of Electrical Engineering, IIT Madras

Dr. Prabha Mandayam, Associate Professor, Dept of Physics, IIT Madras

Dr. Pradeep Sarvepalli, Associate Professor, Dept. of Electrical Engineering, IIT Madras

Dr. Shweta Agrawal, Professor - Dept. of CSE, IIT Madras



Contents

1

Introduction

The emergence of quantum computing has dramatically changed the landscape of the science of computing, with far reaching consequences both algorithmic to experimental, in diverse areas ranging from communication to networks to cryptography to machine learning. In this note, we provide an overview of a selection of these topics.

Post Quantum Cryptography.

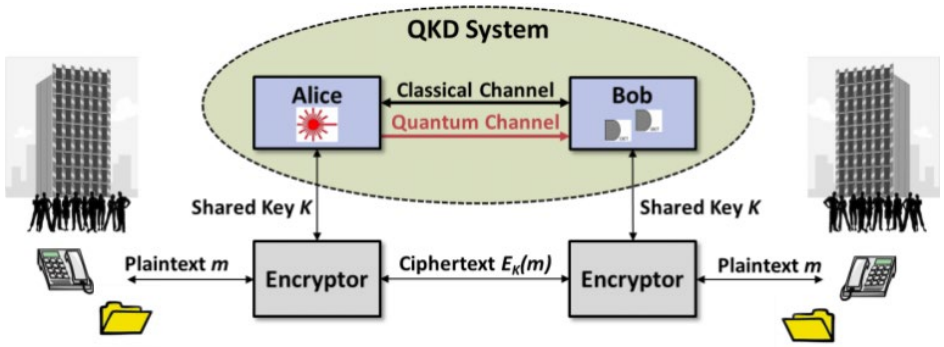
Cryptography is the science of designing methods to achieve certain secrecy goals, for instance that of hiding information, so that breaking security implies a solution to some well known mathematical problem. Choosing the underlying hard problem is thus of paramount importance, and we would like to have strong evidence that current day computing resources do not permit an attacker to solve the problem in any reasonable time. Here, the term "computing resources" warrants further investigation – traditionally, cryptography has been based on problems that are conjectured to be infeasible in the realm of classical computers. However, recent times have seen significant advances in the design and construction of quantum computers, which are more powerful than classical computers. If an attacker has access to a quantum computer, are known cryptosystems safe?

While classical cryptographic techniques have stood the test of time, they are increasingly at risk due to the impending arrival of quantum computers. Quantum computing, powered by principles like superposition and entanglement, promises exponential speedups for certain types of problems, including those that underpin the security of classical

cryptography. Peter Shor's algorithm,[1] for instance, demonstrates the theoretical capability of quantum computers to efficiently factorize large numbers, effectively breaking RSA encryption. This looming threat necessitates the development of

quantum-resistant security measures to safeguard sensitive information in the post-quantum era. The area of cryptography which is secure against quantum attackers is known as "post-quantum" cryptography.

Figure 1.1: A typical point-to-point quantum secure link. [2]



Quantum Key Distribution. Quantum Key Distribution (QKD) operates at the intersection of quantum mechanics and information theory, leveraging the counterintuitive yet empirically verified behaviors of quantum systems to establish secure communication. A typical schema is shown in Fig. 1.1, relying on both classical and quantum channels of communication.

The strength of QKD lies in its reliance on the inherent properties of quantum particles —- properties that are not just unique but also unassailable by classical physics. QKD leverages the principles of quantum mechanics to ensure the secure exchange of cryptographic keys. Unlike classical systems that depend on computational hardness assumptions, QKD offers unconditional security grounded in the laws of quantum information, and has thus emerged as a possible solution to the threat posed by a quantum computer. This distinction makes QKD particularly valuable in an era where classical cryptography may no longer be sufficient to protect critical communications.

Quantum Secret Sharing

Quantum key distribution is perhaps the most studied of all quantum cryptographic protocols. However, there are several other quantum cryptographic protocols that are also important and worth further study; see, for instance,[3]. In this note, we review an important quantum cryptographic primitive, namely, quantum secret sharing. This protocol is of great importance in secure distributed quantum computing. The secret sharing scheme is a protocol to distribute information among untrusted parties so that only certain authorized subsets of parties can recover the secret. The subsets of parties that are not authorized cannot recover the secret. By distributing the secret among various parties, secret sharing also provides a means to combat malicious parties from corrupting the secret.

Quantum Networks

Quantum networks are the basic building blocks that go into achieving the ambitious vision of a quantum internet[4–6] that allows secure quantum communication between any pair of locations across the world. The idea of a quantum network has its genesis in quantum key distribution (QKD), which enables secure key exchange over a public channel between two trusted parties, whose unconditional security is guaranteed by the laws of quantum mechanics (cf. Sec. 3). Today, the scope and impact of quantum networks goes much beyond QKD, with applications that range from quantum secret sharing and secure quantum computing on the cloud[7] to accurate clock synchronization [8] and secure online voting [9].

2

Post Quantum Cryptography

Despite substantial research effort, no efficient quantum algorithms are known for lattice problems that outperform classical ones significantly. In fact, the only advantage quantum computers offer in this regard are modest generic speedups.

At a high level, the mathematical problems underlying post-quantum cryptography may be categorized into the following broad families:

Lattice Based Cryptography[7]: Of all known candidates for post quantum cryptography, perhaps the most popular is lattice based cryptography. Informally, a lattice is a set of points in an n dimensional space with a periodic structure. Lattices occur everywhere, from crystals to stacks of fruit to ancient Islamic art, and have been widely studied, starting with ancient mathematicians such as Lagrange, Minkowski and Gauss upto modern computer scientists. A lattice may be represented using a basis that generates its points, and given a basis, the most basic question that may be posed is that of finding the smallest nonzero point in the corresponding lattice. This classic problem is known as the shortest vector problem (or SVP) and is related to many other lattice problems as we shall see subsequently.

Despite substantial research effort, no efficient quantum algorithms are known for lattice problems that outperform classical ones significantly. In fact, the only advantage quantum computers offer in this regard are modest generic speedups. Besides, lattice based cryptography has many other advantages. Cryptosystems based on lattices are often algorithmically simple, efficient and highly paralellizable. Moreover, lattice based cryptography enjoys a surprising connection between average case and worst case hardness[10] which makes it especially attractive. In more detail, cryptography is based on average case intractable problems, which means that randomly chosen instances of problem must be difficult to solve. On the other hand, complexity theory usually studies worst case hardness, where a problem is considered hard if there merely exists an intractable instance of the problem. In a surprising work, Ajtai[10] showed that certain lattice problems are hard on the average if some related lattice problems are hard in the worst case. This allows for the design of cryptographic schemes that are infeasible to break unless all instances of certain lattice problems are hard to solve.

Multivariate Polynomial Cryptography: Another family of problems that is believed to resist quantum computers is related to solving nonlinear equations over a finite field. Cryptosystems that rely on such problems for their security are clubbed under the banner of "multivariate polynomial cryptography" [11–14]. In more detail, the multivariate quadratic polynomial problem, denoted by MQ, is: given m quadratic polynomials f1, . . . , fm in n variables x1, . . . , xn, with coefficients chosen from a field F, find a solution $z \in F^n$ such that $f_i(z) = 0$ for $i \in [m]$.

Evidently, the parameters are chosen so that simple attacks such as linearization do not apply. Indeed, in the worst case, this problem is known to be NP hard.

The birth of multivariate polynomial cryptography took place in 1988, in an encryption scheme proposed by T. Matsumoto and H. Imai [11]. While this scheme was subsequently broken, the general principle found applicability in many subsequent constructions, such as the "Hidden Field Equations" by Patarin [15] or "Unbalanced Oil and Vinegar" [16]. Presently, there exist candidates for secure cryptosystems based on this class of problems that are believed to be quantum secure. We refer the reader to [17] for a detailed survey.

Code Based Cryptography: Code based cryptography uses the theory of error correcting codes to construct cryptosystems. The first candidate of such a cryptosystem was by McEliece [18], based on the hardness of decoding a general linear code, a problem which is known to be NP-hard. To construct the secret key, an error-correcting code is chosen for which

an efficient decoding algorithm is known, and which is able to correct up to t errors. The public key is derived from the private key by disguising the selected code as a general linear code. The encryptor generates a codeword using the public key, perturbed by upto t errors. The decryptor recovers the message by performing error correction and efficient decoding of the codeword. The security of the above construction depends heavily on the choice of the error correcting code used in the construction: to the best of our knowledge, constructions using Goppa codes have remained resilient to attack [19]. Traditionally the McEliece cryptosystem did not find much deployment due to its large keys and ciphertexts. But there is renewed interest in this family of constructions due to their quantum resilience.

Hash Based Cryptography: Hash based cryptography is a general name given to cryptosystems which derive their hardness from hash functions. The simplest and most well known example of a hash based cryptosystem is the signature scheme by Merkle [20], which converts a weak signature scheme to a strong one, using hash functions. In more detail, the transformation begins with a signature scheme which is only secure for signing a single message and converts it into a many time signature scheme using the so called "Merkle tree structure" and by relying only on the existence of hash functions. Since one time signatures can be based simply on the existence of one way functions, the security of these constructions is well understood even in the quantum setting. However, the efficiency and generality of hash based cryptography is restricted, and this limits its popularity.

2.1 Lattice Based Cryptography

To give the reader a deeper taste of post quantum cryptography, we focus our attention on lattice based cryptography for the remainder of this note. To begin, let us define a lattice formally.

Definition 2.1. An m-dimensional lattice Λ is a full-rank discrete subgroup of Rm. A basis of Λ is a linearly independent set of vectors whose integer linear combinations generate Λ. In cryptography, we are usually concerned with integer lattices, i.e., those whose points have coordinates in Zm.

Among these lattices are the "q-ary" lattices defined as follows: for any integer q ≥ 2 and any A ∈ Zn×m, we define

$$:= \mathbf{e} \in \mathbf{Zm} : \mathbf{A} \cdot \mathbf{e} = \mathbf{0} \bmod \mathbf{q}$$

These lattices are of special interest in cryptography.

The minimum distance of a lattice Λ is the length of a shortest nonzero vector:

$$\lambda 1(\Lambda) = \min_{v \in \Lambda \setminus \{0\}} \|v\|$$

Here, $\|\cdot\|$ denotes the Euclidean norm. In general, the ith successive minima $\lambda i(\Lambda)$ is the smallest radius r such that Λ has i linearly independent vectors of norm at most r.

2.1.1 Classic Computational Lattice Problems

In this section, we discuss some classic computational problems over lattices.

Definition 2.2 (Shortest Vector Problem (SVP)). Given an arbitrary basis B of some lattice $\Lambda = \Lambda(B)$, find a nonzero vector $v \in \Lambda(B)$ such that $\|v\| = \lambda 1(\Lambda(B))$.

We note that there is a bound on $\lambda 1(\Lambda(B))$ by Minkowski's first theorem, which states that for any full rank lattice $\Lambda(B)$ of rank n,

$$\lambda_1(\Lambda(B)) \leq \sqrt{n}\,(\det(\Lambda(B))^{\frac{1}{n}}$$

Next, we define the approximate version of this problem. Let $\gamma \geq 1$ be an approximation factor; this is typically taken as a function of the lattice dimension n.

Definition 2.3 (Approximate Shortest Vector Problem (SVPγ)). Given a basis B of an n dimensional lattice $\Lambda = \Lambda(B)$, find nonzero vector $v \in \Lambda(B)$ s.t. $\|v\| \leq \gamma \cdot \lambda 1(\Lambda(B))$.

Of particular importance in cryptography is the decision version of the approximate shortest vector problem, which we define next.

Definition 2.4 (Decisional Shortest SVP (GapSVPγ)). Given a basis B of an n dimensional lattice and the promise that either $\lambda 1(\Lambda(B)) \leq 1$ or $\lambda 1(\Lambda(B)) \geq \gamma$, determine which is the case.

Definition 2.5 (Shortest Independent Vector Problem (SIVPγ)). Given a basis B of a full rank, n dimensional lattice $\Lambda = \Lambda(B)$, output a set of n linearly independent lattice vectors vectors $S = \{si\}i\in[n]$ s.t. for $i \in [n]$,

$$\|si\| \leq \gamma \cdot \lambda n(\Lambda(B))$$

Finally, we define the "bounded distance decoding" problem, which takes as input a lattice Λ and a target point t, with the promise that t is "close" to Λ, and asks to find the lattice point closest to t.

Definition 2.6 (Bounded Distance Decoding Problem (BDDγ)). Given a basis B of an n dimensional lattice $\Lambda = \Lambda(B)$ and a target point $t \in Rn$ with the promise that $dist(\Lambda, t) < d = \lambda 1(\Lambda(B))/(2 \cdot \gamma)$, find the unique lattice point v such that $\|t - v\| < d$.

Hardness and effect on cryptography. Most of the above problems are known to be NP-hard to solve exactly as well as for sub-polynomial approximation factors. However, cryptographic constructions rely on the hardness of the above problems for polynomial approximation factors, which place them in the realm of NP $\cap$ co-NP. Even for polynomial approximation factors however, we believe these problems are intractable; indeed, no efficient algorithms are known even for sub- exponential approximation factors despite significant research effort by the community. We refer the reader to[21] for an in-depth discussion.

Early lattice based cryptosystems such as by Ajtai and Dwork[22], Goldreich, Goldwasser and Halevi[23], and Regev[24] were based on the above problems or variants thereoff. While these were important theoretical breakthroughs and introduced ideas that form the cornerstone of lattice based cryptographic design even today, they were subsequently replaced by simpler systems relying on hardness of a different set of lattice problems, which may be seen as "better suited" for cryptographic design. We discuss these next.

2.1.2 Modern Computational Lattice Problems

Most modern cryptosystems rely on the hardness of the following problems.

Short Integer Solution Problem (SIS). The short integer solution problem was introduced by Ajtai [10] and is defined below.

Definition 2.7 (Short Integer Solution ($\mathsf{SIS}_{\mathsf{n,m,q},\beta}$))**.** Given a uniformly chosen matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$ and a real valued parameter β, find a nonzero integer vector $\mathbf{e} \in \mathbb{Z}^m$ s.t.

$$\mathbf{A}\,\mathbf{e} = 0 \mod q \quad \text{and} \quad \|\mathbf{e}\| \leq \beta$$

Note that the SIS problem can be seen as an average case short vector problem on the q-ary lattice $\Lambda_q^{\perp}(\mathbf{A})$ defined above.

