Continuous Variable Quantum Distance Bounding

Kevin Bogner
COSIC, KU Leuven
Leuven, Belgium
kevin.bogner@esat.kuleuven.be

Aysajan Abidin
COSIC, KU Leuven
Leuven, Belgium
aysajan.abidin@esat.kuleuven.be

Dave Singelée
COSIC, KU Leuven
Leuven, Belgium
dave.singelee@esat.kuleuven.be

***Abstract*—Quantum distance bounding (QDB) protocols verify the physical distance between communicating parties, crucial for secure authentication. Existing QDB protocols use discrete variable (DV) quantum technologies, which require specialized equipment and face scalability challenges. In contrast, continuous variable (CV) techniques in quantum key distribution (QKD) have demonstrated practicality and compatibility with existing telecommunications infrastructure.**

We introduce a CV QDB protocol that uses entangled EPR states and simple operations by the prover based on a shared secret for secure and precise distance measurements. By utilizing CV, our protocol benefits from quadrature measurements, enhancing practicality in real-world implementations.

This work represents the first exploration of CV techniques in QDB protocols, offering a feasible and robust alternative to DV methods. Our CV QDB protocol aligns with advancements in CV QKD, overcoming limitations associated with DV approaches and paving the way for practical implementations of QDB in secure communication systems.

***Index Terms*—quantum distance bounding, quantum communication, continuous variable quantum protocols, wireless security**

I. Introduction

Distance bounding (DB) protocols [1] are specifically designed to prevent relay attacks by verifying the physical distance between two parties via precise round-trip time measurements. While DB protocols are indeed critical in contactless systems like payments and access control, many classical implementations remain vulnerable because attackers can relay, copy, or amplify signals using advanced techniques, thereby undermining the distance claims.

QDB protocols address these vulnerabilities by exploiting quantum properties (for example, the no cloning theorem and measurement disturbance) to counter distance fraud, mafia fraud, and terrorist fraud. Existing QDB work primarily uses DV encodings, such as single-photon polarization qubits [2]–[5], which provide strong security but require specialized single-photon sources and sensitive detectors.

In contrast, CV protocols rely on standard optical components (e.g., coherent states and homodyne detection) and often achieve higher key transmission rates [6]. Motivated by the success of these techniques in QKD, we propose what is, to the best of our knowledge, the first CV-based QDB protocol. Our design employs entangled EPR states, simple quadrature-based encoding, and continuous quadrature correlations to perform secure, precise distance estimation. By leveraging these practical advantages, the protocol offers a robust alternative to DV approaches, while minimizing the prover's technological requirements and accelerating processing.

As explained in [4], the use of entangled particles allows to use physically random challenges that remain unknown even to the verifier until measurement, reducing the attack surface. In contrast, non-entanglement-based QDB protocols generate a pseudorandom challenge classically before encoding it in a quantum state.

In the next section, we present background and related work on DV QDB and outline the evolution from DV QKD to CV QKD. We then introduce our CV QDB protocol and provide an informal security analysis, focusing on reflection, distance, and mafia attacks. This analysis illustrates how CV entanglement can enhance security in QDB without the need for specialized single-photon hardware.

II. Background and Related Work

This section provides an overview of the key developments in DB protocols, tracing their evolution from classical implementations to quantum-based approaches. It begins by reviewing classical DB protocols, which have established the fundamental principles upon which QDB protocols are built. The discussion then shifts to QDB protocols, first examining DV QDB protocols and their reliance on single-photon technologies. Finally, it explores recent advancements in CV QKD, highlighting how these innovations can inspire the evolution of CV-based QDB systems.

A. Classical Distance Bounding

DB protocols, originally introduced in [1], allow a verifier to not only authenticate a remote prover but also estimate an upper limit on their physical distance. Typically, DB protocols feature three core stages: an initialization phase, a rapid-bit exchange phase, and a final authentication phase.

