Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

High-Capacity Multi-Copy Quantum Key Distribution via Hypercontractive Complexity Games

Nilesh Vyas

nilesh.vyas@airbus.com

Airbus (Germany)

Research Article

Keywords:

Posted Date: November 16th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10354796/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

High-Capacity Multi-Copy Quantum Key Distribution via Hypercontractive Complexity Games

Nilesh Vyas[1*]

[1*]Airbus Central R&T, Taufkirchen, 82024 Germany.

Corresponding author(s). E-mail(s): nilesh.vyas@airbus.com;

Abstract

The rate-loss trade-off in repeaterless quantum key distribution (QKD) bounds the secret key capacity of optical links. The Quantum Computational Timelock (QCT) framework overcomes this limit by utilizing the difference between computational security and quantum memory coherence times. We introduce the Information Reconciled Khot-Vishnoi (IR-KV-QCT) protocol, which maps the Khot-Vishnoi communication complexity game onto a high-dimensional prepare-and-measure QKD scheme under the QCT framework. Using a large-alphabet phase encoding, the protocol transmits $\mathbf{log_2}\, \boldsymbol{n}$ bits per qudit and corrects phase-alignment and channel-induced decoding errors via non-binary Slepian-Wolf Information Reconciliation. To combat channel attenuation, the protocol transmits identical copies of each state. We prove that this multi-copy ensemble is confined to the symmetric subspace, whereby Holevo's theorem strictly bounds the adversary's accessible information from an immediate measurement. Furthermore, we demonstrate that current and near-future quantum error correction thresholds are insufficient to sustain coherent attacks under the QCT framework, thereby limiting the operational threat model to collective attacks. Under this constraint, we bound the adversary's accessible information and prove the security of the protocol using the hypercontractivity of the Khot-Vishnoi game. This exponential suppression of information extraction supports a secure multi-copy transmission threshold of $\boldsymbol{\mathcal{O}(n/\log_2 n)}$. Consequently, the protocol circumvents the exponential rate-loss decay of single-photon schemes, enabling high-capacity key rates with everlasting security against collective attacks.

1 Introduction

Quantum Cryptography:

Quantum cryptography achieves unconditional security by relying on quantum mechanics rather than computational hardness assumptions Bennett and Brassard [2014]. While multi-copy signalling mitigates channel losses and boosts key rates, it introduces a fatal security vulnerability in standard protocols by enabling photon-number-splitting attacks Brassard et al. [2000]. Decoy-state protocols Lo et al. [2005] address this vulnerability and permit higher signal intensities ($\mu \approx 1$); nevertheless, the secret key capacity of conventional prepare-and-measure QKD remains strictly limited by channel loss Diamanti et al. [2016]. While standard prepare-and-measure architectures are strictly limited by the exponential scaling of fiber attenuation (the PLOB bound) Pirandola et al. [2017], techniques like Twin-Field QKD Lucamarini et al. [2018] can overcome this limit. Nevertheless, achieving high-capacity scaling without the infrastructural requirements of global phase-locking remains a primary challenge.

Quantum Computational Timelock (QCT) Framework:

The QCT framework Vyas and Alleaume [2020], Vyas [2021], Mazzoncini et al. [2025] establishes everlasting security by replacing physical channel boundaries with local computational and memory constraints. The security model relies on two core assumptions: (i) a t_{comp}-secure encryption scheme that conceals classical encoding parameters from a computationally bounded adversary for a duration t_{comp}, and (ii) a $(t_{\text{comp}}, \delta)$-noisy quantum memory register $\mathcal{H}_Q$ held by Eve. Because the memory coherence time is assumed as $t_{\text{coh}} \ll t_{\text{comp}}$, the time-dependent storage channel Φ_t decays toward the completely depolarizing channel $\mathcal{F}(\cdot) := \frac{\text{Tr}[\cdot]}{d}\mathbb{I}_d$. This channel degradation is strictly bounded in diamond norm by $\frac{1}{2}\|\Phi_{t_{\text{comp}}} - \mathcal{F}\|_\diamond \leq \delta \ll 1$. Consequently, Eve must execute a basis-independent measurement before the computational lock expires, reducing her quantum storage advantage to bounded classical side information. Since this depolarization is irreversible, future upgrades cannot retroactively recover the lost quantum information. By operating within this hybrid model, the protocol functions in the regime of everlasting security Unruh [2012], enabling high-rate key distribution over lossy links Mazzoncini et al. [2025].

IR-KV-QCT Protocol:

The primary contribution of this work is the Information Reconciled Khot-Vishnoi (IR-KV-QCT) protocol, which maps classical communication complexity to high-dimensional quantum state design. While early QCT protocols like Hidden Matching Mazzoncini et al. [2025] relaxed the single-photon constraint, they relied on bit-wise encoding yielding a classical hardness of $2^{-\Omega(\sqrt{n})}$ Gavinsky et al. [2006], which severely restricted multi-copy transmission thresholds. We overcome this limitation by applying the Khot-Vishnoi game Khot and Vishnoi [2013], Buhrman et al. [2011] to implement a large-alphabet encoding that transmits $\log_2 n$ bits of raw entropy per qudit. Because Bob's optimal quantum strategy for this high-dimensional game requires a probabilistic Fourier measurement, his raw output inherently contains localised physical errors. To resolve this, we integrate a non-binary Slepian-Wolf Information

Reconciliation (IR) scheme Slepian and Wolf [1973], Liveris et al. [2002], Mueller et al. [2024c] tailored for large-alphabet high-dimensional encodings. Although this high-dimensional architecture requires Bob to operate an array of n independent detection channels, it applies a hypercontractive classical hardness bound Bonami [1970], Beckner [1975] that exponentially suppresses the adversary's success probability as $2^{-\Omega(n)}$. This linear dependence in the exponent restricts classical information extraction, permitting a multi-copy transmission threshold of $m \sim \mathcal{O}(n/\log_2 n)$ to offset channel attenuation while preserving a strict exponential security margin.

Protocol Sketch:

The IR-KV-QCT protocol achieves this complexity separation via a prepare-and-measure sequence. Alice executes the Khot-Vishnoi encoding by selecting a vector a from a randomly shifted coset Y on the Boolean hypercube and encoding it into the phase of an n-dimensional quantum state. To secure the multi-copy transmission, Alice transmits m identical copies of the state. Because the underlying string a is sampled uniformly, the transmitted multi-copy ensemble $\rho_{\text{avg}}^{\otimes m}$ forms a statistical mixture of identical pure states. Consequently, the support of this ensemble is strictly confined to the symmetric subspace, enforcing a strict Holevo limit on any immediate adversarial measurement.

To establish an operational asymmetry, the protocol encrypts the classical coset parameters Y and a base Slepian-Wolf syndrome within a short-term computational timelock ciphertext. Bob decrypts this ciphertext upon arrival and dynamically measures the states using a passive Fourier receiver defined by Y. Conversely, Eve must buffer the intercepted photons in a $(t_{\text{comp}}, \delta)$-noisy quantum memory. Because the space-time overhead of fault-tolerant quantum error correction physically precludes coherent attacks during the timelock window, her uncorrected quantum register depolarises ($t_{\text{coh}} \ll t_{\text{comp}}$). This physical constraint restricts the adversary to collective attacks, forcing an immediate, basis-independent measurement that reduces her quantum storage advantage to classical side information. Upon timelock expiration, Eve's extractable information remains bounded by the hypercontractive limits of the Khot-Vishnoi game. Finally, because Bob's raw quantum measurement is probabilistic and subject to physical channel noise, he utilises the decrypted Slepian-Wolf syndrome to reconcile localised errors with high probability before privacy amplification.

Core Advantages:

This hybrid architecture provides two primary operational advantages over conventional QKD:

- *Enhanced Key Rate and Reach:* Traditional QKD restricts signal intensity to prevent photon-number-splitting attacks, causing key rates to decay exponentially with distance. Here, because the timelock protects the basis until Eve's memory depolarises ($t_{\text{coh}} \ll t_{\text{comp}}$), the hypercontractive hardness of the Khot-Vishnoi game allows Alice to scale her transmission to $m \sim \mathcal{O}(n/\log_2 n)$ copies. This multi-copy signalling overcomes channel attenuation to elevate secret key rates, enabling high-capacity key distribution over long distances.

- *Elimination of Receiver Quantum Storage:* Unlike high-capacity alternatives like quantum data locking Lupo [2015], Lupo and Lloyd [2014, 2015] that require a receiver to store fragile states in quantum memory while awaiting classical basis updates, Bob measures incoming qudits dynamically upon arrival.The computationally intensive decryption and decoding steps are executed entirely offline, shifting the core hardware limit away from quantum storage interfaces and onto scalable classical computing.

Structure of the paper:

The remainder of this paper is organised as follows. In Sec. 2, we formalise the QCT threat model, the Khot-Vishnoi game, and the underlying cryptographic primitives. In Sec. 3, we detail the structural mechanics of the IR-KV-QCT protocol, including the prepare-and-measure reduction. Sec. 4 and Sec. 5 provide a comprehensive security analysis against collective attacks, bounding the adversary's accessible information via hypercontractive limits. In Sec. 6, we demonstrate protocol correctness and exact physical channel splitting. Sec. 7 presents the asymptotic and finite-key rate analysis, and Sec. 8 maps the protocol's physical performance against standard bounds. Finally, in Sec. 9, we discuss the technological feasibility and hardware constraints of high-dimensional physical implementations, followed by concluding remarks in Sec. 10.

2 Preliminaries

We formalise the mathematical notation, the adversarial threat model, and the source-coding theorems underpinning the IR-KV-QCT protocol.

2.1 Notation and Cryptographic Primitives

Let $\mathcal{H}$ denote a finite-dimensional Hilbert space. The space of density operators (positive semi-definite, trace-class operators with unit trace) acting on $\mathcal{H}$ is denoted by $\mathcal{D}(\mathcal{H})$, and the space of linear operators is denoted by $\mathcal{L}(\mathcal{H})$. The spectral norm of an operator A is denoted $\|A\|_\infty$, and the trace norm is $\|A\|_1 = \mathrm{Tr}[\sqrt{A^\dagger A}]$. The trace distance between two quantum states ρ and σ is defined as $D(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_1$

For quantum channels (Completely Positive Trace-Preserving maps), distance is measured using the diamond norm $\|\Phi\|_\diamond = \sup_\rho \|(\Phi \otimes \mathbb{I}_{anc})(\rho)\|_1$, which bounds the maximum distinguishability of the channel even when acting on auxiliary, entangled states.

Classical random variables are denoted by capital letters (e.g., X, Y), with specific realisations in lowercase (x, y). The Boolean hypercube is denoted $G = \{0,1\}^n$, where the dimension is strictly a power of two ($n = 2^k$) to ensure the existence of the Galois field $\mathbb{F}_n$. A predefined Hadamard subgroup $H \subset \{0,1\}^n$ of size n partitions G into $2^n/n$ distinct cosets. Corresponding field addition and subtraction are denoted by $\oplus$ and $\ominus$. The uniform random sampling of an element x from a set S is denoted $x \xleftarrow{\$} S$. The operational measure of uncertainty from an adversary's perspective is quantified by the conditional smooth min-entropy $H^\epsilon_{min}(X|E)$, representing the negative logarithm of the maximum probability that an adversary with access to quantum side-information E can correctly guess the variable X, allowing for a failure probability ϵ.