Definition 2.8 (Inhomogeneous Short Integer Solution ($\mathsf{ISIS}_{\mathsf{n,m,q},\beta}$))**.** Given a uniformly chosen matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, a uniformly chosen vector $\mathbf{u} \leftarrow \mathbb{Z}_q^n$ and a real valued parameter β, find a nonzero integer vector $\mathbf{e} \in \mathbb{Z}^m$ s.t.

$$\mathbf{A}\,\mathbf{e} = \mathbf{u} \mod q \quad \text{and} \quad \|\mathbf{e}\| \leq \beta$$

The SIS and ISIS problem can be seen as essentially equivalent, and related to the classic GapSVP problem as follows.

Theorem 2.9. *[10, 25–27] For $m = \mathrm{poly}(n)$, any $\beta > 0$, and sufficiently large $q \geq \beta \cdot \mathrm{poly}(n)$, solving the (average case) $\mathsf{SIS}_{\mathsf{n,m,q},\beta}$ (or $\mathsf{ISIS}_{\mathsf{n,m,q},\beta}$) problem with non-negligible probablity is at least as hard as solving the decisional approximate shortest vector problem GapSVP_γ and the approximate shortest independent vectors problem SIVP_γ on arbitrary n-dimensional lattices (i.e. in the worst case) with overwhelming probability, for some $\gamma = \beta \cdot \mathrm{poly}(n)$.*

We refer the reader to [21] for a detailed discussion regarding the reductions.

While the SIS and ISIS problem can be used to construct primitives like one way functions, collision resistant hash functions and signatures, public-key encryption (and beyond) require the so-called "Learning With Errors" problem LWE [28] or its ring variant RLWE [29]. We define these next.

Definition 2.10 (LWE)**.** Let $q = q(n) \geq 2$ be an integer and let $\chi = \chi(n)$ be a distribution over $\mathbb{Z}$. The $\mathsf{LWE}_{\mathsf{n,q},\chi}$ problem is to distinguish the following two distributions: in the first distribution, sample $(\mathbf{a}_i, b_i)$ uniformly from $\mathbb{Z}_q^{n+1}$. In the second distribution, one first draws $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ uniformly and then samples $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^{n+1}$ by sampling $\mathbf{a}_i \leftarrow \mathbb{Z}_q^n$ uniformly, $e_i \leftarrow \chi$ and setting $b_i = \langle \mathbf{a}_i, \mathbf{s}\rangle + e_i$. The $\mathsf{LWE}_{\mathsf{n,q},\chi}$ assumption is that the $\mathsf{LWE}_{\mathsf{n,q},\chi}$ problem is infeasible.

We will also need the definition of a B-bounded distribution.

Definition 2.11 (B-bounded distribution)**.** A distribution ensemble $(\chi_n)_{n\in\mathbb{N}}$ is called B-bounded if

$$\Pr_{e\leftarrow\chi_n}(\|e\| > B) = \mathrm{negl}(n)$$

Here, $\mathrm{negl}(\cdot)$ refers to a function that decreases faster than the inverse of any polynomial.

Regev [28] proved that for certain moduli q and certain bounded error distributions χ, the $\mathsf{LWE}_{\mathsf{n,q},\chi}$ assumption is true as long as certain worst-case lattice problems are hard to solve using a quantum algorithm. This result was de-quantized by Peikert for exponential modulus [30] and by Brakerski, Langlois, Peikert, Regev, Oded and Stehlé for polynomial modulus [31].

Theorem 2.12. *For integer dimension n, prime integer q and integer $B \geq 2n$, there is an efficiently sampleable B bounded distribution χ such that if there exists an efficient (possibly quantum) algorithm that solves $\mathsf{LWE}_{\mathsf{n,q},\chi}$, then there is an efficient quantum algorithm for solving $\tilde{O}(qn^{1.5}/B)$ approximate worst case SIVP and GapSVP.*

2.2 Cryptographic Constructions

In this section, we discuss how the aforementioned hardness assumptions can be used to design cryptosystems. Due to space constraints we restrict our attention to the primitive of encryption. We describe the public key encryption system based on LWE defined by Regev [28].

Public Key Encryption Recall the notion of public key encryption. At a high level, a public key encryption scheme consists of the following algorithms:

$\mathsf{Setup}(1^n)$: This algorithm takes as input the security parameter (which can be used to fine tune the efficiency-security tradeoff in any construction) and outputs a public key PK and a secret key SK.

$\mathsf{Encrypt}(\mathsf{PK}, M)$: This algorithm takes as input public key PK and a message $M \in \{0,1\}$, and outputs a ciphertext CT.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}, \mathsf{CT})$: This algorithm takes as input the public key PK, the secret key SK and a ciphertext CT and outputs a message M or $\perp$.

Correctness requires that if $(\mathsf{PK}, \mathsf{SK})$ are generated honestly using Setup and CT is generated honestly using Encrypt on inputs (PK, M), then $\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}, \mathsf{CT})$ yields M as desired. Security requires that an encryption of M_0 is indistinguishable from an encryption of M_1 for any M_0, M_1.

We proceed to describe a public key encryption system designed by Regev [28], whose hardness is based on the LWE problem.

$\mathsf{Setup}(1^n)$: On input a security parameter n do:

1. Choose a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$.
2. Choose a uniformly random $\mathbf{s} \xleftarrow{R} \mathbb{Z}_q^n$.
3. Choose a noise vector $\mathbf{e} \leftarrow \chi^m$.
4. Set $\mathbf{b} = \mathbf{A}^\intercal \cdot \mathbf{s} + \mathbf{e}$.

Output $\mathsf{PK} = (\mathbf{A}, \mathbf{b})$ and $\mathsf{SK} = \mathbf{s}$.

$\mathsf{Encrypt}(\mathsf{PK}, M)$: On input public parameters PK and a message $M \in \{0,1\}$, do:

1. Choose a uniformly random vector $\mathbf{r} \xleftarrow{R} \{0,1\}^m$.
2. Compute $\mathbf{c}_0 = \mathbf{A} \cdot \mathbf{r}$ and $c_1 = \mathbf{r}^\intercal \mathbf{b} + M\lfloor \frac{q}{2} \rfloor$.

Output the ciphertext $\mathsf{CT} := (\mathbf{c}_0, c_1)$.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}, \mathsf{CT})$: On input the public parameters PK, the secret key $\mathsf{SK} = \mathbf{s}$ and a ciphertext $\mathsf{CT} = (\mathbf{c}_0, c_1)$, do:

1. Let $d = c_1 - \mathbf{c}_0^\intercal \mathbf{s}$.
2. If d is closer to $q/2$ than to 0 output 1, else output 0.

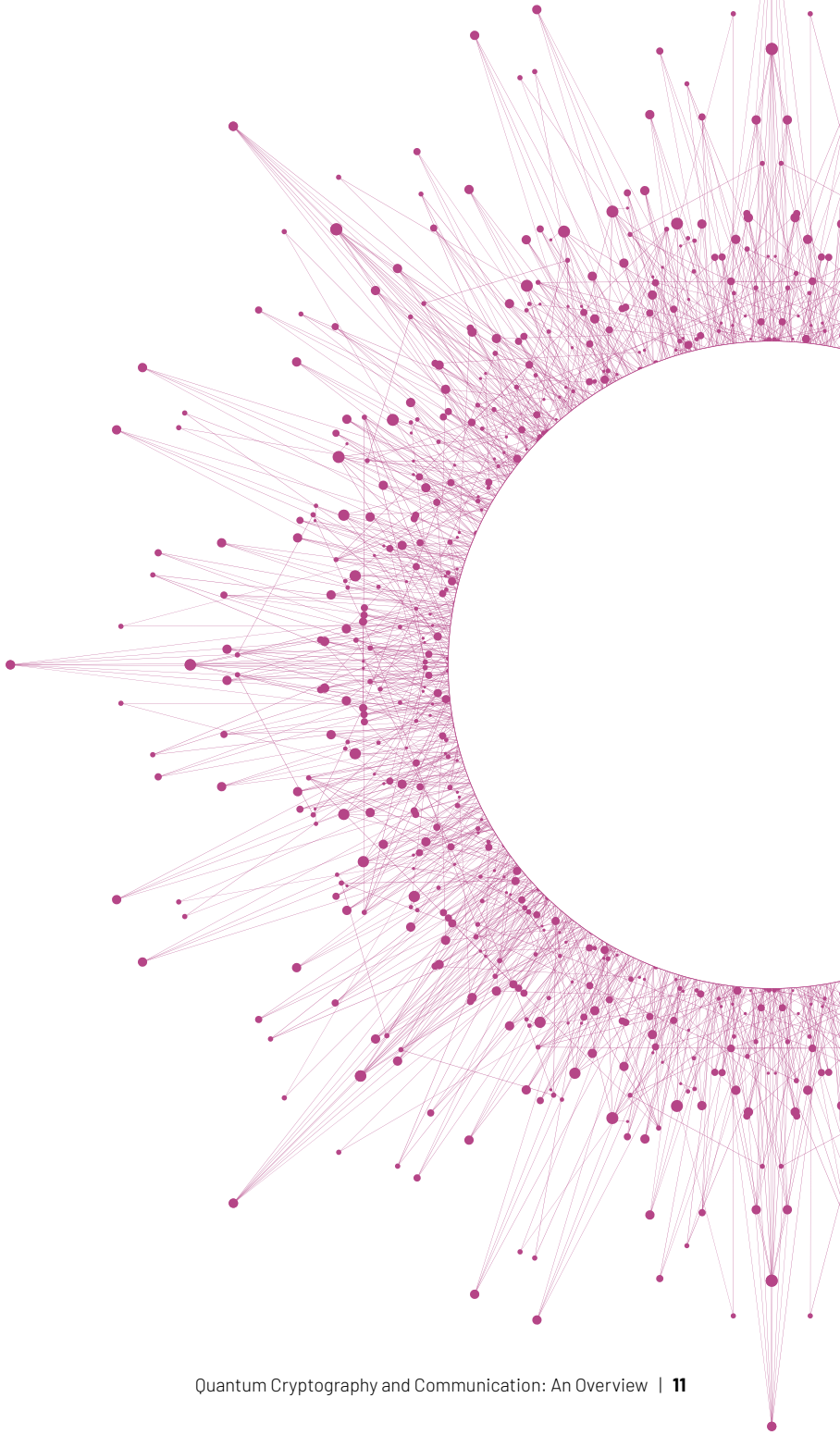
Correctness. To see that the encryption scheme is correct, we walk through the steps of decryption:

$$\begin{aligned} d &= c_1 - \mathbf{c}_0^\intercal \mathbf{s} \\ &= \left(\mathbf{r}^\intercal \mathbf{b} + M\lfloor \frac{q}{2} \rfloor\right) - \left(\mathbf{A} \cdot \mathbf{r}\right)^\intercal \mathbf{s} \\ &= \mathbf{r}^\intercal (\mathbf{A}^\intercal \cdot \mathbf{s} + \mathbf{e}) + M\lfloor \frac{q}{2} \rfloor - \mathbf{r}^\intercal \mathbf{A}^\intercal \mathbf{s} \\ &= \mathbf{r}^\intercal \mathbf{A}^\intercal \mathbf{s} + \mathbf{r}^\intercal \mathbf{e} + M\lfloor \frac{q}{2} \rfloor - \mathbf{r}^\intercal \mathbf{A}^\intercal \mathbf{s} \\ &= \mathbf{r}^\intercal \mathbf{e} + M\lfloor \frac{q}{2} \rfloor \end{aligned}$$

Since $\mathbf{r}$ is binary and $\mathbf{e}$ is chosen from a bounded distribution, it is possible to set the parameters so that $\mathbf{r}^\intercal \mathbf{e}$ is significantly smaller than $q/2$ and can be rounded off to recover the bit M.

Security. Security relies on the LWE assumption. Note that by the leftover hash lemma [32], for $m > 2n \log q$ and randomly chosen $\mathbf{r}$, the product $\mathbf{A} \cdot \mathbf{r} = \mathbf{u}$ (say) is uniform. Then, we observe that the ciphertext $(\mathbf{c}_0, c_1)$ is sampled from the LWE distribution as $(\mathbf{u}, \mathbf{u}^\intercal \mathbf{s} + \mathbf{r}^\intercal \mathbf{e} + M\lfloor \frac{q}{2} \rfloor)$, which by the LWE assumption is indistinguishable from uniform $(\mathbf{u}, v)$ which implies that M is hidden.

Summary. We presented a very high level overview of post quantum cryptography, with a focus on lattice based cryptography. This note is too short to contain anything beyond a flavour of the topic of discussion, which is as deep as it is beautiful. We refer the reader to [21] for an excellent survey of lattice based cryptography and to [19, 33] for more details on post quantum cryptography at large.



3

Quantum Key Distribution

Quantum Key Distribution (QKD) protocols establish information theoretic secure keys between two remote parties. by leveraging some of the unique properties of quantum mechanics, as explained below.

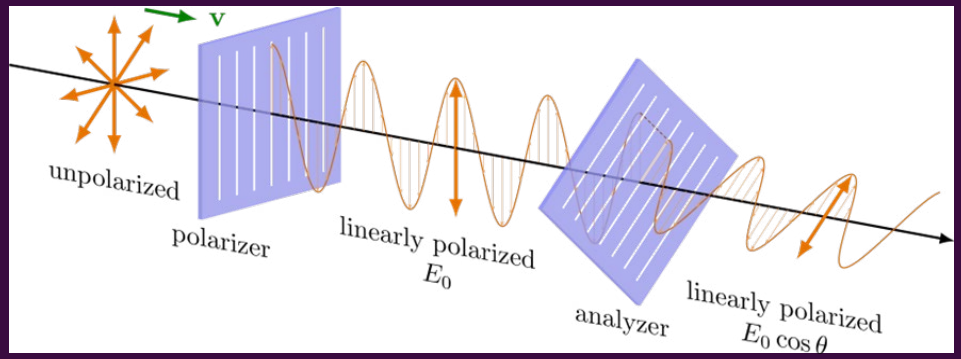


Figure 3.1: The direction of an oscillating electric field is referred to as its polarization. Optical devices that filter (polarizer) and measure (analyzer) this direction are commonly used in experiments [34]

Superposition is a cornerstone of quantum mechanics, describing the ability of a quantum system to exist in multiple states simultaneously until it is measured. For example, a photon, the quantum particle of light, can exist in a superposition of polarization states, such as horizontal (H) and vertical (V), or diagonal (D) and anti-diagonal (A). Thus, classical ideas of polarization, explained schematically in Fig. 3.1, are used to secure information by encoding bits on single photons.

