JOURNAL OF GENERATIVE AI IN PUBLIC SECTOR

VOLUME 1 | ISSUE 1 | AUGUST 2025

ISSN 2995-6366

Location: ASHBURN, VA, United States of America

Table of Contents

Launch Editorial

Dr. Al Naqvi, Editor-in-Chief

Welcome to the inaugural issue of the *Journal of Generative AI in the Public Sector*. We find ourselves at a historic inflection point – an era defined not only by the rapid rise of artificial intelligence, but also by an overwhelming surge of narratives, claims, and hype surrounding it. The line between substance and spectacle has blurred, and for many in the public sector, this creates a cognitive battlefield where clarity is scarce and strategic direction is elusive. Ironically, AI itself contributes to this ambiguity: generative models amplify noise, simulate expertise, and can inadvertently distort decision-making environments they were designed to enhance.

Public institutions, caught in the crossfire, are under immense pressure. On one side, the imperatives of governance and ethics demand caution, restraint, and oversight. On the other, there is a relentless push for aggressive adoption – often framed in existential terms: adopt or perish. This duality places government agencies in a paradoxical bind, forced to embrace a technology they are simultaneously warned to regulate. In this context, thoughtful scholarship and domain-specific inquiry are not luxuries – they are necessities. This journal aims to provide precisely that: a space for grounded, policy-relevant, technically sophisticated dialogue on the strategic, operational, and ethical implications of generative AI in the public sector.

Amid the accelerating pace of change, public sector missions are being disrupted, and institutional clarity is giving way to confusion. Decision-makers, program managers, and technologists alike are navigating an environment in flux – one where even competitors and adversaries are recalibrating their postures under the same generative AI fervor. Yet within this storm of activity, there remains a striking scarcity of thoughtful, balanced analysis. The discourse is largely dominated at both extremes: on one side, popular narratives celebrating superficial use cases and commercial success stories; on the other, technically dense publications rooted in advanced mathematics and architectural abstraction, inaccessible to most practitioners and policymakers.

ISSN 2995-6366 (Online)

What is urgently needed is a middle path: a journal that is rigorous yet accessible, deeply informed but grounded in practice – a platform that engages technical, strategic, and ethical dimensions of GenAI not as isolated curiosities but as integrated elements of real-world public missions. The *Journal of Generative AI in the Public Sector* was created to fill that void. Our aim is to focus not simply on *how* GenAI works, but on *what it enables*, *where it fits*, and *why it matters* – specifically within the vital context of governance, defense, diplomacy, intelligence, public service, and national resilience.

A recent report from Stanford suggested that as many as 95% of AI projects in the private sector are failing to meet their objectives. While this data point reflects commercial implementations, it should serve as a serious warning for public institutions. Unlike the public sector, private enterprises typically enjoy greater agility in procurement, governance, and internal reconfiguration – making them structurally more capable of rapid course correction. If even the most adaptable organizations are struggling with successful AI adoption, it stands to reason that the public sector, often bound by bureaucratic inertia, compliance frameworks, and mission complexity, faces even steeper odds.

This observation is not meant to discourage AI adoption in government – but rather to sharpen our attention to the *quality* of that adoption. It underscores the necessity for a more thoughtful approach: one that goes beyond checklists, procurement cycles, or vendor promises. The public sector must invest in intellectual readiness, architectural foresight, and adaptive capacity – not just technology acquisition. This journal is intended as a forum to support that deeper work.

About the American Institute of Artificial Intelligence

It is with great pride that we launch this journal under the auspices of the *American Institute of Artificial Intelligence (AIAI)*. Headquartered in the Washington D.C. metropolitan area, AIAI has long stood at the intersection of government and commercial innovation in AI. Founded in 2016 – at a time when the artificial intelligence revolution was still underestimated by many – AIAI anticipated the transformational trajectory that AI would have on institutions, economies, and global strategy.

Since its inception, AIAI has remained dedicated to developing not just solutions, but entire fields of applied AI. From crafting original bodies of

ISSN 2995-6366 (Online)

knowledge to advising governments and Fortune 100 companies, the institute has pioneered frameworks and curricula that treat AI not as a narrow technical skillset but as a multidimensional force reshaping the foundations of policy, public service, and institutional design. The launch of this journal represents a continuation of that mission: to deepen the understanding of generative AI's impact – particularly as it reshapes the public sector landscape.

Mission

The mission of this journal is to equip the public sector with actionable, applied insights into generative AI – insights that go beyond abstract theory or vendor hype, and instead support *responsible, impactful, and mission-aligned adoption*. We seek to create a critical bridge between policy and implementation, grounding every issue in the realities of operational constraints, institutional mandates, and the evolving geopolitical and technological landscape. Through research-based visions and solution-oriented articles, we aim to illuminate how generative AI can serve – not destabilize – public missions.

The Journal of Generative AI in the Public Sector will be published on a quarterly basis, with each issue addressing a distinct constellation of challenges and opportunities. In addition to our regular features, we are proud to include in every issue a dedicated article on quantum technologies – an emerging field that intersects profoundly with the future of AI, encryption, and national security. This recurring inclusion reflects our commitment to horizon scanning and intellectual preparedness in the face of exponential technological change.

We are also proud to introduce a significant shift in the norms of academic publishing – one that reflects the very subject matter this journal engages with. *The Journal of Generative AI in the Public Sector* will accept submissions that are authored with the assistance of large language models (LLMs), provided that the work is supervised, directed, and owned by a human author. In our view, restricting the use of such tools in the name of tradition is no different from forcing people to ride horse-drawn buggies in the age of the automobile. It is not only inefficient – it is unjust to progress.

We recognize that LLMs, when used thoughtfully, can enhance clarity, accelerate writing, and expand productivity without compromising originality. What matters is that the core intellectual contributions – research ideas, argumentation, and sourcing – remain the author's own. Our editorial policy

ISSN 2995-6366 (Online)

does not treat LLM use as a barrier to publication; instead, it reflects the evolving reality of how knowledge is produced. As long as the work is responsible, transparent, and anchored in genuine insight, we welcome it – regardless of whether an LLM played a supporting role in its composition.

Framework

The classification framework adopted by the *Journal of Generative AI in the Public Sector* reflects a deliberate effort to move beyond high-level sectoral generalizations and instead mirror the actual operational architecture of government itself. Rather than organizing content solely by academic discipline or technical domain, we have constructed a taxonomy grounded in agency functions, mission mandates, and institutional responsibilities. This approach ensures that our journal speaks directly to the needs of practitioners, policy leaders, and researchers who operate within the concrete realities of public administration. By aligning GenAI application areas with domains such as tax administration, immigration, transportation, democratic integrity, and urban planning, we acknowledge that AI's public impact will unfold not just in theory, but within the workflows, pressures, and constraints of government agencies. This function-centered structure allows for targeted inquiry, facilitates contribution from domain experts, and ensures coverage of both strategic and day-to-day use cases across the entire public sector spectrum.

Domain	Coverage Focus
1. Policy & Regulation	Governance, accountability, foresight
2. National Security	Defense, intelligence, cybersecurity
3. Foreign Affairs	Diplomacy, multilateralism, data sovereignty
4. Justice & Law	Courts, policing, legal systems
5. Civilian Agency Missions	Citizen services, welfare, emergency management
6. Revenue & Finance	Tax, procurement, fraud, forecasting

ISSN 2995-6366 (Online)

7. Health & Human Services	Epidemiology, clinical NLP, benefits eligibility
8. Education & Workforce	GenAI in curriculum, skilling, digital tutors
9. Environment & Infrastructure	Climate modeling, smart grids, predictive maintenance
10. Transportation & Logistics	Urban mobility, postal ops, fleet optimization
11. Immigration & Borders	Entry systems, refugee systems, global mobility
12. Democracy & Civic Trust	Voting, misinformation, engagement tools
13. Urban Systems & Planning	Housing, zoning, land-use simulation
14. Archives & Culture	Preservation, access, digital restoration
15. Internal Ops & Cross-Agency Enablement	Document automation, knowledge management, workforce agents

Timing

We launch this journal at a time of extraordinary urgency and consequence. The convergence of generative artificial intelligence, public governance, geopolitical realignment, and ethical uncertainty marks a generational inflection point for public institutions worldwide. Unlike prior waves of technological innovation, generative AI does not merely improve how agencies operate – it challenges the very identity, legitimacy, and authority of those institutions. Governments are no longer being asked whether to adopt AI, but rather how fast, how deeply, and at what cost to public trust. The dual challenge of transformation and accountability places public servants in a precarious position: to harness a technology they do not fully control, in service of missions that cannot afford to fail. In this volatile and noisy landscape, the public sector requires more than tools – it needs intellectual infrastructure. It needs forums that are not bound by technical novelty alone, but by a commitment to responsible application, strategic foresight, and institutional resilience. *The Journal of Generative AI in the Public Sector* is created in precisely this spirit – to

ISSN 2995-6366 (Online)

bring clarity, discipline, and direction to one of the most consequential public transformations of our time.

Audience

The *Journal of Generative AI in the Public Sector* is intentionally designed as a transdisciplinary platform, engaging a diverse but interconnected community of readers and contributors. Our core audience includes public sector technologists tasked with implementing AI systems within operational constraints; policy professionals and regulators navigating the boundaries of governance, risk, and innovation; and mission owners and program managers seeking practical frameworks for integrating GenAI into critical services. We also speak directly to the defense and intelligence community, where generative systems increasingly shape threat modeling, strategic planning, and autonomous operations. At the same time, the journal invites engagement from academic researchers, particularly those in applied AI, public administration, and computational policy, as well as ethics and governance specialists focused on responsible AI use in complex institutional environments.

