Quantum Secure Key Exchange with Position-based Credentials

Wen Yu Kon, Ignatius William Primaatmaja, Kaushik Chakraborty, and Charles Lim
Global Technology Applied Research, JPMorganChase
(Dated: June 12, 2025)

Quantum key distribution (QKD) provides an information-theoretic way of securely exchanging secret keys, and typically relies on pre-shared keys or public keys for message authentication. To lift the requirement of pre-shared or public keys, Buhrman et. al. [SIAM J. Comput. 43, 150 (2014)] proposed utilizing the location of a party as a credential. Here, we extend upon the proposal, develop a QKD protocol with location credentials using *quantum position verification* (QPV) based message and identity authentication. By using QKD with delayed authentication as a base, and later simplifying QPV-based message authentication, we significantly reduce the number of QPV runs, which currently acts as a bottleneck. Besides demonstrating security for the proposed protocol, we also provide improvements to QPV security analysis, including generalization of the QPV adversary model, tightening a trace distance bound using semidefinite programming, and propose a multi-basis QPV requiring only BB84 state preparation but with multiple measurement basis.

I. INTRODUCTION

As quantum computation capabilities continue to advance, there are increasing concerns that current public key cryptographic systems such as RSA may one day become vulnerable [1]. To guard against harvest now decrypt later attacks on secure communication networks, *quantum key distribution* (QKD) has been proposed as a possible solution. Since the early proposals for QKD implementations [2–4], the security and hardware technology has significantly improved [5, 6], and multiple commercial QKD devices are currently available in the market.

QKD in practice requires pre-shared keys for secure authentication [6, 7], though the use of public key infrastructure for message authentication has been proposed as well [8]. Manual delivery of such pre-shared keys can be onerous, and could in general lead to issues for instance if the pre-shared keys are used up in a denial-of-service attack. In some instances, QKD devices are deployed at trusted location, for instance in data centers, where strict physical security practices are implemented. As such, we can explore a different method of authentication – using the location of the QKD device, or more specifically the spacetime coordinate (P, T) to provide identity authentication.

To realize position-based identity authentication, we rely on *quantum position verification* (QPV), which has received increased attention from the community. QPV serves as a protocol to certify the spacetime coordinate of a party, and any adversary at a different location cannot impersonate one at the right location. After the first proof of security against linearly entangled adversaries [9], results allowing slow quantum communication [10], channel loss tolerance [11], and security against adversaries with linear quantum gates [12]. More recently, a preliminary result for the implementation of SWAP QPV has be presented [13], signaling interest to bring the protocol from theory to reality.

Ref. [14] proposed a QPV-based message authentication protocol, and suggested that utilizing the message authentication protocol to send authenticated messages from Alice to Bob is sufficient for QKD security. This could remove any requirements for pre-shared keys or public key infrastructure for QKD, relying instead on the position of a party for authentication. However, the proposed protocol may not provide sufficient security since Bob has no method of authenticating Alice, i.e. Eve can impersonate Alice and trick Bob into sharing a secret key with Eve[1].

Here, we first expand on the proposal by Buhrman et. al. [14] in a similar adversary model where one-way authentication from Alice to Bob is implicitly assumed. In this scenario, Alice trusts any party that is at location P at time T, and her goal is to exchange keys securely with this party. By relying on QKD protocols where authentication is deferred to the final step [15, 16], the requirements for Bob's authentication can be reduced from multiple QPV runs for message authentication to a single QPV run since only a single bit is necessary for the final authentication step.

We further extend the protocol to a more general model where Alice and Bob share no authenticated channels. This requires replacing Alice's final authenticated communication to Bob with a similar QPV-based message authentication sub-protocol. The QPV-based message authentication sub-protocol we developed integrates Buhrman et. al.'s message authentication protocol [14] with symmetric key authentication, significantly reducing the number of QPV runs required

[1] We note that while the proposed scheme with Alice being the verifiers of QPV cannot provide sufficient security, it is simple to extend the proposal to one where Bob also has separate trusted verifiers that can perform QPV to receive authenticated messages from Alice.

by sending only the key required for symmetric key authentication via Buhrman et. al.'s message authentication protocol. A formal security proof for the full protocol, taking into account also possible differences in abort decisions by Alice and Bob due to lack of ideal authentication, is provided. Interestingly, the proposed protocols has two useful properties: (1) anonymity and (2) decoupling of QKD and QPV process, that may lead to a wider range of applications not afforded to standard QKD.

While the technology and security analysis for QKD is well-established, the same is not true for QPV. As such, improvements in both security analysis and experimental design are necessary to improve the practicality of QPV. As a step towards practical QPV implementation, we provide a series of improvements to QPV security analysis to (1) account for more general adversaries, (2) tighten security bounds, and (3) providing improvements in multi-basis QPV protocol design that can reduce implementation complexity.

In Sec. II, we introduce quantum theory and quantum position verification. Sec. III proposes the key exchange protocol with one-way authentication along with its security analysis, which is further extended to key exchange with location credentials in Sec. IV. Improvements to QPV security and implementation is provided in Sec. V. The paper ends with a discussion in Sec. VI and conclusion in Sec. VII.

More recently, Ref. [17] introduced a tightened security analysis for QPV without qubit loss and achieved a higher error tolerance. It remains to be seen how their analysis can be adapted to a QPV with loss and how the generalizations and improvements presented in this manuscript may be used to strengthen their analysis.

II. PRELIMINARIES

A. Quantum Theory

We define a generic quantum system A by a density matrix ρ_A with unit trace $\mathrm{Tr}[\rho_A] = 1$ and positive semidefinite $\rho_A \geq 0$. A classical system X can be represented as a quantum state $\rho_X = \sum_{x\in\mathcal{X}} p_x \left|x\right\rangle\!\left\langle x\right|_X$, where $p_x = \Pr[X = x]$. Uniformly distributed classical systems can be represented as $\tau_X = \frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}} \left|x\right\rangle\!\left\langle x\right|_X$, while uniformly distributed and matching classical systems X and X' can be represented as $\tilde{\tau}_{XX'} = \sum_{x\in\mathcal{X}} \frac{1}{|\mathcal{X}|} \left|xx\right\rangle\!\left\langle xx\right|_{XX'}$. A classical-quantum state with classical random variable X and quantum subsystem A can be expressed as

$$\rho_{XA} = \sum_{x\in\mathcal{X}} p_x \left|x\right\rangle\!\left\langle x\right|_X \otimes \rho_{A|X=x},$$

where $\rho_{A|X=x}$ is the state of subsystem A conditioned on $X = x$. In general, we label a quantum state conditioned on an event Ω as $\rho_{A|\Omega}$, and we let $\rho_{A\wedge\Omega} = \Pr[\Omega]\rho_{A|\Omega}$. To study the distinguishability of two quantum systems ρ and σ, we use the trace distance measure,

$$\Delta(\rho,\sigma) := \frac{1}{2}\|\rho - \sigma\|_1, \tag{1}$$

where $\|\cdot\|_1$ is the trace norm.

Any general quantum process can be described by a quantum channel that maps input system I to output system O, with fixed inputs x. We label such channels $\mathcal{E}_I^x$, noting the output system is typically obvious. Quantum systems can be measured to give an outcome, and we define a quantum measurement as a positive-valued operator measure (POVM) A_x^θ (or B, for Alice or Bob's measurement operators), where θ is the basis choice, and x is the measurement outcomes.

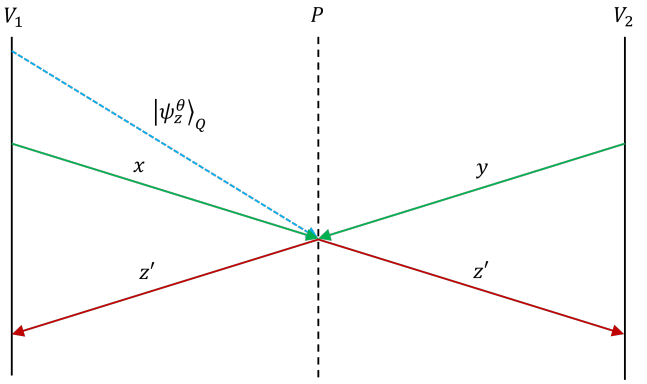

FIG. 1. Spacetime diagram illustrating the classical and quantum communication in $QPV_{BB84}^{\eta,f}$ QPV protocol. Note that the solid lines represent classical communication which occurs at the speed of light while the dotted lines represent quantum communication.

B. Quantum Position Verification

QPV has been shown to be secure against adversaries with linear quantum memory size in Ref. [10], and we briefly present the protocol here. Consider a scenario where a prover is at location P and is co-linear with two verifiers V_1 and V_2. A loss tolerant QPV protocol, labeled $QPV_{BB84}^{\eta,f}$ follows (illustrated in Fig. 1):

1. **Verifier Preparation**: Verifiers V_1 and V_2 randomly select $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$. Verifiers also agree on a time t_0.
2. **Quantum State Transfer**: The first verifier computes $\theta = f(x,y)$ and randomly selects $z \in \{0,1\}$. He then prepares a BB84 state $\left|\psi_z^\theta\right\rangle_Q$ with basis θ and bit value z and sends it to the prover.
3. **Verifier Message**: The verifiers sends x and y such that they both arrive at P at time t_0.

4. **Prover Measurement**: Prover computes $\theta = f(x, y)$ and measures the quantum system Q in basis θ. He immediately sends the outcome z' to both verifiers. If quantum system Q is lost, the prover responds with $\perp$ to both verifiers.

5. **Timing and Validity Check**: The verifiers check if the time they receive the response z' is within certain time threshold and if the responses between verifiers match. Furthermore, the QPV process can be repeated for multiple rounds, and an error rate corresponding to the proportion of rounds where $z \neq z'$ can be computed. QPV can be determined by the verifiers to fail if the time threshold or mismatch of responses occur in any round or if the error rate exceeds some error threshold.

The security of QPV protocol relies on the observation that (1) parties not at location P cannot obtain x and y before the party at location P and (2) quantum information in Q cannot be duplicated, and thus would be unable to respond the correct z' to the verifiers.

III. SECURE KEY EXCHANGE WITH ONE-WAY LOCATION AUTHENTICATION

A. Security Model

In general, there can be multiple methods of combining QKD and QPV into a secure key exchange protocol with some sort of location verification. This would lead to differences in applicability and functionality of the protocols, which depend heavily on the trust and adversary models. One simple model would be to have trusted Alice and Bob just like QKD, but where Alice do not trust the claimed location of Bob. Here, the purpose of QKD and QPV is fully separate, where QKD can be used to perform key exchange since both parties are trusted, and QPV is used to certify the location of Bob at some time T, which may occur during the QKD protocol. However, in this context, we do not truly use the location of Bob as a credential since implicit trust is afforded to him for QKD.

To truly consider the use of a spacetime coordinate as credential, we have to instead assume that any party at this spacetime coordinate has no other credentials, including no access to any method of sending authenticated messages. Moreover, since the spacetime coordinate is the sole credential, we have to assume Alice places full trust on any party at this spacetime coordinate. This placement of trust can rely for instance on physical security at the data centers, where only authorized personnel can gain access to location P at some time T. The goal would be then for Alice and any party at location P and time T to establish secure keys, without any other means of identification of the party other than its location (e.g. with pre-shared keys or public key infrastructure (PKI)). We note here that Alice is allowed to send authenticated messages, though extensions to have both Alice and Bob use location credentials is presented later in Sec. IV.

More formally, we consider a model where Bob is the collection of all parties that will be at location P at time T, and the goal would be for Alice to exchange secret keys with Bob (or one of the parties constituting Bob). We note here that as a consequence of the trust model, any party that is at location P at time T can technically exchange keys with Alice. In this case, Eve would be the collection of all parties that will not be at location P at time T. We also introduce a list of assumptions, including standard QKD assumptions, QPV assumptions and specific model-based ones:

- Alice and Bob's QKD devices are trusted.
- The QPV verifiers are honest.
- Bob is honest, i.e any party at location P at time T is honest[2].
- Alice can send authenticated messages (e.g. by PKI).
- Bob (Parties at location P and time T) is unable to send any authenticated messages.
- The adversary's strategy is limited by similar restrictions placed on the adversary in QPV. This could vary based on the QPV security analysis of interest, but could include bounded quantum memory [10] and linear quantum gates [12][3].

With these set of assumptions, let us consider the ideal functionality for secure key exchange. Since Bob is defined to be the collection of parties that will be at location P at time T, Bob is allowed to share the secret keys. Consequently, we can consider a similar security definition as QKD. We note that in general, the protocol (like QKD) cannot defend against denial-of-service attacks, and therefore may abort. As a result, we can introduce a probability of the protocol aborting, $(1-\tilde{p})$, and an implicit indicator $I_{\tilde{\Omega}}$ as part of E subsystem to indicate if the keys are to be generated,

$$\rho^{\text{ideal}} = \tilde{p}\,\tilde{\tau}_{K_A K_B} \otimes \sigma_E^{\top} + (1-\tilde{p})\,|\perp\perp\rangle\langle\perp\perp|_{K_A K_B} \otimes \sigma_E^{\perp}, \tag{2}$$

where the separate σ_E states can be generated locally by Eve. We note that the fact that Alice does not share a QKD key with parties not at location P at time T is embodied by Eve remaining independent of K_A when

[2] This assumption is necessary, otherwise the key exchange can simply fail, for instance by Bob announcing his raw keys.

[3] We note that since QKD is secure against unbounded adversaries, QKD remains secure against such restricted adversaries as well.

Protocol 1 Secure Key Exchange with One-way Location Authentication

Goal. Alice and Bob performing key exchange with the aid of two verifiers.

1. **Quantum Transmission Phase**: Alice and Bob transfer quantum information, and at the end of the step, Alice and Bob generates raw keys S_A and S_B respectively.
2. **Sifting and Error Correction**: Alice and Bob exchange classical information $M = (M_A, M_B)$, where M_A are messages from Alice to Bob and M_B are messages from Bob to Alice. Messages sent from Alice to Bob are sent through a one-way authenticated channel. Alice and Bob use these messages, along with their respective raw keys to perform sifting and error correction and parameter estimation, where they jointly decide on an indicator I_{PE} indicating if parameter estimation has passed or failed.
3. **Alice's Authenticated Message**: Alice randomly selects a hash function h from a family of hash functions $\mathcal{H}$ and compute the hash of the messages $\hat{M}_B$ she received from Bob. Alice sends the computed hash value $h(\hat{M}_B)$ to Bob via the one-way authenticated channel.
4. **Message Check**: Bob uses the received hash function h computes a hash of his messages, $h(M_B)$, and checks if it matches the hash received, i.e. if $h(M_B) = h(\hat{M}_B)$. If they match, Bob labels an indicator $I = 1$, otherwise they label the indicator $I = 0$.
5. **Quantum Position Verification Sub-protocol**: Alice initiates a QPV sub-protocol. If Bob's indicator signals that the hash matches ($I = 1$), Bob behaves honestly in the QPV. Otherwise, Bob does not provide responses during the QPV. At the end of the sub-protocol, Alice should have received the QPV indicator I_{QPV}, and shared I_{QPV} with Bob.
6. **Privacy Amplification**: If the QPV indicator indicates that QPV passed, $I_{QPV} = 1$, and the parameter estimation passed, $I_{PE} = 1$, Alice and Bob performs privacy amplification independently to generate QKD secret keys K_A and K_B. If either parameter estimation or QPV failed, Alice and Bob aborts the protocol.

keys are generated. We can thus define the security with the trace distance from the ideal functionality

$$\Delta(\rho, \rho^{\text{ideal}}) \leq \varepsilon, \tag{3}$$

where ε is the security parameter for the protocol, and ρ^{ideal} can be any ideal state of the form above.

B. Protocol

The protocol defined relies on QKD protocols where Bob's authentication is left to the final steps [15, 16]. Such QKD protocols can be performed with only one-way authentication, with the final steps of having Alice send a hash of messages received from Bob, for which Bob can check if such messages have been tampered with. This can end with Bob responding with a single bit on whether the QKD protocol should be aborted (e.g. messages tampered), and this is typically send via an authenticated channel[4]. The proposed protocol replaces this final authentication step with a QPV sub-protocol, where Bob (in our case parties with spacetime coordinate (P, T)) can either choose to act honestly to inform Alice that the protocol should not be aborted, or provide no responses to trigger an abort. Taking h to be a 2-universal hash function, the proposed protocol can be summarized in Protocol 1.

C. Security Analysis

In the protocol, an abort occurs when either parameter estimation fails or the QPV check fails. Let us define the events Ω_{PE} and Ω_{QPV} as the event where parameter estimation passes and the event where QPV passes respectively, and let $\Omega = \Omega_{PE} \wedge \Omega_{QPV}$. This event Ω also signals that QKD keys are generated, i.e. the protocol did not abort[5]. The actual protocol output state can thus be expressed as

$$\begin{aligned}\rho =& p_\Omega \left|1\right\rangle\!\left\langle 1\right|_{I_\Omega} \otimes \rho_{K_A K_B E|\Omega} \\ &+ p_{\Omega^c} \left|0\right\rangle\!\left\langle 0\right|_{I_\Omega} \otimes \left|\perp\perp\right\rangle\!\left\langle\perp\perp\right|_{K_A K_B} \otimes \rho_{E|\Omega^c},\end{aligned} \tag{4}$$

where keys are generated only for event Ω.

Formally, the security can be given by

[4] Standard QKD protocols with two-way authentication may not directly translate, since careful design may be required. For instance, we cannot allow Bob's response to the end of the quantum information exchange step to be a simple "received" and Alice replying with her basis choice since it can be easily compromised by performing suitable delay attacks.

