Lightweight Noise Diagnosis for Photonic Quantum Detectable Byzantine Agreement

Kevin Bogner [*], Kuan-Cheng Chen [†], Aysajan Abidin [*], Kin K. Leung [†]
[*]COSIC, KU Leuven, Belgium
[†]Department of Electrical and Electronic Engineering, Imperial College London, United Kingdom

***Abstract*—Detectable Byzantine Agreement (DBA) protocols abort rather than risk inconsistent decisions when verification fails. Quantum variants (QDBA) implement this detectability via multipartite entanglement checks, but in photonic networks non-uniform noise across participants makes these checks brittle: a handful of noisy nodes can trigger needless aborts or conceal adversarial behavior. We introduce two drop-in diagnosis methods that run during the standard entanglement-verification step of QDBA protocols: (i) a *batch health check* that detects both state leakage and insufficient fidelity, and (ii) a *per-node diagnosis* that estimates each participant's error rates and labels loss-biased outliers. The methods require no extra quantum rounds and add only modest classical overhead. In simulations, the batch health check substantially reduces false accepts while preserving clean-batch acceptance, and the per-node diagnosis reliably flags noisy Lieutenants and the Commander at practical verification sizes. The techniques are compatible with existing QDBA protocols.**

I. Introduction

Byzantine Agreement (BA) is foundational to fault-tolerant distributed systems [1]–[3]. Here, we call a party *non-faulty* if it follows the protocol and remains within specified error thresholds; both adversarial deviations *and* non-malicious (accidental) failures count as *faulty*. Quantum Detectable Byzantine Agreement (QDBA) realizes *detectability*: parties either agree or explicitly abort the session based on correlations of distributed entangled quantum states [4]–[7]. Such correlations are routinely verified with entanglement-witness or Bell-type tests [8], [9]. QDBA is used to reach consensus in a distributed quantum-computing network, where quantum networking is native [10]–[12].

In this work we focus on photonic networks where heterogeneous noise (loss and detector asymmetries) is common [10], [13], [14] and can make detectability brittle: different participants experience different fiber path lengths and components, resulting in different noise levels. Single-photon detectors have a threshold for detecting a logical 1 and a non-zero probability of detecting a logical 1 when no photon is present; the $1 \to 0$ (*loss-biased*) error rate therefore typically exceeds the $0 \to 1$ rate. Accordingly, we emphasize the loss-biased subtype in this work. This bias is well documented [15]–[17].

In photonic implementations, hardware imperfections corrupt protocol data in two different ways: (i) *leakage*, which causes photon loss or spurious detection events that fall outside the expected measurement outcomes, and (ii) *in-support drift*, which keeps the qubits within the valid computational space but biases the measured bit-string frequencies. Our batch health check explicitly separates these regimes by employing a leakage-detection gate followed by a conditional fidelity test on the remaining valid outcomes. Furthermore, we identify the noise level per-node to account for the physical asymmetries inherent in photonic hardware.

This brittleness is not addressed by existing quantum error-mitigation techniques, which operate mostly below the protocol layer (e.g., calibration and distillation) and do not localize noisy participants during the protocol execution [18]–[22]; fully fledged quantum error correction could in principle overcome noise but remain resource-intensive in near-term quantum networking [10].

A. Contributions

We add *lightweight, protocol-layer diagnosis* to the entanglement verification step of standard QDBA protocols:

- *Batch Health Check:* Rejects batches with excessive leakage (outcomes that should be impossible for the ideal distributed quantum state) or distributional drift (outcomes are within the allowed results, but their relative frequencies are skewed compared to the distribution of the ideal distributed quantum state).
- *Per-Node Diagnosis:* Tags participants as noisy or clean via one-sided Wilson bounds [23] based on their individual error rates. Noisy participants are further labeled as loss-biased $(1 \to 0)$, depending on the error bias.
- *Compatibility & Cost:* Drop-in at the entanglement verification step; no extra quantum rounds are required, only a modest classical overhead; orthogonal to calibration and distillation.

