Temporal-Imaging-Enhanced Dispersive-Optics Quantum Key Distribution: Approaching the Schmidt Limit of Energy–Time Entanglement

Irfan Ali-Khan[1]

[1]Independent Researcher, Saratoga, California, USA

June 13, 2026

Abstract

Energy–time entangled photon pairs generated by continuous-wave-pumped spontaneous parametric down-conversion carry a Schmidt number $K = T_{\mathrm{coh}}/\tau_c \sim 10^5$–$10^6$, corresponding to 16–20 bits of potential key per coincidence, yet demonstrated high-dimensional quantum key distribution (QKD) systems extract only 3–7 bits, limited principally by single-photon detector timing jitter. We propose incorporating quantum temporal imaging into entanglement-based time–energy QKD: single-photon time lenses placed inside the trusted receivers magnify the biphoton arrival-time structure before detection, reducing the effective timing resolution below the detector jitter by the temporal magnification M. All required components—picosecond-resolution single-photon time lenses with $M > 150$, sub-3-ps-jitter superconducting nanowire detectors, and dispersive-optics security checks based on nonlocal dispersion cancellation—have been demonstrated separately; to our knowledge their integration into a QKD protocol, with an accompanying rate and security analysis, has not been considered. We further introduce a nonlocal configuration in which the chromatic dispersion of the transmission fiber itself serves as the input element of a distributed temporal-imaging system completed entirely within one party's laboratory. We analyze the secret-key gain as a function of magnification and lens efficiency, identify a detector-saturation-limited regime in which temporal magnification increases the key rate essentially without loss penalty, and estimate that 13–15 bits per coincidence are within reach of demonstrated hardware, approaching the 17.3-bit correlation-time floor as lens point-spread widths reach the 100-fs scale. Combining demonstrated source, detector, and lens parameters with wavelength-division multiplexing, the protocol projects secret-key rates of order 10^8 bits per second: roughly two orders of magnitude beyond the highest rates demonstrated with energy–time entangled photons to date, and at parity with the highest secret-key rate yet demonstrated by any QKD system, achieved here in an entanglement-based architecture at an order-of-magnitude higher photon information efficiency. Security follows the dispersive-optics framework, with the time lens entering as a characterized local operation of the trusted receiver, and avoids the postselection loophole of Franson interferometry.

1 Introduction

The arrival times of energy–time entangled photon pairs constitute one of the largest naturally occurring alphabets in quantum communication. For pairs produced by continuous-wave (cw)

pumped spontaneous parametric down-conversion (SPDC), the two-photon temporal wave function factorizes into a correlation envelope of width $\tau_c \sim 100$ fs, set by the phase-matching or filter bandwidth, and a coherence envelope of width $T_{\mathrm{coh}} \sim 0.1$–$1$ μs, set by the inverse pump linewidth. The Schmidt number of this state, $K \simeq T_{\mathrm{coh}}/\tau_c$ [29, 2], counts its information eigenmodes and routinely reaches 10^5–10^6: in principle 16–20 bits of shared randomness per detected pair.

Large-alphabet QKD exploiting this resource was demonstrated in 2007 using binned arrival-time measurements secured by Franson interferometry, achieving 4 bits per coincidence within a 5% error bound, with an alphabet exceeding 10 bits per pair at higher noise [1]. In the years since, the field has advanced along several fronts reviewed in Sec. 2: dispersive optics has replaced interferometric security checks [5, 8], security proofs against collective and coherent attacks have been established [6, 7], layered error-correction codes have raised the photon information efficiency to 6.9 bits per coincidence [9], and superconducting nanowire single-photon detectors (SNSPDs) have reached sub-3-ps jitter [26].

Yet a large gap remains between demonstrated photon information efficiencies and the Schmidt limit, and its dominant cause is unchanged from 2007: *the timing resolution of single-photon detection exceeds the biphoton correlation time by one to three orders of magnitude.* A correlation feature of width 100 fs read out with even a heroic 3-ps detector pair wastes a factor of ~ 40 in resolution, or about 5 bits per pair; with practical 30–70-ps detectors the waste approaches 10 bits. Source brightness, channel loss, and reconciliation efficiency have all improved dramatically; the resolution mismatch has not.

This paper proposes closing that gap with quantum temporal imaging. A time lens—a quadratic temporal phase imparted by electro-optic modulation or nonlinear wave mixing, combined with input and output dispersion—realizes the temporal analogue of an optical magnifier [15, 16, 17]. Operated on single photons, time lenses have compressed and expanded single-photon bandwidths [18, 19], magnified the temporal correlation function of entangled pairs beyond the reach of direct detection [20], and, most relevantly, achieved input-referred timing resolutions of $\sim$1–2 ps with magnification $M = 158$, explicitly sufficient to overcome SNSPD jitter [21]. We propose placing such magnifiers inside the trusted receivers of a dispersive-optics QKD (DO-QKD) link, so that the arrival-time alphabet is read out with an effective resolution $\sim \tau_j/M$ rather than τ_j, where τ_j is the detector jitter. The security architecture of DO-QKD carries over with the lens entering as a characterized local operation, and the protocol inherits immunity to the postselection loophole that afflicts Franson-based security checks [14, 13].

