Quantum Decoy Signature Protocol

[*WHITEPAPER : 0007*]

[Date : 30-09-2025]

Quantum Decoy Signature Protocol

*B M Darshan Kumar, Quantum Research Lead, Aion-IA,
Electronic City, Bangalore 560100
*M Suraj, QML Engineer Aion-IA, Electornic City, Bangalore 560100

QDSP introduces dynamically evolving, decoy-enhanced quantum signatures that make replay and forgery infeasible by binding authenticity checks to live quantum states and decoy statistics, not static classical tokens [1][2][3]. The protocol integrates decoy-state testing, entanglement-assisted verification, and per-transaction signature updates to detect interception and invalidate transcript reuse, while remaining interoperable with quantum networks and classical ledgers [4][5][6].

Introduction

Digital signatures underpin integrity, authenticity, and non-repudiation in modern systems, yet traditional schemes face quantum threats as large-scale quantum computers can undermine number-theoretic assumptions [7]. Quantum digital signatures (QDS) and decoy-state methods provide information-theoretic security mechanisms by exploiting quantum no-cloning, measurement disturbance, and statistical detection of eavesdropping [1][3]. QDSP builds on these foundations by embedding decoy states into quantum signatures and enforcing dynamic state evolution after each verification to eliminate replay vectors and amplify tamper detection [2][4].

Static or long-lived signature artifacts can be intercepted or replayed; QDSP instead encodes signatures in quantum states that are single-use and measurement-sensitive, with decoy pulses that reveal photon-number splitting or other channel attacks via mismatched yields and error statistics [3][8]. Recent demonstrations of quantum signature networks and asynchronous QDS over practical channels suggest feasibility for distributed deployments, forming a basis for QDSP integration into existing infrastructures [5][4].

Background

Decoy-state techniques were introduced to harden coherent-pulse systems against multiphoton attacks such as photon-number splitting by randomly interleaving signal, decoy, and vacuum states and checking yield and error-rate consistency post hoc [3]. Practical engineering guidance shows how decoys are selected with distinct mean photon numbers yet remain indistinguishable to adversaries during transmission, enabling statistical detection of eavesdropping without revealing decoy positions in flight [8]. Quantum digital signatures extend these concepts to integrity and non-repudiation, with proof-of-principle systems demonstrating passive decoy-state QDS over long distances and with improved signature efficiency [1][5].

Replay resistance in quantum-secure systems is often achieved with nonces or one-time transformations; QDSP achieves this natively by evolving quantum signature states after each verification, ensuring that captured transcripts cannot satisfy future verification tests [6][9]. Surveys and recent protocols show QDS variants using QKD-like distribution and verification processes, indicating a maturing toolbox of decoy checks, measurement-device-independence, and asynchronous operation that QDSP leverages for robust, dynamic authentication [4][10].

Problem Statement

Static signatures, even if post-quantum secure, can be recorded and replayed across channels or sessions if freshness is not cryptographically and physically enforced [11]. In photonic quantum channels using weak coherent states, multiphoton emissions enable attacks such as photon-number splitting unless decoy-state countermeasures are applied to validate channel behavior statistically [3]. Without dynamic evolution, a valid quantum signature observed once could enable later impersonation attempts if verification ignores the one-shot nature of the state or lacks decoy-driven tamper evidence [2].

Large-scale, distributed environments demand authentication that can withstand measurement-device imperfections, timing asynchrony, and unknown channel variations, which can otherwise inflate false accept or false reject probabilities [4]. QDSP addresses these gaps by combining decoy-state integrity checks, entanglement-assisted verification hooks,

and per-transaction signature updates to cryptophysically bind acceptance to live, uncompromised quantum interactions [1][5].

QDSP Core Concept

QDSP encodes signatures in quantum states that include randomly positioned decoy qubits (or decoy pulses) whose yields and error statistics serve as a tamper-evidence mechanism for the associated signature qubits [3]. Verification nodes measure both signature and decoy components, rejecting any attempt where decoy statistics deviate from calibrated expectations consistent with secure channels and honest behavior [2]. After each successful verification, the signature state space is rotated or re-prepared, rendering prior transcripts statistically incompatible with future verifications and inherently preventing replay [1].

- Decoy-enhanced signatures: Interleave signal and decoy elements so that eavesdropping or splitting attacks perturb observed yields in a detectable manner, without revealing decoy positions during transmission [8].
- Dynamic evolution: Enforce per-transaction state updates so each signature is one-shot and cannot be reused, echoing the one-shot signature principle in a quantum-native fashion [9].
- Entanglement hooks: Optional entanglement between signer states and verification nodes enables correlation checks that further raise the bar for undetected tampering [4].