In the context of QKD, the superposition principle enables the encoding of information in quantum states. The BB84 protocol, for instance, utilizes superposition by encoding bits in non- orthogonal bases (e.g., H/V and D/A). A bit value of '0' or '1' can be represented by the polarization of a photon in one basis, with the choice of basis adding an additional layer of security.

When a photon is transmitted as part of a quantum key, its exact state remains indeterminate to an eavesdropper. Any attempt to measure the photon's state without prior knowledge of the basis introduces errors due to the probabilistic nature of quantum measurement. This property ensures that key exchange using QKD is inherently resistant to interception.

Quantum measurements force a system in superposition to "collapse" into one of its possible states. The specific outcome of this collapse depends on the measurement basis and is probabilistic in nature. This principle plays a critical role in detecting eavesdropping. Consider a scenario in BB84 where an unauthorized party (commonly referred to as Eve) intercepts a photon intended for the legitimate recipient (Bob). Since Eve does not know the basis in which the photon was prepared, her measurement will collapse the quantum state, yielding a result in one basis while destroying information in the other. When Bob subsequently measures the photon in the correct basis, discrepancies between the expected and actual results reveal the presence of an eavesdropper.

Any attempt to measure quantum states leads to detectable disturbances, safeguarding the integrity of the key distribution process.

Heisenberg's uncertainty principle asserts that certain pairs of complementary proper- ties—such as position and momentum, or polarization along different axes—cannot be measured simultaneously with arbitrary precision. The act of measuring one property necessarily disturbs the other. These disturbances manifest as errors in the shared key, which can be detected during the error-checking phase of the protocol. The uncertainty principle ensures that the process of eavesdropping is fundamentally incompatible with the secure transmission of quantum keys. However, researchers continue to test the infallibility of every QKD implementation by devising attacks on the system.

For instance, in the BB84 protocol, information is encoded in the polarization states of photons using two sets of conjugate bases. If an eavesdropper attempts to measure the polarization in a mismatched basis, the uncertainty principle guarantees that the measurement process will disturb the photon's state resulting in a quantum bit error rate (QBER) above a baseline threshold that is expected on an undisturbed quantum channel.

Quantum entanglement is a phenomenon where two or more particles become correlated in such a way that the state of one particle is intrinsically linked to the state of the other, regardless of the distance separating them. When two particles are entangled, measuring the state of one immediately determines the state of the other, even if they are light-years apart—a phenomenon Einstein famously referred to as "spooky action at a distance."

Entanglement is exploited in QKD protocols such as E91 and BBM92, using entangled photon pairs to establish secure keys. The two parties (Alice and Bob) each receive one half of an entangled pair. The correlations between their measurements, governed by the principles of quantum mechanics,

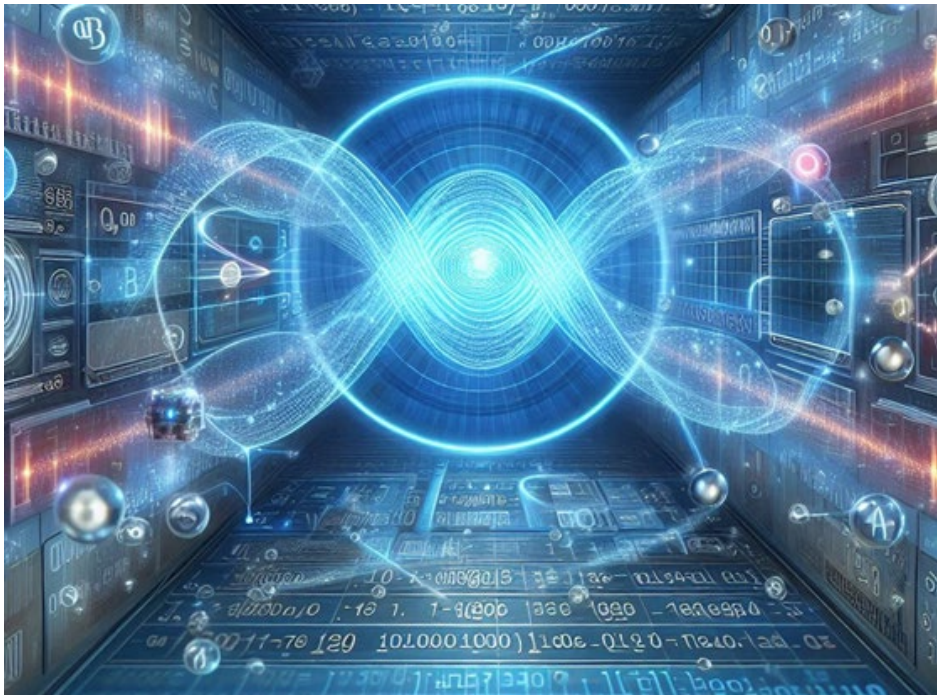
enable the generation of a shared secret key. Entanglement also provides a robust mechanism for detecting eavesdropping. If an unauthorized party attempts to intercept or measure one of the entangled particles, the correlations between the entangled pair are disrupted, indicating the presence of interference. The security of entanglement-based QKD can be verified using tests such as Bell's inequalities, which detect deviations from the expected quantum correlations.

The no-cloning theorem states that it is impossible to create an exact copy of an arbitrary unknown quantum state. This property ensures that quantum information cannot be duplicated without altering the original state, and it prevents an eavesdropper from creating perfect replicas of quantum states to gain information about the key. Any attempt to clone a quantum state introduces errors, which are subsequently detected during the reconciliation phase of the QKD protocol.

3.1 Real-world implementations

Information theoretic proofs ensure the security of QKD by making eavesdropping inherently detectable and by providing mechanisms to discard compromised keys. The security of QKD does not rely on assumptions about the computational capabilities of potential adversaries but relies on the laws of quantum mechanics. An eavesdropper will introduce a detectable error into the quantum channel, making his/her presence felt. There also remains the possibility of denial-of-service attacks by a malicious eavesdropper that can disrupt QKD. Thus, we state that a secret key established using QKD, based on the principles of quantum mechanics, can be secured against an eavesdropper. Implementing these principles in practical QKD systems involves significant technical challenges.

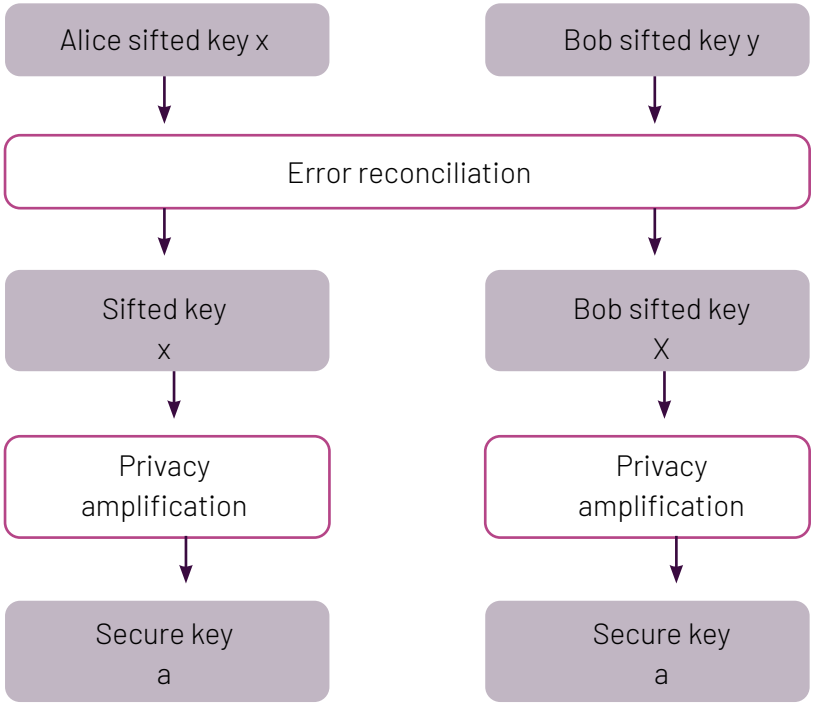
Single-photon sources, high-efficiency detectors, and low-loss optical fibers are critical for ensuring the fidelity of quantum states during transmission. Additionally, protocols must account for environmental



factors such as noise and signal attenuation, which can affect the accuracy of key distribution. Despite these challenges, advances in quantum technology have enabled the successful deployment of QKD systems.

- **Fiber-Based QKD:** Optical fibers are commonly used for transmitting quantum states over moderate distances of 100 km, or shorter distances when the fibre links are lossy. Advances in fiber technology and error-correction techniques have extended the reach of QKD systems to hundreds of kilometers.
- **Satellite-Based QKD:** Satellite systems, such as China's Micius satellite, leverage the principles of quantum mechanics to facilitate long-distance key distribution, overcoming the limitations of terrestrial optical fibers.

Figure 3.2: Classical post-processing steps that are used by Alice and Bob to share a secure key.



All QKD protocols involve many classical post-processing steps that the two authenticated parties (Alice and Bob) will follow, so as to establish the security of the shared secret key. These steps are shown schematically in Fig. 3.2. We now examine several prominent QKD protocols.

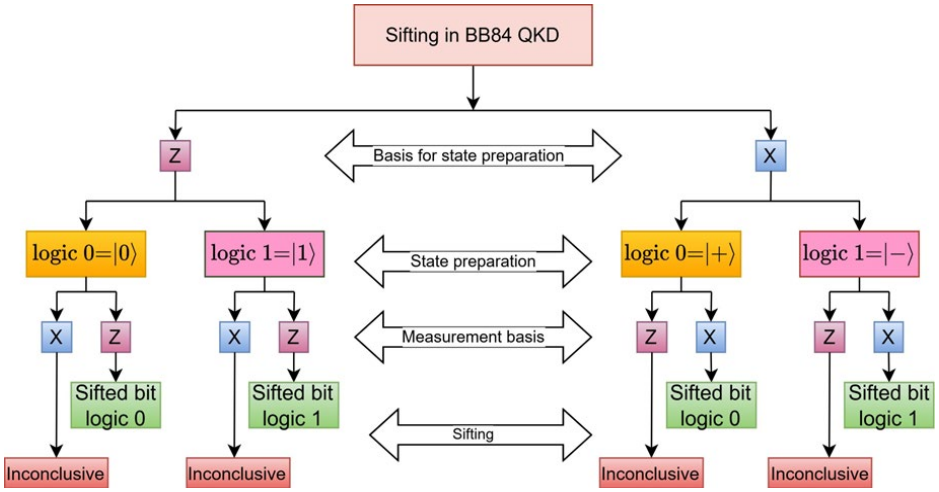
BB84 Protocol introduced by Charles Bennett and Gilles Brassard in 1984, the BB84 protocol is the first and most widely implemented QKD scheme [35]. It utilizes two pairs of conjugate bases for encoding information:

- **Rectilinear Basis (Z-basis):** Horizontal (0°) and Vertical (90°) polarizations.
- **Diagonal Basis (X-basis):** +45° and −45° polarizations. The protocol can be broken into specific steps

1. **Preparation**: The sender (Alice) randomly selects a bit value (0 or 1) and a basis (Z or X) to encode the bit on a photon.
2. **Transmission:** Alice sends the encoded photon to the receiver (Bob) over a quantum channel.
3. **Measurement:** Bob randomly chooses a basis (Z or X) to measure the incoming photon.
4. **Basis Reconciliation:** After transmission, Alice and Bob publicly compare their chosen bases without revealing the actual bit values.
5. **Key Sifting:** They retain only the bits where their bases matched, discarding the rest.
6. **Error Correction and Privacy Amplification:** To ensure the key's integrity and security, they perform error correction to rectify discrepancies and privacy amplification to reduce any partial information an eavesdropper might have gained.

Fig. 3.3 explains the steps in BB84 up to key sifting. Sifting comprises only those cases where the state preparation basis is the same as the measurement basis chosen at the receiver. Ideally, in this case, there should be no error. All other cases are discarded and not considered for sifting. The security of BB84 is rooted in the no-cloning theorem and the disturbance caused by measurement. Any eavesdropping attempt introduces detectable errors, allowing Alice and Bob to identify and mitigate potential security breaches.

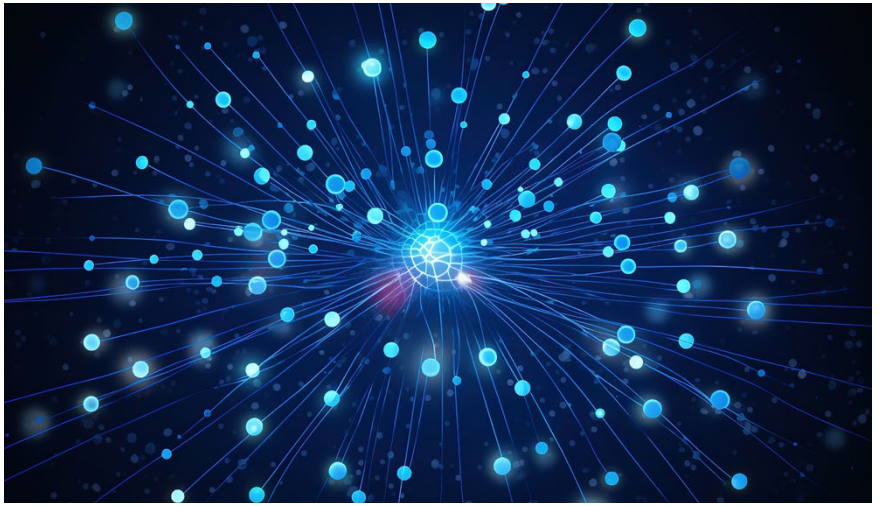
Figure 3.3: Sifting scheme in BB84 QKD protocol.



E91 Protocol proposed by Artur Ekert in 1991, the E91 protocol employs quantum entanglement to establish secure keys [36]. It leverages the correlations between entangled particles and the violation of Bell's inequalities to detect eavesdropping.

The protocol works as follows.

1. **Entanglement Generation:** A source generates pairs of polarization entangled photons and sends one photon to Alice and the other to Bob.
2. **Measurement:** Both parties independently choose one of three measurement settings (corresponding to different polarizer angles) and record their results.
3. **Correlation Analysis:** After multiple rounds, Alice and Bob publicly share their chosen measurement settings (but not the outcomes) and identify the instances where their settings were compatible.
4. **Key Generation:** From the compatible measurements, they derive correlated bits to form the key.
5. **Security Verification:** By analyzing the statistical correlations and checking for violations of Bell's inequalities, they can detect any eavesdropping attempts.



The E91 protocol's security is based on the fundamental properties of entanglement and the statistical correlations that cannot be replicated by classical means. Any eavesdropping disrupts these correlations, making it detectable.