2.2 The Quantum Computational Timelock (QCT) Security Model

The security architecture operates within the QCT framework Vyas and Alleaume [2020], Mazzoncini et al. [2025], which replaces unconditional information-theoretic security with everlasting security. Provided the initial computational encryption holds during the brief quantum transmission window, the distilled keys remain secure against future computationally unbounded adversaries. The model relies on two formal assumptions:

Definition 1 (t_{comp}-secure encryption) An encryption scheme is t_{comp}-secure if it guarantees computational security against an adversary for a time at least t_{comp} after the ciphertext is broadcast.

Achieving this temporal guarantee requires bounding the adversary's parallel computational capacity or utilising sequential time-release cryptography Unruh [2015, 2007] (such as timelock puzzles). Here, Alice and Bob denote authorised parties with access to t_{comp}-secure encryption, while Eve represents the unauthorised adversary.

Definition 2 ((t_{comp}, δ)-noisy quantum memory) A (t_{comp}, δ)-noisy quantum memory is a completely positive, trace-preserving (CPTP) Markovian time-dependent map Φ_t such that at time t_{comp}, its distance to the completely depolarizing channel $\mathcal{F}(\rho) := \frac{\mathrm{Tr}[\rho]}{d}\mathbb{I}_d$ is bounded by δ:

$$\frac{1}{2}\left|\left|\Phi_{t_{comp}} - \mathcal{F}\right|\right|_{\diamond} \leq \delta, \tag{1}$$

where $||\cdot||_{\diamond}$ is the diamond norm, and d is the dimension of the memory.

The parameter $\delta \ll 1$ is fundamentally determined by the coherence time $t_{coh} \ll t_{comp}$. This model assumes Eve's optimal hardware is strictly bounded by this diamond norm distance, and that she cannot implement fault-tolerant Quantum Error Correction (QEC) with sufficient fidelity and low enough overhead to extend the logical coherence time past t_{comp}. This assumption of time-limited quantum storage aligns with the noisy-storage model Wehner et al. [2008] and quantum data locking (QDL) constructions Lupo and Lloyd [2014, 2015].

Definition 3 (QCT security model) The model consists of two concurrent assumptions:

1. Alice and Bob communicate privately using t_{comp}-secure encryption (Definition 1).
2. Eve's quantum memories are restricted to a (t_{comp}, δ)-noisy quantum memory (Definition 2) due to a physical coherence time $t_{coh} \ll t_{comp}$, preventing reliable storage of quantum states beyond t_{comp}.

We operate under a stringent threat model analogous to strong quantum data locking Lupo [2015], where Eve has complete, direct access to both classical and quantum channels, allowing her to perfectly intercept and retain all transmissions.

To establish secure keys, the QCT model leverages the interplay between computational hardness and physical storage constraints. For classical communication, we require an encryption scheme achieving ciphertext indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) for a minimum duration t_{comp}. Crucially, because the adversary is presumed to possess real-time quantum processing capabilities alongside their $(t_{\text{comp}}, \delta)$-noisy quantum memory, this encryption must be, for example, a computationally secure Post-Quantum Cryptography (PQC) algorithm (e.g., lattice-based cryptography). Ensuring the algorithm resists the optimal decryption attack for at least t_{comp} prevents the adversary from instantly extracting the basis before their physical memory undergoes Markovian depolarisation. Crucially, the classical hardware must be hardened against side-channel leakage, as early basis exposure would compromise the quantum min-entropy bounds.

Consequently, the authorised receiver (Bob) can measure incoming states dynamically without quantum storage, whereas Eve must buffer the states in a noisy quantum memory. Because $t_{coh} \ll t_{comp}$, these buffered states strictly depolarise before the computational timelock expires. To avoid total information loss, Eve is forced to execute a collective measurement before basis revelation.

2.3 The Khot-Vishnoi (KV) Game

The Khot-Vishnoi game Khot and Vishnoi [2013], Buhrman et al. [2011] separates randomised classical communication complexity from quantum complexity. The problem is defined over a Boolean hypercube $G = \{0,1\}^n$, where a predefined subgroup $H \subset \{0,1\}^n$ of size n (consisting of Hadamard codewords) partitions G into $2^n/n$ distinct cosets.

Alice receives a uniformly random coset $x = u \oplus H$. Bob receives a correlated coset $y = u \oplus z \oplus H$, where the noise string $z \in \{0,1\}^n$ is generated by independently setting each bit to 1 with probability η. The objective is for Alice to output $a \in x$ and Bob to output $b \in y$ such that $a \oplus b = z$.

The maximum success probability of any randomised classical strategy constrained by a communication budget c is limited by the Bonami-Beckner hypercontractive inequality Bonami [1970], Beckner [1975], Buhrman et al. [2011]:

$$P_{succ}^{classical} \leq 2^{c-\gamma n} \tag{2}$$

where $\gamma = \Omega\left(\frac{\eta}{1-\eta}\right)$. To achieve a non-negligible success probability, an adversary must extract at least $c \geq \gamma n$ bits of classical information.

For a constant noise bias $\eta \in (0, 1/2)$, the hardness parameter $\gamma = \Omega(1)$ is strictly positive. Consequently, if the classical communication budget is sub-linear, such as $c \leq \mathcal{O}(n/\log_2 n)$, the linear penalty $-\gamma n$ strictly dominates the exponent. The maximal classical success probability thus remains exponentially suppressed:

$$P_{succ}^{classical} \leq 2^{-\Omega(n)} \tag{3}$$

Conversely, the optimal quantum strategy achieves an exponential separation in communication complexity Buhrman et al. [2011]. Alice and Bob pre-share an n-dimensional maximally entangled bipartite state, requiring $\log_2 n$ physical qubits per party. Alice measures her subsystem in the Fourier basis corresponding to her coset x and obtains outcome a. This project Bob's subsystem into a phase-encoded state defined by a. Bob then measures his subsystem in the shifted Fourier basis corresponding to his coset y. This global quantum Fourier measurement directly yields an outcome b satisfying $a \oplus b = z$ with a success probability dependent only on the noise bias:

$$P_{succ}^{quant} = (1 - 2\eta)^2 \tag{4}$$

By transmitting only the $\log_2 n$-bit basis description, this quantum strategy succeeds with constant probability utilizing $\mathcal{O}(\log_2 n)$ bits of communication, strictly bypassing the $\Omega(n)$ classical bottleneck.

2.4 Slepian-Wolf Information Reconciliation

The Slepian-Wolf theorem Slepian and Wolf [1973], Mueller et al. [2024c] defines the fundamental limit for lossless compression between correlated data sources. In this protocol, Alice's target string b^* and Bob's noisy measurement b_{out} map to the input and output of an n-ary symmetric channel. To allow Bob to perfectly reconstruct b^*, Alice transmits a compressed syndrome sequence over the Galois field $\mathbb{F}_n$ at a rate bounded by the conditional entropy $H(b^*|b_{\text{out}})$. To accommodate fluctuating channel noise, we implement a rate-adaptive information reconciliation scheme utilising non-binary Low-Density Parity-Check (LDPC) codes over $\mathbb{F}_n$ Liveris et al. [2002], Mueller et al. [2024b], chronologically structured within the Quantum Computational Timelock (QCT) framework (detailed in Appendix B):

1. *Base Syndrome (S_{base}):* Calculated for an expected baseline channel error rate, S_{base} is encapsulated within the computational timelock ciphertext at $t = 0$. This ensures Bob can initiate immediate offline error correction upon basis decryption.
2. *Adaptive Syndrome (S_{adapt}):* If transient channel noise exceeds the baseline, Bob interactively requests additional parity data. Alice immediately encrypts and transmits S_{adapt} using the same t_{comp}-secure scheme.

Crucially, because S_{adapt} is computationally locked, the adversary cannot access this classical side-information until the ciphertexts expire. By that time, Eve's quantum memory has completely depolarised due to coherence time limits ($t_{\text{coh}} \ll t_{\text{comp}}$), ensuring the delayed classical leakage introduces no quantum vulnerabilities.

3 The IR-KV-QCT Protocol

We introduce the Information-Reconciled Khot-Vishnoi (IR-KV-QCT) protocol. This protocol maps a classical communication complexity game onto a high-dimensional prepare-and-measure (P&M) scheme to achieve high-capacity quantum key distribution.

3.1 High-Dimensional Prepare-and-Measure Reduction

While the standard Khot-Vishnoi game requires a bipartite entangled state of dimension $2^n/n$ (representing the total number of cosets) Buhrman et al. [2011], our protocol achieves a significant dimensional reduction via a Prepare-and-Measure (P&M) reduction. By directly encoding the selected n-bit string $a \in X$ into the phases of an n-dimensional computational basis, Alice prepares and transmits the state $|\psi_a\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{a_i} |i\rangle$. This mapping completely decouples the quantum Hilbert space dimension (n) from the number of cosets ($2^n/n$). Consequently, the protocol retains the strict classical hypercontractive hardness bound of $\mathcal{O}(\gamma n)$ derived from the hypercube string length, while restricting the adversary's per-copy Holevo extraction to $\log_2 n$ bits.

Because Alice selects the base string u uniformly at random, the marginal distribution of the encoded vector a is perfectly uniform over $\{0,1\}^n$. Consequently, the statistical mixture of the m-copy transmission forms a uniform ensemble. Since this ensemble consists entirely of identical pure states, its support is strictly confined to the symmetric subspace $\mathrm{Sym}^m(\mathbb{C}^n)$. This geometric restriction bounds the adversary's accessible information to $I_{acc} \leq \mathcal{O}(\log_2 d_{\mathrm{sym}})$, physically shielding the channel.

Remark 1 (Large-Alphabet Encoding vs. Bit-Wise Distillation) Previous QCT protocols Mazzoncini et al. [2025] extract a single secure bit per round using a Goldreich-Levin (GL) reduction Goldreich and Levin [1989]. However, applying single-bit distillation to the probabilistic quantum Fourier measurement required for the Khot-Vishnoi game induces critical error amplification, collapsing the hypercontractive hardness bound (see Appendix F for the complete formal proof). To resolve this, the IR-KV-QCT protocol omits single-bit distillation and operates entirely in the large-alphabet regime, directly transmitting and reconciling the full $\log_2 n$ bits of raw entropy per qudit.

3.2 Protocol Encoding and Decoding

The cryptographic pipeline operates through three successive encoding stages. First, Alice uses a secret base string u and a noise string z to define the shifted coset $Y = u \oplus z \oplus H$, outputting the target string $b^* = a \oplus z \in Y$. Second, she compresses b^* into a k-symbol public syndrome $S = H_{\mathrm{PC}} b^*$ using a non-binary LDPC parity-check matrix $H_{\mathrm{PC}} \in \mathbb{F}_n^{k \times n}$ with arithmetic evaluated over $\mathbb{F}_n$. Finally, Alice maps the string a directly to the phase amplitudes of the n-dimensional quantum state:

$$|\psi_a\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{a_i} |i\rangle \tag{5}$$

Because the parameters defining a are protected within the computational timelock, the multi-copy transmission remains opaque to the adversary during channel transit.

Bob's decoding proceeds by utilising his private key to decrypt the time-locked parameters $\{Y, S_{\mathrm{base}}\}$. He passively measures the incoming states using a QFT receiver configured to the basis $\{|v_b\rangle\}_{b \in Y}$, yielding the noisy raw string b_{out}. Finally, Bob evaluates his local syndrome $S_{Bob} = H_{\mathrm{PC}} b_{out}$ and computes the error syndrome $S_e =$

$S_{Bob} \ominus S_{\text{base}}$ over $\mathbb{F}_n$ to execute Belief Propagation over the LDPC Tanner graph, perfectly reconciling the target string b^* (See Appendix B).

