Chapter X: Formal Statement of Assumptions for Decoy-State BB84 QKD

Introduction: The Assumption Stack as a Bridge between Theory and Practice

The security of any cryptographic protocol rests upon a foundation of assumptions. In the domain of Quantum Key Distribution (QKD), and specifically for the decoy-state Bennett-Brassard 1984 (BB84) protocol, this foundation is a complex, multi-layered structure. It encompasses everything from the fundamental laws of physics to the characterized imperfections of a specific laser diode. To construct a rigorous and practically relevant security proof, one must meticulously define and justify each layer of this "assumption stack." The historical development of QKD security can be understood as a continuous and deliberate process of strengthening this foundation by relaxing strong, idealized assumptions and replacing them with weaker, more realistic, and experimentally verifiable ones.[1] This evolution is paramount for bridging the persistent gap between abstract theoretical models and the tangible realities of physical implementations, ensuring that the promise of information-theoretic security is not merely a mathematical artifact but a robust guarantee for real-world systems.

Early security proofs for BB84 relied on a set of convenient but physically unrealistic idealizations, such as the availability of perfect on-demand single-photon sources, lossless quantum channels, and perfectly aligned optical components.[4] While instrumental in establishing the theoretical plausibility of QKD, these assumptions created a significant vulnerability gap. The practical necessity of using attenuated laser sources, which emit weak coherent pulses (WCPs) instead of single photons, opened the door to devastating attacks like the Photon-Number-Splitting (PNS) attack, where an eavesdropper could break the security without being detected.[3]

The invention of the decoy-state method was a landmark achievement that addressed this specific vulnerability.[8] However, this solution did not eliminate the need for assumptions; rather, it replaced the single, strong assumption of a perfect source with a new, more nuanced set of assumptions regarding the properties of WCPs and the indistinguishability of different pulse types. Similarly, early proofs often assumed that an adversary, Eve, would attack each quantum signal independently and identically (IID attacks).[10] This assumption was later relaxed to accommodate the far more powerful and general class of coherent attacks, where Eve can process all signals in a single, collective quantum operation.[10] This transition, in turn, necessitated the development of more sophisticated proof techniques, such as those based on entropic uncertainty relations or the entropy accumulation theorem.[2]

This chapter provides a formal, exhaustive statement of the assumptions required for a state-of-the-art security proof of the decoy-state BB84 protocol, targeting a finite-key, universally composable security guarantee. Each section will dissect a different layer of the assumption stack, starting from the most abstract adversarial and security models, moving to the physical assumptions about trusted devices and quantum signals, and concluding with the logical and mathematical assumptions that underpin the proof itself. By structuring the analysis in this way, we can clearly trace the dependencies between different assumptions and appreciate the intellectual progression of the field. The following table provides a high-level overview of this hierarchy, contrasting the idealized assumptions of early proofs with the modern, more realistic assumptions that form the basis of current security analyses.

Table X.1: The Hierarchy of Assumptions in Decoy-State BB84

Domain	The Idealized Assumption (Historical View)	The Practical Reality & Threat	The Modern Assumption & Countermeasure	Key Citations
Adversary	Collective IID Attacks	Coherent attacks across all protocol rounds	Unrestricted quantum adversary; Proof against general/coherent attacks	10
Security Goal	Low Mutual Information with Eve	Insecurity under protocol composition	ε-secure in the Universal Composability (UC) framework	12

Source	Perfect single-photon source	Weak Coherent Pulse (WCP) source enables Photon-Number-Splitting (PNS) attack	WCP source with decoy-state analysis to bound single-photon contributions	8
State Prep.	Perfect, symmetric BB84 states	Basis-dependent state preparation flaws (e.g., misalignment)	Characterized source model; Explicit measurement of phase error rate	3
Detector	Perfect photon-number-resolving (PNR) detectors	Imperfect, non-PNR (threshold) detectors	Threshold detectors analyzed via the squashing model	14
Channel	Lossless, noiseless channel	Lossy, noisy channel controlled by Eve	Fully untrusted quantum channel; Channel parameters estimated from data	2
Key Length	Asymptotic regime ($N\longrightarrow\infty$)	Finite number of signals (N) leads to statistical fluctuations	Finite-key analysis using concentration inequalities	14

This structured exploration will clarify the precise conditions under which the security of decoy-state BB84 holds, providing a rigorous foundation for both theoretical analysis and the practical certification of QKD systems.

1. The Abstract Security Framework and Adversarial Model

Before delving into the physical characteristics of the QKD system, a security proof must first establish the abstract "rules of the game." This involves defining the capabilities of the adversary and the precise meaning of a "secure" key. The strength of the final security guarantee is directly determined by the generality of these initial assumptions. Modern proofs adopt a worst-case-scenario approach, granting the adversary maximal power and demanding the strongest possible definition of security.

1.1. The Adversary's Power: The Omnipotent Eavesdropper (Eve)

The security of QKD is information-theoretic, meaning it must hold against an adversary, conventionally named Eve, whose power is not constrained by the technological limitations of today or the foreseeable future. Instead, her capabilities are assumed to be bounded only by the known laws of quantum mechanics.[16] This leads to a standard set of assumptions about her power.

