International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Vulnerabilities and Attacks on Quantum Secret Sharing (QSS) Schemes: A Review

Ajay Kumar[1], Mukesh Kumar[2]

[1,2]Department of Mathematics, Chaudhary Charan Singh University Meerut-250004, India

Abstract

Quantum secret sharing (QSS) allows a dealer to split a secret among several players so that only authorized coalitions can recover it, while any eavesdropping is revealed by quantum disturbance. Since the first proposals in 1999 [3–5], a long series of cryptanalyses has shown that many QSS protocols fail not because of outside eavesdroppers but because of their own players. In this paper, we review the flaws in and attacks on QSS from 1999 to 2026. We classify the attacks into three layers: protocol-level attacks (intercept-resend, entangle-measure, Trojan horse and fake-signal); insider attacks by dishonest or colluding participants, which are especially powerful because insiders control part of the security check; and implementation-level (side-channel) attacks, which exploit imperfect sources, detectors and local oscillators. For each class, we describe the attack mechanism, representative protocols that were broken, and the countermeasures that followed, such as decoy states, one-way transmission with wavelength filtering, measurement-device-independent (MDI) and device-independent (DI) QSS, and composable finite-key proofs that treat dishonest players as adversaries. We conclude that the field is converging on a single lesson: a QSS protocol is only as secure as the participant model behind its proof, so security proofs must treat every player as a potential adversary with full access to their own devices. We end with open problems for QSS in quantum networks.

Keywords: quantum secret sharing; quantum cryptography; participant attack; collusion attack; Trojan horse attack; quantum hacking; measurement-device-independent; device-independent; semi-quantum secret sharing; continuous-variable QSS

1. Introduction

Secret sharing, introduced independently by Shamir [1] and Blakley [2] in 1979, splits a secret into shares so that only qualified groups of shareholders can reconstruct it. Classical schemes are information-theoretically secure once the shares have been delivered, but the delivery itself relies on secure channels that are usually protected only by computationally secure cryptography. Quantum secret sharing addresses this problem: the shares are carried by quantum states, so any interception disturbs them.

Hillery, Bužek and Berthiaume (HBB) proposed the first QSS protocol in 1999 using three- and four-qubit Greenberger–Horne–Zeilinger (GHZ) states [3]. In the same year, Cleve, Gottesman and Lo extended the idea to sharing an unknown quantum state with (k, n) threshold structures [4], and Karlsson, Koashi and Imoto proposed a scheme based on two-particle entanglement [5]. QSS has since been extended to single-qubit sequential schemes [8], graph states [25, 26], continuous variables [27, 28], semi-quantum participants [23, 51–53] and MDI and DI architectures [38–46].

The security record is patchy. Qin et al. identified the participant attack as the most serious threat to QSS [11], and subsequent work has borne this out. The HBB protocol [11], the single-qubit protocol of Schmid et al. [9, 10], multiparty schemes based on single photons and Bell states [14, 16, 17, 19], an MDI deterministic QSS protocol [20–22] and several semi-quantum protocols [23, 24] were all shown to leak the secret to a dishonest insider. In parallel, the quantum-hacking literature on quantum key distribution (QKD) showed that real devices open side channels that idealized proofs ignore [31–34, 55]. Most QSS systems reuse QKD hardware, so these side channels carry over.

This paper makes four contributions:

- A threat model for QSS that separates outside eavesdroppers, single dishonest participants, colluding coalitions and device-level adversaries (Section 3).
- A systematic review of protocol-level and insider attacks, giving the mechanism behind each and the protocols it broke (Section 4).
- A review of implementation-level attacks relevant to discrete- and continuous-variable QSS (Section 5).
- A synthesis of countermeasures, a comparative table of attacks and defences, and a list of open problems, covering work published up to October 2026 (Sections 6–8).

The paper is organized as follows. Section 2 gives background and a taxonomy of QSS schemes. Section 3 defines the threat model. Sections 4 and 5 cover protocol-level and implementation-level attacks, respectively. Section 6 reviews countermeasures, Section 7 compares attacks and defences, Section 8 discusses open problems, and Section 9 concludes.

2. Background

2.1 Classical and quantum secret sharing

A (k, n) threshold scheme distributes a secret S among n players so that any k of them can reconstruct S, while any $k-1$ learn nothing [1, 2]. Quantum secret sharing takes two forms. In the sharing of a classical secret (often called QSS proper, or CQSS), quantum states are used to establish correlated random keys between a dealer and a group of players. In quantum state sharing (QSTS, also called QQSS), the secret is itself an unknown quantum state [4, 6]. Because of the no-cloning theorem, a (k, n) threshold QQSS scheme requires $k > n/2$, and every QQSS scheme corresponds to a quantum error-correcting code in which unauthorized sets learn nothing [4, 6].

2.2 The HBB protocol

In the HBB protocol [3], the dealer Alice prepares the GHZ state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC}$$

and sends one qubit each to Bob and Charlie. Each party measures in the X or Y basis at random. When the bases satisfy the GHZ correlation condition, Bob and Charlie can jointly deduce Alice's result, but neither can do so alone. A subset of rounds is publicly compared to detect eavesdropping. The security of this check depends on the order in which players announce their bases and outcomes, and this dependence is exactly what insider attacks exploit (Section 4.4).