During the initialization phase, the prover commits to a randomly generated nonce. In each round of the rapid-bit exchange, the verifier sends an unpredictable challenge to the prover. The prover then computes a response using a minimal processing operation that combines the challenge with the committed nonce. This simple operation is chosen specifically to minimize processing time, ensuring that the measured elapsed time primarily reflects the propagation delay of the signal rather than any computational delay at the prover's side. The verifier then subtracts an assumed negligible processing

delay at the prover's side to infer the distance based on the speed-of-light constraint.

Security rests on two key assumptions. First, the prover does not learn the challenge in advance, preventing precomputation of responses. Second, the communication signal travels at a known maximum speed. This ensures that an adversary cannot appear closer than they really are without resorting to implausibly small response times.

B. Discrete Variable Quantum Distance Bounding

DV QDB protocols use discrete properties of single photons, such as polarization, to transmit information between communicating parties [2], [3]. The reliance on single-photon equipment is essential for accurate distance estimation, as it ensures that the quantum states used for communication maintain their integrity against potential eavesdropping attempts. Recent advancements in DV QDB [4], [5] have integrated entanglement-based methodologies, where EPR pairs shared between the verifier and the prover enable functionalities such as mutual authentication and device independence.

C. Transition from Discrete to Continuous Variable Quantum Key Distribution

DV QKD protocols, such as BB84 [7] and E91 [8], have demonstrated the feasibility of quantum-secured communications. However, these protocols depend on specialized hardware, which can present scalability and cost challenges. In contrast, CV QKD [6] encodes information in the quadrature amplitudes of light and can be implemented using standard telecom components, potentially reducing costs. Moreover, security analyses indicate that CV QKD resists general attacks [9], suggesting a degree of robustness. The performance of CV QKD thus motivates the investigation of CV-based QDB protocols as a possible means to address the hardware and scalability limitations associated with DV approaches, even though the present work remains primarily theoretical.

Fiber-based CV QKD exhibits well-characterized loss profiles and low noise levels, which facilitate high key rates over long distances. Recent experimental demonstrations have achieved operation over distances of approximately 200 km using ultralow-loss fiber [10], indicating compatibility with existing telecom infrastructure.

Free-space CV QKD, which does not require physical cabling, has been explored for satellite-to-ground links to enable broader coverage. However, free-space implementations must contend with challenges such as atmospheric turbulence, beam alignment, and increased background noise, particularly under daylight conditions [11]. Proof-of-concept demonstrations over short urban links, combined with recent advancements in adaptive optics and reconciliation methods, suggest that longer operational distances may be attainable.

In summary, fiber-based and free-space CV QKD represent complementary approaches for developing a global quantum-secure communication infrastructure. Fiber-based systems are generally more suitable for high key rates over shorter distances (e.g., within city networks), whereas free-space channels may facilitate connectivity between distant nodes or support satellite-based relays. Although the proposed CV QDB protocol is currently theoretical, the successful implementation of CV QKD indicates that similar architectures might be adapted for CV QDB in future research.

III. Continuous Variable Quantum Distance Bounding

The CV QDB protocol (Fig. 1) enables distance estimation through round-trip time measurements, consisting of three phases: initialization, challenge-response, and authentication.

A. Initialization Phase

We assume that the prover and the verifier share a secret key K. In the initialization stage of the protocol, the verifier and the prover exchange nonces n_v and n_p, respectively. Both parties then use a secure pseudorandom function (PRF) to compute the concatenation of two binary strings a and b of equal length:

$$a \,\|\, b = \mathrm{PRF}_K(n_v \,\|\, n_p). \tag{1}$$

These strings are fresh, unpredictable, and known only to the verifier and the prover, assuming both K and the PRF remain secure. They will be used to select quadratures for measuring and encoding information during the subsequent challenge-response phase.

