Quantum contract signing with entangled pairs

P. Yadav\textsuperscript{1,2}, P. Mateus\textsuperscript{1,2}, N. Paunković\textsuperscript{1,2}, A. Souto\textsuperscript{2,3}

\textsuperscript{1}Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa, Av. Rovisco Pais, 1049-001 Lisboa, Portugal
\textsuperscript{2}SQIG – Instituto de Telecomunicações, 1049-001 Lisboa, Portugal and
\textsuperscript{3}LaSIGE, Departamento de Informática, Faculdade de Ciências, Universidade de Lisboa, 1749-016 Lisboa, Portugal

We present a quantum scheme for signing contracts between two clients (Alice and Bob) using entangled states and the services of a third trusted party (Trent). The trusted party is only contacted for the initialization of the protocol, and possibly at the end, to verify clients’ honesty and deliver signed certificates. The protocol is fair, i.e., the probability that a client, say Bob, can obtain a signed copy of the contract, while Alice cannot, can be made arbitrarily small, and scales as $N^{-1/2}$, where $4N$ is the total number of rounds (communications between the two clients) of the protocol. Thus, the protocol is optimistic, as the cheating is not successful, and the clients rarely have to contact Trent to confirm their honesty by delivering the actual signed certificates of the contract. Unlike the previous protocol \cite{17}, in the present proposal only one client can obtain the signed contract, without the need for the other client’s presence. When first contacting Trent, the clients do not have to agree upon a definitive contract. Moreover, even upon terminating the protocol, the clients do not reveal the actual contract to Trent. Being based on the laws of physics, rather than on mathematical conjectures and the exchange of huge number of signed authenticated messages during the actual contract signing process, the protocol is abuse-free, as Alice and Bob cannot prove they are involved in the contract signing process. Finally, we present a version of the protocol that does not rely on stable quantum memories, making it possible to be realized with the current technology used in the standard quantum key distribution implementations.

I. INTRODUCTION

Contract signing \cite{9} is a security protocol that falls within a group of the so-called commitment protocols \cite{11,15,16}. In general, the protocol can be defined for arbitrary number of parties (clients engaged in the protocol). For simplicity, we discuss the case of a two-party protocol, which can be straightforwardly generalized to an arbitrary number of participants.

The participants, usually referred to as Alice and Bob, have a common contract to which they decide to commit upon, or not. The commitments are usually done by simple signatures: having a text of the contract with Bob’s signature stamped on it, Alice can appeal to the authorities (the Judge), that in turn declares the document valid (i.e., bind the contract). In other words, having Bob’s signature gives Alice the power to enforce the terms of the contract. Consequently, signing his name on a copy of the contract means that Bob commits to the contract. The aim of a contract signing protocol is that either both clients obtain each other’s commitments, or none of them does (the protocol is said to be fair).

If only Alice has a copy with Bob’s signature (i.e., only Bob is committed) she can later in time choose to either enforce or not, the terms of the contract. Bob, however, has no power whatsoever – his future behavior is determined solely by Alice’s decisions. For example, Alice may have a document with Bob’s signature on it, declaring that he would buy a car from her, for a fixed amount of money. Knowing that only she has such a document, Alice can continue to negotiate the price of her car with other potential costumers: in case she obtains a better offer, she is free to discard Bob’s offer and thus able to earn more money. Bob does not have such an option: if Alice does not obtain a better offer, she can always force Bob to buy the car from her, by showing to the authorities the contract signed by Bob. Having no proven commitment (signature) from Alice, Bob cannot enforce the contract himself and is thus unable to prevent Alice from such behavior, which puts him in an unfair situation.

Achieving fairness is trivial in cases when clients meet up and simultaneously sign copies of the contract, thus both obtaining each other’s commitments. Unfortunately, doing so when the clients are far apart, e.g., over the internet, is difficult: indeed, sending his signed copy to Alice gives Bob no guarantee that he will obtain one from Alice; on the other hand, obtaining a signature from Alice before actually sending his, gives Bob an advantage of having Alice’s commitment without committing himself.

It has been shown \cite{9,11} that the fairness of a contract signing protocol with spatially distant clients can be achieved only by introducing a trusted third party, usually referred to as Trent, during the phase of exchanging clients’ commitments. Trent’s role is to receive clients’ commitments and perform the exchange only upon obtaining signed copies of the contract from both clients. However simple and straightforward this solution may seem, it has a drawback, as Trent (in practice, a trusted agency accredited by the State that offers its time and resources for
exchange of money, e.g., public notaries) may be expensive. Therefore, the need for protocols using third parties as little as possible arises. Some contract signing protocols \cite{7, 8, 13} do not require a trusted third party, but use a number of transmissions to send the pieces of signatures, or the partial information required to obtain the complete signature, in each message. Another possible way out is to design optimistic and/or probabilistic protocols.

In optimistic contract signing protocols \cite{2}, the exchange of commitments is, unless something goes wrong, executed solely by Alice and Bob. Only in case communication between the clients is interrupted (malfunction of the network, etc.), a trusted third party is involved \cite{3}. In probabilistic protocols \cite{5, 15}, by exchanging messages between each other, clients increase their probabilities to bind the contract. In order to be (probabilistically) fair, such protocols have to ensure that at each stage of the information exchange, the probabilities to bind the contract of both clients can be made arbitrarily close to each other (no client is significantly privileged). One such protocol is \cite{15}, for which the symmetry between the clients’ positions is strengthened by the requirement that the joint probability that one client can bind the contract, while the other cannot, can be made smaller than any given \( \varepsilon < 1 \). Finally, there is both probabilistically fair and optimistic solution, with an optimal number of exchanged messages \cite{4} for which even stronger fairness condition is satisfied: the conditional probability that a client cannot bind the contract, when the other has already done so, can be made arbitrary low.

Recently, a probabilistically fair and optimistic quantum protocol was presented in \cite{17} (see a version using the simultaneous dense coding scheme in \cite{19}). There, the trusted third party, Trent, is required to initiate the protocol and is contacted later only in case something goes wrong. The protocol in \cite{17} is also abuse-free \cite{12}, i.e., the clients cannot provide proofs of being involved in a contract signing procedure. Nevertheless, it has three important disadvantages: (i) Alice and Bob have to share the content of the contract with Trent, (ii) both clients have to be present in order to bind the contract, in case something goes wrong and Trent’s services are required, and (iii) they have to agree upon the content of the contract before the protocol initialization. Moreover, it relies on long-term stable quantum memories, making it infeasible with current technology. In this paper we propose an improved version of the contract signing protocol where (i) the clients never disclose the content of the contract to Trent, (ii) only one client is needed to bind the contract, and (iii) the clients can decide upon the contract after they initially contact Trent. Further, we propose an experimental realization of a version of the protocol that does not require quantum memories.

Regarding point (iii) from the previous paragraph, note that often, when parties initiate business contact, this does not result in making a deal formalized by a contract. Thus, involving Trent, who charges his services, might often result in the waste of clients’ resources, and point (iii) does not really present an advantage. Nevertheless, waiting for the last moment, and contacting Trent only upon successful agreement and contract formulation, might result in the system failure due to possible communication bottlenecks. Imagine the following situation. Alice and Bob negotiate in buying/selling a certain product, knowing that on a given date in the future a big company system failure due to possible communication bottlenecks. Upon the final contract. The problem is, many other users may decide to make similar business contracts at the same period of time, and if they all will have to only then contact Trent, this might cause communication bottleneck upon the final contract. The problem is, many other users may decide to make similar business contracts at the same period of time, and if they all will have to only then contact Trent, this might cause communication bottleneck. In this paper we propose an improved version of the protocol where (i) the clients never disclose the content of the contract to Trent, (ii) only one client is needed to bind the contract, and (iii) they have to agree upon the content of the contract before the protocol initialization.

II. THE PROTOCOL

Consider two orthonormal states \(|0\rangle\) and \(|1\rangle\) of the computational basis \(\mathcal{B}_+\). The diagonal basis \(\mathcal{B}_x = \{\langle-|, |+\rangle\} \) is given by \(|\pm\rangle = \frac{1}{\sqrt{2}}(|1\rangle \pm |0\rangle)\). We also define the measurement observables, \(\hat{O}_+\) and \(\hat{O}_x\), as

\[
\begin{align*}
\hat{O}_+ &= 1 \cdot |1\rangle\langle 1| + 0 \cdot |0\rangle\langle 0|, \\
\hat{O}_x &= 1 \cdot |+\rangle\langle +| + 0 \cdot |-\rangle\langle -|. 
\end{align*}
\]

Let the bit-string \(M\) be the contract that Alice and Bob agree upon. Let \(h\) be a known hash function that they also agree to use. The value \(h^* = h(M)\) will be the only information they provide to Trent, when and if they contact him. Consider the Honest observables, \(\hat{H}_i\), that both honest clients, Alice and Bob, should measure at each step \(i\) of the protocol \((i = 1, \ldots, |h(M)|)\), defined as

\[
\hat{H}_i = \begin{cases} 
\hat{O}_+ & \text{if } h_i(M) = 0, \\
\hat{O}_x & \text{if } h_i(M) = 1,
\end{cases}
\]
The protocol is described below in three parts: (i) Initialization phase – in this stage of the protocol, the trusted party, Trent, prepares and distributes the states among the clients, Alice and Bob, to be used to sign the contract; (ii) Exchange phase – in this stage of the protocol, the clients, using the states and the information provided by Trent, ping-pong the information needed to sign the contract; and (iii) Binding phase – in this stage of the protocol, any one of the parties can contact Trent with his/her results in order to obtain an authorized document declaring the hash value $h^* = h(M)$ valid, which then validates the contract $M$.