[5] Note that WLOG, assuming one-way authenticated channel (without failure) from Alice to Bob, both parties can jointly abort or generate keys (with instructions from Alice). If we relax the assumption on Alice's authentication channel to allow for events where the message is not received or the authentication fails, we have to use analysis similar to that in Sec. IV to account for this difference. However, since this is not the focus of this section, we assume no authentication failure for simplicity.

Theorem 1. *Let ρ^{ideal} be the ideal output state as defined in Eq. (2). Then,*

$$\Delta(\rho_{K_A K_B E}, \rho^{ideal}_{K_A K_B E}) \leq \varepsilon_{QKD} + \frac{1}{l_T} + \varepsilon_{QPV},$$

where ε_{QKD} is the QKD security parameter, l_T is the length of the hash $h(M_B)$ and ε_{QPV} is the winning probability of QPV for an adversary not at position P at time T.

Proof. Refer to Appendix A □

IV. SECURE KEY EXCHANGE WITH LOCATION CREDENTIALS

A. Security Model

Protocol 1 can be extended to one where no authentication channels exists between Alice and Bob, relying instead on location credentials for authentication. Unlike the earlier replacement of the Bob's single bit authenticated response with a single QPV sub-protocol, we require instead a proper message authentication step to replace the step of sending Alice's authenticated message. The QPV-based message authentication protocol in Ref. [14] is a suitable candidate to perform a similar function, though we provide simplifications to improve its performance.

The security model adopted here is similar to that in Sec. III A, with the main difference being Alice's ability and assumptions relating to the QPV-based message authentication protocol. Here, we consider a model where Alice is the collection of all parties at location P_A at time T, and Bob to be the collection of all parties at location P_B at time T', and the goal is for parties at P_A and P_B to securely exchange keys. Since authentication of Alice and Bob are based on the spacetime coordinates alone and require separate verifications, we assume the parties P_A and P_B have access to trusted verifiers (or the parties can individually control parties at locations necessary to act as verifiers in the QPV). Note that Alice and Bob do not have to share the same trusted verifiers, and we will label them Alice verifiers and Bob verifiers according to the party that trusts them. We can thus introduce the set of assumptions:

- Alice and Bob's QKD devices are trusted.
- Alice's and Bob's verifiers are honest.
- Alice (parties at P_A) and Bob (parties at P_B) are honest.
- Neither Alice nor Bob can send any authenticated messages to one another.
- Alice and Bob share an authenticated channel with their respective verifiers.
- Alice and Bob's verifiers devices which performs QPV (for sending authenticated messages) are inbuilt with fixed duration between internal QPV rounds and between entire QPV runs, and the delay between entire QPV runs, Δt, is larger than the duration for each QPV run.
- The adversary's strategy is limited by similar restrictions placed on the adversary in QPV.

Without any ideal authenticated channels, one is no longer able to have Alice and Bob synchronize their key generation. In this instance, it is possible for Bob to generate keys while Alice does not [6, 15, 16]. This is mainly due to an adversary's ability to interfere with the final authentication step (in our case, step 5 of Protocol 1), forcing Alice to abort while Bob have already decided to generate his keys at an earlier step. Therefore, we define a slightly different ideal functionality,

$$\begin{aligned}\rho^{\text{ideal}} = p_{11}\,\tilde{\tau}_{K_A K_B} \otimes \sigma_E^{11} + p_{01}\,|\perp\rangle\langle\perp|_{K_A} \otimes \tau_{K_B} \otimes \rho_E^{01} \\ + p_{00}\,|\perp\perp\rangle\langle\perp\perp|_{K_A K_B} \otimes \sigma_E^{00},\end{aligned} \tag{5}$$

where $p_{00} + p_{01} + p_{11} = 1$, and for secrecy reasons we expect the key K_B to remain secret from any adversary when Alice aborts the protocol.

B. Sending Authenticated Messages with QPV

Buhrman et. al. [14] proposed a message authentication protocol using QPV by assigning the pass/fail of QPV runs as bits 0 and 1, and demonstrated security when proper encoding is utilized. Here, we present an improvement to the protocol by combining it with symmetric key message authentication – using QPV to send the key instead of the full message to reduce QPV runs. We utilize a δ-almost 2-universal hash family $\{h_k : \{0,1\}^n \to \{0,1\}^{l_T}\}_{k\in\mathcal{K}}$, noting that there exists such families with small key length, $l_K = 2\lfloor l_T + \log_2(\frac{n}{l_T}) + 1\rfloor$ with $\delta = 2^{-l_T+1}$ [18].

Intuitively, an adversary not at the right location cannot pass QPV with high probability, thereby allowing him to easily change message bits from 1 to 0 (pass to fail) but not from 0 to 1 (fail to pass). Therefore, to send a message $K \in \{0,1\}^{l_K}$, we encode the message in a codebook with codewords $\{c \in \{0,1\}^{2l_C+2} : HW(c) = l_K + 2, c_1 = c_{2l_C+2} = 1\}$, where $HW(c)$ refers to the Hamming weight of codeword c. For an injective encoding map, we can choose $l_C = \lceil l'_C \rceil$ such that $\binom{2l'_C}{l'_C} > 2^{l_K}$. We label the encoding function $enc : K \to C$ and the decoding function $dec : C \to K$.

We also consider a general QPV sub-protocol, which has a starting time t_{start}. The protocol is assumed to be ε_{rob}-robust (probability of failing QPV when all

Protocol 2 Sending Authenticated Messages with Location Credentials

Goal. Sender sends an authenticated message $M \in \{0,1\}^n$ to the receiver.

1. **Message Exchange**: Message M sent from sender to receiver.
2. **Tag Generation**: Sender randomly selects a key $K \in \{0,1\}^{l_K}$ and generates a tag by hashing the message $T = h_K(M)$. The sender sends the tag T to the receiver.
3. **Encoding Phase**: Sender encodes key into a codeword $C = enc(K)$.
4. **Synchronization Signal**: The sender and receiver agree on a time t_{start} to begin the message transfer.
5. **QPV Sub-protocol Runs**: Repeat for $i = 1, \cdots, 2l_C + 2$:
   (a) Receiver performs a QPV sub-protocol with the sender at $t_{start} + (i-1)\Delta t$.
   (b) If $C_i = 0$, the sender provides no response (i.e. $\perp$), while if $C_i = 1$, the sender replies with honest responses.
   (c) Receiver records $\hat{C}_i = 0$ if the QPV fails and $\hat{C}_i = 1$ if the QPV passes.
6. **Tampering Check**: The receiver checks that $\hat{C}_1 = \hat{C}_{2l_C+2} = 1$ and $HW(\hat{C}) = l_C + 2$. If any checks fail, the protocol is aborted.
7. **Key Decoding**: If the checks pass, the receiver decodes key $\hat{K} = dec(\hat{C})$. Otherwise, the message authentication is deemed to have failed.
8. **Message Authentication**: The receiver hashes the received message $\hat{M}$ and checks if it matches the received tag, i.e. $\hat{T} = h_{\hat{K}}(\hat{M})$. The message authentication passes if a match is obtained.

parties are honest) and ε_{QPV}-sound (probability of adversary forcing QPV to pass). For QPV sub-protocols that requires multiple internal rounds, the security model assumes a pre-agreed delay as prescribed by the protocol, and appropriate timings selected by the sender and receivers with respect to t_{start}, i.e. once t_{start} is synchronized, the QPV sub-protocol runs in a synchronized manner. Across different QPV sub-protocols, a pre-agreed delay Δt is assumed. We note that such assumptions can be rationalized as a manufacturer's design choice, where a QPV device may have fixed intervals for QPV rounds. These assumptions would help simplify the security analysis and prevent many of the synchronization issues highlighted in Ref. [14].

The protocol is presented in Protocol 2, where a tag is generated before the key K is sent from Alice to Bob via $2l_C + 2$ QPV runs. With K sent in an authenticated manner, Bob can use the same hash function to check that the messages that Alice and Bob send and receive matches.

The security of the protocol can be guaranteed from the δ-almost strongly 2-universal property of the hash function to prevent messages M and $\hat{M}$ from mismatch and the QPV sub-protocols, which prevents the tampering of the hash key K being sent from Alice to Bob. More formally, the protocol security can be summarized as

Theorem 2. *If an ε_{rob}-robust, ε_{QPV}-sound QPV sub-protocol and a δ-almost strongly 2-universal family of hash function with key size l_K is utilized, Protocol 2 is $(\lceil \frac{l_K}{2} \rceil + 2)\varepsilon_{rob}$-robust and $(\delta + 2\lceil \frac{l_K}{2} \rceil \varepsilon_{QPV})$-secure, i.e.*

$$\Pr\left[M \neq \hat{M},\ accept\right] \leq \delta + 2\lceil \frac{l_K}{2} \rceil \varepsilon_{QPV}.$$

Proof. See Appendix B. □

C. Secure Key Exchange Protocol

Protocol 1 replaces the final authentication step by a QPV sub-protocol. Here, we further replace the second last authentication step from Alice to Bob by simply sending authenticated messages with QPV-based message authentication. Let $M = (M_A, \hat{M}_B)$ be the classical messages Alice possess, including messages she sent and messages she received from Bob, and let $M' = (\hat{M}_A, M_B)$ be the classical messages Bob possess. Let h_K be a hash function chosen from a δ-almost strongly 2-universal family of hash functions, $\mathcal{H} = \{h_k : \{0,1\}^n \to \{0,1\}^t\}$. The modified protocol is presented as protocol 3.

At the end of the protocol, the overall state can be given by

$$\begin{aligned}\rho_{K_A K_B E} =& p_{11} \sum_{k_A k_B} |k_A k_B\rangle\langle k_A k_B|_{K_A K_B} \otimes \rho_E^{k_A k_B, 11} \\ &+ p_{01} \sum_k |\perp k\rangle\langle \perp k|_{K_A K_B} \otimes \rho_E^{k,01} \\ &+ p_{10} \sum_k |k \perp\rangle\langle k \perp|_{K_A K_B} \otimes \rho_E^{k,10} \\ &+ p_{00} |\perp\perp\rangle\langle\perp\perp|_{K_A K_B} \otimes \rho_E^{00}.\end{aligned} \tag{6}$$

Since the security can be defined by the trace distance between the final state and the ideal functionality, the trace distance naturally splits into cases which we can analyze separately:

Protocol 3 Secure Key Exchange with Location Credentials

Goal. Alice and Bob performing key exchange with the aid of verifiers.

1. **Quantum Transmission Phase**: Alice and Bob transfer quantum information, and at the end of the step, Alice generates an Alice raw key S_A and Bob generates a Bob raw key S_B.
2. **Sifting and Error Correction**: Alice and Bob exchange classical information (M_A, M_B), where M_A are messages from Alice to Bob and M_B are messages from Bob to Alice. They use these messages, along with their respective raw keys to perform sifting, error correction, and parameter estimation, where Alice and Bob arrive on indicators $I_{PE,A}$ and $I_{PE,B}$ respectively indicating if they think parameter estimation has passed or failed.
3. **Alice's Authenticated Message**: Alice randomly selects a seed $K \in \{0,1\}^m$ and computes a message tag $T = h_K(M)$. If $I_{PE,A} = 1$, Alice sends the computed tag T to Bob. Otherwise, Alice sends a random T to Bob.
4. **Authenticated Message Transfer**: After Bob receives the messages, he requests his verifiers to initiate location-based authentication sub-protocol with Alice to receive the seed K as the authenticated message. If $I_{PE,A} = 1$, Alice participates in the message transfer honestly. Otherwise, Alice chooses not to participate in the message transfer (i.e. provide no response to the QPV).
5. **Message Check**: Bob uses the received seed K to compute a tag from his classical messages $T' = h_K(M')$, and checks if it matches the tag received, i.e. if $\hat{T} = T'$. If they match, Bob labels an indicator $I = 1$, otherwise they label the indicator $I = 0$.
6. **Quantum Position Verification Sub-protocol**: Alice requests her verifiers to initiate a partial QPV sub-protocol. If Bob's indicator signals that the hash matches ($I = 1$) and believes parameter estimation passes ($I_{PE,B}$), Bob behave honestly in the QPV. Otherwise, Bob does not provide responses during the QPV. At the end of the sub-protocol, Alice should have received the QPV indicator I_{QPV}.
7. **Privacy Amplification**: If the QPV indicator indicates that QPV passed, $I_{QPV} = 1$, and the parameter estimation passed, $I_{PE,A} = 1$, Alice performs privacy amplification on her corrected keys to generate K_A. Otherwise, Alice aborts and sets $K_A = \perp$. If Bob's indicator $I = 1$ and parameter estimation passed, $I_{PE,B} = 1$, Bob performs privacy amplification on his corrected keys to generate K_B. Otherwise, Bob aborts and sets $K_B = \perp$.

1. Case 10: Bob does not participate in the QPV sub-protocol, which renders it challenging for an adversary to force the QPV sub-protocol to pass, i.e. p_{10} is small.
2. Case 01: Alice can fail to generate keys due to parameter estimation or the QPV sub-protocol. For the former, Alice's non-participation in sending key K makes it difficult for an adversary to pass the message authentication. For the latter, Alice parameter estimation passing and Bob's decision to generate a key means messages are not tampered with high likelihood (from security of sending authenticated messages) and thus keys are secret from QKD security.
3. Case 11: Similar to case 01, where both Alice's and Bob's decision to generate a key means keys are unlikely to be tampered with and thus keys are secret by QKD security.

More formally, the security can be presented as

Theorem 3. *Consider Protocol 3 with a QKD sub-protocol that is ε_{QKD}-secure, QPV sub-protocols that are ε_{QPV}-sound respectively, and a δ-almost strongly 2-universal family of hash functions f_K. Then, the Protocol 3 is $(2\varepsilon_{QKD} + 2\delta + (4\lceil \frac{l_K}{2} \rceil + 2)\varepsilon_{QPV})$-secure. Furthermore, the robustness of the protocol is bounded by $\varepsilon_{rob} = \varepsilon_{rob}^{QKD} + (\lceil \frac{l_K}{2} \rceil + 3)\varepsilon_{rob}^{QPV}$.*

Proof. See Appendix C. □

D. Applications

The protocol proposed can be utilized to address the criticism of requiring pre-shared keys in QKD. Here, the reliance on the spacetime coordinate alone to certify a party lifts the requirement of the pre-shared keys to authenticate messages. As such, it can be useful for QKD where the location of one or more QKD boxes can be trusted, e.g. in a data center.

Besides QKD, the range of applications that the proposed protocol is expanded due to two interesting properties: (1) anonymity and (2) decoupling of QKD and QPV processes. Since location information is sufficient to act as credentials, it brings up the possibility for multiple parties at the same location to generate a secret key, with the key exchange partner none the wiser who the keys are exchanged with. This could be for instance be useful in offices where employees can access databases without the database provider knowing the identity of the employee accessing the database.

The second property stems from the fact that the QKD sub-protocol for secure key exchange is not heavily intertwined with the QPV sub-protocol which dictates the spacetime coordinates. As such, there can be arbitrary delay between the two sub-protocols. This allows for extensions where the QKD sub-protocol can allow for the exchange of keys (or data that can be converted to keys),

and the parties holding onto the keys can later proceed to the two locations P_A and P_B respectively at some designated time T to "activate" the keys by performing the remaining QPV-based steps. It may also allow for delegation of authentication, such as access control. For example, a company's server can be present at P and time T, and an employee at the company wants to exchange keys with Alice. In this case, the employee can perform the QKD sub-protocol with Alice, and request the server to perform QPV to act honestly to "activate" the exchanged key.

V. IMPROVEMENTS TO QPV

A. Generalizing QPV Security

To better facilitate implementations of the proposed protocol, we attempt to improve the security analysis of the QPV sub-protocol, which is a heavy bottleneck in Protocol 3. Let us first generalize the argument of QPV security against entangled (bounded quantum memory) adversaries, before identifying the areas which are examined in this manuscript. In QPV, we can consider in general a pair of adversaries, Alice and Bob, whose aim is to have the verifiers certify that they are at location P when they are not. At the start of the protocol, the adversaries share a joint quantum system σ_{RAB}, where A and B are maximally of dimension 2^q each, and R is the shared randomness, which is classical and not bounded in size. The joint state can be expressed as $\sigma_{RAB} = \sum_r p_r |r\rangle\langle r|_R \otimes \sigma^r_{AB}$. The general attack can be described as follows (adapted from attack 3.2 of Ref. [10]):

1. Alice receives the qubit prepared by verifier 1, $|\psi^\theta_z\rangle_Q$, where the state is prepared in basis $\theta = f(x,y)$ and with bit value z.
2. Alice and Bob receive x and y respectively. They independently apply quantum channels $\mathcal{E}^{xr}_{AQ}$ and $\mathcal{E}^{yr}_B$ on their respective quantum subsystems, which may generate classical messages M_A and M_B to get $\rho^{xy}_{RM_AM_BQAB} = \sum_r p_r |r\rangle\langle r|_R \otimes \mathcal{E}^{xr}_{AQ}(|\psi^\theta_z\rangle\langle\psi^\theta_z|_Q \otimes \mathcal{E}^{yr}_B(\sigma^r_{AB}))$[6].
3. Alice and Bob redistribute their quantum subsystems, with Alice sending her message and part of her quantum sub-systems to Bob and vice versa. In other words, Alice splits $AQ \to A_1A_2$ and Bob splits $B \to B_1B_2$, with both parties sending out A_2 and B_2 respectively.
4. Alice and Bob receive the quantum states exchanged and the other bitstring, with $A' = A_1B_2$ and $B' = B_1A_2$.
5. Alice and Bob independently perform POVMs $\{A^{m_Am_Brxy}_{z_A}\}$ and $\{B^{m_Am_Brxy}_{z_B}\}$ on sub-systems A' and B' respectively, and responds with z_A and z_B respectively.