Tittel, Zbinden and Gisin gave an early experimental demonstration using pseudo-GHZ correlations from energy-time entangled photons [7].

2.3 Taxonomy of QSS schemes

Table 1. Families of QSS schemes and their attack surfaces.

Family	Quantum resource	Typical attack surface	Representative works
Entanglement-based (GHZ, Bell)	Multipartite entangled states	Participant attacks via announcement order; entangle-measure	[3, 5, 11, 13]
Single-qubit sequential	One qubit passed through all players	Coherent insider attacks; Trojan horse on two-way links	[8–10]
Single-photon multiparty-to-multiparty	Sequences of single photons	Trojan horse with multi-photon signals; fake-signal	[16, 17]
Graph-state QSS	Cluster and graph states	Insider and collusion attacks on access structures	[25, 26]
Continuous-variable (CV) QSS	Gaussian-modulated coherent or squeezed states	Dishonest players' coherent attacks; local-oscillator (LO) side channels	[27–30]
Semi-quantum QSS (SQSS)	Classical players limited to Z-basis operations	Double-CNOT, unitary and collusion attacks	[23, 24, 49, 51–53]
MDI-QSS	Untrusted central GHZ or Bell measurement	Participant attacks on announcement order; source flaws	[20–22, 38–42]
DI-QSS	Multipartite Bell or Svetlichny violation	Detection loophole; low rates; finite-size effects	[43–47]

A recent Chinese-language review in *Acta Physica Sinica* [54] discusses the theoretical and experimental progress of these schemes, and Murta et al. [60] review the closely related task of conference key agreement.

3. Threat model and security definitions

A QSS protocol must defend against four types of adversary, listed in order of increasing power:

External eavesdropper (Eve). Controls the quantum channels and listens to the authenticated classical channel, but holds no share.

Single dishonest participant. A legitimate player who tries, without being detected, to learn the secret alone or to learn other players' shares. The insider knows his own basis choices and outcomes and can choose when to announce them, so he can tilt the security check in his favor [11, 12].

Colluding coalition. A non-authorized subset of players, possibly allied with Eve, that pools its information. The classic case is collusion between the first and last players in a chain [19]. In semi-quant-

um and mediated schemes, the coalition may also include a semi-trusted quantum third party [49].

Device-level attacker. Exploits deviations between the physical devices and their theoretical models (e.g., detector-efficiency mismatch, imperfect sources or a transmitted local oscillator) [29, 31–34].

The security goals are:

- **Correctness:** every authorized set of players recovers the dealer's secret with high probability.
- **Secrecy against Eve:** Eve's information about the secret is negligible.
- **Secrecy against unauthorized sets:** any unauthorized coalition, even with full quantum side information about its own systems, learns only a negligible amount about the secret.
- **Cheater detection or robustness:** a player who announces false data is detected, or cannot undetectably change the recovered secret.

Modern proofs express these goals in the composable framework [48, 59], in which the protocol's output must be ε-close to an ideal secret shared only by the honest players. A key step, introduced for CV-QSS by Kogias et al. [27], is to compute the key rate with the dishonest player treated as part of the eavesdropper. For a dealer A and players B and C, the asymptotic rate under a dishonest Bob is

$$K \geq I(A{:}BC) - \max_{\text{Eve},B} \chi(A{:}E\,B)$$

where χ(A:EB) is the Holevo information held jointly by Eve and Bob. A positive rate under every such assignment guarantees security against both outsiders and insiders. Early protocols considered only the first type of adversary, which is why insider attacks broke them.

4. Protocol-level attacks

Protocol-level attacks assume ideal devices and exploit the logic of the protocol: which states are sent, who checks what, and in what order data are announced.

4.1 Intercept-resend attack

Eve measures each transmitted qubit in a basis of her choice and resends the state she observes. In a BB84-style check with two conjugate bases, she chooses the wrong basis half the time, producing a 25% error rate in the check rounds. The detection probability after N check qubits is $1 - (3/4)^N$, which approaches 1 exponentially; this is the standard argument used by most QSS proposals, including recent semi-quantum schemes [51, 52]. Intercept-resend is weak as an outsider strategy but becomes powerful when combined with insider knowledge. Shi et al. [19] showed that in Lin et al.'s protocol with a collective eavesdropping check, the player who performs the last local operation can combine intercept-resend with entanglement swapping to obtain the secret undetected, reducing the earlier two-insider attack to a one-insider attack.

4.2 Entangle-measure attack

Eve couples each qubit to an ancilla through a unitary U and measures the ancilla after the public announcements. In its most general form,

$$U|0\rangle|E\rangle = a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle, \qquad U|1\rangle|E\rangle = c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle$$

Requiring zero disturbance on the check states forces the ancilla states to be independent of the qubit, so Eve learns nothing. This argument underlies the security claims against entangle-measure attacks in schemes based on monotone span programs, restricted threshold access structures and W states [52, 64, 65]. It fails, however, when the attacker is an insider who does not have to pass every check, as Section 4.4 shows.