3.3 Formal Protocol Execution

The execution of the IR-KV-QCT protocol is formalised as follows:

Protocol 1: Information-Reconciled Khot-Vishnoi (IR-KV-QCT) Protocol

---

Public Parameters: Dimension n, predefined Hadamard subgroup $H \subset \{0,1\}^n$, channel error η, multi-copy count $m \leq t$. Bob possesses a public/private key pair (pk_B, sk_B).

Phase 1 **Parameter Generation and Encryption (Alice)**

1. Generate base string $u \xleftarrow{\$} \{0,1\}^n$ and noise string $z \xleftarrow{\$} \{0,1\}^n$ with a predefined physical bias η. This bias mathematically locks in the session's hypercontractive security parameter $\gamma = \Omega\left(\frac{\eta}{1-\eta}\right)$.
2. Define target shifted coset $Y = u \oplus z \oplus H$.
3. Select vector $a \xleftarrow{\$} u \oplus H$ and compute exact target string $b^* = a \oplus z$.
4. Compute a base Slepian-Wolf syndrome $S_{\text{base}} = H_{\text{PC}} b^*$ over $\mathbb{F}_n$, statically scaled to correct an expected baseline quantum bit error rate over the alphabet of Y.
5. Select a random seed for a two-universal hash function F_{PA}.
6. Define lockbox $\mathcal{C}_{\text{lock}} = \{Y, S_{\text{base}}, F_{\text{PA}}\}$ and encrypt using Bob's post-quantum public key to yield $Enc_{pk_B}(\mathcal{C}_{\text{lock}})$.
7. **Transmit** $Enc_{pk_B}(\mathcal{C}_{\text{lock}})$ to Bob via an authenticated classical channel.

Phase 2 **Quantum Transmission & Measurement (Alice & Bob)**

1. Alice prepares the phase-encoded state $|\psi_a\rangle$ in an n-dimensional Hilbert space:

$$|\psi_a\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{a_i} |i\rangle \tag{6}$$

2. Alice prepares m identical copies of this state, forming the composite system $\rho_{in} = (|\psi_a\rangle \langle\psi_a|)^{\otimes m}$.
3. Alice transmits ρ_{in} to Bob over the optical channel.
4. Bob immediately decrypts the classical timelock using sk_B to extract the basis Y.
5. As the photons arrive, Bob passively measures the states using a QFT receiver in the basis defined by Y, yielding the noisy outcome string b_{out}.

Phase 3 **Decoding and Key Recovery (Bob & Alice)**

1. Bob utilises the decrypted base syndrome S_{base} alongside his immediate measurement result b_{out} to execute Information Reconciliation (See Belief Propagation step in Appendix B).
2. If decoding fails due to transient channel noise exceeding the baseline, Alice and Bob interactively reconcile the remaining errors over a public channel via adaptive

shortened symbols S_{adapt}. If the cumulative leakage $|S_{\text{base}}| + |S_{\text{adapt}}|$ exceeds the protocol's abort threshold, the session is terminated.

3. Upon successful reconciliation of the target string b^*, Alice and Bob apply Privacy Amplification $K_{final} = F_{PA}(b^*)$ to extract the secure key.

---

4 Threat Model and Adversary Capabilities

To comprehensively evaluate the protocol's security under a collective attack, we must formalise the adversary's actions on the quantum channel. Upon interception, the adversary captures the m transmitted copies. Because the computational timelock ensures the base string u remains computationally hidden during the transmission window, Eve possesses zero classical mutual information regarding the target vector a before t_{comp}. Since u is chosen uniformly at random, the marginal distribution of a is perfectly uniform over the Boolean hypercube $\{0,1\}^n$.

Consequently, any CPTP map $\mathcal{E}$ she applies at $t = 0$ acts on the statistically averaged density matrix:

$$\rho_{\text{avg}}^{\otimes m} = \frac{1}{2^n} \sum_{a \in \{0,1\}^n} \left(|\psi_a\rangle \langle \psi_a| \right)^{\otimes m} \tag{7}$$

The most general collective attack consists of applying a CPTP map $\mathcal{E} : \mathcal{H}_{\text{channel}}^{\otimes m} \to \mathcal{H}_K \otimes \mathcal{H}_Q$, encoding the transmission into a classical register $\mathcal{H}_K$ (for immediate classical logging) and a quantum memory register $\mathcal{H}_Q$ (for delayed measurement) Mazzoncini et al. [2025], Furrer et al. [2018].

4.1 Coherent Attacks and Quantum Error Correction Constraints

To circumvent physical memory constraints, an adversary may attempt a coherent attack by projecting the intercepted ensemble into the symmetric subspace $\text{Sym}^m(\mathbb{C}^n)$ and applying a Quantum Error Correction (QEC) encoding. This strategy aims to suppress decoherence and artificially extend the memory lifetime beyond t_{comp}, enabling a perfect delayed measurement upon basis revelation.

Within the QCT model, we constrain the adversary's storage capabilities using established QEC space-time overhead limits. To fault-tolerantly preserve the $m \log_2 n$ encoded logical bits for a timelock duration $t_{\text{comp}} \sim 3600$ s, the adversary must scale a topological surface code to a distance d sufficient to suppress logical error rates. As derived in Appendix C for baseline parameters $n = 64$ and $m = 4$, evaluating against a physical gate error rate of 10^{-4}, a syndrome extraction cycle time $\tau_{\text{syn}} = 1$ μs, and a target security parameter $\delta = 10^{-9}$ mandates a minimum code distance $d \geq 17$. This requires $\approx 1.38 \times 10^4$ physical qubits operating continuously with microsecond-level synchronisation. This space-time overhead establishes a quantifiable physical boundary exceeding near-term hardware limits, ensuring that active error suppression fails. Consequently, unavoidable Markovian decoherence reduces the quantum storage register $\mathcal{H}_Q$ to the completely depolarising channel.

5 Security Proof and Strategy Reduction

The security of the proposed protocol is established by bounding the adversary's accessible information throughout the execution of the protocol. Rather than treating the quantum transmission and classical reconciliation phases independently, we employ a sequential reduction that tracks the temporal evolution of the adversary's state.

The security analysis proceeds along three conceptual pillars. First, the native uniform distribution of the Khot-Vishnoi phase encoding strictly confines the multi-copy state to the symmetric subspace, which absolutely bounds the classical information extractable from an immediate measurement. Second, under the noisy-storage model, memory decoherence guarantees that delayed quantum measurements reduce to this bounded classical capacity. Third, the hypercontractivity of the Khot-Vishnoi game ensures that this limited classical budget—even when combined with public error-correction data—is asymptotically insufficient to determine the secret key.

5.1 Main Security Theorem

The following theorem bounds the adversary's ultimate probability of guessing the target string by integrating quantum state indistinguishability, channel depolarisation, and classical hypercontractivity.

Theorem 1 *Let Eve possess a (t_{comp}, δ)-noisy quantum memory Φ acting on the collective storage register $\mathcal{H}_Q$, and let the physical channel exhibit an effective quantum bit error rate e. For any classical-quantum-quantum state generated by a joint CPTP map $\mathcal{E}$ acting on the averaged m-copy input state $\rho_{avg}^{\otimes m}$, the total probability of correctly guessing the target string b^* upon the public revelation of the basis Y and the complete Slepian-Wolf syndromes $\{S_{base}, S_{adapt}\}$ is bounded by:*

$$P_{guess}\left(b^* \mid K\Phi(Q), S_{base}, S_{adapt}, Y\right) \leq 2^{m\log_2(n)+f_{EC}H_n(e)-\gamma n} + \delta \tag{8}$$

where $H_n(e)$ is the exact n-dimensional Shannon entropy, f_{EC} is the error reconciliation inefficiency, $\gamma = \Omega\left(\frac{\eta}{1-\eta}\right)$ is the hypercontractive parameter derived from the physical channel, and δ is the diamond-norm memory penalty.

Proof The security reduction is evaluated chronologically across the adversary's operational phases: the initial classical-quantum extraction at $t = 0$, the memory depolarisation over $0 < t < t_{\text{comp}}$, the public syndrome leakage at decoding, and the final classical estimation game.

Step 1: Initial Extraction and the Holevo Capacity Bound ($t = 0$).

Upon intercepting the channel at $t = 0$, the adversary applies a CPTP map $\mathcal{E}$ to partition the intercepted ensemble into a classical registration register K and a quantum storage register Q. Because the base string u remains computationally hidden within the timelock, the marginal distribution of Alice's encoded vector a is perfectly uniform. Therefore, her effective input is strictly the uniform ensemble $\rho_{\text{avg}}^{\otimes m} = \frac{1}{2^n}\sum_a (|\psi_a\rangle\langle\psi_a|)^{\otimes m}$.

Because this ensemble consists exclusively of identical pure state copies, its support is geometrically confined to the symmetric subspace $\mathrm{Sym}^m(\mathbb{C}^n)$. Consequently, an immediate direct measurement is fundamentally constrained by the physical dimension of this supporting Hilbert space. The optimal adversarial strategy mandates the adversary to use $\mathcal{E}$ merely to extract and store the maximum possible classical correlations in register K, awaiting the delayed broadcast of the public basis Y.

By Holevo's theorem, the classical mutual information c_1 extracted into register K regarding the target string b^* is upper-bounded by the von Neumann entropy of the pre-measurement state. $c_1 = I(b^* : K \mid Y) \leq S(\rho_{\mathrm{avg}}^{\otimes m}) \leq \log_2 d_{\mathrm{sym}}$. For the operational regime where $m \ll n$, we upper-bound this dimension to simplify the classical complexity budget, yielding

$$c_1 \leq m \log_2 n \tag{9}$$

Step 2: Delayed Measurement and Memory Reduction ($t = t_{comp}$).

At the expiration of the computational timelock, the adversary attempts to guess the target string b^* utilizing all available resources: the static classical register K, the syndromes $\{S_{\mathrm{base}}, S_{\mathrm{adapt}}\}$, the basis Y, and the noisy output of the quantum memory $\Phi(Q)$.