We believe that no single discipline, agency, or perspective can fully capture the implications of generative AI. That is why this journal is structured to bridge practice and theory, policy and engineering, mission execution and strategic design. Whether you're building systems, shaping policy, allocating resources, or asking hard questions about AI's role in society, this journal is for you.

Article Types

To serve the breadth of its audience and fulfill its mission, the *Journal of Generative AI in the Public Sector* welcomes a diverse range of submission types. We invite original research articles that contribute empirical, technical, or theoretical insight into the application of generative AI in public systems. We also encourage conceptual essays that reflect on the evolving relationship between GenAI, institutions, and governance. Recognizing the value of experiential knowledge, we seek case studies detailing agency-level implementations, failures, pilot programs, and lessons learned from the field – both domestic and international. To capture the lived expertise of practitioners, the journal also features interviews with AI leaders across government, defense, and policy sectors.

ISSN 2995-6366 (Online)

In addition, the journal provides space for visual models, architectural schematics, and policy frameworks that help translate GenAI concepts into usable tools for decision-makers. Finally, we welcome policy briefs and practitioner guides designed to support operational clarity and adoption-readiness for public sector professionals. This range of formats reflects our editorial philosophy: to bridge insight and application, strategy and action, vision and impact.

Editorial Philosophy

At its core, the *Journal of Generative AI in the Public Sector* is committed to an editorial philosophy that balances rigor with accessibility. We strive to publish content that is intellectually robust and methodologically sound, while remaining readable and actionable for practitioners, policymakers, and multidisciplinary audiences. We are not interested in hype cycles or shallow success stories – we seek original insight over trend-driven enthusiasm, privileging substance, strategic clarity, and real-world applicability. Our editorial process holds deep respect for the principles of AI ethics, safety, transparency, and accountability, and we encourage authors to engage critically with the societal, institutional, and human dimensions of GenAI.

Although the journal is based in the United States, we welcome global perspectives – particularly when they bring applied relevance and comparative value to pressing public sector challenges. Importantly, we also reserve space for uncomfortable truths and dissenting views. We recognize that meaningful progress in public sector AI will require not just consensus, but constructive debate, diverse methodologies, and honest confrontation with failure. In that spirit, our editorial vision is one of inquiry, not ideology – and impact, not orthodoxy.

Vision for Impact

We envision this journal not as a passive repository of information, but as an active platform for shaping how generative AI transforms public institutions. In a time when so much of the discourse around AI is fragmented, politicized, or commodified, there is a pressing need for a publication that centers the public mission, respects institutional complexity, and upholds the long-term stewardship of democratic systems. *The Journal of Generative AI in the Public Sector* is that forum. We do not simply aim to publish what is happening in GenAI

ISSN 2995-6366 (Online)

– we aim to help shape what ought to happen. Through the collective insight of contributors, reviewers, and readers, this journal will help define the principles, frameworks, and innovations that guide the integration of GenAI into the fabric of public service, national strategy, and civic life.

Join us to make a difference

We warmly invite you to become part of this effort. Whether you are a government official exploring GenAI adoption, a technologist developing public-sector tools, a researcher studying institutional AI dynamics, or a policy expert shaping regulatory frameworks – your insights are needed. We welcome article submissions, collaborative contributions from government agencies and research labs, and expressions of interest for guest-edited issues, roundtable discussions, or special features on emerging topics. The *Journal of Generative AI in the Public Sector* is more than a publication – it is a collaborative space for inquiry, dialogue, and impact. We look forward to shaping the future of public service together, with the best ideas and most dedicated voices from across disciplines and across the world.

ISSN 2995-6366 (Online)

The Use Case Illusion: Why the Public Sector's Approach to AI Is Undermining Transformation

By ALI (AL) NAQVI*

Abstract

The public sector's prevailing approach to artificial intelligence (AI) emphasizes use cases and pilot projects as indicators of progress. While well-intentioned, this mindset is deeply flawed. Measuring AI maturity through the number of projects undertaken leads to fragmented, siloed automation efforts that lack systemic coherence and fail to deliver strategic transformation. This article argues that the "use case mindset" stems from legacy business process reengineering paradigms and remains fundamentally ill-suited to generative AI and other advanced systems. The goal of AI is not merely task-level automation but the reconfiguration of work itself – both cognitive and physical – across the organizational graph. Public institutions should move beyond linear workflows and embrace models that treat agencies, economies, and even governments as complex adaptive systems. Only through this systems-based lens can GenAI fulfill its potential to increase institutional productivity, responsiveness, and strategic capability. The article concludes with a call to redefine AI strategy away from pilot counting and toward full-system optimization, offering a framework for agencies to escape the use case trap.

Keywords: US Government, Use Cases, Artificial Intelligence, GenAI

* Ali (Al) Naqvi is the Chief Executive Officer of the American Institute of Artificial Intelligence

ISSN 2995-6366 (Online)

1. Introduction: The Illusion of Progress

Across the U.S. public sector, AI progress is routinely narrated through inventories of "use cases" and project counts. Agencies are required by OMB Memorandum M-24-10 and CIO Council guidance to compile annual, machine-readable catalogs that describe each AI application, indicate stage of deployment, and flag "rights- or safety-impacting" uses [1]. This reporting regime has produced large, public repositories – over two thousand entries drawn from more than forty agencies as of early 2025 – and has normalized a metric in which *more entries* appear to signal *more progress*. Yet such aggregation risks conflating administrative activity with progress and institutional transformation, particularly when the inventories themselves are silent on productivity, cross-workflow coherence, capability development, and mission outcomes.

In this context, the "use case" has become the de facto *unit of strategy*. Operationally, a *use case* denotes a bounded application of AI to a specific task or problem (e.g., document summarization for claims, a citizen-service chatbot, or a fraud-risk triage model). A *project* is the vehicle that funds and executes that bounded application along a lifecycle (exploration, pilot, deployment). Inventories therefore tally projects that instantiate use cases. The seductive simplicity of this framing is managerial: use cases are discrete, estimable, and easy to count; projects are procureable, schedulable, and easy to report. But a list of use cases is not a strategy – it is a collection of point solutions anchored to legacy processes, with no necessary guarantee that they interoperate, scale across silos, or compound into system-level gains. The very guidance that standardizes inventories emphasizes classification and compliance (e.g., rights, governance, ethics, or safety-impacting determinations) rather than systemic redesign, thereby reinforcing a project-centric optics of success [2].

This article interrogates that optics. It argues that counting use cases and projects systematically overstates progress while under-measuring transformation, and that a reliance on inventory metrics can entrench "islands of automation." As the consolidated federal catalogs expand – periodically updated with additional entries from new and existing agencies – the risk is that institutional attention tracks the growth of the spreadsheet rather than the growth of capability [3]. We therefore advance an alternative analytic lens for public-sector AI: shifting from a task- and project-bounded paradigm to a system-level, outcome-oriented view that evaluates whether AI reconfigures work (and its interdependencies) in ways that measurably

ISSN 2995-6366 (Online)

improve mission results. The remainder of the paper develops this claim, situates it within federal policy context, and proposes evaluation criteria that privilege coherence, capability, and impact over inventory size.

We can capture the evolution of Use Case in four stages:

Stage 1 Early Stages: In the 1980s and 1990s we observed the rise of "Use Case" when the term began as a software requirements artifact [4] – a structured narrative of how an *actor* interacts with a *system* to achieve a goal (Jacobson's Objectory, then UML formalization). It is explicitly human–system, goal–flow oriented, built for clarity, testability, and traceability in functional requirements.

Stage 2 Consolidation & Practice (1990s–2000s): Cockburn's "actors & goals" formalized use cases and standardized templates and writing discipline [5]. That is when use cases became the lingua franca for scoping functionality and acceptance tests, and a backbone for stakeholder alignment and documentation.

Stage 3 Agile Adaptation (Use Case 2.0): As delivery shifted to agile, teams kept the narrative power of use cases but sliced them into incremental, releasable "use-case slices", often pairing with user stories for sprint-scale work. The concept retained rigor while gaining iteration speed.

Stage 4 Semantic Expansion in AI Era (2010s–today): In AI, "use case" broadened into a business-level label (e.g., "fraud detection," "document summarization"), and a unit for portfolio planning and governance (AI registries; risk triage). It ceased to be only a stepwise interaction script and became a strategic tag for applications – useful for visibility and oversight, but looser in precision.