Our contribution focuses on diagnosis at the protocol layer, where we analyze the classical measurement records generated by the QDBA entanglement distribution. While the diagnostic computations themselves are classical, they are specifically designed to identify characteristics that arise from the quantum hardware.

B. Related Work

QDBA protocols use multipartite quantum correlations to realize agreement-or-abort in the presence of faulty parties [4], [5]. Entanglement-based variants include the four-photon construction proposed in [24] and experimentally demonstrated in [6]. Recent protocol designs explore GHZ-type resources and EPR-only constructions [25], [26], while resource analyses study verification sample costs under realistic noise [7]. Our work does not modify the underlying QDBA primitive;

instead, it extends the standard entanglement-verification step with a lightweight batch gate and per-node diagnosis tailored to heterogeneous photonic noise.

Section II reviews the baseline protocol we build upon. Section III presents our batch health check and per-node diagnosis. Section IV evaluates these methods via simulation. Finally, Section V discusses implications and outlines future work.

II. Preliminaries

We build on the photonic QDBA protocol of [27] with one Commander and $n-1$ Lieutenants. Each round distributes k copies of an n-party entangled state $|\Psi_n\rangle$ and performs a health check of the distributed quantum state on a public-random subset $\mathcal{S} \subset \{1,\dots,k\}$. The copies not selected for this check are used to execute detectable broadcast, following the remainder of the original protocol without modification.

A. Baseline Protocol

Unlike a standard GHZ state, whose Z-basis measurement produces only two computational-basis outcomes, the state $|\Psi_n\rangle$ of [27] has $|\mathcal{A}| = 2n$ allowed joint outcomes: two deterministic outcomes $(00, 1^{\otimes(n-1)})$ and $(11, 0^{\otimes(n-1)})$, each with probability $1/3$, and $2(n-1)$ probabilistic outcomes where the Commander measures 01 (resp. 10) and exactly one Lieutenant differs from the rest, each with probability $1/(6(n-1))$. Outcomes outside $\mathcal{A}$ are treated as *leakage*.

1) Verification Step (Baseline): The baseline protocol [27] accepts a batch if the support fidelity

$$F_{\text{supp}} = \frac{1}{|\mathcal{S}|}\sum_{i\in\mathcal{S}} \mathbf{1}[(\mathsf{Commander}_i, \mathsf{Lieutenants}_i) \in \mathcal{A}]$$

exceeds $1-\tau_{\text{leak}}$ [27]. In addition, NISQ-compatible mitigation (DD on idle qubits and T-REx at readout) is applied, which does not change our diagnosis logic.

2) System Assumptions: Authenticated classical channels and a short-message broadcast are available [2], [28]; a public randomness beacon (or shared seed) selects $\mathcal{S}$ and measurement settings. Safeguards against transcript fabrication (e.g., trap rounds and commit-and-reveal) are orthogonal to our diagnosis and are not re-proved here.

III. Noise-Diagnosis Methods

We extend the verification step of the baseline protocol [27] with lightweight methods to estimate the overall batch health and the per-node noise levels of Lieutenants and the Commander. All Wilson bounds in this section are one-sided at level $\alpha = 0.05$ [23]. (A Wilson bound is a confidence-interval method for binomial proportions that remains reliable at small sample sizes, unlike the normal approximation.)

We continue to operate on k preparations of $|\Psi_n\rangle$ and reserve $\mathcal{S} \subset \{1,\dots,k\}$ for diagnosis, selected by the same public randomness beacon that selects the verification subset in the baseline protocol [27]. Increasing the verification subset size $\mathcal{S}$ tightens our estimates but leaves fewer rounds available for the consensus protocol.

We divide $\mathcal{S}$ into two subsets: $\mathcal{S}_{\text{det}}$ and $\mathcal{S}_{\text{prob}}$ depending on the Commander's measurement outcome:

- $\mathcal{S}_{\text{det}}$: The subset of indices where the Commander measures $|00\rangle$ or $|11\rangle$ and consensus is reached deterministically.
- $\mathcal{S}_{\text{prob}}$: The subset of indices where the Commander measures $|01\rangle$ or $|10\rangle$ and consensus is reached probabilistically.