B. Challenge-Response Phase

Because a and b each have n bits, the protocol is repeated n times, once for each element a_i (and the corresponding b_i) in these secret strings. In each round i, the following steps are performed:

1) **Entangled State & Challenge Preparation:** The verifier prepares an EPR state, $|\Psi\rangle_{AB}$, comprising two modes labeled *Mode A* and *Mode B*. The verifier keeps *Mode A* locally and sends *Mode B*, the challenge, to the prover via a quantum channel. The moment the verifier sends *Mode B*, it starts a clock to measure the round-trip time. By using an *entangled* CV state (rather than unentangled), the measurement outcome remains inherently quantum-random and thus unpredictable to an adversary before it is actually measured.
2) **Verifier's First Measurement:** Immediately after sending *Mode B*, the verifier performs homodyne detection on *Mode A* according to a_i:

$$a_i = \begin{cases} 0 & \text{measure } \hat{x}_A, \\ 1 & \text{measure } \hat{p}_A. \end{cases} \tag{2}$$

   The outcome of this measurement is recorded as m_i.
3) **Prover measures Challenge:** Upon receiving *Mode B*, the prover measures in the quadrature selected by a_i, matching the verifier's choice:

$$a_i = \begin{cases} 0 & \text{measure } \hat{x}_B, \\ 1 & \text{measure } \hat{p}_B. \end{cases} \tag{3}$$

   The outcome of this measurement is recorded as m_i'.