2. The Use-Case Mindset: Origins and Shortcomings

2.1 Definition of the Mindset

By "use-case mindset" I refer to a planning and reporting posture that treats the use case – a bounded scenario describing how an *actor* (typically a user) interacts with a *system* to achieve a goal – as the *primary unit of strategy*. In software engineering and Human Computer Interaction (HCI), a use case classically captures a dialogue between an external actor and a system, enumerating steps, alternatives, and postconditions. This framing is explicit in the foundational literature (Jacobson's OOSE tradition; Cockburn's requirements guidance) and in UML's formalization of "actors" and "use cases." In short, the mindset assumes that *progress = more well-specified actor–system interactions implemented as projects*. [6]

ISSN 2995-6366 (Online)

2.2 Intellectual Lineage: BPR and Industrial Process Logic

The use-case mindset inherits much of its appeal from the Business Process Reengineering (BPR) era, which privileged decomposition of work into tasks and linear processes amenable to redesign and automation. BPR's promise – dramatic performance gains via radical process redesign – encouraged organizations to view technology as a means to streamline discrete workflows. In public administration, this translated into projectized interventions against specific processes, often evaluated by throughput and cycle-time metrics rather than system-level effects. The result is conceptually tidy portfolios of "use cases," each anchored to an extant process rather than to emergent, cross-boundary capability. [7]

2.3 Why This Template Misfits Generative AI

Generative AI (GenAI) exposes several limits of the use-case template:

a. Unit of analysis – Use cases privilege *user–system* interactions; GenAI routinely operates across *system–system* and *agent–agent* interactions (e.g., autonomous agents negotiating tasks), where no single "primary actor" or stable dialogue suffices. The UML/Cockburn framing is necessary for requirements capture but proves insufficient for modeling multi-actor, multi-modal, continuously learning systems [6].

b. Determinism vs. generativity – Use cases assume relatively deterministic scenarios with enumerated alternatives. GenAI produces probabilistic, context-compositional outputs whose value often lies in *reconfiguring* tasks and information flows, not merely executing a predefined script.

c. Local tasks vs. system behavior – The use-case lens optimizes local tasks; GenAI's highest leverage appears when it alters the topology of work (who does what, in what sequence, with which artifacts), i.e., when organizations are treated as systems of interdependent nodes rather than pipelines of isolated steps.

d. Static boundaries vs. permeable ecologies – Use cases typically presuppose a boundaryable "system under consideration." GenAI thrives in permeable data and capability ecologies (cross-silo retrieval, model ensembles, agent swarms), where value emerges from *interoperation* and *coordination*, not from atomized implementations.

ISSN 2995-6366 (Online)

e. Compliance optics vs. capability growth – Inventories of use cases, standardized for reporting and compliance, encourage counting and classification at the expense of coherence and compounding capability (e.g., shared models, shared data planes, shared assurance). The governance machinery that catalogues uses is valuable, but it can unintentionally entrench project-centric optics. [8]

2.4 Interim Conclusion

In sum, the use-case mindset accurately describes how a user and a system interact, and it remains a useful artifact for requirements elicitation and local delivery. But as a governing logic for GenAI strategy, it under-specifies (i) multi-actor agency, (ii) emergent, non-deterministic behavior, and (iii) the system-level reconfiguration that GenAI enables. Treating inventories of such use cases as proxies for transformation thus risks mistaking activity for capability and projects for progress.

3. Where This Mindset Comes From – and Why It Misfits GenAI

The contemporary use-case mindset inherits its appeal from several intertwined traditions. First, it aligns naturally with the logic of business process reengineering (BPR) and industrial efficiency: decompose work into tasks, optimize the flow between them, and measure cycle time or throughput. Within that paradigm, a use case is an ideal scoping device – clear about user goals, explicit about preconditions and postconditions, and readily testable – so it reliably delivers *local* improvements to a bounded workflow. Second, public-sector technology is typically procurement-driven and projectized. Budgets, schedules, and oversight mechanisms require discrete, auditable units, and the "AI use case" serves as a convenient procurement object and registry entry. This encourages the growth of catalogs of point solutions rather than the cultivation of shared capabilities that compound across missions. Third, classical use cases are rooted in human-centric task decomposition. They formalize an actor–system dialogue (main flows and alternates) and privilege bounded interfaces where a person initiates and supervises the interaction. That modeling choice, powerful for requirements engineering and HCI, underrepresents system-to-system, agent-to-agent, and other emergent patterns of coordination that increasingly characterize contemporary AI ecosystems.

These roots render the use-case template ill-fitted to generative AI. Use cases presuppose enumerable scripts; GenAI is probabilistic and generative, often delivering value precisely by reconfiguring tasks and the topology of information rather than executing a predefined pathway. Traditional actor–system narratives assume a primary human interlocutor; modern deployments increasingly involve agentic

ISSN 2995-6366 (Online)

ecologies – multiple AI services negotiating, planning, and verifying one another's outputs – where value arises from coordination dynamics, not a single dialogic exchange. Catalogs of use cases are excellent for visibility and risk triage, but they privilege countable projects over the properties that determine institutional transformation: coherence across silos, reusability of models and data planes, and compounding capability through shared infrastructure and learned policy. Finally, as an artifact of requirements, the use case excels at describing how existing work should be automated; GenAI invites prior questions – whether the work should exist at all, where to relocate cognition along socio-technical boundaries, and how to re-architect the organizational graph to achieve mission outcomes.

In short, "use case" has evolved from a precise engineering device to a convenient portfolio and governance label, and it remains valuable for communication, traceability, and oversight. But when elevated to the governing logic of AI strategy, it binds institutions to project-centric, task-bounded thinking that systematically undermeasures systemic capability, interoperation, and mission impact – the very arenas where GenAI yields step-change value. Accordingly, this article argues for retaining use cases for cataloging and compliance, while replacing them as the unit of transformation with system-level, outcome-linked capability models that explicitly reward coherence, reuse, and compounded learning across the enterprise.

4. What AI Actually Enables

At its core, contemporary AI – especially large, generative, and agentic systems – is not merely an automation technology. It functions as a cognitive reconfiguration layer that can reorganize information flows, decision rights, and work topologies across an institution. Rather than optimizing a predefined sequence of steps, AI can surface alternative problem framings, synthesize multi-modal evidence, and continuously adapt outputs to shifting context – properties that move beyond classic, task-bound automation. Public guidance already recognizes this socio-technical, system-level character of AI and encourages organizations to evaluate AI not only at the component or application level, but across interactions, contexts, and organizational processes, underscoring that risk and value emerge from the system as a whole [9].

First, AI enables institutions to question the purpose of the task itself, not just how to execute it faster. By generating alternatives, counterfactuals, and synthesized rationales, generative systems can reveal when a task is duplicative, mis-scoped, or better relocated to a different point in the workflow (or eliminated altogether). Evidence from applied domains – such as clinical and administrative uses of LLMs – shows that the principal gains often arise from rethinking information work

ISSN 2995-6366 (Online)

(summarization, triage, drafting, coordination), not merely automating a narrow step, suggesting a broader reframing of what the task should be [10].

Second, AI allows organizations to rethink institutional boundaries. When models can retrieve across silos, reason over heterogeneous data, and interface with other services via tools and APIs, the relevant unit of design shifts from the single process to interdependent systems. Defense research has articulated this as "mosaic" or system-of-systems thinking – composing capabilities dynamically across platforms and echelons – an idea that generalizes to civilian agencies as cross-unit assembly of data, models, and services in pursuit of mission outcomes [11].

Third, AI now permits machines to collaborate in cognition. Multi-agent systems (MAS) and emerging "multi-AI" collaboration frameworks demonstrate how specialized agents can plan, critique, verify, and negotiate with one another to complete complex tasks – behaviors that exceed the classic actor–system dyad of legacy use-case modeling. This agentic ecology foregrounds coordination, role assignment, and protocol design (who does what, when, with which information), making collaboration a first-class design variable rather than an afterthought [12, 13].

Finally, these properties introduce the practical possibility of system-level intelligence: organizations that learn, adapt, and self-reconfigure as complex adaptive systems (CAS). In such systems, value emerges from the interactions among many semi-autonomous components ("agents") that co-adapt over time; AI provides both the computational substrate (models, agents, tool-use) and the governance prompts (profiles, controls) to make this tractable within public institutions. Designing for CAS dynamics – rather than optimizing isolated tasks – aligns evaluation with coherence, compounding capability, and mission outcomes, which system-level frameworks like the NIST AI RMF explicitly encourage [14, 9].

Implication. If AI is treated as cognitive reconfiguration rather than point automation, the unit of strategy must shift accordingly: from counting use cases to engineering system behavior – how information, authority, and action propagate across the enterprise under algorithmic mediation.

5. From Linear Workflows to Complex Adaptive Systems

Public institutions are often managed and measured as if work proceeds along linear workflows – stable, decomposable processes with fixed roles and handoffs. A more accurate and useful lens for AI-era transformation is the complex adaptive system (CAS): a system composed of many interacting components ("agents") whose collective behavior emerges from local interactions and adapts over time through

ISSN 2995-6366 (Online)

learning and feedback. In plain terms, a CAS is an organization that changes how it works as it works, because the parts influence one another and update their behavior in response to outcomes. Foundational accounts emphasize distributed control, rich interdependence, and adaptation as defining features of complexity in social and institutional systems [15].

A CAS view invites graph-based thinking about institutions: people, services, data stores, and algorithms are nodes; relationships, handoffs, and data flows are edges. Network science provides language and tools – paths, centrality, communities, and bottlenecks – to analyze how information and authority propagate, where failures concentrate, and which subgraphs form emergent "functions" even when no single process description exists. This perspective enables optimization not only of steps within a process, but of the topology of the organization – which nodes should connect, which bridges reduce distance, and which communities should be reconfigured to improve outcomes [16, 17].

Within this systems frame, generative AI is not merely a faster step in a fixed chain; it is a cognitive reconfiguration layer that alters the graph itself:

- Rerouting information flows. Retrieval-augmented generation, tool-use, and multi-agent orchestration allow models to pull from, write to, and coordinate across multiple nodes, dynamically re-wiring who informs whom and in what sequence. In practice, this looks like AI agents that plan, critique, and hand off tasks to one another – changing "who talks to whom" inside the enterprise without a human specifying every pathway [18, 19].
- Redesigning work clusters. Network methods identify tightly connected subgraphs ("communities") that function as de facto work clusters. GenAI can consolidate or redistribute their cognitive load (e.g., summarization, triage, drafting, adjudication), enabling new cluster boundaries that cut across legacy silos and shorten decision paths [17].
- Discovering new configurations of mission execution. By composing capabilities across heterogeneous services and teams – often in system-of-systems fashion – AI supports agile recombination of sensors, data, models, and human roles for a given objective. This is the institutional analogue of "mosaic" assembly in defense: building larger, adaptive effects from interoperable, disaggregated pieces. For civilian agencies, the same principle enables cross-program tasking, shared data planes, and reusable model services that assemble on demand around a mission [20].