For the batch health check, proposed in this work, the measured quantities are computed on the whole $\mathcal{S}$. By contrast, our per-node diagnosis is restricted to $\mathcal{S}_{\text{det}}$, where each Lieutenant's expected bit is fixed by the Commander's outcome. Using $\mathcal{S}_{\text{prob}}$ for per-node diagnosis is *not* recommended because it is more susceptible to noise due to the probabilistic nature of the measurement outcomes.

A. Batch Health Check

We extend the baseline verification step with a two-gate batch test that separates (i) *leakage* from (ii) *in-support drift* across allowed patterns. A batch is accepted only if both gates pass; per-node diagnosis is still run regardless of acceptance.

1) Leakage Gate: Let $\widehat{q}_{\text{leak}}$ be the fraction of indices in $\mathcal{S}$ whose joint outcome lies outside $\mathcal{A}$. We reject when the one-sided Wilson upper bound exceeds the tolerance:

$$U(\widehat{q}_{\text{leak}}, |\mathcal{S}|) > \tau_{\text{leak}}.$$

2) In-Support Fidelity Gate: If leakage passes, we condition on $\mathcal{A}$. Let $N_{\mathcal{S}}(\omega)$ count outcome $\omega \in \mathcal{A}$ in $\mathcal{S}$ and define $\tilde{p}_{\mathcal{S}}(\omega) = N_{\mathcal{S}}(\omega) \big/ \sum_{\omega'\in\mathcal{A}} N_{\mathcal{S}}(\omega')$. We compare $\tilde{p}_{\mathcal{S}}$ to the ideal distribution p_{id} (two deterministic patterns at $1/3$ each; $2(n-1)$ probabilistic patterns at $1/(6(n-1))$ each) using

$$F_{\text{c}}(\mathcal{S}) = \Big(\sum_{\omega\in\mathcal{A}} \sqrt{\tilde{p}_{\mathcal{S}}(\omega)\, p_{\text{id}}(\omega)}\Big)^2,$$

and require $F_{\text{c}}(\mathcal{S}) \geq \tau_{\text{fid}}$. Unlike F_{supp}, which is used in the baseline protocol [27], F_{c} is sensitive to *which* Lieutenant becomes an outlier inside the probabilistic branch, which is typical under heterogeneous photonic loss.

B. Per-Node Diagnosis

Per-node diagnosis runs on the deterministic subset $\mathcal{S}_{\text{det}} = \{i \in \mathcal{S} : \mathsf{Commander}_i \in \{00, 11\}\}$, where each Lieutenant's measurement outcome is fixed by the Commander's result.

1) Lieutenant Diagnosis: On $\mathcal{S}_{\text{det}}$ we count outcome-conditional errors for each Lieutenant. With Lieutenants indexed by $\ell \in \{1,\dots,n-1\}$, we form one-sided Wilson bounds $(L_\ell^{(b)}, U_\ell^{(b)})$ for each expected outcome $b \in \{0,1\}$. A Lieutenant is *flagged* as noisy if the lower bound on its worst-case conditional error rate clears a gate:

$$L_\ell^{\text{tot}} \equiv \max\big(L_\ell^{(0)}, L_\ell^{(1)}\big) > \varepsilon_{\text{flag}}.$$

Among flagged Lieutenants we additionally annotate *loss-biased* $(1\!\to\!0)$ if

$$g_\ell \equiv L_\ell^{(1)} - U_\ell^{(0)} > \varepsilon_\Delta.$$

This annotation does not affect batch acceptance; it distinguishes photon loss from false clicks and can guide the appropriate mitigation.

2) Commander Diagnosis: Because the Commander's expected outcome is not directly available from $\mathcal{S}_{\text{det}}$, we instead use indices where Lieutenants are unanimous:

$$\mathcal{S}_{\text{clean}} = \{\, i \in \mathcal{S} : \textsf{Lieutenants}_i \in \{1^{\otimes(n-1)}, 0^{\otimes(n-1)}\}\,\}.$$

For $i \in \mathcal{S}_{\text{clean}}$ we infer the Commander's expected outcome $\hat{b}(i) \in \{00, 11\}$ from unanimity and compare it to the Commander's two measured bits to obtain directional error counts; Wilson bounds and the same flagging and loss-bias rules are then applied. Each node is ultimately labeled *clean* or *flagged (noisy)*, with optional subtype *loss-biased* ($1 \to 0$).