The optimal extraction strategy is modelled as a joint Positive Operator-Valued Measure (POVM), denoted $\Pi = \{\Pi(b^*)\}$, acting globally on the composite Hilbert space $\mathcal{H}_K \otimes \mathcal{H}_Q$. The elements $\Pi(b^*)$ are positive semi-definite operators satisfying the completeness relation $\sum_{b^*} \Pi(b^*) = \mathbb{I}_K \otimes \mathbb{I}_Q$. The maximum guessing probability is:

$$\begin{aligned} &P_{\mathrm{guess}}\left(b^* \mid K\Phi(Q), S_{\mathrm{base}}, S_{\mathrm{adapt}}, Y\right) \\ &\quad = \max_{\Pi} \sum_{b^*} p(b^*) \operatorname{Tr}\left[\Pi(b^*)(\mathbb{I}_K \otimes \Phi)(\rho_{KQ}^{(b^*)})\right], \end{aligned} \tag{10}$$

where $\rho_{KQ}^{(b^*)}$ is the joint state conditioned on b^*, generated by the initial evaluation of $\mathcal{E}$. By the definition of the $(t_{\mathrm{comp}}, \delta)$-noisy quantum memory, the channel Φ is δ-close in diamond norm to the completely depolarizing channel $\mathcal{F}$ acting on $\mathcal{H}_Q$. Adding and subtracting the action of $\mathcal{F}$ yields:

$$\begin{aligned} &P_{\mathrm{guess}}\left(b^* \mid K\Phi(Q), S_{\mathrm{base}}, S_{\mathrm{adapt}}, Y\right) \\ &\quad = \max_{\Pi} \sum_{b^*} p(b^*) \operatorname{Tr}\Big[\Pi(b^*)\Big((\mathbb{I}_K \otimes \Phi)(\rho_{KQ}^{(b^*)}) \\ &\qquad - (\mathbb{I}_K \otimes \mathcal{F})(\rho_{KQ}^{(b^*)}) + (\mathbb{I}_K \otimes \mathcal{F})(\rho_{KQ}^{(b^*)})\Big)\Big]. \end{aligned} \tag{11}$$

Applying Hölder's inequality ($\operatorname{Tr}[XY] \leq \|X\|_\infty \|Y\|_1$) and substituting the spectral norm bound ($\|\Pi(b^*)\|_\infty \leq 1$), we obtain:

$$\begin{aligned} &P_{\mathrm{guess}}\left(b^* \mid K\Phi(Q), S_{\mathrm{base}}, S_{\mathrm{adapt}}, Y\right) \\ &\quad \leq \max_{\Pi} \sum_{b^*} p(b^*)\Big(\Big\|(\mathbb{I}_K \otimes \Phi - \mathbb{I}_K \otimes \mathcal{F})(\rho_{KQ}^{(b^*)})\Big\|_1 \\ &\qquad + \operatorname{Tr}\left[\Pi(b^*)(\mathbb{I}_K \otimes \mathcal{F})(\rho_{KQ}^{(b^*)})\right]\Big). \end{aligned} \tag{12}$$

Because $\|\Phi - \mathcal{F}\|_\diamond \leq \delta$, the trace distance term is strictly bounded by δ. The depolarizing channel $\mathcal{F}$ destroys all remaining quantum correlation between Q and b^*, factorizing the state such that $(\mathbb{I}_K \otimes \mathcal{F})(\rho_{KQ}^{(b^*)}) = \rho_K^{(b^*)} \otimes \frac{\mathbb{I}_Q}{d_Q}$. The trace operation thus collapses to a reduced POVM Π_K acting exclusively on the classical register $\mathcal{H}_K$:

$$P_{\mathrm{guess}}\left(b^* \mid K\Phi(Q), S_{\mathrm{base}}, S_{\mathrm{adapt}}, Y\right)$$

$$\leq P_{\text{guess}}(b^* \mid K, S_{\text{base}}, S_{\text{adapt}}, Y) + \delta. \tag{13}$$

This isolates the adversary's advantage entirely to the classical capacity c_1 extracted in Step 1.

Step 3: Cumulative Error Correction Leakage.

At $t = t_{\text{comp}}$, the protocol publicly broadcasts the remaining Slepian-Wolf error-correction data. By Shannon's source coding theorem, the cumulative classical leakage c_2 required to reconcile the target string is the sum of the bit-lengths of the base and adaptive syndromes, strictly tracked and bounded by:

$$c_2 = |S_{\text{base}}| + |S_{\text{adapt}}| = f_{\text{EC}} H_n(e) \text{ bits} \tag{14}$$

where $H_n(e)$ is the exact n-dimensional Shannon entropy and $f_{\text{EC}}^{\text{eff}}$ is the effective reconciliation inefficiency of the completed interactive session.

Step 4: Hypercontractive Bound of the Classical Endgame.

Stripped of all quantum correlation by the memory reduction, the adversary's final strategy to infer b^* using K, $\{S_{\text{base}}, S_{\text{adapt}}\}$, and Y reduces strictly to a classical communication complexity game. Her total classical communication budget is the sum of the initial extraction and the syndrome leakage:

$$c = c_1 + c_2 \leq m \log_2 n + |S_{\text{base}}| + |S_{\text{adapt}}| \text{ bits} \tag{15}$$

Applying the Bonami-Beckner hypercontractivity theorem for the Khot-Vishnoi game over the Boolean hypercube, the maximal success probability under a classical budget c is:

$$\begin{aligned} P_{\text{guess}}\left(b^* \mid K, S_{\text{base}}, S_{\text{adapt}}, Y\right) &\leq 2^{c-\gamma n} \\ &\leq 2^{m \log_2(n) + f_{\text{EC}} H_n(e) - \gamma n} \end{aligned} \tag{16}$$

Substituting this classical upper bound into the memory reduction inequality (13) yields the unified security bound. This completes the proof. □

5.2 Multi-Copy Operational Limit

To ensure ultimate security against a collective attack, the transmitted number of copies m must satisfy the constraints imposed by the protocol's physical and information-theoretic limits Vyas and Alleaume [2020].

Crucially, the security of the protocol does not require absolute geometric state indistinguishability at $t = 0$. Even if Alice transmits a large block of m copies, the adversary's extractable classical information remains rigidly limited by the physical dimension of the supporting Hilbert space.

The uniform distribution of the Khot-Vishnoi encoding restricts the ensemble to the symmetric subspace, ensuring the adversary's accessible information is strictly constrained by Holevo's theorem. Because the computational timelock ensures the semantic security of the base string u during the transmission window, the adversary is physically forced to average over all possible coset vectors. This ensemble averaging generates the highly mixed state $\rho_{\text{avg}}^{\otimes m}$ and algebraically confines its support strictly to the symmetric subspace $\text{Sym}^m(\mathbb{C}^n)$.

Because the state is confined to this subspace, the classical mutual information accessible to Eve via any joint POVM is governed by the von Neumann entropy of

the ensemble, strictly bounded by the subspace dimension: $c_1 \leq \log_2 d_{\text{sym}} \leq m \log_2 n$. Without this geometric confinement, the adversary could extract extensive raw key information and break the protocol.

To ensure the adversary's guessing probability vanishes during the classical endgame, the cumulative classical budget $c = c_1 + c_2$ must remain strictly below the hypercontractive threshold γn. Substituting the Holevo bound for c_1 and the public information reconciliation leakage $c_2 = f_{\text{EC}} H_n(e)$ yields:

$$m \log_2 n + f_{\text{EC}} H_n(e) < \gamma n \implies m < \frac{\gamma n - f_{\text{EC}} H_n(e)}{\log_2 n} \tag{17}$$

Therefore, the definitive operational limit of the protocol is the Holevo-bounded classical limit. In the finite-key regime (See Section 7.3), maintaining m below this threshold guarantees that the exponent $\gamma n - m \log_2 n - f_{\text{EC}} H_n(e_{\text{true}})$ remains negative, preventing the exponential divergence of the trace-distance smoothing penalty Δ_δ (Equation 28). Under this constraint, Alice can safely scale her transmission up to $m_{\max} \sim \mathcal{O}(n/\log_2 n)$. Even if the m-copy ensemble is distinguishable from the completely mixed state, its restriction to the symmetric subspace $\text{Sym}^m(\mathbb{C}^n)$ limits the adversary's accessible classical information. The uniform distribution of the input states confines the ensemble to this subspace, while the hypercontractivity of the Khot-Vishnoi game bounds the extracted classical mutual information. Together, these constraints preserve the exponential separation between the legitimate and adversarial capacities.

6 Protocol Correctness

To establish the complete security profile of the protocol, the soundness guarantees (security against the adversary) must be complemented by a proof of correctness. We demonstrate that an authorised receiver, equipped with the decrypted seed, achieves a deterministic advantage in both photon detection yield and raw measurement fidelity.

6.1 Photon Detection Yield and Channel Splitting

We model the point-to-point physical link as a lossy channel with system transmissivity $\eta_{\text{sys}} = \eta_{\text{ch}} \eta_{\text{det}}$, where $\eta_{\text{ch}} = 10^{-\alpha L_{\text{fib}}/10}$ represents the distance-dependent channel transmissivity, with $\alpha = 0.2$ dB/km denoting the standard attenuation coefficient of standard optical fiber and L_{fib} the fiber length and η_{det} is the receiver's detector efficiency.

To resolve the n-dimensional target state, Bob's measurement apparatus requires an array of n independent detection channels. Let p_d denote the intrinsic dark count probability per detector per gate window. Because Alice transmits m identical copies of the phase-encoded state $|\Psi_{a,f}\rangle^{\otimes m}$, the total probability that at least one authentic signal photon survives channel attenuation is $P_{\text{signal}} = 1 - (1 - \eta_{\text{sys}})^m$.

A physical advantage of this multi-copy protocol is its redundant signal encoding: because all m identical copies encode the same target vector, each surviving signal

photon independently triggers the identical target detector channel b^*, locally amplifying the Signal-to-Noise Ratio (SNR) against the background noise floor. Assuming the optical link is modelled as a symmetric depolarising channel, the uniform baseline optical misalignment error e_{opt} distributes the erroneous signal probabilities evenly across the detector array as, $P_C = (1 - e_{opt})P_{signal}$ $P_I = \frac{e_{opt}}{n-1} P_{signal}$ where P_C is the signal probability directed to the correct channel, and P_I is the erroneous signal probability directed to each of the $n - 1$ incorrect channels. This symmetric depolarising model accurately reflects high-dimensional spatial-mode encoding through multimode fiber, where homogeneous modal crosstalk and scrambling randomly scatter lost phase information uniformly across all orthogonal spatial modes during channel transit.

Compounding these allocations with the independent per-detector dark count noise, the total click probabilities for the correct ($p_{\text{click},C}$) and incorrect ($p_{\text{click},I}$) channels evaluate to:

$$p_{\text{click},C} = 1 - (1 - P_C)(1 - p_d) \tag{18}$$

$$p_{\text{click},I} = 1 - (1 - P_I)(1 - p_d) \tag{19}$$

A valid logical round is registered if at least one detector fires. The aggregate logical success probability is therefore:

$$P_{\text{succ}}^{\text{det}} = 1 - (1 - p_{\text{click},C})(1 - p_{\text{click},I})^{n-1} \tag{20}$$

6.2 Quantum Measurement Fidelity and Exact QBER

To evaluate the operational fidelity of the system in the presence of multi-click events (where dark counts and authentic signals trigger simultaneously), we define Bob's decoding rule: if multiple detectors fire during a single gate window, the receiver selects one clicking channel uniformly at random.

The total Quantum Bit Error Rate (QBER), denoted e, is defined as the probability that the decoded channel choice deviates from the target string b^*. By evaluating the conditional probabilities of correct vs. incorrect channel clicks, the exact effective QBER is formulated as:

$$\begin{aligned} e &= \frac{p_{\text{click},I}(n-1)}{nP_{\text{succ}}^{\text{det}}} \left[1 - \frac{1 - p_{\text{click},C}}{n}\right] \\ &\approx \frac{P_{\text{signal}} e_{\text{opt}} + P_{\text{dark_total}} \left(\frac{n-1}{n}\right)}{P_{\text{succ}}^{\text{det}}} \end{aligned} \tag{21}$$

where $P_{\text{dark_total}} = 1 - (1 - p_d)^n$.

Modelling the bits of the overall noise string z as independently distributed Bernoulli variables with the predefined algorithmic bias η, the baseline expectation is $\mathbb{E}[(-1)^{z_i}] = 1 - 2\eta$. Consequently, Bob's raw quantum success probability before physical channel degradation evaluates to $P_{\text{succ}}^{\text{quant}} \approx (1 - 2\eta)^2$. The total error reconciled via Slepian-Wolf must account for the convolution of this algorithmic noise with the physical QBER e. The expected success probability of Bob's raw quantum

measurement evaluates to:

$$\begin{aligned} P_{\text{succ}}^{\text{quant}} &= \mathbb{E}_z \left[|\langle v_{b^*} \mid \psi_a \rangle|^2 \right] \\ &= \frac{1}{n^2} \left(n + n(n-1)(1-2e)^2 \right) \\ &= (1-2e)^2 + \frac{1-(1-2e)^2}{n} \end{aligned} \tag{22}$$

Asymptotically ($n \to \infty$), the secondary term vanishes, leaving $P_{\text{succ}}^{\text{quant}} \approx (1-2e)^2$. This completes the exact formulation of the high-dimensional channel noise, grounding the Slepian-Wolf classical leakage analysis in the true physical constraints of the detector hardware.