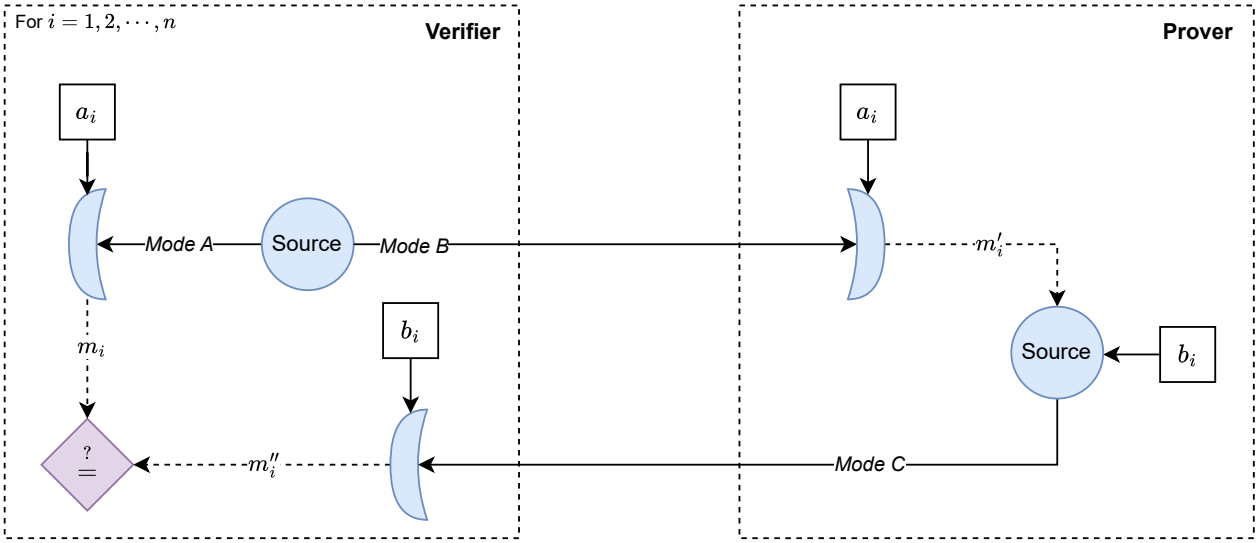

Fig. 1. Schematic illustration of one round of the CV QDB protocol. The verifier begins by preparing an EPR state comprising *Mode A* and *Mode B*. The verifier sends *Mode B* to the prover and starts a clock. Then, the verifier performs homodyne detection on *Mode A*. Specifically, if $a_i = 0$, the verifier measures the x-quadrature; if $a_i = 1$, the verifier measures the p-quadrature. The measurement result is m_i. Upon receiving *Mode B*, the prover measures it in the same quadrature basis used by the verifier (the quadrature basis is determined by a_i: if $a_i = 0$, measure x-quadrature; if $a_i = 1$, measure p-quadrature), obtaining the outcome m_i'. The prover then prepares a new *Mode C* by encoding m_i' into the corresponding quadrature: if $b_i = 0$, the prover substitutes the x-quadrature of *Mode C* with m_i'; if $b_i = 1$, the prover substitutes the p-quadrature with m_i'. Finally, the prover sends *Mode C* back to the verifier. Once the verifier receives *Mode C*, it stops the clock. Depending on the value of b_i, the verifier measures the x-quadrature ($b_i = 0$) or the p-quadrature ($b_i = 1$) of *Mode C*, obtaining outcome m_i''. The verifier checks whether $m_i = m_i''$. If this condition holds and the round-trip time is sufficiently short, the verifier confirms an upper bound on the distance from the verifier to the prover and authenticates the prover's identity.

4) **Prover encodes Response:** The prover then prepares the response, *Mode C*, by encoding the previously measured outcome m_i' according to b_i:

$$b_i = \begin{cases} 0 & \text{substitute into } \hat{x}_C, \\ 1 & \text{substitute into } \hat{p}_C. \end{cases} \tag{4}$$

5) **Returning the Response:** The prover sends *Mode C* back to the verifier. Once the verifier receives *Mode C*, it stops the clock. The measured time will be used to estimate the distance to the prover.
6) **Verifier measures Response:** Upon receiving *Mode C*, the verifier measures the quadrature indicated by b_i:

$$b_i = \begin{cases} 0 & \text{measure } \hat{x}_C, \\ 1 & \text{measure } \hat{p}_C. \end{cases} \tag{5}$$

The outcome of this measurement is recorded as m_i''.

This concludes the challenge-response phase of the protocol.

C. Authentication Phase

At the end of all n rounds, the verifier holds pairs of measurement outcomes $\{m_i\}$ (from *Mode A*) and $\{m_i''\}$ (from *Mode C*). For an ideal EPR state and honest operations, measuring $\hat{x}_A$ and $\hat{x}_B$ when $a_i = 0$ implies

$$\left\langle \left(\hat{x}_A - \hat{x}_B\right)^2 \right\rangle \approx 0, \tag{6}$$

while measuring $\hat{p}_A$ and $\hat{p}_B$ when $a_i = 1$ implies

$$\left\langle \left(\hat{p}_A - \hat{p}_B\right)^2 \right\rangle \approx 0. \tag{7}$$

Thus, in an honest scenario, we expect $m_i \approx m_i'$. Moreover, because b_i determines which quadrature is measured in *Mode C*, the verifier expects

$$m_i \stackrel{?}{=} m_i'' \tag{8}$$

for all rounds i. If $m_i = m_i''$ (within acceptable tolerances) and the round-trip time is sufficiently short, the verifier accepts that round as successful.

By confirming that these correlations hold for every round and that the timing constraints are satisfied, the verifier concludes it is indeed communicating with the legitimate prover. Although each match indirectly indicates that the prover measured and encoded according to the verifier's secret bits a_i and b_i, the primary concern of the verifier is the authenticity and proximity of the prover. Hence, from the combination of correlated outcomes and short round-trip times, the verifier is assured of the prover's identity and its bound on distance.

IV. Security Analysis

In this section, we present a security analysis of our QDB protocol, focusing on three classical attack strategies widely discussed in the literature [2]–[5]: (1) reflection attacks, (2) distance fraud attacks, and (3) mafia fraud attacks. Under the assumption that the secret bits a_i and b_i remain secure, we demonstrate that any adversary lacking knowledge of these

bits must rely on guessing, resulting in success probabilities that decrease exponentially with the number of rounds n.