**Initialization phase:**

**Parties involved:** Alice, Bob and Trent.

**Input:** $8N$ number of entangled pairs.

The Initialization phase (see Fig. 1), consists of the following steps:

1) Trent produces two ordered sets, each consisting of $4N$ entangled pairs ($8N$ pairs in total). Each pair of particles is in the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$. He gives one particle from each pair of the first set to Alice, and from the second set to Bob, keeping the order of the pairs preserved. Let us denote the ordered set of $4N$ particles given to Alice by $A$, and those given to Bob by $B$. The two ordered sets kept by Trent, each consisting of $4N$ particles entangled with the respective particles (2N pairs in total), are denoted by $T^{(A)}$ and $T^{(B)}$, respectively.

2) Trent randomly divides $T^{(A)}$ into two ordered subsets of $2N$ particles each: $T^{(A)}_T$ and $T^{(A)}_B$, such that the original positions in $T^{(A)}$ of each particle from $T^{(A)}_T$ and $T^{(A)}_B$ are preserved. In other words, for each particle from $T^{(A)}_T$ and $T^{(A)}_B$, Trent knows its position in $T^{(A)}$, and hence, to which particle in $A$ it is entangled with. The same is done with particles from $T^{(B)}$ entangled with those in $B$, obtaining $T^{(B)}_T$ and $T^{(B)}_A$ (and keeping the information about the original ordering in $T^{(B)}$).

3) Trent sends the ordered subsets $T^{(A)}_B$ and $T^{(B)}_A$, of $2N$ particles each, to Bob and Alice, respectively. The particles in $T^{(A)}_B$ and $T^{(B)}_A$ are entangled to the corresponding particles (2N of them) in the sets $A$ and $B$, given to Alice and Bob, respectively. He also sends to Alice the positions $i_A \in \{1, \ldots, 4N\}$ of $2N$ particles.

where $h_i(M)$ is the $i$-th bit of the string $h(M)$.

$\phi^+ = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$

**FIG. 1:** Initialization phase: The thick arrows represent the transfer of particles from Trent to Alice and Bob. The dashed connections represent the entanglement between the respective particles. The big boxes represent shielded private laboratories of Alice, Bob and Trent.
from B entangled with the \( j \)-th particle in \( T^{(B)}_A \), given by the function \( f_B \), such that \( i_B = f_B(j) \) (note that \( j = 1, \ldots, 2N \)); and analogously to Bob, the indices \( i_A = f_A(j) \) from \( A \) about \( T^{(A)}_B \). He keeps the subsets \( T^{(A)}_T \) and \( T^{(B)}_T \) to himself, to be used during the Binding phase.

**The Initialization phase ends with the following:**

- Alice has an ordered set \( A \) of \( 4N \) particles, entangled with 2\( N \) particles kept by Trent, \( T^{(A)}_T \), and additional 2\( N \) particles that are given to Bob, \( T^{(A)}_B \). She has another ordered set \( T^{(B)}_A \) of 2\( N \) particles, entangled with 2\( N \) particles given to Bob, chosen at random from \( B \) with their corresponding 2\( N \) indices \( i_B \in \{1, \ldots, 4N\} \).
- Bob has an ordered set \( B \) of \( 4N \) particles, entangled with 2\( N \) particles kept by Trent, \( T^{(B)}_T \), and additional 2\( N \) particles that are given to Alice, \( T^{(B)}_A \). He has another ordered set \( T^{(A)}_B \) of 2\( N \) particles, entangled with 2\( N \) particles given to Alice, chosen at random from \( A \) with their corresponding 2\( N \) indices \( i_A \in \{1, \ldots, 4N\} \).
- Trent keeps two ordered sets of 2\( N \) particles each, \( T^{(A)}_T \) and \( T^{(B)}_T \), entangled with 2\( N \) particles from \( A \) and \( B \), respectively.

**Exchange phase:**

**Parties involved:** Alice and Bob.

**Input:**

- The particles and indices Alice and Bob obtained at the end of the Initialization phase.
- \( h^* = h(M) \), the hash value of the contract \( M \) to be signed, obtained using publicly known function \( h \).

The Exchange phase (see Fig. 2) consists of 4\( N \) rounds. In 2\( N \) (randomly distributed) of them, a client, say Alice, performs a single measurement per round, on a particle (from \( A \)) that is entangled with a particle kept with Trent.
or with Bob (unknown by Alice). In the other 2N rounds, she performs two measurements, one again on a particle (from A) entangled with a particle kept with Trent or Bob, and on another one (from \( T^B_A \)), that Alice knows is entangled with a particle with Bob, and whose outcome she uses to compare it with the result received from Bob, and thus check his behavior. These two kinds of measurements are shown in Fig. 3.

4) At the beginning of the Exchange phase, Alice and Bob are in possession of 6N particles each. Alice has 4N particles denoted by A and 2N particles by \( T^B_A \), and analogously for Bob. On the 4N particles from A Alice measures the Honest observable \( \hat{H}_i \), with \( i = 1, \ldots, 4N \) (note that, in order to exchange the commitments to the whole string \( h(M) \), we have \( 4N = |h(M)| \)). The same observables are measured by Bob on his corresponding particles from B. Their measurement outcomes form ordered sets of binary results \( R^{(A)} \) and \( R^{(B)} \), respectively, where

\[
R^{(A)} = R^{(A)}_T \cup R^{(A)}_B, \\
R^{(B)} = R^{(B)}_T \cup R^{(B)}_A.
\]  

We use \( R^{(A)}_T \) to denote Alice’s measurement results on the particles from A (2N of them) that are entangled with \( T^A_T \) (kept by Trent), and \( R^{(A)}_B \) to denote her measurement results on the rest of the particles from A (2N of them) entangled with \( T^A_B \) (given to Bob); and analogously for Bob’s results, \( R^{(B)}_T \) and \( R^{(B)}_A \). They send these results to each other, one by one: if Alice starts first, in the \( i \)-th step of the exchange she sends to Bob her result \( R^{(A)}_i \), then Bob sends to Alice his result \( R^{(B)}_i \), and so on.

5) For each result \( R^{(A)}_i \in R^{(A)}_B \) (known to Bob) received from Alice, (when \( i = i_A = f_A(j) \) for some \( j \in \{1, \ldots, 2N\} \), i.e., \( i \) is an index corresponding to an index \( j \) from \( T^B_A \)), Bob measures the \( j \)-th particle from \( T^B_A \) in the basis given by \( h_i(M) \) to obtain \( R^{(A)}_{C_j} \). If Alice indeed measured the Honest observable (in the \( h_i(M) \) basis), then \( R^{(A)}_i = R^{(A)}_{C_j} \). In the presence of noise, Bob applies a statistical test to verify if Alice provided enough consistent results (see Appendix A.2). For a result \( R^{(A)}_i \in R^{(A)}_T \), Bob uses this information for the optional Binding phase, when Trent confronts Bob’s information about \( R^{(A)}_i \) with his own measurement outcomes. The same is done by Alice upon receiving \( R^{(B)}_i \) from Bob. Then, (i) if all measurement outcomes, \( R^{(A/B)}_{C_j} \) (2N of them for each client) are found to be consistent by the end of the communication at step 4N, both clients will, during the Binding phase, obtain with certainty the certified document from Trent that allows them to acquire a signed contract from the authorities (see below the description of the Binding phase), (ii) if one of the clients suspects dishonest behavior, the communication is stopped, they measure the Honest observables on all remaining qubits and proceed to the Binding phase.

The Exchange phase ends with the following: If no cheating occurred, Alice and Bob both obtain their own as well as each other’s results, \( R^{(A)} \) and \( R^{(B)} \). In case the communication interrupted at step \( m \), a client, say, Alice, ends up with all of her own results \( R^{(A)} \) and those received from Bob by the step \( m \) (note that those do not necessarily need to be obtained by actually performing measurements on qubits).
FIG. 4: Binding phase: the thick arrows represent the transfer of measurement outcomes from Alice to Trent. The steps for the binding phase are described.

**Binding phase:**

**Parties involved:** Trent and one of the parties, say, Alice.

**Input:**

- The sets $T_{T}^{(A)}$ and $T_{T}^{(B)}$.
- The sets of Alice’s measurement results, $R^{(A)}$, and those sent to Alice by Bob, $R^{(B)}$. Note that in the case of Bob’s cheating, $R^{(B)}$ might contain wrong values and, in case the communication interrupted at step $m$, it is only a partial set of results. For simplicity, we use the same symbol $R^{(B)}$ for both sets of “honest”, as well as “dishonest”, results.
- $h^* = h(M)$, the hash value of the contract $M$ to be signed, obtained using publicly known function $h$.
- A public distribution $p(\alpha)$ to choose the acceptance rate $\alpha$.