ISSN 2995-6366 (Online)

Designing for CAS dynamics aligns with contemporary governance guidance that treats AI as socio-technical and system-level: risk and value emerge from interactions among models, data, people, and procedures, not from components in isolation. Evaluating and steering AI at this level means optimizing coherence, compounding capability, and mission outcomes – not merely counting automated tasks – so that the organization learns to reconfigure itself in response to evidence [9].

6. Strategic Consequences

A use-case/counting posture fragments AI effort – and with it, state capacity. When agencies optimize for inventories of discrete projects rather than for coherence of shared data, model services, and cross-workflow learning, the result is a patchwork of "islands of automation." The federal reporting regime formalizes this bias: OMB's M-24-10 requires agencies (with limited exceptions) to enumerate AI use cases annually and post public inventories, a practice that has produced large consolidated catalogs across dozens of agencies. Recent consolidations and compliance plans describe these inventories in detail and emphasize classification and disclosure – important for transparency, but not substitutes for system design [8, 21].

The risk is measurable: oversight bodies now document rapid growth in reported use cases – for example, GAO notes that counts roughly doubled from 2023 to 2024 at a set of large agencies and that generative-AI use cases increased sharply – yet also catalog persistent governance, workforce, and integration challenges that impede impact. Counting activity, in other words, can outpace alignment [21, 22].

This fragmentation carries national-level consequences. For national security, NSCAI's final report frames AI as a strategic, system-of-systems capability – warning that the United States must organize for integrated adoption to remain competitive. Fiscal sustainability is likewise implicated: duplicative point solutions and siloed procurements raise lifecycle costs while under-delivering shared capability. And for service equity and legitimacy, federal policy explicitly recognizes "rights- or safety-impacting" AI and calls for protections against algorithmic discrimination; a fragmented implementation landscape complicates consistent safeguards across programs and jurisdictions [23, 21, 8, 24].

Meanwhile, peer competitors are moving toward more integrated, systemic AI approaches. China's New Generation AI Development Plan (2017) articulates a top-level design to 2030, and current "AI+" policies stress whole-of-nation deployment across sectors – an explicitly coordinated posture that seeks compounding effects rather than isolated pilots. Independent analyses describe this as a state-directed,

ISSN 2995-6366 (Online)

vertically integrated model across the AI stack. While the efficacy of such policies is debated, the strategic intent is clear: alignment, not merely activity [25, 26].

Finally, U.S. guidance already points beyond inventories. The NIST AI Risk Management Framework treats AI as a socio-technical, system-level phenomenon – placing emphasis on interactions, contexts, and organizational processes. If agencies adopt RMF-style lenses while continuing to report use cases for transparency, they can pivot from project counting to capability alignment: shared data planes; reusable model services; common assurance; and outcome-linked metrics. In short, the United States cannot afford to confuse activity with alignment. The policy scaffolding exists; the strategic task is to organize for coherent, compounded capacity rather than a larger spreadsheet [9].

7. Call to Action: Escaping the Use-Case Trap

Escaping the use-case/counting mindset requires replacing project-by-project optimization with system design. The practical path is diagnostic first, redesign second, and institutional alignment throughout.

Map cognitive workflows. Begin with a cognitive work map – a graph of how information, judgment, and authorization move through the institution. Go beyond swimlanes and SOPs: enumerate decision points, evidence requirements, latency tolerances, handoffs (human↔human, human↔system, system↔system), and failure modes. Treat people, services, data stores, and models as nodes, and their dependencies as edges. The artifact should make visible where cognition is duplicated, starved, or delayed.

Identify redundancies and chokepoints. Use the graph to locate (i) redundant judgments (multiple units re-interpreting the same evidence), (ii) serial bottlenecks (single nodes that gate many downstream actions), (iii) long paths (excessive hops between evidence and decision), and (iv) orphan outputs (work products generated but rarely consumed). These are the targets for consolidation, parallelization, or removal.

Use GenAI for synthetic redesign – not bolt-on automation. Treat GenAI as a cognitive reconfiguration layer:

- Reroute flows by inserting retrieval-augmented agents that deliver just-in-time evidence to the point of decision.
- Collapse steps by co-locating summarization, drafting, critique, and adjudication in a multi-agent pattern (planner, solver, verifier).

ISSN 2995-6366 (Online)

- Relocate cognition by shifting routine judgments from scarce expert nodes to supervised AI agents, reserving humans for exception handling and policy setting.
- Remove work that becomes unnecessary once upstream information is synthesized (design for "non-events," not just faster events).
- Document these changes as capability patterns (reusable blueprints that specify inputs, guardrails, roles, and expected outcomes), not as isolated use cases.

Align funding, procurement, and governance to systemic outcomes.

- Funding. Budget for shared capabilities (data planes, model services, assurance tooling) rather than one-off pilots. Create line items for platform teams and cross-program enablement, with Service Level Objectives tied to mission outcomes (e.g., decision cycle time, error rates, equity measures), not project counts.
- Procurement. Specify interoperability and reuse as first-order requirements (APIs, model cards, evaluation protocols, lineage), and score offers on contribution to shared capability (not just local fit). Prefer modular contracts that allow composition and substitution of models/agents over time.
- Governance. Replace inventory-centric dashboards with system health dashboards: coherence across silos, reuse ratios, outcome deltas, assurance coverage, and incident learning. Institutionalize AI assurance (risk, testing, monitoring) as a continuous function embedded in the platform, not a one-time gate at project end.

Measure what matters. Retire "number of use cases" as a success metric. Track mission-linked outcomes (timeliness, accuracy, equity), topology metrics (average path length from evidence to decision; reduction in redundant nodes), and capability compounding (percentage of workloads using shared models/data; rate of pattern reuse). Publish deprecation plans for legacy steps that redesign makes obsolete.

Organize to sustain change. Stand up a cross-functional AI platform team (engineering, data, security, policy, evaluation) with a mandate to deliver reusable services and patterns. Pair it with mission design cells that apply those patterns to high-value workflows and run controlled trials with rigorous evaluation. Establish a policy-tech review cadence where doctrine, controls, and capabilities evolve together based on evidence.

Codify the portfolio. Maintain a capability portfolio (not a use-case list) that articulates: (i) shared services available, (ii) the patterns they enable, (iii) adoption and reuse metrics, and (iv) outcome impacts across programs. Use the portfolio to guide sequencing, investment, and sunset decisions.

Taken together, these steps shift the unit of strategy from projects to properties of the system – coherence, reuse, assurance, and measurable mission impact – so that

ISSN 2995-6366 (Online)

GenAI is used to redesign how the institution thinks and acts, rather than to decorate existing processes with isolated automations.

8. Conclusion

The public sector's prevailing reliance on use-case inventories and project counts has produced an illusion of progress while entrenching structural fragmentation. The cost of this incoherence is tangible: duplicated effort across silos, brittle point solutions that do not interoperate, escalating lifecycle costs, uneven safeguards, and – most importantly – mission outcomes that fail to improve commensurately with investment. Counting implementations is administratively convenient; it is not analytically meaningful. A larger spreadsheet of isolated automations does not constitute a more capable state.

Generative AI sharpens this diagnosis and widens the opportunity. Its value does not lie primarily in accelerating predefined steps, but in reconfiguring cognition and coordination across the enterprise. That requires moving beyond the question "Which tasks can we automate?" to the prior and more consequential questions: What is the work now? Where should cognition live? How should information, authority, and action propagate? In other words, GenAI demands a redefinition of work, not merely faster execution of legacy workflows.

Accordingly, the unit of strategy must shift from the use case to system-level capability – shared data planes, reusable model services, multi-agent patterns, and embedded assurance that compound across programs. Evaluation must likewise pivot from activity metrics to outcome and topology measures: coherence across silos, reuse ratios, shortened evidence-to-decision paths, improved timeliness, accuracy, equity, and resilience. Institutions that organize around these properties will see GenAI translate into durable capacity; those that do not will continue to amass isolated projects and underperform at the mission edge.

The choice before the public sector is therefore clear: persist with a project-centric optics that mistakes activity for alignment, or design for complex, adaptive systems in which intelligence is a property of the whole. Only the latter approach is proportionate to the promise – and the stakes – of the present moment.

ISSN 2995-6366 (Online)

References

1 CIO.gov Report Guidance for 2024 agency artificial intelligence reporting per EO 14110 (2024) https://www.cio.gov/assets/resources/2024-Guidance-for-AI-Use-Case-Inventories.pdf

2 https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf

3 https://flatgithub.com/ombegov/2024-Federal-AI-Use-Case-Inventory?filename=data%2F2023_consolidated_ai_inventory_raw.csv&sha=2a91f52c539771a57e5f8db19f1560f197a12a6f

4 Jacobson, I. (1987, December). Object-oriented development in an industrial environment. In *Conference proceedings on Object-oriented programming systems, languages and applications* (pp. 183-191).