7 Secret Key Rate Derivation

To translate the physical dynamics and information-theoretic security bounds into quantitative metrics, we first formulate the analytical secret key rates under asymptotic limits, followed by a composable finite-key adaptation.

7.1 Reduction to the Wiretap Channel

Under specific temporal and entropic constraints, the quantum transmission phase reduces identically to a classical broadcast wiretap channel configuration.

In standard quantum key distribution, an unconstrained adversary can retain intercept states in quantum memory to execute deferred joint measurements after public basis revelation. Conversely, under this framework, the descrambling unitaries remain protected by a short-term computationally secure lock. Because any unauthorised quantum storage undergoes complete Markovian decoherence well before this time-lock expires ($t_{\text{coh}} \ll t_{\text{comp}}$), deferred quantum attacks are physically precluded. The adversary is mathematically forced to perform an immediate measurement at $t = 0$, collapsing her entire quantum acquisition into a strictly classical random variable $Z \in \mathcal{Z}$.

Simultaneously, the authorised recipient Bob uses immediate access to the decrypted basis Y to execute a local projective measurement without delay, recording his outcomes as a classical variable $Y \in \mathcal{Y}$. Because the source variable X, the authorised outcomes Y, and the adversarial interception record Z all resolve into discrete classical registers at the time boundary $t = 0$, the quantum link maps cleanly onto a classical Shannon-Wyner wiretap channel. This mapping reduces the quantum link to a classical wiretap channel, permitting the use of standard classical post-processing while maintaining information-theoretic security.

7.2 Asymptotic Secret Key Rate Analysis

Because the protocol reduces to a classical wiretap channel at $t = 0$, we evaluate the secure key capacity using the Csiszár-Körner theorem. The asymptotic secret key rate

R_{sec} per logical round scales with the aggregate detection probability $P_{\text{succ}}^{\text{det}}$:

$$R_{\text{sec}} = P_{\text{succ}}^{\text{det}} \left[I(X;Y) - I(X;Z) \right] \tag{23}$$

The legitimate link between Alice and Bob operates as an n-ary symmetric channel. Since each symbol encodes $\log_2 n$ bits, the classical mutual information between the authorised parties is bounded by the channel noise as $I(X;Y) = \log_2 n - H_n(e)$. Here, $H_n(e) = -(1-e)\log_2(1-e) - e\log_2\left(\frac{e}{n-1}\right)$ is the exact n-dimensional Shannon entropy at the effective QBER e. During information reconciliation, the public channel leaks $\text{Leak}_{\text{EC}} = f_{\text{EC}} H_n(e)$, where f_{EC} is the error correction inefficiency factor. This limits Bob's operational mutual information to $I(X;Y)_{\text{ops}} = \log_2 n - f_{\text{EC}} H_n(e)$.

Eve's operational information regarding Alice's raw key at $t = 0$ is strictly bounded by her min-entropy. To establish a conservative lower bound on the asymptotic rate, we substitute the Shannon entropy with the strictly smaller smooth min-entropy ($H(X|Z) \geq H_{\min}(X|Z)$ implies):

$$I(X;Z) \leq \log_2 n - H_{\min}(X|Z) \tag{24}$$

where $H_{\min}(X|Z) = -\log_2 P_{\text{guess}}(X|Z)$. The delayed Khot-Vishnoi game enforces a strict hypercontractive bound on Eve's guessing probability, establishing a min-entropy floor of $H_{\min}(X|Z) = \gamma n - m\log_2 n$. Thus, the maximum information available to the eavesdropper is bounded by:

$$I(X;Z)_{\max} = \log_2 n - (\gamma n - m\log_2 n) \tag{25}$$

Substituting these operational limits directly into the Csiszár-Körner equation gives the final asymptotic secret key rate:

$$\begin{aligned} R_{\text{sec}} &\geq P_{\text{succ}}^{\text{det}} \left[I(X;Y)_{\text{ops}} - I(X;Z)_{\max} \right] \\ &= P_{\text{succ}}^{\text{det}} \left[\left(\log_2 n - f_{\text{EC}} H_n(e) \right) - \left(\log_2 n - H_{\min}(X|Z) \right) \right] \\ &= P_{\text{succ}}^{\text{det}} \left[H_{\min}(X|Z) - f_{\text{EC}} H_n(e) \right] \\ &= P_{\text{succ}}^{\text{det}} \left[\gamma n - m\log_2 n - f_{\text{EC}} H_n(e) \right] \end{aligned} \tag{26}$$

This final expression clearly illustrates the protocol's fundamental tradeoff: the information cost of transmitting m copies ($m\log_2 n$) directly subtracts from the raw hypercontractive capacity (γn). This provides a precise classical key rate calculation derived directly from the physical constraints of the quantum channel.

7.3 Finite-Key Analysis and Composable Security

In a realistic implementation, the raw block size N_{total} is finite. To establish a rigorous composable ϵ-security framework, Alice and Bob must account for statistical fluctuations during parameter estimation. Out of the $n_u \approx P_{\text{succ}}^{\text{det}} N_{\text{total}}$ sifted symbols, a random subset of k_s symbols is sacrificed for parameter estimation, leaving $n_u - k_s$ active symbols for key distillation.

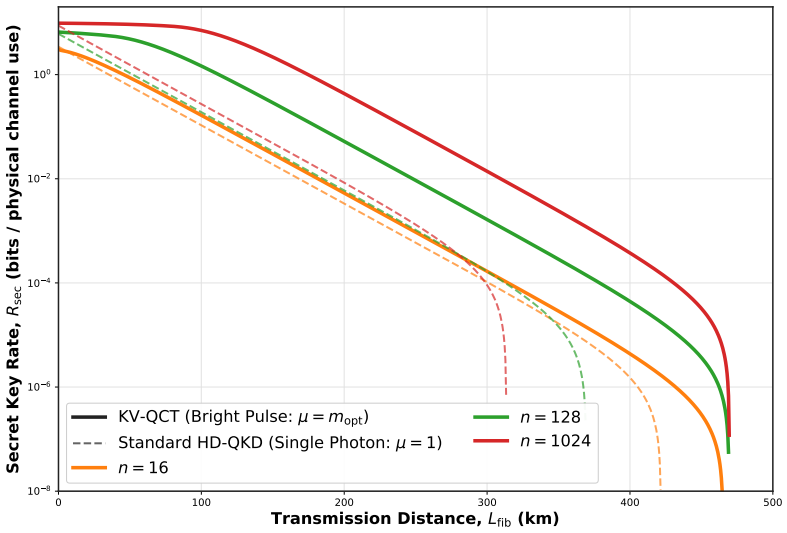


Figure 1 Asymptotic secret key rate R_{sec} as a function of transmission distance L_{fib} for the KV-QCT protocol (solid lines) and standard HD-QKD (dashed lines) across dimensions $n \in \{16, 128, 1024\}$. Simulation parameters are configured to: fiber attenuation $\alpha = 0.15$ dB/km, detector efficiency $\eta_{\text{det}} = 0.9$, dark count probability $p_d = 10^{-8}$ per detector, baseline optical error $e_{\text{opt}} = 0.01$, error correction inefficiency $f_{\text{EC}} = 1.15$, and hypercontractive capacity parameter $\gamma = 0.55$.

Because the $t = 0$ classical reduction guarantees that the measurement outcomes map to independent classical registers, we can safely apply standard Chernoff-Hoeffding bounds to estimate the true worst-case error e_{true} from the sampled subset, and evaluating the smooth min-entropy via the Leftover Hash Lemma, the final extractable secure key length ℓ (in bits) is bounded by:

$$\ell = \lfloor (n_u - k_s) \left[\gamma n - m \log_2 n - f_{\text{EC}} H_n(e_{\text{true}}) - \Delta_\delta \right] - \Delta_{\text{PA}} \rfloor \tag{27}$$

Extracting secure keys against quantum side-information utilising a δ-noisy memory requires applying the Generalised Leftover Hash Lemma. Following the trace-distance smoothing framework established in Tomamichel et al. [2012], Renner [2006], the operational min-entropy evaluated against the ideal completely depolarising channel $\mathcal{F}$ is perturbed by the adversary's actual δ-close memory Φ. This introduces a trace-distance penalty Δ_δ that bounds the smoothing parameter ϵ_s, evaluating strictly to:

$$\Delta_\delta = \log_2 \left(1 + 2\delta \cdot 2^{\gamma n - m \log_2(n) - f_{\text{EC}} H_n(e_{\text{true}})} \right) \tag{28}$$

8 Performance Evaluation and Hardware Feasibility

To evaluate the operational advantage of the IR-KV-QCT architecture, we analyse the secret key rate against standard single-photon high-dimensional QKD over varying transmission distances.

8.1 Operational Scaling and Simulation Results

As illustrated in Fig. 1, standard HD-QKD operating under the strict single-photon constraint ($\mu = 1$) exhibits an exponential decay in secret key capacity as a function of fiber attenuation. Conversely, because our security proof establishes the Holevo-bounded capacity as the true operational limit ($m_{\max} \sim \mathcal{O}(n/\log_2 n)$), Alice can dynamically scale the transmission block size. By optimising the multi-copy parameter to m_{opt}, the protocol overcomes initial channel loss, generating a high-capacity plateau that extends significantly farther than standard bounds before succumbing to detector dark counts.

To maintain physical feasibility, the system dimension n must align with near-term high-dimensional encoding platforms. Consider a practical benchmark utilising $n = 1024$ orthogonal modes. The classical hypercontractive limit restricts the multi-copy parameter to $m \ll 1024/10 \approx 102$. By safely setting Alice's transmission block to $m = 25$ copies, the protocol can operate securely over a 50 km fiber link ($\eta_{\text{sys}} \approx 10^{-1}$). At this distance, the logical detection probability evaluates to $P_{\text{succ}}^{\text{det}} \approx 1-(1-0.1)^{25} \approx 0.93$. While standard single-photon QKD is restricted to a mere 10% physical detection yield at 50 km, this multi-copy encoding boosts the logical block success rate to 93%, guaranteeing a nearly deterministic and highly stable raw key generation rate.

8.2 Quantifying the Slepian-Wolf Leakage Margin

To ensure that the classical information leaked during error correction does not violate the hypercontractive bound, the protocol enforces the strict inequality $c_1 + c_2 < \gamma n$. For an $n = 1024$ system operating at a baseline QBER of $e = 0.10$, the Holevo-bounded initial extraction yields $c_1 = m \log_2 n = 250$ bits. The n-dimensional Shannon entropy of the channel noise evaluates to $H_{1024}(0.10) \approx 1.47$ bits per symbol. Assuming the rate-adaptive LDPC protocol maintains an effective reconciliation inefficiency of $f_{\text{EC}} = 1.15$, the cumulative public leakage is tightly bounded to $c_2 \approx 1.69$ bits.

Because the total classical budget $c \approx 251.69$ bits is dominated by the initial state extraction c_1, the Slepian-Wolf leakage c_2 introduces only a minor correction under nominal operating conditions. However, the inequality $m \log_2 n + c_2 < \gamma n$ serves as the strict abort threshold for the rate-adaptation algorithm. If channel noise causes the interactive LDPC engine to request a volume of supplemental parity symbols that breaches this hypercontractive ceiling, the protocol deterministically aborts the block to preserve everlasting security.