1.1.1. Unrestricted Computational Power

It is assumed that Eve possesses a universal quantum computer and unlimited classical computational resources. This assumption immediately renders any cryptographic security based on computational hardness problems—such as the difficulty of factoring large integers (underpinning RSA) or computing discrete logarithms—obsolete from her perspective.[18] The security of the QKD protocol must therefore derive not from the difficulty of a computation, but from the fundamental principles of quantum physics, such as the no-cloning theorem and the disturbance caused by measurement.[20]

1.1.2. Complete Control of the Quantum Channel

The quantum channel, the physical medium (e.g., optical fiber, free space) through which Alice sends quantum states to Bob, is assumed to be entirely untrusted. It is modeled as a black box that is completely owned and operated by Eve.[2] She can:

- Intercept any and all quantum states transmitted by Alice.

- Store these states indefinitely in a perfect quantum memory.
- Perform any physically-allowed quantum operation (i.e., any completely positive trace-preserving map) on the intercepted states. This includes measuring them, interacting them with her own ancillary quantum systems (ancillas), and modifying them.
- Replace the original states with new states of her own creation to send to Bob.
- Modify the channel properties at will, for instance by introducing or removing loss and noise dynamically throughout the protocol execution.

This assumption ensures that the security proof is robust against any possible physical interaction Eve might have with the transmitted signals.

1.1.3. Coherent Attacks

The most critical assumption regarding Eve's strategy is that she can execute **coherent attacks** (also known as general attacks). In this attack model, Eve is not required to act on each quantum signal independently. Instead, she can collect all the quantum states Alice sends throughout the entire protocol run, store them in her quantum memory, and then perform a single, large, collective quantum measurement on the joint state of all signals at the very end of the protocol, after all classical communication between Alice and Bob has concluded.[10]

This is the most powerful class of attack allowed by quantum mechanics and stands in stark contrast to weaker, more restricted models:

- **Individual Attacks:** Eve interacts with each signal from Alice with a separate ancilla and measures each ancilla independently.
- **Collective Attacks:** Eve interacts with each signal with a separate ancilla but can perform a joint measurement on all her ancillas at the end. This is stronger than individual attacks but still assumes the signals are acted upon in an independent and identically distributed (IID) manner.

A security proof against coherent attacks is the gold standard because it automatically implies security against all less general strategies, including collective and individual attacks.[11] Proving security against coherent attacks is significantly more challenging and often requires sophisticated mathematical tools like the De Finetti theorem, the Postselection Technique, Entropic Uncertainty Relations (EURs), or the Entropy Accumulation Theorem (EAT).[2] Assuming Eve can perform coherent attacks is a necessary step to ensure the protocol is secure against the full range of threats permitted by physics.

1.2. The Definition of Security: ε-Secure and Universally Composable

Having defined the adversary's power, it is necessary to formally define what it means for the protocol to be "secure." A modern security definition must be quantitative, robust, and suitable for practical use. This has led to the adoption of the ε-security and universal composability frameworks.

1.2.1. ε-Security Parameters

The security of a finite-key QKD protocol is not absolute but is quantified by a small, non-zero security parameter, εQKD, which represents the maximum tolerable failure probability of the protocol. This overall parameter is typically the sum of several distinct parameters corresponding to different aspects of the protocol's success [10]:

$$\varepsilon\text{QKD}=\varepsilon\text{correct}+\varepsilon\text{secret}+\ldots$$

The two most fundamental components are correctness and secrecy [10]:

- Correctness (εcorrect): The protocol is considered εcorrect-correct if the final key generated by Alice, KA, and the final key generated by Bob, KB, are identical, except with a probability of at most εcorrect. This is formally stated as:

  $$\Pr\leq\varepsilon\text{correct}$$

  where the probability is taken over all choices made during the protocol and any of Eve's interventions. The 'accept' event signifies that the protocol did not abort.
- Secrecy (εsecret): The protocol is considered εsecret-secret if the final key is nearly uniformly random and independent of any information Eve possesses. This is formally captured using the trace distance metric. Let ρKAE be the joint classical-quantum state describing the correlation between Alice's final key (KA) and Eve's entire system (E), conditioned on the protocol accepting. Let UKA be the state of a perfectly uniform and independent key of the same length. The

secrecy condition is:

$21\mathrm{Tr}|\rho KAE{-}UKA\otimes\rho E|\le\varepsilon secret$

where ρE is the reduced state of Eve's system. This definition ensures that Eve's ability to distinguish the real key from a perfect one is negligible.

Other parameters, such as the failure probability of parameter estimation or error verification, also contribute to the total εQKD.