A. Assumptions and Practical Considerations

Before detailing the attack strategies, we briefly list our main assumptions and acknowledge the practical limits of idealized EPR correlations:

- **Honest Verifier Model.** We assume that the verifier faithfully follows the protocol, generating fresh entangled modes and performing the correct quadrature measurements. Any deviation by the verifier could invalidate the distance-bounding guarantees.
- **Ideal EPR States vs. Real-World States.** Throughout the security analysis, we treat $|\Psi\rangle_{AB}$ as an ideal EPR (maximally entangled) state. In practical implementations, finite squeezing, losses, and detector inefficiencies increase the measured quadrature variance above zero. Nonetheless, one may define a small variance threshold $\sigma_{\max}$ such that an honest implementation with sufficiently strong squeezing keeps the measured quadrature differences below $\sigma_{\max}$ with high probability, whereas any unentangled or adversarially modified mode would yield variances exceeding this threshold. In essence, measuring how closely m_i and m_i'' track each other provides a strong indication of genuine EPR-like correlations.
- **Timing Constraints.** We assume there is a strict time window enforced by the protocol to ensure that any attempt to delay or prematurely send a response (as in distance or mafia fraud) is detected. This timing window is set based on the known maximum propagation speed of signals and the distance bound we wish to guarantee. Due to the stringent turnaround times, any intercept-and-measure strategy would exceed the protocol's time limit and thus be immediately flagged by the verifier.
- **Processing Delays at the Prover.** A key practical consideration is the processing time required by the prover to generate *Mode C*. Even with a strictly enforced timing window, this inherent delay increases the overall round-trip time. If the processing delay constitutes a significant fraction of the signal propagation delay, it introduces additional uncertainty in the timing measurement and effectively establishes a lower bound on the resolvable distance, especially in short-range applications. Consequently, optimizing the prover's hardware and processing to minimize latency is essential. Future work should target these improvements to ensure that processing delays do not compromise protocol performance.

Under these assumptions, we now analyze three major classes of attacks, namely reflection, distance fraud, and mafia fraud, and show why they fail with exponentially small probability in the number of rounds.

B. Reflection Attack

A reflection attack attempts to break the protocol by simply returning the received mode (i.e., *Mode B*) to the verifier without performing any of the secret-dependent measurements or encodings. In our CV QDB protocol, each round i depends on two secret bits:

- a_i, which determines the quadrature measured by both the verifier (in *Mode A*) and the prover (in *Mode B*).
- b_i, which determines how the prover re-encodes the measured outcome (into $\hat{x}$ or $\hat{p}$) and which quadrature the verifier measures upon receiving the returned mode (*Mode C*).

To analyze the attacker's probability of success under a reflection-only strategy, we consider two cases:

a) Case 1: $a_i = b_i$.: When $a_i = b_i$, the honest prover would measure the same quadrature the verifier used (specified by a_i) and then re-encode the measured outcome $\hat{x}$ or $\hat{p}$ into the same quadrature (specified by b_i). Consequently, the final measurement by the verifier on *Mode C* also targets the same quadrature measured in *Mode A*, yielding $m_i = m_i''$. If an adversary instead returns *Mode B* unaltered, the original EPR correlations remain fully intact in this same quadrature, ensuring that the attacker always reproduces the correct correlation in these rounds.

b) Case 2: $a_i \neq b_i$.: When $a_i \neq b_i$, the honest prover measures one quadrature (determined by a_i) but encodes the result into the orthogonal quadrature (determined by b_i). This cross-quadrature encoding enforces, for example, $\hat{x}_A \approx \hat{p}_C$ or $\hat{p}_A \approx \hat{x}_C$. An adversary who simply returns the unmodified *Mode B* fails to establish these cross-quadrature correlations because *Mode B* is still aligned with a_i, not b_i. Consequently, the verifier's final measurement (in the b_i-quadrature) will not match the verifier's first measurement (in the a_i-quadrature), causing an immediate protocol failure in all rounds where $a_i \neq b_i$.