4.3 Trojan horse, invisible-photon and delay-photon attacks

Two-way and circular QSS protocols, in which a photon travels from one player to the next and back, are exposed to Trojan horse attacks. The attacker injects probe photons into an honest player's device, lets them pick up the player's encoding operation, and reads them out on the way back. Deng et al. [14] showed that the Zhang–Li–Man multiparty QSS protocol [13] detects every outsider, but the agent who prepares the signals can steal the other agents' operations with a Trojan horse. The same group showed that the Yan–Gao multiparty-to-multiparty protocol [16] is secure with genuine single photons but insecure with multi-photon signals, because some agents can then read the others' messages [17]. They also analyzed the delay-photon variant, in which probe photons trail the legitimate signal, and the invisible-photon variant, in which the probes are invisible to the honest players' detectors [15]. Gisin et al. [18] analyses the general Trojan horse attack on two-way plug-and-play systems and quantified how much information an attacker can gain.

The Trojan horse threat also applies to continuous variables. Ma et al. [57] demonstrated a Trojan horse attack on two-way CV-QKD that exploits overlapping modulation pulse widths; the same structural weakness applies to CV-QSS designs in which a player modifies a received mode without measuring it. Countermeasures include wavelength filters, photon-number splitters with a monitoring detector on a random fraction of the incoming light, optical isolators and one-way transmission [14, 15, 50].

4.4 Participant (insider) attacks

Participant attacks are the most common failure mode of QSS. Because a dishonest player takes part in the security check, he can often choose his actions so that the check passes with certainty.

Attacks on HBB. Hillery et al. originally analyses an insider intercept-resend attack and an outsider entangle-measure attack [3], and Karlsson et al. [5] demonstrated a cleverer insider attack. Qin et al. [11] gave the first systematic treatment: they cast the attack as discrimination between two mixed states, derived necessary and sufficient conditions for a dishonest participant to obtain the whole secret with zero error, showed that the HBB protocol is insecure against dishonest participants, and constructed an explicit attack. The attack works because the dishonest player can announce last, after seeing the honest player's basis.

Attacks on single-qubit QSS. Schmid et al. [8] proposed and demonstrated a scheme in which one qubit passes through all N players, each of whom applies a phase rotation. He [9] pointed out that this scheme is insecure, and He and Wang [10] later showed that both the original and the modified versions are insecure against coherent attacks: an insider keeps the qubit, sends half of an EPR pair onward, and infers the honest player's phase from the announcements.

Fake-signal and Bell-state attacks. In multiparty QSS protocols built on Bell states and entanglement swapping, a dishonest agent can replace the legitimate signals with entangled fake signals, perform the honest operations on one half, and announce false operations. Gao and co-workers formalized participant attacks in multiparty quantum cryptography in 2007 [12], and a long chain of attacks, comments and replies followed, including Gao's comment showing that some claimed attacks on Zhang et al.'s protocol actually fail [61]. These disputes show that participant attacks must be checked as carefully as the protocols they target.

Attacks on MDI-QSS. Measurement-device independence does not by itself protect against insiders. Gao et al. proposed an MDI deterministic QSS protocol in 2020 [20], and Yang et al. [21] showed that a dishonest participant could obtain the dealer's secret alone without introducing any detectable error. That attack assumed that the dishonest agent announces his single-photon state after the other agents; Yang,

Liu et al. [22] removed this assumption with a stronger attack that works regardless of announcement order.

Attacks on semi-quantum QSS. Semi-quantum schemes restrict classical players to Z-basis measurement and reflection, which limits their ability to verify quantum states. Tsai et al. [23] showed that in a limited-resource SQSS protocol, a malicious agent can use a double-CNOT attack to steal part of another agent's secret shadow undetected. A 2025 cryptanalysis [24] of an efficient controlled SQSS protocol showed that the controller can recover the secret with the help of just one participant, and that an external attacker can mount a denial-of-service attack that makes honest players recover a wrong secret. Most recently, Majhi et al. [49] showed that the classical players' limited quantum capability lets an assisting quantum third party collude with a dishonest classical participant to recover the secret undetected, and proposed a scheme that is information-theoretically secure against this collusion.

4.5 Collusion attacks

In a chain of n players, the first and last players see both the input to and the output from the honest players between them. By colluding, these two can in some cases cancel the honest operations and obtain the secret. Analyses of dynamic QSS protocols have found this flaw repeatedly: the first and last agents can obtain the dealer's master key without the others' cooperation [62]. Threshold schemes based on Shamir's polynomial resist collusions of fewer than k players only if those players cannot also eavesdrop undetected on the honest players' quantum channels [51]. In practice, collusion resistance therefore depends on decoy-state checks on the channel between every pair of players, not only on the classical threshold property.

4.6 Denial-of-service and forgery

Besides learning the secret, an attacker may try to make the honest players reconstruct a wrong one. The 2025 cryptanalysis of controlled SQSS [24] gives an explicit denial-of-service attack of this kind. In threshold schemes in which one player reconstructs the secret and forwards it, that player can read it and pass on a forged value; hash-based verification of the reconstructed secret detects such tampering after the fact [63].