IV. Evaluation

To produce practical, close-to-reality data we use a *fully software simulation* of Perceval by Quandela [29][1] which is an open source python framework for programming photonic quantum computers.

A. Goals and Questions

With our simulations, we validate our contributions by evaluating the following two questions:

Batch Health Check (C1): Compared with the baseline QDBA protocol [27] which only verifies the entanglement quality via F_{supp}, does adding a leakage check reduce false accepts under heterogeneous loss, while preserving the acceptance of clean batches?

Per-Node Diagnosis (C2): For practical verification budgets $\mathcal{S}$, do one-sided Wilson intervals separate noisy participants from clean ones? We examine this in two scenarios: one where a noisy Lieutenant introduces errors, and one where the Commander itself is the noisy party.

While we also claim that our noise diagnosis is lightweight and easy to implement, we do not benchmark runtime on hardware in this paper; instead, we provide an analytical overhead accounting in Section IV-D.

B. Simulation Setup

1) Roles: We simulate $n = 6$ generals (one Commander, five Lieutenants) and distribute k preparations of $|\Psi_n\rangle$ per round. The verification set $\mathcal{S}$ is a fixed fraction of the total, $|\mathcal{S}| = k/4$. This split yields tighter one-sided Wilson bounds, while keeping 75% of preparations available for execution; increasing $|\mathcal{S}|$ narrows confidence intervals.

2) Noise Model: Since our verification data consist of Z-basis bitstrings, we model the detection and readout process at each node as an asymmetric binary channel. For a node x with ideal bit b and observed bit y:

$$\Pr[y = 0 \mid b = 1] = p_x^{1\to 0}, \qquad \Pr[y = 1 \mid b = 0] = p_x^{0\to 1}.$$

In photonics, $p_x^{1\to 0}$ captures loss/inefficiency (dominant) and $p_x^{0\to 1}$ captures false clicks. In our notation, p_{C} and p_{L} parameterize the dominant $1 \to 0$ component for Commander-side and Lieutenant-side measurements, respectively. The Commander is typically co-located with the entanglement source or a well-calibrated central station (shorter paths, fewer connectors), whereas Lieutenants traverse additional fiber and components that introduce insertion loss and efficiency mismatch. Accordingly, we set $p_{\text{C}} = 0.01$ and $p_{\text{L}} = 0.03$ ($p_{\text{C}} < p_{\text{L}}$), unless stated otherwise. Symmetric classical flips are disabled ($q_{\text{class}} = 0$), and rare $0 \to 1$ events are modeled via dark counts in the photonic backend.

We do not model arbitrary qubit-level depolarizing or phase-flip channels in the diagnosis layer; those effects are represented through their impact on the observed outcome distribution induced by the photonic backend.

3) Decision Thresholds: Batch acceptance requires *both* a leakage gate and a fidelity floor to pass:

$$U(\widehat{q}_{\text{leak}}, |\mathcal{S}|) \leq \tau_{\text{leak}} \quad \text{and} \quad F_{\text{c}}(\mathcal{S}) \geq \tau_{\text{fid}}.$$

For our simulations, we use $\tau_{\text{leak}} = 0.135$ and $\tau_{\text{fid}} = 0.89$. Per-Lieutenant diagnosis uses the same one-sided Wilson bounds computed on $\mathcal{S}_{\text{det}}$. Wilson bounds use $\alpha = 0.05$. Nodes get flagged as noisy when $\varepsilon_{\text{flag}} = 0.05$:

$$L_\ell^{\text{tot}} \equiv \max\left(L_\ell^{(0)}, L_\ell^{(1)}\right) > \varepsilon_{\text{flag}} \Rightarrow \text{flagged},$$

and noisy nodes get additionally flagged as *loss-biased* ($1 \to 0$) when

$$g_\ell \equiv L_\ell^{(1)} - U_\ell^{(0)} > \varepsilon_\Delta, \qquad \varepsilon_\Delta = 0.005.$$