c) Overall Success Probability.: Because a_i and b_i are each independently chosen from $\{0, 1\}$ in each round, $\Pr(a_i = b_i) = 1/2$ and $\Pr(a_i \neq b_i) = 1/2$. In the best case for the attacker, they might pass all rounds for which $a_i = b_i$. However, they inevitably fail every round where $a_i \neq b_i$. Thus, the probability of passing all n rounds under a pure reflection strategy is bounded by $(1/2)^n$. This exponential decay in success probability holds unless the attacker can correctly guess or otherwise learn the secret bits a_i and b_i in real time, which our protocol design precludes.

C. Distance Fraud Attack

In a distance fraud attack, a dishonest prover, who indeed knows the bits $\{a_i, b_i\}$ by the sharing of the secret key, attempts to appear closer to the verifier than they really are by sending a stand-in mode (*Mode D*) before legitimately receiving and measuring the entangled *Mode B*. Although the dishonest prover knows which quadratures will be measured (a_i) and how the outcomes should be encoded (b_i), they do not know the random outcome m_i that the verifier obtains by measuring the entangled *Mode A*. This outcome arises from intrinsic quantum fluctuations in the EPR state and thus cannot be guessed reliably. Without actually using the genuine *Mode B*, the dishonest prover's stand-in mode (*Mode D*) lacks the requisite EPR correlations with *Mode A*, causing a

systematic mismatch in the verifier's final check $m_i \stackrel{?}{=} m_i''$. Consequently, under our timing and secrecy assumptions, any attempt at distance fraud cannot succeed in *any* round, ensuring that the dishonest prover is invariably exposed and the distance guarantee remains intact.

D. Mafia Fraud Attack

A mafia fraud attack involves an external adversary attempting to convince the verifier that it is communicating directly with a genuine but potentially distant prover. We distinguish two principal strategies:

1) *Pre-Ask Strategy:* The adversary tries to obtain the prover's responses (or partial information about them) in advance of the verifier's actual challenges and then replays these early-obtained responses at the correct time. In some cases, this may not entail a pure verbatim replay of recorded signals; rather, partial data or side information might be used to craft or approximate a valid response. In the quantum setting, this process is further constrained by the no-cloning theorem and the disturbance caused by measurement.
2) *Intercept-and-Respond Strategy:* The adversary intercepts the verifier's challenge mode (*Mode B*) and attempts to craft a fraudulent response locally, without passing the entangled mode onward to the legitimate prover.

Below, we explain why both variants of mafia fraud fail with overwhelmingly high probability under our CV QDB protocol.

1) Pre-Ask Strategy: A defining feature of our protocol is that each challenge round uses fresh entanglement between the verifier's locally measured mode (*Mode A*) and the traveling mode (*Mode B*). The prover must genuinely use *Mode B* while it remains entangled with *Mode A*; otherwise, the strong EPR-like correlations needed for the protocol's final acceptance test will be lost.

If the adversary attempts to pre-ask or store responses from the honest prover before the verifier's challenge, any stored modes will necessarily lack the entanglement with *Mode A*. From the verifier's perspective, they become separable states that cannot reproduce the near-ideal correlations $\hat{x}_A \approx \hat{x}_B$ or $\hat{p}_A \approx \hat{p}_B$. As soon as the verifier checks $m_i \stackrel{?}{=} m_i''$ at the end, any stored or pre-generated modes are revealed to lack genuine entanglement with *Mode A*. Since those modes cannot reproduce the correct EPR-like correlations, the adversary's pre-ask attack will inevitably fail in every round, making it impossible to deceive the verifier about the prover's identity or distance.