1.2.2. Universal Composability (UC)

A critical, and now standard, assumption is that the security definition must be **universally composable**.[14] Universal composability is a powerful concept that guarantees a protocol remains secure even when it is used as a component—or "subroutine"—within a larger, arbitrary cryptographic application.[25]

The need for this strong definition arises from the insufficiency of simpler security metrics, such as bounding the mutual information between Eve's knowledge and the key, $I(K{:}E)$.[16] An adversary holding a quantum system entangled with the key might gain very little information from a single measurement. However, if she later obtains some partial classical information about the key—for example, by observing how it is used to encrypt a known piece of plaintext—she could use this new information to choose a more effective measurement on her stored quantum state, potentially revealing the rest of the key.[12] This constitutes a "joint attack" across both the QKD protocol and the subsequent application that uses the key.[12]

The UC framework prevents such attacks by demanding a much stronger condition of security.[28] It requires that the real protocol, in any environment, be indistinguishable from an "ideal functionality." In the case of QKD, this ideal functionality is a perfectly secure black box that simply generates a truly random secret key and distributes it to Alice and Bob, with no interaction or leakage to Eve.[16] If a security proof demonstrates that the real protocol is indistinguishable from this ideal one (up to some small probability

ε), then the real protocol can be safely substituted for the ideal one in any larger system. Since the larger system is secure by definition when using the ideal key-distribution box, it must also be secure when using the real QKD protocol. This property of "safe substitution" is the essence of composability and is a fundamental requirement for any key that is intended for real-world cryptographic use.[30]

1.3. The Communication Channels

The protocol relies on two distinct communication channels with starkly different security assumptions.

1.3.1. The Untrusted Quantum Channel

As established in the adversarial model (Section 1.1.2), the quantum channel is assumed to be completely untrusted and under Eve's full control. Alice and Bob make no assumptions about its intrinsic properties, such as its transmission efficiency or noise level. Instead, these parameters are treated as variables that are actively influenced by Eve's attack. The protocol's security relies on Alice and Bob being able to bound the effects of Eve's actions by observing the statistics of the signals that successfully arrive at Bob's station.

1.3.2. The Authenticated Classical Channel

In contrast to the quantum channel, the classical channel used for all public discussion (e.g., basis reconciliation, parameter estimation announcements, error correction messages) is assumed to be **perfectly and unconditionally authenticated**.[17] This means that while Eve can listen to all messages transmitted over this channel (it is public), she cannot modify, inject, or delete messages without being detected by Alice and Bob with overwhelming probability. The channel is also assumed to be reliable and not subject to denial-of-service attacks (i.e., it cannot be jammed).

This assumption is a critical prerequisite for the protocol to function. Unconditional authentication is not possible without a pre-shared secret. Therefore, the security proof assumes that Alice and Bob share a small amount of initial secret key material before the QKD protocol begins. This initial key is used to run a message authentication code (MAC), such as a one-time MAC, to authenticate the classical communication during the first run of the QKD protocol. The QKD protocol is then used to generate a much larger amount of secret key. A portion of this newly generated key can be used to replenish the authentication key for subsequent QKD runs, a process known as **key amortization**.[31] This bootstrapping mechanism is an essential part of the overall security architecture.

2. The Trusted Domain of Alice and Bob

While the quantum channel is untrusted, the security proof must assume that the devices and resources within the physical locations of Alice and Bob are secure. These assumptions define a "trusted perimeter." Any violation of this perimeter constitutes an implementation-specific vulnerability, often termed a side-channel attack, which requires a separate layer of analysis beyond the core protocol security.

2.1. The Secure Laboratory Assumption

The most fundamental assumption is that Alice's and Bob's respective devices are housed within physically secure environments, often referred to as "secure laboratories." Within these perimeters, the following conditions hold:

- **No Physical Access:** Eve has no physical access to the devices. She cannot tamper with components, attach probes, or directly observe their internal states.
- **No Unintended Classical Leakage:** The devices are perfectly shielded from Eve. It is assumed that no information about the internal operations of the devices—such as Alice's choice of basis or bit value—leaks into the environment through unintended classical side channels. This includes, but is not limited to, electromagnetic emissions, fluctuations in power consumption, thermal signatures, or acoustic noise.[33]

This assumption draws a crucial line between **protocol security** and **implementation security**.[2] The formal statement of assumptions in this chapter pertains to protocol security, which analyzes the abstract sequence of operations under the assumption that the devices, while potentially flawed, are contained within this trusted boundary. Implementation security, by contrast, deals with attacks that explicitly breach this boundary.

A prominent example of such an attack is the **Trojan-horse attack**, where Eve injects bright light into Alice's (or Bob's) device and analyzes the back-reflections to learn about the internal settings of optical components like phase or intensity modulators, thereby revealing Alice's secret choices.[3] While a full security analysis must eventually account for such implementation-specific threats, they are typically modeled separately from the core protocol logic. The seminal Gottesman-Lo-Lütkenhaus-Preskill (GLLP) framework was a major step forward, as it began to incorporate models of device flaws

within the trusted perimeter, such as basis-dependent misalignments, moving beyond the unrealistic assumption of perfect internal hardware.[36]

2.2. Assumption of Perfect Local Resources

Within their secure laboratories, Alice and Bob are assumed to have access to certain ideal resources that are fundamental to the execution of the protocol.

2.2.1. Trusted Randomness

It is assumed that both Alice and Bob have access to **perfect, private, and locally-generated random numbers**.[2] These random numbers are used for every probabilistic choice within the protocol, including:

- Alice's choice of bit value to encode (0 or 1).
- Alice's choice of preparation basis (e.g., Z or X).
- Alice's choice of pulse type (e.g., signal, decoy, or vacuum state).
- Bob's choice of measurement basis.
- The random seeds and functions used in classical post-processing steps like error verification and privacy amplification.