5. Cockburn, A. (1997). Structuring use cases with goals. *Journal of object-oriented programming*, *10*(5), 56-62.

6. Cockburn, A. (2000). Writing Effective Use Cases. https://people.inf.elte.hu/molnarba/Informaciorendszerek_ELTE/Writing_effective_Use_cases_Cockburn.pdf

7. https://www.sciencedirect.com/topics/computer-science/reengineering-process

8. https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf

9. Artificial Intelligence Risk Management https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

10. Meng, X., Yan, X., Zhang, K., Liu, D., Cui, X., Yang, Y., Zhang, M., Cao, C., Wang, J., Wang, X., Gao, J., Wang, Y. G., Ji, J. M., Qiu, Z., Li, M., Qian, C., Guo, T., Ma, S., Wang, Z., Guo, Z., … Tang, Y. D. (2024). The application of large language models in medicine: A scoping review. *iScience*, *27*(5), 109713. https://doi.org/10.1016/j.isci.2024.109713

11. Serbu, J. (2020) *DARPA's contribution to JADC2: 'Mosaic' warfare* *https*://federalnewsnetwork.com/defense-main/2020/12/darpas-contribution-to-jadc2-mosaic-warfare/

12. Zhang, X, Dong, X., Wang, Y., Zhang, D., Cao, F A Survey of Multi-AI Agent Collaboration: Theories, Technologies and Applications. https://arxiv.org/html/2501.06322v1

13. Tran, K., Dao, D., Nguyen, M., Pham, Q,, O'Sullivan, B. Nguyen, H. Multi-Agent Collaboration Mechanisms: A Survey of LLMs https://arxiv.org/pdf/2501.06322v1

14. Holland, John H., 'Complex adaptive systems (CAS)', *Complexity: A Very Short Introduction*, Very Short Introductions (Oxford, 2014; online edn, Oxford Academic, 24 July 2014)

15. Mitchell, M. Complexity: A Guided Tour (2009) Oxford University Press

16. Newman, M. E. J. (2010), Networks: An Introduction, Oxford University Press

17. Barabasi, A. L. (2015), Network Science, Cambridge University Press

ISSN 2995-6366 (Online)

18. Wu, Q et al (2023) AutoGen: Enabling Next-Gen LLM Applications via Multi-Agent Conversation https://arxiv.org/abs/2308.08155v2

https://doi.org/10.48550/arXiv.2308.08155

19. Multi-agent Conversation Framework https://microsoft.github.io/autogen/0.2/docs/Use-Cases/agent_chat/

20. https://www.darpa.mil/news/mosaic-warfare

21. https://files.gao.gov/reports/GAO-25-107653/index.html

22. https://www.nextgov.com/artificial-intelligence/2025/07/agency-ai-use-doubled-2024-gao-finds/407067/

23. https://reports.nscai.gov/final-report/

24. https://www.gao.gov/assets/gao-24-107332.pdf

25. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

26. https://www.geopolitechs.org/p/china-releases-ai-plus-policy-a-brief

ISSN 2995-6366 (Online)

This page left blank intentionally

ISSN 2995-6366 (Online)

An Analysis of Quantum Secure Direct Communication

By NURULLAH NAQVI*

Abstract

Quantum secure direct communication is a process in quantum communication to allow users to communicate securely and directly using quantum mechanics and without the need of generating and sharing secure keys. In recent years, many quantum secure direct communication (QSDC) protocols have been established and proposed. This paper seeks to explore three such QSDC protocols. The first protocol relies on hyperentanglement and complete Bell-state measurements for encoding and decoding of classical information. The second protocol relies on hyperentanglement and a complete polarization Bell-state analysis for encoding and decoding of classical information. The third protocol creates a 15-user quantum network and uses a Bell-state measurement based on the sum-frequency generation to decode classical bits. This paper will provide an in-depth look at the steps of these protocols, test these protocols in conjunction with previously designated criteria for QSDC schemes, and compare and contrast these protocols.

Keywords: Quantum, Secure Direct Communications, QSDC Protocols

1. Introduction

As quantum computing has developed as a field in recent years, we have seen a growth in its applications in cryptography, leading to further development in quantum cryptography. Quantum cryptography was originally proposed in the 1970s; however, information theory, classical cryptography, and quantum physics first had to further mature as fields before quantum cryptography could truly develop. (Gisin et al., 2002). As the development of the field has increased, its applications and implementations have also greatly increased. Prior to the introduction of quantum cryptography, traditional secure communication was conducted using encryption, mathematically created in such a way that the computational complexity of breaking it would take too long to be feasible (Gisin et al., 2002). With the implementation of quantum computers, many classical cryptography protocols will be breakable, and thus, vulnerable (Long et al., 2007). This clearly presents an issue, as all modern day encryption may be under threat from quantum computers in the near future. However, with the introduction of quantum cryptography, new techniques have been created to securely communicate.

* Nurullah Naqvi is the President and Chief technology Officer of the American Institute of Artificial Intelligence

ISSN 2995-6366 (Online)

This leads to the field of quantum communication. Quantum communication uses principles of quantum mechanics to ensure the unconditional security of communication (Sheng et al., 2021). The origins of quantum communication began with quantum key distribution (QKD) (Sheng et al., 2021). As stated by Long et al. (2007), quantum key distribution provides a novel way for two legitimate parties to establish a common secret key over a long distance. Thus, QKD makes it possible to create and distribute secure keys for encryption. Further stated by Long et al. (2007), a new method of quantum communication developed, furthering the processes used in QKD. This method is quantum secure direct communication (QSDC). While QSDC is similar to QKD, in that the goal of both is secure communication relying on quantum mechanics, QSDC differs in that the goal is to communicate a message securely without generating a key (Long et al., 2007).

2. Background

One of the first quantum secure direct communication protocols was proposed in 2002 by Beige et al., based on single photon two-qubit states. While this protocol operated similar to a quantum key distribution protocol, a secure message could be read after the transmission of additional classical information with each qubit. Thus, one of the first means of conducting direct secure communication using quantum principles was developed. Since then, many potential protocols have emerged to conduct QSDC. As stated by Sheng et al. (2022), the purpose of quantum secure direct communication is to directly transmit secret messages without the need of generating or sharing a key. Furthermore, as covered by Long et al. (2007), in QSDC, secret messages can be securely communicated directly between a sender (Alice) and receiver (Bob) without the classical communication of ciphertext. Thus, the quantum key generation and distribution and classical communication of a ciphertext message are combined into a singular form of quantum communication. This provides evidence as to why QKD served as a *stepping stone* to QSDC, as well as evidence to why QSDC may be more secure than QKD but more complicated. Since the purpose of QKD is key distribution, this implies that the information shared between parties may not be controllable, and thus random, while in QSDC the goal is to share information directly. This introduces the need to be able to *control* what information is exactly sent. In addition, to securely communicate with QKD, the sender needs to send information classically (Long et al., 2007), while in QSDC information is shared using quantum principles.

Long et al. (2007), goes on to define the criteria and requirements of a quantum secure direct communication protocol - for a real secure QSDC scheme there are four requirements.

1) After the quantum states are transmitted through a quantum channel from the sender (Alice) to the receiver (Bob), Bob should be able to read the secret message directly without the need of any additional classical information to be sent.
2) The eavesdropper (Eve) cannot obtain any useful information about the sent message, regardless of her steps taken.
3) Alice and Bob can detect if Eve is eavesdropping even before they encode the secret messages onto quantum states.
4) The encoded quantum states are transmitted sequentially in a block by block way.

ISSN 2995-6366 (Online)

These four requirements present a basis for satisfying the goals of QSDC. The first criteria helps to ensure that once encoded quantum information has been shared between two users, no classical information needs to be sent, thus, ensuring the quantum and direct aspect of QSDC. The second and third criteria are necessary to ensure that a QSDC protocol is secure. Since QSDC does not use security keys, the safety and security of the protocol lies in the inability of an eavesdropper from obtaining any usable information about a sent message and the ability for the users of the protocol to be aware if any eavesdropping is occurring. Finally, the fourth criteria ensures that direct communication is occurring through a quantum channel. Each of the following three QSDC protocols will be tested against these criteria established by Long et al. (2007).

3. Quantum Secure Direct Communication Protocol 1 (Gao et al., 2021)

This section of this paper will now cover a quantum secure direct communication protocol proposed by Gao et al., in 2021. This section will seek to define, explain, and analyze this protocol, and all information on the protocol is referenced from Gao et at. (2021).

Gao et al.'s protocol for quantum secure direct communication is proposed using the complete Bell-state measurement (CBSM) resorting to linear optical elements and temporal-polarization hyper-entanglement. The proposed protocol relies on polarized entangled photons to be the carriers of information where the detection events of CBSM are identified with common single-photon detectors. Since all two-photon detection events in CBSM are effective and can be preserved with 100% efficiency rather than 50% efficiency of previous QSDC protocols, the quantum efficiency of QSDC is doubled by encoding more messages on entangled photon pairs.

Thus, this protocol of QSDC is based on the polarization entanglement of photons. Four polarized entangled Bell-states are used as the means of securely transmitting a message. These four entangled Bell-states are written as:

$$|\psi^{\pm}(t)\rangle_{AB} = |\psi^{\pm}\rangle_{AB} \otimes |\phi(t)\rangle_{AB},$$
$$|\phi^{\pm}(t)\rangle_{AB} = |\phi^{\pm}\rangle_{AB} \otimes |\psi(t)\rangle_{AB}$$

Step 1: First, Alice prepares *n* pairs of hyperentangled photon pairs $\{A_1B_1, \ldots, A_nB_n\}$, which are in the hyperentangled state $|\phi^{\pm}(t)\rangle_{AB}$. Hyperentanglement is defined as the entanglement in multiple degrees of freedom (DOFs) of a quantum system, such as polarization of photons (Dent et al., 2017). Next, the hyperentangled photon pairs are divided into sequences S_A and S_B, such that $S_A = \{A_1, \ldots, A_n\}$ and $S_B = \{B_1, \ldots, B_n\}$. Alice sends sequence S_B to Bob through an optical channel and retains sequence S_A.