B92 Protocol developed by Charles Bennett in 1992, the B92 protocol is a simplified version of BB84, utilizing only two non-orthogonal quantum states for encoding information[37]. It follows a simpler prepare and measure approach.

1. **Preparation:** Alice randomly selects a bit value (0 or 1) and encodes it into one of two non-orthogonal states (e.g., $|\psi 0\rangle$ and $|\psi 1\rangle$.
2. **Transmission:** Alice sends the encoded photon to Bob.
3. **Measurement:** Bob uses a measurement basis that can distinguish between the two states but with a certain probability of inconclusive results.
4. **Key Sifting:** Bob informs Alice of the instances where he obtained a conclusive result. They then use these instances to form the key.

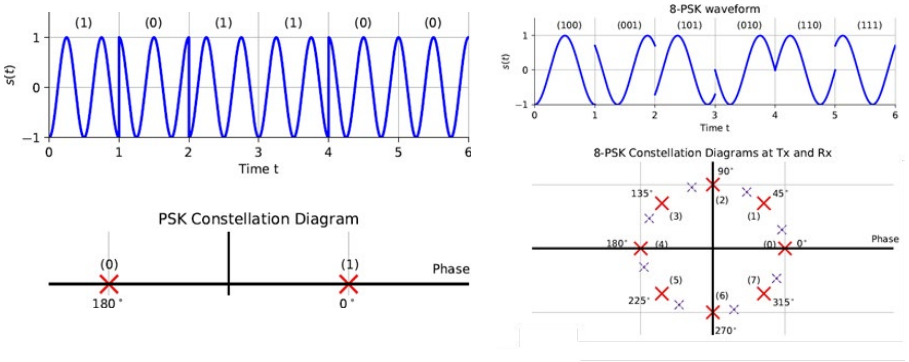
The use of non-orthogonal states ensures that any eavesdropping introduces errors, as an eavesdropper cannot perfectly distinguish between the states without disturbing them.

SARG04 Protocol introduced in 2004 by Scarani, Ac´ın, Ribordy, and Gisin, the SARG04 protocol is a variation of BB84, designed to be more robust against photon-number-splitting (PNS) attacks[38].

1. **Preparation:** Alice prepares photons in one of the four BB84 states.
2. **Transmission:** Alice sends the photons to Bob.
3. **Measurement:** Bob randomly chooses a basis (Z or X) to measure each photon.
4. **Announcement:** Alice announces two non-orthogonal states, one of which corresponds to the sent photon.
5. **Key Sifting:** Bob determines if his measurement result matches exactly one of the announced states. If it does, they sift a bit; otherwise, they discard it.

By associating each state with two possible bit values, SARG04 increases the difficulty for an eavesdropper to gain information without detection, enhancing security against certain attacks. However, implementing the protocol becomes harder.

Figure 3.4: Encoding of information in the phase of an electromagnetic wave[39]. Channel imperfections can lead to a change in the constellation, e.g., as shown between in the 8-PSK constellation as a rotation of the constellation (purple versus red crosses).



Continuous-Variable QKD (CV-QKD), unlike discrete-variable protocols (BB84, E91), employs continuous variables, such as the quadratures of the electromagnetic field [40], to encode information, but is limited by noise in the channel and offers secure communications over shorter links. The techniques used are borrowed heavily from phase-shift keying, shown schematically in Fig. 3.4, commonly used in wireless communications.

1. **Preparation**: Alice modulates the amplitude and phase of a coherent state to encode information.
2. **Transmission**: The modulated coherent state is transmitted to Bob over a quantum channel.
3. **Measurement:** Bob performs homodyne or heterodyne detection to measure the quadratures of the received state.
4. **Key Extraction:** Alice and Bob use classical post-processing techniques, including error correction and privacy amplification, to distill a secure key from their correlated data.

CV-QKD protocols can achieve high key rates and are compatible with existing telecommu- nication infrastructure [41]. Its security relies on the statistical distributions that govern detector shot noise, and the distribution of photons with low mean photon numbers. However, as seen in Fig. 3.4 it is susceptible to channel imperfections that will affect the key rate.

Measurement-Device-Independent QKD (MDI-QKD) was introduced to address vulnera- bilities associated with imperfections in detectors, which can be exploited through attacks like detector blinding [42]. MDI-QKD eliminates all side-channel vulnerabilities related to measurement devices, significantly enhancing the security of practical QKD systems.

MDI-QKD involves the following steps:

1. **Photon Generation and Transmission:**Both Alice and Bob independently prepare weak coherent states or single-photon states encoded with random bits. These states are sent to a third-party, Charlie, who acts as an untrusted intermediary.
2. **Bell-State Measurement (BSM):** Charlie performs a Bell-state measurement (BSM) on the incoming photons. The outcome of the BSM does not reveal any information about the secret key but allows Alice and Bob to correlate their states.
3. **Key Sifting:** Alice and Bob use classical communication over a public channel to reconcile the results of the BSM and their transmitted data. The public channel does not compromise security, as the actual key bits are not transmitted directly.
4. **Error Correction and Privacy Amplification:** As with other protocols, error correction and privacy amplification are applied to generate the final shared key.

The main advantage of MDI-QKD is its resilience to all detector-side-channel attacks, as the security does not depend on trusting the measurement device. Any malicious behavior by Charlie introduces errors that Alice and Bob can detect. Additionally, MDI-QKD enables longer communication distances by combining its security benefits with advancements in quantum technology.

Floodlight QKD is an innovative protocol designed to achieve high secret key rates over metropolitan distances, making it suitable for use in quantum-secure networks where throughput is critical [43]. The protocol is characterized by its use of strong optical pulses as a "floodlight" and weak modulated pulses to encode the key bits.

1. **Floodlight Transmission:** Alice generates strong coherent pulses (floodlight pulses) that are sent to Bob to provide a clock signal and enhance the signal-to-noise ratio.
2. **Key Encoding:** Alice embeds her key information in weak pulses that are time- synchronized with the floodlight pulses. The weak pulses are quantum states used to carry the encoded key bits.
3. **Detection at Bob's End:** Bob detects the weak pulses using time-correlated single-photon detectors, with the floodlight pulses serving to mitigate the effects of environmental noise.
4. **Post-Processing:** Bob uses the time-correlated detection events to decode the key bits, followed by reconciliation and privacy amplification.

Floodlight QKD provides high key rates because the floodlight pulses improve the signal quality, reducing errors caused by noise. The protocol maintains quantum security by carefully balancing the use of classical and quantum light sources [44]. This hybrid approach makes it particularly attractive for real-world applications in dense urban areas.

Twin-Field QKD (TF-QKD) dramatically extends the distance of secure communication, overcoming the limitations imposed by the linear scaling of key rates with channel transmission loss in traditional QKD systems. First proposed in 2018, TF-QKD leverages quantum interference of weak coherent states sent from Alice and Bob to a central relay.

1. **Preparation:** Alice and Bob independently generate weak coherent states modulated with random phase and amplitude, encoding their respective key information.
2. **Interference at Relay:** The states from Alice and Bob are sent to an untrusted relay, which performs interference measurements. The interference pattern depends on the phase difference between the incoming states but does not reveal the actual key bits.
3. **Key Sifting:** Based on the interference outcomes and their initial modulation settings, Alice and Bob establish correlations in their encoded bits.
4. **Error Correction and Privacy Amplification:** Classical post-processing, including error correction and privacy amplification, is used to reconcile the key and remove any partial information potentially available to an eavesdropper.

TF-QKD significantly improves the distance over which secure communication is possible by relying on quantum interference rather than the direct transmission of photons. This feature allows key rates to scale with the square root of the channel transmission efficiency, making it more efficient than conventional QKD protocols over long distances.

Several variations of TF-QKD have been developed to optimize its performance and address practical challenges, including:

- **Phase-Matching QKD:** Improves the stability of interference patterns by actively stabilizing the relative phase between Alice and Bob.
- **Asymmetric TF-QKD:** Allows for asymmetric link distances between Alice and the relay versus Bob and the relay, making it more practical for real-world deployment.

Tomamichel and Leverrier provide a comprehensive security analysis for quantum key distri- bution, establishing rigorous trade-offs between various protocol and security parameters [45]. Proofs for the security of different protocols, under different types of attacks, is an ongoing area of research in quantum information.

Table 1: Comparison of QKD implementations worldwide. SKR = secure key rate.

Implementation	Location	Year	Distance	SKR	Tech.	Duration
DARPA Quantum Network	MA, USA	2004	10 nodes	Variable	Fiber-optic	18 months
SECOQC Network	Vienna	2008	200 km	Variable	Fiber-optic	6 months
SwissQuantum Network	Geneva	2009	67 km	Variable	Fiber-optic	1 year
Tokyo QKD Network	Tokyo	2010	45 km	1 Mbps	Fiber-optic	16 months
Beijing-Shanghai Trunk Line	China	2017	2,032 km	Variable	Fiber-optic	Ongoing
Micius Satellite	China	2016	1,200 km	1 kbps	Free space	2 years
Los Alamos Network	NM, USA	2011	25 km	Variable	Fibre-optic	2 years
Singapore's NQSN+	Singapore	2023	Nationwide	Variable	Fiber-optic	Ongoing
Eagle-1 Satellite	Europe	2025	Global	Variable	Free space	Planned
MAQAN	India	2024	5 node	Variable	Fiber-optic	7 months

Table 1 offers a quick comparison of different implementations. Each QKD protocol offers unique advantages and addresses specific challenges in achieving secure communication. From the foundational BB84 to advanced protocols like Twin-Field QKD and Floodlight QKD, the landscape of QKD continues to evolve, driven by the dual goals of enhancing security and enabling practical implementation in real-world networks. The choice of protocol depends on factors such as the desired communication distance, the level of security required, and the technical constraints of the deployment environment.

3.2 Securing QKD

As an innovative key distribution method working on the basic principles of quantum mechanics, QKD can achieve information-theoretic security in principle but is limited by practical considerations.

Different protocols were proposed to improve the practical security and performance of QKD. For example,

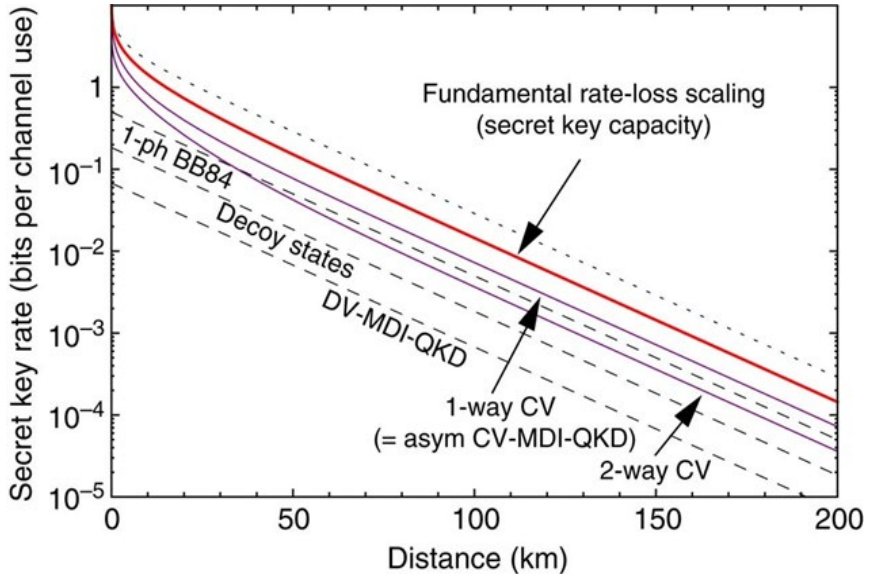
1. Prepare-and-measure protocol proposed by Shor and Preskill in 2000[46]
2. Differential phase shift (DPS) proposed by Inoue et al. in 2002 [47]
3. The decoy state proposed by Hwang et al. in 2003[48]
4. The Scarani-Ac´ın-Ribordy-Gisin protocol proposed in 2004[38]
5. Coherent one way (COW) proposed by Stucki et al. in 2005[49]
6. Measurement-device independent (MDI) proposed by Lo et al. in 2012[42]
7. Round-robin DPS protocol proposed by Sasaki et al. in 2014[50]

All aim to address the issues of device imperfections. These are further described from a historical perspective in Sec. 3.3.

In addition, we must consider limitations imposed on us by

- **Photon Loss:** Over long distances, the probability of photon loss increases, reducing the efficiency of QKD systems. We expect a typical fibre loss of 0.2 dB/km at 1550 nm (C-band of the ITU grid), which means that appproximately 1 in 100 transmitted photons will reach the receiver over a fiber of length 100 km.
- **Key Rate Limitations:** The rate at which secure keys can be generated is limited by factors such as detector efficiency and channel capacity. Most commercial deployments use single photon avalanche diode (SPAD) detectors that have efficiencies of 10-20% with hold-off times of 1 – 10 μs. This automatically limits raw key rates to less than 1 Mbps and a secure key rate (SKR) to a few tens of kbps.

Figure 3.5: Fundamental limits of repeaterless quantum communications[51].



These considerations are well described in recent review articles that summarize the challenges of extending the use of QKD protocols to longer distances[41, 51], without repeaters, and captured in Fig. 3.5.

3.3 Historical Perspectives

Since the BB84 QKD protocol was proposed, researchers have studied its security proofs. Lo-Chau's proof[52] has a relatively intuitive physical image based on the idea of entanglement, but it requires.

Alice and Bob to have quantum computers and be able to perform quantum-logical operations on optical signals. Shor-Preskill showed that the information theory security of the BB84 protocol could also be demonstrated based on classical error correction and privacy amplification procedures, enabling practical QKD deployments[46].

After Shor and Preskill's work, the security proof of BB84 protocol in the ideal situation was completed under the assumption that Alice and Bob's devices are ideal. However, the imperfections of practical devices introduce deviations from the idealized models used in such security analyses and will threaten any practical QKD system. In 2000, G. Brassard et al. pointed out that weak coherent light used in real systems may lead to photon number splitting (PNS) attacks, which significantly compromise the security of QKD over long distance[53]. In doing so, he brought widespread attention to the impact of device imperfections on QKD security.