5. Implementation-level attacks

Implementation attacks target the gap between the device model in a security proof and the hardware in the laboratory. They were developed mostly against QKD [55, 56], but QSS systems use the same sources, modulators and single-photon detectors and, because they involve more parties, more devices that must be trusted. Few of these attacks have been demonstrated on a QSS testbed specifically, but the transfer is direct, and MDI- and DI-QSS were designed precisely to close these channels [38, 43].

5.1 Detector attacks

- **Faked-state attack.** Makarov and Hjelme [32] showed that an attacker who exploits detector imperfections can send tailored bright pulses that make the receiver's detectors click only in the basis she chooses, so that the receiver reproduces her measurement result.
- **Detector blinding.** Lydersen et al. [31] blinded commercial avalanche photodiodes with continuous bright light, turning them into classical linear detectors that the attacker could trigger at will, and recovered the full key from commercial QKD systems without raising the error rate.
- **Time-shift attack.** Zhao et al. [33] exploited the time-dependent efficiency mismatch between two detectors and demonstrated a successful attack on a commercial system by shifting the arrival times of the signals.

In QSS, every player who measures carries detectors of this kind. A dishonest player can blind or time-shift another player's detectors, combining the device-level and insider adversaries of Section 3.

5.2 Source attacks

In practice, QSS experiments use attenuated lasers instead of true single-photon sources. Multi-photon pulses enable the photon-number-splitting (PNS) attack, in which the attacker keeps one photon from each multi-photon pulse and blocks single-photon pulses to hide the resulting loss [34]. Multi-photon pulses also enable the Trojan horse attacks on multiparty QSS described in Section 4.3 [17]. Decoy-state methods [35, 36] bound the single-photon contribution and defeat PNS; in QSS, every source must use decoy intensities.

Sources are also imperfect in other ways: phase correlations between pulses, side-channel leakage from modulators, and back-reflections that permit Trojan horse probing [18] all leak information. MDI-QSS schemes based on entanglement witnesses [66] account for such state-preparation flaws in the key-rate estimate instead of assuming perfect sources.

5.3 Continuous-variable side channels

CV-QSS inherits the local oscillator (LO) weaknesses of CV-QKD. When the LO travels with the signal through an untrusted channel, an attacker can mount wavelength, LO-calibration, LO-fluctuation, clock-synchronization-jitter and LO-polarization attacks, all of which have been demonstrated against CV-QKD [29]. Generating the LO locally (LLO-CVQSS) removes the transmitted LO but introduces new noise terms that must be bounded against both eavesdroppers and dishonest users [29]. Sequential CV-QSS designs [28], in which a coherent state passes through each player in turn and each adds a locally prepared Gaussian-modulated displacement, are also exposed to Trojan horse probing of the players' modulators (Section 4.3).

5.4 Finite-size and parameter-estimation weaknesses

A last class of weakness is statistical. Many protocols are analyzed only in the asymptotic limit; with a finite number of rounds, the error-rate estimate fluctuates, and an attacker can hide inside those fluctuations. Li et al. [39] noted that most QSS protocols in the literature had been analyzed only asymptotically and without considering participant attacks, and they provided a composable finite-size analysis that includes them. Brooks et al. [48] went further in 2026, providing a composable finite-key bound against general attacks, including participant attacks, for a four-party GHZ-based protocol.

6. Countermeasures

6.1 Protocol-design defences

- **Randomized announcement order and commitments.** Most participant attacks on HBB-type protocols rely on the dishonest player announcing last; randomizing the order, or requiring commitments before any announcement, removes this advantage [11, 48].
- **Pairwise decoy checks.** Decoy photons drawn at random from the conjugate bases $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ are inserted on every link and checked before the next step, so that any player who tampers with a link, insider or outsider, is detected exactly as an outsider would be [51–53, 63].
- **Jointly determined secret.** When every party contributes randomness to the final secret, no single player or mediator can impersonate the dealer or control the outcome [53].
- **One-way transmission.** Sending qubits in one direction only removes the return path that Trojan horse attacks need [50]. When two-way links are unavoidable, wavelength filters and photon-number monitoring on a random fraction of the incoming light are required [14, 15].

- **Verification of the reconstructed secret.** Publishing a hash of the secret, or using a verifiable scheme, exposes a reconstructor who forwards a forged value [30, 63].

6.2 Treating dishonest players as adversaries in the proof

The most important conceptual defence is to include insiders in the security proof itself. Kogias et al. [27] proved unconditional security for entanglement-based CV-QSS by treating the dishonest player as part of Eve and all players' devices as black boxes, so that fake announcements and Trojan horse attacks need not be analyzed individually. Grice and Qi [28] proved security against eavesdroppers and dishonest players for a sequential coherent-state CV-QSS scheme, even under high channel loss. A verifiable (k, n) threshold CV-QSS protocol secure against both eavesdroppers and dishonest players was demonstrated in 2023 [30]. For discrete variables, Li et al. [39] and Brooks et al. [48] provide composable finite-size security that includes participant attacks.