8.3 Detector Noise Tolerance

To demonstrate the physical viability of this high-dimensional configuration, we must verify that multiplexing n independent detection modes does not introduce a fatal aggregate dark count penalty.

Let the effective QBER threshold for positive key generation be denoted as $e_{\max}$. By isolating the per-detector dark count probability p_d from the effective QBER approximation (Eq. 21), we establish the strict hardware requirement for the detector array. Notably, in an n-dimensional system, a dark count maps to an erroneous bin

with probability $\frac{n-1}{n}$:

$$p_d \leq \frac{P_{\text{signal}}(e_{\max} - e_{\text{opt}})}{n\left(\frac{n-1}{n} - e_{\max}\right)} \tag{29}$$

Revisiting the 50 km benchmark ($n = 1024$, $m = 25$, $P_{\text{signal}} \approx 0.93$), we assume a baseline optical misalignment error of $e_{\text{opt}} = 1\%$ and a rigorous QBER abort threshold of $e_{\max} = 15\%$. Substituting these parameters into Eq. 29 dictates that the system can tolerate a per-detector dark count probability up to $p_d \leq 1.49 \times 10^{-4}$ per logical gate.

This theoretical tolerance is highly permissive. State-of-the-art commercial Superconducting Nanowire Single-Photon Detectors (SNSPDs) Grünenfelder et al. [2023], Stasi et al. [2023] utilising multi-pixel or interleaved nanowire architectures typically exhibit baseline dark count rates in the range of 10 to 100 counts per second. For a standard 1 ns coincidence window, this corresponds to a per-gate dark count probability of $p_d \sim 10^{-7}$. Consequently, even when aggregating the noise of 1024 parallel detectors, the total baseline array noise ($np_d \sim 10^{-4}$) remains safely below the maximum theoretical failure threshold. This demonstrates that the n-detector multiplexing requirement is highly compatible with near-term quantum optical hardware and does not compromise the protocol's high-dimensional performance advantages over extended distances.

9 Physical Feasibility and Technological Limitations

While the theoretical derivations of the IR-KV-QCT framework establish a novel cryptographic construction that successfully bridges computational complexity with physical-layer quantum security, transitioning this protocol into a scalable optical architecture exposes distinct technological challenges.

9.1 Receiver Complexity and High-Dimensional Interferometry

To fully exploit the $\Omega(n)$ classical hardness gap, the authorised receiver must configure an n-dimensional quantum Fourier transform (QFT) Carolan et al. [2015]. Programmable Mach-Zehnder interferometer (MZI) meshes represent the current state-of-the-art for universal linear optics Carolan et al. [2015], but their $\mathcal{O}(n^2)$ component scaling imposes fundamental insertion-loss limits for massive alphabets ($n \geq 1024$). Alternative approaches, such as orbital angular momentum (OAM) Halevi et al. [2024] or time-bin multiplexing Vagniluca et al. [2020], Mueller et al. [2024a], Wang et al. [2026], bypass spatial scaling limits at the expense of modal crosstalk and temporal latency. As quantitatively detailed in Appendix E, time-bin architectures successfully mitigate spatial array requirements but introduce a super-linear dark count penalty.

Consequently, near-term implementations are best suited for intermediate dimensions (e.g., $n = 64$ or 128), where MZI integrated circuits Carolan et al. [2015] and time-bin multiplexing are physically mature. While the asymptotic hypercontractive advantage scales with larger n, operating at a realistic baseline of $n = 64$ still preserves a sufficient complexity gap. For example, at $n = 64$ with a noise parameter $\gamma = 0.55$, the operational threshold allows a multi-copy scaling of $m = 4$. This multi-copy pool

provides a 6 dB link-budget advantage to offset channel attenuation, allowing the protocol to deliver positive secret key rates over distances where standard single-photon high-dimensional QKD suffers total rate collapse due to insertion loss. This regime balances an exploitable complexity gap ($m \sim \mathcal{O}(n/\log_2 n)$) with the constraints of mature optical hardware.

9.2 Reconciliation Overhead and Computational Latency

The Slepian-Wolf syndrome reconciliation relies on non-binary LDPC codes defined over large Galois fields $\mathbb{F}_n$. While theoretical reconciliation efficiencies of $f_{EC} \approx 1.15$ are achievable Mueller et al. [2024b], executing decoding algorithms over such large fields introduces a significant classical computational limit. The log-domain FFT-SPA decoding complexity scales as $\mathcal{O}(n \log n)$ operations per parity-check node per iteration Savin [2008]. Recent FPGA-based hardware implementations of non-binary LDPC decoders have demonstrated throughputs reaching 800 Mbps Subramaniyan et al. [2020]. While Bob performs information reconciliation using his local measurement outcomes, the high-dimensional decoding latency remains a bottleneck for real-time key distillation. Crucially, the QCT model ensures that the security of the distilled key is maintained because the underlying computational timelock prevents Eve from mounting an effective coherent attack during the post-processing phase. Therefore, even if computational throughput limits the distillation rate, it does not compromise the everlasting information-theoretic security of the key. This shifts the protocol's limitation away from fundamental physical channel loss and onto classical computational capacity, which scales alongside standard advancements in parallelised hardware.

10 Conclusion

This work presents the Information Reconciled Khot-Vishnoi (IR-KV-QCT) protocol under the Quantum Computational Timelock (QCT) security model. By mapping a classical communication complexity game onto a high-dimensional prepare-and-measure setup, we establish a secure framework for long-distance quantum key distribution.

To resolve the probabilistic errors inherent to quantum measurements, we integrated Slepian-Wolf syndrome reconciliation. Our analysis proves the classical information leaked during public error correction remains bounded strictly below the $\Omega(n)$ hypercontractive limit, restricting the eavesdropper. This complexity gap securely supports the transmission of multiple state copies, with the optimal multi-copy parameter scaling up to $\mathcal{O}(n/\log_2 n)$.

By utilising a hybrid security model, combining physical quantum mechanics with short-term computational encryption, the IR-KV-QCT protocol avoids the severe distance limitations of standard QKD. Furthermore, because the authorised receiver immediately decrypts the required measurement basis, the architecture eliminates the need for trusted quantum memory. The resulting asymptotic and finite-key rates demonstrate that this protocol delivers robust secret key capacities against

extreme channel loss. It ensures everlasting security against collective attacks, providing a scalable architectural framework to surpass point-to-point rate-loss bounds in extended-range quantum communication.

Acknowledgements. The author thanks Romain Alléaume for suggesting the initial connection between the Khot-Vishnoi communication complexity game and high-dimensional quantum key distribution.

References

William Beckner. Inequalities in fourier analysis. *Annals of Mathematics*, 102:159–182, 1975.

Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. ISSN 0304-3975. doi: https://doi.org/10.1016/j.tcs.2014.05.025. URL https://www.sciencedirect.com/science/article/pii/S0304397514004241. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

Aline Bonami. étude des coefficients de fourier des fonctions de $l^p(g)$. *Annales de l'Institut Fourier*, 20(2):335–402, 1970. doi: 10.5802/aif.357. URL https://numdam.org.

Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333, Aug 2000. doi: 10.1103/PhysRevLett.85.1330. URL https://link.aps.org/doi/10.1103/PhysRevLett.85.1330.

Harry Buhrman, Oded Regev, Giannicola Scarpa, and Ronald de Wolf. Near-optimal and explicit bell inequality violations. In *2011 IEEE 26th Annual Conference on Computational Complexity*, pages 157–166, 2011. doi: 10.1109/CCC.2011.30.

Jacques Carolan, Christopher Harrold, Chris Sparrow, Enrique Martín-López, Nicholas J. Russell, Joshua W. Silverstone, Peter J. Shadbolt, Nobuyuki Matsuda, Manabu Oguma, Mikitaka Itoh, Graham D. Marshall, Mark G. Thompson, Jonathan C. F. Matthews, Toshikazu Hashimoto, Jeremy L. O'Brien, and Anthony Laing. Universal linear optics. *Science*, 349(6249):711–716, 2015. doi: 10.1126/science.aab3642. URL https://www.science.org/doi/abs/10.1126/science.aab3642.

Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. *npj Quantum Information*, 2(1), November 2016. ISSN 2056-6387. doi: 10.1038/npjqi.2016.25. URL http://dx.doi.org/10.1038/npjqi.2016.25.

Fabian Furrer, Tobias Gehring, Christian Schaffner, Christoph Pacher, Roman Schnabel, and Stephanie Wehner. Continuous-variable protocol for oblivious transfer in the noisy-storage model. *Nature Communications*, 9(1):1450, April 2018.

Dmytro Gavinsky, Julia Kempe, and Ronald de Wolf. Exponential separation of quantum and classical one-way communication complexity for a boolean function, 2006. URL https://arxiv.org/abs/quant-ph/0607174.

Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*

(STOC), pages 25–32. ACM, 1989. doi: 10.1145/73007.73010. URL https://dl.acm.org/doi/10.1145/73007.73010.

GoogleQuantumAI and Collaborators. Quantum error correction below the surface code threshold. *Nature*, 638(8052):920–926, Feb 2025. ISSN 1476-4687. doi: 10.1038/s41586-024-08449-y. URL https://doi.org/10.1038/s41586-024-08449-y.

Fadri Grünenfelder, Alberto Boaron, Giovanni V Resta, Matthieu Perrenoud, Davide Rusca, Claudio Barreiro, Raphaël Houlmann, Rebecka Sax, Lorenzo Stasi, Sylvain El-Khoury, Esther Hänggi, Nico Bosshard, Félix Bussières, and Hugo Zbinden. Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. *Nature Photonics*, 17(5):422–426, May 2023.

Dotan Halevi, Boaz Lubotzky, Kfir Sulimany, Eric G. Bowes, Jennifer A. Hollingsworth, Yaron Bromberg, and Ronen Rapaport. High-dimensional quantum key distribution using orbital angular momentum of single photons from a colloidal quantum dot at room temperature. *Optica Quantum*, 2(5):351–357, Oct 2024. doi: 10.1364/OPTICAQ.528214. URL https://opg.optica.org/opticaq/abstract.cfm?URI=opticaq-2-5-351.

Subhash A. Khot and Nisheeth K. Vishnoi. The unique games conjecture, integrality gap for cut problems and embeddability of negative type metrics into ℓ_1, 2013. URL https://arxiv.org/abs/1305.4581.

Athanasios D. Liveris, Zixiang Xiong, and Costas N. Georghiades. Compression of binary sources with side information at the decoder using LDPC codes. *IEEE Communications Letters*, 6(10):440–442, 2002.

Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005. doi: 10.1103/PhysRevLett.94.230504. URL https://link.aps.org/doi/10.1103/PhysRevLett.94.230504.

M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, May 2018. ISSN 1476-4687. doi: 10.1038/s41586-018-0066-6. URL http://dx.doi.org/10.1038/s41586-018-0066-6.

Cosmo Lupo. Quantum data locking for secure communication against an eavesdropper with time-limited storage. *Entropy*, 17(5):3194–3204, 2015. ISSN 1099-4300. doi: 10.3390/e17053194. URL https://www.mdpi.com/1099-4300/17/5/3194.

Cosmo Lupo and Seth Lloyd. Quantum-locked key distribution at nearly the classical capacity rate. *Physical Review Letters*, 113(16), October 2014. ISSN 1079-7114. doi: 10.1103/physrevlett.113.160502. URL http://dx.doi.org/10.1103/PhysRevLett.113.160502.