Hwang in 2003 presented the decoy state method that could defend against the photon number splitting (PNS) attack[48]. However, the scheme proposed was a solution against PNS attack only. In the face of PNS attacks, it became necessary to revise the security model of QKD protocol based on real systems for weak coherent light sources. The analysis by Gottesman-Lo-Lutkenhaus-Preskill (GLLP), in 2004, gave the security proof of QKD under actual non-ideal devices based on certain assumptions[54]. The "GLLP"

security framework provides an analytical approach to the problem of a multi-photon light source in theory. In particular, the secure information rate is derived from the single-photon components from weak coherent sources. Alice and Bob characterize their devices to see how much deviation there is from the ideal ones used in the security proofs, and adopt typical distance measures like fidelity and trace distance to quantify the deviation. After this analysis, we use the GLLP key rate formula to analyze the security of the BB84 implementation. However, the GLLP security analysis pessimistically assumes all the multi-photon pulses unsuitable for key generation.

In 2005, Lo et al. presented the decoy state QKD. Here, Alice randomly prepares and sends pulses of different intensities at random, and Bob measures and records these pulses according to the basic BB84 protocol. Finally, according to the intensity selection information published by Alice, Bob makes classification statistics for different intensities and solves a series of linear equations. The qubit error rate and detection probability of a single photon can be accurately estimated using this method.

In BB84 QKD, the states must be prepared in two mutually unbiased basis to ensure the security of the keys. However, the use of weak coherent source will not produce the states that satisfy this condition. This leaks sme information about the basis choice of Alice and so is a threat to security. This is called basis dependent flaw and in general is an encoding flaw. Although Gottesman et al. allow the security proof to account for encoding flaws, the key rate drops dramatically under their framework. To address this limitation, researchers have focused on the practical security of QKD systems at the transmitter, proposing alternative analysis methods beyond the GLLP framework. One notable example is the loss-tolerant security analysis framework, which improves the key rate of QKD systems operating over long distances with imperfect sources. The security analysis is carried out considering the source with defects to estimate the information leakage.Loss-tolerant protocol was proposed by Tamaki et al. in 2014 that enables QKD systems to tolerate channel loss in the presence of source flaws (Yin et al., 2014). On the basis of the assumption that the single-photon components of the states prepared by transmitter remain inside a two-dimensional Hilbert space, it was shown that attacker cannot enhance state preparation flaws by exploiting the channel loss, and attacker's information can be bounded by the rejected data analysis. The previous.

loss-tolerant protocol was further developed and demonstrated experimentally for decoy-state BB84 (Xu, Wei et al., 2015; Boaron et al., 2018) and MDI-QKD (G.-Z. Tang et al., 2016). Additionally, researchers have proposed a security analysis method based on the construction of Gram matrices and numerical optimization. This approach allows for the analysis of multiple imperfections in QKD sources, further advancing the practical security of these systems [55, 56].

Attack methods and defense schemes for QKD systems continue to emerge. The single photon detector (SPD) used in the actual QKD system is particularly vulnerable to external influences due to its own characteristics, and a large number of SPD attacks have been studied. For example, the pseudo-state attack proposed in 2005, the time-shift attack proposed in 2007, the blinding attack proposed in 2010, and the fluorescence attack proposed in 2016. To defend against detector attacks, measurement-device-independent quantum key distribution (MDI-QKD) was independently proposed by Lo's group at the University of Toronto in Canada and Braunstein's group at the University of York in the United Kingdom in 2012. In MDI-QKD protocol, both Alice and Bob are transmitters, and they transmit signals to an untrusted third-party Charlie, who is supposed to perform a Bell state measurement. Based on the idea of entanglement exchange and the time-reversal symmetry in entangled state distribution, MDI-QKD can neutralize all attacks against the receiver in a single step while achieving performance demonstration similar to that of traditional quantum key distribution. At

the same time, the protocol can be combined with decoy state scheme to further enhance its security. Inspired by the MDI-QKD protocol, Lucamarini et al. from Toshiba Cambridge Research Institute in the UK proposed a new QKD protocol in 2018: the twin-field QKD protocol (TF-QKD) which shows the possibility of overcoming the secret key capacity.

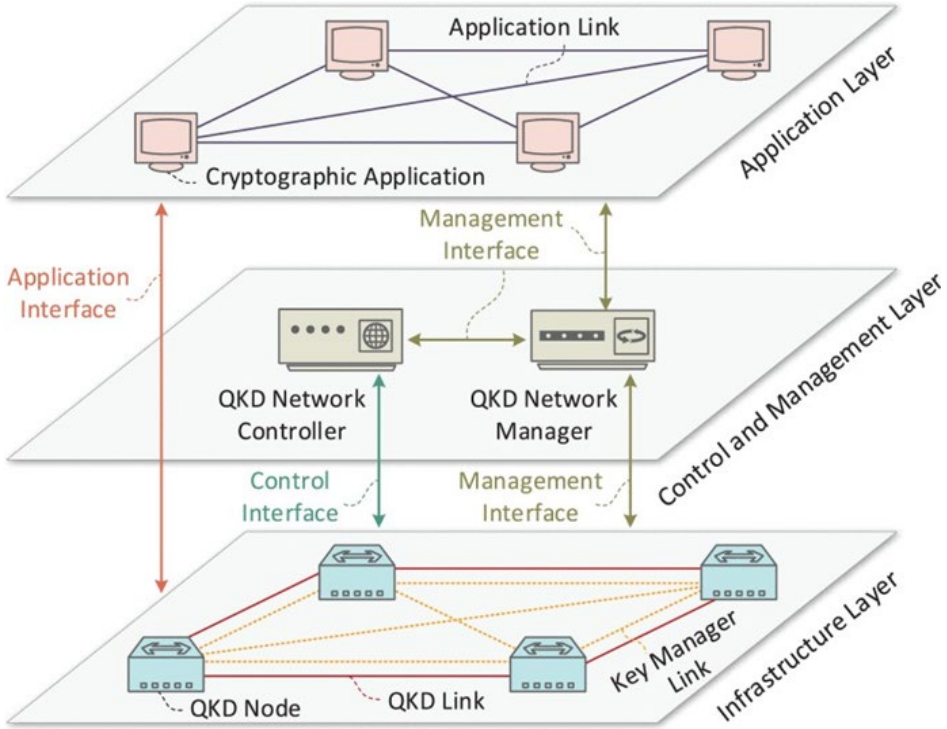
In the theory of CV-QKD security proof, in 2002, F. Grosshans and P. Grangier proposed GG02 protocol. The reverse coordination algorithm was proposed by F. Grosshans et al. in 2003. In 2004, C. Weedbrook et al. proposed the "No-switching" protocol based on GG02 protocol, using heterodyne detection instead of homodyne detection. In 2006, M. Navascues and R. Garcia-Patron respectively proved that the optimal collective eavesdropping of the Gauss modulated continuous variable QKD protocol is Gaussian attack. In 2009, R. Renner and J.I. Cirac used the quantum de Finetti theorem for infinite dimensional systems to extend the security of collective eavesdropping to coherent eavesdropping in general. The asymptotic security proof for unidirectional CV-QKD protocols under the assumption of an infinite data set is obtained. Subsequent studies on the security proof of finite code long-term application and combination have been proposed in recent years. In 2017, the security rate under coherent eavesdropping was further refined to improve the performance of the protocol. In the future, with the continuous improvement of security proof methods for QKD, the security of practical QKD will be further improved.

The continuous advancement of theoretical and practical security analysis in QKD provides solid foundations and the basis for the security evaluation of QKD.

3.4 QKD Networks

Securing of secret keys between two parties also requires us to develop mechanisms to support quantum key distribution networks (QKD). These networks consist of a physical layer that exchanges keys, a key management layer, and an application layer with the aim of sharing a secret key between two or more QKD nodes interconnected by optical fiber or free space links, as shown schematically in Fig. 3.6 [57, 58]. Many of these functionalities are currently being discussed in working groups of different standards bodies, such as ITU, IEEE, IEC/ISO and IETE.

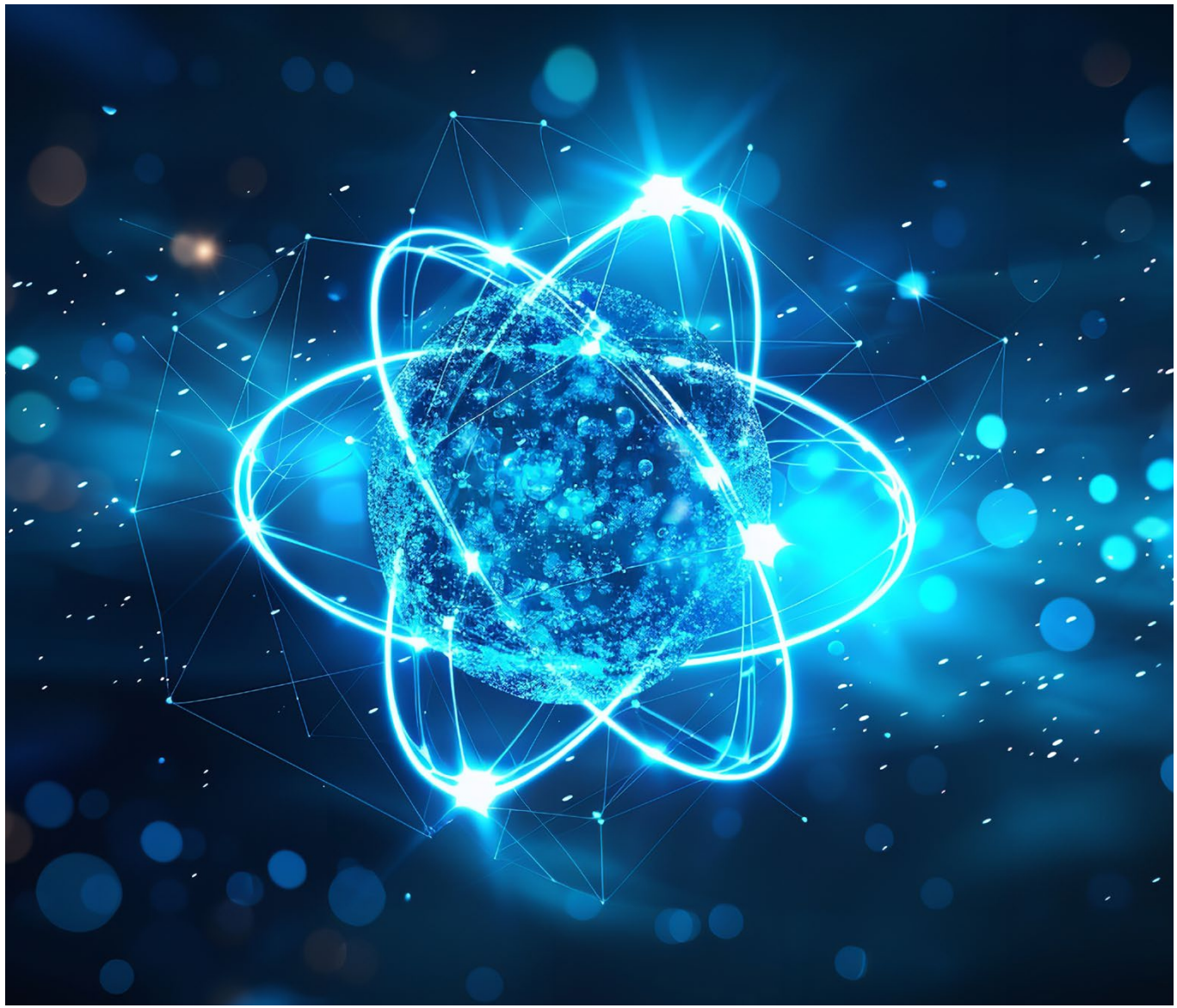
Figure 3.6: Schema for a quantum key distribution network [57].



Note that a QKDN is different from a quantum network. While QKD is distributing a classical key using the quantum properties of light, a quantum network will attempt to connect resources such as quantum computers or quantum sensors using ideas such as entanglement distillation or entanglement distribution. These ideas are described in further detail in Sec. 5.

Summary

The fundamental principles of quantum mechanics—superposition, quantum measure- ment, the uncertainty principle, entanglement, and the no-cloning theorem—form the theoretical backbone of QKD. These principles not only ensure the security of quantum key exchange but also distinguish QKD from classical cryptographic methods by offering a level of security that is invulnerable to technological advancements. As research in quantum technology progresses, these principles continue to guide the development of more robust, scalable, and practical QKD networks, paving the way for secure communication in the quantum era.



4

Quantum Secret Sharing

Secret sharing scheme is a protocol to distribute information among untrusted parties so that only certain authorized subsets of parties can recover the secret. The subsets of parties that are not authorized cannot recover the secret.

Secret sharing scheme is a protocol to distribute information among untrusted parties so that only certain authorized subsets of parties can recover the secret. The subsets of parties that are not authorized cannot recover the secret. By distributing the secret among various parties, secret sharing also provides a means to combat malicious parties from corrupting the secret.

A simple classical example involving n parties would be the following. Let a dealer distribute a classical secret $s \in Z_N$ where $Z_N = \{0, 1, \ldots, N-1\}$ is the set of integers modulo N . The dealer can distribute a random symbol $r_i \in Z_N$ to each of the parties $1 \leq i \leq n-1$. To the nth party the that posses r_i has no information about the secret since r_i is a random symbol and independent of the secret s. The last party also has no information about the secret since its symbol is randomly distributed in Z_N . Intuitively, a subset of parties S, has a system of $|S|$ linear equations in n variables. If $|S| < n$ then S has only at most $|S| < n$ equations so they cannot recover s. On the other hand, when all the n parties collaborate they can solve for s by simply taking the sum of all their shares.

Classical secret sharing was initiated by Shamir and Blakely independently. Since then the field has been extensively studied. In 1999, Hillery et al. initiated the study of quantum secret sharing [59]. Classical secret sharing requires secure communication channels to be safe guarded from eavesdroppers. One could attempt to use QKD to first establish secure communication channels between the various parties and then employ the classical protocol. However, this is cumbersome; therefore, Hillery et al. proposed a direct method using multipartite entangled states. This is the first motivation for studying quantum secret sharing schemes. In addition, these schemes are also able to overcome certain restrictions of the classical schemes.

The second reason being that we would like to share a quantum secret ie a quantum state as opposed to a classical state. Then a classical protocol will not suffice. Cleve et al provided schemes for sharing quantum secrets [60]. Quantum secret sharing schemes for sharing quantum secrets have sometimes been termed quantum state sharing to distinguish them schemes that employ quantum resources for sharing classical secrets. In this note, we will focus on the secret sharing schemes where the secret is assumed to be quantum.