ISSN 2995-6366 (Online)

Step 2: Upon receiving the photon sequence, S_B , sent by Alice, Bob performs a security test. Bob randomly chooses some photons from the sequence to perform a single photon measurement on the polarization degrees of freedom, using the single photon measurement basis of

$\sigma_z = \{|H\rangle, |V\rangle\}$. Bob publicly announces the outcome of his measurements along with the positions and the measurement basis of the detected photons. After, Alice makes the same measurements on the photon sequence she retained, S_A, for the corresponding positions. Alice and Bob should theoretically have the same measurement results for their measured samples. Prior to the protocol, some security threshold is agreed upon between Alice and Bob. If the estimated error rate of the sample measurements falls below the security threshold, Alice and Bob can assume that the quantum channel is secure and no eavesdropping exists. If the estimated error rate of the sampled measurements is greater than the security threshold, then Alice and Bob will cease communication and can assume that eavesdropping may be occurring and that the channel is insecure.

Step 3: Once Alice and Bob have ensured that their estimated error rate falls below the security threshold, Alice will make unitary operations on the polarization modes of the remaining photon sequences in S_A. The unitary operations are defined as:

$$U_i = |H\rangle\langle H| + |V\rangle\langle V|,$$

$$U_x = |V\rangle\langle H| + |H\rangle\langle V|,$$

$$U_y = |V\rangle\langle H| - |H\rangle\langle V|,$$

$$U_z = |H\rangle\langle H| - |V\rangle\langle V|$$

Using the four unitary operations from above, U_i, U_x, U_y, U_z, the initial hyperentangled state of $|\phi^+(t)\rangle_{AB}$ can be transformed into four hyperentangled states: $|\phi^+(t)\rangle_{AB}$, $|\phi^-(t)\rangle_{AB}$, $|\psi^+(t)\rangle_{AB}$, and $|\psi^-(t)\rangle_{AB}$. Prior to the start of transmission, Alice and Bob will agree that the unitary operations U_i, U_x, U_y, U_z denote 00, 01, 10, and 11 bits, respectively. Alice will randomly choose and encode some photons for the purpose of the security check. Then, Alice will send the encoded photon sequences to Bob.

Step 4: Bob performs the complete Bell-state measurement on the polarization degrees of freedom of photon pair sequences, differentiating four temporal-polarization hyperentangled states: $|\phi^+(t)\rangle_{AB}$, $|\phi^-(t)\rangle_{AB}$, $|\psi^+(t)\rangle_{AB}$, and $|\psi^-(t)\rangle_{AB}$. A schematic diagram shows the complete Bell-state measurement, including t_o and t_1 temporal delays, where $t_0 > t_1$. When a photon pair is in each of the four hyperentangled states, two separate detectors for the CBSM will trigger. If two detectors are triggered, the corresponding event is assumed to be successful. There are four detectors present, D_1, D_2, D_3, D_4, and the combination of the detectors and the time delay reveal the encoded bit. If the detectors D_1D_2 or D_3D_4 occur at the same time, then the encoded two photons are in the state $|\phi^+(t)\rangle_{AB}$. If the detectors D_1D_4 or D_2D_3 occur at the same time, then the encoded two photons are in the state $|\phi^-(t)\rangle_{AB}$. If the two detectors D_1D_2, D_3D_4, D_1D_3, or D_2D_4 are triggered with the time delay t_0, the two encoded photons are in the state $|\psi^+(t)\rangle_{AB}$. If the two detectors $D_1D_1, D_2D_2, D_4D_4, D_1D_4$, or D_2D_3 are triggered with the time delay t_1, the two

ISSN 2995-6366 (Online)

encoded photons are in the state $|\psi^-(t)\rangle_{AB}$. Using the previously agreed upon (with Alice) encoding of 00, 01, 10, and 11, Bob is able to determine what encoded bits he received from Alice. Bob will then publicly announce (over a public channel) the successful detection signatures. Alice and Bob will then keep a record of the occurrences with the successful detections and discard all remaining detections as failures. Another security check can then be performed by Alice with Bob estimating the error rate according to the measurement results of the photons. If the security check is passed, and thus, communication secure, error correction and privacy amplification are performed and the secret message is successfully transmitted between Alice and Bob.

The essence of this QSDC protocol lies in the setup of the complete Bell-state measurement design. The CBSM design allows for the ability to detect which hyperentangled state was received after a unitary operation was conducted on it. The CBSM provides a way to distinguish the four hyperentangled states: $|\phi^+(t)\rangle_{AB}$, $|\phi^-(t)\rangle_{AB}$, $|\psi^+(t)\rangle_{AB}$, and $|\psi^-(t)\rangle_{AB}$. The necessity of the detectors and temporal delays in the CBSM is to allow for a proper way to determine which of the four original hyperentangled states was encoded. Upon running the CBSM and recording the results, all Bob must do is compare the results with the predetermined encoding of the classical bits 00, 01, 10, and 11. Thus, it can easily be seen how key distribution is no longer needed. The classical bits are encoded into a quantum state, the quantum state is sent after performing security checks to ensure no eavesdropping, the quantum state is measured using a complete Bell-state measurement, the measurement result is then compared and mapped back to the classical bit. Another security check is performed, and if it passes, a quantum secure direct communication has occurred.

To further verify that this CBSM protocol classifies as a quantum secure direct communication protocol, we will review if it satisfies the four requirements and criteria established by Long et al. (2007) for a QSDC scheme.

1) *After the quantum states are transmitted through a quantum channel from the sender (Alice) to the receiver (Bob), Bob should be able to read the secret message directly without the need of any additional classical information to be sent.*
   In this protocol, the secure quantum channel is established by photon pairs in temporal-polarization hyperentangled states. Once Alice sends the quantum states after the unitary operations are performed, Bob receives the quantum states. Bob then performs a complete Bell-state measurement and can decode the measurement results into classical bits, based upon the agreed upon mappings between Alice and Bob prior to the sending of the quantum states. Thus, after Alice transmits the quantum states through the quantum channel, Bob does not need any classical information to read the message. Therefore, the QSDC protocol satisfies the first criteria.

2) *The eavesdropper (Eve) cannot obtain any useful information about the sent message, regardless of her steps taken.*
   The security of this QSDC protocol is reliant on the non-locality of the hyperentangled photon pair with double security checks. The first security check performed detects if an attack on the first transmitted photon sequence is occurring before the encoding with the block by block transmission technique. The second security check guarantees the security of the second transmitted photon sequence after the encoding has taken place. Thus, the

ISSN 2995-6366 (Online)

security checks performed prevent any information from being obtained by Eve during attempted eavesdropping. Therefore, the QSDC protocol satisfies the second criteria.

3) *Alice and Bob can detect if Eve is eavesdropping even before they encode the secret messages onto quantum st*ates.
The first security check is performed prior to the encoding of the message into the quantum state. Thus, Alice and Bob will be aware of whether Eve is eavesdropping prior to the encoding. Therefore, the QSDC protocol satisfies the third criteria.

4) *The encoded quantum states are transmitted sequentially in a block by block way.*
This QSDC uses a block-transmission technique for encoding and transmission. Thus, the QSDC protocol satisfies the fourth criteria.

Since all four criteria established by Long et al. (2007) are satisfied by this quantum secure direct communication protocol, it can be further concluded that QSDC occurs with this protocol.

The physical implementation of this QSDC protocol requires the use of nonlinear optical elements. Nonlinear optical elements are necessary to differentiate properly between the four Bell-states. However, without the use of nonlinear optical elements (resorting to linear optical elements), it is challenging to properly execute this protocol, in both theory and experimentally. Linear optical elements prove difficult to properly distinguish between the four Bell-states, thus making it difficult to decode the proper message. In previous QSDC protocols relying on Bell-state measurements, the success probability was 50%. Quantum efficiency, defined as the amount of messages encoded on an entangled photon pair, is directly related to the successful probability of the Bell-state measurements. The addition of the complete Bell-state measurement, in which the photon pairs are in the temporal-polarization hyperentangled state, increases the quantum efficiency by encoding two bits of messages (00, 01, 10, 11) on an entangled photon pair. This leads to double the efficiency than previously. Thus, the usefulness of using hyperentangled states and the complete Bell-state measurement can be seen in a quantum secure direct communication protocol.

4. Quantum Secure Direct Communication Protocol 2 (Sheng et al., 2022)

This section of this paper will now cover a quantum secure direct communication protocol proposed by Sheng et al., in 2022. This section will seek to define, explain, and analyze this protocol, and all information on the protocol is referenced from Sheng et al. (2022).

Sheng et al., propose a one-step quantum secure direct communication protocol. This protocol requires the distribution of polarization-spatial-mode hyperentanglement for one round only. The security of this protocol is ensured by preventing any way for an eavesdropper from obtaining information on the message. Furthermore, this protocol is a two-way quantum communication, rather than a one-way message from a sender to a receiver. In addition, this

ISSN 2995-6366 (Online)

protocol has a high capacity to transmit two bits of secret messages with one pair of hyperentanglement, rather than just one bit. Using entanglement fidelities of polarization and spatial-mode degrees of freedom at 0.98, the maximal communication distance of this protocol is 216 km.