Cosmo Lupo and Seth Lloyd. Continuous-variable quantum enigma machines for long-distance key distribution. *Physical Review A*, 92(6), December 2015. ISSN 1094-1622. doi: 10.1103/physreva.92.062312. URL http://dx.doi.org/10.1103/PhysRevA.92.062312.

Francesco Mazzoncini, Balthazar Bauer, Peter Brown, and Romain Alléaume. Hybrid Quantum Cryptography from Communication Complexity. *Quantum*, 9:1862, September 2025. ISSN 2521-327X. doi: 10.22331/q-2025-09-24-1862. URL https://doi.org/10.22331/q-2025-09-24-1862.

Andrew Mueller, Samantha I. Davis, Boris Korzh, Raju Valivarthi, Andrew D. Beyer, Rahaf Youssef, Neil Sinclair, Cristián Pe na, Matthew D. Shaw, and Maria Spiropulu. High-rate multiplexed entanglement source based on time-bin qubits for advanced quantum networks. *Optica Quantum*, 2(2):64–71, Apr 2024a. doi: 10.1364/OPTICAQ.509335. URL https://opg.optica.org/opticaq/abstract.cfm?URI=opticaq-2-2-64.

Ronny Mueller, Domenico Ribezzo, Mujtaba Zahidy, Leif Katsuo Oxenløwe, Davide Bacco, and Søren Forchhammer. Efficient information reconciliation for high-dimensional quantum key distribution. *Quantum Information Processing*, 23 (5):195, May 2024b. ISSN 1573-1332. doi: 10.1007/s11128-024-04395-w. URL https://doi.org/10.1007/s11128-024-04395-w.

Ronny Mueller, Domenico Ribezzo, Mujtaba Zahidy, Leif Katsuo Oxenløwe, Davide Bacco, and Søren Forchhammer. Efficient information reconciliation for high-dimensional quantum key distribution. *Quantum Information Processing*, 23(5), May 2024c. ISSN 1573-1332. doi: 10.1007/s11128-024-04395-w. URL http://dx.doi.org/10.1007/s11128-024-04395-w.

Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1), April 2017. ISSN 2041-1723. doi: 10.1038/ncomms15043. URL http://dx.doi.org/10.1038/ncomms15043.

Renato Renner. Security of quantum key distribution, 2006. URL https://arxiv.org/abs/quant-ph/0512258.

V. Savin. Min-max decoding for non-binary ldpc codes. *IEEE International Symposium on Information Theory*, pages 960–964, 2008.

David Slepian and Jack Keil Wolf. Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, 19(4):471–480, 1973.

Lorenzo Stasi, Gaëtan Gras, Riad Berrazouane, Matthieu Perrenoud, Hugo Zbinden, and Félix Bussières. Fast high-efficiency photon-number-resolving parallel superconducting nanowire single-photon detector. *Phys. Rev. Appl.*, 19:064041, Jun 2023. doi: 10.1103/PhysRevApplied.19.064041. URL https://link.aps.org/doi/10.1103/PhysRevApplied.19.064041.

Srinivasan Subramaniyan, Oscar Ferraz, M. R. Ashuthosh, Santosh Krishna, Guohui Wang, Joseph R. Cavallaro, Vitor Silva, Gabriel Falcao, and Madhura Purnaprajna. Pushing the limits of energy efficiency for non-binary ldpc decoders on gpus and fpgas. In *2020 IEEE Workshop on Signal Processing Systems (SiPS)*, pages 1–6, 2020. doi: 10.1109/SiPS50750.2020.9195258.

Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3(1), January 2012. ISSN 2041-1723. doi: 10.1038/ncomms1631. URL http://dx.doi.org/10.1038/ncomms1631.

Dominique Unruh. Protocol composition and complexity. Excellent Computer Science Dissertations 2006, 2007.

Dominique Unruh. Everlasting multi-party computation. Cryptology ePrint Archive, Paper 2012/177, 2012. URL https://eprint.iacr.org/2012/177.

Dominique Unruh. Revocable quantum timed-release encryption. *J. ACM*, 62(6), December 2015. ISSN 0004-5411. doi: 10.1145/2817206. URL https://doi.org/10.1145/2817206.

Ilaria Vagniluca, Beatrice Da Lio, Davide Rusca, Daniele Cozzolino, Yunhong Ding, Hugo Zbinden, Alessandro Zavatta, Leif K. Oxenløwe, and Davide Bacco. Efficient time-bin encoding for practical high-dimensional quantum key distribution. *Phys. Rev. Appl.*, 14:014051, Jul 2020. doi: 10.1103/PhysRevApplied.14.014051. URL https://link.aps.org/doi/10.1103/PhysRevApplied.14.014051.

Nilesh Vyas. *Quantum cryptography in a hybrid security model*. Theses, Institut Polytechnique de Paris, December 2021. URL https://theses.hal.science/tel-03634698.

Nilesh Vyas and Romain Alleaume. Everlasting secure key agreement with performance beyond qkd in a quantum computational hybrid security model, 2020. URL https://arxiv.org/abs/2004.10173.

Jipeng Wang, Joscha Hanel, Zenghui Jiang, Raphael Joos, Michael Jetter, Eddy Patrick Rugeramigabo, Simone Luca Portalupi, Peter Michler, Xiao-Yu Cao, Hua-Lei Yin, Lei Shan, Jingzhong Yang, Michael Zopf, and Fei Ding. Time-bin encoded quantum key distribution over 120 km with a telecom quantum dot source. *Light: Science & Applications*, 15(1):126, February 2026.

Stephanie Wehner, Christian Schaffner, and Barbara M. Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22), June 2008. ISSN 1079-7114. doi: 10.1103/physrevlett.100.220502. URL http://dx.doi.org/10.1103/PhysRevLett.100.220502.

A The Bonami-Beckner Hypercontractive Inequality

The classical hardness of the KV game stems fundamentally from the Bonami-Beckner hypercontractive inequality Bonami [1970]. For a function $f : \{0,1\}^n \to \mathbb{R}$, we define the p-norm uniformly over the Boolean hypercube as $\|f\|_p = \left(\mathbb{E}_{x\in\{0,1\}^n}[|f(x)|^p]\right)^{1/p}$.

Let T_ρ denote the noise operator acting on the hypercube, defined as $(T_\rho f)(x) = \mathbb{E}_y[f(y)]$, where y is generated from x by flipping each bit independently with probability $\eta = (1-\rho)/2$. The Bonami-Beckner inequality states that for any $1 \le p \le q$ and $\rho \le \sqrt{\frac{p-1}{q-1}}$, the noise operator acts as a contraction:

$$\|T_\rho f\|_q \le \|f\|_p \tag{30}$$

In the context of communication complexity, this inequality rigidly bounds the probability that highly correlated noisy strings fall into specific relational subsets. It implies that any classical strategy attempting to output the target relation $a \oplus b = z$ using a strictly constrained classical communication channel of capacity c bits succeeds with a probability exponentially bounded by:

$$P_{win}^{class} \le 2^{c-\Omega\left(\frac{\eta}{1-\eta}n\right)} \tag{31}$$

This hypercontractive suppression provides the crucial exponential gap exploited by the IR-KV-QCT protocol.

B Non-Binary LDPC Codes for Slepian-Wolf Reconciliation

The Slepian-Wolf theorem proves that correlated discrete memoryless sources can be losslessly compressed at a rate bounded by their conditional entropy. In the IR-KV-QCT protocol, Alice and Bob possess correlated high-dimensional strings b^* and b_{out}, respectively, differing by a localised coset error.

To perform this reconciliation over the effective n-ary symmetric channel, we employ non-binary Low-Density Parity-Check (LDPC) codes defined over the Galois field $\mathbb{F}_n$.

1. Parity-Check Matrix Formulation: Alice and Bob pre-share a sparse parity-check matrix H_{PC} of dimension $k \times n$, where elements are non-zero values drawn from $\mathbb{F}_n$. The sparsity ensures that decoding complexity scales linearly with the block length.

2. Syndrome Generation (Alice): During Phase 1, Alice computes the base classical syndrome $S_{\text{base}} = H_{\text{PC}} b^*$, utilizing Galois field arithmetic over $\mathbb{F}_n$. This explicitly compresses her string to k symbols. She transmits S_{base} via the classical timelocked channel.

3. Belief Propagation Decoding (Bob): During Phase 3, Bob computes his local syndrome $S_{Bob} = H_{\text{PC}} b_{\text{out}}$ and evaluates the error syndrome $S_e = S_{Bob} \ominus S_{\text{base}}$. He utilises the log-domain Fast Fourier Transform Sum-Product Algorithm (FFT-SPA) to perform maximum-likelihood decoding over the bipartite Tanner graph of H_{PC}, isolating the most probable error vector e satisfying $H_{\text{PC}} e = S_e$. Bob recovers the target key by evaluating $b^* = b_{\text{out}} \ominus e$.

4. Rate Adaptation and Temporal Execution: Because the physical quantum bit error rate (QBER) fluctuates, a static fixed-rate LDPC code is inefficient. To resolve this without violating protocol causality, the non-binary LDPC framework splits the reconciliation temporally via rate-adaptive blind reconciliation Mueller et al. [2024b]. During Phase 1, Alice encapsulates a base syndrome S_{base}, calculated for the expected baseline QBER, within the initial ciphertext $Enc_{pk_B}(\mathcal{C}_{\text{lock}})$.

During Phase 3, if Bob's initial decoding fails due to transient channel noise, he immediately requests supplemental parity data at time $0 < t' \ll t_{\text{comp}}$. Alice computes the adaptive syndrome S_{adapt} and transmits it encrypted under the same t_{comp}-secure framework. Because Bob holds the access, he decrypts and concludes reconciliation with zero temporal delay. Conversely, the adversary cannot access this classical side-information until $t' + t_{\text{comp}}$. Since Eve's uncorrected quantum memory undergoes complete Markovian depolarisation at t_{comp} relative to the initial transmission, S_{adapt} is definitively shielded from coherent quantum attacks.

The cumulative public leakage, eventually accessible to the adversary post-timelock, is strictly upper-bounded by the protocol's maximum QBER abort threshold $e_{\max}$:

$$c_2 = |S_{\text{base}}| + |S_{\text{adapt}}| \leq f_{\text{EC}} H_n(e_{\max}) \tag{32}$$

If the channel noise exceeds $e_{\max}$, the required adaptive leakage would breach the hypercontractive bound, triggering a deterministic protocol abort.

C Quantitative Bounds on Adversarial Fault-Tolerant Coherence Extension

To evaluate the fundamental security limits against a sophisticated adversary executing a coherent attack, we analyse the case where Eve embeds the intercepted m-copy ensemble into a topological surface code of distance d to actively suppress Markovian depolarisation.

Let the physical gate error rate of the adversary's quantum infrastructure be ϵ_{phys}. The logical error rate ϵ_{L} per operational cycle of a surface code scales with the code distance d GoogleQuantumAI and Collaborators [2025]:

$$\epsilon_{\text{L}} \approx C \left(\frac{\epsilon_{\text{phys}}}{\epsilon_{\text{th}}} \right)^{\frac{d+1}{2}} \tag{33}$$

where $\epsilon_{\text{th}} \approx 1\%$ is the fault-tolerant threshold for a surface code, and $C \approx 0.03$ is a code-specific fitting constant.