4) Threshold Calibration for Deployment: The numerical thresholds above are fixed for this study; for deployment they should be calibrated from clean reference batches. Choose a target per-gate clean-batch false-reject rate β and collect B clean batches. Set τ_{leak} to the $(1-\beta)$-quantile of $U(\widehat{q}_{\text{leak}}, |\mathcal{S}|)$ over clean batches, and set τ_{fid} to the β-quantile of $F_{\text{c}}(\mathcal{S})$ over clean batches. For per-node labeling, set $\varepsilon_{\text{flag}}$ from an acceptable maintenance-trigger rate (or equivalently from a clean quantile of $\max(L_x^{(0)}, L_x^{(1)})$), and set ε_Δ to the minimum bias gap that warrants different operational interventions. To control family-wise false flags across directional tests, one can use a Bonferroni split $\alpha_{\text{dir}} = \alpha_{\text{FW}}/(2n)$.

5) Photonic Backend: Simulations use the fully software Perceval photonic stack to model source and interferometer effects that primarily distort in-support frequencies. Detector dark counts are modeled by a per-detector rate $d_{\text{cr}} = 10\,\text{Hz}$ and a $1\,\text{ns}$ coincidence window; the accidental-click probability per window is $\approx d_{\text{cr}} \times 1\text{ ns} = 10^{-8}$ and appears as rare out-of-support (leakage) events. Source and interferometer imperfections follow Perceval's built-ins:

$$\left(g^{(2)}(0),\ \texttt{indist},\ \phi_{\text{err}},\ \phi_{\text{imp}}\right) = (0.01,\ 0.92,\ 0.01,\ 0.02),$$

where $g^{(2)}(0)$ proxies multi-photon contamination (lower is better), `indist` is photon indistinguishability (drives interference visibility), and $(\phi_{\text{err}}, \phi_{\text{imp}})$ capture random jitter and static phase offsets in the interferometer. These parameters are distinct from $(p_{\text{C}}, p_{\text{L}})$: they model backend interference quality and phase stability rather than node-local readout

[1] Code: https://github.com/your-user/your-repo.

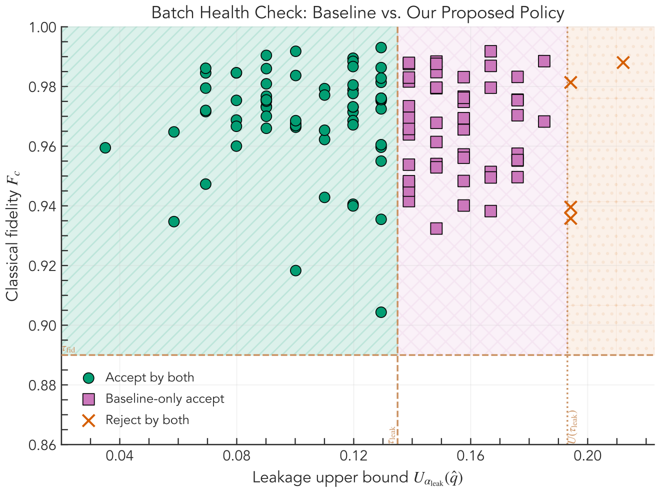

Fig. 1. Batch Health Check (C1). 120 batches populate the policy plane $\big(U(\widehat{q}_{\text{leak}},|\mathcal{S}|),F_{\text{c}}(\mathcal{S})\big)$. Dashed lines mark our gates $\big(U(\widehat{q}_{\text{leak}},|\mathcal{S}|)\le\tau_{\text{leak}},\ F_{\text{c}}(\mathcal{S})\ge 0.89\big)$, and the dotted vertical line marks the baseline support-only boundary $U(\tau_{\text{leak}},|\mathcal{S}|)$. In this run, ● are accepted by both policies (65 batches); ■ are accepted only by the baseline protocol (51 batches); × are rejected by both policies (4 batches).

asymmetry. The global scaling factor is set to 1.0 (all noise channels enabled at nominal strength).