We make four contributions. First, we specify a complete protocol (Sec. 3) integrating temporal magnification, dispersive-optics security, layered reconciliation, and wavelength-division multiplexing. Second, we derive the photon information efficiency as a function of magnification, lens point-spread width, lens efficiency, and detector jitter, and obtain break-even conditions under which the lens increases the secret-key rate (Sec. 4). Third, we identify the detector-saturation-limited regime—increasingly the relevant regime for bright waveguide sources—in which magnification raises the key rate essentially without loss penalty, because lens insertion loss can be compensated at the source without exceeding the detector count-rate ceiling (Sec. 6). Fourth, we introduce and analyze, at the Gaussian-state level, a *nonlocal* temporal-imaging configuration in which the dispersion of the deployed fiber itself acts as the imaging system's input element, with the lens and output dispersion residing entirely in one laboratory (Sec. 5); the formal tools for this analysis exist in the temporal-entanglement propagation literature [22, 23] but, to our knowledge, this operational use and its security treatment are new.

We have attempted to delineate precisely what is and is not new here, and we encourage the reader to consult Sec. 2 before the technical sections.

2 Relation to prior work

Because the present proposal is a synthesis as much as an invention, we state explicitly which ingredients are established.

Large-alphabet time–energy QKD. The use of binned arrival times of energy–time entangled pairs as a large alphabet, with conjugate-basis monitoring for security, originates with Ref. [1], building on the information-content analysis of Ref. [2] and Franson interferometry [3]. Time–energy entanglement is well preserved over long fiber links [32, 33], and higher-dimensional encoding confers noise robustness [34].

Dispersive-optics QKD. Replacing Franson interferometers with group-velocity dispersion—normal on one side, anomalous on the other—so that frequency correlations are read out as timing correlations via nonlocal dispersion cancellation [4, 24], was proposed in Ref. [5]. Security against collective attacks via time–frequency covariance-matrix (TFCM) estimation was proven in Ref. [6], extended to finite-key composable security in Ref. [7], and demonstrated experimentally in Ref. [8]. A recent demonstration extends dispersive-optics security to large-alphabet time-bin encoding and EPR steering [27]. The idea of trading temporal against spectral encoding to match detector capabilities, including dense wavelength-division multiplexing (DWDM) of the SPDC bandwidth, appears in Ref. [12]; related hybrid time–frequency schemes are the subject of U.S. Patent No. 8,744,086 (2014).

High photon-information efficiency and reconciliation. Layered (multilevel) low-density parity-check reconciliation matched to jitter-dominated error statistics achieved 6.9 bits per coincidence [9], with field demonstrations following [10]. Provably secure time-bin qudit QKD with decoy states reached record rates in Ref. [11]. Information-theoretic treatments of jitter-limited secret-key rates and tailored reconciliation codes are given in Ref. [28].

Quantum temporal imaging. Temporal imaging of classical waveforms is a mature field [15, 16, 17]. At the quantum level, time lenses have engineered the spectra of entangled photons [19], compressed single-photon bandwidths electro-optically [18], magnified two-photon temporal correlation functions past the detector-resolution barrier [20], and reached picosecond input-referred resolution at the single-photon level with $M = 158$ [21]. The propagation of temporal entanglement through dispersive and temporal-imaging systems was analyzed in Refs. [22, 23].

Security loopholes of Franson interferometry. The postselection inherent in Franson interferometry admits local-realistic models [14] and has been exploited in a demonstrated classical-light attack [13]; dispersive-optics security checks involve no path postselection and are not subject to this attack.

What is new here. To the best of our knowledge: (i) the incorporation of single-photon temporal magnification into the key-generation basis of an entanglement-based QKD protocol, with quantitative photon-information-efficiency and break-even analysis, has not been proposed or analyzed; (ii) the observation that, in the detector-saturation-limited regime, temporal magnification raises the secret-key rate essentially free of its insertion-loss penalty is new; (iii) the nonlocal temporal-imaging configuration of Sec. 5, in which deployed-fiber dispersion serves as the input element of a distributed magnifier for the biphoton correlation coordinate, has not been proposed for QKD, and its security discussion is new; and (iv) the system-level synthesis with magnification-aware layered reconciliation is new. We claim no priority on any individual

component, and we would be grateful to learn of relevant work we have missed.

3 Protocol

The protocol operates on energy–time entangled pairs distributed from a central (or Alice-held) source, with one photon delivered to each of Alice and Bob over telecom fiber. The steps are as follows.

1. **Distribution.** A cw-pumped waveguide SPDC source (e.g., periodically poled KTP or lithium niobate [31]) produces frequency-anticorrelated pairs of correlation time $\tau_c \sim 100$ fs and coherence time T_{coh} set by the pump linewidth. A shared, public clock defines frames of duration T_f.