The security of the BB84 protocol is critically dependent on the unpredictability of these choices. If Eve could gain any information about Alice's or Bob's random choices, she could adapt her eavesdropping strategy to significantly increase her information gain while reducing the disturbance she causes. For instance, if Eve could predict Alice's basis choices, she could always measure in the correct basis, thereby learning the bit value without introducing any errors and remaining completely undetected.[39] Therefore, the random number generators (RNGs) used must be true quantum or physical RNGs, and they must be trusted to be unbiased and completely inaccessible to Eve.

2.2.2. Trusted Classical Processing

It is assumed that all classical computation performed by Alice and Bob within their secure laboratories is trusted. This includes the hardware (computers) and software used to execute the classical post-processing stages of the protocol.[34] These stages include:

- **Sifting:** Comparing basis choices over the public channel to identify the subset of rounds where their bases matched.
- **Parameter Estimation:** Calculating the gains and quantum bit error rates (QBERs) for each state type to bound Eve's information.
- **Error Correction:** Running an error correction protocol (e.g., based on LDPC codes) to create identical bit strings.
- **Privacy Amplification:** Applying a hash function from a 2-universal family to their error-corrected string to distill a final, secure key.

The assumption is that these classical systems function exactly as specified by the protocol, are free from malware or Trojan horses, and cannot be remotely accessed or manipulated by Eve. If Eve could compromise the computer on which Bob performs privacy amplification, for example, she could simply steal the final key, bypassing all quantum security measures. Securing these classical assets falls under the purview of conventional cybersecurity, which is considered a separate but equally essential prerequisite for overall system security.

3. Modeling the Quantum Signal and Decoy States

The heart of a practical BB84 security proof lies in the assumptions made about the physical quantum states that are prepared by Alice and measured by Bob. The transition from idealized single-photon sources to practical attenuated lasers necessitated the decoy-state method, which carries its own set of critical physical assumptions.

3.1. The Source: Phase-Randomized Weak Coherent Pulses (WCP)

The ideal BB84 protocol assumes Alice uses a perfect single-photon source.[4] Since such sources are not yet technologically mature for high-speed QKD, practical systems use a highly attenuated laser to generate

weak coherent pulses (WCPs).[3] The security proof must therefore be based on a model of these states.

The central assumption is that Alice's source produces **phase-randomized coherent states**. This means that for each pulse sent, the global phase of the coherent state is randomized uniformly and independently over the interval $[0,2\pi)$.[6] A direct consequence of this assumption is that the state emitted by Alice is not a pure coherent state

$|\alpha\rangle$, but rather a statistical mixture of photon number (Fock) states $|n\rangle$. The probability of emitting an n-photon state is given by a Poisson distribution:

$P(n|\mu)=e-\mu n!\mu n$

where $\mu=|\alpha|2$ is the mean photon number, or intensity, of the pulse. The full density matrix for a pulse of intensity μ is thus:
$$ \rho_\mu = \sum_{n=0}^{\infty} P(n|\mu) |n\rangle\langle n| = \sum_{n=0}^{\infty} e^{-\mu} \frac{\mu^n}{n!} |n\rangle\langle n| $$
This description, known as the photon number channel model, is the mathematical foundation upon which the entire decoy-state analysis is built. If the phase is not perfectly randomized, correlations can exist between subsequent pulses. Eve could potentially exploit these correlations using interferometric measurements to gain information about Alice's encoding, which would invalidate the bounds derived from the decoy-state analysis.6 While some proofs can handle imperfect phase randomization, the standard and simplest model assumes it is

perfect.

3.2. The Core Decoy-State Assumption: Indistinguishability

The decoy-state method is a sophisticated strategy to combat the PNS attack, which is enabled by the non-zero probability of multi-photon emissions from a WCP source. The method's validity hinges on a single, powerful assumption: **indistinguishability**.

It is assumed that the quantum states corresponding to signal pulses and decoy pulses are **perfectly indistinguishable** to Eve in every degree of freedom, *except* for the photon number statistics that result from their different intensity settings.[7] This means that a signal pulse (with intensity

μsig), a decoy pulse (with intensity $\mu decoy$), and a vacuum pulse (with intensity $\mu vac=0$) must have identical properties, including:

- Spectrum (wavelength and bandwidth).
- Temporal profile (pulse shape and timing).
- Polarization or phase encoding modes.
- Spatial mode.