6.3 Measurement-device-independent QSS

MDI protocols move all measurements to an untrusted relay, which removes the detector attacks of Section 5.1 by construction [37]. In 2015, Fu et al. [38] proposed long-distance MDI multiparty quantum communication based on a central GHZ-state measurement. Subsequent work has improved both rate and distance: Li et al. [39] used spatial multiplexing to break the rate-distance bound for networks of at least ten parties, raising the secret-key rate by more than two orders of magnitude; Cai et al. [41] used untrusted Bell-measurement relays to double the dealer-sharer distance; Zhang et al. [40] used quantum memories to synchronize heralded single-photon sources in 2024; and a reconfigurable MDI-QSS network based on linear Bell-state analysis was proposed in [42]. MDI security still relies on trusted sources and, as Section 4.4 shows, does not rule out participant attacks [21, 22].

6.4 Device-independent QSS

DI protocols certify security from the observed statistics alone, without any model of the devices, following DI-QKD [67, 68]. Gogioso [47] proposed an early DI-style QSS protocol based on Mermin-type contextuality, secure against non-signaling adversaries. In 2024, a DI-QSS protocol based on violation of the Svetlichny inequality, with noise preprocessing and post selection, was proposed [43], followed by an improved version with an advanced random key-generation basis [44]. A 2025 proposal uses nearly on-demand single-photon sources in a heralded architecture to build long-distance multipartite entanglement while reducing transmission loss [45]. Majhi and Paul [46] proposed a DI-QSS protocol based on a multiparty pseudo-telepathy parity game, in which the same test serves both device certification and key generation, so no dedicated test rounds are needed. DI-QSS provides the strongest guarantees, but current key rates and required detection efficiencies are still impractical.

6.5 Implementation countermeasures

Decoy states defeat PNS attacks [35, 36]. Optical isolators, filters and power monitors limit Trojan horse probing [18]. Generating the LO locally eliminates LO-targeted attacks in CV-QSS but introduces new phase-noise terms that must be bounded [29]. Monitoring the detector photocurrent and randomly varying detector efficiency counter blinding attacks [31], but only MDI and DI designs close detector side channels in general.

7. Comparative analysis

Insider attacks have broken more QSS protocols than any other class of attack, and they are the only class that MDI designs do not remove. Table 2 summarizes each attack, the adversary it requires, examples of affected protocols and the defences that work.

Table 2. Comparison of attacks on QSS and effective defences.

Attack	Layer	Adversary	Example affected protocols	Effective defences
Intercept-resend	Protocol	Outsider; insider when combined with swapping	Lin et al. collective-check QSS [19]	Decoy checks on every link [51, 52]
Entangle-measure	Protocol	Outsider	Generally, fails against decoy checks [64, 65]	Conjugate-basis checks; full unitary analysis
Trojan horse / delay-photon / invisible-photon	Protocol + device	Outsider or signal-preparing insider	Zhang–Li–Man MQSS [13, 14]; Yan–Gao QSS with multi-photon signals [16, 17]	One-way transmission [50]; filters and photon-number monitors [14, 15]
Participant attack (announce-last)	Protocol	Single insider	HBB [3, 11]; single-qubit QSS [8–10]	Randomized order, commitments; insider-aware proofs [27, 48]
Participant attack on MDI-QSS	Protocol	Single insider	MDI deterministic QSS [20–22]	Insider-aware composable analysis [39]
Double-CNOT / unitary attack	Protocol	Insider in SQSS	Limited-resource SQSS [23]; threshold SQSS [51]	Decoy particles carrying secret information [53]
Collusion (first + last, or third party + player)	Protocol	Coalition	Dynamic QSS [62]; controlled SQSS [24]; SQSS with quantum third party [49]	Pairwise checks; collusion-secure designs [49]
Denial-of-service / forgery	Protocol	Outsider or reconstructing insider	Controlled SQSS [24]	Secret verification by hash or VSS [30, 63]
Detector blinding, faked-state, time-shift	Device	Outsider or insider	Any QSS with trusted detectors [31–33]	MDI-QSS [38–42]; DI-QSS [43–46]
Photon-number splitting	Device	Outsider	Weak-coherent-pulse QSS [34]	Decoy states [35, 36]
LO-targeted attacks	Device	Outsider or insider	CV-QSS with transmitted LO [29]	Local LO (LLO-CVQSS) [29]
Finite-size hiding	Statistical	Any	Asymptotic-only analyses [39]	Composable finite-key bounds [39, 48]

Two patterns stand out. First, every protocol-level break involves an adversary that the original security proof did not model, most often a dishonest participant. Second, each architectural advance shifts the residual risk rather than removing it: MDI removes detector attacks but leaves sources and insiders; DI

removes device trust but leaves rate and loophole limits; and semi-quantum designs lower cost but weaken the players' ability to detect insider manipulation.