2. **Passive basis choice.** Each party directs each incoming photon with a fixed, passive beam splitter to one of two arms. The *time arm* contains a single-photon temporal magnifier (input dispersion, time lens, output dispersion; magnification M) followed by an SNSPD and a high-resolution time tagger. The *dispersed arm* applies group-delay dispersion (GDD) $+D$ in Alice's receiver and $-D$ in Bob's, followed by direct SNSPD detection, exactly as in DO-QKD [5].

3. **Measurement.** All detection events are time-tagged relative to the shared clock. Arrival times registered behind the magnifier are divided by M (about the lens's temporal field of view) to refer them to the input time axis.

4. **Sifting.** Alice and Bob publicly announce, per frame, which arm fired (not the time tag). Time–time coincidences form the raw key; dispersed–dispersed coincidences form the security-check ensemble; mixed-basis events are discarded or used for calibration.

5. **Parameter estimation.** From the time-basis ensemble the parties estimate the arrival-time correlation variance; from the dispersed-basis ensemble they estimate the dispersed correlation variance, which through nonlocal dispersion cancellation [4] bounds the frequency-correlation variance. Together these constrain the TFCM, upper-bounding Eve's Holevo information per the security analyses of Refs. [6, 7]. A randomly selected subset of time-arm events, routed around the magnifier by a calibrated bypass switch, audits the magnification and lens calibration.

6. **Reconciliation and privacy amplification.** Each retained arrival time within its frame is expanded into b bit layers (most-significant first). Layered LDPC codes with per-layer rates matched to the jitter-concentrated error profile reconcile the key without discarding events [9, 28], and standard privacy amplification compresses by the Holevo bound plus finite-size terms [37, 7].

The architecture is sketched in Fig. 1.

The SPDC bandwidth ($\sim$THz) may be demultiplexed into N_{ch} anticorrelated DWDM channel pairs, each running the protocol in parallel on its own detector pair [12]; this multiplies throughput and defers detector saturation, and is assumed in the rate estimates of Sec. 6.

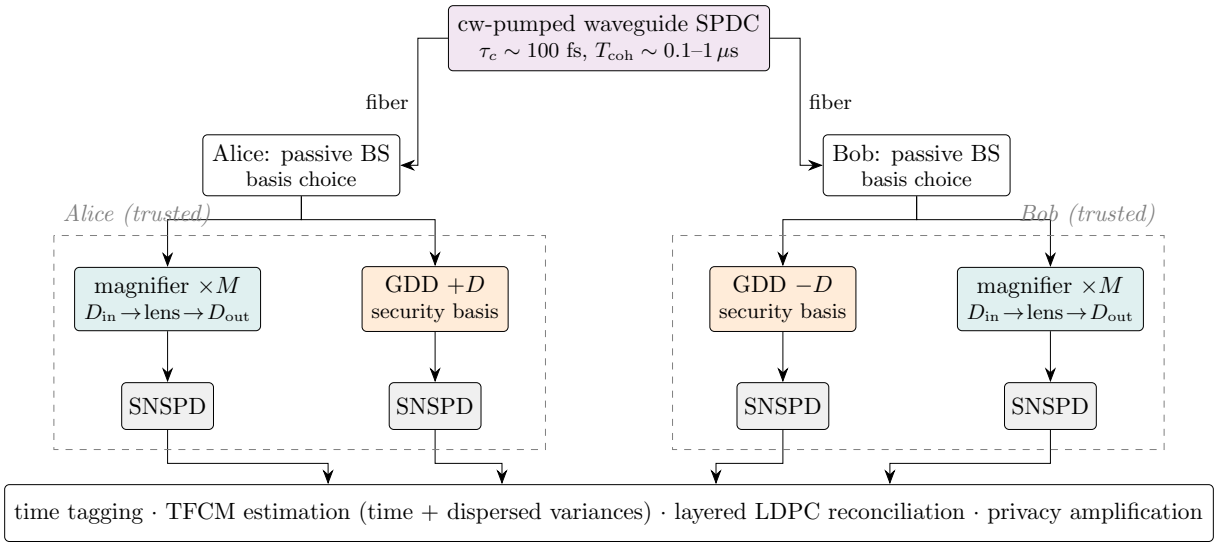

Figure 1: Protocol architecture. Each party passively routes incoming photons either to a *time arm*, where a single-photon temporal magnifier ($\times M$) precedes the SNSPD so that arrival times are resolved at $\sim \tau_j/M$, or to a *dispersed arm* carrying group-delay dispersion of opposite sign at the two receivers; nonlocal dispersion cancellation renders the dispersed-basis coincidence width a probe of the frequency correlations, and the two measured variances jointly constrain the time–frequency covariance matrix that bounds Eve's information [5, 6]. A calibrated bypass switch (not shown) routes a random subset of time-arm events around the magnifier for calibration auditing. In the nonlocal variant of Sec. 5, Bob's magnifier is removed entirely and the deployed fiber's dispersion serves as D_{in} of a distributed imaging system completed in Alice's receiver.