Traditionally, quantum secure direct communication protocols require two-steps. In the first step, two users distribute the entanglement to set up a quantum channel. In the second step, the message sender (Alice) encodes, using the dense encoding approach, and sends their message to the receiver (Bob). One of the photons in each photon pair is sent back to perform a Bell-state analysis to read out the secret message. Major developments have allowed great progress in these protocols in recent years. For example, hyperentanglement, which is the simultaneous entanglement in more than one degree of freedom, has been used to increase channel capacity. This protocol can transmit two bits of secret message by distributing the hyperentanglement in only one round.

This QSDC protocol adopts the polarization-spatial-mode hyperentanglement with the form of:

$$|\Phi^+\rangle = |\phi^+\rangle_P \otimes |\phi^+\rangle_S$$

where $|\phi^+\rangle_P$ is one of the four Bell-states in polarization degrees of freedom with the form:

$$|\phi^\pm\rangle_P = \frac{1}{\sqrt{2}}(/H\rangle/H\rangle \pm /V\rangle/V\rangle),$$

$$|\psi^\pm\rangle_P = \frac{1}{\sqrt{2}}(/H\rangle/V\rangle \pm /V\rangle/H\rangle)$$

and $|\phi^+\rangle_S$ is one of the four Bell-states in spatial-mode degrees of freedom with the form:

$$|\phi^\pm\rangle_S = \frac{1}{\sqrt{2}}(/a_1\rangle/b_1\rangle \pm /a_2\rangle/b_2\rangle),$$

$$|\psi^\pm\rangle_S = \frac{1}{\sqrt{2}}(/a_1\rangle/b_2\rangle \pm /a_2\rangle/b_1\rangle)$$

where $/H\rangle$ denotes horizontal polarization, $/V\rangle$ denotes vertical polarization, and a_1, b_1, a_2, b_2 denote different spatial modes.

To accomplish this quantum secure direct communication protocol, the following steps must be taken:

Step 1: Alice prepares N ordered pairs of polarization-spatial-mode hyperentangled states, $|\Phi^+\rangle_i \, s.t. \, i = 1,2,\ldots,N$. These ordered N pairs construct the message sequence. Alice then prepares an ordered M pairs of hyperentangled states $|\Phi^+\rangle_j \, s.t. \, j = 1,2,\ldots,M$, for the purpose of security testing. The security testing photon pairs are inserted into the message at random. Thus, the complete message sequence has $N + M$ hyperentangled photon pairs.

ISSN 2995-6366 (Online)

Step 2: For every hyperentangled photon pair in the complete message sequence, Alice will retain the first photon and send the second photon to Bob using block transmission. Once the photon transmission has been completed, both Alice and Bob measure the security testing photons and store the remaining photons in quantum memories.

Step 3: In the security checking sequence, Alice will randomly choose the basis $\{|H\rangle, |V\rangle\}$ or $\{|\pm\rangle_P = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)\}$ in polarization degrees of freedom and $\{|a_1\rangle, |a_2\rangle\}$ or $\{|\pm\rangle_S = \frac{1}{\sqrt{2}}(|a_1\rangle \pm |a_2\rangle)\}$ in spatial-mode degrees of freedom for the purpose of measuring the security checking photons. Alice will then tell Bob the position and measurement she has chosen for each security checking photon, and Bob will use the same measurement basis to measure the corresponding photon. Alice and Bob will then compare their measurement results. Alice and Bob communicate the previous two steps over a standard, classical communication channel. If no eavesdropping has occurred, Alice and Bob will obtain the same results in both degrees of freedom. However, if they obtain different measurement results in a degree of freedom, a bit-flip error will occur. If the error rate of the bit-flips is higher in any degree of freedom than some established threshold, Alice and Bob will terminate communication. If the error rate is below the established threshold, then Alice and Bob proceed with the assurance that the photon transmission is secure.

Step 4: After Alice and Bob have completed the security check and if the error rate passes, then Alice distills the photons in the message sequence from the quantum memories and encodes her single photons with four single-qubit unitary operations. These four unitary operations can be written as:

$$U_0 = I = |H\rangle\langle H| + |V\rangle\langle V|,$$

$$U_1 = \sigma_x = |H\rangle\langle V| + |V\rangle\langle H|,$$

$$U_2 = \sigma_z = |H\rangle\langle H| - |V\rangle\langle V|,$$

$$U_3 = i\sigma_y = |H\rangle\langle V| - |V\rangle\langle H|$$

The unitary operation $U_k \; for \; k = 0,1,2,3$ will transform the state of $|\phi^+\rangle_P$ into $|\phi^+\rangle_P, |\psi^+\rangle_P, |\phi^-\rangle_P, |\psi^-\rangle_P$, respectively. The operators U_0, U_1, U_2, U_4 are encoded as 00, 01, 10, and 11, respectively. Notice, some of these steps, equations, and encoding follow very closely to the previous protocol established by Gao et al. (2021). This occurs since both QSDC protocols rely on hyperentanglement and Bell-state measurements.

Step 5: Alice and Bob perform nonlocal complete polarization Bell-state analysis assisted with spatial-mode entanglement. The complete polarization Bell-state analysis measurement result depends on the output modes of Alice and Bob.

Step 6: Alice then publishes the positions and her measurement results of the secret message photons.

ISSN 2995-6366 (Online)

Step 7: Based on Alice's measurement results, Bob can decode the secret messages with his own measurement results. These measurements require similar detectors to the previously referenced QSDC protocol (Gao et al., 2021).

From the steps, it can be seen that the key element in this QSDC protocol is the nonlocal complete polarization Bell-state analysis. In linear optics, it is known that only two of the four Bell-states can be distinguished. However, with hyperentanglement, i.e. with the entanglement in other degrees of freedom, complete polarization Bell-state analysis is possible. Letting D_iD_j represent the photon detectors, then the measurement result of D_1D_5, D_2D_6, D_3D_7 or D_4D_8 represent the state $|\phi^+\rangle_P$. The measurement result of D_1D_7, D_3D_5, D_4D_6 or D_2D_8 represent the state $|\psi^+\rangle_P$. The measurement result of D_1D_6, D_2D_5, D_3D_8 or D_4D_7 represent the state $|\phi^-\rangle_P$. The measurement result of D_1D_8, D_2D_7, D_3D_6 or D_4D_5 represent the state $|\psi^-\rangle_P$.

To ensure that the protocol fulfills the requirements of a QSDC scheme, each of the four criteria established by Long et al. (2007) will be checked:

1) *After the quantum states are transmitted through a quantum channel from the sender (Alice) to the receiver (Bob), Bob should be able to read the secret message directly without the need of any additional classical information to be sent.*
   After Bob receives the encoded message through a quantum channel, Alice and Bob both perform nonlocal complete polarization Bell-state analysis assisted with spatial-entanglement. However, for Bob to truly decode the message, Alice must share her positions and measurement results of the message photons. Thus, this protocol does not satisfy the first criteria since after the quantum states are transmitted, Bob needs additional classical information from Alice, regarding her positions and measurement results.

2) *The eavesdropper (Eve) cannot obtain any useful information about the sent message, regardless of her steps taken.*
   Similarly to the previous protocol established by Gao et al. (2021), this protocol relies on security checks to be performed by Alice and Bob. Alice and Bob will be aware of whether there is eavesdropping occuring. Thus, preventing the chance of eavesdropping from occurring. Therefore, this protocol satisfies the second criteria.

3) *Alice and Bob can detect if Eve is eavesdropping even before they encode the secret messages onto quantum st*ates.
   Alice and Bob perform a security check prior to the encoding done by Alice onto quantum states, i.e. the performance of the unitary operators. Thus, Alice and Bob will know if there is an eavesdropper prior to the encoding of the secret message. Therefore, this protocol satisfies the third criteria.

4) *The encoded quantum states are transmitted sequentially in a block by block way.*
   This QSDC uses a block-transmission technique for encoding and transmission. Thus, the QSDC protocol satisfies the fourth criteria.

ISSN 2995-6366 (Online)

Since this protocol fails the first criteria established by Long et al. (2007) for quantum secure direct communication protocols, this protocol does not fit Long et al.'s (2007) definition for a QSDC. The key failure occurs since Long et al. (2007) requires a QSDC protocol to not need any further classical information to be sent for Bob to decode the message after receiving the quantum states. In this protocol, Alice must send Bob her positions and measurements after Bob has already received the encoded quantum states. Despite failing to fulfill the criteria established by Long et al. (2007) for a QSDC, this protocol still fulfills the pure goal of quantum secure direct communication - to communicate directly and securely using quantum principles without the need for a secret key.

The steps for both protocols present several key differences between this protocol and the QSDC protocol proposed by Gao et al. (2021). While hyperentanglement, forms of complete Bell-state measurements, unitary operators to encode, security checking random phases, and a mapping for encoding and decoding were necessary for both protocols, differences in the implementation arise. For one, while both the Gao et al. (2021) protocol and the Sheng et al. (2022) protocol require Alice to generate two sequences, one of the message itself and one for the security check, in the Sheng et al. (2022) protocol, Alice combines the sequences and retains a photon before transmitting to Bob, rather than sending one sequence to Bob, as in the Gao et al. (2021) protocol. Furthermore, both protocols had a variation in the method of the complete Bell-state measurement. The Gao et al. (2021) protocol included time delays while the Sheng et al. (2022) protocol needed a greater number of photon detectors for the measurement. Finally, there were slight variations in the unitary operators and phase equations between both protocols. Despite these differences, since both protocols use hyperentanglement, they can both transmit two bits of information at a time, leading to higher quantum efficiency than other quantum secure direct communication protocols which can only transmit one bit of information at a time.