We note that there are five main areas of generalization over the current analysis [9, 10]:

1. The inclusion of shared randomness R.
2. The use of mixed states σ_{AB} instead of pure states.
3. Having general quantum channels $\mathcal{E}^{xr}_{AQ}$ and $\mathcal{E}^{yr}_B$ instead of assuming that the channels are unitaries.
4. Lifting the assumption that loss η is independent of inputs (x,y).
5. Allowing unbounded classical outputs from the quantum channels.

In this study, we examine only the first four generalization, leaving the final generalization for future work. We note that if the set of prepared states are qubit states in the X and Z basis, the state preparation in QPV is equivalent to the verifier preparing the Bell state $|\Phi^+\rangle_{VQ}$, and later measuring his quantum system V in basis θ with outcome z such that the post-measured state of Q is $|\psi^\theta_z\rangle_Q$. We label the final state with this replacement (but before V's measurement) as $\rho^{xy}_{RM_AM_BVA'B'}$.

Before proceeding, we provide a brief summary of the QPV security proof for reference [10]. This proof of security can be separated into follows five distinct steps:

1. Formulate a description that can encompass all q-qubit strategies, and argue that we can discretize this set of strategies into a δ-net, where any strategy is δ-close to the center of a net in some distance measure.
2. Consider the same or an optimal set of strategies with low error rate for fixed (x,y), and show that the distance between two low error strategies corresponding to the different measurement basis $\theta = f(x,y)$ is not small, being some distance $\tilde{\delta}$ apart.
3. By choosing $\delta < g(\tilde{\delta})$, we can assign each net to a strategy, and when one of these low error rate strategies are considered for an (x,y) pair, we can correctly classify them. This allows the construction of a classical rounding strategy, where messages x and y can be compressed and still recover $f(x,y)$.

[6] The quantum channel $\mathcal{E}^{xr}_{AQ}$ (resp. $\mathcal{E}^{yr}_B$) applies on quantum systems AQ (resp. B), and can generate a quantum state of at most 2^{q+1} dimensions (resp. 2^q dimensions) and an unbounded classical output M_A (resp. M_B).

4. For bounded memory size q, and if there exists a classical rounding, when a random function f is used, then except with small probability, there is a maximum number of (x, y) pairs that can achieve a low error strategy. This results in an upper bound in the winning probability since the remaining pairs do not have low error.

5. The proof therefore concludes via contradiction that if the error rate detected is low and the memory size is bounded, no such q-qubit strategy can exist and thus with high probability, the response must be from a party at P.

B. Purifying Attack Strategy

The first generalization addresses the use of mixed states and general quantum channels. It is not straightforward to perform the security analysis directly on quantum channels (CPTP) maps and mixed states, so the idea would be to partially purify the final state $\rho_{RVA'B'}$ (Note we do not address the fifth generalization on $M_A M_B$). Let us first define the set of quantum states and channels we are examining. The set $\mathcal{S}_q$ is defined as the set of (mixed) quantum states of dimension 2^q, while $\mathcal{S}_q^p$ is defined as the set of pure quantum states with dimension 2^q. The set $\mathcal{C}_q$ is defined as the set of CPTP maps 2^q-dimension quantum states to 2^q-dimension quantum states, while $\mathcal{C}_q^U$ is defined similarly for the set of unitaries.

Partial purification can be performed with purification of the mixed state σ_{AB}^r by doubling its number of qubits [19], while lifting the quantum channel to a higher dimensional unitary can be performed via Stinespring dilation theorem [19]. We can summarize the purification as a theorem.

Theorem 4. *Any state $\rho_{RA'B'V}^{xy} = \sum_r p_r |r\rangle\langle r|_R \otimes \rho_{A'B'V}^{xyr}$ with $\sigma_{AB}^r \in \mathcal{S}_{2q}$, $\mathcal{E}_{AQ}^{xr} \in \mathcal{C}_{q+1}$ and $\mathcal{E}_B^{yr} \in \mathcal{C}_q$ and be purified with purification systems P of dimension 2^{2q}, P_A of dimension $2^{2(q+1)}$ and P_B of dimension 2^{2q}, i.e. there exists a state $|\psi^r\rangle_{ABP} \in \mathcal{S}_{4q}^p$ and unitaries $U_{AQP_A}^{xr} \in \mathcal{C}_{3(q+1)}^U$ and $U_{BP_B}^{yr} \in \mathcal{C}_{3q}^U$ such that*

$$\rho_{A'B'VPP_AP_B} = \sum_r p_r |r\rangle\langle r|_R \otimes \mathcal{M}[(U_{AQP_A}^{xr} \otimes U_{BP_B}^{yr}) (|\Phi^+\rangle\langle\Phi^+|_{VQ} \otimes |\psi^r\rangle\langle\psi^r|_{ABP} \otimes |0\rangle\langle 0|_{P_AP_B})(U_{AQP_A}^{xr\dagger} \otimes U_{BP_B}^{yr\dagger})]$$

and $\mathrm{Tr}_{PP_AP_B}[\rho_{A'B'VPP_AP_B}] = \rho_{A'B'V}$. Furthermore, the winning probability of the original strategy is upper bounded by the winning probability of the purified strategy.

Proof. Refer to Appendix D 1. □

The fact that purification does not reduce the winning probability allows us to reduce the analysis of the mixed state and quantum channel attacks to one with pure states and unitaries. Since the number of qubits influences the size of the δ-nets formed, we quantify the size of such nets when quantum channels and mixed states are utilized,

Theorem 5. *When a q-qubit mixed state strategy (with q qubits in subsystem A and B respectively), the number of δ-nets that can be formed from the purified state and corresponding unitaries are*

$$\log_2 |\mathcal{N}_S| \leq 2^{4q+1} \log_2 \left(1 + \frac{2}{\delta}\right)$$
$$\log_2 |\mathcal{N}_A| \leq 2^{6q+7} \log_2 \left(1 + \frac{2}{\delta}\right)$$
$$\log_2 |\mathcal{N}_B| \leq 2^{6q+4} \log_2 \left(1 + \frac{2}{\delta}\right)$$

respectively.

Proof. Refer to Appendix D 2. □

C. Transmission and Error Partitioning

The partitioning strategy here aims to address the assumption where loss η is input-independent, and provides account of the shared randomness due to the resulting winning probability that is affine in r. In Ref. [10], the set of low error strategy is defined with the idea of (ε, l)-perfect strategies, where for l pairs of strings (x, y), the attacks declare no photon detection with probability $1 - \eta$ and the conditional error rate is upper bounded by ε. We note that this set of strategies may not encompass all optimal attacks. One particular set of attacks not considered are attacks with loss that varies with (x, y) pairs, and it is unclear if selecting a strategy with the same η for all (x, y) is the optimal strategy.

We also note that in many protocols, it is typical that shared randomness do not provide advantage to adversaries, allowing us to simplify analysis to a single strategy without shared randomness. In fact, this is the case for a lossless QPV [9] since $\sum_r p_r$ commutes with the maximization in Eqn. (D3). This allows us to argue that for any strategy, it would be optimal to pick one corresponding to an r with the highest winning probability. The same argument may no longer hold with loss since η can vary with r, and the optimal winning probability can vary non-linearly with η. As such, an adversary mixing two strategies, one with higher loss and winning probability and one with lower loss and lower winning probability may have a larger winning probability compared to a strategy with an average loss.

We begin our analysis by defining the set of strategies in a different manner, without assuming that η is independent on (x, y) and r.

Definition 1. *For any strategy, the input and shared randomness dependent error rate and transmission rate is defined as*

$$p_{e|rxy} = \sum_z \mathrm{Tr}\Big[(\Pi_z^{f(x,y)} \otimes A_{\bar{z}}^{xyr} \otimes B_{\bar{z}}^{xyr})\rho_{A'B'V}^{xyr}\Big]$$
$$p_{t|rxy} = 1 - \mathrm{Tr}[(\mathbb{I}_V \otimes A_{\perp}^{xyr} \otimes B_{\perp}^{xyr})\rho_{A'B'V}^{xyr}]$$

respectively, and the matching condition is defined as

$$\mathrm{Tr}[(\mathbb{I}_V \otimes A_z^{xyr} \otimes B_{z'}^{xyr})\rho_{A'B'V}^{xyr}] = 0,\ \forall z.$$

A q-qubit strategy is a $(\{p_r\}_r, \varepsilon, \eta)$-strategy with $(\varepsilon_{thres}, \eta_{thres}, \{l_{1,r}, l_{2,r}, l_{3,r}, l_{4,r}\}_r)$-partition if for each r, there are:

1. *$l_{1,r}$ pairs of (x,y) satisfying $p_{e|rxy} \leq \varepsilon_{thres}\eta$, $p_{t|rxy} \geq \eta_{thres}$ and the matching condition,*
2. *$l_{2,r}$ pairs of (x,y) satisfying $p_{e|rxy} \leq \varepsilon_{thres}\eta$, $p_{t|rxy} < \eta_{thres}$ and the matching condition,*
3. *$l_{3,r}$ pairs of (x,y) satisfying $p_{e|rxy} > \varepsilon_{thres}\eta$, $p_{t|rxy} \geq \eta_{thres}$ and the matching condition,*
4. *$l_{4,r}$ pairs of (x,y) satisfying $p_{e|rxy} > \varepsilon_{thres}\eta$, $p_{t|rxy} < \eta_{thres}$ and the matching condition.*

We term the strategy for each r as a sub-strategy with $(\varepsilon_{thres}, \eta_{thres}, l_{1,r}, l_{2,r}, l_{3,r}, l_{4,r})$-partition.

In this definition, there is no explicit assumptions on the r and (x,y)-dependency of loss and error, and all attack strategies can be described by this set of strategies. We note that the definition of threshold values $\varepsilon_{\mathrm{thres}}$ and η_{thres} is simply to aid in the security analysis and is not tied to the strategy. Their choices partition a strategy's attacks into groups, similar to the (ε, l)-perfect strategy definition, where the partitioning is into a group of l pairs of (x,y) with low error rate and the remaining with high error rate. Since their choice do not impact security in practice, we are free to choose the threshold $\varepsilon_{\mathrm{thres}}$ and η_{thres} such that they give the lowest winning probability for each strategy.

Following the idea from the original security analysis [10, 11], we seek to provide an upper bound on the number of low error rounds, specifically $l_{1,r}$ for any strategy. As such, let us focus on this partition and define the set of states that can satisfy the corresponding conditions for different basis value $f(x,y)$.

Definition 2. *Let $\tilde{\varepsilon} \in [0,1]$ and $\tilde{\eta} \in [0,1]$, and define the error, transmission and abort probability for a given choice of measurement operators $\{A_z\}_z$ and $\{B_z\}_z$ as*

$$p_{e,i} = \sum_z \langle\psi|\Pi_z^i \otimes A_{\bar{z}} \otimes B_{\bar{z}}|\psi\rangle$$
$$p_t = 1 - \langle\psi|\mathbb{I}_V \otimes A_{\perp} \otimes B_{\perp}|\psi\rangle$$
$$p_{ab} = \sum_{z \neq z'} \langle\psi|\mathbb{I}_V \otimes A_z \otimes B_{z'}|\psi\rangle$$

The set of output states for a partition for a basis is defined as

$$\mathcal{S}_i^{\tilde{\varepsilon},\tilde{\eta}} = \{|\psi\rangle_{A'B'V} = (U_{AQ} \otimes U_B)(|\psi\rangle_{AB} \otimes |\Phi^+\rangle_{VQ}) :$$
$$\exists\{A_z\}_z, \{B_z\}_z,\ s.t.,\ p_{e,i} \leq \tilde{\varepsilon},\ p_t \geq \tilde{\eta}, p_{ab} = 0\},$$

where U_{AQ}, U_B and $|\psi\rangle_{AB}$ are restricted in the same manner as described in Thm. 4, i.e. U_{AQ} and U_B are purification of CPTP maps for $q+1$ and q qubits respectively, and $|\psi\rangle_{AB}$ remains a purification of a mixed $2q$-qubit state.

For the partition of interest, these sets can be defined with $\tilde{\varepsilon} = \varepsilon_{\mathrm{thres}}\eta$ and $\tilde{\eta} = \eta_{\mathrm{thres}}$. As we demonstrate in Sec. V D, any two states drawn from this set with different bases and with sufficiently low $\tilde{\varepsilon}$ and high $\tilde{\eta}$ would not be close in trace distance. In other words, for any states $|\psi_0\rangle \in \mathcal{S}_0^{\tilde{\varepsilon},\tilde{\eta}}$ and $|\psi_1\rangle \in \mathcal{S}_1^{\tilde{\varepsilon},\tilde{\eta}}$, $\Delta(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) > \tilde{\delta}(\varepsilon_{\mathrm{thres}}, \eta_{\mathrm{thres}}, \eta)$, where we explicitly list the dependency on the partitioning choice. More concretely, we lower bound the trace distance between a larger set where the adversary is unbounded, which in turn bounds the trace distance between the q-qubit limited strategies.

The third step of the security proof involves the formation of a classical rounding.

Definition 3 (Classical Rounding [9, 10])**.** *A function $g : \{0,1\}^{3k} \to \{0,1\}$ is termed a classical rounding of size k if for any function choice $f : \{0,1\}^{2n} \to \{0,1\}$, any $l_{1,r} \in [1, 2^{2n}]$, any sub-strategy with $(\varepsilon_{thres}, \eta_{thres}, l_{1,r}, l_{2,r}, l_{3,r}, l_{4,r})$-partition, there are functions $f_A : \{0,1\}^n \to \{0,1\}^k$, $f_B : \{0,1\}^n \to \{0,1\}^k$ and $\lambda \in \{0,1\}^k$ such that $g(f_A(x), f_B(y), \lambda) = f(x,y)$ for $l_{1,r}$ pairs of (x,y).*

We note that in this case we focus on each sub-strategy instead of the full strategy, but each sub-strategy remains a valid strategy. This allows us to construct a classical rounding.

Theorem 6. *Consider the sets $\mathcal{S}_0^{\tilde{\varepsilon},\tilde{\eta}}$ and $\mathcal{S}_1^{\tilde{\varepsilon},\tilde{\eta}}$ for η_{thres}, ε_{thres} and η values such that $\tilde{\delta}(\varepsilon_{thres}, \eta_{thres}, \eta) > 0$. Then, there exists a classical rounding of size $k = 2^{6q+7}\left\lceil\left\lceil \log_2\left(1 + \frac{12}{\tilde{\delta}}\right)\right\rceil + 1\right\rceil$.*

Proof. Refer to Appendix E 1. □

We follow the original security proof and demonstrate that when a random function is used and when q is bounded, there is a bound on the number of input pairs in the low error, high transmission partition, $l_{1,r}$.

Theorem 7. *Fix a classical rounding with $k = 2^{6q+7}\left\lceil\left\lceil \log_2\left(1 + \frac{12}{\tilde{\delta}}\right)\right\rceil + 1\right\rceil$ and let $q \leq \frac{1}{6}n - q_0$. Then, a uniform random function $f : \{0,1\}^{2n} \to \{0,1\}$ fulfills the following with probability at least $1 - 2^{-\alpha}$:*

For any f_A, f_B and λ, $g(f_A(x), f_B(y), \lambda) = f(x, y)$ holds for less than $2^{2n}(1-\nu)$ pairs of (x, y), for $\nu = h_b^{-1}\left\{1 - 2^{9-6q_0}\left[\left\lceil \log_2\left(1+\frac{12}{\tilde{\delta}}\right)\right\rceil + 1\right] - \frac{\alpha}{2^{2n}}\right\}$, where $h_b(x)$ is the binary entropy function.

Proof. Refer to Appendix E 2. □

Consequently, for any sub-strategies with $l_{1,r} > 2^{2n}(1-\nu)$, they require a large number of qubits to successfully implement.

Theorem 8. *A uniform function $f : \{0,1\}^{2n} \to \{0,1\}$ has the following with probability at least $1 - 2^{-\alpha}$: Any sub-strategy with $l_{1,r} > 2^{2n}(1-\nu)$ requires $q > \frac{1}{6}n - q_0$ to implement.*

Proof. From Thm. 6, we know that a classical rounding exists for suitably chosen η, η_{thres} and $\varepsilon_{\text{thres}}$. Assume there exists a sub-strategy with $l_{1,r} > 2^{2n}(1-\nu)$ that requires $q \leq \frac{n}{6} - q_0$ to implement. By definition, it implies that the sub-strategy satisfies $p_{e|rxy} \leq \varepsilon_{\text{thres}}\eta$, $p_{t|rxy} \geq \eta_{\text{thres}}$ and the matching condition for at least $2^{2n}(1-\nu)$ pairs of (x, y). From the classical rounding, it implies that we can find a f_A, f_B and λ such that $g(f_A(x), f_B(y), \lambda) = f(x, y)$ for at least $2^{2n}(1-\nu)$ pairs of (x, y).