4.1 Quantum secret sharing model and terminology

A secret sharing scheme among n parties involves the following ingredients. There is a distinguished party called the dealer who distributes the secret. The dealer encodes the secret before distributing the secret to the parties. The state given to each of the parties is called the share of the party. We denote the share of the jth party as Wj. The collection of all authorized subsets is called the access structure of the secret sharing scheme. The access structure is often denoted as Γ. Suppose A is an authorized set, then it follows that $B \supseteq A$ is also an authorized set. Therefore the access structure satisfies a monotonic property. The no-cloning theorem requires that we cannot have two disjoint authorized sets. So access structures of sharing quantum secrets are more restricted than the classical schemes. An access structure such that no two authorized sets are disjoint is called a quantum access structure.

A subset is said to be unauthorized if it has no information about the secret. The collection of all unauthorized sets is called the adversary structure. We shall denote the adversary structure by A. Some schemes can also have subsets which can have partial information about the secret but cannot fully recover the secret. Such subsets are called intermediate sets. We shall denote the collection of all intermediate sets as I. We denote by [n] = {1, 2, . . . , n}. The collection of all subsets of [n] is denoted by 2[n]. Then clearly $\Gamma \cup A \cup I = 2[n]$. A secret sharing scheme is said to be perfect if there are no intermediate sets and non-perfect otherwise.

An encoding E from the state space of the secret to the state space of all the parties is said to realize a quantum secret sharing scheme for a quantum access structure $\Gamma \subseteq 2$ if the following conditions are satisfied.

1. **Recoverability:** Any authorized set $A \in \Gamma$ can recover the secret.
2. **Secrecy:** Any unauthorized $B \in A$ cannot recover the secret and has no information about the secret.

Note that we have incorporated the constraint due to the no-cloning theorem into the access structure itself[1]. A consequence of the no-cloning theorem is that the complement of any authorized set must be unauthorized. This condition along with the above two conditions completely characterizes the conditions for a quantum secret sharing scheme.

[1] *A quantum secret sharing scheme for classical secrets is not required to satisfy the no-cloning theorem.*

4.2 An illustrative example

We give an illustrative example of a quantum secret sharing schemes over qutrits ie ternary quantum systems, see Cleve et al. [60]. This will highlight the key parts of the quantum secret sharing protocol. The first step is to design a suitable encoding for the secret. Consider the following encoding.

$$|s\rangle \mapsto \sum_{r\in\mathbb{Z}_3} |r\rangle\,|s+r\rangle\,|r+2s\rangle \tag{4.1a}$$

Here we have ignored the normalization factors for clarity. An arbitrary quantum state $|\psi\rangle = \sum_i \alpha_i\,|i\rangle$ is encoded using the linearity of the above map. A single party does not access to the secret; we can verify this by tracing out the other two parties and we can see that the reduced state is a fully mixed state.

The second step is to demonstrate that authorized parties can recover the secret. In this particular scheme, any two parties can recover the secret. We shall illustrate how parties {1,3} recover the secret. Then they can perform the following sequence of operations. We have access only to the first and third party shares. We can subtract the share of the third party from the first to obtain

$$\sum_{s\in\mathbb{Z}_3}\alpha_s\sum_{r\in\mathbb{Z}_3}|-2s\rangle\,|r+s\rangle\,|r+2s\rangle = \sum_{s\in\mathbb{Z}_3}\alpha_s\sum_{r\in\mathbb{Z}_3}|s\rangle\,|r+s\rangle\,|r+2s\rangle \tag{4.2}$$

Then we can subtract the first share from the third.

$$\sum_{s\in\mathbb{Z}_3}\alpha_s\sum_{r\in\mathbb{Z}_3}|s\rangle\,|r+s\rangle\,|r+s\rangle \overset{(a)}{=} \sum_{s\in\mathbb{Z}_3}\alpha_s\sum_{t\in\mathbb{Z}_3}|s\rangle\,|t\rangle\,|t\rangle \overset{(b)}{=} \left(\sum_{s\in\mathbb{Z}_3}\alpha_s\,|s\rangle\right)\left(\sum_{t\in\mathbb{Z}_3}|t\rangle\,|t\rangle\right) \tag{4.3}$$

where state after (a) is obtained by a change of index. In step (b) we notice that the secret is completely disentangled from the other parties and is present in the share of the first party. Moreover also note that the remaining shares have no information about the secret due to the no-cloning theorem.

4.3 Some important classes of quantum secret sharing schemes

Boradly, we can classify quantum secret sharing schemes into perfect schemes and non-perfect schemes. The most important class of perfect schemes are the threshold schemes [60,61]. A $((t,n))$ quantum threshold scheme (QTS) is a quantum secret sharing scheme with n parties where t or more parties can recover the secret while $z \le t-1$ parties have no information about the secret. In other words,

$$\Gamma = \{A \subseteq [n] : |A| \ge t\} \tag{4.4a}$$
$$\mathcal{A} = \{B \subseteq [n] : |B| < t\} \tag{4.4b}$$

This is by far the most studied quantum secret sharing scheme. They can also be the building blocks for other types of quantum secret sharing schemes.

Among the non-perfect schemes the most important class of schemes are the ramp quantum secret sharing (RQSS) schemes [62,63]. (Under some circumstances a ramp QSS scheme can also be a perfect scheme.) It is denoted $((t,n;z))$ and is defined as follows. Every subset A of size $|A| \ge t$ can recover the secret while every subset B of size $|B| \le z$ has no information about the secret. Sets of size in the range $\{z+1,\ldots,t-1\}$ are intermediate sets. Here t is said to be the threshold and z is said to be the secrecy parameter. We can see that if $z = t-1$, then we have a $((t,n))$ quantum threshold scheme. Every quantum secret sharing scheme with a general access structure can be regarded as a ramp scheme.

4.4 Metrics of performance for quantum secret sharing schemes

We briefly review some of the metrics in quantifying the performance of quantum secret sharing scheme.

- Share size. One of the important metrics for QSS schemes it the size of the share. It has been shown that for perfect schemes the size of the share is at least as large as the size of the secret to be shared.
- Rate. This is a parameter that is closely related to the share size and it is defined to be be as $\rho = \max_j \frac{\dim S}{\dim W_j}$ where $\dim(S)$ is the dimension of the secret and $\dim(W_j)$ is the dimension of the jth share. Alternative metrics to the information rate are the average information rate and the information ratio (which is the inverse of the information rate).
- Storage cost. This is defined as the average of all the share sizes W_j. Ogawa et al. [62] showed that for a $((t,n;z))$ RQSS scheme the average share size is bounded as

$$\frac{1}{n}\sum_j W_j \ge \frac{\dim(S)}{t-z} \tag{4.5}$$

- Communication complexity. When the recovery is defined under the combiner model, this refers to the amount of quantum communication that is required to recover the secret. Given an authorized set A we define the quantum communication cost of recovery for the set A as $\mathrm{CC}_n(A)$. Given an arbitrary scheme we are often interested in the communication cost for sets of a given size in which case we denote

$$\mathrm{CC}_n(d) = \max_{A:|A|=d} \mathrm{CC}_n(A) \tag{4.6}$$

4.5 Some important problems and directions for research

There are several problems of interest for further research in quantum secret sharing. Below we list some of them.

(a) **Efficient construction of quantum secret sharing schemes for general access structures.**
Since quantum secret sharing schemes can be used to share classical as well as quantum states, we can naturally classify them into two categories based on the type of secret being shared. The work of Hillery et al. [59] emphasized the sharing of classical secrets while that of Cleve

et al. [60] focussed on quantum secrets. Since then there has been a substantial body of work around in quantum secret sharing both for classical as well as quantum secrets. Arguably, the emphasis of the schemes sharing classical secrets has been the threshold scheme. There has been little and sporadic work on the construction of the quantum secret sharing schemes with arbitrary access structures. But non-threshold access structures arise naturally when there is a heterogeneity among the participants. Gottesman had characterized QSS schemes for classical secrets and also provided a construction for the threshold schemes [61]. Building upon this characterization, certain families of quantum codes were shown to lead to quantum secret sharing schemes for classical secrets [64]. Certain access structures that cannot be realized classically given constraints on the scheme can be realized using QSS schemes. For quantum secrets, Gottesman and independently Smith [65] have given constructions for arbitrary access structures. However, these are not in general optimal with respect to share size and information rate. Efficient constructions are known when the access structure satisfies certain duality properties [66]. Using the graph state formalism [67], several non-threshold QSS schemes were proposed in [68]. Ogawa et al. proposed a construction for Ramp QSS schemes which are optimal for certain parameters [62]. To conclude despite these works, construction of *efficient* QSS schemes for arbitrary access structures remains one of the basic problems in this area.

(b) **Establishing bounds on the performance of the quantum secret sharing schemes.**

As mentioned earlier, there are several metrics of performance for quantum secret sharing schemes. Establishing tight bounds on the share size or equivalently on the information rate of a quantum secret sharing scheme is a fundamental problem in quantum secret sharing and classical secret sharing. Schemes where the share sizes grow exponentially in the secret size are not likely to useful for the following reasons: (i) Increased costs in storage (ii) Shares with large sizes would lead to larger costs in keeping them secure. So establishing the lower bounds on the size of shares would be of interest from a practical point of view as well.
One of the first bounds on the share size was due to Gottesman who showed that in any perfect quantum secret sharing scheme the size of the share must be as large as that of the secret [61]. An information theoretic proof was later shown in [69]. Ogawa et al. showed that for ramp quantum secret sharing schemes that average share size could be bounded as in Eq. (4.5) [62]. Classically it was known that the optimal secret sharing schemes ie those with rate one or share size same as the secret all come from combinatorial objects known as matroids.
For sharing quantum secrets it was shown that self-dual matroids lead to optimal perfect QSS schemes [66]. Since then Matus has shown that every optimal (perfect) quantum secret sharing scheme must come from a matroid [70].
Compared to the classical setting, there has not been as much work on the bounds on the rate of quantum access structures. One reason for this is that that many of the techniques that can be used in the classical setting cannot be easily adapted for the quantum setting. Lower bounds on the share size are known only for a few QSS schemes, see [71]. Explicit constructions of secret sharing schemes provide upper bounds on the sizes of the shares for realizing an access structure. There remains a big gap between the upper and lower bounds and finding tighter bounds would be of great interest.

(c) **Quantum codes and secret sharing.**
Secret sharing has connections to several fields which allow us to study quantum secret sharing from different points of view. One of the most useful connection is to quantum error correction; this was first shown in [60]. Using this connection we can view every (perfect) quantum secret sharing scheme as a quantum code. The converse however is not true. Every quantum code is not equivalent to a perfect quantum secret sharing scheme. In contrast, every classical linear code leads to a perfect classical secret sharing scheme. So finding new ways to construct perfect secret sharing schemes from quantum codes is an attractive area of research. Quantum codes allow for alternate characterization of the authorized and unauthorized sets [72]. Not only do quantum codes provide a means to construct QSS schemes, but using the decoding algorithms for erasure model one can devise efficient methods to recover the secret. More recently, the framework of entanglement-assisted quantum codes had been to propose protocols for advanced distribution of shares prior to knowing the secret [73]. It was recently shown how to reduce the quantum communication complexity of QSS during secret recovery [74]. Both these works draw substantially on quantum codes for the design of the schemes. Other directions include the use of approximate quantum error correcting codes for approximate quantum secret sharing [75].

(d) **Measurement device independent quantum secret sharing (MDI-QSS).**

While quantum protocols promise greater security than their classical counterparts, in practice some security loop hopes can emerge due to imperfect implementations. These imperfections can be used by attackers for attacking the protocols. This motivates making the protocols resistant to device imperfections. An emerging area in this direction is that of measurement-device-independent (MDI) quantum cryptography. In the recent years there have been several protocols for QSS schemes sharing classical secrets beginning with the work of [76]. Designing MDI QSS schemes for quantum secrets is a very promising direction for futher research.

(e) **Experimental quantum secret sharing.**
Since the proposal of the quantum secret sharing schemes there has been steady progress in experimental demonstration of quantum secret sharing protocols both for classical and quantum secrets. The earliest demonstration of a quantum secret sharing protocol for classical secrets was due to [77] who showed a 3-party protocol for classical secrets. Experimental demonstration of quantum secret sharing for pure quantum states was shown in [78]. There have been several other notable demonstrations of quantum secret sharing with varying number of parties, increased alphabet size, and various different technologies, see [79] and references therein. Recently, [79] explored the implementation of QSS schemes on modern quantum computing hardware. These developments indicate that experimental implementation of QSS schemes is a promising direction of research over the next few years.

4.6 Summary

This section has provided a brief review of quantum secret sharing schemes with an emphasis on sharing quantum secrets. Quantum secret sharing is an important ingredient of secure distributed quantum computation. It is an active area of research with many open problems.

5

Quantum Networks

A quantum channel is a physical medium over which quantum bits or qubits can be sent. In the communication setting, qubits are encoded into photonic states of light and sent over fibre-based links or via free space links.

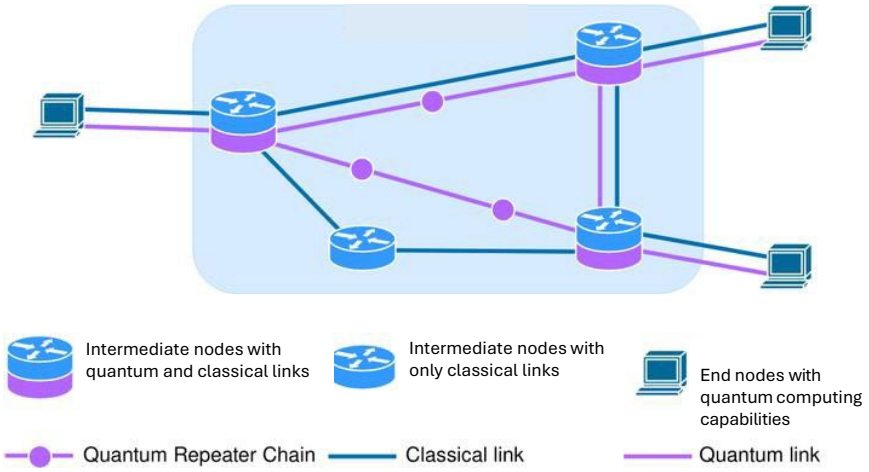
A quantum network [80,81] is a collection of nodes which are all connected by quantum communication links or quantum channels. A quantum channel is a physical medium over which quantum bits or qubits can be sent. In the communication setting, qubits are encoded into photonic states of light and sent over fibre-based links or via free space links. The nodes themselves are of two types: the end nodes are typically of the sender/receiver type and these are realised using photonic devices such as sources and detectors. The nodes in the middle of the network are usually processor nodes with a more nontrivial functionality. These could be quantum memories which are capable of storing qubits or quantum repeaters capable of performing quantum operations such as entanglement swap or entanglement distillation [82].