8. Open problems and future directions

1. **Unified insider-aware proofs for discrete-variable QSS.** CV-QSS has general proofs that treat dishonest players as adversaries [27, 28], and composable DV proofs are now appearing [39, 48]. However, most of the many protocols proposed each year, in journals such as Quantum Information Processing [53], still argue security attack by attack. A common proof template, like the entropic-uncertainty proofs used in QKD, would let new protocols be tested against all insider strategies at once.
2. **Hacking experiments on QSS hardware.** Detector-blinding, time-shift and Trojan horse attacks have been demonstrated on QKD systems [18, 31, 33] but rarely on multiparty testbeds. Star-network experiments such as the 20 km, four-party GHZ experiment of Brooks et al. [48] are natural targets for red-team testing.
3. **Combined insider-device attacks.** A dishonest player who also tampers with an honest player's device is a stronger adversary than either alone. Few analyses have considered this joint model.
4. **Practical DI-QSS.** DI-QSS needs high-fidelity multipartite entanglement and high detection efficiency despite channel loss. Single-photon-source architectures [45] and test-round-free schemes [46] reduce resource demands, but no loophole-free DI-QSS experiment has been reported so far.
5. **Semi-quantum security limits.** When players are limited to Z-basis operations, openings for insider and collusion attacks keep appearing [23, 24, 49]. Which access structures can be realized securely with classical players has not yet been characterized.
6. **QSS in quantum networks.** In networks with untrusted relays, dynamic membership and many parties, QSS must be combined with conference key agreement [60] and with post-quantum classical cryptography for authentication. Recent post-quantum publicly verifiable secret sharing [58] suggests hybrid designs in which quantum shares are verified using post-quantum classical tools.
7. **Standardization and certification.** QKD has emerging security-evaluation standards; QSS has none. Certification methods should cover multiparty trust, announcement order and the devices of all participants.

9. Conclusion

Twenty-seven years after HBB, the main vulnerability of quantum secret sharing remains the participants themselves. Protocol-level outsider attacks, such as intercept-resend and entangle-measure, are reliably detected by decoy checks, but insider attacks have broken GHZ-based, single-qubit, Bell-state, MDI and semi-quantum protocols, often by exploiting nothing more than the order of announcements. Implementation attacks inherited from QKD open a second front, which MDI-QSS and DI-QSS close at increasing cost. The literature from 2023 to 2026 points in a clear direction: security proofs now treat dishonest players as part of the adversary, composable finite-size analyses are replacing asymptotic arguments, and experiments such as the 2026 four-party GHZ demonstration with composable security against participant attacks [48] show that these guarantees can be achieved at useful rates. The next steps are to apply the same insider-aware standard to every new protocol, to test QSS hardware against real hacking attacks, and to make device-independent QSS practical. A QSS protocol should be considered secure only when its proof assigns every player, and every player's device, to the adversary.

References

1. A. Shamir, "How to share a secret," *Commun. ACM* 22(11), 612–613 (1979).
2. G. R. Blakley, "Safeguarding cryptographic keys," *Proc. AFIPS National Computer Conference* 48, 313–317 (1979).
3. M. Hillery, V. Bužek, A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A* 59, 1829 (1999).
4. R. Cleve, D. Gottesman, H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.* 83, 648 (1999). arXiv:quant-ph/9901025
5. A. Karlsson, M. Koashi, N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Phys. Rev. A* 59, 162 (1999).
6. D. Gottesman, "Theory of quantum secret sharing," *Phys. Rev. A* 61, 042311 (2000). arXiv:quant-ph/9910067
7. W. Tittel, H. Zbinden, N. Gisin, "Experimental demonstration of quantum secret sharing," *Phys. Rev. A* 63, 042301 (2001).
8. C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, H. Weinfurter, "Experimental single qubit quantum secret sharing," *Phys. Rev. Lett.* 95, 230505 (2005).
9. G. P. He, "Comment on 'Experimental single qubit quantum secret sharing'," *Phys. Rev. Lett.* 98, 028901 (2007); Schmid et al., Reply, *Phys. Rev. Lett.* 98, 028902 (2007). https://www.xqp.physik.uni-muenchen.de/publications/articles/articles_2007/prl_98_028902.html
10. G. P. He, Z. D. Wang, "Single qubit quantum secret sharing with improved security," arXiv:quant-ph/0703159 (2007, rev. 2011).
11. S.-J. Qin, F. Gao, Q.-Y. Wen, F.-C. Zhu, "Cryptanalysis of the Hillery–Bužek–Berthiaume quantum secret-sharing protocol," *Phys. Rev. A* 76, 062324 (2007). arXiv:0801.2418
12. F. Gao, S.-J. Qin, Q.-Y. Wen, F.-C. Zhu, "A simple participant attack on the Brádler–Dušek protocol," *Quantum Inf. Comput.* 7, 329 (2007).
13. Z.-J. Zhang, Y. Li, Z.-X. Man, "Multiparty quantum secret sharing," *Phys. Rev. A* 71, 044301 (2005).
14. F.-G. Deng, X.-H. Li, H.-Y. Zhou, Z.-J. Zhang, "Improving the security of multiparty quantum secret sharing against Trojan horse attack," *Phys. Rev. A* 72 (2005). arXiv:quant-ph/0506194
15. F.-G. Deng, P. Zhou, X.-H. Li, C.-Y. Li, H.-Y. Zhou, "Robustness of two-way quantum communication protocols against Trojan horse attack," arXiv:quant-ph/0508168 (2005).
16. F.-L. Yan, T. Gao, "Quantum secret sharing between multiparty and multiparty without entanglement," *Phys. Rev. A* 72, 012304 (2005).
17. F.-G. Deng, F.-L. Yan, X.-H. Li, C.-Y. Li, H.-Y. Zhou, T. Gao, "Addendum to 'Quantum secret sharing between multiparty and multiparty without entanglement'," arXiv:quant-ph/0508171 (2005).
18. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Phys. Rev. A* 73, 022320 (2006). arXiv:quant-ph/0507063
19. J. H. Shi, S. L. Zhang, H. L. Zhang, Z. G. Chang, "One-insider attack of quantum secret sharing protocol with collective eavesdropping-check," *Quantum Inf. Process.* 13(1), 33–42 (2014). https://pure.bit.edu.cn:443/en/publications/one-insider-attack-of-quantum-secret-sharing-protocol-with-collec
20. Z. Gao et al., "Measurement-device-independent protocol for deterministic quantum secret sharing," *Sci. China Phys. Mech. Astron.* 63(12), 120311 (2020).
21. Y.-G. Yang, Y.-C. Wang, Y.-L. Yang, X.-B. Chen, D. Li, Y.-H. Zhou, W.-M. Shi, "Participant attack on the deterministic measurement-device-independent quantum secret sharing protocol," *Sci. China*