Since the sub-strategy requires only $q \leq \frac{n}{6} - q_0$ to implement, by Thm. 7, we necessarily have that for a random function f selected has $f(x, y)$ and $g(f_A(x), f_B(y), \lambda)$ matching for less than $2^{2n}(1-\nu)$ pairs of (x, y) with probability of at least $1 - 2^{-\alpha}$. This indicates that except with probability less than $2^{-\alpha}$, the two statement contradicts. As such, for a random function selection, the assumption is not true, i.e. sub-strategies with $l_{1,r} > 2^{2n}(1-\nu)$ requires $q > \frac{n}{6} - q_0$ to implement, with probability at least $1 - 2^{-\alpha}$. □

We immediately have a corollary that if we restrict the sub-strategies to have $q \leq \frac{1}{6}n - q_0$, then the sub-strategies has $l_{1,r} \leq 2^{2n}(1-\nu)$ with high probability.

Corollary 1. *Let the choice of f be a random function, and Alice and Bob are restricted to strategies with $q \leq \frac{1}{6}n - q_0$. Then, for any sub-strategy, $l_{1,r} \leq 2^{2n}(1-\nu)$ except with probability of $1 - 2^{-\alpha}$.*

This allows us to lower bound the overall error (or upper bound the winning probability) for any sub-strategy.

We first consider the total error for a sub-strategy with $l_{1,r} \leq 2^{2n}(1-\nu)$.

Theorem 9. *Let the choice of f be a random function, and Alice and Bob are restricted to strategies with $q \leq \frac{1}{6}n - q_0$. For any sub-strategy with $l_{1,r} \leq 2^{2n}(1-\nu)$ and transmission η_r, the probability of an error is lower bounded by $\max\{\varepsilon_{thres}\eta[\frac{\eta_r - \eta_{thres}}{1-\eta_{thres}} - 1 + \nu], 0\}$.*

Proof. Refer to Appendix E 3. □

With the constraints on the sub-strategies, we can now compute a lower bound on the error (i.e. upper bound on winning probability) on any strategy.

Theorem 10. *Let f be a random function, and Alice and Bob are restricted to strategies with $q \leq \frac{1}{6}n - q_0$. For any $(\{p_r\}_r, \varepsilon, \eta)$-strategy with $(\varepsilon_{thres}, \eta_{thres}, \{l_{1,r}, l_{2,r}, l_{3,r}, l_{4,r}\}_r)$-partition, the error rate conditioned on photon detection is lower bounded by $(1 - 2^{-\alpha})\left(\frac{\eta - \eta_{thres}}{1-\eta_{thres}} - 1 + \nu\right)\varepsilon_{thres}$.*

Proof. From Corollary 1, every sub-strategy involved in this overall strategy has $l_{1,r} \leq 2^{2n}(1-\nu)$ except with probability $1 - 2^{-\alpha}$. As such, from Thm. 9, the actual error for each sub-strategy (without conditioning on photon detection) is given by

$$p'_{err|r} \geq (1 - 2^{-\alpha}) \max\{\eta\varepsilon_{\text{thres}}\left[\frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}} - 1 + \nu\right], 0\}. \tag{7}$$

We can simply bound the overall error as

$$\begin{aligned} p'_{err} =& \sum_r p_r p'_{err|r} \\ \geq& (1 - 2^{-\alpha}) \sum_r p_r \max\{\eta\varepsilon_{\text{thres}}\left(\frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}} - 1 + \nu\right), 0\} \\ \geq& (1 - 2^{-\alpha})\eta\varepsilon_{\text{thres}}\left(\frac{\sum_r p_r\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}} - 1 + \nu\right) \\ =& (1 - 2^{-\alpha})\eta\varepsilon_{\text{thres}}\left(\frac{\eta - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}} - 1 + \nu\right), \end{aligned} \tag{8}$$

where the fact that $p'_{err|r}$ is affine in η_r is utilized. Therefore, the conditional error is simply lower bounded by

$$\varepsilon^{LB} = (1 - 2^{-\alpha})\left(\frac{\eta - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}} - 1 + \nu\right)\varepsilon_{\text{thres}}. \tag{9}$$

□

Since the strategy described in the theorem includes all possible q-qubit strategies, we obtain a valid lower bound on the error rate conditioned on detection. Therefore, if an error rate lower than ε^{LB} is observed in the experiment in the asymptotic regime (no statistical fluctuations), we can be confident that there must be a party present at P participating in the QPV protocol.

We simulate the error rate conditioned on photon detection based on Thm. 10, with ν as defined in Thm. 7, and a choice of $\frac{\alpha}{2^n} = 10^{-10}$ for large n. The value of $\tilde{\delta}$ is computed from the semidefinite program (SDP) in Sec. V D, with an optimization of the threshold values η_{thres} and $\varepsilon_{\text{thres}}$. The results of the simulation are shown in Fig. 2, for three choices of q_0. We observe that larger q_0 (i.e. lower adversary memory size) would naturally lead to better performance. Moreover, the generalization appears to result in worse results relative to the analysis in Ref. [10].

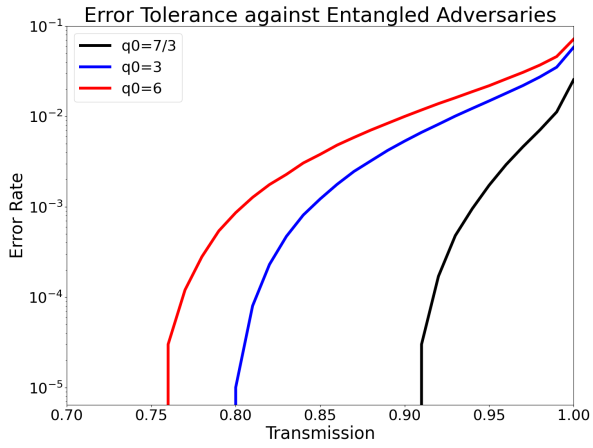

FIG. 2. Plot of error tolerance rate against entangled adversaries with a generalization of the adversary. The plots are provided by choosing $\frac{\alpha}{2^n} = 10^{-10}$ and optimizing over the threshold values of the partitioning.

D. Improvement to Trace Distance Bound

In the security analysis of QPV, one critical step is to lower bound the trace distance between the sets $\mathcal{S}_0^{\tilde{\varepsilon},\tilde{\eta}}$ and $\mathcal{S}_1^{\tilde{\varepsilon},\tilde{\eta}}$. A tighter trace distance bound can result in a better bound on the winning probability of an adversary.

It is difficult to directly bound the trace distance of the two sets containing strategies limited by q-qubits. As such, let us define a larger set $\tilde{\mathcal{S}}_i^{\tilde{\varepsilon},\tilde{\eta}}$ which is defined similar to $\mathcal{S}_i^{\tilde{\varepsilon},\tilde{\eta}}$, except that there are no restrictions on U_{AQ}, U_B and $|\psi\rangle_{AB}$. We note that since $\mathcal{S}_i^{\tilde{\varepsilon},\tilde{\eta}} \subseteq \tilde{\mathcal{S}}_i^{\tilde{\varepsilon},\tilde{\eta}}$, if $\Delta(|\phi_0\rangle, |\phi_1\rangle) > \tilde{\delta}$ for all $|\phi_0\rangle \in \tilde{\mathcal{S}}_0^{\tilde{\varepsilon},\tilde{\eta}}$ and $|\phi_1\rangle \in \tilde{\mathcal{S}}_1^{\tilde{\varepsilon},\tilde{\eta}}$, then $\Delta(|\varphi_0\rangle, |\varphi_1\rangle) > \tilde{\delta}$ for all $|\varphi_0\rangle \in \mathcal{S}_0^{\tilde{\varepsilon},\tilde{\eta}}$ and $|\varphi_1\rangle \in \mathcal{S}_1^{\tilde{\varepsilon},\tilde{\eta}}$.

Consider an arbitrary state $|\Psi_0\rangle \in \tilde{\mathcal{S}}_0^{\tilde{\varepsilon},\tilde{\eta}}$, which we can expand as

$$\begin{aligned} |\Psi_0\rangle =& (U_{AQ} \otimes U_B)(|\psi\rangle_{AB} \otimes |\Phi^+\rangle_{QV}) \\ =& (U_{AQ} \otimes U_B)(|\psi\rangle_{AB} \otimes \frac{|00\rangle_{QV} + |11\rangle_{QV}}{\sqrt{2}}) \\ =& \frac{|0\rangle_V \otimes |\psi_{00}\rangle_{ABQ} + |1\rangle_V \otimes |\psi_{01}\rangle_{ABQ}}{\sqrt{2}}, \end{aligned} \tag{10}$$

where $|\psi_{0i}\rangle = (U_{AQ} \otimes U_B)(|\psi\rangle_{AB} \otimes |i\rangle_Q)$. We can similarly consider an arbitrary state $|\Psi_1\rangle \in \tilde{\mathcal{S}}_1^{\tilde{\varepsilon},\tilde{\eta}}$, which can be expanded as

$$|\Psi_1\rangle = \frac{|0\rangle_V \otimes |\psi_{10}\rangle_{ABQ} + |1\rangle_V \otimes |\psi_{11}\rangle_{ABQ}}{\sqrt{2}}, \tag{11}$$

where $\psi_{1i} = (U'_{AQ} \otimes U'_B)(|\psi'\rangle_{AB} \otimes |i\rangle_Q)$, with possibly a different set of strategy. We can now show that the trace distance between sets $\tilde{\mathcal{S}}_0^{\tilde{\varepsilon},\tilde{\eta}}$ and $\tilde{\mathcal{S}}_1^{\tilde{\varepsilon},\tilde{\eta}}$ can be lower bounded by an SDP, as summarized below.

Theorem 11. *Consider any state $|\Psi_0\rangle \in \tilde{\mathcal{S}}_0^{\tilde{\varepsilon},\tilde{\eta}}$ and any state $|\Psi_1\rangle \in \tilde{\mathcal{S}}_1^{\tilde{\varepsilon},\tilde{\eta}}$, which can be expanded as described above. Furthermore, let the corresponding measurement operators that can achieve the partition for $\tilde{\mathcal{S}}_i^{\tilde{\varepsilon},\tilde{\eta}}$ be labelled by A_z^i and B_z^i. Then, the trace distance between the states would always be lower bounded by a function of the dual solution of an SDP, i.e. $\Delta(|\Psi_0\rangle, |\Psi_1\rangle) \geq \sqrt{1-(d^*)^2}$, where d^* is the dual solution of the SDP*

$$\begin{aligned} \max \quad & \frac{1}{2}\mathrm{Re}[\langle\psi_{00}|\psi_{10}\rangle + \langle\psi_{01}|\psi_{11}\rangle] \\ subj.\,to \quad & \Gamma \geq 0 \\ & \langle\psi_{ij}|\psi_{ij'}\rangle = \delta_{jj'},\ i \in \{0,1\} \\ & \frac{1}{2}\sum_{j=0}^{1} \langle\psi_{ij}|A_0^i B_0^i + A_1^i B_1^i|\psi_{ij}\rangle \geq \tilde{\eta},\ i \in \{0,1\} \\ & \frac{1}{2}[\langle\psi_{00}|A_1^0 B_1^0|\psi_{00}\rangle + \langle\psi_{01}|A_0^0 B_0^0|\psi_{01}\rangle] \leq \tilde{\varepsilon} \\ & \frac{1}{4}\left(\sum_{i,j=0}^{1} \langle\psi_{1i}|A_1^1 B_1^1|\psi_{1j}\rangle + \sum_{i,j=0}^{1} (-1)^{i+j} \langle\psi_{1i}|A_0^1 B_0^1|\psi_{1j}\rangle\right) \leq \tilde{\varepsilon} \\ & \langle\psi_{ij}|A_z^i B_{z'}^i|\psi_{ij}\rangle = 0,\ \forall z \neq z', i, j \in \{0,1\} \\ & [A_j^i, B_{j'}^{i'}] = 0,\ i, i' \in \{0,1\},\ j, j' \in \{0,1,\perp\} \end{aligned}$$

and the Gram matrix having entries

$$\Gamma_{ij} = \langle\xi_i|\xi_j\rangle, \tag{12}$$

with $|\xi_i\rangle$ formed from the NPA hierarchy with states $\{|\psi_{ij}\rangle\}_{ij}$ and operators $\{A_j^i\}_{ij}$ and $\{B_j^i\}_{ij}$.

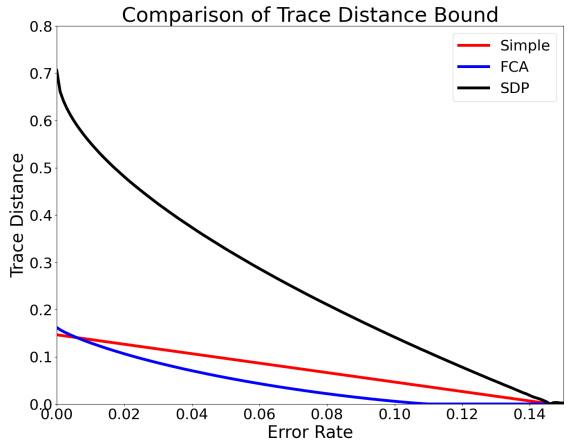

FIG. 3. Plot comparing the trace distance bound for the simple bound from Ref. [10] (in red), the Fano's inequality, complementary-inforamtion tradeoff and Alicki—Fannes—Winter continuity bound (in blue) and the proposed SDP bound (in black).

Proof. Refer to Appendix F. □

To demonstrate the improvement from the trace distance bound, we compare the result with that in Ref. [10] using the distance to a simpler QPV game and Ref. [9] using Fano's inequality, complementary-information tradeoff and Alicki—Fannes—Winter continuity bound. We plot the trace distance bound in Fig. 3 for the three separate analysis method for various $\tilde{\varepsilon}$ error rate. The SDP formulation shows significant improvement to the trace distance bound, and could be tight, matching the $\frac{1}{\sqrt{2}}$ distance at zero error.

E. QPV with Multiple Measurement Basis

In general, QPV protocols where a single slow quantum state is sent to the prover has a loss tolerance that scales as $\eta \sim 1/n$, where n is the number of basis choice. Using BB84 states and measurement leads to a $<50\,\%$ loss tolerance, which may be more challenging to implement in practices. Consequently, the use of multi-basis QPV protocols, such as that proposed in Ref. [10] may be necessary. The key reason for the low loss tolerance is due to a general attack where the adversary can randomly select a basis to measure, and post-select on rounds where the measured basis matches the computed basis. Interestingly, this attack only scales with the number of measurement basis, but not the number of prepared states.

As such, we propose a multi-basis QPV where BB84 states are prepared and sent, and multiple measurement basis on the X-Z plane of the Bloch sphere is utilized. This can reduce the complexity of experimental implementation by reducing the number of states to prepare, and requiring only operations within the X-Z plane (e.g. rotating polarization axis instead of requiring transformation to circular polarization). Moreover, it may provide greater flexibility since the preparation and measurement basis no longer needs to match, removing the need for the party preparing the quantum state and the verifiers to communicate details on state preparation. This can reduce security vulnerabilities since the state preparation information is no longer transferred before the protocol begins.

In the proposed scheme with multiple basis, the prover is still sent BB84 states, $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, but can measure in different basis, e.g. $(X+Z)/\sqrt{2}$ basis. Since the probability of obtaining a measurement is no longer just 0 and 1 (when basis match), we have to generalize the notion of an error rate. Suppose the probability of measuring outcome z in basis θ for a state $|\psi_s\rangle$ is $\eta p(z|s,\theta)$, where η is the probability of detection, we can define a quantity termed deviation as $\left|\langle\psi_s|\Pi_z^\theta|\psi_s\rangle - \eta p(z|s,\theta)\right| = \delta_{zs\theta}$. During the protocol, we measure the deviation instead of the error rate.

The protocol can thus be described in Protocol 4. The security of the scheme is easy to demonstrate for an adversary with no entanglement. The goal of the adversary would be to pass the checks while it is not at position P, i.e. getting as low a deviation as it can. The maximum deviation (analogous to error rate) an adversary can achieve can be computed via an SDP,

$$\begin{aligned} \min \quad & \frac{1}{4n}\sum_{zs\theta}\delta_{zs\theta} \\ \text{subj. to} \quad & \langle\psi_s|A_\perp^\theta \otimes B_\perp^\theta|\psi_s\rangle = 1-\eta \\ & \langle\psi_s|A_z^\theta \otimes B_{z'}^\theta|\psi_s\rangle = 0,\ z\neq z', \forall\theta, s \\ & -\delta_{zs\theta} \leq \langle\psi_s|A_z^\theta \otimes B_z^\theta|\psi_s\rangle - \eta p(z|s\theta) \leq \delta_{zs\theta}, \end{aligned} \tag{13}$$

where we minimize over the average of the deviation values, with conditions (1) loss is $1-\eta$ (where both adversaries respond with $\perp$), (2) classical response cannot have any mismatch (both adversaries cannot give different responses $z \neq z'$), (3) the deviation from the expected probability in the ideal case is bounded by the deviation value $\delta_{zs\theta}$.

We solve the SDP numerically using ncpol2sdpa [20] with cvxpy [21] and SCS solver [22]. Fig. 4 shows the numerical results, for three to five measurement basis choices. The behavior appears to be similar at high transmission values η, before different number of basis choice leads to drop offs in deviation closer to the loss tolerance limit. The numerical results show a $\frac{1}{n}$ loss tolerance, similar to using n basis with n measurement basis. We note that the figure do not show exactly $\frac{1}{n}$,

Protocol 4 QPV with multiple measurement basis

Goal. Verifiers certify that the prover is at position P.
Public Functions. Evaluation function f'.