The Binding phase (see Fig. 4), consists of the following steps:

1. Alice sends $R^{(A)}$, $R^{(B)}$, and $\bar{h} = h(M)$ to Trent.
2. Trent receives $R^{(A)}$, $R^{(B)}$, and $\bar{h}$ from Alice.
3. Trent measures all $N$ particles from $T_{T}^{(A)}$ and all $N$ particles from $T_{T}^{(B)}$ and compares them with the corresponding $N$ results from $R^{(A)}$ and $R^{(B)}$ each, respectively.
4. If at least $\alpha N$ of Alice’s results from $R^{(A)}$ and $R^{(B)}$ are consistent with the corresponding results from $T_{T}^{(A)}$ and $T_{T}^{(B)}$, then Trent provides Alice with a certified document declaring the hash value $h^*$ valid, otherwise does nothing.
5. Alice receives a certified document from Trent declaring the hash value $h^*$ valid, allowing her to obtain the certified copy of the contract $M$, for which $h^* = h(M)$.

6) During the Binding phase, a single client, say Alice, presents her results to Trent, in order to bind the contract: she receives a certified document, signed by Trent’s public key, declaring valid the hash value $h^* = h(M)$. Having such a certificate, Alice can appeal to the authorities to enforce the terms of the contract $M$: she presents the contract $M$ and the signed document declaring the value $h^*$ valid, so that the authorities can verify that indeed $h^* = h(M)$ (note that the function $h$ is publicly known). As pointed out in the Introduction, Trent is an agency accredited by the State (e.g., public notaries). To bind the contract, Alice provides the string $h^* = h(M)$ to Trent and presents her results $R^{(A)}$, as well as those obtained from Bob, $R^{(B)}$ (if the protocol was interrupted before its completion, Alice will guess the rest of Bob’s outcomes; see Appendix for details). Trent measures $2N$
of the 4N particles in his possession – N randomly chosen from the subset $T^A_T$ and other N from $T^B_T$, in the bases given by $h^* = h(M)$ (the other 2N particles are kept for binding the contract for Bob, if requested). He also chooses independently at random $\alpha > 1/2$, according to some publicly known distribution $p(\alpha)$. Trent will give to Alice a certified document declaring the hash value $h^*$ valid ("bind the contract for Alice") if the results $\mathcal{R}^A$ and $\mathcal{R}^B$ satisfy the following two conditions:

(a) at least a fraction $\alpha$ of N Alice’s results from $\mathcal{R}^A_T$ are consistent with Trent’s results on the corresponding entangled N particles from $T^A_T$, and

(b) at least a fraction $\alpha$ of N Bob’s results from $\mathcal{R}^B_T$ are consistent with Trent’s results on the corresponding entangled N particles from $T^B_T$.

The **Binding phase ends with the following:** In case Trent finds Alice’s results consistent with his, she receives an authorized document from Trent declaring the hash value $h^*$ valid, which then allows her to obtain the certified copy of the contract $M$, for which $h^* = h(M)$.

### III. SECURITY DESCRIPTION

Let us define the following probabilities for Alice to pass the above tests (a) and (b), in case the communication was interrupted at step $m$,

\[
P_{BTH}(m; \alpha) = \text{Probability that Bob passes Trent’s test on His own qubits,}
\]

\[
P_{BTA}(m; \alpha) = \text{Probability that Bob passes Trent’s test on Alice’s qubits,}
\]

\[
P_{ATH}(m; \alpha) \text{ and } P_{ATB}(m; \alpha)\]

can be analogously defined as Alice’s probabilities to pass tests (a) and (b). Additionally, we define Bob’s probability to pass Alice’s verification test on the results $\mathcal{R}^A_A \in \mathcal{R}^A_B$ (see step (5) of Section II) received from Alice by step $m$, as

\[
P_{BAS}(m) = \text{Probability that Bob passes Alice’s test on their Shared qubits,}
\]

and, analogously $P_{ABS}(m)$ for Alice.

It is easy to verify that, in the noiseless scenario, the protocol is optimistic. If both clients follow the protocol honestly till the end, both of them are able to enforce the contract: Alice will have all the outcomes of Bob’s measurements in the Honest basis, allowing her to bind the contract with probability 1 (the same happens for Bob).

To analyze the probabilistic fairness quantitatively, we introduce the so-called **probability to cheat**, along the lines of the similar quantity analyzed in [17]. By $P_{bind}(m; \alpha) = P_{BTH}(m; \alpha) \cdot P_{BTA}(m; \alpha)$, we denote the probability that Bob passes Trent’s tests and can thus bind the contract, if the communication is interrupted at step $m$ of the protocol, for a given choice of $\alpha$; and analogously for Alice. To reach step $m$, both clients have to pass each other’s verification, which is given by the probability $P(m) = P_{BAS}(m) \cdot P_{ABS}(m)$. Bob’s probability to cheat at step $m$, for a given $\alpha$, is defined as the probability that he can bind the contract, while Alice cannot, multiplied by the probability to reach step $m$:

\[
P_{ch}(m; \alpha) = P(m) \cdot P_{bind}(m; \alpha) [1 - P_{bind}(m; \alpha)] . \tag{4}
\]

Note that the above probabilities also depend on the particular distribution of entangled pairs, denoted as “configuration $L$”, given by probability $q(L)$, and in case of a dishonest client, the cheating strategy. Also, both the above, as well as *any* probability evaluated (with the exception of $p(\alpha)$) depend of $N$; therefore, we omit to write it, as it is implicitly assumed. Nevertheless, the dependence on configuration $L$ is relevant in calculations, and below we analyze it in detail.

As prescribed by the protocol, Trent gives 6N qubits to Alice – 4N qubits from $A$ and 2N from $T^B_T$ (see Fig. 7), together with their relative positions. Analogously, Bob receives 6N qubits from $B$ and $T^A_T$. We assume that all the classical communications between Trent and clients are private and authenticated, based on, say, pre shared symmetric key schemes. After the communication stopped at step $m$, out of the 4N qubits to measure from $A$ and $B$, Alice and Bob will be left with $\ell^A$ and $\ell^B$ unmeasured qubits, respectively, with $\ell^A = \ell^B = 4N - m$. Note...
that, among the \( \ell^A \) and \( \ell^B \) qubits, not all will be used by Trent to bind the contract for Alice and Bob. In fact, the qubits that are entangled between Alice and Bob are irrelevant for their binding probabilities. They are used by the parties to check each other’s honesty. Let then \( \ell^A \) be decomposed into \( \ell_T^A \) and \( \ell_T^B \), the qubits entangled with those held by Trent and by Bob, respectively. Analogously, let \( \ell^B \) be decomposed into \( \ell_T^B \) and \( \ell_A^B \). Therefore

\[
\begin{align*}
\text{Alice} : (2N + 2N) - m &= \ell^A + \ell^B \\
\text{Bob} : (2N + 2N) - m &= \ell^A + \ell_B
\end{align*}
\]

In order to bind the contract, a client, say Bob, has to present his own measurement results, as well as those obtained from Alice. Then, Trent checks if they are correlated with those obtained on qubits in his possession. Unlike the previous proposal \([17]\), in which both clients had to be present and show their results to Trent in order to both obtain signed contracts during the Binding phase, in the current protocol Bob does not need Alice to be summoned in order to bind the contract (and vice versa). Since the protocol should be symmetric to both clients, it should allow that they both, separately, are able to bind the contract. For this reason, when binding the contract to, say Bob, Trent does not check all of his results from \( \mathcal{T}_T^A \) and \( \mathcal{T}_T^B \) for qubits entangled with \( A \) and \( B \), respectively. Note that to check Bob’s results, Trent has to measure his qubits in the bases given by \( h^* = h(M) \) which is provided by Bob. Therefore, if both clients were using the same sets of qubits (entangled with those in Trent’s possession) to separately bind the contract, a dishonest Bob would have a trivial successful cheating strategy. He measures the Honest observables given by the mutually agreed contract \( M \), which allows him to bind that contract. Nevertheless, in case he later decides not to comply to it, he simply provides Trent with a random \( h' \neq h(M) \). As a consequence, Trent’s results will be uncorrelated to both Bob’s, as well as Alice’s results, i.e., neither client would be able to bind the contract \( M \). This is precisely the reason for checking only \( N \) out of \( 2N \) qubits from \( \mathcal{T}_T^A \) and \( \mathcal{T}_T^B \), each.

Thus, Trent’s qubits are each divided into two equal subsets of the same size, \( \mathcal{T}_T^A = \mathcal{T}_{T1}^A \cup \mathcal{T}_{T2}^A \) and \( \mathcal{T}_T^B = \mathcal{T}_{T1}^B \cup \mathcal{T}_{T2}^B \). the sets with the \( T1 \) subscript are used for binding the contract to Alice, while those with \( T2 \) for Bob. Consequently, we have \( \ell_{T1}^A = \ell_{T1}^A + \ell_{T2}^A \) and \( \ell_{T1}^B = \ell_{T1}^B + \ell_{T2}^B \) (see Fig. 5).