Phys. Mech. Astron. 64(6), 260321 (2021). https://ir.bjut.edu.cn/item/261870

22. Y.-G. Yang, X.-X. Liu, S. Gao, X.-B. Chen, D. Li, Y.-H. Zhou, W.-M. Shi, "A stronger participant attack on the measurement-device-independent protocol for deterministic quantum secret sharing," *Quantum Inf. Process.* 20(7) (2021). https://ir.bjut.edu.cn/item/288936
23. C.-W. Tsai, C.-W. Yang, J. Lin, Y.-C. Chang, R.-S. Chang, "Cryptanalysis of limited resource semi-quantum secret sharing," *Quantum Inf. Process.* 19 (2020). doi:10.1007/s11128-020-02690-w
24. S. Li, X.-Q. Cai, S.-J. Song, C.-Y. Wei, T.-Y. Wang, "Cryptanalysis of efficient controlled semi-quantum secret sharing protocol with entangled state," *Sci. Rep.* 15, 15018 (2025). doi:10.1038/s41598-025-98734-1
25. D. Markham, B. C. Sanders, "Graph states for quantum secret sharing," *Phys. Rev. A* 78, 042309 (2008).
26. B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, M. S. Tame, "Experimental demonstration of graph-state quantum secret sharing," *Nat. Commun.* 5, 5480 (2014).
27. I. Kogias, Y. Xiang, Q. He, G. Adesso, "Unconditional security of entanglement-based continuous-variable quantum secret sharing," *Phys. Rev. A* 95, 012315 (2017). arXiv:1603.03224
28. W. P. Grice, B. Qi, "Quantum secret sharing using weak coherent states," *Phys. Rev. A* 100, 022339 (2019). arXiv:1906.10488
29. Q. Liao, Z. Fei, L. Huang, X. Fu, "Practical continuous-variable quantum secret sharing using local local oscillator," arXiv:2407.13983 (2024).
30. S. Liu, Z. Lu, P. Wang, Y. Tian, Q. Lu, X. Wang, Y. Li, "Experimental demonstration of multiparty quantum secret sharing and conference key agreement," *npj Quantum Inf.* 9, 92 (2023). doi:10.1038/s41534-023-00763-z
31. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nat. Photonics* 4, 686–689 (2010).
32. V. Makarov, D. R. Hjelme, "Faked states attack on quantum cryptosystems," *J. Mod. Opt.* 52, 691–705 (2005).
33. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A* 78, 042333 (2008).
34. G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.* 85, 1330 (2000).
35. W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Phys. Rev. Lett.* 91, 057901 (2003).
36. H.-K. Lo, X. Ma, K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.* 94, 230504 (2005).
37. H.-K. Lo, M. Curty, B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.* 108, 130503 (2012).
38. Y. Fu, H.-L. Yin, T.-Y. Chen, Z.-B. Chen, "Long-distance measurement-device-independent multiparty quantum communication," *Phys. Rev. Lett.* 114, 090501 (2015).
39. C.-L. Li, Y. Fu, W.-B. Liu, Y.-M. Xie, B.-H. Li, M.-G. Zhou, H.-L. Yin, Z.-B. Chen, "Breaking the rate-distance limitation of measurement-device-independent quantum secret sharing," *Phys. Rev. Research* 5, 033077 (2023). doi:10.1103/PhysRevResearch.5.033077