2) Intercept-and-Respond Strategy: Consider an adversary $\mathcal{A}$ who intercepts *Mode B* in transit and does not forward it to the legitimate prover. In each round i, the verifier's secret bits (a_i, b_i) are derived from the strings produced by the PRF, as described in the initialization phase. The adversary then attempts to guess $(a_i^{\mathcal{A}}, b_i^{\mathcal{A}})$. First, it measures *Mode B* along the quadrature $a_i^{\mathcal{A}}$. Next, it encodes the measured outcome into a fresh *Mode C* along quadrature $b_i^{\mathcal{A}}$. Finally, this newly prepared *Mode C* is sent back to the verifier.

Because $\{a_i, b_i\}$ are unknown to the adversary, any mismatch in guessing $(a_i^{\mathcal{A}}, b_i^{\mathcal{A}}) \neq (a_i, b_i)$ will cause the final measurement outcome in *Mode C* to differ from the verifier's outcome in *Mode A*. Specifically, if $a_i^{\mathcal{A}} \neq a_i$, the adversary measures the orthogonal quadrature of *Mode B* and obtains no useful information about the verifier's measurement outcome m_i. Similarly, if $b_i^{\mathcal{A}} \neq b_i$, the adversary re-encodes into the wrong quadrature of *Mode C*, which ensures a mismatch between the adversary's outcome and the verifier's. Only when $(a_i^{\mathcal{A}} = a_i,\, b_i^{\mathcal{A}} = b_i)$ can the adversary's measurements and encodings align with the verifier's.

Since each bit in $\{a_i, b_i\}$ is equally likely to be 0 or 1, the probability of choosing the correct pair in any round is $1/4$. Over n rounds, the probability that the adversary succeeds in guessing *all* pairs $\{a_i, b_i\}$ correctly is $(1/4)^n$, which decreases exponentially in n. Consequently, an intercept-and-respond strategy without knowledge of the secret bits fails with overwhelming probability for large n.

V. Simulation

This section describes the simulation of our proposed CV QDB protocol. This simulation serves as a proof-of-concept to confirm that our conceptual model of the protocol's behavior is sound, rather than to provide a full end-to-end emulation. Our simulation omits both timing components and the actual exchange of challenges and responses; instead, all operations are assumed to be performed locally. Consequently, while the simulation demonstrates the theoretical feasibility of the CV QDB under idealized conditions, it does not constitute experimental proof that the protocol would behave identically in a physical implementation. Algorithm 1 presents the pseudocode for the protocol simulation.

In addition to simulating the standard protocol, one can also simulate the attacks discussed in Section IV. For example, Algorithm 2 demonstrates how a reflection attack can be simulated by simply omitting the response phase of the protocol.

All coding simulations of the protocol and the presented attacks are available in our GitHub repository [12].

VI. Conclusion

This work introduced a CV QDB protocol based on EPR states and homodyne-based quadrature measurements. By using entangled modes and simple quadrature-based encoding at the prover's end, the protocol provides both entity authentication and distance verification. Crucially, its security relies on two key aspects: leveraging nonclassical EPR correlations, which cannot be replicated by classical or independently prepared quantum systems, and enforcing strict timing constraints so that attacks fail under round-trip time checks. Consequently, standard attacks such as reflection, distance fraud, and mafia fraud cannot produce the required correlations without knowledge of the secret bits, causing their overall success probability to decay exponentially with the number of rounds.