C. Metrics

To answer the C1 question, we compare the baseline QDBA protocol [27] with our proposed batch health check: (i) *Support-only*, the baseline protocol's rule that accepts when the support-compliance rate F_{supp} clears $1-\tau_{\text{leak}}$ (equivalently $\widehat{q}_{\text{leak}}\le\tau_{\text{leak}}$); (ii) *Leakage-check*, our batch health check that additionally requires $U\big(\widehat{q}_{\text{leak}},|\mathcal{S}|\big)\le\tau_{\text{leak}}$ and $F_{\text{c}}(\mathcal{S})\ge\tau_{\text{fid}}$. In total we simulate 120 batches: 100 heterogeneous-noisy stress batches and 20 clean reference batches. We have three categories of batches: (i) *Both-accept*, accepted by both policies (baseline [27] and our proposed policy); (ii) *Baseline-only*, accepted only by the baseline protocol [27]; (iii) *Both-reject*, rejected by both policies. This is depicted in Figure 1.

For question C2, Figure 2 shows the per-Lieutenant flag rate by sweeping the verification size $|\mathcal{S}|$ and the Lieutenant's noise rate p_{L} (4%, 6%, and 8%). We set the flag gate to $\varepsilon_{\text{flag}}=0.05$; under this threshold, 6% and 8% are above-threshold noisy cases, while 4% is a near-threshold reference. Every data entry is the average of 100 trials. The detection rises sharply with increasing verification size. Also noisier Lieutenants are easier to detect even with smaller verification size.

For the Commander per-node diagnosis, we do a similar simulation depicted in Figure 3. We set the flag gate to $\varepsilon_{\text{flag}}=0.05$ and every data entry is the average of 100 trials. For the noise rate we set the Commander noise rate to 4%, 6%, and 8% for our simulation. We use the same verification-sizes as in the Lieutenant simulation. Similar as in the Lieutenant simulation, the detection rises sharply with increasing verification size. We do *not* simulate the loss-bias label.

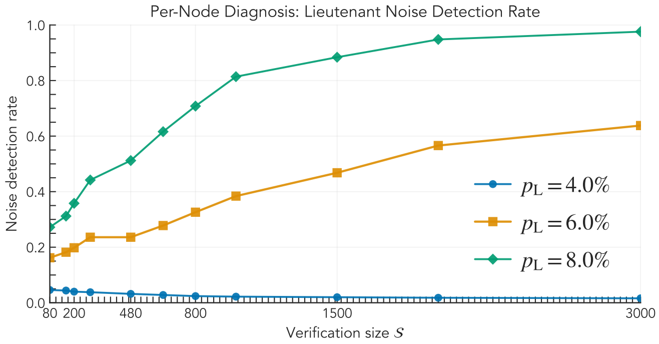

Fig. 2. Per-Node Diagnosis (C2): Per-Lieutenant flag rate as a function of verification budget $\mathcal{S}$ and physical loss p_{L} (simulated at 4%, 6%, and 8%). Flag threshold is $\varepsilon_{\text{flag}}=0.05$. Curves average 100 trials; markers show means, lines join neighbouring budgets.

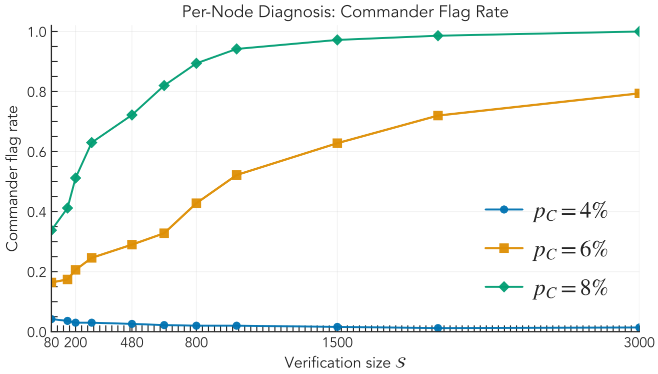

Fig. 3. Per-Node Diagnosis (C2): Per-Commander flag rate as a function of verification budget $\mathcal{S}$ and physical loss p_{C} (simulated at 4%, 6%, and 8%). Flag threshold is $\varepsilon_{\text{flag}}=0.05$. Curves average 100 trials; markers show means, lines join neighbouring budgets.