The overall configuration \( \mathcal{L} \) of the entangled pairs distributed between Alice, Bob and Trent is given by six independent numbers,

\[
\mathcal{L} = \left\{ \ell_B^A, \ell_T^A, \ell_T^B, \ell_A^B, \ell_T^B \right\}, \quad \text{with} \quad q(\mathcal{L}) = q(\ell_B^A) \cdot q(\ell_T^A) \cdot q(\ell_T^B) \cdot q(\ell_A^B) \cdot q(\ell_T^1) \cdot q(\ell_T^2).
\]
Therefore, Bob’s probability to cheat, given by equation (4), now written with the explicit dependence on the configuration $\mathcal{L}$, is
\[
P_{ch}^B(m; \alpha|\mathcal{L}) = P(m|\ell_2(A), \ell_2(B)) \cdot P_{bind}(m; \alpha|\ell_{T_2}(A), \ell_{T_2}(B)) \times \left[1 - P_{bind}^A(m; \alpha|\ell_{T_1}(A), \ell_{T_1}(B))\right].
\] (7)

Averaging the “constituent” probabilities from the above equation over their respective configurations from $\mathcal{L}$ gives
\[
P(m) = \langle P_{ABS}(m|\ell(A)) \rangle_{\ell(A)}, \langle P_{BAS}(m|\ell(A)) \langle \ell(B) \rangle \rangle_{\ell(B)},
\]
\[
P_{bind}(m; \alpha) = \langle P_{BTH}(m; \alpha|\ell_{T_2}(A)) \langle \ell_{T_2}(B) \rangle \rangle_{\ell_{T_2}(B)},
\]
\[
P_{bind}^A(m; \alpha) = \langle P_{ATH}(m; \alpha|\ell_{T_1}(A)) \langle \ell_{T_1}(B) \rangle \rangle_{\ell_{T_1}(B)},
\]
where $\langle A \rangle_\ell$ represents the expectation value of $A(\ell)$ over the values of $\ell$. To simplify notation, in the following we will use $P_{ABS}(m) = \langle P_{ABS}(m|\ell(A)) \rangle_{\ell(A)}$ and $P_{BTH}(m; \alpha) = \langle P_{BTH}(m; \alpha|\ell_{T_2}(B)) \langle \ell_{T_2}(A) \rangle \rangle_{\ell_{T_2}(A)}$, and analogously for the other four probabilities from the right hand sides of the above three equations.

Hence, with Bob’s probability to cheat, averaged over all configurations $\mathcal{L}$,
\[
P_{ch}^B(m; \alpha) = \sum_{\mathcal{L}} q(\mathcal{L}) P_{ch}^B(m; \alpha|\mathcal{L})
\]
\[
= P(m) \cdot P_{bind}(m; \alpha) \left[1 - P_{bind}^A(m; \alpha)\right],
\] (9)

we have the expected probability to cheat as
\[
\bar{P}_{ch}^B(m) = \int p(\alpha) P_{ch}^B(m; \alpha) d\alpha.
\] (10)
For honest clients that follow the protocol, the above probability is determined by the steps prescribed by the protocol (the “honest strategy”). In case a client, say Bob, does not follow the protocol, the above probability depends on the “cheating strategy” of a dishonest client. It turns out (see Appendix [A]), that the quantum part of the honest and the optimal cheating strategies are the same, i.e., the (quantum) measurements performed by a cheating Bob are the same as that of an honest one, given by the Honest observables \( \hat{H}_i \). In other words, the best a cheating Bob can do is to send to Alice wrong results determined by a frequency \( f \). This is a consequence of the fact that Bob does not know which of the qubits given to him are used to bind the contract by Trent, and which to check his honesty by Alice (for details, see Appendix [B]).

In Appendix [A] we derive the explicit expressions for the expected probability to cheat \( P_{ch} \) for honest clients that follow the protocol, in the ideal noiseless case (Appendix [A1]), as well as for noisy environments (Appendix [A2]), thus showing the soundness of the protocol. In Figs. [6] (a), (b), (d) and (e) we present the values of the maximal expected probability to cheat as a function of the total number of photons for the values of \( 4N \) up to 6000. In both cases (as well as for the case of a cheating client discussed below), the results are obtained for the uniform \( p(\alpha) \) on the intervals \([0.9, 0.99]\), \([0.8, 0.99]\) and \([0.7, 0.99]\), and with a noise parameter \( \kappa = 0.05 \). The observed dependence \( \max_m P_{ch}^{A/B}(m) \propto N^{-1/2} \) is confirmed by the proof of the asymptotic behavior, \( P_{ch}(m; \alpha) \in \mathcal{O}(N^{-1/2}) \) (see Theorem 1 from Appendix [A]).

In Appendix [B] we evaluated the corresponding probabilities for the case of a cheating client who deviates from the protocol, in the presence of noise. On Figs. [6] (c) and (f), we plot the values of the maximal expected probability to cheat against \( 4N \), for the optimal cheating strategy, showing the same dependence \( \propto N^{-1/2} \). Further, in Appendices [A] and [B] we have analyzed the decrease of the expected probabilities to cheat in case the cheating strategy deviates from the optimal values of \( m \) or \( f \).

IV. PRACTICAL IMPLEMENTATION WITH CURRENT TECHNOLOGY

The protocol introduced in Section [II] assumes that the clients keep their part of entangled pairs for a long time. With current technology, this assumption is quite limiting, as long-term stable quantum memories do not exist. Thus, both Trent, as well as Alice and Bob, are forced to perform the measurements on their respective states as they are produced/arrive. Since Trent is honest, his measurement collapses the respective photons sent to Alice and Bob in one of the four BB84 pure states. Note that, not knowing the message \( M \), Trent measures his particles either in the computational, or the diagonal basis, chosen uniformly at random. The same applies to the honest Alice and Bob.

Thus, the practical problem of long-term stable quantum memories can be overcome by a simple modification: instead of EPR pairs, Trent sends two ordered sets of photons in pure BB84 states, \( |\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\} \), one for Alice and the other for Bob. As soon as the clients receive their particles, they measure on them the Honest observables according to \( h(M) \). Thus, all the information kept by the parties is classical. Trent keeps with him a record of the classical information of the states sent to Alice and Bob, respectively, to use it to check their honesty in the Binding phase. However, the practical implementation of the protocol requires twice as many photons to be sent to the clients, \( 8N \) to each, instead of previous \( 4N \), as now Trent’s choices of the preparation bases are not given by \( h(M) \), but are random. As such, during the Binding phase they will coincide with a client’s measurement choices on about half of the runs only. Thus, in this practical implementation the length of the hash function is \( |h(M)| = 8N \).

From the set of \( 8N \) particles sent to a client, say Alice, Trent randomly chooses \( 4N \) particles, and sends to Bob the classical information about their states and the indices. Bob uses this information to check Alice’s honesty during the Exchange phase. Note that, similarly as when comparing Trent’s with a client’s results (during the Binding phase), here as well on about half of the \( 4N \) cases the preparation bases will coincide with Alice’s measurement bases given by \( h(M) \), and only those Bob can effectively use for verification. Trent sends the analogous information to Alice about the particles sent to Bob.

Once the clients contact Trent and the Initialization phase begins, Trent starts continuously broadcasting photons in BB84 states. After Alice and Bob agree on some contract \( M \), they also agree on the moment when they execute the Exchange phase. However, they need not inform Trent until the final, Binding phase. Trent has to store the classical records of the transmitted BB84 states to Alice and Bob each in a large, but finite, buffer, erasing older values and replacing them with new ones. Therefore, when the clients first contact Trent to use his services, they are informed about the time interval between the Exchange and the Binding phases, after which Trent starts resetting the records. Assuming Trent produces photons at a clock rate of the order of GHz [6], with about 1000 terabyte of classical information storage per contract, he can keep the measurement results for around one week before erasing previous ones. Note that the feature of being able to postpone exchanging the commitments arises only in specific cases, when major investments are involved, and the possibility of a bottleneck scenario arises. It is natural to assume that in such cases both the clients, as well as the agency providing Trent’s assistance, would be willing to spend significant amounts of funds for such services, and invest considerable resources in equipping the premises, respectively. With
the projected decrease in the storage memory prices, the estimated times will only increase in the future.

Although the cheating probability asymptotic behavior $P_{ch}(m; \alpha) \in O(N^{-1/2})$ shows that arbitrarily high levels of security can be achieved, it would be interesting to compare the protocol’s efficiency with today’s technology. Requiring a security level of the order of, say $10^{-6}$, it would need $N \approx 10^{12}$ photons. A single-photon source with rates of the order of GHz [3] would achieve this number in about 15 minutes. While it is indeed not highly efficient, it can still be considered useful, and the future advances in technology will only enhance the protocol’s efficiency. Note though that such high security levels, that would correspond to a 6-digit PIN (Personal Identification Number), are applied only for the most sensitive cases. In the majority of everyday applications, security levels of the order of $10^{-4}$ would suffice (indeed, many of the credit cards have 4 digits long PINs), resulting in much shorter execution times of the order of a second.

Finally, regarding lossy channels, they will only affect the number of received photons, and not the probabilities to cheat. In other words, given certain number of received photons, $N_R$, the security of the protocol would stay the same as in the ideal case of $N = N_R$ emitted photons. Given that the losses are of the form $N_R = 10^{-\alpha L/10} N$, where $L$ is the the distance travelled by photons, requiring the same order of the number of received and emitted photons, say $N_R = N/2$, for $\alpha = 0.2 \text{ km}^{-1}$, one gets the maximal length between the clients of the order of $L_{max} = 15 \text{ km}$. This is already enough to cover the size of medium to large cities, and will only increase in the future. In particular, drastic changes are to be expected with the development of the satellite-based quantum communications [20], which are likely to allow covering large parts of the Earth.