4 Information efficiency with temporal magnification

4.1 State and resolution model

With a cw pump of frequency ω_p, the post-filter biphoton amplitude is well approximated by

$$|\psi\rangle \propto \int dt_1\, dt_2\; e^{-(t_1-t_2)^2/4\tau_c^2}\; e^{-(t_1+t_2)^2/16T_{\mathrm{coh}}^2}\; e^{-i\omega_p(t_1+t_2)/2}\; \hat{a}_1^\dagger(t_1)\hat{a}_2^\dagger(t_2)\,|0\rangle\,, \tag{1}$$

with Schmidt number $K \simeq T_{\mathrm{coh}}/\tau_c$ [29, 30]. The arrival-time difference $t_- = t_1 - t_2$ carries the key correlations; the maximum extractable information per pair is $\log_2 K$.

Detection introduces, per receiver, a Gaussian-equivalent timing error ϵ combining detector jitter τ_j and, when a magnifier of magnification M and input-referred point-spread (impulse-response) width $\delta\tau_L$ is present,

$$\epsilon = \sqrt{(\tau_j/M)^2 + \delta\tau_L^2}\,, \qquad \sigma_{\mathrm{obs}} = \sqrt{\tau_c^2 + \epsilon_A^2 + \epsilon_B^2}\,, \tag{2}$$

where σ_{obs} is the observed width of the coincidence peak in t_-. Without magnifiers ($M = 1$, $\delta\tau_L = 0$), $\sigma_{\mathrm{obs}} \approx \sqrt{2}\,\tau_j$ for $\tau_j \gg \tau_c$. The demonstrated single-photon magnifier of Ref. [21] corresponds to $M = 158$ with input-referred resolution ≈ 1.3–2 ps inclusive of electronics; electro-optic lenses [18] trade aperture against point-spread width and are projected to reach sub-picosecond $\delta\tau_L$ with deeper phase modulation.

Binning t_- within the frame at width $\delta = \alpha\,\sigma_{\rm obs}$ (guard factor $\alpha \approx 3$–5, with residual neighbor-bin errors absorbed by the layered code) yields an alphabet $D = T_f/\delta$ and an ideal photon information efficiency

$$I_{AB} \approx \log_2 \frac{T_f}{\alpha\,\sigma_{\rm obs}}\,. \tag{3}$$

The gain from magnification is therefore

$$\Delta I = I_{AB}(M) - I_{AB}(1) \approx \log_2 \frac{\sqrt{2}\,\tau_j}{\sqrt{\tau_c^2 + 2\left[(\tau_j/M)^2 + \delta\tau_L^2\right]}}\,. \tag{4}$$

Two regimes follow. With state-of-the-art $\tau_j = 3$ ps SNSPDs [26] and $\delta\tau_L = 0.5$ ps, $M \gtrsim 10$ gives $\Delta I \approx 2.4$ bits. With practical $\tau_j = 30$ ps detectors and the demonstrated lens of Ref. [21] ($M = 158$, $\delta\tau_L \approx 1.3$ ps), $\Delta I \approx 4.5$ bits—and, notably, the combination of an inexpensive detector and a demonstrated lens outperforms the most exotic detector alone. Magnification substitutes a room-temperature optical component for cryogenic jitter engineering. For the frame parameters used throughout this paper ($T_f = 64$ ns, $\alpha = 4$), the correlation-time floor itself lies at $\log_2[T_f/(\alpha\tau_c)] = 17.3$ bits per coincidence.

4.2 Break-even against lens loss

A magnifier has finite efficiency η_L (conversion plus insertion; $\eta_L \sim 0.2$–0.5 for four-wave-mixing lenses, with electro-optic lenses potentially higher). In the *source-limited* regime, where the coincidence rate R_c is proportional to delivered pair flux, the secret-key rate scales as $R_c\,\eta_L\,I_{\rm sec}(M)$ in the time basis, so the lens helps when

$$\eta_L > \frac{I_{\rm sec}(1)}{I_{\rm sec}(M)}\,, \tag{5}$$

where $I_{\rm sec}$ is the secret fraction per coincidence after reconciliation and privacy amplification. For the 30-ps-detector example above (I from ≈ 8.6 to ≈ 13.1 bits at $T_f = 64$ ns, $\alpha = 4$), break-even requires only $\eta_L \gtrsim 0.66$; for the 3-ps example the requirement is more stringent. Equation (5) is the honest statement of when the lens pays for itself photon-for-photon.

The more favorable and, for modern systems, more relevant case is the *detector-saturation-limited* regime. Waveguide SPDC sources deliver pair rates far exceeding the maximum useful count rate $R_{\rm det}^{\rm max}$ of an SNSPD channel (dead-time and pile-up limited, typically 10^6–$10^7\,{\rm s}^{-1}$). When the operating point is set by $R_{\rm det}^{\rm max}$ rather than by available pairs, lens loss is compensated upstream by pump power at no cost to the detected rate, and the key rate becomes

$$R_{\rm key} \approx N_{\rm ch}\,R_{\rm det}^{\rm max}\,\kappa\,I_{\rm sec}(M)\,, \tag{6}$$

with κ the coincidence-to-singles ratio: every bit of ΔI multiplies the key rate directly. The cost reappears only through the multi-pair emission probability per frame, which grows with pump power and feeds the accidental-coincidence floor and Eve's multi-pair information; this is bounded by frame-occupancy statistics in the standard way [6, 9] and constrains the usable T_f and pump strength jointly. We emphasize that Eq. (6) is the operating point that bright modern sources actually reach, and it is the regime in which temporal magnification is most valuable.