D. Overhead Accounting

Our proposed modifications add no extra quantum rounds. For a batch, leakage and histogram tallying over $\mathcal{S}$ is $O(|\mathcal{S}|)$, and computing F_{c} is $O(|\mathcal{A}|)$ with $|\mathcal{A}|=2n$ for $|\Psi_n\rangle$. Per-node analysis over $\mathcal{S}_{\text{det}}$ costs $O(n|\mathcal{S}_{\text{det}}|)$ for directional error counting plus $O(n)$ Wilson evaluations. Classical communication changes little versus the baseline protocol [27]: parties already exchange verification outcomes, and our method primarily adds local post-processing.

V. Discussion and Future Work

Our simulations show that adding *protocol-layer diagnosis* to the entanglement verification step can improve robustness of photonic QDBA under heterogeneous noise without additional quantum rounds. A leakage gate plus an in-support fidelity floor rejects noisy entanglement batches that a support-only check would accept (Figure 1), while per-node diagnostics can separate clean from noisy participants (Figures 2 and 3). All results use a fully software-based PERCEVAL stack; hardware validation is needed to further test these assumptions.

Beyond the reported experiments, a potentially useful direction is to broaden simulations in scale, noise, and protocol variants. Current experiments inject only one noisy party; with multiple noisy parties we expect concurrent flags when enough samples remain, but detection power decreases as leakage and Commander noise increase. Adversarial behavior (e.g., classically simulating outcomes) is outside this paper's formal analysis and is addressed by trap rounds and commit-and-reveal. Our diagnosis is orthogonal to the calibration of devices and can serve as adjustment signals for hardware maintenance. Finally, our approach makes diagnosis sensitive to Commander noise; when the Commander drifts, the diagnosis degrades. Quantifying and reducing this sensitivity is a future target. Overall, we provide a minimal drop-in batch and per-node diagnosis layer.

Acknowledgment

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203, and by the European Commission through the Horizon Europe research and innovation programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement ID: 101114043).

References

[1] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[2] D. Dolev and H. R. Strong, "Authenticated algorithms for Byzantine agreement," *SIAM Journal on Computing*, vol. 12, no. 4, pp. 656–666, 1983.

[3] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of Distributed Consensus with One Faulty Process," *Journal of the ACM*, vol. 32, no. 2, pp. 374–382, 1985.

[4] M. Fitzi, N. Gisin, and U. Maurer, "Quantum Solution to the Byzantine Agreement Problem," *Physical Review Letters*, vol. 87, no. 21, p. 217901, 2001.

[5] M. Fitzi, D. Gottesman, M. Hirt, T. Holenstein, and A. D. Smith, "Detectable Byzantine Agreement Secure Against Faulty Majorities," in *Proceedings of the twenty-first annual symposium on Principles of distributed computing*, 2002, pp. 118–126.

[6] S. Gaertner, M. Bourennane, C. Kurtsiefer, A. Cabello, and H. Weinfurter, "Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection," *Physical Review Letters*, vol. 100, no. 7, p. 070504, 2008.

[7] Z. Guba, I. Finta, Á. Budai, L. Farkas, Z. Zimborás, and A. Pályi, "Resource Analysis for Quantum-Aided Byzantine Agreement with the Four-Qubit Singlet State," *Quantum*, vol. 8, p. 1324, 2024.

[8] G. Tóth and O. Gühne, "Detecting Genuine Multipartite Entanglement with Two Local Measurements," *Physical Review Letters*, vol. 94, no. 6, p. 060501, 2005.

[9] N. D. Mermin, "Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct States," *Phys. Rev. Lett.*, vol. 65, no. 15, pp. 1838–1840, 1990.