This assumption is the cornerstone of the method. Because Eve cannot differentiate whether an incoming pulse was intended by Alice to be a signal or a decoy, she is forced to apply the same eavesdropping strategy to all pulses that have the same photon number, n. Consequently, the probability that an n-photon pulse will result in a detection at Bob's side (the yield, Yn) and the probability that such a detection will be erroneous (the quantum bit error rate for n-photon events, en) must be independent of the pulse's original intensity setting. Formally:

$$Yn(\mu sig)=Yn(\mu decoy)=Yn$$
$$en(\mu sig)=en(\mu decoy)=en$$

This allows Alice and Bob to use the publicly observable statistics from all intensity settings—namely, the overall gain $Q\mu$ (total detection probability for intensity μ) and overall QBER $E\mu$—to solve a system of linear equations and derive tight upper and lower bounds on the unobservable quantities of interest: the single-photon yield, Y1, and the single-photon error rate, e1. These values are then used in the final key rate formula to determine the amount of secure key that can be extracted from the single-photon contributions to the sifted key.8

If this assumption of indistinguishability is violated, it creates a **side channel**. For example, if decoy pulses have a slightly different temporal shape than signal pulses, Eve could use a fast detector to distinguish them and attack them differently. She could let all decoy pulses pass untouched to fool Alice and Bob into thinking the channel is secure, while selectively attacking only the signal pulses. Such a strategy would completely invalidate the security proof.[3] Therefore, ensuring this indistinguishability in hardware is a critical task for experimentalists.

3.3. The Detector Model: Threshold Detectors and the Squashing Model

Just as the source model must be practical, so too must the detector model. While ideal photon-number-resolving (PNR) detectors, which can count the exact number of photons in a pulse, would simplify the analysis, they are not widely used in high-speed QKD systems.

The standard assumption is that Bob uses **threshold detectors**.[1] These detectors have only two possible outcomes: "no click" (no photons detected) or "click" (one or more photons detected). They cannot distinguish a single-photon event from a multi-photon event.[14]

This practical limitation presents a theoretical challenge. Eve could potentially design an attack that exploits the different ways Bob's detectors might respond to single- versus multi-photon pulses. To close this loophole, security proofs rely on a powerful theoretical tool known as the **squashing model**.[14]

The squashing model assumes that Bob's entire measurement apparatus—including all passive optical elements (like beam splitters and polarizers) and the threshold detectors themselves—can be mathematically described by a single positive operator-valued measure (POVM) acting on the incoming optical modes. The security proof then assumes that this POVM can be conceptually "squashed" into a measurement on a single qubit. In this virtual process, any part of the incoming signal that exists outside the intended qubit space (e.g., multi-photon components) is effectively measured, and the outcome is given to Eve. The remaining state is then projected (or "squashed") onto the qubit space before Bob's measurement is applied. This ensures that any information that could be gained from the multi-photon nature of the state is conservatively assumed to be in Eve's possession. The squashing model provides a rigorous method to prove the security of protocols using imperfect, non-number-resolving detectors, making it an indispensable assumption for practical

QKD.

4. Foundational Assumptions in the Security Proof Logic

The final layer of the assumption stack consists of the abstract mathematical and logical principles that structure the security argument itself. These assumptions connect the physical model of the protocol to the final calculation of a secure key rate.

4.1. The Entanglement-Based Viewpoint

A cornerstone of many modern security proofs, particularly those following the lineage of Shor-Preskill and GLLP, is the assumption of security equivalence between the real **prepare-and-measure (P&M)** protocol and a virtual **entanglement-based (EB)** protocol.[36]

In the real P&M protocol, Alice actively prepares quantum states in one of the BB84 bases and sends them to Bob. In the virtual EB protocol, one imagines that Alice instead prepares a maximally entangled state (e.g., a Bell pair $|\Phi+\rangle=21(|00\rangle+|11\rangle)$), keeps one particle for herself, and sends the other to Bob. She then measures her particle in either the Z or X basis, which has the effect of "steering" or projecting Bob's particle into the corresponding BB84 state.

The assumption is that, from Eve's perspective, these two scenarios are indistinguishable. Any attack Eve can mount against the P&M protocol has a corresponding attack in the EB protocol that yields the same observable statistics. This equivalence is a profoundly useful analytical tool for several reasons:

1. **Symmetry:** It simplifies the analysis by allowing the use of more symmetric entangled states.
2. **Entanglement Distillation:** It connects the problem of QKD security to the well-understood field of entanglement distillation and purification.[41] The secure key rate can be directly related to the rate at which Alice and Bob can distill perfect entangled pairs from the noisy, Eve-disturbed pairs they share.

3. **Defining the Phase Error Rate:** Most importantly, the EB viewpoint provides a clear, unambiguous definition of the **phase error rate**. In the P&M scheme, the phase error rate is a counterfactual quantity—it is the error rate that Alice and Bob *would have* observed had they measured in the conjugate basis. In the EB protocol, this is no longer counterfactual. The bit error rate (ebit) is found by comparing their measurement outcomes when they both measure in the Z basis. The phase error rate (ephase) is found by comparing their outcomes when they both measure in the X basis. Both are well-defined physical quantities in the virtual protocol.

This assumption allows the security proof to be framed as a task of bounding the phase error rate based on the observable bit error rate, which is the central challenge addressed in the following section.

4.2. Channel Symmetry and the Phase Error Rate

The relationship between the bit error rate and the phase error rate is one of the most critical and subtle aspects of the BB84 security proof. The evolution of assumptions in this area is a clear indicator of the increasing sophistication and practicality of the proofs.