4.3 Security considerations

The security architecture is that of DO-QKD [5, 6, 7]: Alice and Bob's measured time-basis and dispersed-basis correlation variances constrain the time–frequency covariance matrix of the joint state delivered by the (adversarial) channel, and Gaussian extremality yields an upper bound on Eve's Holevo information; finite-key corrections follow Ref. [7]. Three points specific to the present proposal deserve statement.

First, the magnifier is a *local operation of the trusted receiver*, applied after the channel and after basis selection. As such it cannot increase Eve's information; its calibrated map ($t \to Mt$ within the field of view, efficiency η_L, point spread $\delta\tau_L$) is inverted in software, and miscalibration appears as excess noise in the estimated time-basis variance, which the security bound treats conservatively (i.e., attributes to Eve). The random lens-bypass audit of Sec. 3 bounds calibration drift and tampering of the lens pump.

Second, the lens's own optical pump (for four-wave-mixing implementations) is a potential side channel: pump leakage correlates with lens timing, and an active Eve might attempt to probe or inject light at lens wavelengths. Standard countermeasures—spectral isolation, watchdog photodiodes, and optical isolators at the receiver input—apply, and the conservative variance accounting above covers residual effects. We flag a full device-level analysis as necessary future work; the situation is analogous to, and no worse than, detector-side channels in any QKD receiver.

Third, because neither basis involves interferometric path postselection, the protocol is structurally immune to the Franson postselection attack [14, 13]. Frame postselection (discarding frames without coincident detections) is loss postselection of the kind already treated in the DO-QKD security analyses [6, 7].

5 Nonlocal temporal magnification

We now describe the configuration that we regard as the most physically interesting contribution of this paper. In a frequency-anticorrelated biphoton, group-delay dispersion applied to one photon acts, at the level of the two-photon amplitude in the difference coordinate t_-, equivalently to dispersion applied to its partner: writing $\omega_{1,2} = \omega_p/2 \pm \Omega$ for a narrow pump, GDD phases $\exp[iD_A\Omega^2/2]$ and $\exp[iD_B\Omega^2/2]$ applied separately to the two photons combine into a single phase $\exp[i(D_A + D_B)\Omega^2/2]$ on the joint amplitude. This is the content of nonlocal dispersion cancellation [4, 24, 25]: only the *sum* of the dispersions broadens the coincidence peak.

Temporal imaging of a waveform requires input dispersion D_{in}, a quadratic phase (focal GDD D_f), and output dispersion D_{out} satisfying the imaging condition

$$\frac{1}{D_{\text{in}}} + \frac{1}{D_{\text{out}}} = \frac{1}{D_f}\,, \qquad M = -\frac{D_{\text{out}}}{D_{\text{in}}}\,, \tag{7}$$

in direct analogy to the thin-lens equation [15, 16]. The observation above implies that, for the biphoton difference coordinate, the three elements of Eq. (7) need not reside on the same photon's path. In particular, the uncompensated chromatic dispersion D_{fib} of Bob's deployed fiber—ordinarily an impairment requiring compensation—can serve as D_{in}, with the time lens and the output dispersion D_{out} located entirely in Alice's receiver acting on her photon. At the Gaussian level, propagating the state of Eq. (1) through this distributed system (the formalism of Refs. [22, 23] applies directly) is expected to yield a coincidence distribution in t_- magnified

by M, even though no single photon traverses a complete imaging system, and even though Bob's receiver contains nothing but a detector. We state plainly that this derivation has not been carried through in full here: it is published as an explicitly open claim, labeled as such in the claim ledger accompanying this work, and its confirmation or refutation is invited as a community contribution to the public record of this paper.

Operationally this has three attractive features. (i) Bob's receiver is reduced to a passive splitter, a dispersive element for the security basis, and detectors—all magnification hardware concentrates at Alice, which suits asymmetric deployments (a central exchange serving thin clients). (ii) The channel's own dispersion is conscripted as a functional element rather than compensated, in the same spirit in which DO-QKD conscripts dispersion for security. (iii) Singles distributions on both sides remain nanosecond-scale featureless blurs; the magnified structure exists only in coincidences, which is operationally pleasant (an intercepting Eve gains nothing detector-resolution-limited to exploit) though we emphasize it confers no security beyond the TFCM bound.

Two honest caveats accompany this proposal. First, the temporal field of view of the lens must cover the arrival-time uncertainty of the photon within a frame; with a cw pump this uncertainty is the full frame, which strains electro-optic apertures. A pulsed or phase-modulated pump that pre-localizes pair generation into known sub-frame slots (at some cost in T_{coh} and hence K), or a triggered lens architecture, addresses this; the optimization of frame structure against lens aperture is an open design problem, for which temporal self-imaging (Talbot) pump combs are a natural candidate. Second, because the lens now acts on a photon that has not traversed the channel, the calibration audit of Sec. 3 must additionally verify the *sign and magnitude* of the deployed-fiber dispersion serving as D_{in}; an Eve with access to the fiber could alter its dispersion, which would appear as a magnification miscalibration. The conservative variance accounting of Sec. 4.3 again covers this—altered dispersion inflates the measured time-basis variance and reduces the certified key rather than compromising it—but a dedicated analysis is warranted and is identified as future work.