[10] S. Wehner, D. Elkouss, and R. Hanson, "Quantum Internet: A Vision for the Road Ahead," *Science*, vol. 362, no. 6412, p. eaam9288, 2018.

[11] N. H. Nickerson, Y. Li, and S. C. Benjamin, "Topological Quantum Computing with a Very Noisy Network and Local Error Rates Approaching One Percent," *Nature Communications*, vol. 4, no. 1, p. 1756, 2013.

[12] C. Monroe, R. Raussendorf, A. Ruthven, K. R. Brown, P. Maunz, L.-M. Duan, and J. Kim, "Large-Scale Modular Quantum-Computer Architecture with Atomic Memory and Photonic Interconnects," *Physical Review A*, vol. 89, no. 2, p. 022317, 2014.

[13] H. J. Kimble, "The Quantum Internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[14] S. Slussarenko and G. J. Pryde, "Photonic Quantum Information Processing: A Concise Review," *Applied Physics Reviews*, vol. 6, no. 4, p. 041303, 2019.

[15] V. Makarov, A. Anisimov, and J. Skaar, "Effects of Detector Efficiency Mismatch on Security of Quantum Cryptosystems," *Physical Review A*, vol. 74, no. 2, p. 022313, 2006.

[16] Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, "Quantum Hacking: Experimental Demonstration of Time-Shift Attack Against Practical QKD Systems," *Physical Review A*, vol. 78, no. 4, p. 042333, 2008.

[17] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination," *Nature Photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[18] E. Magesan, J. M. Gambetta, and J. Emerson, "Scalable and Robust Randomized Benchmarking of Quantum Processes," *Physical Review Letters*, vol. 106, no. 18, p. 180504, 2011.

[19] Z. Cai, S. C. Benjamin *et al.*, "Quantum Error Mitigation," *Reviews of Modern Physics*, vol. 95, no. 4, p. 045005, 2023.

[20] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels," *Physical Review Letters*, vol. 76, no. 5, pp. 722–725, 1996.

[21] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels," *Physical Review Letters*, vol. 77, no. 13, pp. 2818–2821, 1996.

[22] W. Dür and H. J. Briegel, "Entanglement Purification and Quantum Error Correction," *arXiv preprint arXiv:0705.4165*, 2007.

[23] E. B. Wilson, "Probable Inference, the Law of Succession, and Statistical Inference," *Journal of the American Statistical Association*, vol. 22, no. 158, pp. 209–212, 1927.

[24] A. Cabello, "Solving the Liar Detection Problem using the Four-Qubit Singlet State," *Physical Review A*, vol. 68, no. 1, p. 012304, 2003.

[25] Z. Qu, Z. Zhang, and B. Liu, "Quantum Detectable Byzantine Agreement for Distributed Data Trust Management in Blockchain," *Information Sciences*, vol. 637, p. 118858, 2023.

[26] T. Andronikos and A. Sirokofskich, "A Quantum Detectable Byzantine Agreement Protocol Using Only EPR Pairs," *Applied Sciences*, vol. 13, no. 14, p. 8405, 2023.

[27] K.-C. Chen, M. Prest, F. Burt, S. Yu, and K. K. Leung, "Noise-Aware Detectable Byzantine Agreement for Consensus-based Distributed Quantum Computing," in *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*. IEEE, 2025, pp. 210–215.

[28] G. Bracha, "Asynchronous Byzantine Agreement Protocols," *Information and Computation*, vol. 75, no. 2, pp. 130–143, 1987.

[29] N. Heurtel, A. Fyrillas, G. d. Gliniasty, R. Le Bihan, S. Malherbe, M. Pailhas, E. Bertasi, B. Bourdoncle, P.-E. Emeriau, R. Mezher, L. Music, N. Belabas, B. Valiron, P. Senellart, S. Mansfield, and J. Senellart, "Perceval: A Software Platform for Discrete Variable Photonic Quantum Computing," *Quantum*, vol. 7, p. 931, Feb. 2023. [Online]. Available: https://doi.org/10.22331/q-2023-02-21-931