1. For $i = 1, \cdots, N$, repeat the following process:

   (a) **Verifier Preparation**: At the start of round i, the first and second verifiers randomly select $x'_i \in [2^n]$ and $y'_i \in [2^n]$ respectively. Verifiers also communicate and agree on a time $t_{P,i}$.

   (b) **Quantum State Transfer**: A third party prepares a quantum system $|\psi_s\rangle_Q$, which corresponds to one of the four BB84 states, $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The third party sends the quantum system to the prover.

   (c) **Verifier Message**: V_1 and V_2 sends x'_i and y'_i respectively at $t_{P,i} - d_{V_1P}/c$ and $t_{P,i} - d_{V_2P}/c$ such that they both arrive at P at time $t_{P,i}$.

   (d) **Quantum Measurement**: The prover computes $\theta_i = f'_\theta(x'_i, y'_i)$ and measures quantum system Q in the computed basis. The prover announces $b_{det,i} = 1$ if a photon is detected (i.e. measurement generates an outcome), and sends the measurement outcome $z_{1,i} = z_{2,i} = z_i$. If no photon is detected, it announces $b_{det,i} = 0$.

   (e) **Timing and Validity Check**: V_1 and V_2 record the arrival time of the respective responses $b_{det,i}$, $z_{1,i}$ and $z_{2,i}$ as $t_{b,i}$, $t_{z_1,i}$ and $t_{z_2,i}$. The verifiers first checks if the responses are valid, i.e. (1) $z_{1,i} = z_{2,i}$. The verifiers then check if the timings are valid, (2) $t_{z_1,i} - t_{P,i} \leq d_{V_1P}/c + t_\delta$, and (3) $t_{z_2,i} - t_{P,i} \leq d_{V_2P}/c + t_\delta$ for some threshold t_δ. If any checks fail, the protocol aborts immediately.

2. **Deviation Estimation**: V_1 and V_2 computes the deviation $\delta_{zs\theta} = \left| \frac{N_{zs\theta}}{N_{s\theta}} - \eta p(z|s\theta) \right|$ for each outcome z, state s and basis choice θ, where $N_{zs\theta}$ is the number of rounds with outcome z for state s and basis choice θ and $N_{s\theta} = \sum_z N_{zs\theta}$. The verifier check if the total deviation δ_T (weighted if necessary) exceed a threshold $\delta_T > \delta_{thres}$. If the threshold is exceeded, the protocol aborts.

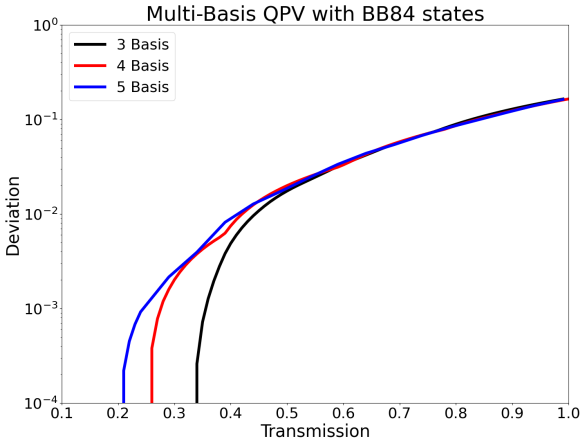

FIG. 4. Plot of Deviation against Transmission for proposed multi-basis QPV protocol using BB84 states.

but at the cut-off right before $\frac{1}{n}$ due to the choice of precision of 0.01 for η in the numerical simulation.

Since loss tolerance may appear to scale with $\frac{1}{n}$ without entanglement, we expect that the loss tolerance with entanglement to also improve with more measurement basis. In a more practical setting where finite-size effects and imperfect devices are present, the loss tolerance value would similarly improve with more basis choice, but the scaling would be worse. Honest parties performing QPV with imperfect devices can deviate from ideal target behavior of $\eta p(z|s,\theta)$, which leads to a systematic error that translate to a non-zero average deviation value. On the other hand, if finitely many rounds are performed, the statistical fluctuations can lead to non-zero observed deviation[7]. These effects would provide a guide on the deviation tolerance δ_{tol} and number of rounds one should set for a robust protocol (low abort rate for honest parties).

VI. DISCUSSION

While not explicitly addressed in the manuscript, there is a mismatch in the adversary models of QKD and QPV. QKD security is typically provided against unbounded adversaries, while QPV require quantum memory or quantum computational power restrictions. Reconciling the two models would involve lowering the QKD security guarantees to that of the QPV adversary, though it is important to note that QPV restrictions can sometimes be only for the duration of the protocol. For instance, for bounded quantum memory, there can be potential for QKD to provide better key rates since the adversary's quantum side-information E is restricted in size. For restriction in computational power during the protocol, one has to note that the computational power

[7] Note that if there are finitely many rounds, the observed loss may also have some deviation from $1 - \eta$.

assumed may for QKD and QPV be different since their run times can differ significantly. As such, weakening of the adversary is unlikely to have much impact.

In the security analysis for secure key exchange, some assumptions are made to simplify the analysis. For instance, we assume implicitly that the protocol completes at some fixed time T. One could relax this assumption to explore the actual spacetime region (over some locations and times) where parties would have to trust instead of a fixed T. Assumptions to reduce synchronization issues, such as agreed duration between QPV rounds and QPV runs, and having Δt to be larger than QPV run times can also be relaxed. Without these assumptions, the adversary may easily remap bits, for instance from 10101 to 10011 if it is allowed to delay the third QPV run of the sender to match the fourth QPV run of the receiver. Therefore, alternative schemes such as the encoding scheme proposed in Ref. [14] may be necessary to lift the assumption. It is thus interesting to explore methods of relaxing various assumptions made and generalize the adversary.

Alternative adversary models can also be explored, since there can be multiple ways of integrating QKD and QPV. For instance, the current adversary model does not admit scenarios where one party can exchange QKD with Alice at a location P' and have a collaborator at point P to perform QPV. While this may be a useful "activation" property, it may be a problem in other applications where the desire is to only exchange keys with the party at P. In such scenarios, a stronger adversary model is necessary, and greater integration of QKD and QPV may be required.

While we tackle some open problems in QPV security analysis with our generalization, the performance of the QPV scheme worsens as a result. This is to be expected as a more powerful adversary is studied, but this may lead to more challenges in implementation. It is possible to improve the number of partitions to enhance the performance. However, an issue observed is that more than half of the inputs are always attributed to the $l_{1,r}$ partition (low loss, low error) by nature of the security argument, leading to a penalty to the error tolerance by a factor of 2. As such, it would be interesting to explore alternative methods of analysis that can provide better performance.

There are more open problems in QPV that can be further explored to improve the theoretical support and practical implementation of QPV. One major problem in our generalization that is not addressed is the possibility for the adversary to generate long classical strings from measurements as part of quantum channels $\mathcal{E}_{AQ}^{xr}$ and $\mathcal{E}_{B}^{yr}$. Introducing such an additional classical register would lead to an increase in the dimension of the quantum channel and the corresponding unitary, which poses a problem for the security analysis. Other open problems that are of interest include studying security based on bounds on the adversary's entanglement as opposed to its memory, and determining the function properties that are necessary for QPV security.

VII. CONCLUSION

In summary, the manuscript proposes a secure key exchange protocol that relies on location credentials of parties, utilizing QPV sub-protocol to provide the necessary authentication. We demonstrate that based on our security model, the security of the overall protocol splits into the QKD, QPV and hash family security conditions, allowing for separate analysis of the sub-protocols.

Further noting that QPV security and implementation is relatively less mature compared to QKD, we provide some improvements, namely a generalization of the adversary, tightening of the security bound via SDP, and proposing a simpler multi-basis QPV protocol that can achieve similar loss tolerance. This provides a first step towards the practical implementation of QPV, and its potential application to allow location credentials as an alternative means of authentication in QKD without any pre-shared keys.

ACKNOWLEDGMENTS

This paper was prepared for informational purposes by the Global Technology Applied Research center of JPMorgan Chase & Co. This paper is not a product of the Research Department of JPMorgan Chase & Co. or its affiliates. Neither JPMorgan Chase & Co. nor any of its affiliates makes any explicit or implied representation or warranty and none of them accept any liability in connection with this paper, including, without limitation, with respect to the completeness, accuracy, or reliability of the information contained herein and the potential legal, compliance, tax, or accounting effects thereof. This document is not intended as investment research or investment advice, or as a recommendation, offer, or solicitation for the purchase or sale of any security, financial instrument, financial product or service, or to be used in any way for evaluating the merits of participating in any transaction.

[1] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994)

pp. 124–134.
[2] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical Computer Science **560**, 7 (2014).
[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without bell's theorem, Physical Review Letters **68**, 557 (1992).
[4] A. K. Ekert, Quantum cryptography based on bell's theorem, Physical Review Letters **67**, 661 (1991).
[5] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Reviews of Modern Physics **92**, 025002 (2020).
[6] C. Portmann and R. Renner, Security in quantum cryptography, Reviews of Modern Physics **94**, 025008 (2022).
[7] J. L. Carter and M. N. Wegman, Universal classes of hash functions, Journal of Computer and System Sciences **18**, 143 (1979).
[8] M. Mosca, D. Stebila, and B. Ustaoğlu, Quantum key distribution in the classical authenticated key exchange framework, in *Post-Quantum Cryptography*, edited by P. Gaborit (Springer Berlin Heidelberg, Berlin, Heidelberg, 2013) pp. 136–154.
[9] A. Bluhm, M. Christandl, and F. Speelman, A single-qubit position verification protocol that is secure against multi-qubit attacks, Nat. Phys. **18**, 623 (2022).
[10] L. m. c. Escolà-Farràs and F. Speelman, Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers, Phys. Rev. Lett. **131**, 140802 (2023).
[11] R. Allerstorfer, A. Bluhm, H. Buhrman, M. Christandl, L. Escolà-Farràs, F. Speelman, and P. V. Lunel, Making existing quantum position verification protocols secure against arbitrary transmission loss, arXiv preprint arXiv:2312.12614 (2023).
[12] V. Asadi, R. Cleve, E. Culf, and A. May, Linear gate bounds against natural functions for position-verification, Quantum **9**, 1604 (2025).
[13] K. Kanneworff, M. Poortvliet, D. Bouwmeester, R. Allerstorfer, P. V. Lunel, F. Speelman, H. Buhrman, P. Steindl, and W. Löffler, Towards experimental demonstration of quantum position verification using true single photons (2025), arXiv:2502.04125 [quant-ph].
[14] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, Position-based quantum cryptography: Impossibility and constructions, SIAM Journal on Computing **43**, 150 (2014).
[15] E. O. Kiktenko, A. O. Malyshev, M. A. Gavreev, A. A. Bozhedarov, N. O. Pozhar, M. N. Anufriev, and A. K. Fedorov, Lightweight authentication for quantum key distribution, IEEE Transactions on Information Theory **66**, 6354 (2020).
[16] W. Y. Kon, J. Chu, K. H. Y. Loh, O. Alia, O. Amer, M. Pistoia, K. Chakraborty, and C. Lim, Quantum authenticated key expansion with key recycling (2024), arXiv:2409.16540 [quant-ph].
[17] L. Escolà-Farràs and F. Speelman, Quantum position verification in one shot: parallel repetition of the f-bb84 and f-routing protocols (2025), arXiv:2503.09544 [quant-ph].
[18] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover hashing against quantum side information, IEEE Transactions on Information Theory **57**, 5524 (2011).
[19] M. M. Wilde, *Quantum Information Theory*, 2nd ed. (Cambridge University Press, 2017).
[20] W. Peter, Algorithm 950: Ncpol2sdpa—sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables, ACM Transactions on Mathematical Software **41** (2015).
[21] S. Diamond and S. Boyd, CVXPY: A Python-embedded modeling language for convex optimization, Journal of Machine Learning Research (2016), to appear.
[22] B. O'Donoghue, E. Chu, N. Parikh, and S. Boyd, SCS: Splitting conic solver, version 3.2.7, `https://github.com/cvxgrp/scs` (2023).
[23] R. Vershynin, Introduction to the non-asymptotic analysis of random matrices, in *Compressed Sensing: Theory and Applications*, edited by Y. C. Eldar and G. Kutyniok (Cambridge University Press, 2012) p. 210–268.
[24] M. C. Caro, H.-Y. Huang, M. Cerezo, K. Sharma, A. Sornborger, L. Cincio, and P. J. Coles, Generalization in quantum machine learning from few training data, Nat. Commun. **13**, 4919 (2022).
[25] J. H. van Lint, Mathematical background, in *Introduction to Coding Theory* (Springer Berlin Heidelberg, Berlin, Heidelberg, 1999) pp. 1–21.
[26] M. Navascués, S. Pironio, and A. Acín, Bounding the set of quantum correlations, Phys. Rev. Lett. **98**, 010401 (2007).
[27] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New Journal of Physics **10**, 073013 (2008).
[28] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, 2004).

Appendix A: Secure Key Exchange with One-way Location Authentication Security Analysis

To aid in our analysis, we define a few important events:

- Ω_M: Message sent by Bob M_B matches that received by Alice $\hat{M}_B$.
- Ω'_{PE}: Idealized parameter estimation, which corresponds to a parameter estimation performed with the actual messages M_A and M_B, passes.
- Ω_H: Hash of Bob's received message matches hash of Bob's actual message, i.e. $h(M_B) = h(\hat{M}_B)$.
- Ω_{QPV}: QPV sub-protocol passes, i.e. $I_{QPV} = 1$.
- Ω: Alice and Bob decides to generate a key (does not abort).

We note that the parameter estimation and idealized parameter estimation matches when the messages sent by Bob matches, $\Omega_{PE} \wedge \Omega_M = \Omega'_{PE} \wedge \Omega_M$. We also note that if Bob does not end up checking the hash, for instance if no parties are at the right spacetime coordinates, the event is part of Ω_H^c.

Looking at the form of the output state and ideal state, we can define a specific ideal state with the following: (1) $\tilde{p} = p_\Omega$, (2) $\sigma_E^1 = \rho_{E|\Omega}$, and (3) $\sigma_E^0 = \rho_{E|\Omega^c}$. With this substitution, the trace distance can be expanded as

$$\begin{aligned}
&\Delta(\rho, \rho^{\text{ideal}}) \\
=&p_\Omega \Delta(\rho_{K_A K_B E|\Omega}, \tilde{\tau}_{K_A K_E} \otimes \rho_{E|\Omega}) \\
=&\Delta(\rho_{K_A K_B E \wedge \Omega}, \tilde{\tau}_{K_A K_E} \otimes \rho_{E \wedge \Omega}) \\
\leq&\Delta(\rho_{K_A K_B E \wedge (\Omega \wedge \Omega_M)}, \tilde{\tau}_{K_A K_E} \otimes \rho_{E \wedge (\Omega \wedge \Omega_M)}) + p_{\Omega \wedge \Omega_M^c} \\
\leq&\Delta(\rho_{K_A K_B E \wedge (\Omega'_{PE} \wedge \Omega_{QPV} \wedge \Omega_M)}, \tilde{\tau}_{K_A K_E} \otimes \rho_{E \wedge (\Omega'_{PE} \wedge \Omega_{QPV} \wedge \Omega_M)}) + p_{\Omega \wedge \Omega_M^c} \\
\leq&\Delta(\rho_{K_A K_B E \wedge \Omega'_{PE}}, \tilde{\tau}_{K_A K_E} \otimes \rho_{E \wedge \Omega'_{PE}}) + p_{\Omega \wedge \Omega_M^c \wedge \Omega_H} + p_{\Omega \wedge \Omega_M^c \wedge \Omega_H^c} \\
\leq&\varepsilon_{QKD} + p_{\Omega \wedge \Omega_M^c \wedge \Omega_H} + p_{\Omega \wedge \Omega_M^c \wedge \Omega_H^c} \\
\leq&\varepsilon_{QKD} + \Pr[\Omega_H | \Omega_M^c] + \Pr[\Omega_{QPV} | \Omega_H^c] \\
\leq&\varepsilon_{QKD} + \varepsilon_{auth} + \varepsilon_{QPV}.
\end{aligned} \tag{A1}$$

The first line expands the two states and the terms corresponding to event Ω^c cancels out. The second line simplifies the expression while the third line splits the state into two scenarios based on the event Ω_M, noting that the trace of $\rho_{E \wedge \Omega'}$ is $p_{\Omega'}$. The fourth line expands $\Omega = \Omega_{QPV} \wedge \Omega_{PE}$, and uses the fact that $\Omega_M \wedge \Omega_{PE} = \Omega_M \wedge \Omega'_{PE}$. The fifth line uses the fact that completely-positive non-trace-increasing (CPNTI) maps cannot increase trace distance to remove extra conditions and splits the probability $p_{\Omega \wedge \Omega_M^c}$ based on the event Ω_H. The sixth line notes that when parameter estimation using the data from Alice and Bob (the party at location P at time T) passes, it matches the security condition of the original QKD sub-protocol where these data are exchanged with authentication. The seventh line upper bounds the respective probability terms, noting $p_{A \wedge B} \leq \Pr[A|B]$. In the final line, the probability $\Pr[\Omega_H | \Omega_M^c]$ represents the probability that the hash matches, conditioned on the fact that Bob's messages do not, which is upper bounded by the 2-universal property of the hash function family, $\varepsilon_{auth} = \frac{1}{l_T}$. The probability $\Pr[\Omega_{QPV} | \Omega_H^c]$ represents the probability that QPV has passed, conditioned on the fact that the hash does not match, i.e. Bob responds to QPV challenge with random responses. This probability is equivalent to an adversary not at location P passing QPV, which can be bounded by the winning probability, ε_{QPV}.