6 Rate estimates

Table 1 assembles representative operating points. We stress that the entries for the proposed protocol are design estimates from Eqs. (2)–(6) using demonstrated component parameters, not measurements, and that finite-key, reconciliation-inefficiency ($\beta \approx 0.9$), and privacy-amplification deductions are folded into an assumed secret fraction $I_{\mathrm{sec}} \approx 0.6\, I_{AB}$, consistent with the accounting achieved in Ref. [9].

Three observations. First, against the 2007 baseline the proposed system gains roughly six orders of magnitude in key rate, of which approximately three are generational (source brightness, detector efficiency, multiplexing), one to two come from reclaiming alphabet depth via magnification and zero-discard layered reconciliation, and the remainder from saturation-limited operation. Second, against the state of the art [9, 11] the distinctive gain of this proposal is the 7–10 bit-per-coincidence increase in PIE at fixed detector technology, worth a factor of ∼30–100 in rate when detectors, not photons, are the scarce resource. Third, the protocol degrades gracefully: every parameter (M, T_f, α, layer rates) is computational or locally physical, so the operating point can be re-optimized in post-processing as channel conditions or adversarial activity (reflected in the TFCM estimates) evolve—preserving the software-reoptimization philosophy of Ref. [1].

System	Detector	PIE (bits/coin)	Coincidence rate	Key rate
Ref. [1] (2007)	SPCM, 350 ps	4	~ 50 Hz	$\sim 2 \times 10^2$ b/s
Ref. [9] (2015)	SNSPD, ∼70 ps	6.9	$\sim 10^6$ s^{-1}	2.7×10^6 b/s
Proposed, local lenses	SNSPD, 30 ps; M=158	13	10^7 s^{-1} ($\times N_{\mathrm{ch}}$)	$\sim 10^8$ b/s
Proposed, 3 ps + lens	SNSPD, 3 ps; M=30	14–15	10^7 s^{-1} ($\times N_{\mathrm{ch}}$)	$\gtrsim 10^8$ b/s

Table 1: Representative operating points. PIE: photon information efficiency before secret-fraction deductions; proposed-system rows assume $T_f = 64$ ns, $\alpha = 4$, $\delta\tau_L = 1.3$ ps (M=158 row, per Ref. [21]) or 0.5 ps (projected electro-optic lens), DWDM parallelization $N_{\mathrm{ch}} = 8$–16 [12], and detector-saturation-limited operation, Eq. (6). Channel loss shortens all rates equally and is omitted for comparability.

It is fair to ask how the projected $\sim 10^8$ b/s compares with the best QKD systems of any architecture, and whether the exercise is therefore worthwhile. The highest secret-key rate demonstrated to date is 115.8 Mb/s over 10 km of standard fiber, achieved with decoy-state BB84, a multipixel SNSPD, and 2.5-GHz-class clocking [35]; a contemporaneous time-bin system reached 64 Mb/s at 10 km [36], and continuous-variable systems have recently reported still higher composable rates at metropolitan distances in preprint form (e.g., arXiv:2503.14843). Our projection is thus at *parity* with the demonstrated record, not beyond it, and we do not claim raw-rate supremacy over mature prepare-and-measure systems at metro distances. The case for the present protocol is threefold. First, it is entanglement-based: security does not rest on trusting the source, and the architecture extends naturally to untrusted-node and multiuser network settings where prepare-and-measure does not. Second, and centrally, it achieves its rate at a photon information efficiency of order 10 bits per detected coincidence, versus $\lesssim 1$ bit per detected photon for the record systems above; wherever detected photons rather than clock cycles are the scarce resource—long-haul and satellite links, loss-dominated channels, detector-saturation-limited receivers, and heavily multiplexed networks—photon information efficiency, not source clock rate, sets the achievable key rate, and there the advantage of this approach is a genuine order of magnitude. Third, against its own family—entanglement-based time–energy QKD, whose demonstrated rates stand at 2.7 Mb/s in the laboratory [9] and 1.2 Mb/s over deployed fiber [10]—the projected gain is roughly two orders of magnitude.

7 Discussion

The proposal advanced here is conservative in its physics—every element has been demonstrated—and aggressive only in its integration. The experimental program it implies is staged and each stage is independently publishable: (1) a tabletop demonstration that a single-photon magnifier on one arm of a cw-pumped DO-QKD link increases measured PIE per Eq. (4); (2) closure of the security loop with TFCM estimation and the lens-bypass audit; (3) the nonlocal configuration over a fiber spool serving as D_{in}; (4) DWDM parallelization. Stage (1) requires only the marriage of two published experimental capabilities [8, 21].