Concerning security, having to measure the photons immediately after receiving them from Trent, makes it harder to cheat, as a dishonest client cannot adjust his/her cheating strategy according to the honest client’s results. Along the lines of the theoretical version, the security analysis of this practical version of the protocol can be, for both noiseless and realistic noisy scenarios, conducted straightforwardly.

V. DISCUSSION AND CONCLUSIONS

We presented a quantum protocol for signing contracts. We showed that, under the realistic assumptions of noise and measurement errors, the protocol is fair, and consequently optimistic as well. Unlike the classical counterparts, the protocol is based on the laws of physics, and the clients do not need to exchange huge number of signed authenticated messages during the actual contract signing process (the Exchange phase). Thus, the protocol is abuse-free: a client cannot prove to be involved in the actual act of signing the contract. In the classical counterparts, having the signed and authenticated messages received during the Exchange phase, a client could show them to other interested clients to negotiate better terms of a financial transaction. In other words, classically a dishonest client can abuse the signing process by falsely presenting his/her interest in the deal, while actually using the protocol to achieve different goal(s). Unlike generic quantum security protocols (say, quantum key distribution), preforming quantum measurements different from those prescribed by the protocol cannot help a cheating client (see Appendix [8] for details). The security mechanism of our protocol is somewhat different from that in standard quantum cryptographic protocols, as learning the states/measurement outcomes of the other client does not help a dishonest client. In the current proposal, each client can independently obtain the signed contract, without the other client being present, which was not possible in [17]. Thus, the probability to cheat is assigned to a real event (whereas in [17], it is just a formal figure of merit). Unlike the classical counterparts (and the previous quantum proposal [17]), when first contacting Trent, the clients do not need to agree upon a definitive contract. Moreover, Trent never learns the actual content of the protocol, as the clients provide Trent its hash value, $h^* = h(M)$, given by publicly known hash function $h$. Finally, we present a version of the protocol that does not rely on stable quantum memories, making it possible to achieve with the current technology.

Acknowledgments

The authors acknowledge the support of SQIG – Security and Quantum Information Group, the Instituto de Telecomunicações (IT) Research Unit, ref. UID/EEA/50008/2013, the IT project QbigD funded by Fundação para a Ciência e Tecnologia (FCT) PEst-OE/EEI/LA0008/2013, the FCT project Confident PTDC/EEL-CTP/4503/2014 and the project QuantumMining POCI-01-0145-FEDER-031826 supported by FCT, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020), and by the Regional Operational Program of Lisbon. AS also acknowledges funds granted to LaSIQE Research Unit, ref. UID/CEC/00408/2013. PY acknowledges the support of DP-PMI and FCT (Portugal) through the scholarship PD/BD/113648/2015. NP acknowledges Aleksandra Dimić for fruitful discussions.
APPENDIX

In this Appendix, we analyze protocol’s security in case the communication is interrupted at step $m$. To proceed to the Binding phase, the two clients measure the Honest observable on the rest of their qubits, thus increasing their probability to pass Trent’s test (a) on qubits shared with him. For the qubits shared between Trent and the other client, used in test (b), the best they can do is to guess their outcomes. Note that this strategy is optimal for both the case of honest clients, studied in Appendix A, as well as for a dishonest client, discussed in Appendix B.

Before discussing protocol’s correctness for the case of honest, and security for dishonest clients, we present the overall set-up: the “configuration” $\mathcal{L}$ and the details of the structure of the figure of merit, the expected probability to cheat for Bob and Alice. We assume the scenario in which the communication is interrupted upon both clients received $m$ measurement outcomes from the other. The biased case of one client having $m$, while the other $m-1$, results is described analogously. A simplified protocol description is given in Fig. 7.

**Appendix A: Probabilistic fairness for honest clients**

In this scenario, we assume that both Alice and Bob are honest until step $m$ after which the communication is interrupted. Without loss of generality, we assume that Alice was the first one to start the information exchange. To analyze the fairness of the protocol, we consider the case when the communication is interrupted after Alice has sent $m$ outcomes to Bob but received only $m-1$ outcomes in return, so Bob has a slight advantage over Alice. The case where both Alice and Bob have $m$ outcomes each is perfectly symmetric (that is, both Bob and Alice have the same expected probability to bind). In this Section, we will analyze the ideal case of a noiseless channel, as well as the protocol’s robustness in the presence of noise.
1. Noiseless channel

In the absence of any noise, both honest Alice and Bob obtain perfect correlations on their respective qubits shared (entangled) with Trent and among themselves. Hence, both clients will, with certainty, pass each other verification tests, \( P_{ABS}(m) = P_{ABS}(m) = 1 \), and thus \( P(m) = P_{ABS}(m) \cdot P_{ABS}(m) = 1 \) (i.e., the reason for communication interruption is the failure of the network). Then, the probability to cheat, say, for Bob is given by

\[
P_{ch}^B(m; \alpha) = P_{bind}^B(m; \alpha) \left[ 1 - P_{bind}^A(m; \alpha) \right].
\]  

(A1)

Moreover, the probabilities for the clients to pass Trent’s test on their own qubits, \( P_{ATH}(m; \alpha) \) and \( P_{BTH}(m; \alpha) \), are also 1. Thus, Bob’s probability to bind the contract is given by

\[
P_{bind}^B(m; \alpha) = P_{BTH}(m; \alpha)P_{ATH}(m; \alpha) = P_{BTH}(m; \alpha)
\]

and analogously for Alice.

Out of the \( m \) correct results that Bob received from Alice (note that we assume ideal noiseless scenario), \( N - \ell_{T2}^{(A)} \) are also relevant when presenting to Trent to prove Alice’s commitment. With a chosen randomly by Trent, let \( \left[ \alpha N \right] \) be the number of correct results corresponding to \( N \) qubits from \( T_{T2}^{(A)} \) and \( T_{T2}^{(B)} \) each, that Trent needs to receive from Bob in order to bind the contract for him. For the case \( \left[ \alpha N \right] \leq N - \ell_{T2}^{(A)} \), Bob already has more than the required number of correct results, hence his probability to bind the contract will be 1. When \( \left[ \alpha N \right] > N - \ell_{T2}^{(A)} \), Bob must correctly guess at least \( n_c = \left[ \alpha N \right] - \left( N - \ell_{T2}^{(A)} \right) \) out of the remaining \( \ell_{T2}^{(A)} \) results to convince Trent to bind the contract for him. Hence, his probability to bind the contract is given by

\[
P_{bind}^B(m; \alpha|\ell_{T2}^{(A)}) = P_{BTH}(m; \alpha|\ell_{T2}^{(A)}) = \begin{cases} 1 & \text{if } \left[ \alpha N \right] \leq N - \ell_{T2}^{(A)} \\ 2^{\ell_{T2}^{(A)}} \sum_{n=n_c}^{\ell_{T2}^{(A)}} \binom{\ell_{T2}^{(A)}}{n} & \text{if } \left[ \alpha N \right] > N - \ell_{T2}^{(A)} \end{cases}
\]

(A3)

Here, \( \binom{\ell_{T2}^{(A)}}{n} \) gives the number of possible choices for \( n \) out of \( \ell_{T2}^{(A)} \), and \( 2^{\ell_{T2}^{(A)}} - 2^{-n} - 2^{-(\ell_{T2}^{(A)} - n)} \) gives the probability of guessing correctly exactly \( n \) results (incorrectly on the rest \( \ell_{T2}^{(A)} - n \) results).

Averaging over \( \ell_{T2}^{(A)} \) gives the binding probability for Bob, as a function of measurement outcomes obtained from Alice, \( m \) (the round of communication interruption), and the parameter \( \alpha \)

\[
P_{bind}^B(m; \alpha) = \sum_{\ell_{T2}^{(A)}} q\left( \ell_{T2}^{(A)} \right) P_{bind}^B(m; \alpha|\ell_{T2}^{(A)})
\]

(A4)

with the probability distribution for \( \ell_{T2}^{(A)} \) given by

\[
q\left( \ell_{T2}^{(A)} \right) = \binom{m}{N - \ell_{T2}^{(A)}} \binom{4N - m}{\ell_{T2}^{(A)}} \binom{4N}{N}
\]

(A5)

To verify the last expression, note that at the \( m \)-th step: (i) there are \( \binom{m}{N - \ell_{T2}^{(A)}} \) ways of choosing the \( N - \ell_{T2}^{(A)} \) results already obtained from Alice; (ii) \( \binom{4N - m}{\ell_{T2}^{(A)}} \) ways of choosing the \( \ell_{T2}^{(A)} \) results from the remaining \( 4N - m \) to guess; (iii) there are \( \binom{4N}{N} \) ways of choosing the \( N \) results, relevant for binding the contract for Bob, from the total \( 4N \) results.

Note that in general \( \ell_{T2}^{(A)} \) takes values from 0 to \( N \), but for the step \( m \) of communication interruption, \( \ell_{T2}^{(A)} \) is constrained to the following values

\[
\ell_{T2}^{(A)} = N - m, \ldots, N \quad \text{for } m < N,
\]

\[
\ell_{T2}^{(A)} = 0, \ldots, N \quad \text{for } N \leq m < 3N,
\]

\[
\ell_{T2}^{(A)} = 0, \ldots, 4N - m \quad \text{for } 3N \leq m.
\]

(A6)
The above ranges define our summation \( \sum_{\ell(A)} \). When \( \ell(A)_{T_2} \) is out of the first or the third range, we have \( m < N - \ell(A)_{T_2} \), and \( 4N - m < \ell(A)_{T_2} \), respectively. Since in those cases the binomials \( \binom{m}{N - \ell(A)_{T_2}} \) and \( \binom{4N - m}{\ell(A)_{T_2}} \) are by definition equal to zero, we can always take the \( \ell(A)_{T_2} = 0, \ldots, N \) range.