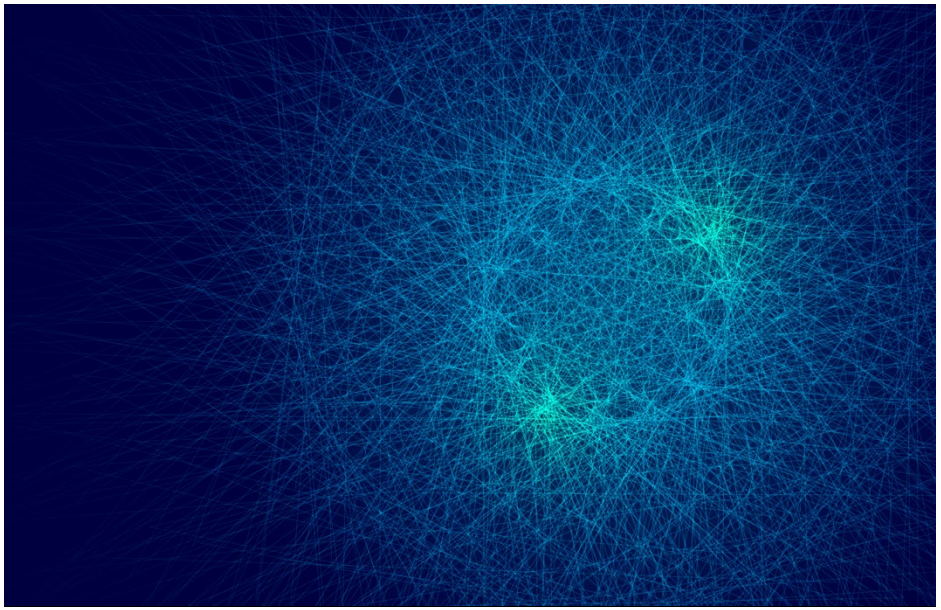
While several of the tools and techniques developed in the context of classical networks maybe used to design and implement quantum networks, the latter presents some unique challenges and opportunities because of certain fundamental differences between classical and quantum information. For example, **the no-cloning theorem**[84] states that arbitrary quantum states

cannot be copied without damaging the original version. This implies that classical protocols which rely on the ability to read and copy classical data for retransmission and signal amplification, cannot be directly reused in the quantum setting, thus in making long-distance quantum communication particularly challenging. The other uniquely quantum feature that plays an important role in quantum networks is of course **entanglement**[85]. Entanglement describes quantum correlations that go beyond what is classically possible and survive over long distances. Like the no-cloning theorem, quantum entanglement also makes quantum communication protocols secure against quantum adversaries, but their physical realization poses certain challenges as described below.

In what follows we give a brief overview of the key ingredients that go into the design and development of quantum networks, the theoretical protocols that form the backbone of these networks and summarize the state-of-the-art today. We refer to [6, 86] for a more detailed review.

Figure 5.1: Schematic sketch of a quantum network, indicating the end nodes, intermediate nodes, quantum repeaters, and the quantum as well as classical links (adapted from [83]).





5.1 Prepare-and-Measure Networks

The simplest approach to transmitting information across a network is the so-called prepare-and- measure scheme. Here, secure quantum communication is only enabled between pairs of nodes, which each act as sender and receiver respectively, and then intermediate trusted nodes[87] are used to achieve end-to-end communication. The main functionality of such a network is to allow for QKD between pairs of nodes or, at best, entanglement sharing between pairs of nodes. Such networks do not offer end-to-end security; rather, they only enable secure communication between the two end nodes provided all the intermediate nodes are trusted.

Going beyond QKD, such trusted node networks also allow for implementation of other two- party quantum cryptographic schemes such as secure identification [88] and imperfect quantum bit commitment [89].

There are two main shortcomings of the prepare-and-measure networks. Firstly, the functionality of such a network relies heavily on post-selection, that is, the receiver nodes have to ignore the non-detection events and announce that the qubit is lost. Secondly, since each secure link relies on a specific encoding of the qubits, these networks do not allow for end-to-end transmission of arbitrary quantum states.

5.2 Entanglement-based Quantum Networks

Going beyond prepare-and-measure schemes, the next stage in the development of quantum networks is to realise entanglement-based networks. These rely on establishing shared entanglement between every pair of nodes. Recall that a maximally entangled state of a pair of qubits (labeled A and B) has the form,

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B], \tag{5.1}$$

where $|0\rangle$ and $|1\rangle$ represent two orthogonal states of the qubit. Using this pair of entangled qubits, both classical and quantum information can be transmitted from one node to the other either via QKD or quantum teleportation. The E91 QKD protocol [36] enables sharing of a secure classical key over the link established between A and B, making use of one pair of entangled qubits for each classical bit of information. On the other hand, quantum teleportation [90] allows for arbitrary quantum states to be communicated from A to B, making use of the shared entanglement between the two nodes.

Quantum teleportation also provides a mechanism to extend short-distance entanglement to larger distances via a protocol known as entanglement swapping [91]. Suppose shared entanglement has been generated between nodes A and B, and also between nodes B and C. Then, it is possible to generate entanglement between A and C using the help of B, as follows – B teleports the qubit that was entangled with node A to node C, making use of the entanglement she shares with C.

The generation of entanglement between a pair of nodes can happen either in a deterministic or a heralded fashion. A deterministic protocol succeeds with (near) unit probability and near impossible to achieve in practice [92]! Heralding is a slightly weaker form of deterministic entanglement generation in which the successful generation of entanglement is signaled with an event that is independent of the direct measurement of the entangled qubits themselves. Essentially, this ensures that the generation of entanglement is deterministic, conditioned on a successful heralding signal.

Quantum channels are inherently lossy and this make both entanglement generation as well as the entanglement swapping operations noisy. With each link and each swap the quality of the entanglement, quantified by the so-called fidelity, degrades. However, it is possible to create higher fidelity entangled pairs from two or more lower quality pair states through a process called entanglement distillation [93].

5.3 Processing Nodes and Quantum Repeaters

Processing nodes are intermediate nodes with an optical interface that are capable of storing qubits and also performing universal quantum computation. Physical platforms that could realise such nodes include NV centres in diamond [94–96], ion traps [97], and neutral atoms [98].

The objective of quantum repeaters [99] is to enable the transmission of qubits over long distances. They essentially work on the principle of entanglement swapping described in Sec. 5.2 above [93, 100]. Any physical system that forms a quantum processing node, can also be used as a repeater platform. In addition, there exist specific hardware platforms tailored to perform the

task of a quantum repeater. For example, there are proposals for multiplexed quantum repeaters using atomic ensembles[101], which could generate entanglement faster via temporal and spatial multiplexing. We refer to [102] for a recent survey on quantum repeaters and their physical realisations.

5.4 Scheduling and Routing Protocols

Routing in quantum networks is a nontrivial problem both due to the non-local and transient nature of entangled pairs as well as the lossy channels over which the quantum states are sent. Qubit lifetimes are short (of the order of microseconds or milliseconds) and this directly impacts the ability to generate long-distance entanglement. The entanglement swapping protocol requires both entangled pairs of qubits to be available on two separate links at the same time, and so the intermediate node must be able to store the first pair until it receives the second pair. If one of the qubits decoheres, the pair is lost and the entire process must start over.

The question of scheduling and routing entanglement generation, that is, making decisions on how end-to-end entanglement can be established in a fast and robust manner between users in quantum networks, has received a fair amount of attention in the recent literature [103–107]. There have also been studies on how queuing of noisy qubits can affect the overall throughput of quantum communication links [108, 109]. The long term goal is to build a quantum network stack along the lines of the TCP/IP protocol, that is agnostic to the specific hardware or protocol being implemented. Preliminary works in this direction include the development of a link-layer protocol that combines information from the quantum and classical links[110] as well as the design of an end-to-end quantum network protocol that take into account the effects of finite qubit lifetimes and channel losses[83].

5.5 Quantum Networks in the NISQ Era

We are today in an era of noisy, intermediate scale quantum (NISQ) hardware[111], with channel loss and noisy quantum memories impeding the performance of present day quantum technologies. Two critical parameters for the performance of quantum networks are the entanglement-generation rate rgen between nodes and the decoherence rate r_{dec}. Their ratio $\eta = r_{gen}/r_{dec}$, often referred to as the **quantum link efficiency (QLE)** [112, 113], quantifies how effectively entangled states can be preserved over the timescales necessary to generate them. A QLE > 1 is required in order to

be able to distribute entanglement over long distances. In this regard, NV Center based platforms seem to be the most promising candidates for building quantum networks with a QLE of 8, with trapped ions (TLE ≈ 5) and neutral atoms (TLE ≈ 2) being close contenders[86].

Here we survey the state of the art in physical realizations of quantum networks. Although no long-distance quantum networks exist at the moment, short distance prepare-and-measure links that are hundreds of kilometers long [114–116] have been combined together classically to realise trusted node networks [117–119] as described in Sec. 5.1 above. Such networks, however, require a significant level of physical security to protect the intermediate, trusted nodes. We refer to [119] for a comparison of the different local area networks that have been implemented thus far. Quantum nodes that produce short-lived, short-distance entanglement[120] have also been realised.

Realisations of longer range quantum networks with more advanced functionalities, are still in early stages of development. Entanglement between a pair of distant nodes ~1200 km apart has been generated

using a satellite [121]. However, the data rates are still rather low, and the entanglement is short-lived. The current record for producing heralded entanglement between distant sites is 1.3 km in a solid state quantum device using nitrogen-vacancy (NV) centres in diamond [95].

One of the key hurdles in realising long-distance quantum networks is the design and development of good quantum repeaters. There have been recent demonstrations of high fidelity quantum repeaters on ion traps [122] and photonics-based platforms [123], but these are still in the laboratory domain and some distance away from being deployed on the ground.

5. Summary and Outlook

Quantum networks offer the promise of a futuristic internet capable of performing various communication and remote computational tasks in an unconditionally secure manner. However there remain several theoretical and experimental challenges that need to be overcome in order to build robust, long-distance quantum networks with the desired functionalities. Recent experimental progress in entanglement generation rates and memory lifetimes is very promising, but overcoming the effects of decoherence and channel losses remains a significant hurdle. Integrating ideas from quantum computing such as error correction and fault tolerance will be required in order to design and engineer the next generation of quantum repeaters which can lead to large-scale, fault-tolerant quantum networks.

Finally, we note that a crucial component of quantum communication is also the ability to send classical data, not just as a reconciliation step for quantum protocols, but also as a means to incorporate post-quantum cryptographic (PQC) schemes into the quantum network architecture. We expect that quantum networks will therefore be deployed alongside classical networks with a quantum data plane coexisting with the classical one.

References

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994, pp. 124–134, 1994.

[2] https://www.insightsonindia.com/science-technology/communication-and-it- technology/quantum-cryptography/.

[3] A. Broadbent and C. Staffner, "Quantum cryptography beyond quantum key distribution," Designs, Codes and Cryptography, vol. 78, pp. 351–382, 2016.

[4] H. J. Kimble, "The quantum internet," Nature, vol. 453, no. 7198, pp. 1023–1030, 2008.

[5] D. Castelvecchi, "The quantum internet has arrived (and it hasn't).," Nature, vol. 554, no. 7690, pp. 289–293, 2018.

[6] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," Science, vol. 362, no. 6412, p. eaam9288, 2018.

[7] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in 2009 50th annual IEEE symposium on foundations of computer science, pp. 517–526, IEEE, 2009.

[8] P. Komar, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, "A quantum network of clocks," Nature Physics, vol. 10, no. 8, pp. 582–587, 2014.

[9] M. Ganz, "Quantum leader election," Quantum Information Processing, vol. 16, pp. 1–17, 2017.

[10] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC '96, 1996.

[11] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature- verification and message-encryption," in Advances in Cryptology — EUROCRYPT '88, (Berlin, Heidelberg), pp. 419–453, Springer Berlin Heidelberg, 1988.

[12] M. Bardet, J.-C. Faugere, B. Salvy, and P.-J. Spaenlehauer, "On the complexity of solving quadratic boolean systems," Journal of Complexity, vol. 29, no. 1, pp. 53 – 75, 2013.

[13] C. Wolf, Multivariate Quadratic Polynomials In Public Key Cryptography. PhD thesis, KATHOLIEKE UNIVERSITEIT LEUVEN, 2005.

[14] J. Ding and B.-Y. Yang, Multivariate Public Key Cryptography, pp. 193–241. Springer Berlin Heidelberg, 2009.

[15] J. Patarin, "Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms," in Advances in Cryptology — EUROCRYPT '96 (U. Maurer, ed.), 1996.

[16] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in Advances in Cryptology — EUROCRYPT '99 (J. Stern, ed.), 1999.

[17] Y. Hashimoto, "Multivariate public key cryptosystems," in Mathematical Modelling for Next-Generation Cryptography, pp. 17–42, Springer, 2018.

[18] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," Deep Space Network Progress Report, vol. 44, pp. 114–116, Jan. 1978.

[19] R. Overbeck and N. Sendrier, "Code-based cryptography," in Post-Quantum Cryptography (D. J. Bernstein, J. Buchmann, and E. Dahmen, eds.), 2009.

[20] R. Merkle, Secrecy, authentication and public key systems / A certified digital signature. PhD thesis, Stanford University, 1979.

[21] C. Peikert, A Decade of Lattice Cryptography, vol. 10, pp. 283–424. 03 2016.

[22] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, pp. 284– 293, ACM, 1997.

[23] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," in Annual International Cryptology Conference, pp. 112–131, Springer, 1997.

[24] O. Regev, "New lattice-based cryptographic constructions," Journal of the ACM (JACM), vol. 51, no. 6, pp. 899–942, 2004.

[25] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on gaussian measures," SIAM Journal on Computing (SICOMP), vol. 37, no. 1, pp. 267–302, 2007. extended abstract in FOCS 2004.

[26] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in STOC, pp. 197–206, 2008.

[27] D. Micciancio and C. Peikert, "Hardness of sis and lwe with small parameters," in Crypto, 2013.

[28] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," J.ACM, vol. 56, no. 6, 2009. extended abstract in STOC'05.

[29] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings.," in EUROCRYPT, vol. 6110, 2010.

[30] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem," in STOC, pp. 333–342, 2009.

[31] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehl´e, "Classical hardness of learning with errors," in Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing, STOC '13, ACM, 2013.

[32] B. Barak, Y. Dodis, H. Krawczyk, O. Pereira, K. Pietrzak, F.-X. Standaert, and Y. Yu, "Leftover hash lemma, revisited," in Annual Cryptology Conference, pp. 1–20, Springer, 2011.