Architecture

QDSP comprises a Quantum Signature Generator, a Verification Node, and a Dynamic Update Module organized around secure quantum channels and an auditable classical control plane [1]. The Signature Generator prepares a composite sequence of signal and decoy qubits (or pulses) with secret positioning and calibrated intensities or states, ensuring indistinguishability to adversaries in flight [8]. The Verification Node measures according to configured bases and thresholds, evaluating decoy yields and signature correlations, and only accepts if all checks fall within composable security bounds [2].

The Dynamic Update Module triggers immediate evolution of the signature state space—via basis rotation schedules, new decoy distributions, or re-prepared states—after each verification, thus invalidating stale transcripts by design [9]. For operational assurance, the system logs verification results and metadata into a tamper-resistant ledger or quantum-secure network layer that supports audit without exposing decoy placements or raw quantum outcomes [5].

Protocol Design

Step 1 — Initialization: The Signature Generator calibrates channel parameters and selects decoy configurations, including mean photon numbers for signal, decoy, and vacuum pulses if using weak coherent states, or equivalent state ensembles for single-photon sources [3]. Practical models prescribe occurrence percentages and indistinguishability criteria for decoys, ensuring that adversaries cannot identify them prior to public sifting [8]. Optional entanglement resources are provisioned between signer and verifier to enable correlation-based verification where supported [4].

Step 2 — Transmission: The composite sequence containing signature and decoy states is sent over high-fidelity quantum channels, with classical metadata withheld until measurement completion to prevent targeted manipulation of identified decoys [1]. Channel conditions may be stabilized by standard optical engineering and memory-assisted designs to preserve state integrity over distance and time alignment [12]. Any required classical side-channel communications are authenticated using quantum-safe means to avoid undermining the quantum layer [7].

Step 3 — Verification: The Verification Node measures received states, then participates in a sifting and parameter estimation phase where decoy positions and settings are revealed to assess yields and error rates against expected profiles [2]. Acceptance requires that decoy statistics match calibrated thresholds and that the signature portion satisfies integrity checks defined by the protocol’s correlation or content-binding tests, analogous to QDS correctness criteria [1]. Asynchronous operation is possible by aligning with QDS frameworks that decouple strict timing from correctness, improving practicality in networks [4].

Step 4 — Dynamic Update: Upon acceptance, the Dynamic Update Module rotates or re-prepares the signature state, altering basis choices, decoy distributions, and internal keys so that the next transaction uses a fresh quantum signature instance that is statistically unrelated to prior transcripts [9]. If verification fails or anomalies are detected, the system initiates re-preparation with stricter thresholds or invokes mitigation such as altering intensities or routes to counter suspected attacks [3]. This ensures replayed captures cannot satisfy future acceptance tests due to mismatch with updated decoy and basis patterns [8].

Step 5 — Record & Audit: Outcomes, thresholds, and high-level proofs-of-verification are recorded in a tamper-resistant ledger or quantum-secure network layer, enabling auditability without leaking decoy placements or raw quantum states [5]. This record can be cross-verified against expected decoy statistics and entanglement-correlation evidence, providing a compliance-friendly trail that preserves operational secrecy [1]. Integration with broader security domains allows policy enforcement and incident response tied directly to quantum-layer evidence [6].

Security Analysis

Resistance to quantum interception arises from the decoy-state method's ability to detect photon-number splitting and related attacks, as adversarial interactions unavoidably skew yields and error rates across signal and decoy ensembles [3]. Formal analyses show decoy-state security against arbitrary attacks in coherent-state systems and provide calibration techniques for practical parameter estimation and threshold setting [2]. Passive decoy-state QDS demonstrations confirm feasibility and robustness in experimental conditions, supporting QDSP's reliance on decoy statistics for tamper evidence [1].

Replay attacks are neutralized by the dynamic update after each verification; captured classical transcripts or partial quantum observations cannot regenerate a valid future signature because acceptance depends on fresh decoy placement and state parameters unknown in advance [8]. Integrations with QDS that support asynchronous and measurement-device-independent styles mitigate side-channel risks and device imperfections that could otherwise be exploited to forge or bias outcomes [4]. Ledger-based auditing and

network-scale deployments demonstrate that quantum signatures can deliver integrity and non-repudiation at commercial scales with strong evidence trails [5].