By replacing \( m \) with \( m - 1 \) in equation (A5), one obtains Alice’s probability to bind the contract \( P^A_{\text{bind}}(m; \alpha) \) (note that, having one less measurement results than Bob, she therefore has a small disadvantage).

Bob’s probability to cheat (A1), when the communication is interrupted at step \( m \), and for a fixed \( \alpha \), is given by \( P^B_{\text{ch}}(m; \alpha) = P^B_{\text{bind}}(m; \alpha) \left[ 1 - P^A_{\text{bind}}(m; \alpha) \right] \). Using (A4) and its counterpart for Alice one can evaluate the expected probability to cheat \( P^B_{\text{ch}}(m) = \int p(\alpha) P^B_{\text{ch}}(m; \alpha) \) for every \( m \). In Fig. 8, we plot the expected probability to cheat, \( P^B_{\text{ch}}(m) \), against the step of communication interruption \( m \) (running from 1 to 4\( N \)), for the simplest case of the uniform distribution \( p(\alpha) \) on the interval \([0, 0.99]\). Since Alice starts first, and Bob is thus privileged, we have that \( P^A_{\text{ch}}(m) \leq P^B_{\text{ch}}(m) = P_{\text{ch}}(m) \). The maximal value shows the behavior \( \max_m P_{\text{ch}}(m) \propto N^{-1/2} \), as presented in Figs. 6(a) and 6(d), from the main text.

In addition to the quantitative results for up to \( 4N = 6000 \), below we present an analytic proof of the asymptotic behavior for the maximal expected probability to cheat, showing that as \( N \to \infty \) we have \( P_{\text{ch}}(m; \alpha) \propto N^{-1/2} \). The proof for the case of a noisy channel follows analogously (see 14 for the analysis for the contract signing presented in 17).

**Theorem 1.** In the honest noiseless case, for uniformly chosen \( \alpha \in (1/2, 1) \), we have that

\[
P_{\text{ch}}(m; \alpha) \in \mathcal{O}(N^{-1/2}).
\]

**Proof.** We are going to show that for all \( 1 < m < 4N \) and \( \alpha \in (1/2, 1) \) we have that \( P_{\text{ch}}(m; \alpha) \in \mathcal{O}(N^{-1/2}) \) and therefore, the statement follows straightforwardly.

Recall that a Binomial distribution \( B(k, p) \), with \( k \) sufficiently large and \( p \) bounded away from 0 and 1 (that is, does not tend to 0 or 1 as \( N \) grows to infinity), can be approximated by a Normal distribution with mean, \( kp \), and variance, \( kp(1-p) \) as \( N(kp, kp(1-p)) \). In our case (with \( k = \ell(A)_{T_2} \)), for \( \ell(A)_{T_2} \) sufficiently large and \( p = 1/2 \) (guessing probability of a binary bit), the Binomial distribution, \( B(\ell(A)_{T_2}, 1/2) \) can be approximated by \( N(\ell(A)_{T_2}/2, \ell(A)_{T_2}/4) \).

Hence, approximating \( P^B_{\text{bind}}(m; \alpha|\ell(A)_{T_2}) \) for the case \( |\alpha N| > N - \ell(A)_{T_2} \), we have

\[
P^B_{\text{bind}}(m; \alpha|\ell(A)_{T_2}) = 2^{-\ell(A)_{T_2}} \sum_{n=n_c}^{\ell(A)_{T_2}} \binom{\ell(A)_{T_2}}{n} \approx \int_{n_c}^{\infty} \sqrt{2\pi\sigma^2} e^{-\frac{(n-n_c)^2}{2\sigma^2}} dn = \frac{1}{2} \text{erfc} \left[ \sqrt{\frac{2}{\ell(A)_{T_2}}} \left( n_c - \frac{\ell(A)_{T_2}}{2} \right) \right],
\]

with \( n_c = |\alpha N| - (N - \ell(A)_{T_2}) \), and Binomial mean and variance given by \( \mu_B = \ell(A)_{T_2}/2 \) and \( \sigma_B^2 = \ell(A)_{T_2}/4 \), respectively.
Therefore
\[
P_{\text{bind}}^B(m; \alpha|\ell_T^{(A)}) \approx \begin{cases} 
1 & \text{if } |\alpha N| \leq N - \ell_T^{(A)}, \\
\frac{1}{2} \text{erfc} \left[ \frac{2}{\ell_T^{(A)}} \left( N(\alpha - 1) + \frac{\ell_T^{(A)}}{2} \right) \right] & \text{if } |\alpha N| > N - \ell_T^{(A)},
\end{cases}
\] (A8)

where \text{erfc}(\beta) is the complementary error function, defined as
\[
\text{erfc}(\beta) = \frac{2}{\sqrt{\pi}} \int_{\beta}^{\infty} e^{-\gamma^2} d\gamma.
\] (A9)

For the case \(|\alpha N| > N - \ell_T^{(A)}\), we expand \(P_{\text{bind}}^B(m; \alpha|\ell_T^{(A)})\) around \(\ell_T^{(A)} = 2N(1 - \alpha)\) where it has the value 1/2, to obtain
\[
\frac{1}{2} \text{erfc} \left[ \frac{2}{\ell_T^{(A)}} \left( N(\alpha - 1) + \frac{\ell_T^{(A)}}{2} \right) \right] = \frac{1}{2} + c_1(\ell_T^{(A)} - 2N(1 - \alpha)) + c_2(\ell_T^{(A)} - 2N(1 - \alpha))^2 + O((\ell_T^{(A)} - 2N(1 - \alpha))^3). \tag{A10}
\]

Let \(P_1(m; \alpha|\ell_T^{(A)}) = \frac{1}{2} + c_1(\ell_T^{(A)} - 2N(1 - \alpha)) + c_2(\ell_T^{(A)} - 2N(1 - \alpha))^2\). We also obtain the limits for \(\ell_T^{(A)}\) where this function becomes 1 and 0, denoted by \(\ell_{\text{inf}}^{(A)}\) and \(\ell_{\text{sup}}^{(A)}\), respectively.

We know that
\[
P_{\text{bind}}^B(m; \alpha) = \sum_{\ell_T^{(A)}} q\left(\ell_T^{(A)}\right) P_{\text{bind}}^B(m; \alpha|\ell_T^{(A)}),
\tag{A11}
\]

with the probability distribution for \(\ell_T^{(A)}\) given by
\[
q\left(\ell_T^{(A)}\right) = \frac{\left(\frac{m}{N} - \ell_T^{(A)}\right) \left(\frac{4N - m}{\ell_T^{(A)}}\right)}{4N}. \tag{A12}
\]

By Feller’s result \cite{10} on the approximation of hypergeometric distribution, one can approximate \cite{12} for \(N \to \infty\), \(\frac{N}{4N} \to t \in (0, 1)\) to a Normal distribution as
\[
q(\ell_T^{(A)}) \sim \frac{e^{-\left(\ell_T^{(A)} - \mu_{\ell}\right)^2/2\sigma_{\ell}^2}(1-t)}{\sqrt{2\pi\sigma_{\ell}^2(1-t)}} = P_2(\ell_T^{(A)}), \tag{A13}
\]

with mean, \(\mu_{\ell} = N - m/4\), variance, \(\sigma_{\ell}^2 = N\left(\frac{m}{4N}\right)^2\left(\frac{4N - m}{4N}\right)^2\), and \(t = 1/4\). Hence, \(\text{(A11)}\) can be upper bounded (shifting the limit \(\ell_T^{(A)} = N(1 - \alpha)\) to \(\ell_T^{(A)} = \ell_{\text{inf}}^{(A)}\) and using the approximation \(\text{(A10)}\) from \(\ell_{\text{inf}}^{(A)}\) to \(\ell_{\text{sup}}^{(A)}\) by
\[
P_{\text{bind}}^B(m; \alpha) \leq \int_{\ell_{\text{inf}}^{(A)}}^{\ell_{\text{sup}}^{(A)}} P_2(\ell_T^{(A)}) \, d\ell_T^{(A)} + \int_{\ell_{\text{inf}}^{(A)}}^{\ell_{\text{sup}}^{(A)}} P_2(\ell_T^{(A)}) \cdot \left[ P_1(m; \alpha|\ell_T^{(A)}) + k \left(\ell_T^{(A)} - 2N(1 - \alpha)\right)^3 \right] \, d\ell_T^{(A)}
\]

\[
\leq \int_{\ell_{\text{inf}}^{(A)}}^{\ell_{\text{sup}}^{(A)}} P_2(\ell_T^{(A)}) \, d\ell_T^{(A)} + O(N^{-1/2}), \tag{A14}
\]

where the \(O(N^{-1/2})\) in Eq. \(\text{(A15)}\) was obtained by computing limits for \(B_1\) and \(B_2\) for \(N \to \infty\) with the Mathematica software package. To compute the limit for \(B_1\), from \cite{4} we used the fact that by change of variable \(N = 1/x\), if \(\lim_{x \to 0^+} f(x) = 0\) then \(\lim_{N \to \infty} f(N) = 0\) and obtained the desired bound. For computing \(B_2\), we upper bounded \(P_{\text{bind}}^B(m; \alpha|\ell_T^{(A)})\) by \(\frac{1}{2} \text{erfc}|\lambda N|\) for some constant \(\lambda > 0\) and used the upper bound for complementary error function, which also led to the \(O(N^{-1/2})\) bound.
To obtain the expression for Alice’s probability to bind, $P_{\text{bind}}^A(m;\alpha)$, we have

$$q\left(\ell_{T_1}^{(B)}\right) = \frac{m - 1}{N - \ell_{T_1}^{(B)}} \left(\frac{4N - m + 1}{\ell_{T_1}^{(B)}}\right) \left(\frac{4N}{N}\right).$$  \hspace{1cm} (A16)