5. Quantum Secure Direct Communication Protocol 3 (Qi et al., 2021)

This section of this paper will now cover a quantum secure direct communication protocol proposed by Qi et al., in 2021. This section will seek to define, explain, and analyze this protocol, and all information on the protocol is referenced from Qi et al. (2021).

Qi et al. (2021) published a framework for a new QSDC protocol. The goal of this protocol was to overcome two major issues of QSDC. One, overcoming the difficulty of differentiating simultaneously between four sets of encoded entangled states. Two, overcoming the traditional limitations of one-to-one communication between one sender and one receiver. The Qi et al. (2021) protocol manages to accomplish these tasks by creating a QSDC network based on time-energy entanglement and sum-frequency generation that connects 15 users together with a greater than 97% fidelity rate. Furthermore, this protocol's results maintain a fidelity rate of greater than 95% for any two users performing QSDC over a 40 km optical fiber over the network.

Assume that any two users, U_1 and U_2, wish to communicate directly, where U_1 wants to send information to U_2. They will share N pairs of the time-energy entangled states:

$$|\phi^+\rangle = \frac{|ss\rangle + |ll\rangle}{\sqrt{2}},$$

ISSN 2995-6366 (Online)

where s and l indicate whether the entangled photons travel through a short or long path. The steps of this protocol are as follows:

Step 1: Detect the quantum channel to ensure its absolute safety.

Step 2: The users agree that $|\phi^+\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$, $|\psi^-\rangle$ encode the bit values 00, 01, 10, and 11, respectively. $|\phi^\pm\rangle = \frac{/ss\rangle \pm /ll\rangle}{\sqrt{2}}$ and $|\psi^\pm\rangle = \frac{/ls\rangle \pm /sl\rangle}{\sqrt{2}}$ are the four sets of Bell-states.

Step 3: User 1 will perform one of four unitary operations, $I, \sigma_x, \sigma_z, i\sigma_y$, on the photons in their possession to convert $|\phi^+\rangle$ into $|\phi^+\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$, $|\psi^-\rangle$, respectively. Thus, after the unitary operation, the converted $|\phi^+\rangle$ will represent an encoded bit value of 00, 01, 10, or 11.

Step 4: User 2 performs the Bell-state measurement based on the sum-frequency generation to decode the information, allowing User 2 to differentiate between the four sets of encoded Bell-states.

The main factor of this QSDC protocol lies in its network design. The network composition is divided into two layers, the communication network and the subnet. The quantum network is fully connected by five subnets (A, B, C, D, and E). The communication network is the network connecting these 5 subnets. These 5 subnets are made of 3 users each. Between the five subnets are a total of ten connections that represent the correlated time-energy photon pairs between subnets. Thus, each subnet is connected to the other four subnets. Each subnet contains a 1 x 3 passive beam splitter and a delay controlling module, which functions to split a frequency-correlated entangled photon pair and randomly sends them to the three users in that subnet. The ten time-energy-entangled photon pairs between the subnets are divided into 20 ITU (International Telecommunication Union) channels via a 100 GHz DWDM (dense wavelength division multiplexing). DWDM is placed in the quantum-network processor, and then, the output modules of the multichannel are connected to the users in each subnet. To properly realize the interconnection between the three users of a subnet, the quantum processor must distribute five pairs of entangled photons.

To ensure that the protocol fulfills the requirements of a QSDC scheme, each of the four criteria established by Long et al. (2007) will be checked:

1) *After the quantum states are transmitted through a quantum channel from the sender (Alice) to the receiver (Bob), Bob should be able to read the secret message directly without the need of any additional classical information to be sent.*
   After a sender, Alice, sends the receiver(s) the encoded quantum message, all the receiver is required to do is to perform a Bell-state measurement on the sum-frequency generation, and thus, decoding the message. Since, the receiver(s) do not need any further information after they receive the quantum states, this protocol does satisfy the first criteria.

2) *The eavesdropper (Eve) cannot obtain any useful information about the sent message, regardless of her steps taken.*
   The security of this protocol lies in the ability of the users to perform eavesdrop and security checking at any time in the process. If the monitored error rate is lower than a predetermined threshold, then the communication is successful. Thus, this protocol satisfies the second criteria.

ISSN 2995-6366 (Online)

3) *Alice and Bob can detect if Eve is eavesdropping even before they encode the secret messages onto quantum st*ates.
Since the users can perform security checking at any time, and thus, in this protocol perform a security check prior to the sender encoding the secret message onto quantum states, the sender and receiver(s) can determine if eavesdropping is occurring. Therefore, this protocol satisfies the third criteria.

4) *The encoded quantum states are transmitted sequentially in a block by block way.*
This QSDC uses the block-transmission and step-by-step transmission methods for transmission. Thus, the QSDC protocol satisfies the fourth criteria.

Since this protocol satisfies all four criteria established by Long et al. (2007) for quantum secure direct communication protocols, this protocol does fit Long et al.'s (2007) requirement for a QSDC.

In summary, this QSDC protocol establishes a fully connected entanglement-based QSDC network with five subnets and 15 users. Then, using the frequency correlations of the 15 photon pairs via time-division multiplexing and dense wavelength division multiplexing, an experiment was performed using a 40 km optical fiber and two-step transmission between users without generating any secure keys. The spectrum of the source single-photon is divided into 30 International Telecommunication Union channels, for which a coincidence event will occur between each user by performing a Bell-state measurement based on the sum-frequency generation. This coincidence even allows the four sets of encoded entangled states to be identified simultaneously without any post selection. Furthermore, in this QSDC network, each user can request to communicate with others at any time once the network is established. This connection relies on transmitting entangled photon states between multiple users. Thus, a fully secure quantum network is established between 15 users, allowing for secure and direct communication.

6. Conclusion

After reviewing all three protocols, several important similarities and key differences arise. All three protocols use Bell-states, entanglement, Bell-state measurements, unitary operations, and security checks. All three protocols depend on four Bell-states being used to encode four classical bits of information, 00, 01, 10, and 11. These Bell-states vary between the protocols; however, the process of encoding is similar. For each protocol, the user starts with a single Bell-state, and the goal, once security is established, is for the sender to conduct a unitary operation from a set of four unitary operators, that will transform the Bell-state either back into itself or into one of the other three Bell-states. When the receiver has received this transformed Bell-state, they conduct the Bell-state measurement indicated by their protocol to decode the quantum state back into the classical bits.

This process is where the key differences arise between the three protocols. The Gao et al. (2021) protocol uses a complete Bell-state measurement with four detectors and two time delays to decode the quantum state into classical bits. The Sheng et al. (2022) protocol uses a complete polarization Bell-state analysis with eight detectors to decode into classical bits, also requiring positional information and the sender's own measurements to decode. The Qi et al. (2021) protocol

ISSN 2995-6366 (Online)

requires a Bell-state measurement based on the sum-frequency generation to decode into classical bits. In addition, the Qi et al. (2021) protocol establishes a larger quantum network of 15 users, rather than just two users. Despite these major differences, the overarching goal of all three quantum secure direct communication protocols is to differentiate between four sets of encoded entangled states. Furthermore, all three protocols allow the receiver to decode two bits of classical information rather than one. In addition, the Qi et al. (2021) protocol establishes a quantum network of multiple users. These protocols have shown the abilities to communicate directly and securely using quantum mechanics, with multiple users, and with more classical information encoded. Thus, it can be seen that the recent developments of protocols of quantum secure direct communication have led to major advancements in QSDC and will greatly enhance the viability and importance of quantum communication.

References

1. A. Beige, B.-G. Englert, Ch. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A 101, 357 (2002).
2. Deng, F.-G., Ren, B.-C., & Li, X.-H. (2017). Quantum hyperentanglement and its applications in Quantum Information Processing. *Science Bulletin*, *62*(1), 46–68. https://doi.org/10.1016/j.scib.2016.11.007
3. Gao, C. Y., Guo, P. L., & Ren, B. C. (2021). Efficient Quantum Secure Direct Communication with complete bell-state measurement. *Quantum Engineering*, *3*(4). https://doi.org/10.1002/que2.83
4. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145–195. https://doi.org/10.1103/revmodphys.74.145
5. Long, G.-lu, Deng, F.-guo, Wang, C., Li, X.-han, Wen, K., & Wang, W.-ying. (2007). Quantum secure direct communication and deterministic secure quantum communication. *Frontiers of Physics in China*, *2*(3), 251–272. https://doi.org/10.1007/s11467-007-0050-3
6. Qi, Z., Li, Y., Huang, Y., Feng, J., Zheng, Y., & Chen, X. (2021). A 15-user quantum secure direct communication network. *Light: Science & Applications*, *10*(1). https://doi.org/10.1038/s41377-021-00634-2
7. Sheng, Y.-B., Zhou, L., & Long, G.-L. (2022). One-step quantum secure direct communication. *Science Bulletin*, *67*(4), 367–374. https://doi.org/10.1016/j.scib.2021.11.002
8. Ye, Z.-D., Pan, D., Sun, Z., Du, C.-G., Yin, L.-G., & Long, G.-L. (2020). Generic Security Analysis Framework for Quantum Secure Direct Communication. *Frontiers of Physics*, *16*(2). https://doi.org/10.1007/s11467-020-1025-x
9. Zhang, H., Sun, Z., Qi, R., Yin, L., Long, G.-L., & Lu, J. (2022). Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light: Science & Applications*, *11*(1). https://doi.org/10.1038/s41377-022-00769-w

ISSN 2995-6366 (Online)