Future investigations may explore a wider range of adversarial strategies, address realistic device imperfections (such as noise, state preparation errors, and detection inefficiencies),

Algorithm 1: CV QDB

Data: n (number of runs)
Result: Correlation between $|m|$ and $|m''|$

Generate two random binary arrays a and b of length n;
for $i \leftarrow 1$ **to** n **do**
  // Challenge Phase (Modes A and B)
  Prepare an EPR state $|\Psi\rangle_{AB}$;
  if $a[i] = 0$ **then**
    Measure Mode A in the $\hat{x}_A$ quadrature;
    Measure Mode B in the $\hat{x}_B$ quadrature;
  else
    Measure Mode A in the $\hat{p}_A$ quadrature;
    Measure Mode B in the $\hat{p}_B$ quadrature;
  Record the measurement outcomes $m[i]$ and $m'[i]$;
  // Response Phase (Mode C)
  Prepare a single-mode Gaussian state;
  if $b[i] = 0$ **then**
    Displace Mode C using $m'[i]$ (angle 0);
    Measure Mode C in the $\hat{x}_C$ quadrature;
  else
    Displace Mode C using $m'[i]$ (angle $\pi/2$);
    Measure Mode C in the $\hat{p}_C$ quadrature;
  Record the measurement outcome $m''[i]$;
Compute the correlation between $|m|$ and $|m''|$ over all runs;
Output: the computed correlation.

Algorithm 2: CV QDB – Reflection Attack

Data: n (number of runs)
Result: Correlation between $|m|$ and $|m''|$

Generate two random binary arrays a and b of length n;
for $i \leftarrow 1$ **to** n **do**
  // Challenge Phase (Modes A and B)
  Prepare an EPR state $|\Psi\rangle_{AB}$;
  if $a[i] = 0$ **then**
    Measure Mode A in the $\hat{x}_A$ quadrature;
  else
    Measure Mode A in the $\hat{p}_A$ quadrature;
  if $b[i] = 0$ **then**
    Measure Mode B in the $\hat{x}_B$ quadrature;
  else
    Measure Mode B in the $\hat{p}_B$ quadrature;
  Record the measurement outcomes $m[i]$ (Mode A) and $m''[i]$ (Mode B);
Compute the correlation between $|m|$ and $|m''|$ over all runs;
Output: the computed correlation.

and assess the protocol's feasibility under practical conditions. Overall, this protocol offers a framework for CV QDB that warrants further theoretical and experimental study.

ACKNOWLEDGMENT

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203, and by the European Commission through the Horizon Europe research and innovation programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043).

REFERENCES

[1] S. Brands and D. Chaum, "Distance-bounding protocols," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1993, pp. 344–359.
[2] A. Abidin, E. Marin, D. Singelée, and B. Preneel, "Towards quantum distance bounding protocols," in *Radio Frequency Identification and IoT Security: 12th International Workshop, RFIDSec 2016, Hong Kong, China, November 30–December 2, 2016, Revised Selected Papers 12*. Springer, 2017, pp. 151–162.
[3] A. Abidin, "Quantum distance bounding," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 233–238.
[4] A. Abidin, K. Eldefrawy, and D. Singelée, "Entanglement-based mutual quantum distance bounding," in *Cyber Security, Cryptology, and Machine Learning: 8th International Symposium, CSCML 2024, Be'er Sheva, Israel, December 19–20, 2024, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 2024, p. 219–235.
[5] K. Bogner, D. Singelée, and A. Abidin, "Entangled states and bell's inequality: A new approach to quantum distance bounding," in *2024 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2024, pp. 1–6.
[6] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical review letters*, vol. 88, no. 5, p. 057902, 2002.
[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical computer science*, vol. 560, pp. 7–11, 1984.
[8] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.
[9] A. Leverrier, "Security of continuous-variable quantum key distribution via a gaussian de finetti reduction," *Physical review letters*, vol. 118, no. 20, p. 200501, 2017.
[10] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Physical review letters*, vol. 125, no. 1, p. 010502, 2020.
[11] M. Ghalaii and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution in free-space channels," *Physical Review A*, vol. 108, no. 4, p. 042621, 2023.
[12] K. Bogner, "Quantum distance bounding code repository," https://github.com/kevinbogner/quantum_distance_bounding/tree/main/cv, 2025, accessed: 2025-02-16.