Making the same approximations, we get $P_2\left(\ell_{T_1}^{(B)}\right)$ similar to (A13), with $m$ replaced by $m - 1$. Hence

$$P_{\text{bind}}^A(m;\alpha) \geq \int_0^{\ell_{inf}} P_2(\ell_{T_1}^{(B)} \ell_{T_1}^{(B)}) - \int_0^{\ell_{inf}} (1 - P_{\text{bind}}^A(m;\alpha|\ell_{T_1}))P_2(\ell_{T_1}^{(B)}) \ell_{T_1}^{(B)} \right) \ell_{T_1}^{(B)} \right) \right) + \int_0^{\ell_{inf}} P_2(\ell_{T_1}^{(B)}) P_{\text{bind}}^A(m;\alpha|\ell_{T_1}) \ell_{T_1}^{(B)} \right) \right).$$  \hspace{1cm} (A17)

$$\geq \int_0^{\ell_{inf}} P_2(\ell_{T_1}^{(B)}) \ell_{T_1}^{(B)} - O(N^{-1/2}),$$  \hspace{1cm} (A18)

where the bounds in Eq. (A18) was obtained with the help of the Mathematica software package. Since we are computing the lower bound, one can drop $A_2$ and it suffices to show that the integral of $A_1$ computed between $N(1 - \alpha)$ (as $P_{\text{bind}}^A(m;\alpha|\ell_{T_1})$ is 1 upto $N(1 - \alpha)$) and $\ell_{inf}$ vanishes when $N \to \infty$. Since $(1 - P_{\text{bind}}^A(m;\alpha|\ell_{T_1})) < 1$, we can drop this and compute the limit of the integral of $P_2(\ell_{T_1}^{(B)})$, which also provides the bound.

If the communication was interrupted at step $m$, for all choices of $\alpha \in (1/2, 1)$ by Trent, we want to compute, say for Bob, the probability to cheat, given by

$$P_{\text{ch}}^B(m;\alpha) = P_{\text{bind}}^B(m;\alpha) \left[1 - P_{\text{bind}}^A(m;\alpha)\right]$$  \hspace{1cm} (A19)

$$\leq \left[\int_0^{\ell_{inf}} P_2(\ell_{T_2}^{(A)}) \ell_{T_2}^{(A)} + O(N^{-1/2})\right] \left[1 - \int_0^{\ell_{inf}} P_2(\ell_{T_1}^{(B)}) \ell_{T_1}^{(B)} + O(N^{-1/2})\right]$$  \hspace{1cm} (A20)

$$= O(N^{-1/2}),$$  \hspace{1cm} (A21)

where the $O(N^{-1/2})$ in Eq. (A21) was again obtained by computing a limit with the Mathematica software package.

\[ \square \]

2. Noisy channel

For the case of a noisy channel, a binomial test could be used by both parties for the permitted number of wrong results from the other party. Consider white noise in the channel that decreases the degree of correlation between the honest clients’ results. The depolarizing channel, modeling the effects of white noise on a two-qubit mixed state $\rho$, is given by ($I$ is the identity matrix for dimension 4, and $\kappa \in [0, 1]$):

$$\mathcal{E}_d(\rho) = (1 - \kappa)\rho + \kappa\frac{I}{4}.$$  \hspace{1cm} (A22)

Hence, both Alice and Bob receive some inevitable number of incorrect results, due to the noise considered, in spite of both of them measuring their respective qubits in the Honest basis. Let us denote by $p(xy)$ the probability of Alice and Bob obtaining the results $x$ and $y$, respectively, corresponding to measurements of $\mathcal{E}_d(\rho)$ in either computational or diagonal basis, for the case of the entangled two-qubit state $\rho = |\psi^+\rangle\langle\psi^+|$. Given both Alice and Bob measure the correct observable, that is, $H_i$, we have the following probabilities of obtaining different results

$$p(00) = (2 - \kappa)/4,$$

$$p(01) = \kappa/4,$$

$$p(10) = \kappa/4,$$

$$p(11) = (2 - \kappa)/4.$$  \hspace{1cm} (A23)
For a given probability of the favorable event (in our case, \(p(00) + p(11)\), of obtaining consistent results), and the total number of such events (say, \(m_r\)), the probability of obtaining exactly \(r\) correct results is given by the binomial distribution

\[
P(r|\psi^+; m_r, \kappa) = \binom{m_r}{r} \left(p(00) + p(11)\right)^r \left(p(01) + p(10)\right)^{m_r-r},
\]

with mean and variance given by

\[
\mu = m_r \left(p(00) + p(11)\right) = m_r \left(1 - \frac{\kappa}{2}\right),
\]

\[
\sigma^2 = m_r \left(p(00) + p(11)\right) \left(1 - p(00) - p(11)\right) = m_r \left(1 - \frac{\kappa}{2}\right) \frac{\kappa}{2}.
\]

Suppose that each party applies a 3-sigma “acceptance criterion”, then a client will continues as long as he/she has at least \(\mu - 3\sigma\) consistent results from the other.

From [8], Bob’s probability to bind the contract is \(P_{\text{bind}}^B(m; \alpha) = \langle P_{BTB}(m; \alpha|\ell_{T_2}^{(B)}) \rangle \cdot \langle P_{BTA}(m; \alpha|\ell_{T_2}^{(A)}) \rangle\).

While Bob’s probability to pass the test on his qubits, \(P_{BTB},\) does not depend on step \(m\) nor on \(\ell_{T_2}^{(B)}\) (he measures all of his qubits), the probability to pass the test on Alice’s qubits, \(P_{BTA}\), depends on \(m\), as well as on \(\ell_{T_2}^{(A)}\) (for simplicity, we omit the implicit dependence on the noise parameter \(\kappa\)). Thus, we have

\[
P_{\text{bind}}^B(m; \alpha) = P_{BTB}(\alpha) \cdot \langle P_{BTA}(m; \alpha|\ell_{T_2}^{(A)}) \rangle \cdot \ell_{T_2}^{(A)},
\]

with

\[
P_{BTB}(\alpha) = \sum_{s=\lfloor \alpha N \rfloor}^{N} {\binom{N}{s}} \frac{P_s}{P_{\neq}},
\]

where \(P_{\neq} = p(00) + p(11)\) and \(P_{\neq} = p(10) + p(01)\). Analogously, we define \(P_{\text{bind}}^A(m; \alpha) = P_{ATH}(\alpha) \cdot \langle P_{BTH}(m; \alpha|\ell_{T_2}^{(B)}) \rangle \cdot \ell_{T_2}^{(B)}\) for Alice.

To obtain Bob’s probability to cheat [9], \(P_{\text{ch}}^B(m; \alpha) = P(m)P_{\text{bind}}^B(m; \alpha) \left[1 - P_{\text{bind}}^A(m; \alpha)\right]\), we now estimate \(P(m) = P_{ABS}(m) \cdot P_{BAS}(m)\). \(P_{BAS}(m)\), the probability that Bob passes Alice’s tests on their Shared qubits (from the \(m - 1\) results sent by him to Alice). Note that, in order to reach at step \(m\), Bob has to pass the test at all the steps 2, \(\ldots\), \(m - 2\), \(m - 1\). Thus, we can bound \(P_{BAS}(m)\) from above by the probability to pass Alice’s test at step \(m - 1\) only

\[
P_{BAS}(m) = \sum_{\ell_{T_2}^{(B)}} q(\ell_{T_2}^{(B)}) \times \sum_{v=\mu-3\sigma}^{2N-\ell_{T_2}^{(B)}-v} {\binom{2N-\ell_{T_2}^{(B)}}{v}} P_v \cdot P_{\neq}^{2N-\ell_{T_2}^{(B)}-v} P_{\neq},
\]

with \(\mu\) and \(\sigma\) defined by [A25], where \(m_r = 2N - \ell_{T_2}^{(B)}\). The probability distribution for \(\ell_{T_2}^{(B)}\) given by

\[
q(\ell_{T_2}^{(B)}) = \frac{m_r - 1}{2N} \binom{4N - m + 1}{\ell_{T_2}^{(B)}} \frac{4N}{2N}.
\]
FIG. 9: Honest scenario (noisy channel): the expected probability to cheat, $P_{ch}(m)$, is plotted against the step of communication interruption $m$ (from 1 to $4N$), for $\alpha$ chosen uniformly over the interval [0.9, 0.99]. The noise parameter is $\kappa = 0.05$.