In an early, idealized BB84 protocol, a crucial simplifying assumption was often made: the phase error rate is equal to the bit error rate, i.e., ephase=ebit. The justification for this stems from the perfect symmetry of the protocol. If Alice prepares one of the four states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ with perfect fidelity, and the Z and X bases are perfectly orthogonal, then there is no information available in the physical states themselves that could allow Eve to distinguish which basis was used for preparation. Any attack Eve applies must therefore be symmetric with respect to the Z and X bases. A symmetric attack that causes a certain rate of bit flips (Z-basis errors) must necessarily cause the same rate of phase flips (X-basis errors).[13] This assumption is powerful because it allows Alice and Bob to estimate the unobservable phase error rate simply by measuring the bit error rate from a random sample of their sifted key, without needing to "waste" key bits by explicitly measuring in the X basis.

However, this elegant symmetry breaks down in the face of real-world device imperfections. In any practical implementation, the state preparation will have small, basis-dependent flaws.[3] For example:

- **Polarization Misalignment:** The angle between the Z and X basis states on the Bloch sphere may not be exactly π/2.
- **Intensity Fluctuations:** The intensity of the laser pulse might fluctuate differently when preparing Z-basis states versus X-basis states.

These imperfections create **basis-dependent flaws** in the source.[13] Such flaws act as a side channel, providing Eve with a handle to gain information about Alice's basis choice. Once Eve can distinguish the bases, even with a small probability, her attack no longer needs to be symmetric. She could, in principle, devise a sophisticated attack that minimizes the disturbance in the Z basis (leading to a low observed ebit) while maximizing the disturbance in the X basis (leading to a high, unobserved ephase). If Alice and Bob were to naively assume ephase=ebit, they would drastically underestimate the amount of information Eve has gained and, as a result, distill a final key that is not secure.

Therefore, a modern, robust security proof **must not assume that ephase=ebit**. Instead, it must assume that they are unequal and that the phase error rate must be bounded directly from experimental data. This has a direct impact on the protocol design. It necessitates that Alice and Bob sacrifice a randomly chosen fraction of their sifted key bits for the express purpose of parameter estimation in the conjugate basis. For instance, in the "efficient BB84" protocol, where the Z basis is used more often for key generation, a smaller fraction of rounds are designated where both parties agree to announce their X-basis measurement outcomes to directly estimate and bound ephase.[14] This explicit measurement is the only way to guarantee security in the presence of realistic, basis-dependent source flaws.

4.3. Finite-Key Analysis

The final major logical assumption relates to the length of the key. Early security proofs were often performed in the **asymptotic limit**, where the number of signals exchanged, N, approaches infinity ($N \to \infty$). In this limit, the law of large numbers applies perfectly. The observed frequencies of events (e.g., the QBER) are assumed to be exactly equal to their true underlying probabilities.

While mathematically convenient, this assumption is physically unrealistic. Any real-world implementation of QKD involves the exchange of a **finite** number of signals.[11] Therefore, a practical security proof must be conducted under the assumption of a finite block size

N.

This has profound consequences for the security analysis. All parameters estimated from the experimental data—such as the gains Q_μ and error rates E_μ—are now statistical estimates based on finite samples, not certainties. They are subject to statistical fluctuations. The proof must account for this uncertainty by using concentration inequalities, such as the Chernoff bound or Hoeffding's inequality.[14] These tools allow one to state that, with a very high confidence level (e.g.,

$1-\epsilon_{PE}$ where ϵ_{PE} is the failure probability of parameter estimation), the true value of a parameter lies within a certain confidence interval around the observed value.

The implication is that Alice and Bob must take a more conservative (worst-case) estimate of the channel parameters. For example, to calculate the key rate, they must use an upper bound on the single-photon error rate (e_1) and a lower bound on the single-photon yield (Y_1). These bounds become wider for smaller block sizes N. As a result, the final secure key length is not just a function of the observed channel parameters but is also strongly dependent on the total block size N and the chosen security parameter ϵ_{QKD}. The finite-key assumption is thus essential for providing security guarantees that are valid for real, operational QKD systems.

5. Summary and Conclusion: A Hierarchy of Trust

The security of the decoy-state BB84 protocol is not a monolithic statement but a conclusion derived from a carefully constructed hierarchy of assumptions—an "assumption stack" that bridges the abstract world of quantum theory with the messy reality of experimental physics. This chapter has systematically dissected this stack, revealing that the strength of a modern QKD security proof lies not in its appeal to perfection, but in its rigorous accounting of imperfection.

The foundation of the stack is the abstract adversarial model, where an omnipotent eavesdropper is granted the full power allowed by quantum mechanics, including the ability to perform general coherent attacks. The security goal is defined against this powerful adversary, demanding a key that is not only secret in isolation but also universally composable, ensuring its safe use in any subsequent application. This framework is built upon the assumption of trusted domains for Alice and Bob, where their local randomness and classical processing are secure, drawing a clear line between protocol security and implementation security.

Building upon this, the physical layers of the stack replace idealized components with realistic models. The perfect single-photon source is replaced by a phase-randomized weak coherent pulse source, a move that necessitates the decoy-state method. The validity of this method, in turn, rests on the crucial assumption that signal and decoy pulses are physically indistinguishable to the adversary. Similarly, perfect detectors are replaced by practical threshold detectors, a gap bridged by the theoretical construct of the squashing model.