Appendix B: Sending Authenticated Messages with QPV Security Analysis

We break the security analysis into two parts, one on the secure transmission of K, and the second involves the security of the symmetric key authentication. The security of the QPV-based authenticated message transmission can be defined by the probability that the tampering check passes, while the message sent does not match, i.e. $\Pr\left[K \neq \hat{K} \wedge \Omega_{TC}\right]$. Since every message can be mapped to a unique codeword, the probability is equivalent to a mismatch of codewords,

$$\Pr\left[K \neq \hat{K} \wedge \Omega_{TC}\right] \leq \Pr\left[C \neq \hat{C} \wedge HW(\hat{C}) = l_C + 2\right], \tag{B1}$$

which can be bounded by the nature of QPV.

We consider a QPV sub-protocol, which is secure when an adversary (not at position P) has a low winning probability ε_{QPV} (soundness of QPV) while an honest party has a high winning probability given by $1 - \varepsilon_{rob}$ (robustness of QPV). We note that by assumption, the delay between QPV rounds and the delay between QPV runs are fixed, i.e. the adversary can only break synchronization by having the two parties use different start times, t_{start}. We also assume that the delay between QPV sub-protocols, Δt, is larger than the duration for each run of the QPV sub-protocol. As such, we claim that any attempts at causing the sender and receiver to lose synchronization, i.e. having different t_{start}, would result in low probability of passing the tampering check.

Having the sender's t_{start} to not begin at the receiver's $t_{start} + \Delta t$ would result in some internal rounds within each QPV sub-protocol to run without the presence of the receiver. This results in to a larger chance of failure for rounds with $C_i = 1$ while not providing any advantage since none of the displaced internal rounds can contribute

other runs when the delay between QPV runs Δt is larger than the duration of each QPV run. Therefore, it would be optimal for the adversary to select attacks that have the sender's and receiver's start time to differ by a factor of Δt. In this scenario, either the first or final QPV run would occur in the absence of the sender. Since $C_1 = C_{2l_C+1} = 1$ is expected, the adversary has to force the QPV round to pass, which by the security of QPV, can only occur with probability less than ε_{QPV}.

Let us now consider the case where synchronization is maintained. Since $\hat{C} \neq C$ while $HW(\hat{C}) = l_C + 2$ requires at least a swap from 0 to 1 for some C_i and 1 to 0 from some C_j with indices $i, j \in \{1, \cdots, 2l_C + 1\}$, we can bound

$$\begin{aligned}\Pr\Big[K \neq \hat{K} \wedge \Omega_{TC}\Big] \leq& \Pr\Big[\exists i, j \in \{1, \cdots, 2l_C + 1\},\, s.t.\, \hat{C}_i = 1, C_i = 0, \hat{C}_j = 0, C_j = 1\Big] \\ \leq& \Pr\Big[\exists i \in \{1, \cdots, 2l_C + 1\},\, s.t.\, \hat{C}_i = 1, C_i = 0\Big] \\ \leq& l_C \varepsilon_{QPV},\end{aligned} \tag{B2}$$

where we note having $\hat{C}_j = 0$ while $C_j = 1$ can be performed with high probability and that there are l_C QPV runs with $C_i = 0$ where an adversary can attempt to force $\hat{C}_i = 1$. Combining the cases, the message authentication protocol runs with security $l_C \varepsilon_{QPV}$. Noting that we can simplify

$$\binom{2l'_C}{l'_C} \leq 2^{l_K} \implies 2^{2l'_C h_b(1/2)} \leq 2^{l_K} \implies l'_C \leq \frac{l_K}{2}, \tag{B3}$$

we can bound the security by $\lceil \frac{l_K}{2} \rceil \varepsilon_{QPV}$.

For a scenario where all parties are honest, there can be a chance where the sender's responses in QPV is recorded as a failure when $C_i = 1$. The message authentication is robust when authentication passes if all parties are honest, i.e. $HW(\hat{C}) = l_C + 2$. We can lower bound this by the probability that $C = \hat{C}$, i.e. no accidental tampering occurred. The probability can be computed

$$\begin{aligned}\Pr\Big[C = \hat{C}\Big] =& 1 - \Pr\Big[C \neq \hat{C}\Big] \\ \geq& 1 - \sum_{i=1}^{2l_C+2} \Pr\Big[C_i \neq \hat{C}_i\Big] \\ \geq& 1 - (l_C + 2) \Pr\Big[C_i = 1, \hat{C}_i = 0\Big] \\ \geq& 1 - (l_C + 2)\varepsilon_{rob},\end{aligned} \tag{B4}$$

where we note the non-response of the sender would force $\hat{C}_i = 0$ whenever $C_i = 0$. Therefore, the protocol has a robustness of $(\lceil \frac{l_K}{2} \rceil + 2)\varepsilon_{rob}$.

For the overall authenticated message protocol, we have to additionally consider the possibility that an adversary can delay some steps. The main delay tactic that an adversary can perform is to delay the arrival of M and T to the receiver. In this case, the adversary is able impersonate the receiver and perform QPV with the sender to learn of the key K before sending a different message-tag pair (M', T') that the receiver would accept. However, such a delay would require the adversary to later pass the QPV-based authenticated messaging step by representing a K' to the receiver while not being at the right location. On the other hand, if the step order is obeyed, the δ-almost strongly 2-universal family of hash functions guarantee that without knowledge of secret K (which has yet to be announced at step 2), the adversary is unable to find a second message-tag pair with probability greater than δ.

More formally, defining $T' = h_{\hat{K}}(\hat{M})$ and Ω_{MT} as the event where the message and tag arrives at the receiver before QPV is performed, the soundness (probability where messages do not match but tampering check test passes) can be

reduced to

$$\begin{aligned}
&\Pr\Big[M \neq \hat{M}, T' = \hat{T}\Big] \\
=&\Pr\Big[M \neq \hat{M}, T' = \hat{T}, \Omega_{MT}\Big] + \Pr\Big[M = \hat{M}, T' = \hat{T}, \Omega_{MT}^c\Big] \\
\leq&\Pr\Big[M \neq \hat{M}, T' = \hat{T}, \Omega_{MT}, K = \hat{K}\Big] + \Pr\Big[K \neq \hat{K}, \Omega_{TC}\Big] + \Pr[\Omega_{TC}|\Omega_{MT}^c] \\
\leq&\Pr\Big[M \neq \hat{M}, h_K(\hat{M}) = \hat{T}, \Omega_{MT}\Big] + 2\lceil\frac{l_K}{4}\rceil\varepsilon_{QPV} \\
\leq&\delta + 2\lceil\frac{l_K}{2}\rceil\varepsilon_{QPV},
\end{aligned} \tag{B5}$$

where the first line splits the delay and non-delay strategies. In the second line, we further split the probabilities based on the event $K = \hat{K}$, i.e. whether the key K is sent without tampering, and using the fact that Ω_{TC} is implicit in $T' = \hat{T}$ since no T' is generated when tampering checks fails. In the third line, the latter two terms corresponds to (1) the event where tampering check passes, but the message sent is different, and (2) the event where tampering checks pass with the sender not participating. Both events corresponds to successful attacks of the QPV-based authenticated transmission of K, which is bounded by the soundness $\lceil\frac{l_K}{2}\rceil\varepsilon_{QPV}$. The final line gives the probability that an adversary can find a message-tag pair $(\hat{M}, \hat{T})$ without knowing K (since it is announced after $\hat{T}$ arrives at Bob), and thus is bounded by the δ-almost two-universal property of the hash family. The robustness of Protocol 2 matches that of the robustness of the QPV-based message authentication protocol since no additional avenues of abort is introduces, i.e. the protocol is $(\lceil\frac{l_K}{2}\rceil + 2)\varepsilon_{rob}$-robust.

Appendix C: Secure Key Exchange with Location Credentials Security Analysis

We show the security of Protocol 3 reduces to the security of the QKD sub-protocol, the QPV sub-protocol and the δ-almost strongly 2-universal hash family. We can consider a QPV sub-protocol with ε_{rob}-robustness and ε_{QPV}-soundness and a δ-almost strongly 2-universal hash family, which allows the sending of an authenticated message with QPV as discussed in Sec. IV B. We can also consider a QKD sub-protocol with delayed authentication, with the QPV steps replaced by authentication channels, i.e. messages are transmitted without tampering and loss. We note that such protocols exists [15, 16], and can assume that they have been properly designed to provide QKD security at ε_{QKD}. More specifically, consider the events

1. Ω_M: Event where messages match, $M_A = \hat{M}_A$ and $M_B = \hat{M}_B$ (equivalently $M = M'$).
2. $\Omega_{PE,A}$ and $\Omega_{PE,B}$: Event where Alice and Bob believes parameter estimation passes, $I_{PE,A} = 1$ and $I_{PE,B} = 1$.
3. $\Omega'_{PE,A}$ and $\Omega'_{PE,B'}$: Event where $I_{PE,A} = 1$ and $I_{PE,B} = 1$ if they are determined from M_A and M_B (untampered messages).
4. Ω_K: Event where the sending of authenticated hash function key is successful ($K = \hat{K}$).
5. Ω_T: Event where tag T is not tampered by the adversary.
6. Ω_H: Event where $I = 1$, i.e. the tags match $\hat{T} = h_{\hat{K}}(M')$.

If the QPV sub-protocol (step 6) and authenticated message transfer (steps 3 to 5) are replaced by perfect authentication channels, both Alice and Bob would decide to jointly generate keys in the event where the messages match perfectly and parameter estimation passes, $\Omega_{PE,A} \wedge \Omega_{PE,B} \wedge \Omega_M$. As such we define the QKD security as

$$\varepsilon_{QKD} = \Delta(\rho_{K_AK_BE\wedge\Omega'_{PE,A}\wedge\Omega'_{PE,B}\wedge\Omega_M}, \tilde{\tau}_{K_AK_B} \otimes \rho_{E\wedge\Omega'_{PE,A}\wedge\Omega'_{PE,B}\wedge\Omega_M}), \tag{C1}$$

where we note that $\Omega_M \wedge \Omega_{PE,A} \wedge \Omega_{PE,B} = \Omega_M \wedge \Omega'_{PE,A} \wedge \Omega'_{PE,B}$, which provides a security guarantee independent on the method of sending authenticated messages.

In the proposed protocol, Alice generates a secret key when $\Omega_A = \Omega_{QPV} \wedge \Omega_{PE,A}$ while Bob generates a secret key when $\Omega_B = \Omega_H \wedge \Omega_{PE,B}$. As such, the security can be split based on the scenarios,

$$\begin{aligned}
\Delta(\rho_{K_AK_BE}, \rho^{ideal}_{K_AK_BE}) \leq&\Pr[\Omega_A \wedge \Omega_B^c] + \Delta(\rho_{K_BE\wedge\Omega_B\wedge\Omega_A^c}, \tau_{K_B} \otimes \rho_{E\wedge\Omega_B\wedge\Omega_A^c}) \\
&+ \Delta(\rho_{K_AK_BE\wedge\Omega_A\wedge\Omega_B}, \tilde{\tau}_{K_AK_B} \otimes \rho_{E\wedge\Omega_A\wedge\Omega_B}),
\end{aligned} \tag{C2}$$

and we can analyze each term separately.

The first term is the probability that Alice generates a key while Bob does not. Since Bob does participate in the QPV sub-protocol when he aborts, it is difficult for any adversary to force QPV to pass for Alice, i.e.

$$\Pr[\Omega_A \wedge \Omega_B^c] \leq \Pr[\Omega_{QPV}|\Omega_B^c] \leq \varepsilon_{QPV}, \tag{C3}$$

with a guarantee by the soundness of QPV.

The second term corresponds to the case where Bob generates a key while Alice does not. We can remove the condition where Alice does not generate a key,

$$\Delta(\rho_{K_B E \wedge \Omega_B \wedge \Omega_A^c}, \tau_{K_B} \otimes \rho_{E \wedge \Omega_B \wedge \Omega_A^c}) \leq \Delta(\rho_{K_B E \wedge \Omega_H \wedge \Omega_{PE,B}}, \tau_{K_B} \otimes \rho_{E \wedge \Omega_H \wedge \Omega_{PE,B}}). \tag{C4}$$

The trace distance can be simplified by splitting it into three mutually exclusive regions,

$$\begin{aligned} &\Delta(\rho_{K_B E \wedge \Omega_H \wedge \Omega_{PE,B}}, \tau_{K_B} \otimes \rho_{E \wedge \Omega_H \wedge \Omega_{PE,B}}) \\ \leq &\Delta(\rho_{K_B E \wedge \Omega_H \wedge \Omega_{PE,B} \wedge \Omega_{PE,A} \wedge \Omega_M}, \tau_{K_B} \otimes \rho_{E \wedge \Omega_H \wedge \Omega_{PE,B} \wedge \Omega_{PE,A} \wedge \Omega_M}) \\ &+ \Pr[\Omega_H \wedge \Omega_{PE,A} \wedge \Omega_{PE,B} \wedge \Omega_M^c] + \Pr\big[\Omega_H \wedge \Omega_{PE,B} \wedge \Omega_{PE,A}^c\big]. \end{aligned} \tag{C5}$$

Since $\Omega_M \wedge \Omega_{PE,A} \wedge \Omega_{PE,B} = \Omega_M \wedge \Omega'_{PE,A} \wedge \Omega'_{PE,B}$, we can upper bound the first component by

$$\begin{aligned} &\Delta(\rho_{K_B E \wedge \Omega_H \wedge \Omega_{PE,B} \wedge \Omega_{PE,A} \wedge \Omega_M}, \tau_{K_B} \otimes \rho_{E \wedge \Omega_H \wedge \Omega_{PE,B} \wedge \Omega_{PE,A} \wedge \Omega_M}) \\ \leq &\Delta(\rho_{K_B E \wedge \Omega'_{PE,B} \wedge \Omega'_{PE,A} \wedge \Omega_M}, \tau_{K_B} \otimes \rho_{E \wedge \Omega'_{PE,B} \wedge \Omega'_{PE,A} \wedge \Omega_M}) \\ \leq &\Delta(\rho_{K_A K_B E \wedge \Omega'_{PE,B} \wedge \Omega'_{PE,A} \wedge \Omega_M}, \tilde{\tau}_{K_A K_B} \otimes \rho_{E \wedge \Omega'_{PE,B} \wedge \Omega'_{PE,A} \wedge \Omega_M}) \\ \leq &\varepsilon_{QKD}, \end{aligned} \tag{C6}$$

where the second inequality uses the fact that partial trace of K_A cannot increase trace distance. The second component follows from the the security of the message authentication from QPV protocol,

$$\Pr[\Omega_H \wedge \Omega_{PE,A} \wedge \Omega_{PE,B} \wedge \Omega_M^c] \leq \Pr\Big[M \neq \hat{M}, T' = \hat{T}\Big] \leq \delta + 2\lceil \frac{l_K}{2} \rceil \varepsilon_{QPV}. \tag{C7}$$

The final term describes the scenario that Alice decides that parameter estimation has failed, $I_{PE,A} = 0$, where she does not participate in sending the authenticated message K. As such, we can bound

$$\Pr\big[\Omega_H \wedge \Omega_{PE,B} \wedge \Omega_{PE,A}^c\big] \leq \Pr\big[\Omega'_{QPV}|\Omega_{PE,A}^c\big] \leq \varepsilon_{QPV}, \tag{C8}$$

where Ω'_{QPV} refers to the first QPV run within Protocol 2, noting that we can bound the overall probability of obtaining $HW(\hat{C}) = l_C + 2$ by the probability of passing the first QPV run and forcing $\hat{C}_1 = 1$ when Alice does not participate. Combining the results, the second term yields

$$\Delta(\rho_{K_B E \wedge \Omega_B \wedge \Omega_A^c}, \tau_{K_B} \otimes \rho_{E \wedge \Omega_B \wedge \Omega_A^c}) \leq \varepsilon_{QKD} + \delta + (2\lceil \frac{l_K}{2} \rceil + 1)\varepsilon_{QPV}, \tag{C9}$$

which are dependent on the security of the component protocols.

The final term can be simplified in a similar manner, splitting into two mutually exclusive regions,

$$\begin{aligned} &\Delta(\rho_{K_A K_B E \wedge \Omega_A \wedge \Omega_B}, \tilde{\tau}_{K_A K_B} \otimes \rho_{E \wedge \Omega_A \wedge \Omega_B}) \\ \leq &\Delta(\rho_{K_A K_B E \wedge \Omega_{QPV} \wedge \Omega_{PE,A} \wedge \Omega_H \wedge \Omega_{PE,B} \wedge \Omega_M}, \tilde{\tau}_{K_A K_B} \otimes \rho_{E \wedge \Omega_{QPV} \wedge \Omega_{PE,A} \wedge \Omega_H \wedge \Omega_{PE,B} \wedge \Omega_M}) \\ &+ \Pr[\Omega_{QPV} \wedge \Omega_{PE,A} \wedge \Omega_H \wedge \Omega_{PE,B} \wedge \Omega_M^c], \end{aligned} \tag{C10}$$

where the latter term is bounded by $\delta + 2\lceil \frac{l_K}{2} \rceil \varepsilon_{QPV}$. The first term can be simplified by removing conditions except $\Omega_{PE,A} \wedge \Omega_{PE,B} \wedge \Omega_M$, reducing it to the QKD security parameter, ε_{QKD}.