Threat Model

QDSP assumes adversaries capable of intercept-resend strategies, photon-number splitting, beam-splitting on multiphoton pulses, and adaptive attacks exploiting detector or channel imperfections [3]. Decoy-state verification detects deviations in yields and error rates consistent with such attacks, and thresholds can be tuned using formal security analyses to minimize false accept probability under realistic noise [2]. Adversarial timing and asynchrony are addressed by protocols supporting asynchronous QDS, ensuring that temporal desynchronization does not open acceptance loopholes [4].

Classical control-plane attacks, including replay or transcript substitution, are countered by the quantum-layer's one-shot nature and by classical authentication hardened with post-quantum signatures for metadata exchange and logging [7]. Systematic side-channel risks from implementation flaws are mitigated by adopting modeling and V&V practices for decoy-state systems that enforce indistinguishability and proper occurrence distributions in real hardware [8].

Implementation Considerations

Hardware: Implementations can use weak coherent sources with carefully managed intensities for signal, decoy, and vacuum pulses, or heralded single-photon sources enhanced by quantum memories to stabilize timing and reduce multiphoton events [12]. Detector efficiencies, dark count rates, and basis-alignment tolerances must be characterized to set decoy thresholds that are tight yet feasible under operational conditions [8]. For extended distances, optical engineering and memory-assisted techniques can preserve usable statistics for verification without undermining indistinguishability [12].

Integration: QDSP interoperates with existing QDS/QKD infrastructures, reusing secure channels and post-processing stacks for sifting, parameter estimation, and error analysis [1]. Networked deployments can tie verification outcomes to ledger-based proofs and orchestrate

policy using a quantum-secure network layer demonstrated in recent large-scale experiments [5]. Classical metadata, including sifting and audit records, should be protected with NIST-tracked post-quantum signature schemes to avoid weakening the trust chain [7].

Performance and Scalability

Passive and decoy-state QDS experiments report long-distance operation and multi-bit signing within seconds, demonstrating that decoy-enhanced signatures can be practical over metropolitan-scale links with proper calibration [1]. Network-scale deployments show major efficiency improvements by optimizing distribution and verification workflows, indicating that QDSP can sustain high throughput when combined with modern quantum networking techniques [5]. Asynchronous QDS models reduce sensitivity to strict timing alignment, which eases scaling across heterogeneous network paths and devices [4].

Performance trade-offs include selecting decoy intensities and occurrence rates that maximize detection power without excessive overhead, and balancing signature length against verification latency for targeted security levels [8]. Memory-assisted and MDI-inspired approaches can mitigate device-side vulnerabilities and improve tolerance to loss, supporting broader topologies and multi-user authentication at scale [12].

Use Cases

Secure Financial Transactions: QDSP prevents tampering and replay in payment flows by requiring live decoy-consistent signatures per transaction, adding quantum-layer freshness beyond classical one-time tokens [1]. Ledger-backed audit trails deliver non-repudiation with quantum evidence, increasing assurance for high-value transfers and interbank operations [5]. Asynchronous modes support diverse transaction latencies without sacrificing detection [4].

Digital Identity Verification: Sensitive access can be bound to one-shot quantum signatures whose validity hinges on decoy and correlation checks, eliminating reuse or duplication of credential artifacts [3]. Post-quantum hardening of the classical control plane complements the quantum layer, producing end-to-end resilience against quantum and

classical adversaries [7]. The dynamic update ensures that even successful observations cannot be replayed in subsequent sessions [8].

Critical Infrastructure Control: Control commands and telemetry can be authenticated with live QDSP signatures, where channel attacks or device compromise manifest as statistical anomalies in decoy yields or signature correlations [2]. Network-scale quantum signature frameworks indicate feasibility for integrating QDSP into operational grids and industrial networks with centralized auditing [5]. Memory-assisted and MDI variants can address hardware constraints and untrusted nodes in distributed control environments [12].

Interoperability and Standards

QDSP's decoy and verification parameters align with established decoy-state methodologies, facilitating reuse of well-studied occurrence distributions, mean photon numbers, and estimation techniques [3]. System-level modeling practices for decoy-state implementations provide templates for verification and validation, enabling predictable deployments and compliance testing [8]. For classical interop, NIST PQC processes guide selection of digital signature algorithms for securing control-plane exchanges and logs [7].

Integration with asynchronous and MDI QDS standards can improve device-agnostic security and ease multi-vendor interoperability across quantum networks [4]. Network-layer frameworks that demonstrated scalable quantum signatures suggest profiles for audit data, privacy-preserving proofs, and operational metrics that QDSP can adopt for consistent end-to-end assurance [5].