Finally, the logical structure of the proof itself contains foundational assumptions. The entanglement-based viewpoint provides the language to discuss the critical phase error rate. The historical assumption of channel symmetry, leading to ephase=ebit, is now understood as an oversimplification that fails in the presence of realistic basis-dependent source flaws. It has been replaced by the more robust requirement that the protocol must explicitly test for phase errors. Crowning the entire structure is the assumption of a finite key length, which moves the proof from an asymptotic ideal to a practical reality by incorporating the unavoidable effects of statistical fluctuations.

The evolution from the early GLLP framework [36] to the state-of-the-art, finite-size, composable decoy-state proofs [1] exemplifies a mature scientific process: a vulnerability is identified due to an unrealistic assumption; the assumption is relaxed to reflect reality; and a new theoretical tool is developed to re-establish security under the weaker, more realistic conditions. The set of assumptions detailed in this chapter represents the current consensus for this rigorous foundation. They provide a clear and defensible basis for the analysis, evaluation, and certification of practical QKD systems.[2] The ongoing work in the field continues this trajectory, aiming to further weaken these assumptions by, for example, developing proofs that are more resilient to a wider range of side channels or that require less a priori device characterization, continually strengthening the bridge between the theory of quantum security and its practice.[15]

منابع مورداستناد

1. QKD security proofs for decoy-state BB84: protocol variations, proof ..., زمان دسترسی: اوت 11, 2025، https://arxiv.org/abs/2502.10340
2. QKD security proofs for decoy-state BB84: protocol variations, proof techniques,

gaps and limitations - arXiv, زمان دسترسی: اوت 11, 2025، https://arxiv.org/html/2502.10340v1

3. Security of the decoy-state BB84 protocol with imperfect state ..., زمان دسترسی: اوت 11, 2025، https://arxiv.org/pdf/2310.01610
4. PowerPoint Presentation - University of Toronto, زمان دسترسی: اوت 11, 2025، https://www.fields.utoronto.ca/programs/scientific/04-05/quantumIC/abstracts/lo.ppt
5. Modeling, Simulation, and Performance Analysis of Decoy State ..., زمان دسترسی: اوت 11, 2025، https://www.mdpi.com/2076-3417/7/2/212
6. Hacking on decoy-state quantum key distribution system with partial phase randomization, زمان دسترسی: اوت 11, 2025، https://pmc.ncbi.nlm.nih.gov/articles/PMC3996487/
7. Performance analysis of decoy state quantum key distribution over underwater turbulence channels - University of Edinburgh Research Explorer, زمان دسترسی: اوت 11, 2025، https://www.research.ed.ac.uk/files/280501433/Amir_decoyQKD_preprint.pdf
8. Decoy State Quantum Key Distribution | Phys. Rev. Lett., زمان دسترسی: اوت 11, 2025، https://link.aps.org/doi/10.1103/PhysRevLett.94.230504
9. (PDF) Decoy State Quantum Key Distribution - ResearchGate, زمان دسترسی: اوت 11, 2025، https://www.researchgate.net/publication/7670797_Decoy_State_Quantum_Key_Distribution
10. Finite-Size Analysis of Prepare-and-Measure and Decoy-State Quantum Key Distribution via Entropy Accumulation - Physical Review Link Manager, زمان دسترسی: اوت 11, 2025، https://link.aps.org/doi/10.1103/PRXQuantum.6.020342
11. [2405.16578] A consolidated and accessible security proof for finite-size decoy-state quantum key distribution - arXiv, زمان دسترسی: اوت 11, 2025، https://arxiv.org/abs/2405.16578
12. The Universal Composable Security of Quantum Key Distribution - ResearchGate, زمان دسترسی: اوت 11, 2025، https://www.researchgate.net/publication/221354090_The_Universal_Composable_Security_of_Quantum_Key_Distribution
13. Security of the Decoy-State BB84 Protocol with Imperfect State ..., زمان دسترسی: اوت 11, 2025، https://pmc.ncbi.nlm.nih.gov/articles/PMC10670654/
14. Efficient decoy-state quantum key distribution with quantified security, زمان دسترسی: اوت 11, 2025، https://opg.optica.org/oe/abstract.cfm?URI=oe-21-21-24550
15. Modified BB84 quantum key distribution protocol robust to source imperfections | Phys. Rev. Research - Physical Review Link Manager, زمان دسترسی: اوت 11, 2025، https://link.aps.org/doi/10.1103/PhysRevResearch.5.023065
16. The Universal Composable Security of Quantum Key Distribution - IACR, زمان دسترسی: اوت 11, 2025، https://www.iacr.org/cryptodb/archive/2005/TCC/3598/3598.pdf
17. Quantum key distribution - Wikipedia, زمان دسترسی: اوت 11, 2025، https://en.wikipedia.org/wiki/Quantum_key_distribution
18. Quantum Key Distribution (QKD) - ETSI, زمان دسترسی: اوت 11, 2025،