Therefore, the overall security can be given by

$$\Delta(\rho_{K_A K_B E}, \rho_{K_A K_B E}^{ideal}) \leq 2\varepsilon_{QKD} + 2\delta + (4\lceil \frac{l_K}{2} \rceil + 2)\varepsilon_{QPV}. \tag{C11}$$

The robustness of the protocol is a simple combination of the robustness of the QKD protocol ε_{rob}^{QKD}, the QPV sub-protocol ε_{rob}^{QPV}, and the authenticated message transfer protocol ε_{rob}^{auth},

$$\begin{aligned}\varepsilon_{rob} =& \Pr[\Omega_A^c \vee \Omega_B^c] \\ =& \Pr\left[\Omega_{QPV}^c \vee \Omega_{PE,A}^c \vee \Omega_{PE,B}^c \vee \Omega_H^c\right] \\ \leq& \Pr\left[\Omega_{PE,A}^{'c} \vee \Omega_{PE,B}^{'c}\right] + \Pr[\Omega_H^c \wedge \Omega_{PE,A}] + \Pr\left[\Omega_{QPV}^c \wedge \Omega_H \wedge \Omega_{PE,B}\right] \\ \leq& \varepsilon_{rob}^{QKD} + \varepsilon_{rob}^{auth} + \varepsilon_{rob}^{QPV} \\ \leq& \varepsilon_{rob}^{QKD} + (\lceil \frac{l_K}{2} \rceil + 3)\varepsilon_{rob}^{QPV}\end{aligned} \tag{C12}$$

where the third line splits the probability into mutually exclusive regions, and notes that the messages are not tampered in the honest case, i.e. $\Omega_{PE,A/B} = \Omega'_{PE,A/B}$. In the fourth line, we notice that failing any parameter estimation tests corresponds to the robustness of QKD, failing the authenticated message transfer when Alice is involved in the protocol corresponds to the robustness of authenticated message transfer, and failing QPV when Bob is involved in the protocol corresponds to the robustness of the single QPV sub-protocol run.

Appendix D: Purifying QPV Attacks

1. Partial Purification

We first define the winning probability by through an optimization problem:

$$\begin{aligned}\max_{\substack{\sigma_{AB}^r \in \mathcal{S}_{2q} \\ \mathcal{E}_{AQ}^{xr} \in \mathcal{C}_{q+1}, \mathcal{E}_B^{yr} \in \mathcal{C}_q \\ \{A_z^{xyr}\}, \{B_z^{xyr}\}}} & \sum_{rzxy} \frac{p_r}{|\mathcal{X}||\mathcal{Y}|} \mathrm{Tr}\left[(\Pi_z^{f(x,y)} \otimes A_z^{xyr} \otimes B_z^{xyr}) \rho_{A'B'V}^{xyr}\right] \\ subj.to \quad & \sum_{xyr} \frac{p_r}{|\mathcal{X}||\mathcal{Y}|} \mathrm{Tr}[(\mathbb{I}_V \otimes A_\perp^{xyr} \otimes B_\perp^{xyr}) \rho_{A'B'V}^{xyr}] = 1 - \eta \\ & \mathrm{Tr}[(\mathbb{I}_V \otimes A_z^{xyr} \otimes B_{\bar{z}}^{xyr}) \rho_{A'B'V}^{xyr}] = 0, \, \forall z, x, y, r\end{aligned}, \tag{D1}$$

where

$$\rho_{A'B'V}^{xyr} = \mathcal{M} \circ \mathcal{E}_{AQ}^{xr}(\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|_{VQ} \otimes \mathcal{E}_B^{yr}(\sigma_{AB}^r)) \tag{D2}$$

and $\mathcal{M}$ refers to the map from AB to $A'B'$.

The purification can be performed in two steps. We first purify the quantum system by introducing a quantum system P of dimension 2^{2q}, and selecting a purification such that $\mathrm{Tr}_P[|\psi_r\rangle\langle\psi_r|_{ABP}] = \sigma_{AB}^r$ [19]. Furthermore, we can lift the quantum channels to higher dimensional unitaries by introducing quantum systems P_A and P_B, of dimension $2^{2(q+1)}$ and 2^{2q} respectively, and selecting the unitaries such that $\mathrm{Tr}_{P_A}[U_{AQP_A}^{xr}(\rho_{AQ} \otimes |0\rangle\langle 0|_{P_A}) U_{AQP_A}^{xr\dagger}] = \mathcal{E}_{AQ}^{xr}(\rho)$ for any state ρ_{AQ} and $\mathrm{Tr}_{P_B}[U_{BP_B}^{yr}(\rho_B \otimes |0\rangle\langle 0|_{P_B}) U_{BP_B}^{yr\dagger}] = \mathcal{E}_B^{yr}(\rho_B)$ for any state ρ_B [19]. We note that the states and channels for different value r can be separately purified, with the purification system being of the same Hilbert space, since they can be distinguished from the value of r. Collating the changes, this leads to the partially purified state

$$\rho_{A'B'VPP_AP_B} = \sum_r p_r |r\rangle\langle r|_R \otimes \mathcal{M}[(U_{AQP_A}^{xr} \otimes U_{BP_B}^{yr})(\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|_{VQ} \otimes |\psi^r\rangle\langle\psi^r|_{ABP} \otimes |0\rangle\langle 0|_{P_AP_B})(U_{AQP_A}^{xr} \otimes U_{BP_B}^{yr})^\dagger]$$

and $\mathrm{Tr}_{PP_AP_B}[\rho_{A'B'VPP_AP_B}] = \rho_{A'B'V}$.

As a consequence, any mixed state strategy can be expressed as a pure state strategy of the higher dimension. As such, optimizing over the larger set of higher dimension pure state strategy can only lead to a larger winning

probability, given by

$$\begin{aligned} \max_{\substack{|\psi^r\rangle_{ABP}\in\mathcal{S}^p_{4q} \\ U^{xr}_{AQP_A}\in\mathcal{C}^U_{3(q+1)}, U^{yr}_{BP_B}\in\mathcal{C}^U_{3q} \\ \{A^{xyr}_z\},\{B^{xyr}_z\}}} & \sum_{rzxy} \frac{p_r}{|\mathcal{X}||\mathcal{Y}|} \operatorname{Tr}\left[(\Pi_z^{f(x,y)} \otimes A_z^{xyr} \otimes B_z^{xyr}) \left|\Psi_{xyr}\right\rangle\!\left\langle\Psi_{xyr}\right|\right] \\ subj.to \quad & \sum_{xyr} \frac{p_r}{|\mathcal{X}||\mathcal{Y}|} \operatorname{Tr}[(\mathbb{I}_V \otimes A_\perp^{xyr} \otimes B_\perp^{xyr}) \left|\Psi_{xyr}\right\rangle\!\left\langle\Psi_{xyr}\right|] = 1-\eta \\ & \operatorname{Tr}[(\mathbb{I}_V \otimes A_z^{xyr} \otimes B_{\bar{z}}^{xyr}) \left|\Psi_{xyr}\right\rangle\!\left\langle\Psi_{xyr}\right|] = 0,\ \forall z,x,y,r \end{aligned}, \tag{D3}$$

where

$$\left|\Psi_{xyr}\right\rangle_{A'B'V} = \mathcal{M}'(U^{xr}_{AQP_A} \otimes U^{yr}_{BP_B})(\left|\Phi^+\right\rangle_{VQ} \otimes \left|\psi_r\right\rangle_{ABP}), \tag{D4}$$

and M' is the permutation matrix representing the mapping from AQB to $A'B'$.

2. Net Size of Purified Strategy

It is known that the upper bound of the covering number of a hypersphere with norm 1 can be given by [23]

Theorem 12. *Let $\|.\|$ be any norm on points $x \in \mathbb{R}^d$. The covering number for a δ-net for a norm-ball of unit radius can be bounded by*

$$|\mathcal{N}| \leq \left(1+\frac{2}{\delta}\right)^d$$

As such, we can compute the covering number for the set of pure states,

Theorem 13. *The set of pure states in a Hilbert space with dimension d, i.e. $\{|\psi\rangle : |\psi\rangle \in \mathcal{H}_d\}$, has a δ-covering net in the Euclidean norm with covering number*

$$|\mathcal{N}_S| \leq \left(1+\frac{2}{\delta}\right)^{2d}$$

Proof. The set of pure states in a Hilbert space with dimension d, can be described by

$$\left|\psi\right\rangle = \sum_{j=1}^{d} (a_j + b_j i) \left|j\right\rangle, \tag{D5}$$

for any orthonormal basis $\{|j\rangle\}_j$, with the normalization constraint $\sqrt{\sum_j (a_j^2+b_j^2)} = 1$. As such, the set of pure states forms a unit sphere in Euclidean norm, with $x = (\{a_j\}_j, \{b_j\}_j)$, i.e. $x \in \mathbb{R}^{2d}$, and with $\|x\|_2 = 1$ for all states. Therefore, by Thm. 12, $|\mathcal{N}_S| \leq \left(1+\frac{2}{\delta}\right)^{2d}$. □

Consequently, since we consider $4q$-qubit pure states,

$$\log_2 |\mathcal{N}_S| \leq 2^{4q+1} \log_2 \left(1+\frac{2}{\delta}\right). \tag{D6}$$

We can also compute the covering number for a unitary matrix in operator norm, using ideas from Ref. [24]. We note that operator norm here is defined to be induced from the 2-norm, i.e. $\|A\|_{op} = \max_{\|x\|_2 \leq 1} \|Ax\|_2$.

Theorem 14. *The set of unitary matrices that acts on a Hilbert space with dimension d, i.e. $\{U|U : \mathcal{H}_d \to \mathcal{H}_d\}$, has a δ-covering net in the operator norm with covering number*

$$|\mathcal{N}_U| \leq \left(1+\frac{2}{\delta}\right)^{2d^2}.$$

Proof. Since all unitary operators do not alter the Euclidean norm of any vector, all unitary operators have operator norm 1, $\|U\|_{op} = 1$. As such, we can describe the set of unitary operators $U = \sum_{jk}(a_{jk} + b_{jk}i)\,|j\rangle\langle k|$ by a vector $x = (\{a_{jk}\}_{jk}, \{b_{jk}\}_{jk})$, with $x \in \mathbb{R}^{2d^2}$, since the unitary contain d^2 complex entries. The set of unitaries are constrained by $\|x\|_{opvec} = 1$, where $\|.\|_{opvec}$ is a norm on the vector $x \in \mathbb{R}^{2d^2}$, and is computed by reforming x into the corresponding unitary matrix and computing the corresponding operator norm. Therefore, by Thm. 12, $|\mathcal{N}_U| \leq \left(1 + \frac{2}{\tilde{\delta}}\right)^{2d^2}$. □

Consequently, for the two unitary matrices we consider, we have

$$\begin{aligned} \log_2 |\mathcal{N}_A| &\leq 2^{6q+7} \log_2 \left(1 + \frac{2}{\delta}\right) \\ \log_2 |\mathcal{N}_B| &\leq 2^{6q+4} \log_2 \left(1 + \frac{2}{\delta}\right). \end{aligned} \tag{D7}$$

In the proof of Thm. 14, we have not made used of the fact that U_A and U_B are purification of their corresponding CPTP maps. This purification property implies that only the first 2^q row of the unitary matrix is relevant to describe the strategy since the states are always initialized as $|0\rangle$ in systems $P_A P_B$. As such, it may be possible to further reduce the covering number by restricting the set of unitaries discussed. For simplicity, we leave any such optimization to future work.

Appendix E: Transmission and Error Partitioning Security

1. Proof of Thm. 6

Let us choose $\delta < \frac{\tilde{\delta}}{6}$. Consider δ-nets $\mathcal{N}_S$, $\mathcal{N}_A$ and $\mathcal{N}_B$, corresponding to that for the set of pure states of dimension $4q$ in Euclidean norm, the set of unitaries acting on Hilbert space with dimension $3(q+1)$ in operator norm, and the set of unitaries acting on Hilbert space with dimension $3q$ in operator norm. Let $|\phi_\lambda\rangle \in \mathcal{N}_S$, $U_A^{x'} \in \mathcal{N}_A$ and $U_B^{y'} \in \mathcal{N}_B$, where λ, x' and y' label the choice of the nets. Define an set that extends $\mathcal{S}_i^{\tilde{\varepsilon},\tilde{\eta}}$ by a 3δ-ball, $\mathcal{S}_{i,3\delta}^{\tilde{\varepsilon},\tilde{\eta}} = \{|\psi\rangle : \exists\, |\phi\rangle \in \mathcal{S}_i^{\tilde{\varepsilon},\tilde{\eta}}, \Delta(|\psi\rangle, |\phi\rangle) \leq 3\delta\}$. Note that by choice of δ and the fact that $\mathcal{S}_0^{\tilde{\varepsilon},\tilde{\eta}}$ and $\mathcal{S}_1^{\tilde{\varepsilon},\tilde{\eta}}$ are more than 6δ apart in trace distance, the two extended sets do not intersect. This allows us to define a function g that computes an output for each net,

$$g(x', y', \lambda) = \begin{cases} 0 & (U_A^{x'} \otimes U_B^{y'})(|\phi_\lambda\rangle \otimes |\Phi^+\rangle) \in \mathcal{S}_{0,3\delta}^{\tilde{\varepsilon},\tilde{\eta}} \\ 1 & (U_A^{x'} \otimes U_B^{y'})(|\phi_\lambda\rangle \otimes |\Phi^+\rangle) \in \mathcal{S}_{1,3\delta}^{\tilde{\varepsilon},\tilde{\eta}} \\ 0/1 & (U_A^{x'} \otimes U_B^{y'})(|\phi_\lambda\rangle \otimes |\Phi^+\rangle) \notin \mathcal{S}_{0,3\delta}^{\tilde{\varepsilon},\tilde{\eta}}, \mathcal{S}_{1,3\delta}^{\tilde{\varepsilon},\tilde{\eta}} \end{cases}. \tag{E1}$$

We note here that the choice of 0 or 1 does not matter in the final scenario, and a random choice can be made.

What remains is to prove that the g defined forms a classical rounding. For any sub-strategies with $(\varepsilon_{\text{thres}}, \eta_{\text{thres}}, l_{1,r}, l_{2,r}, l_{3,r}, l_{4,r})$-partition, we can define $x' = f_A(x)$, $y' = f_B(y)$, λ as the labels indicating the closest unitary and state (of the nets) to $U_{AQP_A}^{xr}$, $U_{BP_B}^{yr}$ and $|\psi_r\rangle_{ABP}$. For any of the $l_{1,r}$ (x, y) pairs, the strategy satisfies $p_{e|rxy} \leq \varepsilon_{\text{thres}}\eta$, $p_{t|rxy} \geq \eta_{\text{thres}}$ and the matching condition. As such, the state generated before measurement is given by $(U_{AQP_A}^{xr} \otimes U_{BP_B}^{yr})\,|\psi_r'\rangle \in \mathcal{S}_{f(x,y)}^{\tilde{\varepsilon},\tilde{\eta}}$, where we define $|\psi_r'\rangle = |\psi_r\rangle \otimes |\Phi^+\rangle$. By definition of the δ-net, we can always find the a closest unitary and state $U_A^{x'}$, $U_B^{y'}$ and $|\phi_\lambda\rangle$, each of which is δ-close to the strategy. We can therefore show that

$(U^{xr}_{AQP_A} \otimes U^{yr}_{BP_B}) |\psi'_r\rangle$ and $(U^{x'}_A \otimes U^{y'}_B) |\phi'_\lambda\rangle$ are close, where we define $|\phi'_\lambda\rangle = |\phi_\lambda\rangle \otimes |\Phi^+\rangle$

$$\begin{aligned}
&\Delta((U^{xr}_{AQP_A} \otimes U^{yr}_{BP_B}) |\psi'_r\rangle, (U^{x'}_A \otimes U^{y'}_B) |\phi'_\lambda\rangle) \\
\leq &\left\| (U^{xr}_{AQP_A} \otimes U^{yr}_{BP_B}) |\psi'_r\rangle - (U^{x'}_A \otimes U^{y'}_B) |\phi'_\lambda\rangle \right\|_2 \\
\leq &\left\| (U^{xr}_{AQP_A} \otimes U^{yr}_{BP_B}) |\psi'_r\rangle - (U^{x'}_A \otimes U^{yr}_{BP_B}) |\psi'_r\rangle \right\|_2 + \left\| (U^{x'}_A \otimes U^{yr}_{BP_B}) |\psi'_r\rangle - (U^{x'}_A \otimes U^{y'}_B) |\psi'_r\rangle \right\|_2 \\
&+ \left\| (U^{x'}_A \otimes U^{y'}_B) |\psi'_r\rangle - (U^{x'}_A \otimes U^{y'}_B) |\phi'_\lambda\rangle \right\|_2 \\
\leq &\left\| (U^{xr}_{AQP_A} - U^{x'}_A) \otimes \mathbb{I} \right\|_{op} \left\| (\mathbb{I} \otimes U^{yr}_{BP_B}) |\psi_r\rangle' \right\|_2 + \left\| \mathbb{I} \otimes (U^{yr}_{BP_B} - U^{y'}_B) \right\|_{op} \left\| (U^{x'}_A \otimes \mathbb{I}) |\psi'_r\rangle \right\|_2 \\
&+ \| |\psi'_r\rangle - |\phi'_\lambda\rangle \|_2 \\
\leq &3\delta.
\end{aligned} \tag{E2}$$

Therefore, $(U^{x'}_A \otimes U^{y'}_B) |\phi'_\lambda\rangle \in \mathcal{S}^{\tilde{\varepsilon},\tilde{\eta}}_{f(x,y),3\delta}$, and we can correctly assign the value of $g(x', y', \lambda) = f(x, y)$. We note that the δ-net for unitaries are defined by norm $\|\cdot\|_{opvec}$, and $\|u - v\|_{opvec} = \|U - V\|_{op}$, where u and v are vector representation of the unitaries U and V. Since this works for all $l_{1,r}$ pairs of (x, y) and for any sub-strategies, we can conclude that g is a valid classical rounding.