Several theoretical problems remain open and are stated here as invitations. A full multimode (beyond-Gaussian) security analysis incorporating the lens map, its pump side channel, and the nonlocal configuration's dependence on channel dispersion is the most important. The joint optimization of pump format (cw, pulsed, or Talbot-comb), frame structure, and lens aperture is the most practical. And the information-theoretic question of optimal reconciliation when

the error kernel is a known, magnification-rescaled jitter distribution connects directly to the coding-theory program of Ref. [28].

Energy–time entanglement has always promised more bits than our detectors could read. Dispersive optics taught us to let the channel's dispersion stand guard; temporal imaging now offers to let optics, rather than cryogenics, supply the missing resolution. The Schmidt limit is not yet in hand, but for the first time the gap between it and demonstrated hardware is an engineering integration problem rather than a detector-physics problem.

Note added (12 June 2026)

Hours after the v1.0.0 release, an author reality check sharpened red-team Finding 3, and per the living-record doctrine of this publication the amendment is absorbed here rather than exiled to errata. Temporal magnification dilates the lens's accepted input window by M: an aperture of duration T_a occupies MT_a at the output, so apertures cannot be packed and each lens-plus-detector channel accepts only $\sim 1/M$ of continuous input time under cw pumping. At any useful M, this per-channel acceptance penalty overwhelms the $\sim 1.5\times$ gain in bits per detected pair, and the rate projections of Table 1 therefore implicitly assume an aperture architecture this paper did not specify. The photon-information-efficiency claims (bits per detected coincidence) are unaffected. The rate projections are now labeled *architecture-dependent*, pending a quantified treatment of one of three candidate architectures: (a) a pulsed or temporal-Talbot pump aligning pair generation into accepted apertures (repetition rate $\lesssim 1/(MT_a)$, with a correspondingly reduced frame alphabet); (b) M-way time-demultiplexing of the magnified output onto a detector array; or (c) wavelength-division parallelization scaled toward $\sim M$ channels. Claim C07 in the public ledger is amended accordingly, and the full statement is recorded as issue #1 of the public repository. The archived v1.0.0 of record remains frozen at Zenodo; this note is part of the living record that supersedes it.

Reproducibility

Every quantitative claim in this paper (Schmidt numbers, magnification gains, break-even efficiencies, Table 1, and rate comparisons) is recomputed from its stated assumptions by an open verification script, `verify_numbers.py`, distributed with this manuscript. Readers are invited to rerun it, vary the assumptions, and report discrepancies. The archived version of record carries DOI 10.5281/zenodo.20673750 (concept DOI 10.5281/zenodo.20670769, always resolving to the latest version); each release hash is independently anchored in the Bitcoin blockchain via OpenTimestamps.

Acknowledgments

The author acknowledges the substantive use of an AI assistant (Claude, Anthropic) in this work, including literature search, prior-art analysis, drafting, rate modeling, and the figure and verification tooling. Beyond its scientific content, this paper is offered as a demonstration of AI-assisted independent research published in a verified-open format, whose governing invariant is honest labeling rather than universal verification: every claim is typed and routed to a verifier in a public claim ledger; numerical claims are recomputed by an open script under continuous integration; citations are audited against primary sources; and claims that no human or machine

has independently verified—including the nonlocal-imaging derivation of Sec. 5—are labeled as open rather than asserted. The author's review was conducted at the level of consistency, plausibility, and reality checks on end results, not independent re-derivation, and responsibility for the work rests with the author on that explicitly stated basis. Confirmations, refutations, and corrections are invited through the public repository accompanying this paper, where they become part of its versioned record.

References

[1] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Large-alphabet quantum key distribution using energy-time entangled bipartite states, Phys. Rev. Lett. **98**, 060503 (2007).

[2] I. Ali Khan and J. C. Howell, Experimental demonstration of high two-photon time-energy entanglement, Phys. Rev. A **73**, 031801(R) (2006).

[3] J. D. Franson, Bell inequality for position and time, Phys. Rev. Lett. **62**, 2205 (1989).

[4] J. D. Franson, Nonlocal cancellation of dispersion, Phys. Rev. A **45**, 3126 (1992).

[5] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, High-dimensional quantum key distribution using dispersive optics, Phys. Rev. A **87**, 062322 (2013).

[6] Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry, Phys. Rev. Lett. **112**, 120506 (2014).

[7] M. Y. Niu, F. Xu, J. H. Shapiro, and F. Furrer, Finite-key analysis for time-energy high-dimensional quantum key distribution, Phys. Rev. A **94**, 052323 (2016).

[8] C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R. D. Horansky, V. B. Verma, A. E. Lita, R. P. Mirin, F. Marsili, M. D. Shaw, S. W. Nam, G. W. Wornell, F. N. C. Wong, J. H. Shapiro, and D. Englund, Entanglement-based quantum communication secured by nonlocal dispersion cancellation, Phys. Rev. A **90**, 062331 (2014).

[9] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong, Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding, New J. Phys. **17**, 022002 (2015).

[10] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. B. Dixon, F. N. C. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, High-rate field demonstration of large-alphabet quantum key distribution, arXiv:1611.01139 (2016).