For the adversary to successfully preserve the phase configuration of the Khot-Vishnoi encoding up to the computational unlock time t_{comp}, the total accumulated logical error across the memory storage duration must be strictly bounded. Unlike the uncorrected memory, which decays to the completely depolarising channel $\mathcal{F}$, a successful QEC attack requires the final storage channel $\Phi_{t_{\text{comp}}}$ to remain δ-close to the ideal identity channel $\mathcal{I}$ in the diamond norm.

The number of syndrome extraction cycles required over the duration t_{comp} is given by $N_{\text{cycles}} = \frac{t_{\text{comp}}}{\tau_{\text{syn}}}$, where τ_{syn} is the physical measurement cycle time (typically $1\ \mu s$ in superconducting hardware GoogleQuantumAI and Collaborators [2025]). The total logical survival probability P_{surv} is:

$$P_{\text{surv}} = (1 - \epsilon_{\text{L}})^{N_{\text{cycles}}} = \left[1 - C \left(\frac{\epsilon_{\text{phys}}}{\epsilon_{\text{th}}} \right)^{\frac{d+1}{2}} \right]^{\frac{t_{\text{comp}}}{\tau_{\text{syn}}}} \tag{34}$$

For a target security parameter δ, the trace distance degradation from the perfect identity channel must satisfy:

$$\frac{1}{2} \| \Phi_{t_{\text{comp}}} - \mathcal{I} \|_{\diamond} \leq 1 - P_{\text{surv}} \leq \delta \tag{35}$$

Substituting the logical scaling into the inequality yields:

$$\frac{t_{\text{comp}}}{\tau_{\text{syn}}} \cdot C \left(\frac{\epsilon_{\text{phys}}}{\epsilon_{\text{th}}} \right)^{\frac{d+1}{2}} \geq \ln \left(\frac{1}{1 - \delta} \right) \approx \delta \tag{36}$$

Solving explicitly for the required code distance d as a function of the computational timelock duration t_{comp} yields:

$$d \geq \frac{2 \ln\left(\frac{\delta \cdot \tau_{\text{syn}}}{C \cdot t_{\text{comp}}}\right)}{\ln\left(\frac{\epsilon_{\text{phys}}}{\epsilon_{\text{th}}}\right)} - 1 \tag{37}$$

Given that a surface code requires $2d^2 - 1$ physical qubits per logical qubit, protecting the $m \log_2 n$ bits of encoded entropy requires a total physical qubit overhead scaling as:

$$\text{Qubits}_{\text{total}} \approx m \log_2 n \times (2d^2 - 1) \tag{38}$$

For protocol baseline parameters ($n = 64, m = 4$), evaluating against an advanced adversary with physical error rates of $\epsilon_{\text{phys}} = 10^{-4}$, alongside $\tau_{\text{syn}} = 1\ \mu s$ and a timelock scaling to $t_{\text{comp}} = 3600$ s (1 hour) for a security parameter $\delta = 10^{-9}$, mandates a minimum surface code distance of $d \geq 17$. Because the symmetric subspace state contains up to $m \log_2 n = 24$ logical qubits, this demands $\approx 1.38 \times 10^4$ fault-tolerant physical qubits operating continuously with microsecond-level synchronisation. This extensive space-time overhead establishes a strict, quantifiable physical boundary validating the protocol's security, even against an adversary equipped with highly optimised fault-tolerant hardware.

D Finite-Key Statistical Derivations

To establish a rigorous composable ϵ-security framework, Alice and Bob reserve a subset of k_s sifted symbols for parameter estimation (PE), leaving $n_u - k_s$ active qudit symbols of alphabet size n.

1. Statistical Error Correction Bounds: In the asymptotic derivations, we utilised the exact physical QBER, denoted e. For finite-key parameter estimation (PE) in practical implementations, the receiver computes an empirically observed error rate, denoted e_{emp}, which deviates from the theoretical true channel error e_{true} due to finite sampling variance. By applying the Chernoff-Hoeffding tail inequality with a failure probability ϵ_{PE}, the true error e_{true} (which replaces the asymptotic QBER e in all subsequent entropy calculations) is bounded from above by:

$$e_{\text{true}} \leq e_{\text{emp}} + \Delta_{\text{PE}}, \quad \Delta_{\text{PE}} = \sqrt{\frac{\ln(2/\epsilon_{\text{PE}})}{2k_s}} \tag{39}$$

The Slepian-Wolf syndrome leakage over the active block is rigorously quantified by the n-dimensional Shannon entropy: $\text{Leak}_{\text{EC}} = (n_u - k_s) f_{\text{EC}} H_n(e_{\text{true}})$.

2. Block-Wise Min-Entropy Estimation: Since the raw key rounds are independent, the joint guessing probability of the sequence $B^{*(n_u - k_s)}$ given Eve's total classical side-information $E_{\text{tot}} = \{K, Syn(b^*), Y\}$ is bounded by the product of the single-round

probabilities:

$$P_{\text{guess}}\left(B^{*(n_u-k_s)}\middle|E_{\text{tot}}\right) \leq \prod_{j=1}^{n_u-k_s} P_{\text{guess}}\left(b_j^*\middle|K_j, Syn(b_j^*), Y_j\right)$$
$$\leq \left(2^{m\log_2(n)+f_{\text{EC}}H_n(e_{\text{true}})-\gamma n}+\delta\right)^{n_u-k_s} \tag{40}$$

Applying the definition of conditional smooth min-entropy to the joint block:

$$H_{\min}^{\epsilon_s}\left(B^{*(n_u-k_s)}\middle|E_{\text{tot}}\right) \geq -\log_2 P_{\text{guess}}\left(B^{*(n_u-k_s)}\middle|E_{\text{tot}}\right)$$
$$\geq (n_u-k_s)\left[\gamma n - m\log_2 n - f_{\text{EC}}H_n(e_{\text{true}}) - \Delta_\delta\right] \tag{41}$$

where Δ_δ maps the trace distance penalty δ of Eve's memory to the smooth min-entropy: $\Delta_\delta = \log_2\left(1+2\delta\cdot 2^{\gamma n - m\log_2(n) - f_{\text{EC}}H_n(e_{\text{true}})}\right)$.

3. Privacy Amplification and Security Margins: Distilling the final key utilising 2-universal hash functions introduces a finite-key penalty governed by the target correctness (ϵ_{cor}) and secrecy (ϵ_{sec}) parameters under the Leftover Hash Lemma:

$$\Delta_{\text{PA}} = \log_2\left(\frac{2}{\epsilon_{\text{cor}}}\right) + 2\log_2\left(\frac{1}{\epsilon_{\text{sec}}}\right) \tag{42}$$

E Scaling Analysis of Time-Bin Multiplexed High-Dimensional Receivers

To eliminate the requirement of a spatial array of n separate physical single-photon detectors, we map the n-dimensional Khot-Vishnoi phase states onto a temporal alphabet using time-bin encoding. Bob's receiver is structured as an asymmetric Mach-Zehnder Interferometer (MZI) tree consisting of $\log_2 n$ stages of nested fiber delay lines and high-speed 2×2 optical switches.

Let the transmission efficiency of a single fast optical switch/coupler stage be η_{sw}. For a tree configuration of depth $\log_2 n$, the intrinsic structural insertion loss η_{tree} scales as:

$$\eta_{\text{tree}} = (\eta_{\text{sw}})^{\log_2 n} = n^{\log_2 \eta_{\text{sw}}} \tag{43}$$

For a fiber link of length L with attenuation coefficient α (dB/km), the total photon arrival probability at the receiver's single-photon detectors is $\eta_{\text{total}} = 10^{-\frac{\alpha L}{10}} n^{\log_2 \eta_{\text{sw}}}$. The total dark count probability per time-bin frame is bounded by $P_{\text{dc}} = np_{\text{dark}}$, where p_{dark} is the intrinsic dark count probability per detector gate window.

For a transmission block with average photon number μ, the signal-to-noise ratio (SNR) scales as:

$$\text{SNR}(n) = \frac{\mu\eta_{\text{total}}}{\mu\eta_{\text{total}} + np_{\text{dark}}}$$
$$= \frac{1}{1+\frac{p_{\text{dark}}}{\mu 10^{-\frac{\alpha L}{10}}} n^{1-\log_2 \eta_{\text{sw}}}} \tag{44}$$

Because $\eta_{\text{sw}} < 1$, the exponent $(1 - \log_2 \eta_{\text{sw}})$ is strictly greater than 1. Consequently, scaling the dimension n to achieve hypercontractive hardness induces a super-linear dark count penalty. To optimise this structural trade-off, we restrict the operating ceiling to $n = 64$. Utilizing superconducting nanowire single-photon detectors (SNSPDs) with $p_{\text{dark}} = 10^{-7}$ and low-loss switches ($\eta_{\text{sw}} = 0.95$), the multi-copy signal pool ($\mu = m = 4$) completely offsets this super-linear penalty, maintaining an operational SNR > 15 dB at a deployment distance of $L = 100$ km.

F Incompatibility of Goldreich-Levin Reduction with Khot-Vishnoi Encoding

Early QCT protocols Mazzoncini et al. [2025] utilize the Goldreich-Levin (GL) hardcore predicate Goldreich and Levin [1989] to extract a single secure bit from an n-dimensional state. To encrypt a secret data bit $\omega \in \{0, 1\}$, Alice samples a uniformly random public string $r \in \{0, 1\}^n$ and computes the parity bit $c = \omega \oplus (b^* \cdot r) \pmod 2$. She then transmits the classical tuple (r, c) alongside the quantum state.

Applying this single-bit reduction to the Khot-Vishnoi game introduces critical error amplification. In our protocol, Bob measures the incoming state using a Quantum Fourier Transform (QFT) configured to the shifted coset $Y = u \oplus z \oplus H$. The algorithmic basis mismatch z, compounded by physical channel depolarization, renders this measurement probabilistic. Bob's raw outcome is a noisy string $b_{\text{out}} = b^* \oplus h$, where $h \in \{0, 1\}^n$ denotes the error vector.

Using the GL reduction, Bob attempts to extract the bit by computing $c_{\text{out}} = \omega \oplus (b_{\text{out}} \cdot r) \pmod 2$. Substituting the error vector yields:

$$c_{\text{out}} = \omega \oplus ((b^* \oplus h) \cdot r) = c \oplus (h \cdot r) \pmod 2 \tag{45}$$

Because r is sampled uniformly from $\{0, 1\}^n$, the inner product $(h \cdot r) \pmod 2$ evaluates to 1 with probability $1/2$ for any strictly non-zero error vector ($h \neq 0$). Consequently, a single localized bit error in the n-dimensional measurement string b_{out} propagates into a global error, randomizing the distilled GL bit with probability $1/2$.

To establish a secure key, the effective Quantum Bit Error Rate (QBER) of the distilled GL bit, denoted e_{GL}, must remain strictly below the Shannon information limit. Let P_{block} denote the probability that $h \neq 0$. Equation 45 dictates that $e_{\text{GL}} = \frac{1}{2} P_{\text{block}}$. Constraining e_{GL} requires strictly suppressing P_{block}, which implies restricting the per-qubit physical error rate to $\eta \ll 1$.

However, the hypercontractive hardness bound of the Khot-Vishnoi game scales as $\gamma = \Omega\left(\frac{\eta}{1-\eta}\right)$. As $\eta \to 0$ to satisfy the GL error threshold, the classical hardness parameter γ vanishes. Without this strictly positive exponential gap, the classical communication complexity bound $2^{-\Omega(\gamma n)}$ collapses, permitting an adversary to extract the basis and completely compromise the multi-copy transmission. Therefore, abandoning single-bit distillation and directly reconciling the full high-dimensional alphabet is mathematically necessary to decouple physical noise tolerance from the hypercontractive security parameter.