https://www.etsi.org/technologies/quantum-key-distribution

19. Advance in Security Proofs of Quantum Key Distribution and Its Challenges towards Practical Implementation, زمان دسترسی: اوت 11, 2025، https://www.imes.boj.or.jp/research/papers/english/25-E-03.pdf
20. BB84 - Wikipedia, زمان دسترسی: اوت 11, 2025، https://en.wikipedia.org/wiki/BB84
21. Quantum Key Distribution (QKD) and the BB84 Protocol, زمان دسترسی: اوت 11, 2025، https://postquantum.com/post-quantum/qkd-bb84/
22. [2507.04248] Security of the BB84 protocol with receiver's passive biased basis choice, زمان دسترسی: اوت 11, 2025، https://arxiv.org/abs/2507.04248
23. Experimental composable security decoy-state quantum key distribution using time-phase encoding - preprints from Optica Open, زمان دسترسی: اوت 11, 2025، https://preprints.opticaopen.org/articles/preprint/Experimental_composable_security_decoy-state_quantum_key_distribution_using_time-phase_encoding/24698046
24. [2504.20417] Protocol-level description and self-contained security proof of decoy-state BB84 QKD protocol - arXiv, زمان دسترسی: اوت 11, 2025، https://arxiv.org/abs/2504.20417
25. [1006.2215] Composability in quantum cryptography - arXiv, زمان دسترسی: اوت 11, 2025، https://arxiv.org/abs/1006.2215
26. Composability in quantum cryptography - Research Collection, زمان دسترسی: اوت 11, 2025، https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/16804/2/M%C3%BCller-Quade_2009_New_J._Phys._11_085006.pdf
27. Security of differential-phase-shift quantum key distribution against individual attacks | Phys. Rev. A - Physical Review Link Manager, زمان دسترسی: اوت 11, 2025، https://link.aps.org/doi/10.1103/PhysRevA.73.012344
28. Universally Composable Privacy Amplification Against Quantum Adversaries - IACR, زمان دسترسی: اوت 11, 2025، https://www.iacr.org/archive/tcc2005/3378_406/3378_406.pdf
29. What is universal composability guaranteeing, specifically? Where does it apply, and where does it not? - Cryptography Stack Exchange, زمان دسترسی: اوت 11, 2025، https://crypto.stackexchange.com/questions/85739/what-is-universal-composability-guaranteeing-specifically-where-does-it-apply
30. [PDF] The Universal Composable Security of Quantum Key Distribution - Semantic Scholar, زمان دسترسی: اوت 11, 2025، https://www.semanticscholar.org/paper/The-Universal-Composable-Security-of-Quantum-Key-Ben-Or-Horodecki/ddb468e0267d904d7a8edb83fb489a883ee35e54
31. Security of the decoy state method for quantum key distribution - ResearchGate, زمان دسترسی: اوت 11, 2025، https://www.researchgate.net/publication/347592839_Security_of_the_decoy_state_method_for_quantum_key_distribution
32. Practical issues in quantum-key-distribution postprocessing | Phys. Rev. A, زمان دسترسی: اوت 11, 2025، https://link.aps.org/doi/10.1103/PhysRevA.81.012318
33. On the Security of Quantum Key Distribution Networks - MDPI, زمان دسترسی: اوت 11,

2025، https://www.mdpi.com/2410-387X/7/4/53

34. ETSI GS QKD 005 V1.1.1 (2010-12), زمان دسترسی: اوت 11, 2025، https://www.etsi.org/deliver/etsi_gs/qkd/001_099/005/01.01.01_60/gs_qkd005v010101p.pdf
35. Security of the decoy-state BB84 protocol with imperfect state ..., زمان دسترسی: اوت 11, 2025، https://arxiv.org/abs/2310.01610
36. [quant-ph/0212066] Security of quantum key distribution with imperfect devices - arXiv, زمان دسترسی: اوت 11, 2025، https://arxiv.org/abs/quant-ph/0212066
37. Security of quantum key distribution with imperfect devices | Request PDF - ResearchGate, زمان دسترسی: اوت 11, 2025، https://www.researchgate.net/publication/350096334_Security_of_quantum_key_distribution_with_imperfect_devices
38. Security of quantum key distribution with imperfect ... - John Preskill, زمان دسترسی: اوت 11, 2025، https://preskill.caltech.edu/pubs/preskill-2004-imperfect.pdf
39. Randomness determines practical security of BB84 quantum key distribution - PMC, زمان دسترسی: اوت 11, 2025، https://pmc.ncbi.nlm.nih.gov/articles/PMC4639782/
40. Enhancing the Security of the BB84 Quantum Key Distribution Protocol against Detector-Blinding Attacks via the Use of an Active Quantum Entropy Source in the Receiving Station - MDPI, زمان دسترسی: اوت 11, 2025، https://www.mdpi.com/1099-4300/25/11/1518
41. [quant-ph/0105121] Proof of security of quantum key distribution with two-way classical communications - arXiv, زمان دسترسی: اوت 11, 2025، https://arxiv.org/abs/quant-ph/0105121
42. Decoy-state quantum key distribution with two-way classical postprocessing | Phys. Rev. A, زمان دسترسی: اوت 11, 2025، https://link.aps.org/doi/10.1103/PhysRevA.74.032330
43. Numerical security proof for the decoy-state BB84 protocol and measurement-device-independent quantum key distribution resistant against large basis misalignment | Phys. Rev. Research, زمان دسترسی: اوت 11, 2025، https://link.aps.org/doi/10.1103/PhysRevResearch.4.043097