[11] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, Sci. Adv. **3**, e1701491 (2017).

[12] J. Mower, F. N. C. Wong, J. H. Shapiro, and D. Englund, Dense wavelength division multiplexed quantum key distribution using entangled photons, arXiv:1110.4867 (2011).

[13] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson, Hacking the Bell test using classical light in energy-time entanglement-based quantum key distribution, Sci. Adv. **1**, e1500793 (2015).

[14] S. Aerts, P. Kwiat, J.-Å. Larsson, and M. Żukowski, Two-photon Franson-type experiments and local realism, Phys. Rev. Lett. **83**, 2872 (1999).

[15] B. H. Kolner and M. Nazarathy, Temporal imaging with a time lens, Opt. Lett. **14**, 630 (1989).

[16] B. H. Kolner, Space-time duality and the theory of temporal imaging, IEEE J. Quantum Electron. **30**, 1951 (1994).

[17] R. Salem, M. A. Foster, and A. L. Gaeta, Application of space-time duality to ultrahigh-speed optical signal processing, Adv. Opt. Photon. **5**, 274 (2013).

[18] M. Karpiński, M. Jachura, L. J. Wright, and B. J. Smith, Bandwidth manipulation of quantum light by an electro-optic time lens, Nat. Photonics **11**, 53 (2017).

[19] J. M. Donohue, M. Mastrovich, and K. J. Resch, Spectrally engineering photonic entanglement with a time lens, Phys. Rev. Lett. **117**, 243602 (2016).

[20] S. Mittal, V. V. Orre, A. Restelli, R. Salem, E. A. Goldschmidt, and M. Hafezi, Temporal and spectral manipulations of correlated photons using a time lens, Phys. Rev. A **96**, 043807 (2017).

[21] C. Joshi, B. M. Sparkes, A. Farsi, T. Gerrits, V. Verma, S. Ramelow, S. W. Nam, and A. L. Gaeta, Picosecond-resolution single-photon time lens for temporal mode quantum processing, Optica **9**, 364 (2022).

[22] M. Tsang and D. Psaltis, Propagation of temporal entanglement, Phys. Rev. A **73**, 013822 (2006).

[23] G. Patera, J. Shi, D. B. Horoshko, and M. I. Kolobov, Quantum temporal imaging: application of a time lens to quantum optics, J. Opt. **19**, 054001 (2017).

[24] S.-Y. Baek, Y.-W. Cho, and Y.-H. Kim, Nonlocal dispersion cancellation using entangled photons, Opt. Express **17**, 19241 (2009).

[25] J.-P. W. MacLean, J. M. Donohue, and K. J. Resch, Direct characterization of ultrafast energy-time entangled photon pairs, Phys. Rev. Lett. **120**, 053601 (2018).

[26] B. Korzh, Q.-Y. Zhao, J. P. Allmaras, S. Frasca, T. M. Autry, E. A. Bersin, A. D. Beyer, R. M. Briggs, B. Bumble, M. Colangelo, et al., Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector, Nat. Photonics **14**, 250 (2020).

[27] K.-C. Chang, M. C. Sarihan, X. Cheng, Z. Zhang, and C. W. Wong, Large-alphabet time-bin quantum key distribution and Einstein-Podolsky-Rosen steering via dispersive optics, Quantum Sci. Technol. **9**, 015018 (2024).

[28] J. J. Boutros and E. Soljanin, Time-entanglement QKD: secret key rates and information reconciliation coding, IEEE Trans. Commun. **71**, 7174 (2023).

[29] C. K. Law and J. H. Eberly, Analysis and interpretation of high transverse entanglement in optical parametric down conversion, Phys. Rev. Lett. **92**, 127903 (2004).

[30] W. P. Grice and I. A. Walmsley, Spectral information and distinguishability in type-II down-conversion with a broadband pump, Phys. Rev. A **56**, 1627 (1997).

[31] T. Zhong, F. N. C. Wong, A. Restelli, and J. C. Bienfang, Efficient single-spatial-mode periodically-poled $KTiOPO_4$ waveguide source for high-dimensional entanglement-based quantum key distribution, Opt. Express **20**, 26868 (2012).

[32] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Violation of Bell inequalities by photons more than 10 km apart, Phys. Rev. Lett. **81**, 3563 (1998).

[33] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, Distribution of time-bin entangled qubits over 50 km of optical fiber, Phys. Rev. Lett. **93**, 180502 (2004).

[34] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of quantum key distribution using d-level systems, Phys. Rev. Lett. **88**, 127902 (2002).

[35] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Q. Li, Y. Liu, Q. Zhang, C.-Z. Peng, L. You, F. Xu, and J.-W. Pan, High-rate quantum key distribution exceeding 110 $\mathrm{Mb\,s^{-1}}$, Nat. Photonics **17**, 416 (2023).

[36] F. Grünenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hänggi, N. Bosshard, F. Bussières, and H. Zbinden, Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems, Nat. Photonics **17**, 422 (2023).

[37] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. **85**, 441 (2000).