The sizes of the discretized sets are given by Eqn. (D6) and Eqn. (D7). Therefore, we select the maximum set size as k, with

$$k = 2^{6q+7} \left[\left[\log_2 \left(1 + \frac{12}{\tilde{\delta}} \right) \right] + 1 \right], \tag{E3}$$

where we note that δ can be selected close enough to $\frac{\tilde{\delta}}{6}$ to cause a single bit change in the logarithm value.

2. Proof of Thm. 7

For a fixed classical rounding of size k, it is possible to implement a maximum of $2^k \times (2^k)^{2^n} \times (2^k)^{2^n} = 2^{k(2^{n+1}+1)}$ functions. Therefore, for a random function f, the probability that we can find a suitable f_A and f_B such that $g(f_A(x), f_B(y), \lambda)$ and $f(x, y)$ differ in at most $2^{2n}\nu$ (x, y) pairs (represented by the Hamming distance between a bitstring describing the output for each input) is

$$\begin{aligned}
&\Pr\left[f : \exists f_A, f_B, \lambda \, s.t. \, d_H(f, g) \leq 2^{2n}\nu \right] \\
= &\frac{\left| f : \exists f_A, f_B, \lambda \, s.t. \, d_H(f, g) \leq 2^{2n}\nu \right|}{|\{f : \{0,1\}^{2n} \to \{0,1\}|} \\
\leq &\frac{|f : \exists f_A, f_B, \lambda \, s.t. \, d_H(f, g) = 0| [\sum_{i=0}^{2^{2n}\nu} \binom{2^{2n}}{i}]}{2^{2^{2n}}} \\
\leq &2^{k(2^{n+1}+1) + 2^{2n} h_b(\nu) - 2^{2n}} \\
\leq &2^{2n} \left\{ h_b(\nu) - 1 + 2^{9-6q_0} \left[\left[\log_2 \left(1 + \frac{12}{\tilde{\delta}} \right) \right] + 1 \right] \right\},
\end{aligned} \tag{E4}$$

where the third line upper bounds the number of functions with Hamming distances less than $2^{2n}\nu$ by considering functions with zero Hamming distance and including a ball of functions that are less than $2^{2n}\nu$ in Hamming distance from these functions, and the fourth line provides a bound on the sum of binomial coefficients [25] using binary entropy $h_b(x)$, while the final line expands k and performs some upper bounding to simplify the equation. We want to select a suitable ν such that being able to find f_A and f_B is the exception that occurs with probability less than $2^{-\alpha}$, which implies

$$\nu = h_b^{-1} \left\{ 1 - 2^{9-6q_0} \left[\left[\log_2 \left(1 + \frac{12}{\tilde{\delta}} \right) \right] + 1 \right] - \frac{\alpha}{2^{2n}} \right\}, \tag{E5}$$

where we note $\nu \in [0, \frac{1}{2}]$ for the inverse of binary entropy to exist.

3. Proof of Thm. 9

We can compute the total error of any sub-strategy with $(\varepsilon_{\text{thres}}, \eta_{\text{thres}}, \{l_{1,r}, l_{2,r}, l_{3,r}, l_{4,r}\}_r)$-partition by

$$p_{err|r} = \frac{1}{2^{2n}} \sum_{i=1}^{4} l_{i,r} p_{err|i}, \tag{E6}$$

where $p_{err|i}$ is the average error for events in their respective partitions. We can lower bound this error probability by the definition of the partitions.

$$p_{err|r} > \frac{1}{2^{2n}} \varepsilon_{\text{thres}} \eta (l_{3,r} + l_{4,r}). \tag{E7}$$

Similarly, we have that the average transmission of the sub-strategy is bounded,

$$\begin{aligned} \eta_r =& \frac{1}{2^{2n}} \sum_{i=1}^{4} l_{i,r} \eta_{r|i} \\ \leq& \frac{1}{2^{2n}} [(l_{1,r} + l_{3,r}) + (l_{2,r} + l_{4,r}) \eta_{\text{thres}}] \\ =& \frac{1}{2^{2n}} [(l_{1,r} + l_{3,r})(1 - \eta_{\text{thres}}) + 2^{2n} \eta_{\text{thres}}], \end{aligned} \tag{E8}$$

noting that $\sum_{i=1}^{4} l_{i,r} = 2^{2n}$ since the partitions sum to include all (x, y) pairs. As such, we can formulate a linear program (LP) to find a valid lower bound on p_{err}. By defining $l'_{i,r} = \frac{1}{2^{2n}} l_{1,r}$, the lower bound can be given by

$$\begin{aligned} \min \quad & (l'_{3,r} + l'_{4,r}) \varepsilon_{\text{thres}} \eta \\ \textit{subj. to} \quad & l'_{1,r} + l'_{2,r} + l'_{3,r} + l'_{4,r} = 1 \\ & l'_{i,r} \geq 0, \forall i \\ & l'_{1,r} \leq 1 - \nu \\ & l'_{1,r} + l'_{3,r} \geq \frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}} \end{aligned} \tag{E9}$$

We can solve the LP analytically.

We consider two cases, one where $1 - \nu > \frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}}$ and one where $1 - \nu \leq \frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}}$. In the first case, one primal solution is $(l'_{1,r}, l'_{2,r}, l'_{3,r}, l'_{4,r}) = (\frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}}, 1 - \frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}}, 0, 0)$, if $\eta_r \geq \eta_{\text{thres}}$, or $(l'_{1,r}, l'_{2,r}, l'_{3,r}, l'_{4,r}) = (0, 1, 0, 0)$, if $\eta_r < \eta_{\text{thres}}$. In both scenarios, we have that a primal value of 0. In the second case, we can have a primal solution $(l'_{1,r}, l'_{2,r}, l'_{3,r}, l'_{4,r}) = (1 - \nu, 1 - \frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}}, \frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}} - 1 + \nu, 0)$, which gives a primal value of $(\frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}} - 1 + \nu) \varepsilon_{\text{thres}} \eta$.

To prove that these solutions are optimal, we construct the dual of the LP. We first note that for simplicity, we can combine the first two constraints by removing $l'_{2,r}$, giving $l'_{1,r} + l'_{3,r} + l'_{4,r} \leq 1$. We then construct a Lagrangian,

$$\begin{aligned} \mathcal{L}(\{l_{i,r}\}_i, \{\lambda_j\}_j) =& (l'_{3,r} + l'_{4,r}) \varepsilon_{\text{thres}} \eta + \lambda_1 (-l'_{1,r}) + \lambda_2 (-l'_{3,r}) + \lambda_3 (-l'_{4,r}) + \lambda_4 (1 - l'_{1,r} - l'_{3,r} - l'_{4,r}) \\ & + \lambda_5 (l'_{1,r} - 1 + \nu) + \lambda_6 \left(\frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}} - l'_{1,r} - l'_{3,r} \right), \end{aligned} \tag{E10}$$

where $\lambda_i \geq 0$ are the dual variables. We can therefore construct the dual problem, as

$$\begin{aligned} \max \quad & -\lambda_4 - \lambda_5 (1 - \nu) + \lambda_6 \frac{\eta_r - \eta_{\text{thres}}}{1 - \eta_{\text{thres}}} \\ \textit{subj. to} \quad & \lambda_j \geq 0, \forall j \\ & \lambda_1 + \lambda_6 = \lambda_4 + \lambda_5 \\ & \lambda_2 + \lambda_6 = \lambda_4 + \varepsilon_{\text{thres}} \eta \\ & \lambda_3 = \lambda_4 + \varepsilon_{\text{thres}} \eta. \end{aligned} \tag{E11}$$

Consider the first case of $1-\nu > \frac{\eta_r-\eta_{\text{thres}}}{1-\eta_{\text{thres}}}$. We can choose the dual solution $\vec{\lambda} = (0, \varepsilon_{\text{thres}}\eta, \varepsilon_{\text{thres}}\eta, 0, 0, 0)$, which satisfies all constraints and gives a dual value of 0. For the second case of $1-\nu \leq \frac{\eta_r-\eta_{\text{thres}}}{1-\eta_{\text{thres}}}$, we can take the dual solution $\vec{\lambda} = (0, 0, \varepsilon_{\text{thres}}\eta, 0, \varepsilon_{\text{thres}}\eta, \varepsilon_{\text{thres}}\eta)$, which gives dual value $\varepsilon_{\text{thres}}\eta[\frac{\eta_r-\eta_{\text{thres}}}{1-\eta_{\text{thres}}} - 1 + \nu]$. Since LP has strong duality, the matching primal and dual solution provides the optimal solution, which can be summarized as

$$p_{err|r} \leq \max\{\varepsilon_{\text{thres}}\eta[\frac{\eta_r - \eta_{\text{thres}}}{1-\eta_{\text{thres}}} - 1 + \nu], 0\}. \tag{E12}$$

Appendix F: Improvement to Trace Distance Bound Proof

Since $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are pure states in the same Hilbert space, their trace distance is related to their inner product (or fidelity) via [19]

$$\Delta(|\Psi_0\rangle, |\Psi_1\rangle) = \sqrt{1 - |\langle\Psi_0|\Psi_1\rangle|^2}. \tag{F1}$$

The states also must satisfy the constraints from $\tilde{\mathcal{S}}_i^{\tilde{\varepsilon},\tilde{\eta}}$, namely the error rate, transmission rate and mismatch responses. The mismatch of responses implies that the state is chosen such that $A_z^i \otimes B_{z'}^i$ measurements for $z \neq z'$ yield 0 expectation value, i.e. for any i, j and $z \neq z'$,

$$\langle\psi_{ij}|A_z^i \otimes B_{z'}^i|\psi_{ij}\rangle = 0. \tag{F2}$$

The transmission rate for each state is given by the probability that Alice and Bob do not respond with $\perp$,

$$\langle\Psi_i|\mathbb{I} \otimes (A_0^i \otimes B_0^i + A_1^i \otimes B_1^i)|\Psi_i\rangle \geq \tilde{\eta}, \tag{F3}$$

which gives

$$\frac{1}{2}\sum_{j=0}^{1} \langle\psi_{ij}|A_0^i \otimes B_0^i + A_1^i \otimes B_1^i|\psi_{ij}\rangle \geq \tilde{\eta} \tag{F4}$$

when expanded. The error rate for each state is given that the probability that Alice and Bob's responses do not match with the verifiers. For basis 0, the Z-basis, this is given by

$$\langle\Psi_0|(|0\rangle\langle 0| \otimes A_1^0 \otimes B_1^0 + |1\rangle\langle 1| \otimes A_0^0 \otimes B_0^0)|\Psi_0\rangle \leq \tilde{\varepsilon}, \tag{F5}$$

which can be expanded as

$$\frac{1}{2}[\,\langle\psi_{00}|A_1^0 \otimes B_1^0|\psi_{00}\rangle + \langle\psi_{01}|A_0^0 \otimes B_0^0|\psi_{01}\rangle] \leq \tilde{\varepsilon}. \tag{F6}$$

For basis 1, the X-basis, this is given instead by

$$\langle\Psi_1|(|+\rangle\langle +| \otimes A_1^1 \otimes B_1^1 + |-\rangle\langle -| \otimes A_0^1 \otimes B_0^1)|\Psi_1\rangle \leq \tilde{\varepsilon}, \tag{F7}$$

which can be expanded as

$$\frac{1}{4}\left(\sum_{i,j=0}^{1} \langle\psi_{1i}|A_1^1 \otimes B_1^1|\psi_{1j}\rangle + \sum_{i,j=0}^{1} (-1)^{i+j}\langle\psi_{1i}|A_0^1 \otimes B_0^1|\psi_{1j}\rangle\right) \leq \tilde{\varepsilon}. \tag{F8}$$

By the nature of the states $|\psi_{0j}\rangle$, we have an additional property, where

$$\begin{aligned}\langle\psi_{0j}|\psi_{0j'}\rangle =& (\langle\psi| \otimes \langle j|)(U_{AQ}^\dagger \otimes U_B^\dagger)(U_{AQ} \otimes U_B)(|\psi\rangle \otimes |j'\rangle) \\ =& \langle j|j'\rangle \\ =& \delta_{jj'},\end{aligned} \tag{F9}$$

since $\{|j\rangle\}_j$ form an orthonormal basis of the single qubit system Q. A similar relation is true for $|\psi_{1j}\rangle$. As such, the optimization problem

$$\begin{aligned}
\min \quad & \sqrt{1-|\langle\Psi_0|\Psi_1\rangle|^2} \\
\textit{subj. to} \quad & \langle\psi_{ij}|\psi_{ij'}\rangle = \delta_{jj'},\ i\in\{0,1\} \\
& \frac{1}{2}\sum_{j=0}^{1}\langle\psi_{ij}|A_0^i\otimes B_0^i + A_1^i\otimes B_1^i|\psi_{ij}\rangle \geq \tilde{\eta},\ i\in\{0,1\} \\
& \frac{1}{2}[\,\langle\psi_{00}|A_1^0\otimes B_1^0|\psi_{00}\rangle + \langle\psi_{01}|A_0^0\otimes B_0^0|\psi_{01}\rangle] \leq \tilde{\varepsilon} \\
& \frac{1}{4}\left(\sum_{i,j=0}^{1}\langle\psi_{1i}|A_1^1\otimes B_1^1|\psi_{1j}\rangle + \sum_{i,j=0}^{1}(-1)^{i+j}\langle\psi_{1i}|A_0^1\otimes B_0^1|\psi_{1j}\rangle\right) \leq \tilde{\varepsilon} \\
& \langle\psi_{ij}|A_z^i\otimes B_{z'}^i|\psi_{ij}\rangle = 0,\ \forall z\neq z',\ i,j\in\{0,1\}
\end{aligned} \tag{F10}$$

provides a valid lower bound, noting that relaxing the set of constraints in a minimization problem can only reduce the optimal value.

To arrive at an SDP, changes have to made to the optimization problem. We first note that minimizing $\sqrt{1-x^2}$ with constraints on x is equivalent to computing $\sqrt{1-S^2}$, where S is the maximization of x with the same constraints. To simplify the maximization of $|\langle\Psi_0|\Psi_1\rangle|$, we first note that all the constraints are invariant to a global phase applied on $|\Psi_1\rangle$. Since the global phase can be freely chosen, maximizing $|\langle\Psi_0|\Psi_1\rangle|$ is equivalent to maximizing $\mathrm{Re}[\langle\Psi_0|\Psi_1\rangle]$, since $\mathrm{Re}[\langle\Psi_0|\Psi_1\rangle] \leq |\langle\Psi_0|\Psi_1\rangle|$, and there exist a global phase where $\langle\Psi_0|\Psi_1\rangle \in \mathbb{R}$. Finally, we can relax the maximization problem into an SDP using the NPA hierarchy [26, 27]. The tensor product structure of measurement operators A_j^i and $B_{j'}^{i'}$ can be relaxed to consider commuting operators $[A_j^i, B_{j'}^{i'}] = 0$. We consider the set of states $\{|\psi_{ij}\rangle\}_{ij}$ and the set of operators $\{A_j^i\}_{ij}$ and $\{B_j^i\}_{ij}$, and we can consider successively bigger sets of states $|\xi_i\rangle$ (a hierarchy) formed from product of the operators one of the state. This allows us to construct a Gram matrix Γ as described in the theorem, which is positive semi-definite. Since all other terms in the maximization can be described by entries of the Gram matrix (note commutation relation can be enforced by equating terms in the Gram matrix), the resulting optimization problem

$$\begin{aligned}
\max \quad & \frac{1}{2}\,\mathrm{Re}[\langle\psi_{00}|\psi_{10}\rangle + \langle\psi_{01}|\psi_{11}\rangle] \\
\textit{subj. to} \quad & \Gamma \geq 0 \\
& \langle\psi_{ij}|\psi_{ij'}\rangle = \delta_{jj'},\ i\in\{0,1\} \\
& \frac{1}{2}\sum_{j=0}^{1}\langle\psi_{ij}|A_0^iB_0^i + A_1^iB_1^i|\psi_{ij}\rangle \geq \tilde{\eta},\ i\in\{0,1\} \\
& \frac{1}{2}[\,\langle\psi_{00}|A_1^0B_1^0|\psi_{00}\rangle + \langle\psi_{01}|A_0^0B_0^0|\psi_{01}\rangle] \leq \tilde{\varepsilon} \\
& \frac{1}{4}\left(\sum_{i,j=0}^{1}\langle\psi_{1i}|A_1^1B_1^1|\psi_{1j}\rangle + \sum_{i,j=0}^{1}(-1)^{i+j}\langle\psi_{1i}|A_0^1B_0^1|\psi_{1j}\rangle\right) \leq \tilde{\varepsilon} \\
& \langle\psi_{ij}|A_z^iB_{z'}^i|\psi_{ij}\rangle = 0,\ \forall z\neq z', i,j\in\{0,1\} \\
& [A_j^i, B_{j'}^{i'}] = 0,\ i,i'\in\{0,1\},\ j,j'\in\{0,1,\perp\}
\end{aligned} \tag{F11}$$

is a valid SDP that can be solved using convex optimization methods. Importantly, due to the weak duality property of convex optimization problems, the dual solution of the SDP guarantees a valid lower bound on the trace distance [28].