[33] "Report on post-quantum cryptography." https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[34] https://tikz.net/optics polarization/.

[35] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179, 1984.

[36] A. K. Ekert, "Quantum cryptography based on bell's theorem," Physical review letters, vol. 67, no. 6, p. 661, 1991.

[37] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Physical Review Letters, vol. 68, pp. 3121–3124, 1992.

[38] V. Scarani, A. Ac´ın, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Physical Review Letters, vol. 92, p. 057901, 2004.

[39] https://wirelesspi.com/i-q-signals-101-neither-complex-nor-complicated/.

[40] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Physical Review Letters, vol. 88, p. 057902, 2002.

[41] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," Applied Physics Reviews, vol. 11, p. 011318, 03 2024.

[42] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Physical Review Letters, vol. 108, p. 130503, 2012.

[43] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, "Floodlight quantum key distribution: A practical route to gbps secret-key rates," Physical Review A, vol. 94, p. 012322, 2016.

[44] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, "Floodlight quantum key distribution: Demonstrating a framework for high-rate secure communication," Physical Review A, vol. 95, p. 012332, 2017.

[45] M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof for quantum key distribution," Quantum, vol. 1, p. 14, 2017.

[46] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," Physical Review Letters, vol. 85, pp. 441–444, 2000.

[47] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," Physical Review Letters, vol. 89, p. 037902, 2002.

[48] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Physical Review Letters, vol. 91, p. 057901, 2003.

[49] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system," New Journal of Physics, vol. 4, p. 41, 2002.

[50] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," Nature, vol. 509, pp. 475–478, 2014.

[51] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," Nature Communications, vol. 8, p. 15043, Apr. 2017.

[52] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science, vol. 283, pp. 2050–2056, 1999.

[53] G. Brassard, N. Lu¨tkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," Physical Review Letters, vol. 85, pp. 1330–1333, 2000.

[54] D. Gottesman, H.-K. Lo, N. Lutkenhaus, , and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Information and Computation, vol. 4, pp. 325– 360, 2004.

[55] Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, "Characterising the correlations of prepare-and-measure quantum networks," npj Quantum Information, vol. 5, p. 17, 2019.

[56] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, "Versatile security analysis of measurement-device-independent quantum key distribution," Physical Review A, vol. 99, p. 062332, 2019.

[57] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839–894, 2022.

[58] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, and M. Voznak, "Quantum key distribution: A networking perspective," ACM Comput. Surv., vol. 53, Sept. 2020.

[59] M. Hillery, V. Bu˘zek, and A. Berthiaume, "Quantum secret sharing," Phys. Rev. A, vol. 59, pp. 1829–1834, Mar 1999.

[60] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," Phys. Rev. Lett., vol. 83, pp. 648–651, Jul 1999.

[61] D. Gottesman, "Theory of quantum secret sharing," Phys. Rev. A, vol. 61, p. 042311, Mar 2000.

[62] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," Phys. Rev. A, vol. 72, no. 3, p. 032318, 2005.

[63] P. Zhang and R. Matsumoto, "Quantum strongly secure ramp secret sharing," Quantum Information Processing, vol. 14, no. 2, pp. 715–729, 2015.

[64] P. K. Sarvepalli and A. Klappenecker, "Sharing classical secrets with calderbank-shor-steane codes," Phys. Rev. A, vol. 80, p. 022321, Aug 2009.

[65] A. D. Smith, "Quantum secret sharing for general access structures," e-print quant-ph/0001087, 2000.

[66] P. Sarvepalli and R. Raussendorf, "Matroids and quantum-secret-sharing schemes," Phys. Rev. A, vol. 81, p. 052333, May 2010.

[67] D. Markham and B. C. Sanders, "Graph states for quantum secret sharing," Phys. Rev. A, vol. 78, p. 042309, Oct 2008.

[68] P. Sarvepalli, "Nonthreshold quantum secret-sharing schemes in the graph-state formalism," Phys. Rev. A, vol. 86, p. 042303, Oct 2012.

[69] H. Imai, J. Mu¨ller-Quade, A. C. Nascimento, P. Tuyls, and A. Winter, "A quantum information theoretical model for quantum secret sharing schemes," e-print quant-ph/0311136, 2003.

[70] F. Matus, "Polymatroids and polyquantoids," 2012.

[71] P. Sarvepalli, "Bounds on the information rate of quantum-secret-sharing schemes," Phys. Rev. A, vol. 83, p. 042324, Apr 2011.

[72] R. Matsumoto, "Coding theoretic construction of quantum ramp secret sharing," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E101.A, no. 8, pp. 1215–1222, 2018.

[73] R. Masumori, S. Matsumoto, "Advance sharing with Ogawa et al.'s ramp quantum secret sharing scheme," 2024.

[74] K. Senthoor and P. K. Sarvepalli, "Communication efficient quantum secret sharing," Phys. Rev. A, vol. 100, no. 5, p. 052313, 2019.

[75] C. Cr´epeau, D. Gottesman, and A. Smith, "Approximate quantum error-correcting codes and secret sharing schemes," in Advances in Cryptology – EUROCRYPT 2005 (R. Cramer, ed.), (Berlin, Heidelberg), pp. 285–301, Springer Berlin Heidelberg, 2005.

[76] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, "Long-distance measurement-device- independent multiparty quantum communication," Phys. Rev. Lett., vol. 114, p. 090501, Mar 2015.

[77] W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing," Phys. Rev. A, vol. 63, p. 042301, Mar 2001.

[78] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, "Tripartite quantum state sharing," Phys. Rev. Lett., vol. 92, p. 177903, Apr 2004.

[79] J. Graves, M. Nelson, and E. Chitambar, "Implementing quantum secret sharing on current hardware," 2024.

[80] R. Van Meter, Quantum networking. John Wiley & Sons, 2014.

[81] M. Hajdu˘sek and R. Van Meter, "Quantum communications," arXiv preprint arXiv:2311.02367, 2023.

[82] E. O. Kiktenko, A. Tayduganov, and A. K. Fedorov, "Routing Algorithm Within the Multiple Non-Overlapping Paths' Approach for Quantum Key Distribution Networks," Entropy, vol. 26, no. 12, p. 1102, 2024.

[83] W. Kozlowski, A. Dahlberg, and S. Wehner, "Designing a quantum network protocol," in Proceedings of the 16th international conference on emerging networking experiments and technologies, pp. 1–16, 2020.

[84] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, no. 5886, pp. 802–803, 1982.

[85] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," Reviews of modern physics, vol. 81, no. 2, pp. 865–942, 2009.

[86] W. Kozlowski and S. Wehner, "Towards large-scale quantum networks," in Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication, NANOCOM '19, (New York, NY, USA), Association for Computing Machinery, 2019.

[87] L. Salvail, M. Peev, E. Diamanti, R. All´eaume, N. Lu¨tkenhaus, and T. L¨anger, "Security of trusted repeater quantum key distribution networks," Journal of Computer Security, vol. 18, no. 1, pp. 61–87, 2010.

[88] I. Damg˚ard, S. Fehr, L. Salvail, and C. Schaffner, "Secure identification and qkd in the bounded-quantum-storage model," Theoretical Computer Science, vol. 560, pp. 12–26, 2014.

[89] A. Chailloux and I. Kerenidis, "Optimal bounds for quantum bit commitment," in 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, pp. 354–362, IEEE, 2011.

[90] C. H. Bennett, G. Brassard, C. Cr´epeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," Physical review letters, vol. 70, no. 13, p. 1895, 1993.

[91] M. Zukowski, A. Zeilinger, M. Horne, and A. Ekert, "" event-ready-detectors" bell experiment via entanglement swapping.," Physical review letters, vol. 71, no. 26, 1993.

[92] K. Koshino, K. Inomata, Z. Lin, Y. Tokunaga, T. Yamamoto, and Y. Nakamura, "Theory of deterministic entanglement generation between remote superconducting atoms," Physical Review Applied, vol. 7, no. 6, p. 064006, 2017.

[93] H.-J. Briegel, W. Du¨r, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," Physical Review Letters, vol. 81, no. 26, p. 5932, 1998.

[94] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, et al., "Heralded entanglement between solid-state qubits separated by three metres," Nature, vol. 497, no. 7447, pp. 86–90, 2013.

[95] B. Hensen, H. Bernien, A. E. Dr´eau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abell´an, et al., "Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres," Nature, vol. 526, no. 7575, pp. 682–686, 2015.

[96] T. H. Taminiau, J. Cramer, T. van der Sar, V. V. Dobrovitski, and R. Hanson, "Universal control and error correction in multi-qubit spin registers in diamond," Nature nanotechnology, vol. 9, no. 3, pp. 171–176, 2014.

[97] L.-M. Duan and C. Monroe, "Colloquium: Quantum networks with trapped ions," Reviews of Modern Physics, vol. 82, no. 2, pp. 1209–1224, 2010.

[98] J. P. Covey, H. Weinfurter, and H. Bernien, "Quantum networks with neutral atom processing nodes," npj Quantum Information, vol. 9, no. 1, p. 90, 2023.

[99] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters," IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 78–90, 2015.

[100] W. Du¨r, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," Physical Review A, vol. 59, no. 1, p. 169, 1999.

[101] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," Reviews of Modern Physics, vol. 83, no. 1, pp. 33–80, 2011.

[102] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, "Quantum repeaters: From quantum networks to the quantum internet," Reviews of Modern Physics, vol. 95, no. 4, p. 045006, 2023.

[103] R. Van Meter, T. Satoh, T. D. Ladd, W. J. Munro, and K. Nemoto, "Path selection for quantum repeater networks," Networking Science, vol. 3, pp. 82–95, 2013.

[104] M. Caleffi, "Optimal routing for quantum networks," Ieee Access, vol. 5, pp. 22299–22312, 2017.

[105] L. Gyongyosi and S. Imre, "Decentralized base-graph routing for the quantum internet," Physical Review A, vol. 98, no. 2, p. 022310, 2018.

[106] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, "Routing entanglement in the quantum internet. npj quantum information 5 (1): 1–9," arXiv preprint arXiv:1708.07142, 2019.

[107] C. Cicconetti, M. Conti, and A. Passarella, "Request scheduling in quantum networks," IEEE Transactions on Quantum Engineering, vol. 2, pp. 2–17, 2021.

[108] P. Mandayam, K. Jagannathan, and A. Chatterjee, "The classical capacity of additive quantum queue-channels," IEEE Journal on Selected Areas in Information Theory, vol. 1, no. 2, pp. 432– 444, 2020.

[109] W. Dai, T. Peng, and M. Z. Win, "Quantum queuing delay," IEEE Journal on Selected Areas in Communications, vol. 38, no. 3, pp. 605–618, 2020.

[110] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpedek, M. Pompili, A. Stolk, P. Pawe-lczak, R. Knegjens, J. de Oliveira Filho, et al., "A link layer protocol for quantum networks," in Proceedings of the ACM special interest group on data communication, pp. 159– 173, 2019.

[111] J. Preskill, "Quantum computing in the nisq era and beyond," Quantum, vol. 2, p. 79, 2018.

[112] C. Monroe, R. Raussendorf, A. Ruthven, K. R. Brown, P. Maunz, L.-M. Duan, and J. Kim, "Large-scale modular quantum-computer architecture with atomic memory and photonic interconnects," Physical Review A, vol. 89, no. 2, p. 022317, 2014.

[113] D. Hucul, I. V. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. M. Clark, and C. Monroe, "Modular entanglement of atomic qubits using photons and phonons," Nature Physics, vol. 11, no. 1, pp. 37–42, 2015.

[114] M. Peev, C. Pacher, R. All'eaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, et al., "The secoqc quantum key distribution network in vienna," New journal of physics, vol. 11, no. 7, p. 075001, 2009.

[115] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, et al., "Long-term performance of the swissquantum quantum key distribution network in a field environment," New Journal of Physics, vol. 13, no. 12, p. 123001, 2011.

[116] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, et al., "Field and long-term demonstration of a wide area quantum key distribution network," Optics express, vol. 22, no. 18, pp. 21739–21756, 2014.

[117] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al., "Field test of quantum key distribution in the tokyo qkd network," Optics express, vol. 19, no. 11, pp. 10387–10409, 2011.

[118] R. Courtland, "China's 2,000-km quantum link is almost complete [news]," IEEE Spectrum, vol. 53, no. 11, pp. 11–12, 2016.

[119] J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, J. Cho, et al., "Cambridge quantum network," npj Quantum Information, vol. 5, no. 1, p. 101, 2019.

[120] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, "Entanglement distribution over 300 km of fiber," Optics express, vol. 21, no. 20, pp. 23241–23249, 2013.

[121] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, et al., "Satellite-based entanglement distribution over 1200 kilometers," Science, vol. 356, no. 6343, pp. 1140–1144, 2017.

[122] P. Drmota, D. Main, D. Nadlinger, B. Nichol, M. Weber, E. Ainley, A. Agrawal, R. Srinivas, G. Araneda, C. Ballance, et al., "Robust quantum memory in a trapped-ion quantum network node," Physical Review Letters, vol. 130, no. 9, p. 090803, 2023.

[123] Z.-D. Li, R. Zhang, X.-F. Yin, L.-Z. Liu, Y. Hu, Y.-Q. Fang, Y.-Y. Fei, X. Jiang, J. Zhang, L. Li, et al., "Experimental quantum repeater without quantum memory," Nature photonics, vol. 13, no. 9, pp. 644–648, 2019.

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

The National Centre of Excellence (NCoE) for Cybersecurity Technology Development is conceptualized by the Ministry of Electronics & Information Technology (MeitY), Government of India, and the Data Security Council of India (DSCI). Its primary objective is to catalyze and accelerate cybersecurity technology development and entrepreneurship within the country. NCoE plays a crucial role in scaling up and advancing the cybersecurity ecosystem, focusing on various critical and emerging security areas. Equipped with state-of-the-art facilities, including advanced lab infrastructure and test beds, NCoE facilitates research, technology development, and solution validation for adoption across government and industrial sectors. Adopting a concerted strategy, NCoE endeavors to translate innovations and research into market-ready deployable solutions, thereby contributing to the evolution of an integrated technology stack comprising cutting-edge, homegrown security products and solutions.

DATA SECURITY COUNCIL OF INDIA

+91-120-4990253 | ncoe@dsci.in

https://www.n-coe.in/

4 Floor, NASSCOM Campus, Plot No.
7-10, Sector 126, Noida, UP -201303

Follow us on

@CoeNational

nationalcoe

nationalcoe

NationalCoE