$P_{ABS}(m)$, the probability that Alice passes Bob’s test on their Shared qubits (from the $m$ results she sends to Bob), as well as its bound $P_{ABS}(m)$, are defined analogously. Thus, the overall probability to reach at step $m$ is given by $P_{ABS}(m) \cdot P_{BAS}(m) \leq P_{ABS}(m) \cdot P_{BAS}(m)$.

Hence, the average probability for Bob to cheat, with both Alice and Bob having reached the step $m$ by passing each other’s tests, is

$$P_{ch}^B(m) \leq P_{ABS}(m) \cdot P_{BAS}(m) \int_\alpha p(\alpha) P_{bind}^B(m; \alpha) \left(1 - P_{bind}^A(m; \alpha)\right) \, d\alpha.$$  \hspace{1cm} (A31)

In Fig. 9 we present the expected probability to cheat, $P_{ch}(m)$, plotted against the total number of communications between Alice and Bob, $4N$, for the 3-sigma acceptance criterion of both Alice and Bob (as before, $p(\alpha)$ is uniform on the interval [0.9, 0.99]). The maximal value again shows the behavior $\max_m P_{ch}(m) \propto N^{-1/2}$, as presented in Figs. 9(b) and 9(c), from the main text.

Appendix B: Security analysis (probabilistic fairness) against a dishonest client

In order to cheat, a dishonest client, say Bob, would want to obtain a signed copy of the contract for message $M$ that Alice and Bob initially agreed upon, without letting Alice obtain a signed copy for herself, so that he can use it later on, if he wants to.

The qubits from $\mathcal{T}_B^{(A)}$ are used to verify Alice’s honesty, and therefore Bob measures them according to the protocol (note that he knows which qubits from $\mathcal{A}$ are entangled with $\mathcal{T}_B^{(A)}$). Regarding qubits from $\mathcal{B}$, unlike the standard quantum cryptographic protocols, where the task of an adversary (say Eve, in key distribution schemes) is to distinguish between mutually non-orthogonal states, in this protocol a cheating Bob knows the pure states of his qubits: he knows which observables Trent and an honest Alice measure, and thus by measuring that observable can check which of the two mutually orthogonal states they (will) collapse his system to. Note that Bob cannot take advantage of measuring observables different from those prescribed by the protocol. Since Alice’s and Bob’s measurements are local, they commute and thus their time order is irrelevant. Thus, by deviating from the protocol, a dishonest Bob can only spoil the correlations between his and Alice’s outcomes, a task he can achieve by any random source. Regarding Trent, the time ordering matters, as it is Bob who tells Trent which single-qubit observables to measure. Nevertheless, since Bob’s aim is to have his results as correlated as possible with Trent’s, without spoiling the correlations established with Alice’s results, Bob should measure all the qubits from $\mathcal{B}$ according to the protocol.

As argued above, for a cheating client Bob, even knowing to which states the particles sent to him are collapsed to (due to Alice’s and Trent’s measurements), does not help. This is because he still does not know which of those particles are entangled with Alice and which ones are with Trent. Bob’s cheating strategy should allow him to bind the contract, such that Alice is unable to bind the contract even with Trent’s help. In order to bind the contract for himself, Bob must pass the test by providing to Trent at least a fraction $\alpha$ of correct measurement results on the qubits entangled with $\mathcal{T}_T^{(A)}$, as well as $\mathcal{T}_T^{(B)}$, respectively. At the same time, Bob does not want Alice to pass the test on the results sent by him (corresponding to qubits entangled with $\mathcal{T}_T^{(B)}$) to her. Making measurements in a basis other than the Honest basis on some of the qubits and sending those results to Alice does not help him in any
way, because then he ends up with incorrect results on some of his qubits in $T_{T2}^{(B)}$ entangled with Trent. While these incorrect results will spoil Alice’s chances to bind the contract, they will equally decrease Bob’s chances too. Hence, the best strategy is to measure all his qubits in Honest basis to pass the test on all $T_{T2}^{(B)}$ qubits, and send random bits to Alice, by choosing a random probability $f$ to decide whether or not to flip the result that he sends to Alice (the frequency of sending wrong results). Therefore, the probability for Alice to obtain correct results on these qubits will be

$$\tilde{P}_c = (1-f)P_+ + fP_{\neq},$$  \hspace{1cm} (B1)$$

where $P_+ = p(00) + p(11)$ and $P_{\neq} = p(10) + p(01)$.

The communication is interrupted at step $m$, after Alice stops sending the measurement outcomes to Bob upon suspecting a dishonest behavior. Recall that we are considering the case where Alice is the first one to start the communication, and therefore, in the worst case scenario after the $m$-th step Alice and Bob each have $m$ measurement results from each other.

With $m$ measurement results each, the probability for Alice and Bob to pass Trent’s test on her/his own qubits, $P_{ATH}(\alpha)$ and $P_{BTH}(\alpha)$ respectively, remains the same as in the honest noisy case. Since Bob decides to flip the results randomly, based on $f$, he is bound to send wrong results on some of the qubits. Hence, Alice receives more incorrect results from Bob as compared to the honest noisy case. Bob on the other hand receives the same number of correct results as in the honest noisy case. Therefore, $P_{ATS}(m)$ and $P_{BTA}(m; \alpha)$ remain the same, while $P_{ATH}(m; \alpha)$ and $P_{BAS}(m)$ are modified by replacing $P_+$ and $P_{\neq}$ by $\tilde{P}_c$ and $\tilde{P}_{\neq} = 1 - \tilde{P}_c$ \hspace{1cm} [B1].

The expected probability to cheat, $\tilde{P}_{ch}(m, f)$, is plotted in Fig. 10. The same behavior (as in the case of honest clients), $\max_{m,f} \tilde{P}_{ch}(m, f) \propto N^{-1/2}$, is observed, as in Figs. 6(c) and 6(f) from the main text.

\[ \]

[1] Á. J. Almeida, A. D. Stojanović, N.á Paunković, R. Loura, N. J. Muga, N. A. Silva, P. Mateus, P. S. André, and A. N. Pinto. Implementation of a two-state quantum bit commitment protocol in optical fibers. Journal of Optics, 18(1):015202, 2016.
[2] N. Asokan, M. Schunter, and M. Waidner. Optimistic protocols for fair exchange. In Proceedings of the 4th ACM conference on Computer and communications security, pages 7–17. ACM, 1997.

[3] N. Asokan, V. Shoup, and M. Waidner. Optimistic fair exchange of digital signatures. Advances in Cryptology EUROCRYPT ’98, pages 591–606, 1998.

[4] Michael Beeson and Freek Wiedijk. A rigorous theory of infinite limits. 10 2000.

[5] M. Ben-Or, O. Goldreich, S. Micali, and Ronald L. Rivest. A fair protocol for signing contracts. IEEE Transactions on Information Theory, 36(1):40–46, 1990.

[6] Alberto Boaron, Boris Korzh, Raphael Houlmann, Gianluca Bosco, Davide Rusca, Stuart Gray, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Simple 2.5 ghz time-bin quantum key distribution. Applied Physics Letters, 112(17):171108, 2018.

[7] S. Even. A protocol for signing contracts. ACM SIGACT News, 15(1):34–39, 1983.

[8] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. Communications of the ACM, 28(6):637–647, 1985.

[9] S. Even and Y. Yacobi. Relations among public key signature systems. Technical Report, page 175, 1980. (unpublished).

[10] William Feller. An Introduction to Probability Theory and its Applications: Volume 1. J. Wiley & Sons: New York, 1968.

[11] Michael J. Fischer, Nancy A. Lynch, and Michael S. Paterson. Impossibility of distributed consensus with one faulty process. Journal of the ACM (JACM), 32(2):374–382, 1985.

[12] Juan A. Garay, M. Jakobsson, and P. MacKenzie. Abuse-free optimistic contract signing. In Annual International Cryptology Conference, pages 449–466. Springer, 1999.

[13] O. Goldreich. A simple protocol for signing contracts. In Advances in Cryptology, pages 133–136. Springer, 1984.

[14] Hana Almoner Louka. Necessity of parameter randomization in quantum contract signing. Matematički Vesnik, 69:65–74, 2017.

[15] R. Loura, Álvaro J. Almeida, Paulo S. André, Armando N. Pinto, P. Mateus, and N. Paunković. Noise and measurement errors in a practical two-state quantum bit commitment protocol. Phys. Rev. A, 89:052336, May 2014.

[16] R. Loura, D. Arsenović, N. Paunković, Duška B. Popović, and S. Prvanović. Security of two-state and four-state practical quantum bit-commitment protocols. Phys. Rev. A, 94:062335, Dec 2016.

[17] N. Paunković, J. Bouda, and P. Mateus. Fair and optimistic quantum contract signing. Physical Review A, 84(6):062331, 2011.

[18] Michael O. Rabin. Transaction protection by beacons. Journal of Computer and System Sciences, 27(2):256–267, 1983.

[19] H. Situ, D. Qiu, P. Mateus, and N. Paunković. Secure n-dimensional simultaneous dense coding and applications. International Journal of Quantum Information, 13(07):1550051, Oct 2015.

[20] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. Science, 356(6343):1140–1144, 2017.