Limitations and Open Problems

Weak coherent sources are vulnerable to multiphoton events, requiring careful decoy calibration; aggressive thresholds may increase false rejects under fluctuating channel noise [3]. Implementation non-idealities risk leaking decoy information or biasing statistics, underscoring the need for rigorous modeling, indistinguishability enforcement, and continuous V&V [8]. Achieving device-independent guarantees remains challenging; asynchronous and MDI styles help but may add complexity and lower raw rates [4].

Dynamic update policies must be cryptographically and operationally sound; misconfiguration could allow partial transcript usefulness or degrade availability if updates are too frequent or too weak [9]. Scaling to high-density networks hinges on memory-assisted distribution, robust timing, and standardized audit semantics to avoid fragmentation and maintain composable security margins [12]. Further work is needed to quantify optimal decoy schedules and per-transaction state rotations for varied topologies and threat environments [2].

Future Work

Adaptive decoy placement driven by quantum-aware machine learning can optimize detection power versus overhead by learning channel behaviors and adversarial signatures in real time [13]. Integration with multi-channel schemes like entanglement-assisted verification can raise detection sensitivity and throughput by leveraging diversified state resources and routing [4]. Large-scale simulations and field trials should evaluate end-to-end performance, update cadences, and audit aggregation in metro and WAN settings [5].

Exploration of one-shot signature paradigms in tandem with QDSP may yield hybrid constructions where classical one-shot controls complement quantum one-shot state evolution for layered replay resistance [9]. Memory-assisted and MDI-QKD advances can directly inform QDSP transport and verification layers, enhancing resilience against device-side vulnerabilities and asynchronous operation constraints [12]. Formal composable proofs tailored to QDSP's decoy and dynamic-update semantics will be essential for certification and standardization [2].

Conclusion

QDSP secures authentication with dynamically evolving, decoy-enhanced quantum signatures that expose interception and render replay infeasible, delivering information-theoretic assurances beyond classical schemes [3]. By uniting decoy-state verification, optional entanglement-assisted checks, and one-shot state evolution, QDSP provides practical, scalable authentication for financial, identity, and critical infrastructure scenarios over real networks [1]. With advancing asynchronous, memory-assisted, and network-scale QDS frameworks, QDSP offers a

deployable foundation for quantum-secure authentication and auditable assurance at scale [4][5][12].

References

[1] Proof-of-Principle Demonstration of Passive Decoy-State ...
https://link.aps.org/doi/10.1103/PhysRevApplied.10.034033
[2] Security of the decoy state method for quantum key ...
https://arxiv.org/abs/2101.10128
[3] Decoy State Quantum Key Distribution | Phys. Rev. Lett.
https://link.aps.org/doi/10.1103/PhysRevLett.94.230504
[4] Asynchronous measurement-device-independent quantum ...
https://link.aps.org/doi/10.1103/PhysRevA.110.012609
[5] Experimental quantum secure network with digital signatures ...
https://academic.oup.com/nsr/article/10/4/nwac228/6769862
[6] Experimental authentication of quantum key distribution ...
https://www.nature.com/articles/s41534-021-00400-7
[7] PQC Digital Signature Second Round Announcement | CSRC
https://csrc.nist.gov/news/2024/pqc-digital-signature-second-round-announcement
[8] Implementing the decoy state protocol in a practically ...
https://journals.sagepub.com/doi/10.1177/1548512917698053
[9] One-Shot Signatures: A New Paradigm in Quantum ...
https://www.btq.com/blog/one-shot-signatures-new-paradigm-in-quantum-cryptography
[10] A research on quantum digital signatures
https://www.ewadirect.com/proceedings/ace/article/view/4563
[11] Securing the future internet of things with post-quantum ...
http://buyya.com/papers/SecuringIoT2022.pdf
[12] Practical Decoy-State Memory-Assisted Measurement-Device ...
https://link.aps.org/doi/10.1103/PhysRevApplied.20.024029
[13] A improved group quantum key distribution protocol with ...
https://www.nature.com/articles/s41598-024-84244-z
[14] Quantum digital signature based on single-qubit without a ...
https://arxiv.org/html/2410.13397v2
[15] Boosting quantum key distribution via the end-to- ...
https://arxiv.org/pdf/2109.05575.pdf
[16] Implementation of decoy state QKD https://xqp.physik.uni-muenchen.de/publications/files/theses_master/master_auer.pdf

[17] Chip-integrated quantum signature network over 200 km
https://www.nature.com/articles/s41377-025-01775-4
[18] Quantum-Key Distribution using Decoy Pulses to Combat ...
https://inspirehep.net/literature/2874237