40. C. Zhang et al., "Memory-assisted measurement-device-independent quantum secret sharing," arXiv:2405.16970 (2024).
41. X.-Q. Cai, Z.-F. Liu, T.-Y. Wang, "Measurement-device-independent quantum secret sharing," arXiv:2305.10755 (2023).
42. T. Liu, J. Lai, Z. Li, T. Li, "Measurement-device-independent quantum-secret-sharing networks with linear Bell-state analysis," arXiv:2410.23562 (2024).
43. Q. Zhang et al., "Device-independent quantum secret sharing with noise preprocessing and postselection," arXiv:2403.10137 (2024).
44. Q. Zhang, J.-W. Ying, Z.-J. Wang, W. Zhong, M.-M. Du, S.-T. Shen et al., "Device-independent quantum secret sharing with advanced random key generation basis," arXiv:2410.04003 (2024).
45. Q. Zhang, C. Zhang, W. Zhong, M.-M. Du, L. Zhou, Y.-B. Sheng, "High-efficient long-distance device-independent quantum secret sharing based on single-photon sources," arXiv:2505.10797 (2025).
46. S. Majhi, G. Paul, "Device independent quantum secret sharing using multiparty pseudo-telepathy game," arXiv:2512.09699 (2025; rev. Jan. 2026).
47. S. Gogioso, "Device-independent quantum secret sharing using Mermin-type contextuality," arXiv:1510.05044 (2015).
48. R. M. J. Brooks, J. Ho, J. Niblo, J. Memmen, A. Pappa, J. Eisert, N. Walk, A. Fedrizzi, "High-rate multipartite quantum secret sharing with composable security," arXiv:2609.13367 (Sept. 2026).
49. S. Majhi et al., "Collusion-secure semi-quantum secret sharing scheme using a quantum third party," arXiv:2610.10176 (Oct. 2026).
50. C.-W. Tsai, C.-H. Wang, J. Lin, C.-W. Yang, "Multiparty-to-multiparty mediated quantum secret sharing protocol in a restricted quantum environment," *EPJ Quantum Technol.* 12, 99 (2025). doi:10.1140/epjqt/s40507-025-00404-8
51. J. Cao, J. Xu, "Efficient (k, n) threshold semi-quantum secret sharing protocol," *Front. Phys.* 13, 1542675 (2025). doi:10.3389/fphy.2025.1542675
52. K. Xing, R. Lu, S. Liu, L. Lan, "An efficient and secure semi-quantum secret sharing scheme based on W state sharing of specific bits," *Entropy* 27(11), 1107 (2025). https://www.mdpi.com/1099-4300/27/11/1107
53. F. He, X. Xin, C. Li, F. Li, "Semi-quantum secret sharing protocol based on decoy particles carrying secret information," *Quantum Inf. Process.* 24(8), 258 (2025). doi:10.1007/s11128-025-04872-w
54. H.-L. Yin, J.-Y. Shen, N. Chen, Z.-B. Chen, "Research status and prospects of quantum secret sharing," *Acta Phys. Sin.* 74(16), 160301 (2025). doi:10.7498/aps.74.20250586
55. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.* 92, 025002 (2020).
56. S. Pirandola et al., "Advances in quantum cryptography," *Adv. Opt. Photon.* 12, 1012–1236 (2020).
57. H.-X. Ma, W.-S. Bao, H.-W. Li, C. Zhou, "Quantum hacking of two-way continuous-variable quantum key distribution using Trojan-horse attack," *Chin. Phys. B* 25(8), 080309 (2016). https://cpb.iphy.ac.cn/EN/10.1088/1674-1056/25/8/080309
58. A. Kate, P. Mukherjee, H. Saleem, P. Sarkar, R. Sinha, "Practical post-quantum secure publicly verifiable secret sharing and applications," *Cryptology ePrint Archive* 2026/813 (2026). https://eprint.iacr.org/2026/813
59. C. Portmann, R. Renner, "Security in quantum cryptography," *Rev. Mod. Phys.* 94, 025008 (2022).

60. G. Murta, F. Grasselli, H. Kampermann, D. Bruß, "Quantum conference key agreement: A review," *Adv. Quantum Technol.* 3, 2000025 (2020).
61. G. Gao, "Comment on 'Cryptanalysis and improvement of multiparty quantum secret sharing schemes'," arXiv:1107.4529 (2011).
62. T.-Y. Wang, Y.-P. Li, "Cryptanalysis of dynamic quantum secret sharing," *Quantum Inf. Process.* 12, 1991–1997 (2013). doi:10.1007/s11128-012-0508-2
63. S. Roy, S. Mukhopadhyay, "(t, n) threshold d-level quantum secret sharing based on quantum Fourier transformation," arXiv:2009.14598 (2020).
64. S. Luo, Z. Li, D. Meng, J. Guo, "Efficient quantum secret sharing scheme based on monotone span program," arXiv:2303.00226 (2023); published version doi:10.1088/1555-6611/acd630.
65. L. Li, Z. Li, "An efficient quantum secret sharing scheme based on restricted threshold access structure," *Entropy* 25(2), 265 (2023). doi:10.3390/e25020265
66. X. Yang, K. Wei, H. Ma, S. Sun, H. Liu, Z. Li, Z. Yin, Y. Du, L. Wu, "Measurement-device-independent quantum secret sharing," arXiv:1608.00114 (2016).
67. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.* 98, 230501 (2007).
68. D. P. Nadlinger et al., "Experimental quantum key distribution certified by Bell's theorem," *Nature* 607, 682–686 (2022).